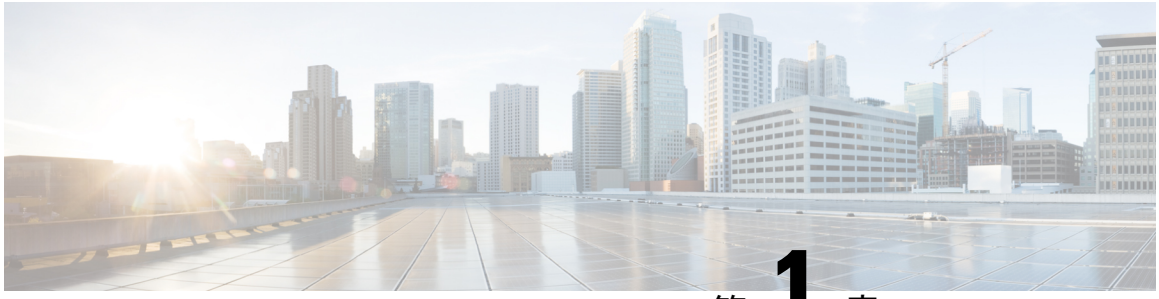
Cisco Expressway 管理者ガイド（X14.0）

初版：2021 年 4 月 12 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

目 次



第 1 章

はじめに

変更履歴

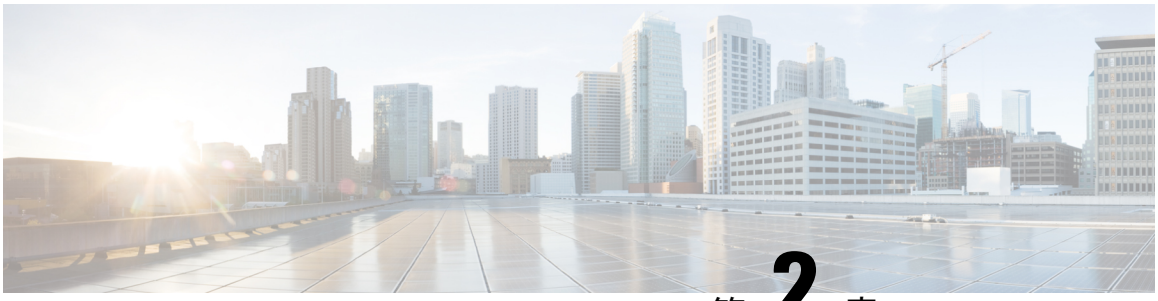
表 *1 :* 管理者ガイドの変更履歴

日付	変更内容	理由
2020 年 12 月	X12.7 の更新。	X12.7 リリース
2020 年 10 月	• 事前設定済みのゾーンで、日付の設定の欠落および古い設定を更新します。 • HSM について重複しているコンテンツを削除します。 • 外部またはサードパーティ製のゲートキーパが、RMS ライセンスを使用する場合の意味を明確化します。	ドキュメントの訂正
2020 年 10 月	事前設定済みのゾーンで、日付の設定の欠落および古い設定を更新します。	ドキュメントの訂正
2020 年 10 月	X12.6.4 メンテナンスリリースの更新（ソフトウェア バグ ID CSCvv92477 の修正 - H.323-SIP インターワーキング用に設定可能な DH キー長）。 **厳格なパスワード**を適用すると 、X12.6 以降、ローカルの管理者アカウントに適用されるのではなく、すべてのローカルで管理されているアカウントに適用されるという反映を反映する「パスワードセキュリティの設定」トピックの変更。	X12.6.4 メンテナンスリリース/ドキュメント修正
2020 年 8 月	X12.6.2 メンテナンス リリースを更新。	X12.6.2 メンテナンス リリース

日付	変更内容	理由
2020 年 7 月	ロギングと有用性に関連したコンテンツを再構築し、旧 Expressway Serviceability Guide を含む、このガイドに統合されたコンテンツを統合します。また、トラブルシューティングおよび診断情報を独自の章に再組み込みします。	ドキュメントの再編成
2020 年 7 月	MRA 登録数を含む X12.6.1 メンテナンスリリースの更新。Expressway-E TURN サーバは、汎用 STUN サーバとして機能しなくなりました。	X12.6.1 メンテナンス リリース
2020 年 6 月	STUN パケット内の IP アドレスの不一致が発生した場合について説明するため、「ファイアウォールトラバーサル」 項を更新します。	ドキュメントの説明
2020 年 6 月	X12.6 の更新で、Web UI に表示されない場合は、「[アプリケーション (Applications]」 メニューを復元するプロセスを追加します。	X12.6 リリース
2020 年 2 月	「Kari の法則」を含む X12.5.7 メンテナンスリリースの更新。 （注） X12.5.7 は廃止され、X12.5.9 に置き換えられました。 CE1200 アプライアンスのオプションキーを明確化。	X12.5.7 メンテナンス リリース
2020 年 1 月	クラスタ ライセンスの使用方法とキャパシティのガイドライン セクションを更新。小規模 VM のクラスタからキャパシティは得られないことを明確化。	ドキュメントの訂正
2019 年 12 月	製品に他のソフトウェアをインストールしないことを明確化。 VM サイズ フィールドの場所を修正。	ドキュメントの説明 ドキュメントの訂正
2019 年 11 月	X12.5.6 メンテナンス リリースを更新。	X12.5.6 メンテナンス リリース
2019 年 7 月	X12.5.4 に関する内容を更新。X8.6.x 以降のソフトウェア上のシステムを 12.5.4 以降にアップグレードする必要がないため、リリース キーへの参照を削除。 「ネットワーク サービス」セクションの「「HTTP リクエストを HTTPS にリダイレクト」」のデフォルト値の誤りを修正。CSCvq39362 を参照してください。	X12.5.4 リリース
2019 年 6 月	RMS ライセンス消費テーブルが更新され、RMS ライセンスを消費するシナリオのみが含まれるようになりました。	ドキュメントの訂正

日付	変更内容	理由
2019 年 5 月	Meeting Server のロード バランシング設定に関する説明で、488 レスポンス コードへの誤った参照を修正。	ドキュメントの訂正
2019 年 4 月	X 12.5.2 メンテナンス リリースの更新（VMware ESXi プラットフォーム上で仮想化された小規模 VM のサポートが含まれています）。	X12.5.2 メンテナンス リリース
2019 年 3 月	X12.5.1 メンテナンス リリースを更新。	X12.5.1 メンテナンス リリース
2019 年 2 月	表「「同時にホストできるサービス」」を「概要」セクションに復帰。	ドキュメントの訂正
2019 年 1 月	X12.5 の更新。	X12.5 リリース
2018 年 12 月	X8.11.4 の表題を変更（実質的な更新なし）。CSCvn73111 の B2BUA コール ステータスに関するセクションを調整。	X8.11.4 メンテナンス リリース
2018 年 10 月	X8.11.3 メンテナンス リリースを更新。	X8.11.3 メンテナンス リリース（破棄）
2018 年 9 月	Webex と Spark プラットフォームのリブランド、CE1200 アプライアンス、および X8.11.1 リリースに応じて更新。	X8.11.1 リリース（破棄）
2018 年 7 月	X8.11 の更新。	X8.11 リリース（破棄）
2017 年 7 月	X8.10 の更新。	X8.10 リリース
2017 年 1 月	全般的な訂正と更新。新しい機能を追加。	X8.9.1 メンテナンス リリース
2016 年 12 月	新しい機能と全体的な訂正。	X8.9 リリース
2016 年 9 月	新しいコールポリシールールの設定を含むヘルプと管理者ガイドの更新。	X8.8.2 メンテナンス リリース
2016 年 7 月	MRA の概要を訂正および Xconfig SIP Advanced CLI コマンドを追加。	X8.8 ドキュメントの訂正

日付	変更内容	理由
2016 年 6 月	X8.8 の更新。	X8.8 リリース
2016 年 4 月	全般的な訂正と更新。新しい機能を追加。	X8.7.2 メンテナンス リリース
2016 年 2 月	全般的な訂正と更新。マニュアルの変更履歴（この表）を追加。DNS ゾーン パラメータとアラーム リファレンスを更新。	X8.7.1 メンテナンス リリース



第 2 章

このバージョンの新機能

このバージョンの新機能

ソフトウェア バージョン X 12.5 以降の新機能は、Cisco VCS ではサポートされておらず、Cisco Expressway 製品のみに適用されます。VCS システムの場合、このバージョンはメンテナンスおよびバグ修正のみを目的として VCS に用意されています。

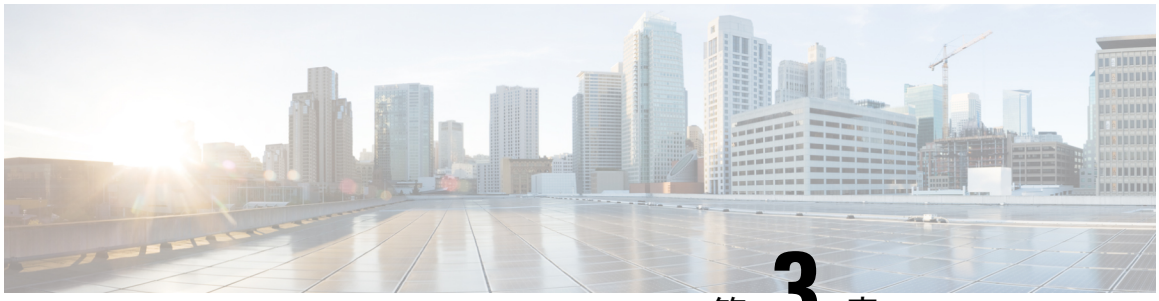
表 *2:* リリース番号別の機能

機能/変更	ステータス（Status）
専用管理インターフェイス	X12.7 以降でサポート
MRA のファストパス登録（登録のためのキャッシング最適化）	X12.7 以降でサポート
Webex VDI for MRA	X12.7 以降でサポート
仮想化システム - ESXi 7.0 認定	X12.7 以降でサポート
ハードウェア セキュリティ モジュール（HSM）のサポート	プレビュー
MRA SIP 登録フェールオーバー（電話 HA サポート）	プレビュー
MRA モバイルアプリケーション管理クライアント	プレビュー
IM&P 用の MRA Android プッシュ通知パブリッシャー	プレビュー（X12.6.2 からはデフォルトで無効）
Cisco Contact Center の MRA ヘッドセット機能	プレビュー

このバージョンの新機能

詳細情報

特定の機能については、該当するソフトウェア バージョンのリリース ノートを参照してください。



第 3 章

はじめに

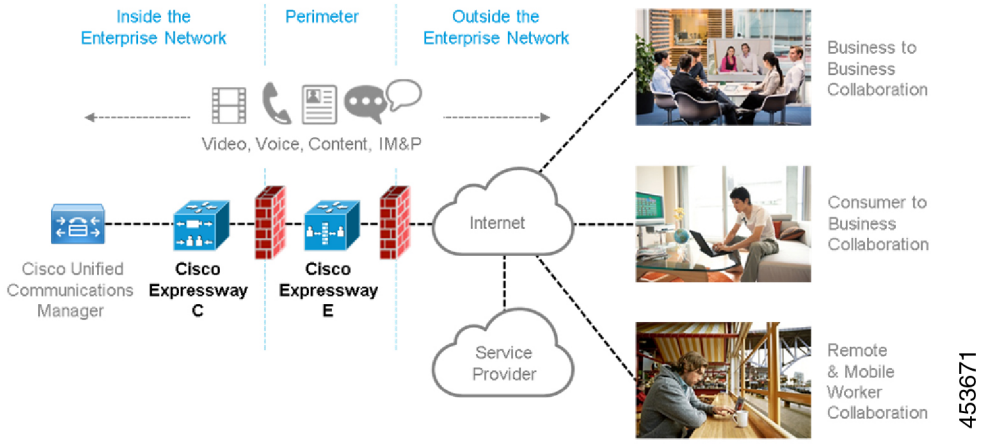
Expressway について

Cisco Expressway シリーズ（Expressway）は、幅広いコラボレーションサービスを目的として特別に設計されています。Cisco Expressway は、確立されたファイアウォール トラバーサル テクノロジーを採用し、従来のエンタープライズコラボレーションの境界を再定義します。当社の Any-to-Any コラボレーションのシスコのビジョンに対応しています。

Expressway の主な機能と利点は次のとおりです。

- 高度にセキュアなファイアウォールトラバーサル技術を提供します。
- 企業間、ビジネス対コンシューマ、およびビジネス対クラウドサービスプロバイダーの接続を容易化します。
- 個別の VPN クライアントを必要とせずに、リモートワーカーのコラボレーションサービスへのセッションベースのアクセスを容易にします。
- スマートフォン、タブレット、デスクトップ用の Cisco Jabber により、幅広い範囲のデバイスをサポートします。
- リモートおよびモバイルワーカーのための個人所有デバイスの持ち込みの戦略やポリシーを補完します。

典型的な Expressway は、Unified CM へのトランク側と回線側の接続を備えた Expressway-C と、DMZ に配置して Expressway-C へのトラバーサル ゾーンを設定する Expressway-E のペアで展開されます。



Expressway は CE12100 などの専用物理アプライアンスで使用することも、Cisco UCS サーバ上で仮想マシン（VM）として使用することもできます。

Expressway のタイプ

各 Expressway はさまざまな機能を提供する 2 つのタイプのいずれかとして設定できます。

Expressway-C

Expressway-C は、エニーツーエニーのエンタープライズ規模の会議およびセッションの管理機能、およびインターワーキング機能を提供します。Session Initiation Protocol（SIP）準拠のエンドポイントや H.323 準拠のエンドポイント間でのインターワーキングや、サードパーティ製エンドポイントとのインターワーキングが可能になり、テレプレゼンス会議の対象範囲が広がります。Unified CM と統合すると、サードパーティ製 IP 構内交換機（IP PBX）ソリューションをサポートすることができます。Expressway-C により、ルーティング、ダイヤル プラン、および帯域幅使用率の定義などを含む、クリエイティブなセッション管理に必要なツールが実装されると同時に、組織レベルの要件に合わせてカスタマイズされたコール管理アプリケーションの定義が可能になります。

Expressway-E

Expressway-E は Expressway-E と一緒に導入され、社外とのスムーズなビデオ通信を簡単かつ安全に実現します。Business-to-Business（B2B）のビデオ コラボレーションを可能にし、リモート ワーカーや自宅ワーカーの生産性を向上させ、サービス プロバイダーによる顧客へのビデオ通信の提供を可能にします。このアプリケーションは、すべての SIP デバイスと H.323 デバイス向けの各種の標準規格に準拠し、かつ、セキュアなファイアウォール トラバーサルを通じて安全に実行します。その結果、組織は、従業員の生産性の向上や、パートナーと顧客とのコミュニケーションの強化からメリットを得ることができます。

VCS Expressway は、ファイアウォールの背後のエンドポイントが、メディアを通過させることができるパスを検出し、これらのパスをそれぞれ経由するピアツーピア接続を確認した後に

最適なメディア接続パスを選択できるインテリジェントなフレームワークを使用します。これにより、企業のファイアウォールを再設定する必要がなくなります。

Expressway-E は高い信頼性と拡張性を備えており、マルチベンダーのファイアウォールをサポートし、SIP プロトコルでも H.323 プロトコルでも、任意の数のファイアウォールを通過できます。

標準機能

Expressway には次の機能が標準で装備されています。

- 別途 VPN クライアントを用意する必要のない、セキュアなファイアウォール トラバーサルとリモート ワーカー向けの Cisco Unified Communications Manager へのセッション ベース アクセス
- エンドポイントの登録サポート。
- SIP レジストラ（ルームまたはデスクトップ SIP プロキシが必要です。SIP プロトコルと H.323 プロトコルは、新しいインストールではデフォルトで無効になり、**[設定（Configuration）]** > **[プロトコル（Protocols）]**の [登録ライセンス（Registration licenses）] から有効にできます）。
- SIP と H.323 をサポート（SIP/H.323 のインターワーキングを含む）
- IPv4 と IPv6 をサポート（IPv4/IPv6 のインターワーキングを含む）
- TURN リレー ライセンスが必要です（TURN relay licenses）
- 高度なネットワーキング
- デバイスのプロビジョニングと FindMe サービス
- H.323 ゲートキーパー
- QoS タギング
- コール単位と総使用率ベースの両方で帯域幅を管理（ローカル サブゾーン内でのコールと外部システムおよびゾーンへのコールに対して個別に設定が可能）
- 使用可能な帯域幅を超えたコールに対する自動ダウンスピードのオプション
- DNS を経由する URI ダイヤリングおよび ENUM ダイヤリングによるグローバルな接続
- リッチメディアセッション（RMS）のサポート
- 最大 2,000 の一致を含む 1,000 の外部ゾーン
- 1,000 のサブゾーン、および最大 3,000 のメンバーシップ ルールのサポート
- プレフィックス、サフィックス、および正規表現を使用した柔軟性のあるゾーン設定
- スタンドアロンの Expressway として機能したり、または他の Expressway やゲートキーパー、SIP プロキシなどの他のシステムとの隣接が可能

- 最大 6 つの Expressway でのクラスタ化による n+1 の冗長性の提供と、最大 4 倍の個別キャパシティの提供が可能
- 単一番号のダイヤリング機能やネットワーク フェールオーバー機能用のインテリジェントなルート ダイレクタ
- エンドポイントの認証オプション
- どのエンドポイントを登録できるようにするかを制御
- コール ポリシー（アドミニストレータ ポリシーとも呼ぶ）（CPL のサポートを含む）
- 外部ポリシー サーバのサポート
- Cisco TelePresence Management Suite 13.2 以降で管理が可能
- Active Directory 認証
- Cisco Unified Communications Manager と Nortel 通信サーバ用に事前設定されたネイバーゾーンのデフォルト
- 初期設定にシリアル ポートを使用する組み込みセットアップ ウィザード
- Web インターフェイスまたは SSH を使用したシステム管理。CE*nnnn* 物理アプライアンスでは CIMC ポート経由でシステムを管理
- 侵入からの保護

他の Cisco 製やサードパーティ製のソフトウェアは、Expressway にインストールしない

Cisco では、明示的に指定しない限り、他の Cisco 製またはサードパーティ製ソフトウェア、アプリケーション、または Expressway のエージェント（VM や物理アプリケーション）のインストールはサポートしていません。Expressway 以外の製品により、プログラムのコードが破損する可能性があるため、インストールしてはいけません。

ハードウェア アプライアンスおよび仮想マシンのオプション

Expressway はオンプレミス アプリケーションやクラウドアプリケーションをサポートし、専用のアプライアンスまたは仮想化されたアプリケーションとして VMware 上で使用でき、さらに Cisco Unified Computing System（Cisco UCS）プラットフォームもサポートします。

仮想マシンのオプション

Expressway での仮想アプリケーションの導入には、次の 3 つのタイプがあります。

- Small（Cisco Business Edition 6000 またはサポートされている VMware ESXi プラットフォームは、必要最低限のハードウェア仕様に準拠しています）
- 中（標準インストール）

- 大（高パフォーマンスと拡張性機能）

Expressway 設置ガイドページの『*Cisco Expressway* 仮想マシン設置ガイド』を参照してください。

ハードウェア CE シリーズのアプライアンス

Expressway は、UCS ハードウェア ベースの専用 CE シリーズのアプライアンスとして使用できます。たとえば、UCS C220 M5L ベースの CE1200 アプライアンスは中容量または大容量の Expressway として動作します。

（注） CE1200 アプライアンスでは、Cisco VCS シリーズはサポートされません。

デフォルトのシステム サイズの変更

Expressway-E として導入されたアプライアンスの場合は、アプライアンスのデフォルトのシステムサイズを手動で [大（Large）] から [中（Medium）]、またはその逆に変更できます。この機能が導入された理由は、1 Gbps の NIC（SFP モジュール）を搭載し、中規模システムとして設定されたアプライアンスでのメディア トラバーサル用の逆多重化ポートでの問題を軽減するためです。

アプライアンスのサイズを変更するには、**[システム（System）] > [管理設定（Administration settings）]** ページに移動して、**[展開設定（Deployment Configuration）]** リストから必要なサイズを選択します。

インストールに関する情報

Expressway 設置ガイドページの『*Cisco Expressway CE1200* アプライアンス設置ガイド』を参照してください。

このガイドについて

このガイドでは、Expressway のさまざまな特徴、サービス、および機能について説明しています。十分な機能を備えた Expressway のバージョンを想定しているため、詳述したすべての項目が導入時にサポートされていない場合があります。

このガイドは、Cisco Expressway シリーズの製品にのみ適用されます。Cisco VCS の詳細については、Cisco TelePresence ビデオ通信サーバの管理および運用ガイド ページの 「*X12.5.x Cisco VCS* 管理者ガイド」を参照してください。

Expressway のほとんどの設定タスクは、Web ユーザインターフェイスまたはコマンドラインインターフェイス（CLI）を介して実行できます。このマニュアルでは主に Web ユーザー インターフェイスの使用方法について説明します。一部の機能は CLI を介してのみ使用でき、これらは関連する場合に説明されています。

Web ユーザインターフェイスの方向は、遷移するページの**名前**に続く **[メニュー（Menu）]** > **[サブメニュー（Submenu）]** のフォーマットで表示されます。

CLI コマンドを次の形式で示します。

```
xConfiguration <Element> <SubElement>
xCommand <Command>
```

トレーニング

トレーニングはオンラインおよびシスコ指定のトレーニング会場で受講できます。当社が提供するすべてのトレーニングの詳細およびトレーニング オフィスの場所については、www.cisco.com/go/telepresencetraining を参照してください。

用語集

TelePresence 用語の用語の用語集は、https://tp-tools-web01.cisco.com/start/glossary/から参照できます。

アクセシビリティ通知

シスコは、利用しやすい製品およびテクノロジーの設計および提供に取り組んでいます。

Cisco Expressway の Voluntary Product Accessibility Template（VPAT）は、ここで入手可能です。

http://www.cisco.com/web/about/responsibility/accessibility/legal_regulatory/vpats.html#telepresence

アクセシビリティの詳細については、次を参照してください。

http://www.cisco.com/web/about/responsibility/accessibility/index.html

関連資料

表 *3*：関連ドキュメントとビデオへのリンク

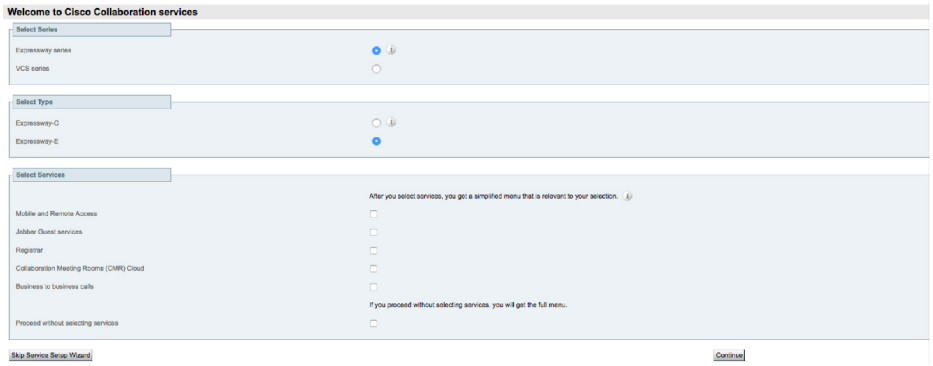
サポート ビデオ	Cisco TAC エンジニアから提供された一般的な Expressway 設定手順に関するビデオは、Expressway/VCS スクリーンキャストビデオ リストページで入手できます（「「Expressway ビデオ」」を検索）。
仮想マシンのインストール	Expressway 設置ガイド ページの『*Cisco Expressway* 仮想マシン設置ガイド』
物理アプライアンスのインストール	Expressway 設置ガイドページの『*Cisco Expressway CE1200* アプライアンス設置ガイド』
シングルボックス システムの基本設定	Expressway 設置ガイドページの『*Cisco Expressway* レジストラ導入ガイド』

ペアリングされたボックスシステムの基本設定（ファイアウォール トラバーサル）	Expressway 基本設定ガイドのページの『*Cisco Expressway-E* および *Expressway-C* 基本設定展開ガイド』
管理およびメンテナンス	Expressway メンテナンスおよび操作ガイドページの『*Cisco Expressway* 管理者ガイド』（有用性情報を含む）
クラスタリング	Expressway コンフィギュレーションガイドページの『*Cisco Expressway* クラスタの作成とメンテナン導入ガイド』
証明書	Expressway コンフィギュレーションガイドページの『*Cisco Expressway* 証明書の作成と使用導入ガイド』
ポート	Expressway コンフィギュレーションガイドページの『*Cisco Expressway IP* ポートの使用コンフィギュレーションガイド』
ユニファイド コミュニケーション	Expressway コンフィギュレーションガイドページの『*Cisco Expressway* 経由の *Mobile & Remote Access*』
Cisco Meeting Server	Expressway コンフィギュレーションガイドページの『*Cisco Expressway* による *Cisco Meeting Server* 導入ガイド』 Cisco Meeting Server プログラミングガイドのページの『*Cisco Meeting Server API* リファレンスガイド』 その他の Cisco Meeting Server のガイドは、Cisco Meeting Server コンフィギュレーションガイドページに用意されています。
Cisco Webex ハイブリッド サービス	ハイブリッド サービス ナレッジ ベース
Cisco Hosted Collaboration Solution（HCS）	HCS のお客様用マニュアル
Microsoft インフラストラクチャ	Expressway コンフィギュレーションガイドページの『*Cisco Expressway* および *Microsoft* インフラストラクチャ導入ガイド』 Expressway コンフィギュレーションガイドページの『*Cisco Jabber* およびビジネス版 *Microsoft Skype* インフラストラクチャ構成チートシート』
REST API	Expressway コンフィギュレーションガイドページの『*Cisco Expressway REST API* サマリー ガイド』（API が自己文書化されている高レベル情報のみ）
MultiWay 会議	Expressway コンフィギュレーションガイドページの『*Cisco TelePresence Multiway* 導入ガイド』

サービスセットアップウィザードについて（サービス選択ページ）

サービスセットアップウィザードを使用すると、環境で Expressway を選択した目的で簡単に設定し、Web ユーザインターフェイスを簡素化します。ウィザードを実行して初期設定を実行する場合と同様に、いつでもサービスの選択ページにアクセスできます（**[概要（Overview）]**> **[概要（Overview）]**）。サービスセットアップウィザードの使用方法についての詳細は、Expressway 設定ガイド ページの『*Cisco Expressway-E* および *Expressway-C Basic* 設定導入ガイド』を参照してください。

図 *1:* サービスセットアップウィザード - サービス選択ページの例



（注） スマートライセンシングを使用する場合は、サービスの選択ページ/ウィザード（Expressway を VCS 製品に変換する）から **[シリーズ（Series）]** 設定を変更できません。代わりに、このプロセスは工場出荷時の状態にリセットして開始する必要があります（VCS ではサポートされていないため、スマートライセンシングを無効にする）。この例で示す他の設定のいくつかは、スマートライセンシングには不要であり、スマートライセンシングを使用する Expressway のウィザードには表示されません。

同時にホストできるサービス

サービスによっては、互換性がないために同時に選択できないものがあります。次の表に、サービスの互換性マトリックスを示します。このマトリックは、システムまたはクラスタで同時に使用できるサービスを示しています。

表 *4*：同時にホストできるサービス

	Cisco Webex ハイブリッド サービス（コネクタ	モバイル & リモート アクセス	**Jabber**	**Microsoft** ゲートウェイ サーバ	レジストラット	**CMR Cloud**	企業間取引コール（ハイブリッド コールサービスを含む）
Cisco Webex ハイブリッドサービス（コネクタ）	Y	N	N	N	N	Y	Y
Mobile and Remote Access および/または（X8.9 から）Meeting Server Web プロキシ	N	Y	N	N	Y	Y	Y*
Jabber Guest サービス	N	N	Y	N	Y	Y	Y
Microsoft ゲートウェイ サービス	N	N	N	Y	N	N	N
レジストラ	N	Y	Y	N	Y	Y	Y
CMR Cloud	Y	Y	Y	N	Y	Y	Y
企業間取引コール（ハイブリッドコールサービスを含む）	Y	Y*	Y	N	Y	Y	Y

表の見方

Y：はい。これらのサービスは同じシステムまたはクラスタでホストできます

N：いいえ。これらのサービスは同じシステムまたはクラスタでホストできません

ルール（Rule）

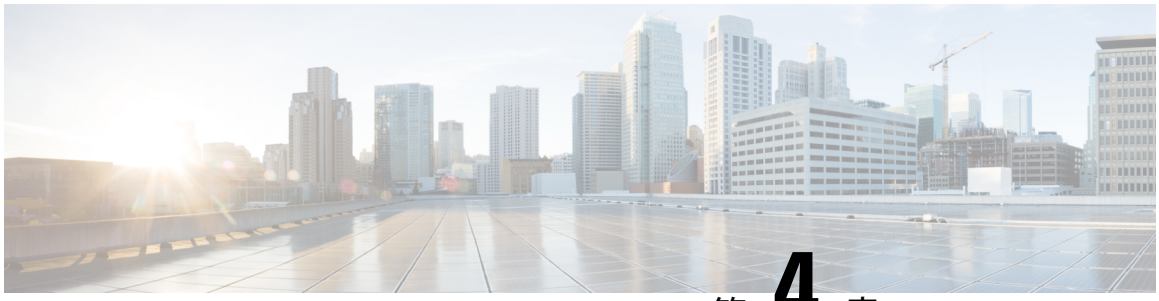
- ハイブリッド サービス コネクタは、コール サービスに使用されるトラバーサル ペアの Expressway-C と共存できますが、ユーザ数に制限があります。

  * ハイブリッド コール サービス（または B2B）トラバーサル ペアも MRA に使用する場合、ハイブリッド サービス コネクタを別個の Expressway-C 上に配置する必要があります。これは、MRA 用に使用されている Expressway-C 上でホストされているコネクタは、シスコではサポートすることができないためです。

- Microsoft ゲートウェイ サービスには、専用の VCS Control または Expressway-C（ヘルプとドキュメントでは「「Gateway VCS」」または「「Gateway Expressway」」と呼ばれます）が必要です。

- Jabber GuestはMRA （技術的な制約を使用できません）

- 現在、MRA は IPv6 専用モードではサポートされません。同じ Expressway トラバーサル ペアで IPv6 B2B コールと IPv4 MRA を共存させる場合、Expressway-E と Expressway-C を両方ともデュアル スタック モードにする必要があります。



第 4 章

Expressway インターフェイス

このセクションでは、Expressway Web ユーザインターフェイスと CLI と API についてまとめています。管理トラフィックに LAN3 を使用するオプションの専用管理インターフェイス（DMI）については、専用管理インターフェイス（DMI）の設定を参照してください。

SMC Web インターフェイスについて

このセクションでは、Expressway Web ユーザインターフェイスと CLI と API についてまとめています。

通常、システム設定は Web インターフェイスを通じて実行します。Web インターフェイスを使用するには、次の手順を実行します。

1. ブラウザウィンドウを開き、アドレスバーにシステムの IP アドレスまたは FQDN を入力します。
2. 有効な管理者の**ユーザ名**と**パスワード**を入力し、**[ログイン（Login）]** をクリックします（管理者アカウントの設定方法について詳しくは、ユーザアカウントの項を参照してください）。**[Overview]** ページが表示されます。

Expressway のセキュリティ証明書に関する警告メッセージが表示された場合は、システムの保護の準備が整うまで、これを無視できます。

フィールド マーカ

- 赤のアスタリスク * が付いたフィールドは必須フィールドです
- オレンジ色のダガー † が付いたフィールドは、クラスタ内の各ピアで設定する必要があるフィールドです。

サポートされるブラウザ

Expressway の Web インターフェイスは、Internet Explorer 8 および 9（非互換モード）、Internet Explorer 10 および 11、Firefox、Chrome に対応するように設計され、テストされています。他のブラウザを UI へのアクセスに使用することは、正式にはサポートされていません。

Expressway の Web インターフェイスを使用するには、JavaScript と Cookie を有効にする必要があります。

HTTP メソッド（HTTP Methods）

Expressway の Web サーバでは、次の HTTP メソッドが許可されています。

方法	Web UI での使用	API での使用	用途
GET	はい	はい	指定したリソースからデータを取得します。たとえば、Expressway の Web インターフェイスの特定のページを返します。
POST	はい	はい	Web リソースにデータを適用します。たとえば、管理者が Expressway の Web インターフェイスを使用して、設定の変更を保存する場合などです。
オプション	いいえ	はい	指定した URL に対し、サーバでサポートされている HTTP メソッドを返します。たとえば、Expressway は OPTIONS を使用して HTTP/1.1 コンプライアンス用にプロキシ サーバをテストできます。
PUT	いいえ	はい	指定した URI に保存するリソースを送信します。REST API コマンドはこのメソッドを使用して、Expressway 設定を変更します。
DELETE	いいえ	はい	指定したリソースを削除します。たとえば、REST API はレコードの削除に DELETE を使用します。

API へのユーザ アクセスを無効にする方法

管理者はデフォルトで API にアクセスできます。これは、次の 2 つの方法で無効化できます。

- Expressway が高度なアカウント セキュリティ モードで動作している場合、API アクセスはすべてのユーザで自動的に無効になります。
- 個別の管理者の API アクセスは、ユーザ設定オプションを使用して無効にできます。

Web ページの機能とレイアウト

このセクションでは、Expressway Web インターフェイスページで使用可能な機能について説明します。

図 2 : リストページの例

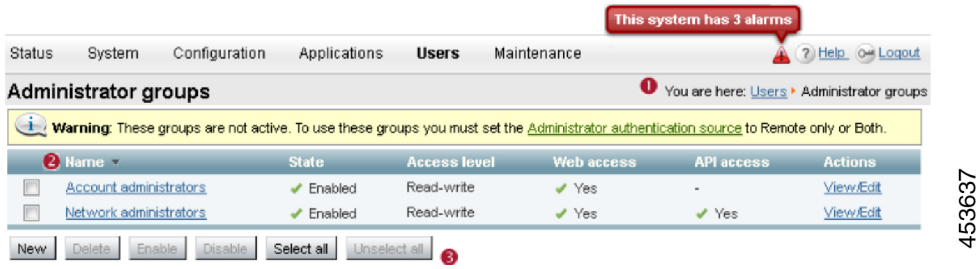
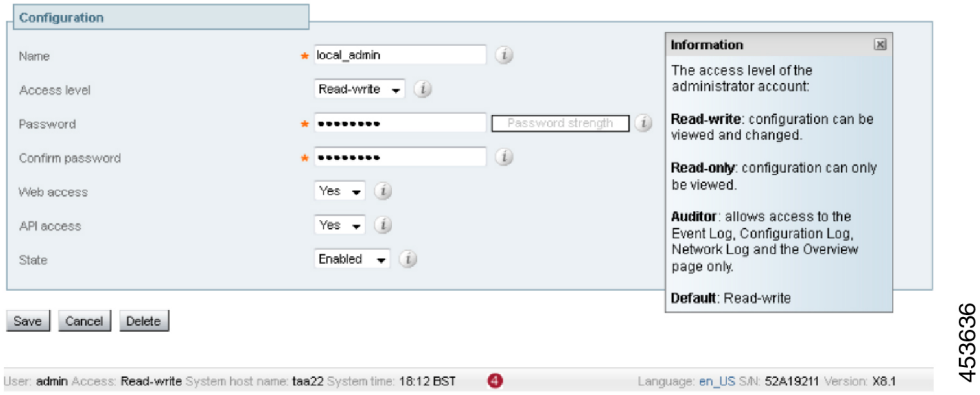


図 3 : 設定ページの例



次の表で、ここに示した Web ページの例に表示されている要素について説明します。

ページの要素		説明
ページの名前と場所	1	各ページには、ページ名とそのページへのメニュー パスが表示されます。メニュー パスの各部分にはリンクが貼られています。上位のメニュー項目をクリックすると、該当のページが表示されます。
システム アラーム	⚠	このアイコンは、システムアラームがあるすべてのページの上部右隅に表示されます。このアイコンをクリックすると、アラームとその推奨される解決策に関する情報が表示される [アラーム（Alarms）] ページに移動します。

ページの要素		説明
ヘルプ		このアイコンは、各ページの右上に表示されます。このアイコンをクリックすると、表示されているページに固有のヘルプが示された新しいブラウザ ウィンドウが開きます。このウィンドウには、そのページの目的の概要が表示され、そのページでの設定に関する説明が示されます。
ログアウト		このアイコンは、各ページの右上に表示されます。このアイコンをクリックすると、管理者セッションが終了します。
フィールド レベルの情報		情報アイコンをクリックするか、またはフィールドの内部をクリックすると、情報ボックスが設定ページに表示されます。このボックスには、該当する場合には有効な範囲やデフォルト値などを含む、特定のフィールドに関する情報が表示されます。情報ボックスを閉じるには、右上の [X] をクリックします。
情報バー		Expressway では、設定を保存したときや、さらにアクションが必要な場合などの特定の状況でフィードバックを提供します。このフィードバックは、ページ上部に黄色の情報バー内に表示されます。
カラムのソート		カラム見出しをクリックすると情報が昇順または降順で並べ替えられます。
[すべてを選択（Select All）] と [選択をすべて解除（Unselect All）]		リスト内のすべての項目を選択または選択解除するには、これらのボタンを使用します。
必須フィールド		完了する必要のある入力フィールドを示します。
ピア固有の設定項目		Expressway がクラスタの一部である場合は、設定のほとんどの項目がクラスタ内のすべてのピアに適用されます。ただし、† で示された項目は、クラスタ ピアごとに個別に指定する必要があります。

ページの要素		説明
システム情報	4	現在ログインしているユーザの名前とそれらのユーザのアクセス権限、システム名（システム名が設定されていない場合は LAN 1 IPv4 アドレス）、ローカル システム時刻、現在選択されている言語、シリアル番号と Expressway ソフトウェア バージョンがページの下部に表示されます。

（注） 管理者アカウントに読み取り専用特権が指定されている場合は、設定値を変更できません。

Web ユーザインターフェイスのアプリケーションメニューがない

Expresswayがインストールされている場合、Webユーザインターフェイスに表示されるメニューは、サービスセットアップウィザードで選択したサービスの選択に合わせて調整されます。場合によっては、選択したサービスの組み合わせによっては、**[アプリケーション（Applications）]** メニューがインターフェイスに表示されない場合があります。このような場合にメニューを復元する場合は、次の手順を実行します。

1. **[ステータス（Status）]** > **[概要（Overview）]** に移動し、**[サービスセットアップの実行（Run service setup）]** をクリックして、サービスセットアップオプションに戻ります。
2. サービスを選択せずに続行オプションにチェックを入れ、**[続行（Continue）]** をクリックします。

コマンドラインインターフェイスについて

コマンドラインインターフェイス（CLI）は、SSH 経由でおよびアプライアンスベースのシステムのシリアル ポート経由でデフォルトで使用できます。これらの設定は、**[システム管理（System administration）]** ページで制御します。

CLI を使用するには

1. SSH セッションを開始します。
2. Expressway の IP アドレスまたは FQDN を入力します。
3. 管理者のユーザ名とパスワードを使用してログインします。

   プライベートキーを使用して認証する場合は、Expressway への SSH アクセスの有効化を参照してください。
4. これで、適切なコマンドを入力して CLI を使用できるようになりました。

コマンド タイプ

コマンドは次のグループに分類されます。

- **xStatus** はシステムの現在のステータスに関する情報を返します。現在のコール数や登録数などの情報は、このコマンド グループを使用して入手できます。さらに、コマンド リファレンス - xStatusで **xStatus** コマンドの詳細なリストを参照してください。
- **xConfiguration**は、これらのコマンドを使用すると、1つのデータ項目（IPアドレスやゾーンなど）を追加したり編集したりできます。さらに、コマンド リファレンス — xConfigurationで **xConfiguration** コマンドの詳細なリストを参照してください。
- **xCommand**は、これらのコマンドを使用すると、項目を追加および設定したり、情報を取得したりできます。さらに、コマンド リファレンス — xCommandで **xCommand** コマンドの詳細なリストを参照してください。
- **xHistory**は、コールと登録に関する履歴情報を提供します。
- **xFeedback** は、コールや登録など、イベントが発生した場合に関する情報を提供します。

便利な制御

- CLI に **`xConfiguration`** パスを入力すると、その要素（および該当する場合はサブ要素）に現在設定されている値のリストが返されます。
- CLI に **`xConfiguration`** のパスを入れて、その後に？を入力すると、その要素とサブ要素の使用方法に関する情報が返されます。
- CLI に **`xCommand`** コマンドを？付きで、または？を付けずに入力すると、その要素の使用方法に関する情報が返されます。

API について

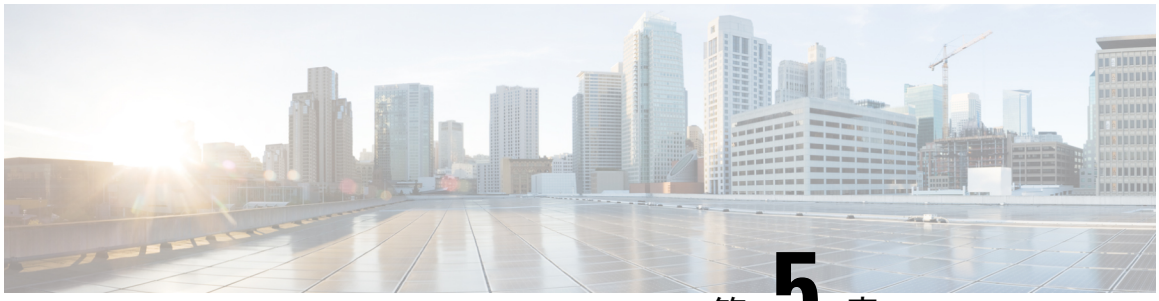
Expressway が詳細アカウント セキュリティモードになっているか、管理者のユーザ設定オプションで個別のアクセスが無効になっている場合を限り、管理者はデフォルトで Expressway REST API にアクセスできます。

API は、RAML を使用して文書化されています。Expressway 設定ガイドページには *REST API* サマリーガイドが用意されており、基本 URL と RAML 定義へのアクセス方法と、要求と応答の例を挙げています。

ハードウェアプラットフォームでサポートされるソフトウェア バージョン

表 *5 :* このリリースでサポートされている *Expressway* プラットフォーム

プラットフォーム名	シリアル番号	ソフトウェア バージョンのサポート範囲
小規模 VM（OVA）	（自動生成）	X8.1 以降
中規模 VM（OVA）	（自動生成）	X8.1 以降
大規模 VM（OVA）	（自動生成）	X8.1 以降
CE1200 Hardware Revision 2（UCS C220 M5L にプレインストール）	52E1####	X12.5.5 以降。
CE1200 Hardware Revision 1（UCS C220 M5L にプレインストール）	52E0####	X8.11.1 以降。
CE1100（UCS C220 M4L にプレインストールされた Expressway）	52D#####	メンテナンスとバグ修正のみを目的とするX12.6.xバージョンでの限定的なサポートを除き、（X12.5.x以降）サポートされていません。
CE1000（UCS C220 M3L にプレインストールされた Expressway）	52B#####	サポート対象外（X8.10. x 以降）
CE500（UCS C220 M3L にプレインストールされた Expressway）	52C#####	サポート対象外（X8.10. x 以降）



第 5 章

Expressway の容量とサイジング

概要

Cisco Expressway シリーズ（Cisco VCS 以外）でサポートされる最大容量とサイズは、次の表にリストされています。実際の導入でパフォーマンスに影響を与える要因が多いため、これらの図はガイドラインについてのみ掲載していますが動作を保証しているわけではありません。Expressway がサポートしているユース ケースが多いので、独自で行う特定の導入に対応する容量制限を実現することはできません。

Expressway のサイジングと容量の情報は、サポートされている同時登録またはコールの数に基づいて分類されています。

重要な警告

- ここで示す図は、必要なすべてのソフトウェアライセンスが適用されている場合を想定しています。
- この数値は、特定かつ専用の Expressway シナリオでテストされたものです。Expressway またはクラスタに基づいて、単一のサービスまたはシナリオに使用されます（たとえば、MRA または B2B コールに対する場合など）。マルチサービス導入のためのテスト済みキャパシティガイドラインを提供することはできません。
- 最大 6 つの Expressway システムをクラスタ化できますが、キャパシティは**最大で 4 つ**増加します（ゲインがないスモール VM を除く）。

- 小規模な VM の場合、クラスタリングは冗長性のためだけに使用され、スケーリングには使用されず、**クラスタリングによる容量の増加もありません**。
- ビデオコールと音声専用コールに提供される数字は選択肢です。指定されたキャパシティはビデオと音声のどちらでも使用できます。両方には使用できません。

依存関係

コールに対応する数は、同時コール数を表します。

同時コールとリッチメディアセッション（RMS）ライセンスは、1 対 1 の関係がありません。さまざまな要因によって RMS ライセンスの使用が決定されます。つまり、いくつかのコールが「自由」に使用されており、他のコールは複数のライセンスを使用している場合があります。

6000 TURN リレーをサポートするには、大規模システム（大規模な VM または CE1200）に対して 「[大規模 Expressway の TURN ポートを多重化（TURN Port Multiplexing on Large Expressway）]」 を有効にする必要があります（**[設定 (Configuration)]** > **[トラバース（Traversal）]** > **[TURN]**）。

小規模 VM は、Cisco Business Edition 6000 プラットフォームまたは Cisco Business Edition 6000 仕様に一致する汎用ハードウェア / ESXi でサポートされています。小規模 VM の数字は、M5 ベースの BE6000 アプライアンスに対応しています。

スタンドアロン システムのキャパシティ数

次の表は、スタンドアロン Expressway の基本キャパシティを表しています。

表 *6:* スタンドアロンキャパシティのガイドライン：シングル *Expressway*

プラットフォーム（**Platform**）	登録（ルーム/デスクトップ）	コール（ビデオまたは音声のみ）	**RMS** ライセンス	**MRA** 登録（プロキシ実施済み）	**TURN** リレー*
CE1200	5,000	500 ビデオまたは 1000 音声	500	5000	6000
大規模 VM	5,000	500 ビデオまたは 1000 音声	500	3500	6000
中規模 VM	2,500	100 ビデオまたは 200 音声	100	3000	1800

プラットフォーム（Platform）	登録（ルーム/デスクトップ）	コール（ビデオまたは音声のみ）	RMS ライセンス	MRA 登録（プロキシ実施済み）	TURN リレー*
小規模 VM	2000	40の 非 MRA ビデオ、または 20 MRA ビデオまたは 40 音声	75	200	1800

クラスタ システムのキャパシティ数

次の表は、4 つの Expressways（スケール ゲインの最大クラスタ サイズ）を搭載したクラスタ システムのキャパシティが増えた状態を示しています。

2 つまたは 3 つのノードを持つクラスタのキャパシティを決定するには、2 または 3 の因数をそれぞれスタンドアロンの数字に適用します。クラスタ化システムとスタンドアロンシステムの数値が常に同じ小規模VMを除きます（小規模VMのクラスタ化によってキャパシティゲインが得られるため）。

表 *7*: クラスタ化されたキャパシティのガイドライン：*4* つの機能を搭載したクラスタの例

プラットフォーム（Platform）	登録（ルーム/デスクトップ）	コール（ビデオまたは音声のみ）	RMS ライセンス	MRA 登録（プロキシ実施済み）	TURN リレー*
CE1200	20,000	2000 ビデオまたは 4000 音声	2000	20,000	24,000
大規模 VM	20,000	2000 ビデオまたは 4000 音声	2000	10,000	24,000
中規模 VM	10,000	400 ビデオまたは 800 音声	400	10,000	7200
小規模 VM	2000	40の 非 MRA ビデオ、または 20 MRA ビデオまたは40 音声	75	200	1800

導入例

たとえば、デスクトップへの登録を最大 750 件同時に実施して 250 件のリッチメディアセッションを処理できる耐障害性クラスタを導入する必要があるとします。この場合は、次のようにして 4 つのピアを設定することができます。

	ピア 1	ピア 2	ピア 3	ピア 4	総クラスタ容量
デスクトップ登録ライセンス	250	250	250	0	750
リッチ メディア セッション	100	100	50	0	250

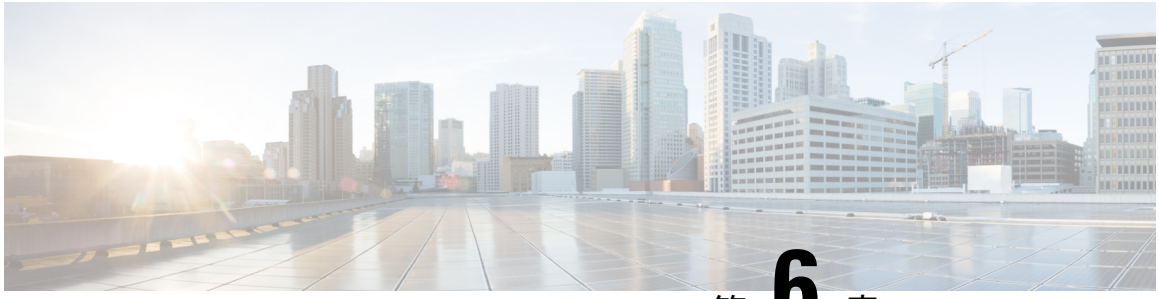
この例ではライセンスはすべてのピアで共有されるため、エンドポイントがどのピアに登録するかは問題になりません。ピアのいずれかが一時的にサービスを中断しても、一連のコールライセンスのすべてを、そのままクラスタ全体で使用できます。

クラスタ内のコール

エンドポイントが同じクラスタ内の異なるピアに登録されたライセンス使用状況は、クラスタ全体のコール メディア トラバーサルによって異なります。

- コールメディアがクラスタピアを通過しない場合、エンドポイント間のコールは RMS ライセンスを使用しません（「「登録済み」」のコールです）。
  - エンドポイントの 1 つがシスコインフラストラクチャに登録されていない場合、コールは RMS ライセンスを使用します。
- コールメディアがクラスタピアを通過する場合、エンドポイント間のコールでは、B2BUA が使用されている場合に、管理対象の RMS ライセンスが使用されます。
  - 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、コールは、実効的なライセンスを使用しません。

クラスタ化システムでのライセンスの使用方法の詳細については、このガイドの「ライセンス」セクションを参照してください。



第 6 章

ライセンスの管理

ここでは、Cisco Expressway で使用できるライセンスオプションおよびそれらを管理する方法について説明します。スマートライセンスモードは Cisco VCS 製品ではサポートされておらず、Cisco Expressway シリーズでのみサポートされていることに注意してください。

スマートライセンシングと PAK ライセンス（オプション キー）の比較

Cisco Expressway では、次の 2 つのライセンスモードのいずれかがサポートされています。

- **PAK ベースのライセンス**。従来の方法では、オプション キー（製品アクティベーション キーとも言う）を使用して Expressway にライセンスをインストールします。オプション キーは、ライセンスだけでなく、特定の機能とサービスを有効にするためにも使用されます。
- **スマートライセンシング**X12.6 から Expressway で使用できる新しいライセンス方式。この方法は、通常、クラウドベースの Cisco Smart Software Manager（CSSM）を使用して管理されます。または、オンプレミスでの対応が必要な環境の場合は、Smart Software Manager オンプレミス製品（旧称 「Smart Software Manager サテライト」）を使用できます。

常に 1 つのライセンス モードのみサポートされます。

Expressway は、デフォルトでは PAK ベースのライセンスに設定されています。Web インターフェイスからスマートライセンスに切り替えられます（**[メンテナンス（Maintenance）]** > **[スマートライセンス（Smart licensing）]**）。ただし、**PAK へ切り替えて戻すには工場出荷リセット**が必要です。

オプションキー（HSM を含む）を使用する機能ではスマートライセンスを使用できない。 Expressway の一部の機能は、オプションキーにより有効になっています。オプションキーはスマートライセンスと互換性がないため、オプションキーを必要とする機能が必要な場合、スマートライセンスではなく、PAK ベースのライセンスを使用する必要があります。

オプション キーの管理

このセクションが適用されるのは、Expressway がスマートライセンスについてではなく、従来の PAK ベースのライセンスモードを使用している場合です。PAK モードでは、オプションキー（製品アクティベーションキーとも呼ばれる）を使用して、Expressway に追加の機能またはライセンスを追加します。オプション キーは、一定期間または期間無制限で有効にすることができます。

（注） Expressway でスマートライセンシングが有効になっている場合、オプションキーは使用できません。また、これらのキーはシステムに影響を及ぼす事はありません。

[オプションキー（Option keys）] ページ（**[メンテナンス（Maintenance）]** > **[オプションキー（Option keys）]**）は、Expressway に現在インストールされているオプションの一覧で、新しいキーを追加できます。**[システム情報（System information）]** セクションには Expressway にインストールされている既存の機能の要約が示され、インストールされている各キーの有効期間が表示されます。

オプションキーを取り外しています。また、バージョン X12.6 以降の CE1200 ベースのアプライアンスでも、次のキーだけが（PAK ベースの）Expressway システムに対して有効です。

- **[リッチメディアセッション（Rich media sessions）]**：Expressway（または Expressway クラスタ）で常に許可される非ユニファイドコミュニケーションコールの数を決定します。詳細については、コール タイプとライセンスのセクションを参照してください。
- **[TelePresence デスクトップシステム（TelePresence Desktop Systems）]**：Expressway に登録する可能性があるデスクトップ システムの数まで追加します。
- **[TelePresence Room システム（TelePresence Room Systems）]**：Expressway に登録する可能性があるルーム システムの数まで追加します。
- **HSM**：Expressway でのハードウェアセキュリティモジュールのサポートを有効します。HSM 機能は、**Expressway ソフトウェアバージョンに応じてのみプレビューのステータス**になる場合があります。この場合は、HSM を使用する前に、Expressway バージョンのリリースノートを確認してください。

- **[高度なアカウント セキュリティ（Advanced account security）]**：高度なセキュリティ機能と高レベルセキュリティのインストールの制限事項を有効にします。
- **[Microsoft 相互運用性（Microsoft Interoperability）]**：Microsoft Lync 2010 Server サーバで暗号化されたコール（ネイティブ SIP コールと H.323 からインターワーキングされたコールの両方）を送受信できるようにします。また、Lync 2010 クライアントへの ICE について コールを確立するときも Lync B2BUA で必要になります。Lync 2013 とのすべての通信タイプに必要です。

古いソフトウェアを実行している Expressway は、ソフトウェアバージョンに応じて、次のオプションキーの一部またはすべてを使用する場合があります。

- **[Expressway シリーズ（Expressway Series）]**：Expressway シリーズ システム機能のために製品を特定して設定します。
- **[トラバーサル サーバ（Traversal Server）]**：Expressway をファイアウォール トラバーサル サーバとして機能できるようにします。
- **[暗号化（Encryption）]**：AES（および DES）暗号化がこのソフトウェア ビルドでサポートされていることを示します。
- **[SIP インターワーキング ゲートウェイへの H.323（H.323 to SIP Interworking gateway）]**：H.323 コールを SIP に変換したり、その逆に変換したりできるようにします。

キーの追加

このタスクは PAK ベースのライセンスを使用する場合にのみ適用されます。オプションキーがスマートライセンシングで無効である場合です。Web UI または CLI を使用してオプションキーを追加できます。

これらの手順と Cisco TAC エンジニアによって提供されるプロセスのビデオ デモンストレーションは、「Expressway/VCS スクリーン キャスト ビデオ リスト（Expressway/VCS Screencast Video List）」ページにあります。

65 個のオプション キーの制限

65 個を超えるオプション キー（ライセンス）を追加しようとすると、**[オプション キー（Option keys）]**ページでは通常どおりに表示されていても、適用されるオプション キーは最初の 65 個のみです。66 個目以降のオプション キーは追加されているように見えても実際には Expressway によって処理されません。CDETS CSCvf78728 を参照してください。

はじめる前に

1. 有効なオプション キーを用意しておきます。
2. システムに、該当するオプション用のデモ オプション キーが存在する場合は、それらのキーを削除してからシステムを再起動します。そうしないと、時間制限のあるデモ オプション キーの期限が切れると機能が動作しなくなります。

Web UI を使用したオプション キーの追加

1. **[オプション キーの追加（Add option key）]** フィールドに、追加するオプションのキーを入力します。
2. [オプションの追加（Add option）] をクリックします。

オプションキーによっては、システムを再起動しなければ有効にならない場合があります。これに該当するキーには以下が含まれます。

- トラバーサル サーバ（Traversal Server）
- Expressway シリーズ
- 高度なアカウント セキュリティ（Advanced Account Security）（FIPS モードを開始する場合）

再起動が必要な場合は、Webインターフェイスにアラームが表示され、再起動するまで通知としてそのまま表示されます。表示されている間も、引き続き Expressway を使用したり設定したりできます。

CLI を使用したオプション キーの追加

すでにシステムにインストールされているすべてのオプション キーのインデックスを戻すには、次のコマンドを実行します。

xStatus Options

システムに新しいオプション キーを追加するには、次のコマンドを実行します。

xConfiguration Option [1..64] Key

（注） CLIを使用してオプションキーを追加する場合は、未使用のオプションインデックスを使用できます。どのインデックスが現在使用されているかを確認するには、**xConfiguration option** と入力します。既存のオプションインデックスを選択すると、そのオプションが上書きされ、そのオプションキーで提供される追加機能が失われます。

コール タイプとライセンス

コール タイプ

Expressway は次の種類のコールを区別します。

- 登録済み。つまり、ルームとデスクトップの登録
- リッチ メディア セッション（RMS）

登録済み

ローカルに登録されているエンドポイント（Unified CM または Expressway に登録されている）間のコールはライセンスを消費しません。その権限は登録に含まれるからです。次のシナリオでは、ライセンス登録にコールの権限が含まれます。

- コールがネイバー ゾーンまたはトラバーサル ゾーン経由でルーティングされる場合、同じネットワーク内の Unified CM または Expressway に登録されているほかのエンドポイントへのコール。
- Unified CM リモート セッション。これらは、モバイルおよびリモート アクセス（MRA）コールです。つまり、Expressway ファイアウォール トラバーサル ソリューションを使用して、Unified CM に登録されているエンドポイントにルーティングされる、企業外にあるデバイスからのビデオまたは音声コールです。
- シスコの会議リソース（CMR、TelePresence Server TelePresence Conductor、Acano サーバ）へのコール。

（注）
- これらのコールもボックスの物理的な制約数に計上されます。
- Expressway は、1xx 暫定メッセージの SDP で ICE 候補をサポートしていません

RMS

リッチ メディア セッション（RMS）ライセンスを消費するこれらのコールには、Expressway 経由でルーティングされるビデオまたは音声コールのそのほかすべてのタイプが含まれます。次のシナリオでは、RMS ライセンスが Expressway の終了ノードで消費されます。

- B2B
- Jabber Guest
- サードパーティ製ソリューションへの作業間コールまたはゲートウェイ化されたコール（サードパーティ製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ない場合）

Expressway はメディア、またはシグナリングのみを取得する場合があります。

音声のみの SIP コールはビデオ SIP コールとは別に処理されます。各 RMS ライセンスで、1 つのビデオ コールまたは 2 つの音声のみの SIP コールが許可されます。したがって、RMS ライセンスが 100 個ある場合、90 のビデオ コールと 20 の SIP 音声専用コールが同時に許可されます。その他のタイプの音声専用コールは、1 つのライセンスを使用します。

（注）

- Expressway は「「音声専用」」SIP コールを SDP で単一の「「m=」」行でネゴシエートされたコールと定義します。たとえば「「電話」」コールが発信された一方、SIP UA が SDP に追加の m= 行を含めると、そのコールはビデオコールライセンスを使用します。
- 「「音声専用」」SIP コールが確立されている間は、（ライセンス供与された）ビデオコールとして扱われます。「「音声専用」」としてライセンスされるのは、コール設定が完了してからです。これは同時に行われた場合、システムがライセンスの最大数の制限に近づいていると、一部の「「音声専用」」コールに接続できない可能性があることを意味します。
- Expressway はコール中のライセンス最適化はサポートしていません。
- TelePresence Conductor を使用した導入環境で、ライセンス消費が適用されるのは、TelePresence Conductor が B2BUA 基本設定を使用して導入されていて、ポリシー サーバベースの導入ではない場合のみです。
- SIP から H.323へのインターワーキングは、インターワーキングが行われるノードでRMS ライセンスを使用します（エンドポイントのいずれかがシスコインフラストラクチャに登録されていない場合）。

Expresswayの会議室やデスクトップ登録

Expressway が SIP レジストラまたは H.323 ゲートキーパーとして設定されている場合は、同時コールではなく、同時システム（Unified CMモデル）のライセンスが必要です。

SIP 導入の場合は、次のライセンス タイプのいずれか、または両方を Cisco Expressway-C あるいは Cisco Expressway-E に追加して、この要件を満たします。

- TelePresence ルーム システム ライセンス
- デスクトップ システム ライセンス

次の SIP デバイスをデスクトップ システムとして登録します。そのほかすべてのデバイスはルーム システムと見なされます。

- Cisco TelePresence EX60
- Cisco TelePresence EX90
- Cisco Webex DX70
- Cisco Webex DX80
- Cisco Jabber Video for TelePresence（Movi）ソフト クライアント（現在は販売終了）を使用する場合、これらのクライアントもデスクトップ システムとして Expressway に登録します。

（注） デスクトップシステムとして登録するには（SIP の場合）、DX システムがバージョン CE8.2 以降で稼働し、EX システムが TC7.3.6 以降で稼働している必要があります。それよりも前のバージョンで稼働している DX および EX システムは、SIP に登録されますが、ルーム システム ライセンスを使用します。

H.323 導入では、すべて のエンドポイントは TelePresence ルーム システム ライセンスを使用します。これはデスクトップで特定のタイプのエンドポイントの違いを定めないH.323の制限に起因します。したがって、優先シグナリングプロトコルとして SIP を推奨しますが、H.323 は SIP をサポートしないエンドポイントのフォールバックとして使用できます。

Expressway が SIP レジストラ/H.323 ゲーテキーパーである場合のライセンスに関する検討事項

- ローカル登録用のライセンスを含むオプション キーは、エンドポイントの登録先に応じて、Cisco Expressway-C または Cisco Expressway-E、あるいはこの両方にインストールされます。これらのライセンスはクラスタにプールされるので、Expressway ピアは互いのライセンスを使用できます。ただし、ルームではデスクトップ ライセンスを使用できず、デスクトップ システムではルーム ライセンスを使用できません。
- ネットワーク外からの登録は Expressway-E によって Expressway-C にプロキシされます。Expressway-E に直接登録する場合は、同じドメインを使用できないことに注意してください。
- Expressway-C にライセンスがすでに存在する場合、ライセンスが適用された既存のエンドポイントの一部またはすべてを Expressway-E に登録するには、該当するライセンスを手動で Expressway-C から削除してから、Expressway-E にリロードします。
- 大容量 VM および CE1200 および CE1100 アプライアンスは、適切なライセンスに従って最大 5000 の登録をサポートできます。（CUCM にプロキシされる）MRA 登録の場合、最大登録件数は CE1200 では 5000、大規模 VM および CE1100 では 2500 に制限されます。ローカル登録、プロキシ登録（Expressway-E 経由）および MRA 登録のすべてが、この登録制限数に計上されます。
- プロキシ登録は SIP エンドポイントでのみ可能で、H.323 エンドポイントには適用されません。
- FindMe デバイスのプロビジョニングは Cisco TMSPE でサポートされています（ただし、このサポートは Expressway バージョン X12.5 では推奨されません）。

デバイスが SIP と H.323 の両方に登録される場合のライセンスに関する検討事項

同じデバイスが SIP と H.323 の両方として Expressway に登録されている場合は、複数のライセンスが消費される点に注意してください。たとえば、DX80 が SIP ユーザエージェントとして Expressway-C に登録され、H.323 エンドポイント（同じまたは異なる URL/DN）として登録されるなどです。デスクトップシステムライセンスは SIP 登録のために消費され、TelePresence Room システムライセンスは H.323 エンドポイント登録で消費されます。Cisco Webex Room が

SIP と H.323 の両方に同様に登録する場合など、同じデュアルライセンスの使用法が適用されます。

RMS ライセンスの使用状況

ライセンス モデルでは、次のシナリオで使用されるリッチ メディア セッション（RMS）ライセンスの数が削減されます。

- 登録ライセンスの支払いがすでに完了している場合、次のコールタイプには、RMS ライセンスが使用されません。
  - 登録されているシステム間のコール。この「「登録されているシステム」」とは、Expressway に直接登録されているシステム、Expressway-E から Expressway-C へのプロキシによって登録されているシステム、Expressway ペア（MRA）から隣接 Unified CM へのプロキシによって登録されているシステムを意味します。
  - 登録されているシステム（前述）からCiscoインフラストラクチャへのコール。現在、これは、Cisco Meeting Server と、TelePresence Conductor によって管理されるCiscoTelePresence Server および TelePresence MCU に対してのみ拡張されています。ただし、Conductor によって管理されない MCU からのコールは RMS ライセンスを使用します。
  - 登録されているシステム（前述）から Cisco Collaboration Cloud へのコール。
- 登録されたシステムから他のすべてのシステムへのコールは、1 つの RMS ライセンスを使用します。以下のコールタイプが含まれますが、これらに限定されません。
  - ビジネス ツー ビジネス コール。Expressway-E に RMS ライセンスが 1 つ必要です。
  - ビジネス ツー コンシューマ コール（Jabber Guest）。Expressway-E に RMS ライセンスが 1 つ必要です。
  - Microsoft Lync / Skype for Business およびサードパーティ コール制御サーバを含む相互運用性ゲートウェイ コールには、Expressway-C で 1 つの RMS ライセンスが必要です。

デバイス登録でのライセンスの使用状況

Expressway（Cisco Expressway-C または CiscoExpressway-E）に直接登録されているデバイスは、次のライセンスを消費します。

- SIP。Cisco TelePresence EX60、Cisco TelePresence EX90、Cisco DX70、および Cisco DX80 エンドポイントは、デスクトップ ライセンスを消費します。そのほかの SIP エンドポイントは、ルーム システム ライセンスを消費します。
- H. 323。登録されている各 H.323 エンドポイントがルーム システム ライセンスを消費します。

Cisco Expressway-C への SIP プロキシ登録では、直接 SIP 登録と同じライセンスが消費されます。Cisco Expressway-E への SIP プロキシ登録では、ライセンスは消費されません。

（注） 登録数は、デバイス（IPアドレス）ごとではなく、エイリアスごとにカウントされます。したがって、MCU のように複数のエイリアスを指定した登録要求は、1 つのデバイスだけを Expressway に登録するとしても、複数のルーム ライセンスを消費します。

RNS リソースライセンス消費表

次の表は、Expressway が消費する RMS ライセンスのシナリオの一覧です。「サードパーティのゲートキーパ」への参照は、ゲートキーパが Expressway-C に接続されていることを意味し、「外部」への参照は、ゲートキーパが Expressway-E に接続されていることを意味します。

コール発信側エンドポイントの登録先	コール着信側エンドポイントの登録先	Expressway-C	Expressway-E
Unified CM	Expressway-C （Lync）	1 つの Expressway-C （Lync ゲートウェイ）	0
Unified CM	External	0	1
Unified CM	サードパーティのゲートキーパー	1	0
Expressway-C	External	0	1
Expressway-C（リモート [SIP] - プロキシ）	External	0	1
Expressway-C （SIP）	サードパーティのゲートキーパー	1	0
Expressway-C （H323）	サードパーティのゲートキーパー	1	0
Expressway-C（リモート [SIP] - プロキシ）	サードパーティのゲートキーパー	1	0
Expressway-C	Expressway-C （Lync）	0	1 つの Expressway-C （Lync ゲートウェイ）
Expressway-C （リモート）	Expressway-C （Lync）	0	1 つの Expressway-C （Lync ゲートウェイ）
Expressway-C （SIP）	サードパーティ製SIP サーバ	1	0

コール発信側エンドポイントの登録先	コール着信側エンドポイントの登録先	Expressway-C	Expressway-E
Expressway-C （H323）	サードパーティ製SIPサーバ	1	0
Expressway-E（SIP）	外部	-	1
Expressway-E（H.323）	外部	-	1

コラボレーション会議室（CMR）へのコールのライセンスのバイパス

Expressway では、クラウドベースの CMR とのコールにリッチ メディア セッション ライセンスは不要になりました。これには、コラボレーション クラウドと CMR ハイブリッド ソリューション間の SIP/ H.323 コールが含まれます。

（注） これは、ダイヤルしたストリングが Expressway でのトランスフォーメーションを必要としない場合にのみ適用されます（user@sitename.webex.com など）。

クラウドベースの CMR への変換が行われていない SIP コールはライセンスを使用しませんが、リソースは使用し、Expressway がフル キャパシティの場合は進行しないことがあります。

CMR の施設内コールにライセンス バイパスはありません。クラウドベースの CMR への H.323 コールは CMR ライセンスを消費しますが、RMS ライセンスは消費しません。

クラスタ システムのライセンス使用状況

PAK ベースのライセンス

従来の（PAK ベースの）ライセンスでは、次のライセンスタイプは、ライセンスがインストールされているピアに関係なく、クラスタ内のピアで使用するためにプールされます。

- RMS ライセンス
- TURN リレー ライセンス（X 8.11 より前のソフトウェアを実行しているシステム）

可能であれば、ライセンスの数はクラスタ内のすべてのピア全体に均一に配布することを推奨します。各クラスタ ピアにインストールされているすべてのライセンスの概要を確認するには、「**オプション キー（Option keys）**」ページに移動して、**[現在のライセンス（Current licenses）]** までスクロールします。

クラスタ ピアが使用できなくなった場合は、そのピアにインストールされた共有可能なライセンスは、ピアへの接続をクラスタが失った時から 2 週間の期間中、残りのクラスタ ピアにそのまま使用できます。これにより、クラスタの全体的なライセンス キャパシティが一時的に維持

されます（ただし、各ピアはその物理キャパシティによって制限されることに注意してください）。2 週間の期間が過ぎると、使用できないピアに関連付けられたライセンスがクラスタから削除されます。クラスタに対して同じキャパシティを維持する必要があり、そのクラスタを使用しないピアを修復できない場合は、別のピアに新しいオプション キーをインストールする必要があります。

クラスタ内のコール

エンドポイントが同じクラスタ内の異なるピアに登録されたライセンス使用状況は、クラスタ全体のコール メディア トラバーサルによって異なります。

- コールメディアがクラスタピアを通過しない場合、エンドポイント間のコールは RMS ライセンスを使用しません（「「登録済み」」のコールです）。
  - エンドポイントの 1 つがシスコインフラストラクチャに登録されていない場合、コールは RMS ライセンスを使用します。
- コールメディアがクラスタピアを通過する場合、エンドポイント間のコールでは、B2BUA が使用されている場合に、管理対象の RMS ライセンスが使用されます。
  - 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、コールは、実効的なライセンスを使用しません。

使用制限

使用制限には、物理的なキャパシティとライセンスの 2 つの側面があります。Expressway クラスタの物理的な制約によって最終的な制限が決定され、システムが使用可能なキャパシティはライセンスによって決定されます。

物理的な容量の制限

各 Expressway ピアが実際に使用できるライセンスの最大数は、アプライアンスまたは VM の物理キャパシティによって異なります。たとえば、大規模 Expressway VM がサポートする最大キャパシティは、500 の同時ビデオ コールです。

次の使用率のしきい値のいずれかに到達した場合は、容量アラームが発生します。

- 同時発生コールの数がクラスタの容量の 90% に到達した
- 任意の 1 台のユニットで同時発生コールの数がユニットの物理的な容量の 90% に到達した

ライセンスの制限

クラスタのライセンス容量は、システムが従来の PAK ベースのライセンスを使用するかスマートライセンスを使用するかによって異なります。たとえば、PAK ベースの場合、2 台の大規模

VM がクラスタ化され、それぞれ 300 の有効なライセンスがインストールされている場合、クラスタの実効容量は 600 の同時ビデオコールです。クラスタから 1 つのピアが削除された場合、残りのピアは 600 RMS のすべてのライセンスを 14 日間保持しますが、最大 500 の同時ビデオ コールのみをサポートします。

スマートライセンスシステムの場合、ライセンス容量は、Cisco Smart Software Manager で組織の登録済みアカウントに割り当てられているライセンスプールによって異なります。

スマートライセンスについて

このセクションは、バージョン X12.6 から利用可能な Expressway シリーズシステムにスマートライセンシングを使用する場合に適用されます。(スマートライセンシングは Cisco VCS システムではサポートされていません)。PAK ライセンスを使用する場合は、代わりにオプションキーの管理を参照してください。

スマート ライセンスの仕組み

Cisco Smart Software Licensing（スマートライセンス）は、シスコ製品全体で有効にされるライセンスに対する新しい方法です。ライセンスを簡素化し、ライセンス所有権と使用量を明確にします。デバイスは、ライセンス消費を自己登録およびレポートするため、オプション キー（製品アクティベーション キー）を使用する必要がなくなります。ライセンスの権限は、1 つのアカウントにプールされます。会社が所有しているすべての互換性のあるデバイスでライセンスを使用して、組織のニーズに合わせてライセンスを移動することができます。

スマートライセンシングを使用して、Expressway を Cisco Smart Software Manager（または Cisco Smart Software Manager On-Prem）に登録します（下記参照）。そこから、ライセンスを管理し、スマートライセンスの使用状況を監視できます。

オンプレミスのオプション - Smart Software Manager オンプレミスの使用

ポリシーまたはネットワーク可用性のために、Cisco Smart Software Manager を使用したシスコ製品の直接管理を希望されない場合は、代わりに Smart Software Manager オンプレミスを利用できます。これは、Cisco Smart Licensing のオンプレミスコンポーネントであり、製品は Cisco Smart Software Manager と同じ方法でライセンス消費を登録およびレポートします。

cisco.com に直接接続できるかどうかに応じて、Smart Software Manager オンプレミスを接続または切断のいずれかのモードで導入できます。

- **接続済み**cisco.com への直接接続がある場合に使用されます。スマート アカウントの同期が自動的に実行されます。
- **切断されました**。cisco.com への直接接続がない場合に使用されます。Smart Account の同期を手動でアップロードおよびダウンロードする必要があります。

詳細情報

Cisco Smart Software Manager の詳細な製品情報については、Cisco Smart Software Manager を参照してください。また、オンプレミスマネージャーの詳細については、Smart Software Manager オンプレミスを参照してください。

スマートライセンシングを有効にする前に

この項には、Expressway にスマートライセンスを実装する前に知っておくべきいくつかの注意事項があります。

注意 スマートライセンシングを有効にした後、PAK ベースのライセンスに戻る（または Expressway システムを Cisco VCS システムに変換する）には、工場出荷時の状態にリセットする必要があります。工場出荷時のリセットによってソフトウェアイメージが再インストールされ、Expressway の設定がデフォルトにリセットされるので、スマートライセンスを有効にする前に、Expressway のデータのバックアップを作成することを強く推奨します。

製品インスタンスの評価モード

スマートライセンシングを有効にした後、Expressway は 90 日間の評価期間で実行されます。評価期間中、Expressway ではクラスタ関連の設定を許可できません。評価期間の後、Expressway が CSSM またはスマートソフトウェアマネージャオンプレミスに登録されていない場合、製品は不正な状態に移動し、製品が登録されるまで新しいデバイス登録を許可しません。

スマート ライセンスを有効にした後は、お使いの Expressway でオプション キーを使用することはできません。したがって、オプションキーが必要な Expressway 機能を使用する場合は、PAK ベースのライセンスを使用する必要があります。

コール タイプとライセンスに関する一般的な Expressway ライセンス情報を確認することをお勧めします。

スマートアカウントと仮想アカウントをセットアップする必要があります。詳細については、「Cisco スマートアカウント」を参照してください。

スマートライセンシングの設定

ここでは、Expressway Web インターフェイスのスマートライセンシング設定を使用して次を実行する方法について説明します。

- スマートライセンシングを有効にします。
- 事前に CSSM または Smart Software Manager On-Prem を使用して Expressway を登録および登録解除します。
- 登録およびライセンス承認を手動で更新します。

- CSSM または Smart Software Manager On-Prem にレポートされているシステムライセンスの使用情報を表示します。（ライセンスは組織のスマートアカウントに割り当てされ、デバイスに対してロックされません。）

（注） このセクションでは、Webインターフェイスについて説明します。スマートライセンシングのCLIコマンドの詳細については、このガイドの「コマンドリファレンス（*Command Reference*）」セクションを参照してください。

表 *8 : Expressway* のスマートライセンシング設定

フィールド	説明
Smart ライセンスモード	このExpressway製品インスタンスでスマートライセンシングを有効にします。このオプションを選択する前に、スマートライセンシングの設定セクションを確認してください。

フィールド	説明
トランスポートの設定	この Expressway 製品インスタンスが CSSM と通信して使用情報を送受信する方法を決定します。 **注意** Expressway 製品インスタンスがすでに登録されている場合、トランスポート設定をダイレクト（CSSM）から On-Prem に変更する場合、または逆の方法で変更する場合は、最初に登録を解除する必要があります。 *[ダイレクト（Direct）]*：Expressway が使用状況情報をインターネット上で直接送信します。追加のコンポーネントは不要です。これがデフォルトの設定です。 ダイレクトオプションを使用するには、Expressway で DNS を設定して、cisco.com の問題を解決できます。 Expressway 上でドメインと DNS を設定しない場合は、代わりに Smart Software Manager On-Prem またはプロキシサーバを選択できます。展開で DNS サーバを使用せず、インターネットに接続しないことを選択した場合には、切断モードで手動同期を使用する Cisco Smart Software Manager On-Prem を選択できます。 *Smart Software Manager On-Prem*：Expressway がオンプレミスの CSSM に使用情報を送信します。定期的な情報交換により、Smart Software Manager On-Prem と CSSM 間でデータベースの同期が維持されます。 **[URL]** フィールドに、**Smart Software Manager On-Prem** の正確なスマートトランスポート URL を必ず入力してください。「*SmartTransport*」のプレフィックスである衛星サーバのプロトコルと FQDN を入力します。次に、有効なトランスポート URL の例を示します。 *https://example.com/SmartTransport* Smart Software Manager On-Prem のインストールまたは設定の詳細については、https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager.html を参照してください。 プロキシサーバ：オプションでこの設定を使用して、Expressway がプロキシサーバを介してインターネット上で使用情報を送信できます。次の詳細を入力します。 • プロキシサーバの**プロキシアドレス** IPv4 アドレスまたは FQDN。 • **ポート**プロキシサーバがリクエストをリスニングするポート。 • **ユーザ名**プロキシサーバでの要求を承認するユーザ名です。 • **パスワード**認証済みユーザを認証する場合のパスワード。

フィールド	説明
ホスト名または IP アドレスを Cisco と共有しない	この Expressway 製品インスタンスのホスト名と IP アドレスを CSSM または Cisco Smart Software Manager On-Prem と交換する必要ない場合は、このチェックボックスをオンにします。
その他の操作	**[追加操作（Additional operations）]**ドロップダウンリストは、登録が成功するとアクティブになります。 • *[今すぐ承認を更新（Renew authorization now）]*：CSSM のネットワーク接続の問題によって自動承認ステータスの更新が失敗した場合は、この操作を実行します。 • *[今すぐ承認を更新（Renew authorization now）]*：CSSM のネットワーク接続の問題によって自動登録の更新が失敗した場合は、この操作を実行します。 • *[登録解除（Deregister）]*：製品は未登録モードに戻ります。製品で使用されるすべてのライセンス付与がバーチャルアカウントにすぐに戻されて、他の製品インスタンスで使用できるようになります。製品は、評価期間の終了まで評価モードに戻ります。
製品インスタンス登録トークン	CSSM または Smart Software Manager On-Prem から生成した製品インスタンス登録トークンを入力して製品を登録します。
すでに登録されている場合は、この製品インスタンスを再登録します	この Expressway 製品インスタンスを別の仮想アカウントに再登録するには、このチェックボックスをオンにします。
登録	**[登録（Register）]**をクリックして CSSM または Smart Software Manager On-Prem で Expressway を登録します。（登録に成功した後の**再登録**への変更。）
ライセンスのステータス	
登録ステータス（**Registration status**）	この Expressway 製品インスタンスの登録ステータスを表示します。 • 登録済み：製品が登録されます。 • 未登録：製品が登録されていません。 • 未登録：登録期限切れ：この製品の登録有効期限が切れています。 • 未登録：登録保留中 ：登録中です。 • 未登録：登録失敗：トークンが無効または期限切れのため、製品登録に失敗しました。

フィールド	説明
ライセンス認証ステータス	このExpressway製品インスタンスのライセンス認証ステータスを表示します。 • 認証済み：製品は認証され、準拠状態です。 • 認証の有効期限切れ：認証の有効期限が切れています。これは通常、製品がシスコと90日間連続して通信していない場合に発生します。 • コンプライアンス違反：ライセンスが不十分な状態で、本製品のステータスがコンプライアンスに従っていません。 • 使用中のライセンスなし：製品により消費されているライセンスがありません。 • 評価モード：製品は評価モードで、シスコにはまだ登録されていません。 • 期限切れ評価：評価期間が期限切れになっています。 • 適用外：製品が現在の登録ステータスを判断できません。
スマートアカウント	顧客のCiscoスマートアカウントに関する情報を表示します。スマートアカウントは、Cisco Software Centralの**[管理（Administration）]**セクションにある*[スマートアカウントの要求（Request Smart Account）]*オプションから作成されます。
バーチャルアカウント	会社の組織を反映する自己定義の要素。ライセンスと製品インスタンスを仮想アカウントに分配できます。CSSMまたはSmart Software Manager On-Premの管理者によって作成され、保守されています。管理者は、会社の資産を完全に可視化する必要があります。
輸出規制による機能限定	次の状態の1つが表示されます。 • 許可：この製品が登録されたトークン内でエクスポート制御機能が有効になります。 • 禁止：この製品が登録されたトークン内でエクスポート制御機能は有効にされません。 **[このトークンで登録されている製品の輸出規制による機能限定を許可する（Allow export-controlled functionality on the products registered with this token）]**チェックボックスは、輸出規制による機能限定の使用を許可されないスマートアカウントの場合には表示されません。
ライセンス使用状況	

フィールド	説明
使用詳細の更新	ライセンスの使用方法では、CSSM または Smart Software Manager On-Prem にレポートされているシステムライセンスの使用状況に関する概要と詳細情報を提供します。情報は 6 時間ごとに自動更新されます。 必要に応じて、**[使用状況の詳細の更新（Update usage details）]** をクリックして、使用詳細を手動で更新できます。ただし、これはリソースを多用する操作であり、頻繁に使用することは推奨しません。システムのサイズによっては、1 分以上かかる場合があります。
ライセンスタイプ	ライセンスタイプ（リッチメディアセッションまたはルーム/デスクトップ登録）を一覧表示します。
現在の使用状況	ライセンスタイプ別に現在のライセンス使用量が表示されます。ライセンスタイプが使用されていない（消費されている）場合、ここには表示されません。
ステータス（Status）	各ライセンス タイプのステータスが表示されます。 • 承認の期限切れ：承認された期間が期限切れです。 • 評価モード：エージェントは、この資格の評価期間を使用しています。 • 期限切れ評価：評価期間が期限切れになっています。 • 承認済み：準拠（承認済み）です。 • 無効：エラー状態です。 • 無効なタグ： 資格タグは無効です。 • 未承認：強制モードは適用されません。 • コンプライアンス違反：コンプライアンス違反。 • 待機中：許可要求の応答を待っている間の、許可要求後の初期状態です。

スマート ライセンスの設定

このセクションでは、スマートライセンシングを設定するために必要なタスクについて説明します。

はじめる前に

スマートライセンシングを有効にする前にの注意事項およびその他の情報を確認してください。

次の追加の設定に関する警告が適用されます。

- サポートされているトランスポートプロトコルは、Expressway と CSSM / Smart Software Manager On-Prem 間の HTTPS のみです。
- Expressway 製品インスタンスの登録の際に登録サーバで通信の問題が発生すると、登録が失敗して次のようなメッセージが表示されます。次の理由により、スマート ソフトウェア ライセンスの登録の前回の試行が進行中です：*HTTP* サーバー エラー：操作タイムアウト（*The last attempt to renew smart software licensing registration is in progress because of the following reason: HTTP Server Error 200: Operation timed out*）。

  製品インスタンスは、15 分間隔で再登録を試みます。現在の登録ステータスを確認するには、再試行するたびにページを最新の情報に更新します。再試行中に通信の問題が解決した場合は、製品が登録されます。製品が複数回の再試行後に登録されない場合は、登録サーバに何らかの通信問題があるかどうかを確認し、手動で製品インスタンスを再登録します。
- システムを復元する場合、復元されるスマートライセンス設定は、バックアップを同じシステムに復元するか、あるいは別のシステムに復元するかによって異なります。
  - 同じシステムに復元する場合は、スマートライセンスが有効になり、復元されたシステム上で登録設定が復元されます。
  - 別のシステムに復元する場合は、復元されたシステム上でスマートライセンスが有効になりますが、登録キーを使用して製品を再度登録する必要があります。
- Smart Software Manager On-Prem を設定する場合は、必ずスマートトランスポートコンポーネントの正確な URL を入力してください（詳細および スマートライセンシングの設定の例を参照）。

プロセスのまとめ

1. タスク 1：製品インスタンスの登録トークンの取得
2. タスク 2：Expressway でのスマートライセンシングの有効化
3. タスク 3：Expressway のトランスポート設定を構成する
4. タスク 4：Cisco Smart Software Manager への登録

タスク 1：製品インスタンスの登録トークンの取得

このタスクでは、CSSM または Smart Software Manager On-Prem から製品インスタンス登録トークンを取得し、製品インスタンスを登録します。トークンは、エクスポート制御機能の使用または使用なしで生成できます。詳細については 、Cisco Software Central から確認できます 。

手順

ステップ 1 CSSM または Smart Software Manager On-Prem でスマートアカウントにログインします。

ステップ 2 Expressway に関連付ける仮想アカウントに移動します。

ステップ 3 製品インスタンス登録トークンを生成します。

ステップ 4 このトークンで登録された製品でエクスポート制御機能を有効にするには、**[このトークンで登録されている製品の輸出規制による機能限定を許可する（Allow export-controlled functionality on the products registered with this token）]** のチェックボックスを選択します。

注意 このオプションは、輸出規制機能に準拠している場合のみ使用します。

このチェックボックスをオンにして条件に同意して、この登録トークンに登録されている製品の高度な暗号化を有効にします。デフォルトでは、このチェックボックスはオンになっています。製品のエクスポート制御機能を禁止するには、このチェックボックスのチェックを外すことができます。

[このトークンで登録されている製品の輸出規制による機能限定を許可する（Allow export-controlled functionality on the products registered with this token）] のチェックボックスは、輸出規制による機能限定の使用を許可されないスマートアカウントの場合には表示されません。

ステップ 5 トークンをコピーするか、別の場所に保存します。

タスク 2：Expressway でのスマートライセンシングの有効化

このタスクにより、Expressway でのスマートライセンシングが有効になります。これを行う前に、スマート ライセンスの設定のセクションを確認してください。

手順

ステップ 1 Expressway Web インターフェイスで、**[メンテナンス（Maintenance）]** > **[スマートライセンシング（Smart licensing）]** に移動します。

ステップ 2 **[設定（Configuration）]** セクションで、**[スマートライセンシング モード（Smart Licensing mode）]** を *[オン（On）]*（デフォルトは *[オフ（Off）]*）に設定します。

ステップ 3 [保存（Save）] をクリックします。

タスク 3：Expressway のトランスポート設定を構成する

このタスクでは、Expressway が CSSM と通信するためのトランスポート設定を選択します。

手順

ステップ 1 Expressway Web インターフェイスで、**[メンテナンス（Maintenance）]** > **[スマートライセンシング（Smart licensing）]** に移動します。

ステップ 2 **[トランスポート設定（Transport settings）]** に移動し、次のいずれかのトランスポートオプションを選択します。

- *[ダイレクト（Direct）]*：Expressway が使用状況情報をインターネット上で直接送信します。追加のコンポーネントは不要です。これはデフォルトです。
- *Smart Software Manager On-Prem*：Expressway がオンプレミスの CSSM に使用情報を送信します。
- プロキシサーバ： Expressway がプロキシサーバを使用し、インターネット経由で使用情報を送信します。

トランスポート設定の詳細については、スマートライセンシングの設定を参照してください。Expressway 製品インスタンスがすでに登録されている場合、トランスポート設定をダイレクト（CSSM）から On-Prem に変更する場合、または逆の方法で変更する場合は、最初に登録を解除する必要があることを覚えておいてください。

ステップ 3 この製品インスタンスのホスト名と IP アドレスを CSSM または Cisco Smart Software Manager On-Prem と交換する必要はない場合は、**[ホスト名または IP アドレスをシスコと共有しない（Do not share my hostname or IP address on-Prem）]** をオンにしてください。

ステップ 4 [保存（Save）] をクリックします。

タスク 4：Cisco Smart Software Manager への登録

このタスクは、Expressway を CSSM または Smart Software Manager On-Prem に登録します。登録するまで、製品は評価モードで実行されます。製品インスタンス登録トークンが必要です（タスク 1：製品インスタンスの登録トークンの取得を参照）、トランスポート設定は前のタスクの説明に従って設定する必要があります。

手順

ステップ 1 Expressway Web インターフェイスで、**[メンテナンス（Maintenance）]** > **[スマートライセンシング（Smart licensing）]** に移動します。

ステップ 2 **[登録（Registration）]** セクションで、CSSM または Smart Software Manager On-Prem を使用して生成した製品インスタンス登録トークンを貼り付けます。

ステップ 3 [登録（Register）] をクリックして、登録プロセスを完了します。（正常に登録されると、ボタンは **[再登録（Reregister）]** に変わります。）

ステップ 4 **[ライセンスの使用状況レポート（License Usage Report）]** セクションで、**[使用状況の詳細の更新（Update Usage Details）]** をクリックして、システムのライセンスの使用状況の情報を手動で更新します。これはリソースを大量に消費し、システムのサイズによっては数分かかる場合があります。

スマートライセンシングの設定が完了しました。

次のセクションでは、スマートライセンシングの登録と承認を管理する方法について説明します。この例では、Expressway のホスト名が将来変更された場合や、そのホスト名を永続的にシャットダウンする場合の処理も含まれます。

スマートライセンシングの登録および承認管理

このセクションでは、次を含むスマートライセンシング操作について説明します。

- 認証の更新：ライセンスタイプの下に表示されるすべてのライセンスのライセンス認証ステータスを手動で更新するのに使用します。ライセンス認証は 30 日ごとに自動的に更新されます。認証ステータスは、CSSM または Smart Software Manager On-Prem に接続していない場合、90 日後に期限切れになります。
- 登録の更新：登録情報を手動で更新するために使用します。初回登録の有効期間は 1 年です。登録の更新は、製品が CSSM または Smart Software Manager On-Prem に接続されている場合は、6 ヵ月ごとに自動的に行われます。
- 登録解除：事前に CSSM またはスマート ソフトウェア マネージャから Expressway を切断するために使用します。製品は、評価期間の終了まで評価モードに戻ります。製品で使用されているすべてのライセンス権限は、バーチャルアカウントにすぐにリリースされ、他の製品インスタンスで使用できるようになります。
- *Cisco Smart Software Manager* へのライセンスの再登録：事前に CSSM または Smart Software Manager On-Prem を使用して Expressway を再登録するために使用します。新しいバーチャル アカウントのトークンを使用して再登録すると、製品が異なるバーチャル アカウントに移行される場合があります。

認証を更新

この手順を使用すると、**ライセンス**タイプの下に表示されるすべてのライセンスのライセンス認証ステータスを手動で更新できます。このプロセスでは、製品が CSSM または Smart Software Manager On-Prem に登録されていることが前提になります。

手順

ステップ 1 Expressway Web インターフェイスで、**[メンテナンス（Maintenance）]** > **[スマートライセンシング（Smart licensing）]** に移動します。

ステップ 2 **[アクション（Action）]** セクションの **[追加操作（Additional operations）]** ドロップダウンリストから、*[今すぐ認証の更新（Renew registration now）]* を選択します。

ステップ 3 [保存（Save）] をクリックします。

Expressway は、Cisco Smart Software Manager または Smart Software Manager On-Prem に要求を送信し、「ライセンス認証ステータス」と Cisco Smart Software Manager または Smart Software Manager On-Prem が Cisco Expressway にステータスを返送します。

ステップ 4 **[ライセンスの使用状況レポート（License Usage Report）]** セクションで、**[使用状況の詳細の更新（Update Usage Details）]** をクリックして、システムのライセンスの使用状況の情報を手動で更新します。これはリソースを大量に消費し、システムのサイズによっては数分かかる場合があります。

登録の更新

製品を Cisco Smart Software Manager または Smart Software Manager On-Prem に登録する間、製品の識別にはセキュリティアソシエーションが使用され、登録証明によってアンカーが設定されます。この有効期限（登録期間）は 1 年間です。これは登録トークン ID の有効期限とは異なり、トークンの時間制限が有効になります。この登録期間は6か月ごとに自動的に更新されます。ただし、問題がある場合は、この登録期間を手動で更新できます。

このプロセスでは、製品が CSSM または Smart Software Manager On-Prem に登録されていることが前提になります。

手順

ステップ 1 Expressway Web インターフェイスで、**[メンテナンス（Maintenance）]** > **[スマートライセンシング（Smart licensing）]** に移動します。

ステップ 2 **[アクション（Action）]** セクションの **[追加操作（Additional operations）]** ドロップダウンリストから、*[今すぐ登録の更新（Renew registration now）]* を選択します。

ステップ 3 [保存（Save）] をクリックします。

Expressway は、「登録ステータス」と CSSM / Smart Software Manager On-Prem がステータスを Cisco Unified Communications Manager にレポートするために、CSSM または Smart Software Manager On-Prem に要求を送信します。

ステップ 4 **[ライセンスの使用状況レポート（License Usage Report）]** セクションで、**[使用状況の詳細の更新（Update Usage Details）]** をクリックして、システムのライセンスの使用状況の情報を手

動で更新します。これはリソースを大量に消費し、システムのサイズによっては数分かかる場合があります。

登録解除

CSSM または Smart Software Manager On-Prem から Expressway を登録解除し、現在の仮想アカウントからすべてのライセンスをリリースするには、次の手順を実行します。この手順では、Expressway と CSSM/Smart Software Manager On-Prem の接続も切断します。製品で使用されているすべてのライセンス権限は、バーチャルアカウントにリリースされ、他の製品インスタンスで使用できるようになります。

Expressway が CSSM または Smart Software Manager On-Prem に接続できず、製品がまだ登録解除されている場合は、警告メッセージが表示されます。メッセージによって、ライセンスを解放するために、CSSM/Smart Software Manager On-Prem から製品を手動で削除する必要があるという通知が表示されます。

手順

ステップ 1 Expressway Web インターフェイスで、**[メンテナンス（Maintenance）]** > **[スマートライセンシング（Smart licensing）]** に移動します。

ステップ 2 **[アクション（Action）]** セクションの **[追加操作（Additional operations）]** ドロップダウンリストから、**[登録解除（Deregister）]** を選択します。

ステップ 3 [保存（Save）] をクリックします。

ステップ 4 **[ライセンスの使用状況レポート（License Usage Report）]** セクションで、**[使用状況の詳細の更新（Update Usage Details）]** をクリックして、システムのライセンスの使用状況の情報を手動で更新します。これはリソースを大量に消費し、システムのサイズによっては数分かかる場合があります。

Cisco Smart Software Manager への登録

CSSM または Smart Software Manager On-Prem を使用して Expressway を再登録するには、次の手順を使用します。製品インスタンス登録トークンが必要です（スマートライセンシングの登録および承認管理を参照）。

手順

ステップ 1 Web インターフェイスから、**[メンテナンス（Maintenance）]** > **[スマートライセンシング（Maintenance Smart licensing）]** を選択します。
スマートライセンスウィンドウが表示されます。

ステップ 2 **[登録（Registration）]** セクションで、CSSM または Smart Software Manager On-Prem を使用して生成した「登録トークンキー」を貼り付けます。

ステップ 3 **再登録**をクリックして、再登録プロセスを完了します。

ステップ 4 **[ライセンスの使用状況レポート（License Usage Report）]** セクションで、**[使用状況の詳細の更新（Update Usage Details）]** をクリックして、システムのライセンスの使用状況の情報を手動で更新します。これはリソースを大量に消費し、システムのサイズによっては数分かかる場合があります。

Expressway のホスト名への変更を登録する方法

Expressway のホスト名を変更して CSSM の変更を反映する場合は、**Expressway スマートライセンシングの Web ページ**に移動し、「**[今すぐ登録の更新 (Renew Registration Now]**」 をクリックします)

Expresswayが永続的にシャットダウンされている場合は、最初に登録を解除します。

Expressway マシンを永続的にシャットダウンする場合は、最初に Expressway スマートライセンシング Web ページから製品インスタンスの登録を解除することをお勧めします。これは、未使用の製品インスタンスが CSSM に残るのを避けるためです。

忘れた場合は、CSSM ポータルから Expressway 製品インスタンスを削除するための代替方法があります。

再起動や一時的なシャットダウンでは、この手順は不要です。

PAK ベースのライセンスからスマートライセンスへの変換

PAK ベースのライセンスを現在使用している場合は、このセクションでスマートライセンシングへの変換方法について説明します。ライセンス登録ポータルでライセンス変換を行う事も、Cisco Smart Software Support Service の契約をアクティブにしている場合は Cisco Smart Software Manager を使用することもできます。PAK ベースのライセンスを変換できるのは、PAK で使用可能な同等のスマートライセンスがある場合のみです。

未処理の PAK または部分的に処理された PAK の変換

ライセンス登録ポータルの使用

手順

ステップ 1 ライセンス登録ポータルにログインします。

ステップ 2 [**PAK** または **トークン**] タブをクリックします。

ステップ 3 **[仮想アカウント]** ドロップダウンリストから、変換する PAK ライセンスを持つ仮想アカウントを選択します。

ステップ 4 変換する未設定または部分的に処理された PAK の横にあるチェックボックスをオンにします。

ステップ 5 青の矢印アイコンをクリックし、ドロップダウンリストから **[スマートライ センシングに変換（Covert to Smart Licensing）]** を選択します。
[スマートエンタイトルメントへの変換] ダイアログボックスが表示されます。

ステップ 6 ライセンスが仮想アカウントに割り当てられていない場合は、**[仮想アカウント（Virtual Account）]** ドロップダウンリストから仮想アカウントを選択します。

ステップ 7 **[変換する数量]** の列に、変換するライセンスの数を入力して **[送信（Submit）]** を クリックします。

ステップ 8 確認のメッセージが表示されます。選択した機能がスマートな権利に正常に変換されたため、**[閉じる（Close）]** をクリックします。

ステップ 9 **[ステータス（Status）]** 列のライセンスのステータスを確認します。これは、完全な変換の場合は *Converted*、部分的な変換の場合は *Partially* を表します。

Cisco Smart Software Manager の使用

手順

ステップ 1 Cisco Smart Software Manager にログインします 。

ステップ 2 **[スマートライセンシングに変換]** > **[PAKに変換]** タブをクリックします。

ステップ 3 変換する PAK を見つけて、**[アクション]** 列の **[スマートライセンシングに変換]** リンクをクリックします。
[スマートソフトウェアライセンスに変換] ダイアログ ボックスが表示されます。

ステップ 4 **[宛先仮想アカウント]** ドロップダウンリストから、宛先仮想アカウントを選択します。

ステップ 5 **[SKU]** セクションで、SK/PAK をチェックし、**[変換する数量]** 列に変換するライセンス数を入力 します。部分的な契約の変更が許可されていない場合は、すべてのライセンスを SKU に変換する必要があります。

ステップ 6 [Next] をクリックします。

ステップ 7 詳細を確認して、**[ライセンスの変換（Convert Licenses）]** をクリックします。

ステップ 8 PAK ライセンスが正常に変換されたことを確認するには、**[インベントリ（Inventory）]** > **[ライセンス（Licenses）]** をクリックします。

PAK 登録からデバイスまたは製品への変換

ライセンス登録ポータルの使用

手順

ステップ 1 ライセンス登録ポータルにログインします。

ステップ 2 [デバイス] タブをクリックします。

ステップ 3 **[仮想アカウント（Virtual Account）]** ドロップダウンリストから、デバイスまたは製品に関連付けられている仮想アカウントを選択します。

ステップ 4 変換するライセンスが含まれているデバイスを選択します。

ステップ 5 青の矢印アイコンをクリックして、[スマートライセンシングに**ライセンスを変換する**（Covert licenses to Smart Licensing）] をクリックします。**[スマートエンタイトルメントへの変換]** ダイアログボックスが表示されます。

いずれかの PAK ライセンスが変換の対象とならない場合、*[対象外]* ステータスが **[変換する数量]** の列に表示されます。

ステップ 6 **[宛先仮想アカウント]** ドロップダウンリストから、宛先仮想アカウントを選択します。

ステップ 7 SKU を選択し、変換するライセンスの数を選択します。

ステップ 8 [送信（Submit）] をクリックします。

ライセンス変換が完了すると、スマートエンタイトルメント（ライセンス）が CSSM のスマートアカウントに反映されます。

Cisco Smart Software Manager の使用

手順

ステップ 1 Cisco Smart Software Manager にログインします 。

ステップ 2 **[スマートライセンシング変換（Convert to Smart Licensing）]** > **[ライセンスを変換（Convert Licenses）]** をクリックします。

ステップ 3 変換するライセンスが含まれているデバイスを選択し、**[アクション]** カラムの **[スマートライセンシングに変換]** リンクをクリックします。

ステップ 4 **[接続先の仮想アカウント]**フィールドで、接続先の仮想アカウントを選択します。**[スマートエンタイトルメントへの変換]** ダイアログ ボックスが表示されます。

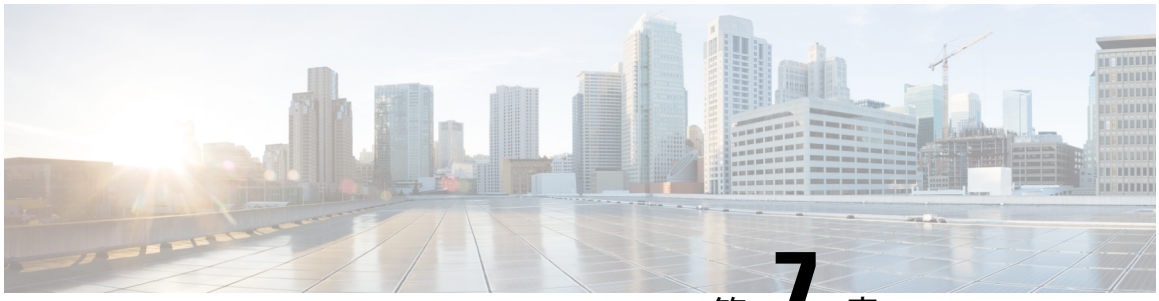
いずれかの PAK ライセンスが変換の対象とならない場合、*[*対象外*]* ステータスが **[変換する数量]** の列に表示されます。

ステップ 5 SKU を選択し、**[変換する数量]** の列に変換するライセンスの数を入力 します。

ステップ 6 [Next] をクリックします。

ステップ 7 詳細を確認して、**[ライセンスの変換（Convert Licenses）]** をクリックします。

ステップ 8 PAK ライセンスが正常に変換されたことを確認するには、**[インベントリ（Inventory）]** > **[ライセンス（Licenses）]** をクリックします。



第 7 章

セキュリティの管理

このセクションでは、Expresswayのセキュリティの概念と設定について説明します。（ユーザアカウントの管理、デバイス認証、および登録アクセス制御に関する情報は、このガイドの後の別の章で説明します。）

セキュリティの基本

保管中のデータ

X8.11 以降、すべてのソフトウェアインストールには一意の信頼できるルートが使用されるようになっています。それぞれの Expressway システムには、そのシステムにローカルなデータを暗号化するために使用される一意のキーがあります。これにより、保管中のデータのセキュリティが次のように強化されます。

- X8.11 より前のバージョンを X8.11 以降にアップグレードすると、新しいキーが作成されます。最初の再起動時に、このキーを使用してすべてのデータが暗号化されます。

- このシステムから取得したデータを復号できるのは、このキーのみです。ほかのExpressway キーでは、このシステムのデータを復号することはできません。
- キーは UI 上で公開される事も、ローカルでもリモートでもログは記録されません。

TLS および証明書

クライアントとサーバ間の接続で TLS 暗号化を正常に機能させるためには以下が必要です。

- サーバには、アイデンティティを検証する認証局（CA）によって署名された証明書がインストールされている必要があります。
- クライアントはサーバが使用する証明書に署名した CA を信頼する必要があります。

Expressway では、TLS 接続で、クライアントまたはサーバとして Expressway を表すことができる証明書をインストールすることができます。Expressway は、HTTPS 経由のクライアント接続（通常は Web ブラウザから）を認証することもできます。また、LDAP サーバおよびHTTPS クライアント証明書の検証に使用されるCAの証明書失効リスト（CRL）をアップロードすることができます。Expresswayは、サーバ証明書署名要求（CSR）を生成することができます。そのため、これを行う外部メカニズムを使用する必要はありません。

（注） セキュアな通信（HTTPSおよびSIP/TLS）のために、Expresswayのデフォルトの証明書を、信頼できる CA が生成した証明書に置き換えることを推奨します。

表 *9:* 接続タイプ別の *Expressway* の役割

接続先	Expressway の役割
エンドポイント	TLS サーバ
LDAP サーバ	クライアント
2 つの Expressway システム間	どちらかの Expressway がクライアントになる可能性があります。もう一方の Expressway は TLS サーバです。
HTTPS 経由	Webブラウザはクライアントです。Expressway はサーバです。

（注） また、TLS用にLDAPサーバが正しく設定されていることを検証するためにサードパーティのLDAP ブラウザを使用することが推奨されます。

TLS は設定が難しい場合があります。たとえば、LDAP サーバで使用する場合は、TLS との接続を保護する前に、システムがTCP上で正しく動作することを確認することをお勧めします。

注意 証明書は RFC に準拠している必要があります。CA 証明書または CRL の期限は、CA によって署名された証明書が拒否される可能性があるため許可されません。

証明書および CRL ファイルは、Web インターフェイスを介して管理され、CLI を使用してインストールすることはできません。

証明書ベースの認証の設定

「証明書ベースの認証設定（Certificate-based authentication configuration）」ページ（**[メンテナンス（Maintenance）] > [セキュリティ（Security）] > [証明書ベースの認証設定（Certificate-based authentication configuration）]**）を使用して、クライアント ブラウザの証明書から Expressway が許可クレデンシャル（ユーザ名）を取得する方法を設定します。

この設定は、**[クライアント証明書ベースのセキュリティ（Client certificate-based security）]**（[ネットワーク サービス] ページで定義）を *[証明書ベースの認証（Certificate-based authentication）]* に設定している場合に必要です。この設定により、標準的なログイン メカニズムが使用できなくなります。また、管理者（および Expressway 経由でアクセスした場合は FindMe アカウント）は通常、スマート カード（Common Access Card（CAC）とも呼ばれる）を介して提供された有効なブラウザ証明書を提示し、その証明書に適切な認証レベルの適切なクレデンシャルが含まれている場合にのみログインできることを意味します。

証明書ベースの認証の有効化

次に、証明書ベースの認証を有効にするための推奨手順について説明します。

手順

ステップ 1 Expressway の信頼できる CA 証明書とサーバ証明書ファイルを（「**信頼された CA 証明書（Trusted CA certificate）**」ページと「**サーバ証明書（Server certificate）**」ページそれぞれに）追加します。

ステップ 2 証明書失効リストを設定します（「**CRL 管理（CRL management）**」ページ）。

ステップ 3 「**クライアント証明書テスト（Client certificate testing）**」ページを使用して、使用するクライアント証明書が有効であることを確認します。

ステップ 4 **[クライアント証明書ベースのセキュリティ（Client certificate-based security）]** を *[証明書の検証（Certificate validation）]* に設定します（「**システム管理（System Administration）**」ページ）。

ステップ 5 Expressway を再起動します。

ステップ 6 「**クライアント証明書テスト（Client certificate testing）**」ページを再度使用して、必要な正規表現と形式パターンをセットアップし、証明書からユーザ名クレデンシャルを抽出します。

ステップ 7 正しいユーザ名が証明書から取得されていることが確認された場合にのみ、**[クライアント証明書ベースのセキュリティ（Client certificate-based security）]** を *[*証明書ベースの認証（*Certificate-based authentication*）*]* に設定します。

認証と許可

Expressway が証明書ベースの認証モードで動作しているときに、ユーザ認証は Expressway 外にあるプロセスを通じて管理されます。

ユーザが Expressway にログインしようとすると、Expressway はクライアント ブラウザからの証明書を要求します。ブラウザはカード リーダと連携してスマート カードから証明書を取得します（または、証明書がすでにブラウザにロードされている場合もあります）。カードまたはブラウザから証明書をリリースするには、通常、ユーザはPINを入力して自分自身を認証するように求められます。Expresswayが受信したクライアント証明書が有効な場合（信頼できる認証局によって署名され、期限が切れておらず、CRL で失効になっていない）、ユーザは認証されていると見なされます。

ユーザの許可レベル（読み書き、読み取り専用など）を特定するには、Expresswayがユーザの許可ユーザ名を証明書から抽出し、それを関連するローカルまたはリモートの許可メカニズムに提示する必要があります。

（注） クライアント証明書が（PIN またはその他の何らかのメカニズムによって）保護されていない場合は、Expressway への認証されていないアクセスが可能になることがあります。この保護の欠如は、証明書がブラウザに保存されていない場合にも該当しますが、証明書ストアのパスワード保護を許可するブラウザもあります。

証明書からのユーザ名の取得

ユーザ名はクライアント ブラウザの証明書から **[正規表現（Regex）]** フィールドと **[ユーザ名の形式（Username format）]** フィールド（「**証明書ベースの認証設定（Certificate-based authentication configuration**）」ページ上）で定義されたパターンに従って抽出されます。

- **[正規表現（Regex）]** フィールドに（**?<name>regex**）シンタックスを使用してキャプチャ グループ用の名前を指定し、関連付けられた **[ユーザ名の形式（Username format）]** フィールドで一致サブパターンを置換できるようにします。次に例を示します。

  /(Subject:.*, CN=(?<Group1>.*))/m.

  ここで定義する正規表現は、*PHP* 正規表現のガイドラインに準拠する必要があります。

- **[ユーザ名の形式（Username format）]** フィールドには、固定テキストと **[正規表現（Regex）]** で使用したキャプチャ グループの名前を組み合わせて含めることができます。各キャプチャ グループ名を#で区切ります。例：**prefix#Group1#suffix** 各キャプチャ グループ名は正規表現の処理から取得されたテキストに置き換えられます。

「クライアント証明書のテスト」ページを使用して、**[正規表現（Regex）]** と **[ユーザ名の形式（Username format）]** のさまざまな組み合わせを証明書に適用した結果をテストできます。

緊急アカウントと証明書ベースの認証

高度なアカウント セキュリティ モードでは、リモート認証だけでなく、認証サーバが利用できない場合のために緊急アカウントも指定する必要があります。高度なアカウント セキュリティ モードの設定を参照してください。

証明書ベースの認証を使用している場合、緊急アカウントでは、クレデンシャルの一致する有効な証明書を提示することで認証できる必要があります。

緊急アカウントのクライアント証明書を作成し、CN を [ユーザ名の形式（Username format）] と一致させ、この証明書を緊急管理者の証明書ストアにロードする必要があります。

信頼された CA 証明書リストの管理

「信頼できる CA 証明書（Trusted CA certificate）」 ページ（**[メンテナンス（Maintenance）]** > **[セキュリティ（Security）]** > **[信頼できる CA 証明書（Trusted CA certificate）]**）で、この Expressway が信頼する証明局（CA）の証明書のリストを管理できます。Expressway への TLS 接続が証明書検証を要求したときは、Expressway に提示された証明書が、このリストの信頼できる CA によって署名され、ルート CA に対する完全なトラスト チェーン（中間 CA）がある必要があります。

- 1 つ以上の CA 証明書を含む新しいファイルをアップロードするには、**[参照（Browse）]** をクリックして必要な PEM ファイルの場所を指定し、**[CA 証明書の追加（Append CA certificate）]** をクリックします。これにより、新しい証明書が CA 証明書の既存リストに加えられます。特定の発行者およびサブジェクトの既存の証明書を交換する場合は、手動で以前の証明書を削除する必要があります。
- 現在アップロードされたすべての CA 証明書をシステムの信頼できる CA 証明書の元のリストと交換するには、[Reset to default CA certificate] をクリックします。
- 現在アップロードされた信頼できる CA 証明書のリスト全体を表示する場合、人間可読形式で表示するには **[Show all (decoded)]** をクリック、または raw 形式でファイルを表示するには **[Show all (PEM file)]** をクリックします
- 個別の信頼できる CA 証明書を表示するには、特定の CA 証明書の行で **[View (decoded)]** をクリックします。
- 1 つ以上の CA 証明書を削除するには、該当する CA 証明書の隣にあるボックスにチェックを入れて、[Delete] をクリックします。

（注） TLS の暗号化された LDAP を使用したリモート アカウント認証の設定（アカウント認証用）を確認する証明書失効リストを有効にしている場合は、信頼できるCA証明書ファイルにPEMでエンコードされた CRL データを追加する必要があります。

デフォルトで含まれるルート CA

Expressway X12.6 以降には、次の信頼されたルート CA が含 まれます。*Cisco Intersection CA* バンドルの一部としてインストールされます 。

- O=Internet Security Research Group, CN=ISRG Root X1
- O=Digital Signature Trust Co., CN=DST Root CA X3

Expressway のサーバ証明書の管理

サーバ証明書ページ（[メンテナンス（Maintenance）] > [セキュリティ（Security）] > [サーバ証明書（Server certificate）]）を使用して Expressway サーバ証明書を管理します。Expressway は、HTTPS 経由で TLS 暗号化および Web ブラウザを使用してクライアントシステムと通信するときに Expressway を識別します。

現在ロードされている証明書の詳細を表示して、CSR の生成、新しい証明書のアップロード、ACME サービスを設定できます。これらのタスクについては、「Expressway 設定ガイド」ページの 「*Cisco Expressway* 証明書の作成と使用導入ガイド」を参照してください。

（注） RSA キーに基づく証明書を使用することを強く推奨します。

DSA キーに基づく証明書など他のタイプの証明書はテストされておらず、あらゆるシナリオで Expressway と連携するとは限りません。

ACME サービスの使用

X12.5 以降、Cisco Expressway シリーズでは、ACME (AutomatedCertificate Management Environment) プロトコルをサポートするようになっています。このプロトコルにより、Let's Encrypt などの認証局から Expressway-E に署名済みの証明書を自動的に導入することが可能になります。

サーバ証明書とクラスタ化システム

CSR の生成時には、1 つの要求および秘密キーの組み合わせがそのピア専用に生成されます。Expresswayのクラスタがある場合は、各ピアで個別の署名要求を生成する必要があります。これらの要求はその後、認証局に送信し、返されたサーバ証明書を関連する各ピアにアップロードする必要があります。

正しいサーバ証明書が適切なピアにアップロードされていることを確認する必要があります。そうでないと、各ピアに保存された秘密キーがアップロードされた証明書に対応しません。

サーバ証明書とユニファイドコミュニケーション

モバイルおよびリモートアクセスを導入する場合は、Unified Communication と Expressway の証明書要件の詳細については、「Expressway 設定ガイド」ページの「*Cisco Expressway* 証明書の作成と使用導入ガイド」を参照してください。

証明書失効リスト（CRL）の管理

証明書失効リストファイル（CRL）は、TLS/HTTPS を介して Expressway と通信するクライアントブラウザおよび外部システムにより提示される証明書を検証するために Expressway によって使用されます。CRL は、廃棄され Expressway との通信に使用できなくなった証明書を識別します。

TLS/HTTPS クライアントおよびサーバ証明書に署名する CA の CRL データをアップロードすることを推奨します。イネーブルの場合、CRL のチェックはトラストチェーンのすべての CA に適用されます。

証明書失効ソース

Expressway は複数のソースから証明書失効情報を取得できます。

- CRL 分散ポイントからの CRL データの自動ダウンロード
- 証明書内のチェック対象 OCSP（Online Certificate Status Protocol）レスポンダ URI 経由（SIP TLS のみ）
- CRL データの手動アップロード
- Expressway の**信頼できる CA 証明書**ファイル内に組み込まれた CRL データ

制限事項と使用上のガイドライン

次の制約事項および使用上のガイドラインが適用されます。

- SIP TLS 接続を確立するときに、設定ページの **[証明書失効確認（Certificate revocation checking）][SIP]**の設定が CRL データ ソースに適用されます。
- 自動的にダウンロードされた CRL ファイルが、手動でロードされた CRL ファイルを上書きする場合（SIP TLS 接続を確認する場合、手動でアップロードされた CRL データと自動でダウンロードされた CRL データの両方を使用する可能性がある場合は除く）
- 外部ポリシーサーバによって提示された証明書を検証する際に、Expressway は手動でロードされた CRL のみを使用します。

- リモート ログイン アカウントを認証するために LDAP サーバの TLS 接続を確認する場合、Expressway は**信頼できる CA 証明書（[ツール（Tools）]> [セキュリティ（Security）]> [信頼できる CA 証明書（Trusted CA certificate）]**）に組み込まれた CRL データのみを使用します。

  LDAP 接続の場合、Expressway はサーバの証明書配布ポイントの URL または発行する CA 証明書から CRL をダウンロードしません。また、[CRL 管理（CRL management）] ページの手動または自動更新設定も使用しません。

自動 CRL 更新

（注） 自動 CRL 更新を実行するように Expressway を設定することを推奨します。これにより、最新の CRL が証明書の検証に使用できるようになります。

手順

ステップ 1 **[メンテナンス（Maintenance）]>[セキュリティ（Security）]>[CRL 管理（CRL management）]** に移動します。

ステップ 2 **[自動 CRL 更新（Automatic CRL updates）]** を *[有効（Enabled）]* に設定します。

ステップ 3 Expressway が CRL ファイルを取得できる **HTTP/HTTPS 分散ポイント**のセットを入力します。

（注）
- 新しい行にそれぞれ分散ポイントを指定する必要があります。
- HTTP/HTTPS 分散ポイントのみがサポートされます。HTTPS を使用する場合、分散ポイントのサーバ自体に有効な証明書が必要です。
- PEM および DER エンコード CRL ファイルがサポートされています。
- 分散ポイントは、CRL ファイルまたは複数の CRL ファイルを含む ZIP および GZIP アーカイブを直接示す場合があります。
- URL またはダウンロードしたアーカイブから解凍されたファイルのファイル拡張子は、Expressway がその基盤となるファイル タイプを決定するため、重要ではありませんが、代表的な URL は次の形式となります。
  - http://example.com/crl.pem
  - http://example.com/crl.der
  - http://example.com/ca.crl
  - https://example.com/allcrls.zip
  - https://example.com/allcrls.gz

ステップ 4 **[Daily update time]** を入力します（UTC 単位で）。これは、Expressway が分散ポイントからその CRL の更新を試行するおおよその時刻です。

ステップ 5 [保存（Save）] をクリックします。

手動 CRL 更新

CRL ファイルは Expressway に手動でアップロードできます。外部ポリシー サーバによって提示された証明書は、手動でロードされた CRL に対してのみ検証できます。

手順

ステップ 1 **[メンテナンス（Maintenance）]** > **[セキュリティ（Security）]** > **[CRL 管理（CRL management）]** に移動します。

ステップ 2 **[参照（Browse）]** をクリックして、ファイル システムから必要なファイルを選択します。また、PEM エンコード形式である必要があります。

ステップ 3 [CRL ファイルのアップロード（Upload CRL file）] をクリックします。

これによって、選択したファイルがアップロードされ、以前にアップロードした CRL ファイルが置換されます。

Expressway から手動でアップロードされたファイルを削除する場合は、**[失効リストの削除（Remove revocation list）]** をクリックします。

注：認証局の CRL が期限切れの場合、その CA から発行されたすべての証明書が無効として扱われます。

オンライン証明書ステータス プロトコル（OCSP）

Expressway は OCSP レスポンダとの接続を確立して特定の証明書のステータスを照会することができます。Expressway は使用する OCSP レスポンダを、確認する証明書に示されているレスポンダ URI から決定します。OCSP レスポンダは「良好（good）」、「失効（revoked）」、または「不明（unknown）」で証明書のステータスを送信します。

OCSP の利点は、失効リスト全体をダウンロードする必要がないことです。OCSP は SIP TLS 接続のみでサポートされます。OCSP を有効にする方法については、以下を参照してください。

OCSP レスポンダへ接続するには、Expressway-E からのアウトバウンド通信が必要です。使用している OCSP レスポンダのポート番号（通常はポート 80 または 443）をチェックし、Expressway-E からそのポートへのアウトバウンド通信が可能であることを確認します。

SIP TLS 接続を確認する失効の設定

また、証明書失効確認が SIP TLS 接続でどのように管理されるかを設定する必要があります。

1. **[Configuration]** > **[SIP]** を選択します。
2. **[証明書失効確認（Certificate revocation checking）]** セクションまでスクロールし、適宜設定を行います。

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：*[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。

MRA オンボーディングの mTLS クライアント証明書検証の管理

mTLS の CA 証明書ページには、**「信頼できる CA 証明書リストの管理（Managing the Trusted CA Certificate List）」**ページ（**[メンテナンス（Maintenance）]**> >**[セキュリティ（Security）]**> **[信頼できる CA 証明書（Trusted CA certificate）]**）からアクセスできます。このページが適用されるのは、Cisco Unified Communications 製品でモバイルおよびリモート アクセス（MRA）用に Expressway を使用していて、アクティベーション コードによるオンボーディングが MRA に対して有効にされている場合のみです。

クライアント証明書のテスト

ここでは、**「クライアント証明書テスト（Client certificate testing）」**ページ（**[メンテナンス（Maintenance）]**>**[セキュリティ（Security）]**> **[クライアント証明書テスト（Client certificate testing）]**）を使用して、クライアント証明書を確認してから、ネットワーク サービス を有効にします。方法は以下のとおりです。

- Expressway の現在の信頼できる CA リストおよびロードされている場合は失効リスト（証明書失効リスト（CRL）の管理）を参照）と照合して確認し、クライアント証明書が有効であるかどうかをテストします。
- 証明書の許可クレデンシャル（ユーザ名）を取得する正規表現とテンプレート パターンを適用した結果をテストします。

ローカルファイルシステムまたはブラウザで現在ロードされている証明書について、証明書とテストできます。

証明書が有効かどうかをテストするには

手順

ステップ 1 [証明書の送信元（Certificate source）] を選択します。次のいずれかを選択できます。

- PEM またはプレーン テキストのいずれかの形式のファイル システムからテスト ファイルをアップロードする（この場合は、**[参照（Browse）]** をクリックしてテストする証明書ファイルを選択します）。
- 現在ブラウザにロードされている証明書と照合してテストする（システムが *[*証明書の検証（*Certificate validation*）*]* を使用するようにすでに設定されていて、現在、証明書がロードされている場合にのみ使用できます）。

ステップ 2 **[証明書ベースの認証パターン（Certificate-based authentication pattern）]** セクションを無視します。このセクションは許可クレデンシャルを証明書から抽出する場合にのみ使用します。

ステップ 3 [証明書の確認（Check certificate）] をクリックします。
テストの結果が **[証明書のテスト結果（Certificate test results）]** セクションに表示されます。

証明書から許可クレデンシャル（ユーザ名）を取得するには

手順

ステップ 1 **[証明書の送信元（Certificate source）]** を上記で説明したように選択します。

ステップ 2 **[正規表現（Regex）]** フィールドと [ユーザ名の形式（Username format）] フィールドを必要に応じて設定します。これは、証明書内で該当する文字列パターンを検索する正規表現を指定することで、指定した証明書からユーザ名を抽出することを目的としています。現在、これらのフィールドはデフォルトで「**証明書ベースの認証設定（Certificate-based authentication configuration）**」ページの設定になるように設定されていますが、必要に応じて変更できます。

- **[正規表現（Regex）]** フィールドに（**?<name>regex**）シンタックスを使用してキャプチャグループ用の名前を指定し、関連付けられた **[ユーザ名の形式（Username format）]** フィールドで一致サブパターンを置換できるようにします。次に例を示します。

  /(Subject:.*, CN=(?<Group1>.*))/m.

  ここで定義する正規表現は、PHP 正規表現のガイドラインに準拠する必要があります。

- **[ユーザ名の形式（Username format）]** フィールドには、固定テキストと **[正規表現（Regex）]** で使用したキャプチャ グループの名前を組み合わせて含めることができます。各キャプチャ グループ名を#で区切ります。例：**prefix#Group1#suffix** 各キャプチャ グループ名は正規表現の処理から取得されたテキストに置き換えられます。

ステップ 3 [証明書の確認（Check certificate）] をクリックします。
テストの結果が **[証明書のテスト結果（Certificate test results）]** セクションに表示されます。**[結果の文字列（Resulting string）]** の項目はユーザ名クレデンシャルであり、関連する許可メカニズムと照合して確認され、ユーザの許可（アカウント アクセス）レベルが決定します。

ステップ 4 必要に応じて **[正規表現（Regex）]** フィールドと **[ユーザ名の形式（Username format）]** フィールドを変更し、正しい結果が得られるまでテストを繰り返すことができます。

（注） **[証明書の送信元（Certificate source）]** がアップロードされた PEM またはプレーン テキスト ファイルの場合は、テストを初めて実行したときに選択したファイルが一時的に Expressway へアップロードされます。

- 同じファイルに対して **[正規表現（Regex）]** と **[ユーザ名の形式（Username format）]** をさまざまに組み合わせてテストを続ける場合は、テストごとにファイルを再選択する必要はありません。
- ファイルシステムのテストファイルの内容を変更する、または別のファイルを選択する場合は、**[参照（Browse）]** を再度選択して、新しいファイルまたは変更したファイルを選択してアップロードします。

ステップ 5 [正規表現（Regex）] フィールドと [ユーザ名の形式（Username format）] フィールドをデフォルト値から変更して Expressway の実際の設定の値（[証明書ベースの認証設定（Certificate-based authentication configuration）] ページで指定）を使用した場合、[これらの設定を永続的にする（Make these settings permanent）] をクリックします。

（注）
- アップロードしたテスト ファイルは、ログイン セッションの終了時点で Expressway から自動的に削除されます。
- 正規表現は符号化された証明書のプレーンテキストバージョンに適用されます。システムは **openssl x509 -text -nameopt RFC2253 -noout** コマンドを使用して、符号化された形式からプレーン テキストの証明書を抽出します。

セキュア トラバーサルのテスト

このユーティリティは、Expressway-C と Expressway-E の間でセキュアな接続を確立できるかどうかをテストします。セキュアな接続は、ユニファイドコミュニケーションのトラバーサル ゾーンでは必須ですが、通常のトラバーサル ゾーンでは任意（推奨）です。

セキュア トラバーサルのテストが失敗した場合、可能な場合はこのユーティリティによって適切な解決策を示した警告が発行されます。

手順

ステップ 1 **Expressway-C で [メンテナンス（Maintenance）] > [セキュリティ（Security）] > [セキュア トラバーサルのテスト（Secure traversal test）]** に移動します。

ステップ 2 この Expressway-C とペアにする Expressway-E の FQDN を入力します。

ステップ 3 ペアの Expressway-E に表示されるとおりに、この Expressway-C の TLS 確認名を入力します。

この設定は、Expressway-E のトラバーサルゾーンの設定ページの SIP セクションにあります。

ステップ 4 [テスト接続（Test connection）] をクリックします。

セキュア トラバーサルのテスト ユーティリティは、トラバーサル ゾーンの両側のホストが互いに認識し合い、もう一方の証明書チェーンを信頼しているかどうかを確認します。

（注） Expressway でサポートされている最小 TLS バージョンを有効にするセキュアな接続の適切性をテストするには、**HTTPS 最小 TLS バージョン**を選択する必要があります。また 、**HTTPS 暗号**を同じ目的で選択します。この *HTTPTLSversion* の選択は 、VCSE、CUCM、CUP、UCXN などの Unified Communication サーバとの接続確立に必要です。これらの設定は、**[暗号（Ciphers）]**ページ（**[メンテナンス（Maintenance）]** > **[セキュリティ（Security）]** > **[暗号（Ciphers）]** で設定されます。

HSM を使用した Expressway のサーバ証明書の管理

重要 ExpresswayでのHSM機能のサポートは、Expressway ソフトウェアのバージョンによっては、**プレビュー機能のみ**になる場合があります。たとえば、バージョン X12.6 のプレビュー機能です。HSM を使用する前に Expressway バージョンのリリースノートを確認し、そのステータスがソフトウェアバージョンのプレビューである場合は、**プレビュー機能として実装する意思があり、Expressway リリースノートに含まれるプレビューの免責事項に従う場合にのみ、HSM を有効にしてください。**現時点で、この機能を構成および有効にする手順は、Expressway リリースノートに記載されています。

これらの手順は、HSM が Expressway ですでに有効になっていることを前提としています（**[メインテナンス（Maintenance）] > [セキュリティ（security）] > [HSM 設定（HSM configuration）]**）。

手順

ステップ 1 **[メンテナンス（Maintenance）]** > **[セキュリティ（Security）]** > **[サーバ証明書（Server certificate）]** に移動します。

ステップ 2 [CSR の作成（Generate CSR）] をクリックします。**[CSR の生成（Generate CSR）]** ページに移動します。

[サーバ証明書の種類（Server certificate type）] の項は **[CSR 生成（Generate CSR）]** ページの上部に表示されます。HSM の使用法が構成されていない場合、この項は表示されません。

Expressway クラスタがある場合は、CSR フィールドが誤って完了した場合に問題が発生する可能性があります。これらのフィールドを入力する方法の詳細については、「*Cisco Expressway* シリーズ設定ガイド」ページの「Cisco Expressway クラスタの作成とメンテナンスの導入ガイド」を参照 してください。

ステップ 3 HSM 秘密キーと CSR として生成した後、**サーバ証明書**ページに戻ります。

ステップ 4 **証明書署名要求（CSR）** の項から、生成された HSM CSR を表示およびダウンロードできます。

ステップ 5 **[ダウンロード（Download）]** をクリックして、証明書をダウンロードします。

ステップ 6 証明書署名機関を使用して証明書に署名します。

プライベートキーと証明書のインストール

（注） ハードウェアセキュリティモジュール（HSM）機能を使用する場合にのみ、次の手順を使用します。

手順

ステップ 1 署名付き証明書をアップロードするには、**[ファイルの選択（Choose File）]** をクリックして場所に移動し、証明書を選択します。

ステップ 2 証明書ファイルと対応する証明書タイプを選択し、**[サーバ証明書データのアップロード（Upload server certificate）]** をクリック して証明書をアップロードします。

詳細については、Expressway のサーバ証明書の管理に関するセクションを参照してください。

クラスター全体で HSM キー ハンドルをダウンロードする

HSM 証明書と秘密きーを Expressway に展開した後、HSM 証明書と秘密キーをクラスタ内の他の Expressway に展開できます。手順は、次のとおりです。

手順

ステップ 1 プライマリピア。1 つ目の Expressway から、この 2 つのキーをダウンロードします。**[サーバ証明書データ（Server certificate data）]** セクションに、オプションの証明書とプライベートキーを導入した後、**[HSM キーハンドルのダウンロード（Download HSM key handle）]** ボタンが表示されます。

ステップ 2 クラスタピア上。**[新しい証明書のアップロード（Upload new certificate）]** セクションから、HSM 証明書を含む HSM 秘密キーをクラスター内の他のピアにアップロードします。署名付き HSM 証明書とプライベートキーを参照して選択します。

Expressway を再起動

HSM 証明書が Expressway にインストールされた後、**サーバー証明書**ページのバナーにより、Expressway を再起動するように求められます。アラームも発生して再起動します。証明書がインストールされているが、Expressway が証明書を使用し始めるには再起動が必要です。

再起動後、アラームは消え、Expressway上のすべてのサービスが新しい HSM 証明書を使用します。

ハードウェアセキュリティモジュールの機能設定

HSM 設定ページ（**[メンテナンス（Maintenance）]** > **[セキュリティ（Security）]** > **[HSM 設定（HSM configuration）]**）は、Expressway を使用する場合に、そのデバイスを管理するために使用します。

重要 HSM 機能は、Expressway ソフトウェアバージョンに応じて、**プレビュー機能のみ**使用できます。たとえば、バージョン X12.6 のプレビュー機能です。HSM を使用する前に、Expressway バージョンのリリースノートを確認してください。ソフトウェアバージョンのステータスがプレビューである場合は、プレビュー機能として実装する場合にのみ HSM を有効にしてください。現時点で、このセクションでは、Expressway リリースノートに記載されているのではなく、その方法について説明しています。

最小限 TLS バージョンと暗号スイートの設定

[メンテナンス（Maintenance）] > [セキュリティ（Security）] > [暗号（Ciphers）] ページは、Expressway 上のサービスの最小 TLS バージョンと、関連する暗号スイートを管理するために使用されます。

（注） セキュリティを強化するため、すべての暗号化セッションに TLS のバージョン 1.2 以降を推奨します。

以下のセキュアな接続を確立する場合、Expressway はデフォルトで TLS 1.2 に設定されます。

- HTTPS
- 証明書のチェック機能
- Cisco Meeting Server の検出
- SIP
- XMPP
- UC サーバ ディスカバリ
- リバース プロキシ
- LDAP
- [SMTP メールサーバ]
- TMS プロビジョニングサービス

場合によっては、再起動が必要です。

暗号スイートの設定または TLS プロトコルのバージョンを次のバージョンに変更した後、再起動する必要があります。

- SIP
- XCP

最小TLSバージョン

既存のシステムのアップグレードでは、以前の動作とデフォルトが維持され、デフォルトは TLS 1.2 に設定されません。

新しいインストールの場合は、Expressway に接続する必要があるすべてのブラウザおよび他の機器が TLS 1.2 をサポートしています。

必要に応じて（通常は旧式の機器との互換性のため）、サービスごとに最小 TLS バージョンはバージョン 1.0 または 1.1 を使用するように構成できます。

暗号スイート

Expressway のサービスに暗号スイートとサポートされる最小 TLS バージョンを設定できます。暗号スイートを表に示します（暗号文字列は OpenSSL 形式です）。

Expressway がクライアント（HTTPS など）として動作できるサービスの場合、同じ最小 TLS バージョンと暗号スイートがネゴシエートされます。

サービス	暗号スイートの値（デフォルト）
HTTPS 暗号方式	EECDH:EDH:HIGH:- AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL
リバース プロキシの TLS 暗号方式	EECDH:EDH:HIGH:- AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL
SIP TLS 暗号方式	EECDH:EDH:HIGH:- AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:+ADH
UC サーバ ディスカバリの TLS 暗号方式	EECDH:EDH:HIGH:- AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL
XMPP TLS 暗号方式	EECDH:EDH:HIGH:- AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL
LDAP TLS 暗号方式	EECDH:EDH:HIGH:- AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL
TMS TLS 暗号方式	EECDH:EDH:HIGH:- AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL
SMTP 暗号	EECDH:EDH:HIGH:- AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL

SIP 動作 - ADH 勧告を無効にする

E20 など、一部のエンドポイントは、接続するときに匿名 Diffie-Hellman（ADH）のみをサポートし、ADH はデフォルトの暗号スイートで有効になっています。ただし、インバウンド接続の場合は、セキュリティ上の理由から、`!ADH` を追加して常に無効にする必要があります

SIP から ADH を削除すると、一部のレガシーエンドポイントへの発信接続が失敗することに注意してください。

SSH の設定

トンネルの設定

Expressway ペアでは SSH トンネルを使用して Expressway-E から Expressway-C にセキュアにデータを転送します。Expressway-E が接続を開く必要はありません。Expressway-C は、固定 TCP ポートでリッスンしている Expressway-E との TCP セッションを開始します。セッション開始後、Expresswayペアは選択済みの暗号方式とアルゴリズムを使用して、データをセキュアに共有するために暗号化されたトンネルを確立します。

ペアが SSH トンネルの暗号化に使用する暗号とアルゴリズムは次のように構成されています。

1. **[メンテナンス（Maintenance）] > [セキュリティ（Security）] > [SSH 接続（SSH configuration）]** に移動します。
2. 必要に応じて、次の設定を変更します。

設定	説明
暗号	*aes256 ctr*：CTR（カウンタ）モードを使用して 256 ビットのブロックを暗号化する Advanced Encryption Standard。（デフォルト）
公開キー アルゴリズム	*X509v3-sign-rsa*（デフォルト） *X509v3*、*ssh*、*rsa*
キー交換アルゴリズム	*ecdh-sha2-nistp256* *nistp384 sha2 ecdh*（デフォルト)

3. [保存（Save）] をクリックします。

Remote Access Configuration

ペアが SSH クライアントとサーバー間のリモートアクセスを暗号化するために使用する暗号とアルゴリズムは、次のように構成されています。

1. **[メンテナンス（Maintenance）] > [セキュリティ（Security）] > [SSH 接続（SSH configuration）]** に移動します。
2. 必要に応じて、次の設定を変更します。

設定	説明
暗号	*“aes256-gcm@openssh.com,aes128-gcm@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr”*
キー交換アルゴリズム	*“ecdh-sha2-nistp521,ecdh-sha2-nistp384,ecdh-sha2-nistp256,diffie-hellman-group14-sha1”*
MAC アルゴリズム	*“hmac-sha2-512,hmac-sha2-256,hmac-sha1”*

3. [保存（Save）] をクリックします。

高度なセキュリティ

「高度なセキュリティ（Advanced Security）」ページ（**[メンテナンス（Maintenance）] > [高度なセキュリティ（Advanced security）]**）を使用して、極めてセキュアな環境で使用するように Expressway を設定します。このページを表示するには、**[高度のアカウント セキュリティ（Advanced Account Security）]** オプション キーをインストールする必要があります。

システムを次のように設定できます。

- 高度なアカウント セキュリティ モードの設定
- FIPS140-2 暗号化モードの設定

高度なアカウント セキュリティ モードの設定

高度なアカウント セキュリティを有効にすると、Web インターフェイスを使用してリモートから認証されたユーザのみにログインアクセスが限定され、一部のシステム機能へのアクセスも制限されます。Expressway が高度なアカウント セキュリティ モードになっていることを示すために、**[分類バナー（Classification banner）]** メッセージとして指定したテキストがすべての Web ページに表示されます。

高度なアカウント セキュリティ モードへの変更を有効にするには、システムをリブートする必要があります。

HTTP メソッド

Expressway の Web サーバでは、次の HTTP メソッドが許可されています。

方法	Web UI での使用	API での使用	用途
GET	はい	はい	指定したリソースからデータを取得します。たとえば、Expressway の Web インターフェイスの特定のページを返します。
POST	はい	はい	Web リソースにデータを適用します。たとえば、管理者が Expressway の Web インターフェイスを使用して、設定の変更を保存する場合などです。

方法	Web UI での使用	API での使用	用途
オプション	いいえ	はい	指定した URL に対し、サーバでサポートされている HTTP メソッドを返します。たとえば、Expressway は OPTIONS を使用して HTTP/1.1 コンプライアンス用にプロキシ サーバをテストできます。
PUT	いいえ	はい	指定した URI に保存するリソースを送信します。REST API コマンドはこのメソッドを使用して、Expressway 設定を変更します。
DELETE	いいえ	はい	指定したリソースを削除します。たとえば、REST API はレコードの削除に DELETE を使用します。

API へのユーザ アクセスを無効にする方法

管理者はデフォルトで API にアクセスできます。これは、次の 2 つの方法で無効化できます。

- Expressway が高度なアカウント セキュリティ モードで動作している場合、API アクセスはすべてのユーザで自動的に無効になります。
- 個別の管理者の API アクセスは、ユーザ設定オプションを使用して無効にできます。

前提条件

高度なアカウント セキュリティ モードを有効にするには、次の項目が必須です。

- 管理者アカウントにLDAP を使用したリモート アカウント認証の設定を使用するようにシステムを設定する必要があります。
- **高度なアカウント セキュリティ**のオプション キーをインストールする必要があります。
- リモート認証が利用できない場合にアクセスできるように、ローカル管理者アカウントを作成し、緊急アカウントとして指定する必要があります。この目的にリモート アカウントを使用することはできません。

  組み込み *admin* アカウントを使用しないでください。

⚠

注意 Expressway は、緊急アカウントを除いたすべてのアカウントでローカル認証を許可していません。モードを有効にする前に、リモート ディレクトリ サービスが正常に機能していることを確認します。

また、以下のようにシステムを設定することを推奨します。

- SNMP 設定値の設定を無効にする。

- ネットワーク サービスをゼロ以外の値に設定する。
- ネットワーク サービスを有効にする。
- LDAP を使用したリモート アカウント認証の設定の設定では TLS 暗号化を使用し、証明書失効リスト（CRL）を [すべて（All）] に設定する。
- ロギングの設定を無効にする。
- インシデントレポートを無効にする。
- 接続を外部マネージャ設定値の設定に対して行う場合は、HTTPS を使用し、証明書の確認を有効にする。

推奨されていない設定にはアラームが発行されます。

高度なアカウント セキュリティの有効化

高度なアカウント セキュリティを有効にするには、次の手順を実行します。

手順

ステップ 1 **[メンテナンス（Maintenance）]** > **[高度なセキュリティ（Advanced security）]** に移動します。

ステップ 2 [分類バナー（Classification banner）] に入力します。

ここで入力したテキストがすべての Web ページに表示されます。

ステップ 3 **[高度なアカウント セキュリティ モード（Advanced Account Security）]** を *[オン（On）]* に設定します。

ステップ 4 **[保存（Save）]** をクリックします。

ステップ 5 Expressway を再起動します（**[メンテナンス（Maintenance）]** > **[オプションの再起動（Restart options）]**）。

Expressway 機能：変更と制限

セキュア モードのとき、標準的な Expressway 機能に対して次の変更と制限が適用されます。

- SSH を使用したシリアル ポートを通じたアクセスが無効になり、オンにできない（pwrec パスワード リカバリ機能も使用できなくなる）。
- HTTPS を使用したアクセスが有効になり、オフにできない。
- コマンドライン インターフェイス（CLI）と API アクセスが使用できない。
- 管理者アカウントの認証ソースが [リモートのみ（Remote Only）] に設定され、変更できない。
- ローカル認証が無効になる。緊急アカウントを除いて、root アカウントまたはローカル管理者アカウントではアクセスできない。

- 緊急アカウントのみが緊急アカウントを変更できる。
- 証明書ベースの認証を使用している場合は、緊急アカウントをクライアントの証明書のクレデンシャルで認証する必要がある。緊急アカウントと証明書ベースの認証を参照してください。
- 同じユーザまたは異なるユーザによるログイン試行が3回連続で失敗した場合にExpresswayのログイン アクセスを 60 秒間ブロックする。
- ログイン直後に現在のユーザに以前ログインした日時とそのアカウントを使用してログインに失敗した試行の詳細を表示します。
- 読み取り専用または読み取り/書き込みのアクセス レベルを持つ管理者アカウントは、[イベント ログ（Event Log）]、[設定ログ（Configuration Log）]、[ネットワーク ログ（Network Log）] ページを表示できない。これらのページを表示できるのは、監査役のアクセス レベルを持つアカウントのみである。
- 「**アップグレード（Upgrade）**」ページに**システム プラットフォーム**コンポーネントのみが表示される。

Expressway が高度なアカウント セキュリティ モードから実行されるたびに、イベント ログ、設定ログ、ネットワーク ログ、通話履歴、検索履歴、登録履歴がクリアされます。

（注） 自動化された侵入からの保護の設定を有効にすると、ブロックされている既存のアドレスのブロックが解除された状態になります。

高度なアカウント セキュリティの無効化

（注） この操作によりすべての設定が消去されます。このモードを終了した場合、設定または履歴を維持することはできません。システムは出荷時の状態に戻ります。

手順

ステップ 1 緊急アカウントでログインします。
ステップ 2 高度なアカウント セキュリティ モードを無効にします（**[メンテナンス（Maintenance）]** > **[高度なセキュリティ（Advanced security）]**）。
ステップ 3 サインアウトします。
ステップ 4 コンソールに接続します。
ステップ 5 **root** としてサインインし、**factory-reset** を実行します。

詳細については、デフォルト設定の復元（初期設定へのリセット）を参照してください。

FIPS140-2 暗号化モードの設定

FIPS140 は暗号モジュールのセキュリティ要件を指定する米国およびカナダ政府の標準規格です。FIPS140-1 は 1994 年に機密データ保護のための必須の標準規格になり、2001 年に FIPS140-2 に取って代わられました。Expressway X8.8 以降には、FIPS140-2 対応機能が実装されています。

FIPS140-2 の暗号化モードの場合、暗号化のワークロードの増加によりシステム パフォーマンスが影響を受ける可能性があります。

FIPS140-2 モードが有効化された Expressway をクラスタ化できます。

前提条件

FIPS140-2 モードを有効にする前に、次のことを実行します。

- デバイスの認証にシステムが NTLM プロトコル チャレンジと Active Directory サービスの直接接続を使用していないことを確認する。NTLM は FIPS140-2 モードのときは使用できません。
- リモート LDAP サーバを経由したログイン認証が設定されている場合、SASL バインドを使用しているときは TLS 暗号化を使用することを確認する。
- **高度なアカウント セキュリティ**のオプション キーをインストールする必要があります。

FIPS140-2 のコンプライアンスには次の制限事項も必要です。

- システム全体の SIP トランスポート モードの設定で、[TLS] は *[オン（On）]*、[TCP] は *[オフ（Off）]*、[UDP] は *[オフ（Off）]* に設定する必要があります。
- すべての SIP ゾーンが TLS を使用する必要があります。
- SNMP と NTP のサーバ接続には、強力なハッシュと暗号化を使用する必要があります。次の設定を使用します。

  System > SNMP > v3 Authentication > Type = *SHA*

  System > SNMP > v3 Privacy > Type = *AES*

  System > Time > NTP server *n* > Authentication= 対称 キーです。

  System > Time > NTP server *n* > Hash= *SHA-1*

システムが仮想化アプリケーションとして実行され、アップグレードプロセスを実行しきったことない場合は、続行する前にシステムアップグレードを実行します。現在実行しているものと同じソフトウェア リリースのバージョンにシステムをアップグレードできます。この手順を実行しないと、以下で説明するアクティベーション プロセスが失敗します。

FIPS 140-2 暗号化モードの有効化

注意 FIPS 140-2 暗号モードへの移行には、システムのリセットを実行する必要があります。これにより、既存のすべての設定データが削除されます。データを保持するには、リセットを実行する直前にバックアップを実行し、リセットが完了した時点でバックアップ ファイルを復元します。

リセットによりすべての管理者アカウント情報が削除され、デフォルトのセキュリティ証明書が元の状態に戻ります。リセット完了後にログインするには、最初にインストール ウィザードを完了する必要があります。

システムを FIPS 140-2 暗号対応システムに変えるには、次の手順を実行します。

手順

ステップ 1 FIPS 140-2 暗号化モードの有効化

1. **[メンテナンス（Maintenance）] > [高度なセキュリティ（Advanced security）]** に移動します。
2. **[FIPS-2 暗号化モード（FIPS140-2 cryptographic mode）]**を *[オン（On）]* に設定します。
3. **[保存（Save）]** をクリックします。

ステップ 2 準拠していない設定を報告するために発生したアラームを修正します。

（注） モバイルおよびリモートアクセスのシナリオで FIPS を有効にすると、アラームが #40042 場合（一部の SIP 設定は TLS トランスポートを使用しません。FIPS 140-2 コンプライアンスでは TLS が要求されます）、この機能を無効にして有効にしてアラームをクリアできます。

ステップ 3 現在の設定データを維持する場合は、システム バックアップの作成を実行します。

（注） すべてのバックアップをパスワードで保護する必要があることに注意してください。

ステップ 4 システムをリセットし、FIPS140-2 モードのアクティベーションを実行します。

1. **root** として Expressway にログインします。
2. **`fips-activate`** と入力します。

このリセットは、完了するまでに最大 30 分かかります。

ステップ 5 指示に従ってインストール ウィザードを完了します。

ステップ 6 設定が適用されてシステムが再起動したら、設定したパスワードを使用して **`admin`** としてログインします。

FIPS 140-2 のコンプライアンス違反に関連するアラームが表示される場合があります。リセット前に実行したバックアップを復元する場合は、これらのアラームは無視します。バックアップを復元してもアラームが続く場合は対処する必要があります。

ステップ 7 必要に応じて、以前のデータを以前のバックアップの復元します。

（注） FIPS 140-2 モードでは 、**FIPS 140-2 暗号モード**が *[*オン（*On*）*]* に設定されている場合に撮影されたバックアップファイルのみ復元できます。以前の管理者アカウント情報とパスワードは復元されますが、以前の **root** アカウントのパスワードは復元されません。復元するデータに信頼できないセキュリティ証明書が含まれている場合は、復元プロセスの一環として行われるリスタートが完了するまでに最大6分かかる場合があります。

ステップ 8 X12.6 から、SIP TLS Diffie-Hellman キーサイズをデフォルトの 1024 ビットから少なくとも 2048 に手動で変更する必要があります。この操作を行うには、Expressway コマンドラインインターフェイスで次のコマンドを入力します（キー サイズが 2048 を超える場合は、最終的な要素の値を変更します）：*xconfiguration SIP Advanced SipTlsDhKeySize: "2048"*

FIPS140-2 対応機能

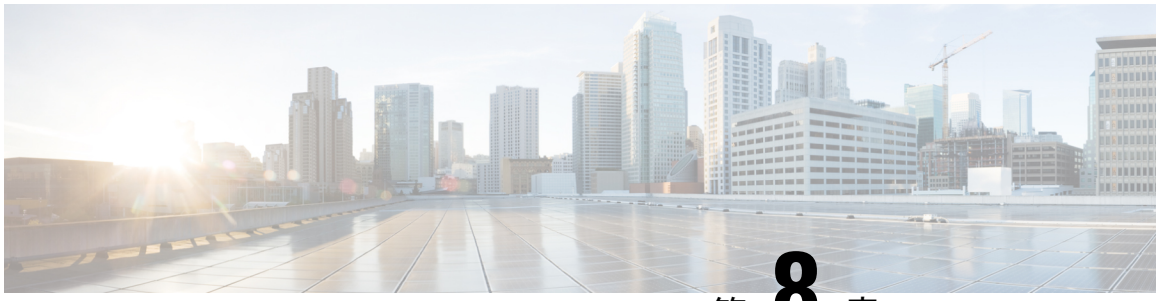
次の Expressway 機能は FIPS140-2 に対応しているか、または FIPS140-2 対応アルゴリズムを使用します。

- Web インターフェイスを使用した管理
- クラスタリング
- XML と REST API
- SSH アクセス（AES または 3DES 暗号のみの使用に限定）
- リモート LDAP サーバを介してのログイン認証（SASL バインドを使用している場合は TLS を使用すること）
- クライアント証明書の確認
- SIP 証明書の失効機能
- SNMP（SNMPv3 認証は SHA1 のみに、SNMPv3 プライバシーは AES のみに限定）
- NTP（対称キーを使用した NTP サーバ認証は SHA1 のみに限定）
- ローカル データベースと照合してのデバイス認証
- TLS を使用している場合の Expressway への、または Expressway からの SIP 接続
- Expressway への、または Expressway からの H.323 接続
- 委任クレデンシャル チェック
- SRTP メディア暗号化

- SIP/H.323 インターワーキング
- ユニファイド コミュニケーションの Mobile & Remote Access（MRA）
- TURN サーバ認証
- バックアップ/復元操作
- 外部マネージャへの接続
- 外部ポリシー サービスへの接続
- リモート ロギング
- インシデント レポート
- CSR の生成

その他の Expressway 機能は次を含めて FIPS140-2 に対応していません。

- NTLM/Active Directory による SIP 認証
- H.350 ディレクトリ サービスと照合する SIP/H.323 デバイス認証
- Microsoft 相互運用性サービス
- Cisco TMSPE の使用



第 8 章

有用性、ロギング、監視、およびメトリック

このセクションでは、ロギング、システムモニタリング、メトリック収集、および電子メール通知など、Expresswayに関するサービスアビリティ情報について説明します。管理トラフィックにLAN3を使用するオプションの専用管理インターフェイス（DMI）については、専用管理インターフェイス（DMI）の設定を参照してください。

診断およびデバッグツール、ネットワークテストユーティリティ、およびインシデントレポートについては、診断とトラブルシューティングを参照してください。

ロギングの設定

Expresswayはトラブルシューティングと監査を目的としたsyslog処理機能を提供します。イベントログはローテーションローカルログで、送受信されたコール、登録、およびメッセージなどの情報を記録します。

Expressway ロギングオプションを設定するには、**[メンテナンス（Maintenance）]** > **[ロギング（Logging）]** に移動します。**[ロギング（Logging）]** ページから次のタスクを実行できます。

- イベントログ冗長性の変更を指定して、ローカルに記録されるイベント情報の詳細レベルを変更する
- コールのメディア統計情報ロギングを切り替える
- コール詳細レコードのキャプチャを切り替える
- 認定対応のロギングを切り替える
- 1 つ以上のリモート syslog サーバへのログの公開 アドレスを定義する
- 各リモート syslog サーバに送信されるイベントを重大度でフィルタリングする

- システムメトリック収集（収集済み）を設定する方法を切り替える

イベントログ冗長性の変更

ローカルイベントログの冗長性を 1～4 の間で設定することで、ローカルログの冗長性をオプションで制御できます。すべてのイベントには、1～4の範囲で関連付けられたレベルがあり、レベル 1 のイベントが最も重要と見なされます。

（注） レベル 3 またはレベル 4 のロギングは通常運用には推奨しません。このような詳細なロギングによって 2 GB のログが早急にローテーションする可能性があります。ただし、トラブルシューティングではこのレベルの詳細を記録する必要がある場合があります。

イベントは、リモートロギングが有効になっているかどうかに関係なく、常にローカルに（イベントログに）記録されます。

次の表に、さまざまなイベントに割り当てられるレベルの概要を示します。

レベル	割り当てられるイベント
1	登録要求やコール試行などの高レベルイベント。人間が簡単に読み取れます。次に例を示します。 • コール試行/接続/切断 • 登録試行/承認/拒否
2	すべてのレベル 1 のイベントに加えて、次のイベントがあります。 送受信されたプロトコルメッセージのログ（SIP、H.323、LDAP など）。H.460.18 キープアライブや H.245 ビデオ高速更新などのノイズの多いメッセージは除きます。
3	すべてのレベル 1 およびレベル 2 のイベントに加えて、次のイベントがあります。 • プロトコルのキープアライブ • コール関連の SIP シグナリング メッセージ
4	最も詳細なレベル：レベル 1、レベル 2、およびレベル 3 のすべてのイベントに加えて、次のイベントがあります。 • ネットワーク レベルの SIP メッセージ

ログレベルを変更すると、Web インターフェイスを通じて表示するイベント ログと、別のリモートログサーバにコピーされる情報の両方に影響します。変更は振り分け的な操作ではなく、変更後にログに記録される情報にのみ影響します。

Expressway はローカルログに次の機能を使用します。（ローカル）機能にマッピングするソフトウェアコンポーネント/ログが強調表示されます。

- 0（kern）
- 3（daemon）
- 16（local0）管理者
- 17（local1）設定
- 18（local2）*Mediastats*
- 19（local3）*Apache* エラー
- 20（local4）*etc/opt/apache2*
- 21（local5）開発者
- 22（local6）ネットワーク

イベントとレベルセクションには、Expressway によってログに記録されるすべてのイベントと、それらがログに記録される詳細レベルの完全なリストがあります。

認定対応のロギング

環境によっては、Expressway のログがセキュリティ認定の要件を満たすようにする必要があります。セキュリティと診断目的のログの間にはトレードオフがあります。認定対応モードでは、コールの問題の正確な原因を判定できない場合があります。

認定対応ロギングの設定方法

手順

ステップ 1 **[メンテナンス（Maintenance）]** > **[ロギング（Logging）]** に移動します。

ステップ 2 **[ロギングオプション（Logging options）]** セクションで、**[認定ロギング（Certification logging）]** モードを次のいずれかに設定します。

認証ロギング モード	説明
診断	このモードは認証対応ではありませんが、コールの問題の診断には最も役立ちます。
秘密（*Secretive*）	このモードは認定対応ではありません。

認証ロギング モード	説明
秘密と詳細（*Secretive and Verbose*）	このモードも認証対応ですが、Syslog サーバへのセキュアな接続を使用して一部のログ情報を収集できます。これらのログは、診断の意味では特に役立つものではありません。

リモート syslog サーバへのログの公開

syslog は、複数のシステムからのログ メッセージを 1 つの場所に集約するための便利な方法です。これは、クラスタ内のピアの場合に特に推奨します。

- 最大 4 つのリモート syslog サーバにログ メッセージをパブリッシュするように Expressway を設定できます。
- syslog サーバは次の標準プロトコルのいずれかをサポートする必要があります。
  - BSD（RFC 3164 で定義）
  - IETF（RFC 5424 で定義）

リモート syslog サーバの設定

（注）

- **[キーワード別にフィルタリング（Filter by Keywords）]** オプションは、重大度別にすでにフィルタリングされているメッセージに適用されます。
- 単語のグループ（「「login successful」」など）を含め、最大 5 つのキーワードをカンマで区切って使用できます。
- 最大 256 文字をキーワードに使用できます。
- システムのパフォーマンスへの影響を回避するために、最も関連性の高いキーワードを最初に検索することを推奨します。これにより、syslog サーバに関連するログ メッセージができるだけ早期にプッシュされます。

手順

ステップ 1 **[メンテナンス（Maintenance）]** > **[ロギング（Logging）]** に移動し、このシステムがログメッセージを送信する **リモート syslog サーバ** の IP アドレスまたは完全修飾ドメイン名（FQDN）を入力します。

ステップ 2 各サーバの [オプション（Options）] ボタンをクリックします。

ステップ 3 使用する**転送**プロトコルと**ポート**を指定します。TLS を使用する場合、syslog サーバに対して証明書失効リスト（CRL）を有効にするオプションが表示されます。

ステップ 4 [メッセージ形式（Message Format）] フィールドで、リモート Syslog メッセージの作成形式を選択します。デフォルトは [レガシー BSD（Legacy BSD）] です。

ステップ 5 **[重大度別にフィルタリング（Filter by Severity）]** オプションを使用して、送信する詳細レベルを選択します。Expressway は選択した重大度のメッセージと、より厳しいメッセージすべてを送信します。

ステップ 6 **[キーワード別にフィルタリング（Filter by Keywords）]** オプションは、特定のキーワードを含むメッセージを送信する場合に使用します。

ステップ 7 [保存（Save）] をクリックします。

使用される一般的な値

次の表に、ロギング サーバとネットワーク設定に最適な形式を選択する上で役立つ情報と、一般的な値を示します。

表 *10 : Syslog* のメッセージ形式

メッセージ形式	トランスポート プロトコル	提案されたポート	RFC
レガシー *BSD* 形式	UDP	514	BSD 形式。RFC 3164 を参照
IETF syslog format	UDP	514	IETF 形式。RFC 5424 を参照
TLS 接続を使用した *IETF syslog*	TLS	6514	IETF 形式。RFC 5424 を参照

（注）

- UDP プロトコルはステートレスです。ご使用の環境で syslog メッセージの信頼性が非常に重要である場合は、別のトランスポート プロトコルを使用する必要があります。
- Expressway と syslog サーバ間にファイアウォールがある場合、適切なポートを開いてメッセージを通過させる必要があります。
- TLS トランスポートを選択した場合は、Expressway は Syslog サーバの証明書を信頼しなければなりません。必要に応じて、Syslog サーバの CA 証明書をローカル信頼ストアにアップロードします。
- TLS の使用時は CRL チェックはデフォルトで無効になっています。CRL を有効にするには、**[CRL チェック（CRL checking）]** を *[オン（On）]* に設定し、関連する証明書失効リスト（CRL）がロードされるようにします。

  詳細については、セキュリティの基本を参照してください。
- リモート サーバを別の Expressway として使用することはできません。
- Expressway は他のシステムのリモート ログ サーバとして機能できません。
- Expressway はリモート ロギングに次の機能を使用します。（ローカル）機能にマッピングするソフトウェア コンポーネント/ログが強調表示されます。
  - 0（kern）
  - 3（daemon）
  - 16（local0）管理者
  - 17（local1）設定
  - 18（local2）*Mediastats*
  - 19（local3）*Apache* エラー
  - 20（local4）*etc/opt/apache2*
  - 21（local5）開発者
  - 22（local6）ネットワーク

コールのメディア統計情報ロギング

メディア統計情報を有効にする方法

必要に応じて、Expressway 上でのメディア統計情報の収集を有効にするには、**[メンテナンス（Maintenance）] > [ロギング（Logging）]** に移動し、**[メディア統計情報（Media statistics）]** を *[オン（On）]* に設定します。これにより、システムは各コールのメディア統計情報をロー

カル ハード ディスクの **/mnt/harddisk/log** に記録するようになります。それぞれ 10 MB のファイルが 200 個まで保存されます。200 番目のファイルが一杯になると、最も古いファイルが削除されます。

収集されるメディア統計情報は、転送されたパケット数、損失したパケット数、ジッター、メディア タイプ、コーデック、実際のビットレートなどです。

メディア統計情報も Syslog メッセージとしてパブリッシュされます。メディア統計情報ロギングが有効にされている間、Expressway は機能 18（local2）を使用して、設定したすべてのリモート Syslog サーバに統計情報をパブリッシュします。メッセージの重大度は *[*情報提供（*Informational*）*]* に設定されますが、メディア統計情報メッセージは重大度フィルタに関係なく常にパブリッシュされます。

コール詳細レコードのキャプチャ

サービスを有効にする必要がある場合（デフォルトはオフ）、Expressway では、必要に応じて CDR をキャプチャできます。CDR は 7 日の間ローカルに保存され、リモートログを使用している場合は、syslog メッセージとしても公開できます。

CDR の設定方法

Expressway で CDR を設定するには、次の手順を実行します。

手順

ステップ 1 **[メンテナンス（Maintenance）]** > **[ロギング（Logging）]** に移動します。

ステップ 2 **[ロギング オプション（Logging options）]** セクションで、**[コール詳細レコード]** フィールドを必要なオプションに設定します。

- サービスとロギング：CDRs は 7 日間ローカルに保存された後、削除されます。レコードはローカルのイベントログからアクセス可能で、外部ロギングが有効な場合、syslog ホストに INFO メッセージとして送信されます。
- サービスのみ：CDRs は 7 日間ローカルに保存された後、削除されます。このレコードには、Web ユーザインターフェイスからアクセスできません。CDR は REST API を介してのみ読み取り可能です。
- オフ：CDR はローカルではログは記録されません。これがデフォルト設定です。

CDR プロパティ

この表では、CDR に表示されるプロパティを定義します。

フィールド	定義
uuid	CDR エントリの ID。
service_uuid	レコードの収集元がプロキシか、Lync 2BUA か、または暗号化 B2BUA かの識別に使用する ID。
active	コールがライブまたは履歴か。
initial_call	コールが複数コンポーネントの場合（B2BUA ホップが含まれる）、B2BUA コールに内部的に関連付けるために使用します。
licensed	コールでライセンスが使用された場合に表示されます。
licensed_as_traversal	コールでトラバーサルライセンスが使用された場合に表示されます。
status	200 OK メッセージは、コールが成功されたことを示します。コールが失敗した場合のエラーメッセージが含まれます。
tag	コール ID。
box_call_serial_number	（B2BUA を介したなど）複数のコールを関連付けするために追加された追加 ID。
start_time	コールの日時。タイムゾーンは、**[システム（System）] > [時刻（Times）] > [タイムゾーン（Time Zone）]** で設定でき、日付形式は YYYY-MM-DD です。
end_time	コールの終了時間。
source_alias	発信者のエイリアス。
destination_alias	呼び出し先のエイリアス。
aside_destination_alias	発信者（または、Lync と相互運用の場合は MS Lync クライアント）のエイリアス。
bside_destination_alias	呼び出し先（または Lync 以外のクライアント）のエイリアス。
aside_request_uri	発信者（または Lync と相互運用の場合は MS Lync クライアント）の要求 URI。
bside_request_uri	呼び出し先（または Lync 以外のクライアント）の要求 URI です。
protocol	コールが SIP <-> SIP, SIP <-> H323, H323 <-> SIP, or H323 <-> H323であったかどうかを示します。

フィールド	定義
protocol_summary	上記のように、コールがマルチコンポーネント、DVO などの追加情報を持つ場合があります。
media_routed	コール中にメディアが送信されたか（NAT/IWF/B2BUA など）が表示されます。
audio	通話が音声専用の通話だったのか示します。
traversal_license_tokens	コールフォーク/ブランチがメディアを使用したかどうかを示します（オーディオは 1 トークン、ビデオは 2 に相当します）。*
non_traversal_license_tokens	コールフォーク/ブランチがメディアを取得する必要がなかったかどうかを示します（オーディオは 1 トークンおよびビデオ 2 に相当します）。*
disconnect_reason	通常のコールティアダウンや他のエラー（つまり最後のステータス）など、コールドロップの理由を示します。
details	メディア統計を含む、コールの詳細を表示します。
last_updated_timestamp	上記のフィールドのいずれかが最後に更新されたとき。

* コールが設定されると、これらのエントリのいずれかがゼロ以外の値になります（応答したフォーク/ブランチについてのみ）。

CDR にアクセスする API

次のセキュアな REST API を使用して、CDR を収集できます。

- get_all_records（最長で 7 日前までのすべてのレコードを返します）。
- get_records_for_interval（指定された時間のレコードを返します）。
- get_records_for_filter（任意の組み合わせを使用して結果をフィルタリングします）。
- get_all_csv_records（最長で 7 日前までのすべてのレコードを csv 形式で返します）。

重要 通話履歴はローカルに 7 日間のみ保存された後、自動的に削除されます。

目的の API にアクセスするには、次の URL を使用します。

https://%3CExpressway_IP%3E/api/external/callusage/%3CAPI%3E

API の例

- http://%3CExpressway_IP%3E/api/external/callusage/get_all_records
- `http://<Expressway_IP>/api/external/callusage/get_records_for_interval?fromtime=<fromtime>&totime=<to_time>`

  これらの数が多い場合—

  ```
  https://203.0.113.17/api/external/callusage/
  get_records_for_interval?fromtime=2014-05-09 2000:00:00&totime=
  2014-05-10 2000:00:00
  ```

入力パラメータ

パラメータ	説明
fromtime	必須。CDR レコードが必要な期間の開始時刻。 **形式**：*YYYY-MM-DD HH:MI:SS*
totime	必須。CDR レコードが必要な期間の終了時刻。 **形式**：*YYYY-MM-DD HH:MI:SS*

- `http://<Expressway_IP>/api/external/callusage/get_records_for_interval?fromtime=<fromtime>&totime=<to_time>`

  これらの数が多い場合—

  ```
  https://203.0.113.17/api/external/callusage/
  get_records_for_interval?fromtime=2014-05-09 2000:00:00&totime=
  2014-05-10 2000:00:00
  ```

- `http://<Expressway_IP>/api/external/callusage/get_records_for_filter?uuid=<uuid>&src_alias=<src_alias>&dest_alias=<dest_alias>&protocol=<protocol>`

  これらの数が多い場合—

  ```
  https://203.0.113.17/api/external/callusage/
  get_records_for_filter?uuid=6e3b5a8a-346c-421b-aa2e-f4409c43a81a
  &src_alias=TC149-057-h323@domain.com&dest_alias=
  TC149-065-h323@domain.com&protocol=H323 <-> H323
  ```

入力パラメータ

パラメータ	説明
uuid	記録の一意の識別子。
src_alias	コールの発信元。
dest_ alias	コールの宛先ポイント。
protocol	コールに使用されたプロトコル（SIP、H323 など）。

- http://%3CExpressway_IP%3E/api/external/callusage/get_all_csv_records

CDR の例

サンプル CDR

このサンプルの場合、CSV を除くすべての API に適用されます。

[{"initial_call": "false", "protocol": "SIP <-> SIP", "protocol_summary": "", "disconnect_reason": "200 OK", "licensed": "false", "tag": "b8d52a60-16a1-4bdb-be93-f5a675408811", "aside_request_uri": "", "box_call_serial_number": "22cd0e7d-c498-4068-9239-624038fe5130", "source_alias": "sip:10000005@10.196.4.82", "uuid": "800fe013-83f4-4094-a5e6-e2f9489912e2", "last_updated_timestamp": 1444725389, "details": "{\"Call\":{\"SerialNumber\": \"800fe013-83f4-4094-a5e6-e2f9489912e2\",\"BoxSerialNumber\": \"22cd0e7d-c498-4068-9239-624038fe5130\",\"Tag\": \"b8d52a60-16a1-4bdb-be93-f5a675408811\",\"State\": \"Disconnected\",\"StartTime\": \"2015-10-13 01:36:26.485636\",\"InitialCall\": \"False\",\"Licensed\": \"False\",\"LicensedAsTraversal\": \"False\",\"SourceAlias\": \"sip:10000005@10.196.4.82\",\"DestinationAlias\": \"sip:10000010@cucm-82\",\"ToLocalB2BUA\": \"False\",\"Audio\": \"False\",\"License\":{\"Traversal\": \"0\",\"NonTraversal\": \"0\",\"DemotedTraversal\": \"0\",\"CollaborationEdge\": \"0\",\"Cloud\": \"0\"},\"Duration\": \"3\",\"Legs\":[{\"Leg\":{\"Protocol\": \"SIP\",\"SIP\":{\"Address\": \"10.196.4.61:5073\",\"Transport\": \"TLS\",\"Aliases\":[{\"Alias\":{\"Type\": \"Url\",\"Origin\": \"Unknown\",\"Value\": \"sip:10000005@10.196.4.82\"}}]},\"Targets\":[{\"Target\":{\"Type\": \"Url\",\"Origin\": \"Unknown\",\"Value\": \"sip:10000010@10.196.4.116\"}}],\"BandwidthNode\": \"DefaultZone\",\"EncryptionType\": \"AES\",\"Cause\": \"200\",\"Reason\": \"OK\"}},{\"Leg\":{\"Protocol\": \"SIP\",\"SIP\":{\"Address\": \"10.196.4.71:7001\",\"Transport\": \"TLS\",\"Aliases\":[{\"Alias\":{\"Type\": \"Url\",\"Origin\": \"Unknown\",\"Value\": \"sip:10000010@cucm-82\"}}]},\"Source\":{\"Aliases\":[{\"Alias\":{\"Type\": \"Url\",\"Origin\": \"Unknown\",\"Value\": \"10000005@10.196.4.82\"}}]},\"BandwidthNode\": \"Traversal-zone\",\"EncryptionType\": \"AES\",\"Cause\": \"200\",\"Reason\": \"OK\"}}],\"Sessions\":[{\"Session\":{\"Status\": \"Completed\",\"MediaRouted\": \"False\",\"CallRouted\": \"True\",\"Participants\":{\"Leg\": \"1\",\"Leg\": \"2\",\"Incoming\":{\"Leg\": \"1\"},\"Outgoing\":{\"Leg\": \"2\"}}}}],\"EndTime\": \"2015-10-13 01:36:29.745651\"}}", "status": "Disconnected", "destination_alias": "sip:10000010@cucm-82", "licensed_as_traversal": "false", "service_uuid": "e6723fd0-5ca2-11e1-b86c-0800200c9a66", "start_time": "2015-10-13 01:36:26.485636", "traversal_license_tokens": 0, "bside_destination_alias": "", "active": "false", "media_routed": "false", "aside_destination_alias": "", "non_traversal_license_tokens": 0, "bside_request_uri": "", "end_time": "2015-10-13 01:36:29.745651", "audio": "false”}]

csv CDR の例

```
uuid,service_uuid,active,initial_call,licensed,licensed_as_traversal,
status,tag,box_call_serial_number,start_time,end_time,source_alias,
destination_alias,aside_destination_alias,bside_destination_alias,
aside_request_uri,bside_request_uri,protocol_summary,protocol,
media_routed,audio,traversal_license_tokens,non_traversal_license_tokens,
disconnect_reason,details,last_updated_timestamp
```

```
800fe013-83f4-4094-a5e6-e2f9489912e2,e6723fd0-5ca2-11e1-
b86c-0800200c9a66,false,false,false,false,Disconnected,b8d52a60-16a1-
4bdb-be93-f5a675408811,22cd0e7d-c498-4068-9239-624038fe5130,2015-10-
13 01:36:26.485636,2015-10-13
```

01:36:26.485636,2015-10-13 01:36:29.745651,sip:10000005@10.196.4.82,sip:10000010@cucm-82,,,,,,SIP <-> SIP,false,false,0,0,200 OK,"{""Call"":{""SerialNumber"": ""800fe013-83f4-4094-a5e6-e2f9489912e2"",""BoxSerialNumber"": ""22cd0e7d-c498-4068-9239-624038fe5130"",""Tag"": ""b8d52a60-16a1-4bdb-be93-f5a675408811"",""State"": ""Disconnected"",""StartTime"": ""2015-10-13 01:36:26.485636"",""InitialCall"": ""False"",""Licensed"": ""False"",""LicensedAsTraversal"": ""False"",""SourceAlias"": ""sip:10000005@10.196.4.82"",""DestinationAlias"": ""sip:10000010@cucm-82"",""ToLocalB2BUA"": ""False"",""Audio"": ""False"",""License"":{""Traversal"": ""0"",""NonTraversal"": ""0"",""DemotedTraversal"": ""0"",""CollaborationEdge"": ""0"",""Cloud"": ""0""},""Duration"": ""3"",""Legs"":[{""Leg"":{""Protocol"": ""SIP"",""SIP"":{""Address"": ""10.196.4.61:5073"",""Transport"": ""TLS"",""Aliases"":[{""Alias"":{""Type"": ""Url"",""Origin"": ""Unknown"",""Value"": ""sip:10000005@10.196.4.82""}}]},""Targets"":[{""Target"":{""Type"": ""Url"",""Origin"": ""Unknown"",""Value"": ""sip:10000010@10.196.4.116""}}],""BandwidthNode"": ""DefaultZone"",""EncryptionType"": ""AES"",""Cause"": ""200"",""Reason"": ""OK""}},{""Leg"":{""Protocol"": ""SIP"",""SIP"":{""Address"": ""10.196.4.71:7001"",""Transport"": ""TLS"",""Aliases"":[{""Alias"":{""Type"": ""Url"",""Origin"": ""Unknown"",""Value"": ""sip:10000010@cucm-82""}}]},""Source"":{""Aliases"":[{""Alias"":{""Type"": ""Url"",""Origin"": ""Unknown"",""Value"": ""10000005@10.196.4.82""}}]},""BandwidthNode"": ""Traversal-zone"",""EncryptionType"": ""AES"",""Cause"": ""200"",""Reason"": ""OK""}}],""Sessions"":[{""Session"":{""Status"": ""Completed"",""MediaRouted"": ""False"",""CallRouted"": ""True"",""Participants"":{""Leg"": ""1"",""Leg"": ""2"",""Incoming"":{""Leg"": ""1""},""Outgoing"":{""Leg"": ""2""}}}}],""EndTime"": ""2015-10-13 01:36:29.745651""}}",1444725389

アラームベースの電子メール通知の設定

Expressway は、アラームの重大度およびオプションでアラーム ID に基づく電子メールベースの通知をサポートします。設定されている場合、アラームがシステムに生成されると、設定されている宛先アドレスに電子メール通知が送信されます。アラームの重大度分類ごとに、通知の緊急性を区別するために、異なる電子メール ID を定義できます。同じ重大度のアラームに対して、複数の電子メール ID を設定できます。

X12.6.2 から、特定のアラーム ID の通知を特定の電子メール ID に送信したり、特定のアラーム ID に対する通知を無効にしたりすることもできます。

重要 電子メール ID の最大許容長は 256 文字です。

この機能は、Kari の法律を実装したい米国を拠点とするお客様にもご利用いただけます。Expressway を経由して直接 9-1-1 をダイヤルする基準を満たす 9-1-1 コールが行われた場合、重大度のアラーム緊急が生成され、(設定されている場合)、重大度のアラーム緊急用に設定された電子メール ID に通知が送信されます。

はじめる前に

- 電子メールを送信するための接続を確立するために、SMTP サーバの詳細を提供する必要があります。

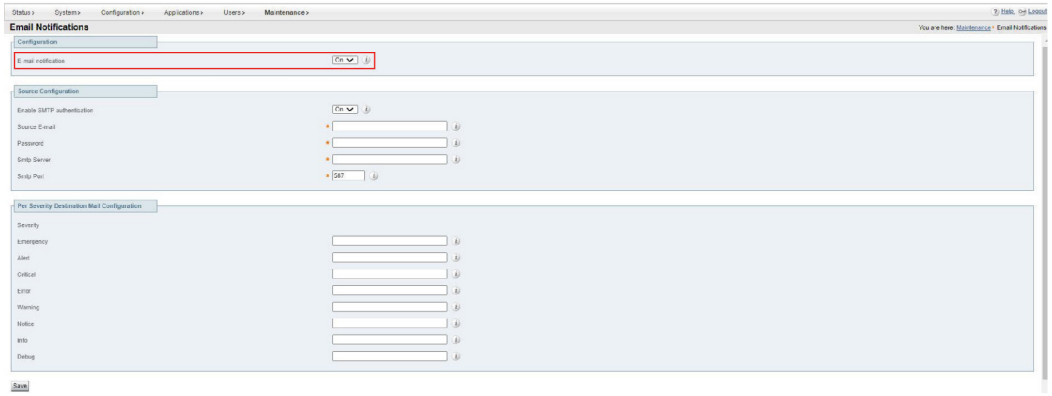
- Expressway は、SMTP サーバとの TLS 接続のみをサポートしています。
- SMTP サーバは、Expressway から直接、または SMTP プロキシを使用して到達できる必要があります。SMTP 用の HTTP プロキシの使用はサポートされていません。
- 送信元の電子メールとパスワードは、SMTP サーバで検証してから、メールを送信します。

アラームベースの電子メール通知を設定をするプロセス

手順

ステップ 1 **[メンテナンス（Maintenance）]** > **[電子メール通知（Email Notifications）]**に移動します。

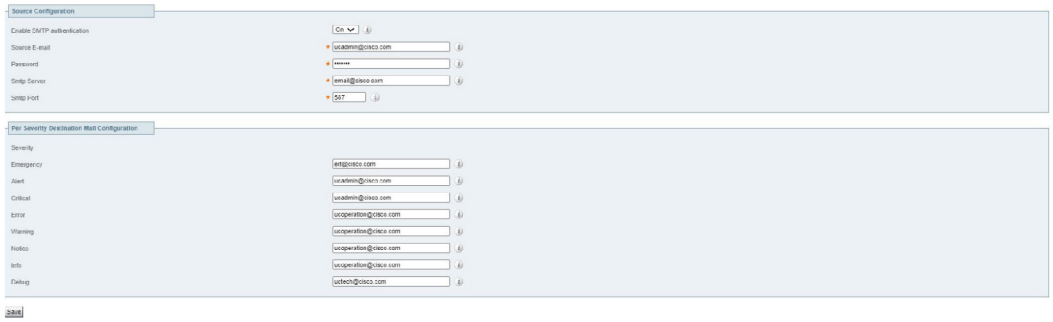
ステップ 2 **[電子メール通知（Email Notifications）]** ドロップダウンリストで、*[オン（On）]* を選択します。



ステップ 3 **[送信元の設定（Source Configuration）]** セクションに次の情報を入力します。

- 設定された宛先アドレスに通知が送信される送信元のメールアドレス。
- 電子メール通知の送信に使用される SMTP サーバの IP アドレスまたは FQDN。
- **[重大度ごとの宛先メール構成]**セクションで、特定の重大度のアラームの通知を受信する電子メールアドレスを入力します。
- [保存（Save）] をクリックします。

図 *4:* 電子メール通知の設定例



通知のカスタマイズ方法 - 無効化または電子メールアドレスへ送信

必要に応じて、このプロセスを使用して、特定のアラーム ID の通知を特定の電子メールアドレスに送信したり、特定のアラーム ID に対する通知を無効にしたりすることができます。たとえば、指名された個人にしきい値警告アラームを送信したり、不要なアラームによる通知を停止したりすることができます。

手順

ステップ 1 **「電子メール通知」** ページの **「カスタム通知」** セクションに移動します。ここで、既存のカスタム通知を表示、編集、および削除し、新しい通知を追加できます。

ステップ 2 カスタマイズされた通知を作成するには

1. [追加（Add）] をクリックします。
2. 使用するアラーム ID を選択します。
3. **[通知]** ドロップダウンリストで、選択したアラームの電子メール通知先を定義する場合は *[カスタム]* を選択し、このアラームに対して電子メールを送信しない場合は *[無効にする]* を選択します。
4. [カスタム] を選択した場合は、**[電子メール]** フィールドに、選択したアラーム通知の送信先である通知先の電子メールアドレス を入力します。
5. [保存（Save）] をクリックします。
6. アラーム通知が意図した通り動作することをテストするには、次の作業を実行します。
   1. **[アラームの選択]** ドロップダウンから、テストするアラームを選択します。
   2. **[今すぐテスト（Test Now）]** ボタンをクリックします。

3. テストから受信した電子メール通知が期待通りか確認します。

システム メトリック コレクション

システムメトリックの収集は、システムパフォーマンスに関する統計情報をパブリッシュする機能で、パフォーマンスをリモートからモニタできるようにします。Expressway は、ハードウェア、OS、およびアプリケーションのパフォーマンスに関する統計情報を収集し、データを集約するリモートホスト（通常はデータ分析サーバ）にそれらの統計情報をパブリッシュします。この機能は Web インターフェイスまたはコマンドラインで設定できます。

（注） 1 つのピアからの設定はクラスタ全体に適用されます。クラスタをモニタする場合は、プライマリピアに System Metrics Collection を設定することをお勧めします。

リモートサーバの設定も必要です。収集されたスレッドはサーバ上で実行されている必要があります。収集されたネットワークプラグインは、クライアントに見えるアドレスをリッスンするように設定されています。設定の詳細はモニタリング環境によって異なり、このガイドの範囲を超えています。

収集したデータの使用方法

Expressway から収集されたデータに基づいて、グラフを生成し、統計を集約し、パフォーマンスを解析するために、Circonus および Graphite などのツールを使用できます。また、トレンドを表示し、潜在的な問題を予想する場合にも使用できます。表示できるメトリックには、次のものがあります。

- ゾーン単位およびシステム別のアクティブコール
- キープロセスメトリック：キープロセスのシステム CPU、ユーザ CPU、およびメモリ使用量
- アラーム

システムメトリック収集（収集済み）を設定する方法

Expressway を設定する

必要に応じて、Web ユーザインターフェイスから Expressway を設定し、統計を収集、指定されたサーバに公開するには、次の手順を使用します。

手順

ステップ 1 Expressway にログインし、**[メンテナンス（Maintenance）]** > **[ロギング（Logging）]** に移動します。

ステップ 2 **[システム メトリックの収集（System Metrics Collection）]** を *[オン（On）]* に切り替えます。

ステップ 3 [収集サーバのアドレス（Collection server address）] に入力します。

IP アドレス、ホスト名、または FQDN を使用してリモートサーバを特定できます。

ステップ 4 必要に応じて、デフォルトの**収集サーバポート**（リスニングポート）を変更します（収集サーバがデフォルト以外のポートでリッスンしている場合）。

ステップ 5 必要に応じて、デフォルトの**収集間隔**を変更します（ポリシーでデフォルトの間隔の 60 秒よりも細かく調整されたメトリックが必要な場合）。

ステップ 6 [保存（Save）] をクリックします。

収集したものを設定する CLI コマンドの例

CLI を使用する場合は、関連するコマンドの例を以下となります。

表 *11* : 収集を設定する *CLI* コマンド

コマンドの機能	コマンド例
メトリック収集のオンとオフの切り替え	**xconfig log SystemMetrics mode: on**
サーバアドレスの指定	**xconfig log SystemMetrics network address: address**
リスニングポートの指定	**xconfig log SystemMetrics network port: 25826**
収集間隔の指定	**xconfig log SystemMetrics interval: 60**
システムメトリック設定の読み取り	**xstatus SystemMetrics**

リモートサーバを設定する

使用している環境でのデータ分析に選択するサーバの使用と設定は、このマニュアルでは扱いません。回収された情報を処理できるアプリケーションの一例です。分析ツールは、collectd デーモンからのデータの受信をサポートする必要があります。このデーモンは Expressway で実行され、collectd ネットワーク プラグインを使用してメトリックを分析サーバにプッシュします。

ネットワーク プラグインは、データのカプセル化のための収集したバイナリプロトコルを実装します。分析サーバは、このデータを解析し、提示できる必要があります。分析サーバには、collectd ソフトウェアまたは代替ソフトウェアに基づいてデータの収集方法や表示方法を設定するための独自の UI が備わっている可能性があります。

分析サーバで collectd を使用している場合は 、*collectd.conf* ファイルを変更 して、サーバが次の条件を実行します。

- 収集されたクライアント（Expressway など）からデータをリッスンします。ネットワークプラグインを有効にして、サーバの IP アドレスでリッスンブロックを設定する必要があります。次に例を示します。

```
<Plugin "network">
                Listen "198.51.100.15"
        </Plugin>
```

- 受信したデータを人が読み取り可能な形式（CSV ファイルなど）に格納します。csv プラグインを有効にして、ファイルの書き込み場所を知る必要があります。次に例を示します。

```
<Plugin "csv">
                 DataDir "/var/lib/collectd/csv"
                 StoreRates true
        </Plugin>
```

詳細情報

- https://collectd.org/wiki/index.php/Networking_introduction
- https://collectd.org/documentation/manpages/collectd.conf.5.shtml#plugin_network
- https://collectd.org/wiki/index.php/Binary_protocol
- https://collectd.org/wiki/index.php/Plugin:CSV
- https://collectd.org/documentation/manpages/collectd.conf.5.shtml#plugin_csv

トラブルシューティング

Expressway がデータを送信するかどうかを確認するには、Expressway から TCP ダンプを設定し、データ分析サーバのアドレスに送信されたパケットを確認します。**[メンテナンス（Maintenance）] > [診断（Diagnostics）] > [診断のログ（Diagnostics logging）]** に移動し、**ロギング中に tcpdump を取得（Take tcpdump while logging）** チェックボックスをオンにし、ロギングを開始します。

Expressway から収集されたメトリック

次のハードウェア統計情報がモニタされます。

- aggregation-cpu-sum
- aggregation-cpu-average
- システム内の各コアのコア単位の CPU 使用状況
- df
- ディスク

- 負荷
- protocols-Tcp
- protocols-Udp
- swap
- ユーザ
- メモリ
- アップタイム（Uptime）
- プロセス

次のアプリケーションデータは、collectd のカスタム exec-app プラグインによってモニタされます。

- `gauge-active_alarms` は、この Expressway 上のアクティブなアラームの数です。
- `gauge-active_calls` は、この Expressway によって処理中のコールの数です。
- `gauge-<service name>`は、各システムサービスのステータスです。
- `gauge-<zone name>_ActiveCalls`は、名前付きゾーン内のアクティブコールをカウントします。
- `gauge-<zone name>_BandwidthAllocated`は、指定されたゾーンに割り当てられた合計帯域幅を測定します。
- `gauge-<zone name>_BandwidthLimit`

これらのメトリックのそれぞれが自由形式のデータを許可する collectd GAUGE データソースタイプを使用します。収集サーバでは、たとえば、*collectdHostnamecollectd.exec-app.gauge-active_calls* のように、完全な collectd 値の名前が表示されます。

（注） ゾーン名はユーザが設定できる構成のため、収集されたメトリックの名前スキーマと競合している可能性があります。収集サーバがスキーマを適用している場合、一部のゾーンからのメトリックが受け付けられない可能性があります。

収集サーバに送信されるデータ

ネットワークプラグインは収集されたバイナリプロトコルを使用して、モニタ対象のハードウェアリソースやソフトウェアプロセスを表す数字、文字列、および値データをカプセル化します。ネットワークプラグインは、デフォルトで UDP 25826 を使用して、分析サーバにメトリックのデータパケットを間隔ごとに1回プッシュします。分析サーバはデータを解析し、人間が判読できる形式で表示します。

分析サーバが収集されたネットワークプラグインと csv プラグインを使用している場合、メトリック名とタイムスタンプを使用してファイル名を作成し、メトリックは小規模な CSV ファイルとして保存されます。たとえば、*gauge-H323-2015-05-21*

収集されたプラグイン

収集されたこれらのプラグインは、Expressway に実装されます。

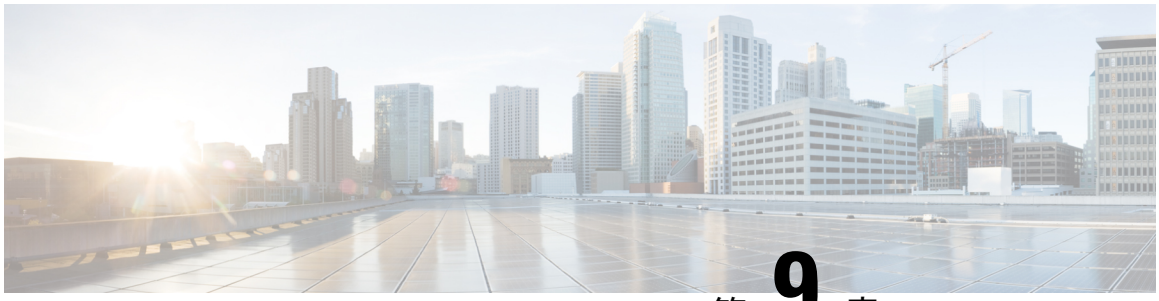
プラグイン名	説明
アグリゲーション	CPU 値をカウンタの `aggregation_cpu_sum` と `aggregation_cpu_average` に集約します。
CPU	プロセッサ情報raw 情報が `aggregation_cpu_average` と `aggregation_cpu_sum` に集約されます。
DF	ファイル システム情報。collectd Wiki の DF の説明を参照してください。
ディスク	ハードディスクのパフォーマンス。collectd Wiki のディスクの説明を参照してください。

プラグイン名	説明
Exec-app	コール、アラーム、ゾーン、およびサービスに関する特定の Expressway 情報を返すカスタマイズされた **exec** バージョン • gauge-active_alarms • gauge-active_calls • gauge-B2BUA • gauge-cafemanager • gauge-callusagemanager • gauge-<zone>_ActiveCalls • gauge-<zone>_BandwidthAllocated • gauge-c_mgmt • gauge-collectd • gauge-developer • gauge-edgeconfigprovisioning • gauge-fail2ban • gauge-findmed • gauge-forwardproxy • gauge-H323 • gauge-http • gauge-https • gauge-importcontrol • gauge-jabberd • gauge-LCDd • gauge-managementconnector • gauge-opends • gauge-phonebookserver • gauge-portforwarding • gauge-provisioningd • gauge-provisioningserver • gauge-proxy-registrationd

プラグイン名	説明
Exec-app	• gauge-restmanager • gauge-samlverifier • gauge-singlesignon • gauge-SIP • gauge-snmpd • gauge-sshd • gauge-sshdpfwd • gauge-sslh • gauge-telnetd • gauge-trafficserver • gauge-transcodermanager • gauge-tty • gauge-winbindd
負荷	タスクキューに基づくシステム負荷。
メモリ	メモリの統計情報。
ネットワーク	リモートアドレスへのパブリッシュを可能にします。このプラグインは、データのカプセル化のための collectd バイナリプロトコルを実装します。リモートサーバには適切な解析ツールが必要です。
プロトコル	Expressway で使用されるプロトコルの設定可能なサブセット。

プラグイン名	説明
プロセス	システムプロセスをカウントし、状態（実行中、スリープ中、ゾンビなど）ごとにグループ化します。また、特定のプロセスの詳細な統計情報を収集します。プラグインは次のプロセスを詳しくモニタします。 • app • bramble • credentialmanagerservermain • cvs_main • erlang-beam • erlang-epmd • httpd • httpserver • ivy • licensemanagerservermain • managementconnectormain • managementframework • openssl2nss • policyservermain • sshdpfwd • syslog-ng • traffic_server • XCP

プラグイン名	説明
Statsd	特定の Expressway 情報を返すカスタマイズされたバージョン。たとえば、ICE 使用法です。 • gauge-ICEPassthroughMetrics.b2buacalls • gauge-ICEPassthroughMetrics.candidatesofferedmissingiceconfig • gauge-ICEPassthroughMetrics.failedicenegotiationcalls • gauge-ICEPassthroughMetrics.hosthostcalls • gauge-ICEPassthroughMetrics.hostrelaycalls • gauge-ICEPassthroughMetrics.hostsrvrflxcalls • gauge-ICEPassthroughMetrics.icecalls • gauge-ICEPassthroughMetrics.icecandidatecalls • gauge-ICEPassthroughMetrics.iceconfiguredcalls • gauge-ICEPassthroughMetrics.noicecandidatesoffered • gauge-ICEPassthroughMetrics.onepartyicecandidatecalls • gauge-ICEPassthroughMetrics.relayrelaycalls • gauge-ICEPassthroughMetrics.srvrflxrelaycalls • gauge-ICEPassthroughMetrics.srvrflxsrvrflxcalls
Swap	ディスクに書き込まれるシステムメモリの量。
アップタイム（Uptime）	システムの稼働時間を追跡し、平均実行時間や特定の期間の最大アップタイムなどのカウンタを提供します。collectd Wiki のアップタイムの説明を参照してください。
ユーザ	現在ログインしているユーザの数。



第 9 章

ネットワークとシステムの設定

ここでは、Web インターフェイスの **[システム（System）]** メニューに表示されるネットワーク サービスと設定に関連するオプションについて説明します。これらのオプションによって、IP 設定、ファイアウォール ルール、侵入からの保護、Expressway が使用する外部サービス（DNS、NTP、SNMP など）といった、Expressway が存在するネットワークに関連する設定を行うことができます。

ネットワーク設定

ここでは、Webインターフェイスの[システム（System）]メニューに表示されるネットワークサービスと設定に関連するオプションについて説明します。これらのオプションによって、IP設定、ファイアウォールルール、侵入からの保護、Expresswayが使用する外部サービス（DNS、NTP、SNMPなど）といった、Expresswayが存在するネットワークに関連する設定を行うことができます。

イーサネット設定

（注） このページで設定する速度は、Cisco Expressway 物理アプライアンス上で稼働するシステムにのみ適用されます。仮想マシン（VM）ベースのシステムには適用されません。VM システムに対して示される接続速度は無効であり、基礎となる物理 NIC の実際の速度とは関係なく常に 10000 Mb/s として表示されます。これは、VM では物理 NIC から実際の速度を取得できないためです。

「イーサネット（Ethernet）」ページ（**[システム（System）]**>**[ネットワークインターフェイス（Network interfaces）]**>**[イーサネット（Ethernet）]**）には、Expressway とその接続先イーサネットネットワークとの間の接続速度が表示されます。Expressway では自動ネゴシエーションのみがサポートされるため、**[速度（Speed）]** は常に *[自動（Auto）]* に設定されます。Expressway とこれに接続されているスイッチは、接続の速度とデュプレックス モードを自動的にネゴシエートします。

IP の設定

「IP」ページ（**[システム（System）]**>**[ネットワーク インターフェイス（Network interfaces）]**>**[IP]**）を使用して、Expressway の IP プロトコルとネットワーク インターフェイスの設定を行います。

IP プロトコルの設定

Expressway が IPv4 と IPv6 のどちらを使用するか、あるいは IP プロトコル スイートの両方のバージョンを使用するかを設定できます。デフォルトは *[両方（Both）]* です。

- *[IPv4 のみ（IPv4 only）]*：IPv4 アドレスを使用したエンドポイントからの登録のみを許可し、IPv4 で通信する 2 つのエンドポイント間のコールのみを受け入れます。IPv4 でのみ他のシステムと通信します。
- *[IPv6 のみ（IPv6 only）]*：IPv6 アドレスを使用したエンドポイントからの登録のみを許可し、IPv6 で通信する 2 つのエンドポイント間のコールのみを受け入れます。IPv6 でのみ他のシステムと通信します。
- *[両方（Both）]*：IPv4 または IPv6 のいずれかのアドレスを使用したエンドポイントからの登録を許可し、どちらのプロトコルを使用したコールでも受け入れます。IPv4 のみのエンドポイントと IPv6 のみのエンドポイント間のコールの場合は、Expressway が IPv4 から IPv6 へのゲートウェイとして機能します。他のシステムとはいずれかのプロトコルで通信します。

一部のエンドポイントは IPv4 と IPv6 の両方をサポートしますが、Expressway に登録するときにエンドポイントが使用できるプロトコルは 1 つのみです。エンドポイントに Expressway の IP アドレスを指定するために使用した形式によって、どちらのプロトコルを使用するかが決定します。IPv4 または IPv6 のいずれかを使用してエンドポイントを登録すると、Expressway はこのアドレッシング スキームを使用してコールのみを送信します。別のアドレッシング スキームを使用した別のデバイスからのそのエンドポイントへのコールは Expressway によって変換されます（ゲートウェイ機能）。

Expressway で設定されたすべての IPv6 アドレスは、/64 ネットワーク プレフィックス長があるものとして処理されます。

IPv4 と IPv6 のインターワーキング

Expressway は IPv4 デバイスと IPv6 デバイス間のコールのゲートウェイとして機能します。この機能を有効にするには、**[IP プロトコル（IP protocol）]** に *[両方（Both）]* を選択します。

Expressway が IPv4 から IPv6 へのゲートウェイとして機能するコールはトラバーサル コールであるため、リッチ メディア セッション ライセンスが必要です。

IP ゲートウェイ

Expressway が使用するデフォルトの **[IPv4 ゲートウェイ（IPv4 gateway）]** と **[IPv6 ゲートウェイ（IPv6 gateway）]** を設定できます。これらは、Expressway のローカル サブネットの範囲内にない IP アドレスに対して IP 要求を送信するゲートウェイです。

- デフォルトの **[IPv4 ゲートウェイ（IPv4 gateway）]** は 127.0.0.1 です。デフォルトを変更する場合は、コミッション プロセス時に変更する必要があります。
- 入力されている場合、[IPv6 ゲートウェイ（IPv6 gateway）] はスタティック グローバル IPv6 アドレスである必要があります。リンクローカルまたはステートレス自動設定（SLAAC）IPv6 アドレスを指定することはできません。

LAN の設定

Expressway のプライマリ ネットワーク ポートは LAN 1 です。**このポートに [IPv4 アドレス（IPv4 address）]** と [サブネットマスク（subnet mask）]、**[IPv6 アドレス（IPv6 address）]** と **[最大転送単位（MTU）（Maximum transmission unit (MTU)）]** を設定できます。Expressway は、両方の LAN ポートにデフォルトの IP アドレス 192.168.0.100 が設定された状態で出荷されます。これにより、Expressway をネットワークに接続し、デフォルトのアドレスを使用してアクセスすることで、リモートから設定できます。

入力されている場合、[IPv6 アドレス（IPv6 address）] はスタティック グローバル IPv6 アドレスである必要があります。リンクローカルまたはステートレス自動設定（SLAAC）アドレスを指定することはできません。

デフォルトでは、**[最大転送単位（MTU）（Maximum transmission unit (MTU)）]** は 1,500 バイトに設定されます。

高度なネットワーキングが有効になっている場合は、LAN 2 ポートに対してもこれらのオプションを設定できます。

専用管理インターフェイス

Expressway の DMI を有効にする場合は、次の方法を実行します。

手順

ステップ 1 **[専用管理インターフェイスの使用（Use Dedicated Management Interface）]** を *[はい（Yes）]* に設定します。

ステップ 2 **[LAN3 - DMI]** セクションで、次を実行します。

1. LAN3 ポートの IPv4 アドレスまたは IPv6 アドレスを指定します。
2. IPv4 では、サブネットマスクも指定します。

3. IPv6 の場合は、静的なグローバルアドレスを使用します。リンクローカルまたはステートレスの SLAAC は使用できません。
4. 必要に応じて、ポートの**最大伝送ユニット（MTU）**を設定することで、DMI 経由で送信できるイーサネットパケットの最大サイズを変更します。デフォルト値は 1500 バイトです。

ステップ 3 システムを再起動します。これらの変更を有効にするには、再起動が必要です。

これで、DMI が管理トラフィック用のインターフェイスとして LAN3 でアクティブ化されました。DMI を管理用の唯一のインターフェイスとして使用する場合は、次のタスクに進みます。

次のタスク

DMI 単独のインターフェイス作成

DMI 単独のインターフェイス作成

（オプション）DMI を唯一のインターフェイスにする - サーバ管理トラフィック

Expressway がサーバである場合に、このタスクを使用して、管理トラフィックに DMIを使用します。

1. これは、管理サービス（Web ユーザインターフェイス、REST API、CLI）または SNMP に対して実行できます。DMI 専用に設定するサービスに応じて、次の手順のいずれかまたは両方を実行します。
   - **[システム（System）] > [SNMP]** ページに進み、**[設定（Configuration）]** セクションで、**[専用管理インターフェイスのみを使用する（Use Dedicated Management Interface）]** を *[はい（Yes）]* に設定します。
   - **[システム（System）] > [管理設定（Administration settings）]** に進み、**[サービス（Services）]** セクションで、**[管理インターフェイスのみを使用する（管理用）（Use Dedicated Management Interface only (for administration)）]** を *[はい（Yes）]* に設定します。
2. 変更を Web ユーザインターフェイスと API に適用するにはシステムを再起動する必要があります。再起動するまで LAN1/LAN2 からアクセスできる状態が維持されます。変更は、再起動に関係なく、コマンドラインインターフェイス（SSH）および SNMP サービスに対して即時に有効になります。

指定された管理サービスに、DMI/LAN3 ポートからのみアクセスできるようになりました。

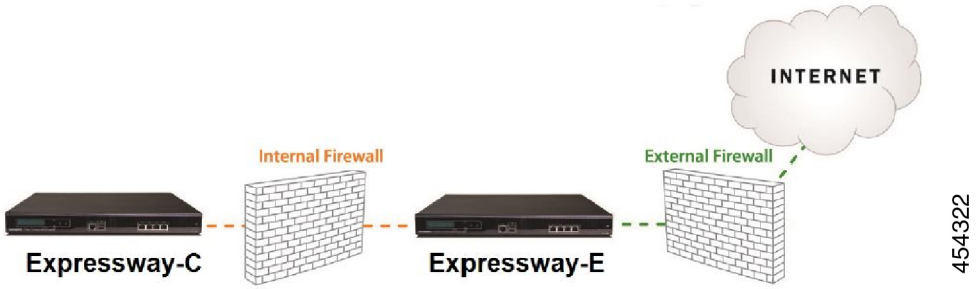
（注） Expressway では、管理サービスが DMI を唯一のインターフェイスとして使用するように設定されている間は、この DMI を無効にすることはできません。

（オプション）DMI を唯一のインターフェイスにする - サブネット外のクライアント管理トラフィック

Expressway ソフトウェアのバージョンに応じて、Expressway がクライアントとして動作する管理トラフィックでは、ターゲットサーバが DMI/LAN3 ポートと同じサブネット内にある場合にのみ、トラフィックを DMI に送信できます。リリースノートをチェックして、この問題が適用されるのか確認してください。適用される場合、LAN3 と同じサブネットにサーバを導入できない場合は、オプションで、サービスごとに LAN3 用のスタティック IP ルートを設定することで、Expressway 管理トラフィックに DMI の使用を強制できます。

高度なネットワーキングおよびデュアルネットワークインターフェイスについて

高度なネットワーキング機能を使用すると、Expressway-E の LAN 2 イーサネット ポートを有効にして、Expressway のセカンダリ IP アドレスを取得できます。この機能には Expressway-E がスタティック NAT デバイスの背後にある導入環境に対するサポートも含まれているため、個別のパブリック IP アドレスとプライベート IP アドレスを取得できます。



デュアル ネットワーク インターフェイスの設定

デュアルネットワークインターフェイスは、**Expressway-E システムでのみサポート されています**。Expressway-C では展開できません。

デュアル ネットワーク インターフェイスは、Expressway-E が個別のネットワーク セグメント上にある 2 つの個別ファイアウォール間の DMZ に存在する導入環境用のインターフェイスです。このような導入環境では、ルータが内部ネットワーク上のデバイスが IP トラフィックをパブリックインターネットにルーティングできないようにしますが、その代わりに、トラフィックは Expressway-E などのアプリケーション プロキシを通過する必要があります。

デュアルネットワークインターフェイスを有効にするには

始める前に

- LAN 1 ポートを設定し、Expressway を再起動してから LAN 2 ポートを設定してください。
- LAN 1 インターフェイスと LAN 2 インターフェイスは、重複しない別のサブネット上にある必要があります。

- Expressway-E が DMZ にある場合、Expressway-E の外部 IP アドレスはパブリック IP アドレスである必要があります。また、スタティック NAT モードが有効になっている場合は、スタティック NAT アドレスにパブリック ネットワークからアクセス可能である必要があります。
- また、Expressway-E を企業内の内部ファイアウォールを通過するために使用することができます。この場合、「「パブリック」」IP アドレスはパブリックネットワークからアクセスできませんが、企業内の別の部分へのアクセスが可能な IP アドレスです。
- インターフェイスの一方または両方の IP アドレスを変更する必要がある場合は、UI または CLI を使用して変更することができます。必要に応じて、両方を同時に変更できます。また、新しいアドレスは、再起動後に有効になります。

手順

ステップ 1 **[デュアル ネットワーク インターフェイスを使用する（Use dual network interfaces）]** を *[*はい（*Yes*）*]* に設定します。

ステップ 2 *[*外部 *LAN* インターフェイス（*External LAN interface*）*]* 設定では、インターフェイスとして **[LAN2]** を選択します。

外部インターフェイスのスタティック NAT を有効にする選択を行えるようになりました。この設定はどのポートが TURN サーバ リレーを割り当てるかを決定します。

トラブルシューティングのヒント

高度なネットワーキングを有効にしていても、イーサネットポートの 1 つのみを設定する場合は、**[デュアルネットワークインターフェイスを使用する（Use dual network interfaces）]** を *[*いいえ（*No*）*]* に切り替えます。

スタティック NAT の設定

スタティック NAT デバイスの背後に Expressway-E を導入して、パブリック IP アドレスとプライベート IP アドレスを個別に取得できるようにします。この機能は、Expressway-E が DMZ 内にあり、**高度なネットワーキング**機能が有効にされた展開環境で使用することを目的としています。

このような展開環境では、プライベート IPv4 アドレスとパブリック IPv4 アドレスの両方を使用するために、外向きの LAN ポートで NAT が有効にされいます。内向きの LAN ポートではスタティック NAT が有効にされないため、単一の IP アドレスを使用します。このような導入環境においては、Expressway-E の内向きの IP アドレスを使用するようにトラバーサル クライアントを設定する必要があります。

静的 NAT を有効にするには

外部に面した LAN ポートに対して、次の設定を指定します。

手順

ステップ 1 **[IPv4アドレス（IPv4 address）]** フィールドに、ポートのプライベート IP アドレスを入力します。

ステップ 2 **[IPv4スタティックNATモード（IPv4 static NAT mode）]** を *[オン（On）]* に設定します。

ステップ 3 **[IPv4 スタティック NAT アドレス（IPv4 static NAT address）]** フィールドに、ポートのパブリック IP アドレスを入力します。これは、（NAT 要素外部での）アドレス変換後の IP アドレスです。

IPv6 モードの機能と制限

Expressway の IP インターフェイスを *[IPv6 のみ（IPv6 Only）]* モードに設定すると、これらのインターフェイスは IPv6 のみを使用します。これらは他のシステムとの通信に IPv4 を使用せず、IPv4 と IPv6 の間（デュアル スタック）でインターワーキングを行いません。

サポートされている IPv6 の明示的な機能

- Expressway 登録された IPv6 エンドポイント間のコール。
- DiffServ トラフィック クラス（TC）のタギング。
- TURN サーバ（Expressway-E 上）。
- 自動侵入防御。
- DNS ルックアップ。
- ポートの使用およびステータス ページ。

サポートされている RFC

- RFC 2460：Internet Protocol, Version 6 (IPv6) Specification（この仕様のうち、スタティック グローバル アドレスのみを実装）。
- RFC 2464：Transmission of IPv6 Packets over Ethernet Networks。
- RFC 3596：DNS Extensions to Support IP Version 6。
- RFC 4213：Basic Transition Mechanisms for IPv6 Hosts and Routers。
- RFC 4291：IP Version 6 Addressing Architecture。
- RFC 4443：Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification。
- RFC 4861：Neighbor Discovery for IP version 6 (IPv6)。
- RFC 5095：Deprecation of Type 0 Routing Headers in IPv6。

- RFC 6156：Traversal Using Relays around NAT (TURN) Extension for IPv6。

IPv6 モードの既知の制限

- IPv6 アドレスはスタティックである必要があります。これらは、リンクローカルまたは SLAAC アドレスにはなれません。
- IP アドレスまたはそのゲートウェイの IP アドレスを変更した場合は、Expressway を再起動する必要があります。
- Mobile & Remote Access（MRA）は、IPv6 モードでテストまたはサポートされません。MRA の場合、プライマリ コール制御エージェントは IPv6 をサポートしない Unified CM です。
- 分散証明書失効リストからの失効ステータスの取得は、IPv6 モードではサポートされません。

DNS の設定

[DNS] ページ（**[システム（System）]** > **[DNS]**）を使用して、Expressway の DNS サーバと DNS を設定します。

システム ホスト名とドメイン名の設定

[システム ホスト名（System host name）] で、この Expressway を表す DNS ホスト名を定義します。

- システム ホスト名はクラスタ内の各ピアに一意である必要があります。
- リモートログサーバ上の Expressway を識別するために使用します（**[システムホスト名（System host name）]** を指定しない場合は、デフォルト名の「「TANDBERG」」が使用されます。）
- 名前には、英字、数字、ハイフン、下線のみを使用できます。最初の文字は英字、最後の文字は英字または数字にする必要があります。

[ドメイン名（Domain name）] は、非修飾サーバ アドレス（例：ldapserver）の解決を試みるときに使用されます。クエリが DNS サーバに送信される前に、非修飾サーバ アドレスの末尾に追加されます。サーバアドレスが完全修飾の場合（ldapserver.mydomain.com など）、または IP アドレスの形式である場合は、DNS サーバに問い合わせるまではサーバアドレスの後ろにドメイン名は追加されません。ドメイン名は次の Expressway 設定に適用されます。

- LDAP サーバ
- NTP サーバ
- 外部マネージャ サーバ
- リモート ロギング サーバ

すべてのサーバ アドレスには IP アドレスまたは FQDN（完全修飾ドメイン名）を使用することをお勧めします（Expressway の FQDN は、**システムのホスト名**と**ドメイン名**をつなげた形式になります）。

SIP メッセージングへの影響

システムのホスト名と**ドメイン名**は、SIP メッセージングでのこの Expressway への参照を識別するためにも使用されます。この場合、エンドポイントではその SIP プロキシとして、Expressway を（推奨されていない IP アドレス形式ではなく）FQDN 形式で設定しています。

この場合、たとえばエンドポイントに設定されている FQDN が Expressway に設定されている**システム ホスト名**と**ドメイン名**とが一致しなければ、Expressway は INVITE 要求を拒否します。

（注） SIP プロキシ FQDN は、エンドポイントが Expressway に送信した SIP 要求のルートヘッダーに組み込まれているために、このチェックが行われます。

カスタム ドメイン検索

[ドメイン検索（Search domains）] 設定は、外部ホストが Expressway-C とは異なる DNS ドメイン内にあり、非修飾ホスト名が設定されているエッジ展開に適しています。必要に応じて、この設定を使用して 1 つ以上の DNS ドメインを指定できます。Expressway は、指定されたドメインを 1 つずつ非修飾ホスト名に追加し、作成された FQDN を DNS でクエリします。DNS から IP アドレスが返されるまで、このプロセスが繰り返されます。つまり、ホスト間の接続を設定する際は、FQDN を入力する必要はありません。

複数のアドレスはスペースで区切ります。

DNS 要求

デフォルトでは、DNS 要求はシステムのエフェメラル ポート範囲にあるランダム ポートを使用します。その代わりに、必要に応じて、**[DNS 要求のポート範囲（DNS requests port range）]** を [カスタムポート範囲を使用（Use a custom port range）] に設定してから、[DNS 要求のポート範囲の開始（DNS requests port range start）] フィールドと [DNS 要求のポート範囲の終了（DNS requests port range end）] フィールドを定義することによって、カスタム ポート範囲を指定できます。

（注） 設定したソースポート範囲が狭いと、DNS スプーフィング攻撃に対する脆弱性が高まります。

DNS サーバ アドレスの設定

次の場合は、アドレス解決のために 1 つ以上の DNS サーバをクエリするように指定する必要があります。

- 外部アドレスの指定時に、IP アドレスではなく FQDN を使用する場合（LDAP および NTP サーバや、ネイバー ゾーン、ピアなど）。
- URI ダイヤリングについてや ENUM ダイヤリングについてなどの機能を使用する場合。

デフォルトの DNS サーバ

最大 5 つのデフォルトの DNS サーバを指定できます。Expressway は一度に 1 つのサーバをクエリします。そのサーバが利用不可の場合、Expressway はリスト内の別のサーバを試します。

サーバを指定する順序は重要ではありません。Expressway は、最後に利用可能であることが既知となったサーバを優先します。

ドメイン単位の DNS サーバ

5 つのデフォルトの DNS サーバに加え、指定したドメインに 5 つの明示的 DNS サーバを指定できます。これは、特定のドメイン階層が明示的部署にルーティングされる必要がある場合、導入で役に立ちます。

追加するドメイン別 DNS サーバの各アドレスに、最大 2 つの**ドメイン名**を指定できます。これらのドメインでの DNS クエリは、デフォルト DNS サーバではなく、指定した DNS サーバに転送されます。

ドメインごとの冗長サーバを指定するには、ドメインごとの DNS サーバ アドレスをさらに追加し、そのアドレスを同じ**ドメイン名**に関連付けます。これらのドメインに対する DNS 要求は両方の DNS サーバに同時に送信されます。

特定のホスト名の要求に、どのドメインネーム サーバ（DNS サーバ）が応答しているかを確認するには、DNS ルックアップツール（**[メンテナンス（Maintenance）]** > **[ツール（Tools）]** > **[ネットワークユーティリティ（Network utilities）]** > **[DNS ルックアップ（DNS lookup）]**）を使用します。

転送プロトコル

Expressway は UDP と TCP を使用して DNS 解決を行います。DNS サーバからは、通常、UDP と TCP 応答が送られます。UDP 応答が 512 バイトの UDP メッセージ サイズの制限を超えていると、Expressway は UDP 応答を処理できません。一般に、これが問題になることはありません。Expressway は代わりに TCP 応答を処理できるためです。

ただし、ポート 53 での TCP インバウンドをブロックしている場合、UDP 応答のサイズが 512 バイトを超えていると、Expressway は DNS からの応答を処理できません。この場合、DNS ルックアップ ツールを使用しても結果は表示されず、要求したアドレスを必要とするすべての操作は失敗します。

DNS レコードのキャッシング

DNS ルックアップをキャッシュすることでパフォーマンスを向上させることができます。DNS 設定が変更されるたびに、キャッシュが自動的に消去されます。必要に応じて、[DNS キャッシュの消去（Flush DNS cache）] をクリックして強制的に消去することもできます。

DSCP / Quality of Service の設定

DSCP マーキングについて

X8.9 から、Expressway では Mobile & Remote Access を含む、ファイアウォールを通過するトラフィックに対する、改善された DSCP（DiffServ コード ポイント）パケット マーキングがサポートされます。DSCP は、パケットの QoS レベルの測定です。トラフィックの優先順位付けに対してきめ細かい制御を提供するために、DSCP 値はこれらの個々のトラフィック タイプに対して送信（マーキング）されます。

トラフィックのタイプ	提供されたデフォルト値	Web UI フィールド
ビデオ	34	QoS Video
音声	46	QoS Audio
XMPP	24	QoS XMPP
シグナリング	24	QoS Signaling

X8.9 以前は、すべてのシグナリングとメディア トラフィックにまとめて DSCP 値を適用する必要がありました。

必要に応じて、**[システム（System）] > [QoS（Quality of Service）]** の Web UI ページ（または [CLI]）から、デフォルトの DSCP 値を変更できます。

注：

- DSCP 値「「0」」は標準のベストエフォートサービスを指定します。
- DSCP マーキングは SIP と H.323 トラフィックに適用されます。
- TURN トラフィックが実際に Expressway により処理される場合は、DSCP マーキングは TURN メディアに適用されます。
- メディアタイプが特定できない場合、トラフィックタイプ「「ビデオ」」がデフォルトで割り当てられます。（たとえば、異なるメディア タイプが同じポートに多重化されている場合です）。

既存の QoS/DSCP コマンドと API の廃止

（注） X8.9 から QoS/DSCP 値を指定する、以前の方法をサポートしていません。以前の Web UI 設定の QoS モードおよび QoS 値、CLI コマンド `xConfiguration IP QoS Mode` と `xConfiguration IP QoS Value` および対応する API は廃止されました。これらのコマンドは使用しないでください。

現在これらのコマンドを使用している場合

Expressway をアップグレードするときに、定義された既存の QoS の値は新規フィールドに自動的に適用され、提供されたデフォルトを置き換えます。たとえば、値20を定義したら、4つの DSCP すべての設定（QoS Audio、QoS Video、QoS XMPP、QoS Signaling）も 20 に設定されます。

ダウングレードはサポートされません。アップグレード前のソフトウェアバージョンに戻る必要があると、QoS の設定は、最初に提供されるデフォルト値にリセットされます。つまり、QoS モードは [なし（None）] に、QoS 値は [0] に設定されます。手動で、使用する値を定義し直す必要があります。

DSCP 値の設定

必要に応じて、指定された DSCP のデフォルト値を変更するには、**[QoS（Quality of Service）]** ページ（**[システム（System）]** > **[QoS（Quality of Service）]**）に移動し、使用する新しい値を指定します。

スタティック ルート

Expressway から IPv4 または IPv6 のアドレス範囲へのスタティック ルートを定義できます。**[システム（System）]** > **[ネットワーク インターフェイス（Network interfaces）]** > **[スタティック ルート（Static routes）]** に移動します。

このページでは、スタティック ルートを表示、追加、削除できます。

[高度なネットワーキング（Advanced Networking）] オプションを使用して DMZ に Expressway を導入する場合は、スタティック ルートが必要になることがあります。また、他の複雑なネットワーク導入環境でも必要になることがあります。

スタティック ルートの追加：

手順

ステップ 1 この Expressway からの新しいスタティックルートの基本宛先アドレスを入力します。

`203.0.113.0` または **`2001:db8::`** などと入力します。

ステップ 2 範囲を定義するプレフィックス長を入力します。

この例を拡張する場合、**`24`** と入力して IPv4 範囲の 203.0.113.0 ～ 203.0.113.255 を定義するか、または **`32`** と入力して IPv6 範囲の 2001:db8:: ～ 2001:db8:ffff:ffff:ffff:ffff:ffff:ffff を定義します。

アドレス範囲フィールドに、IP アドレスとプレフィックス長から Expressway が計算した範囲が表示されます。

ステップ 3 新しいルート用にゲートウェイの IP アドレスを入力します。

ステップ 4 新しいルートのイーサネットインターフェイスを選択します。

このオプションは、2つ目のイーサネットインターフェイスが有効な場合にのみ、使用できます。*[LAN 1]* または *[LAN 2]* を選択してそのインターフェイスを介したルートを適用するか、*[*自動（*Auto*）*]* を選択して Expressway がいずれのインターフェイスでもこのルートをとれるようにします。

ステップ 5 **[ルートの作成（Create route）]** をクリックします。

新しいスタティックルートがテーブルに表示されます。必要に応じて、このテーブルからルートを削除できます。

（注）
- IP ルートは CLI を使用して設定することもできます。その場合は、xCommand RouteAdd コマンドと xConfiguration IP Route コマンドを使用します。
- 最大 50 のネットワークとホストの組み合わせを設定できます。
- `root` としてログインし、`ip route` ステートメントを使用して IP ルートを設定しないでください。

侵入からの保護

ファイアウォール ルールの設定

ファイアウォール ルールは Expressway へのアクセスを IP レベルで制御する IP テーブル ルールを設定する機能を提供します。Expressway では、これらのルールが複数のグループに分類されており、次の順序で適用されます。

- **動的システム ルール**：これらのルールは、すべての確立された接続/属性を維持します。これらには、特定のアドレスをブロックするなど、自動検出機能によって挿入された任意のルールも含まれます。最後に、ループバック インターフェイスからのアクセスを許可するルールが含まれます。
- **設定不可のアプリケーション ルール**：このルールはアプリケーション固有の必要なすべてのルール（SNMP トラフィックや H.323 ゲートキーパー検出を許可するなど）を組み込みます。
- **ユーザ設定が可能なルール**：このオプションは、手動で設定したすべてのファイアウォール ルール（この項で説明）を組み込みます。このルールは、何が Expressway にアクセス可能なのか（通常は何を制限するか）を詳細に定義します。このグループには、Expressway LAN 1 インターフェイス（および**高度なネットワーキング** オプション キーがインストールされている場合には LAN 2 インターフェイス）に送信されるすべてのトラフィックを許可する最終的なルールがあります。

また、以前のルールによってまだ明確に許可されていない、または拒否されていないブロードキャストやマルチキャストのトラフィックを破棄する、設定できない最終的なルールもあります。

デフォルトでは、Expressway の特定の IP アドレスに送信されるトラフィックはアクセスが許可されますが、Expressway が明示的にそのトラフィックをリッスンしていない場合はそのトラフィックが破棄されます。仕様に対してシステムをロック ダウンするには、追加のルールをアクティブに設定する必要があります。

（注） 発信接続からのリターントラフィックは常に受け入れ可能です。

ユーザ設定ルール

通常、ユーザ設定のルールは、何が Expressway へアクセスできるかを制限するために使用されます。次の操作を実行できます。

- そこからのトラフィックを許可または拒否する、発信元 IP アドレスのサブネットを指定します。
- 拒否されたトラフィックをドロップするか却下するかを選択します。

  シナリオによっては、ファイアウォール ルールでドロップまたは拒否するように設定されているインバウンド トラフィックでも、Expressway がプロキシする場合があります。これは、□ファイアウォール ルールは新しいインバウンド トラフィックにのみ適用されるためです。内部ネットワーク上のデバイスがアウトバウンド接続を開始した場合、外部ネットワーク上のデバイスは同じポートを使用して応答します。IP テーブルには既存のメディア パス情報が含まれているため、□ファイアウォール ルールよりも優先されます。
- SSH、HTTP/HTTPS などのよく知られたサービスを設定するか、トランスポート プロトコルとポート範囲に基づいてカスタマイズされたルールを指定します。
- LAN 1 インターフェイスと LAN 2 インターフェイスには異なるルールを設定します（**高度なネットワーキング** オプション キーがインストールされている場合）。ただし、マルチキャスト アドレスなどの特定の宛先アドレスは設定できません。
- ルールを適用するプライオリティを指定します。

ファイアウォール ルールの設定およびアクティブ化

[ファイアウォール ルールの設定（Firewall rules configuratio）] ページを使用して、一連の新しいファイアウォール ルールを設定し、アクティブにします。

表示されたルールセットが最初に、現在アクティブなルールのコピーになります。（ファイアウォール ルールが定義されていないシステムでは、リストは空です。）ルールの数が多い場合は、**[フィルタ（Filter）]** オプションを使用して表示されるルール セットを限定できます。

（注） 組み込みルールは、このリストには表示されません。

一連のファイアウォール ルールを変更するには、新しいルールを追加するか、または既存のルールを修正または削除します。現在のアクティブなルールに加えた変更は保留状態に維持されます。変更が完了したら、新しいルールをアクティブにして前のセットを置き換えます。UDP 関連のルールの場合、新しいルールは次のシステムの再起動時にのみ有効になります（ただし、UDP ルールを削除すると、ルール セットをアクティブにした後すぐに無効になります）。

ルールを設定しアクティブにするには、次の手順を実行します。

手順

ステップ 1 **[システム（System）] > [保護（Protection）] > [ファイアウォールルール（Firewall rules）] > [設定（Configuration）]** に移動します。

ステップ 2 必要に応じてルールを追加、変更、または削除して変更を加えます。

ルールの順序を変更するには、上下矢印キー と を使用して、隣接するルールのプライオリティを入れ替えます。

- 新規または変更されたルールは **[保留中（Pending）]**（**[状態（State）]** カラム内）として表示されます。
- 削除されたルールは、[削除保留中（Pending delete）] として表示されます。

ステップ 3 新しい一連のファイアウォールルールの設定が終了したら、**[ファイアウォールルールのアクティブ化（Activate firewall rules）]** をクリックします。

ステップ 4 新しいルールをアクティブ化することを確認します。これにより、既存のアクティブなルールセットが設定したばかりのルール セットに置き換えられます。

新しいルールをアクティブ化することを確認した後、これらは検証され、エラーがあれば報告されます。

ステップ 5 エラーがなければ、新しいルールが一時的にアクティブ化され、「**ファイアウォール ルールの確認（Firewall rules confirmation）**」ページが表示されます。

ここで、15 秒以内に新しいルールを保存することを確認します。

- **[変更内容を受け入れる（Accept changes）]** をクリックして永続的にルールを適用します。
- 15 秒の制限時間をすぎた場合、または **[変更のロールバック（Rollback changes）]** をクリックすると、以前のルールが復帰し、設定ページに戻ります。

  15 秒の時間制限によって実行される自動ロールバック機能により、新しいルールが適用された後でも、変更がアクティブ化されたクライアント システムは、以前と同様にシステムにアクセスできます。クライアント システムが（Web インターフェイスにアクセスでき

なくなったために）変更を確認できない場合、ロールバックにより、再びシステムにアクセスできるようになることが確認されます。

ステップ 6 この手順は、UDP ルールを追加する場合にのみ適用されます。つまり、**[転送（Transport）] =***[UDP]* を設定した 1 つ以上のカスタムルールです。新しい UDP ルールは、次にシステムを再起動するまで有効になりません。この特殊なケースでは、ファイアウォール ルールの有効化だけでは十分ではありません。削除された UDP ルールにはこの要件はなく、ルール セットを有効にするとすぐに無効になります。

ファイアウォールルールを設定すると、**[すべての変更内容を復元（Revert all changes）]** オプションも表示されます。これによって、保留中のすべての変更が破棄され、ルールの作業中のコピーが現在のアクティブなルールと一致するようにリセットされます。

ルール設定

各ルールの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
優先度（Priority）	ファイアウォール ルールを適用する順序。	最もプライオリティの高いルール（1、次が 2、その次が 3 など）が最初に適用されます。 ファイアウォール ルールのプライオリティは一意にする必要があります。同じプライオリティを持つルールが複数あるとルールのアクティブ化が失敗します。
インターフェイス	アクセスを制御する LAN インターフェイス。	これは、**高度なネットワーキング**のオプションキーがインストールされている場合にのみ適用されます。

フィールド	説明	使用方法のヒント
IP アドレス（IP address）とプレフィックス長（Prefix length）	これら 2 つのフィールドによって、ルールが適用される IP アドレスの範囲が決定されます。	**[アドレス範囲（Address range）]** フィールドに、**[IP アドレス（IP address）]** と **[プレフィックス長（Prefix length）]** の設定の組み合わせに基づき、ルールが適用される IP アドレスの範囲が表示されます。 プレフィックス長の範囲は、IPv4 アドレスの場合は 0 ～ 32、IPv6 アドレスの場合は 0 ～ 128 です。
サービス	ルールが適用されるサービスを選択するか、*[カスタム（Custom）]* を選択して、独自の転送タイプとポート範囲を指定します。	**（注）** サービスの宛先ポートをこの後で Expressway 上に再設定する場合は（80～8080 など）、以前のポート番号を含むファイアウォールルールは自動的に更新されません。
トランスポート（Transport）	ルールが適用されるトランスポート プロトコル。	サービスを *[カスタム（Custom）]* に指定している場合のみ適用されます。
ポート範囲の開始と終了	ルールが適用されるポート範囲。	UDP または TCP の *[カスタム（Custom）]* サービスを指定している場合のみ適用されます。

フィールド	説明	使用方法のヒント
アクション（Action）	ルールに一致する IP トラフィックに対して実行されるアクション。 *[*許可（*Allow*）*]*：トラフィックを受け入れます。 *[*ドロップ（*Drop*）*]*：送信者に応答せずにトラフィックをドロップします。 *[*拒否（*Reject*）*]*：「「unreachable」」という応答によりトラフィックを拒否します。	トラフィックをドロップすると、潜在的な攻撃者には、どのデバイスがパケットをフィルタリングするか、またその理由などの情報が提供されません。 導入の環境をセキュアにするため、まずすべてのサービスへのアクセスを拒否するプライオリティの低いルール セット（たとえばプライオリティ 50000）を設定してから、特定の IP アドレスへのアクセスを選択的に許可するプライオリティのより高いルール（たとえばプライオリティ 20）を設定することができます。
説明	（オプション）ファイアウォール ルールのフリー形式の説明。	ルールの数が多い場合は、オプションの説明により **[フィルタ（Filter）]** を使用して、関連するルール セットを見つけることができます。

現在アクティブなファイアウォール ルール

[現在アクティブなファイアウォールルール（Current active firewall rules）] ページ（**[システム（System）] > [保護（Protection）] > [ファイアウォール ルール（Firewall rules）] > [現在アクティブなルール（Current active rules）]**）には、システムに現在設定されているユーザ設定のファイアウォールルールが表示されます。このリストに表示されない組み込みルール セットもあります。

ルールを変更するには、「**ファイアウォールのルール設定（Firewall rules configuration）**」ページに移動する必要があります。ここで、新しいルールセットの設定とアクティブ化ができます。

自動化された侵入からの保護の設定

自動保護サービスを使用して、悪意のあるトラフィックを検出およびブロックし、辞書ベースでの不正ログイン攻撃から Expressway を保護することができます。

これは、システム ログ ファイルを解析して、SIP、SSH、Web/HTTPS アクセスなど、特定のサービス カテゴリへの繰り返されるアクセスの失敗を検出することにより機能します。指定し

た時間ウィンドウ内の失敗の数が設定したしきい値に達すると、送信元のホストアドレス（侵入者）と宛先ポートは、指定した期間ブロックされます。この期間を過ぎると、一時的にブロックされた可能性のある悪意のないのホストを締め出すことがないよう、ホストアドレスは自動的にブロック解除されます。

1 つまたは複数のカテゴリで例外となるアドレス範囲を設定することができます（下記の、例外の設定を参照してください）。

ファイアウォール ルールの設定は、ファイアウォール ルールと組み合わせて使用する必要があります。特定の脅威を動的に検出して一時的にブロックするのには、自動保護を使用し、一定範囲の既知のホスト アドレスを永続的にブロックするのには、ファイアウォール ルールを使用します。

保護カテゴリについて

Expressway で使用可能な一連の保護カテゴリは、実行中のソフトウェアのバージョンに応じて事前に設定されています。各カテゴリを有効化、無効化、および設定することはできますが、新たなカテゴリを追加することはできません。

また、特定のログ ファイル メッセージを各カテゴリに関連付けるルールは事前に設定されており、変更できません。**[システム（System）]** > **[保護（Protection）]** > **[自動検出（Automated detection）]** > **[設定（Configuration）]** に移動してカテゴリの名前をクリックすることにより、特定のカテゴリへのアクセスの失敗/侵入として処理されたログファイルエントリのサンプルを確認することができます。サンプルは、ページ下部の **[ステータス（Status）]** セクションの上部に表示されます。

自動保護の有効化

X8.9以降、次を含むさまざまなカテゴリの自動侵入防御がデフォルトで有効になっています。

- HTTP プロキシ認証の失敗
- HTTPプロキシプロトコル違反
- SSH認証エラー
- SSHプロトコル違反
- XMPPプロトコル違反

この変更は新しいシステムに影響します。アップグレードされたシステムは既存の防御設定を維持します。

手順

ステップ 1 **[システム（System）]** > **[管理（Administration）]** に移動します。
ステップ 2 **[自動保護サービス（Automated protection service）]** を *[オン（On）]* に設定します。
ステップ 3 **[保存（Save）]** をクリックします。

これでサービスは実行されますが、環境に必要な保護カテゴリと例外を設定する必要があります。

保護カテゴリの設定

[自動検出の概要（Automated detection overview）] ページ（**[システム（System）]** > **[保護（Protection）]** > **[自動検出（Automated detection）]** > **[設定（Configuration）]**）を使用して、Expressway の保護カテゴリを有効にして設定し、現在のアクティビティを表示します。

このページには、以下に示す、すべての使用可能なカテゴリの概要が表示されます。

- **[ステータス（Status）]**：カテゴリが *[オン（On）]* または *[オフ（Off）]* のどちらに設定されているかを示します。*[オン（On）]* の場合、さらにカテゴリの状態が示されます。通常は *[アクティブ（Active）]* の状態になっていますが、カテゴリが有効化または無効化された直後は一時的に *[初期化中（Initializing）]* または *[シャットダウン中（Shutting down）]* と表示される場合があります。[失敗（Failed）] と表示されている場合は、アラームを確認してください。
- **[現在ブロック中（Currently blocked）]**：このカテゴリで現在ブロックされているアドレスの数。
- **[失敗の合計（Total failures）]**：このカテゴリに関連付けられているサービスへの失敗したアクセス試行の合計数。
- **[ブロックの合計（Total blocks）]**：ブロックがトリガーされた回数。

（注）
- 通常、**[ブロックの合計（Total blocks）]** の数は **[失敗の合計（Total failures）]** の数よりも少なくなります（**[トリガー レベル（Trigger level）]** が 1 に設定されている場合を除く）。
- 同じアドレスが複数回、カテゴリごとにブロックおよびブロック解除される場合があり、各ブロックが個別にカウントされます。

- **[除外（Exemptions）]**：このカテゴリで例外として設定されているアドレスの数。

このページから、現在ブロックされているアドレスや特定のカテゴリに適用されている例外も確認できます。

カテゴリの有効化または無効化

手順

ステップ 1 **[システム（System）] > [保護（Protection）] > [自動検出（Automated detection）] > [設定（Configuration）]** に移動します。

ステップ 2 有効または無効にするカテゴリの隣にあるチェックボックスを選択します。

ステップ 3 必要に応じて **[有効（Enable）]** または **[無効（Disable）]** をクリックします。

カテゴリのブロッキングルールの設定

手順

ステップ 1 **[システム（System）] > [保護（Protection）] > [自動検出（Automated detection）] > [設定（Configuration）]** に移動します。

ステップ 2 設定するカテゴリの名前をクリックします。このカテゴリの設定ページが表示されます。

ステップ 3 必要に応じて、カテゴリの以下の項目を設定します。

- **[状態（State）]**：このカテゴリへの保護を有効にするか無効にするかを指定します。
- **[説明（Description）]**：フリー形式のカテゴリの説明。
- **[Trigger level] および [Detection] ウィンドウ**：これらの設定の組み合わせにより、カテゴリのブロッキングしきい値を定義します。これらにより、失敗したアクセス試行が何回発生したらブロックをトリガーするか、および、これらの失敗の発生数をカウントする時間ウィンドウを指定します。
- **[ブロック期間（Block duration）]**：ブロックが維持される期間。

ステップ 4 [保存（Save）] をクリックします。

例外の設定

[自動検出の除外（Automated detection exemptions）] ページ（**[システム（System）] > [保護（Protection）] > [自動検出（Automated detection）] > [除外（Exemptions）]**）を使用して、1つまたは複数の保護カテゴリから常に除外する IP アドレスを設定できます。

手順

ステップ 1 **[システム（System）] > [保護（Protection）] > [自動検出（Automated detection）] > [例外（Exemptions）]** に移動します。

ステップ 2 設定する **[アドレス（Address）]** または **[新規（New）]** をクリックして新しいアドレスを指定します。

ステップ 3 **[アドレス（Address）]** および **[プレフィックス長（Prefix length）]** に値を入力して、除外する IP アドレスの範囲を定義します。

ステップ 4 このアドレスを例外とするカテゴリを選択します。

ステップ 5 [Add address] をクリックします。

（注） 現在ブロックされているアドレスを除外する場合、（「**ブロックされたアドレス（Blocked addresses）**」ページで手動でブロック解除しない限り）そのアドレスはブロック期限が切れるまでブロックされ続けることに注意してください。

ブロックされたアドレスの管理

「ブロックされたアドレス（Blocked addresses）」ページ（**[システム（System）] > [保護（Protection）] > [自動検出（Automated detection）] > [ブロックされたアドレス（Blocked addresses）]**）を使用して、自動保護サービスにより現在ブロックされているアドレスを管理できます。

- これにより、現在ブロックされているすべてのアドレス、それらのアドレスがどのカテゴリからブロックされているかが表示されます。
- アドレスをブロック解除するか、または、アドレスのブロック解除と同時にそれを例外リストに追加することができます。アドレスを永続的にブロックする場合は、そのアドレスを設定済みのファイアウォール ルールの設定に追加する必要があります。

「**自動検出の概要（Automated detection overview）**」ページに記載のリンクによってこのページにアクセスした場合、選択したカテゴリによってページの内容がフィルタリングされています。また、アドレスがそのカテゴリからブロック解除されるまでの残り時間も表示されます。

アクセスの失敗および侵入の調査

特定のアクセスの失敗または侵入の試行を調査する必要がある場合、各カテゴリに関連付けられた関連トリガーのログ メッセージをすべて確認することができます。目的

手順

ステップ 1 **[システム（System）] > [保護（Protection）] > [自動検出（Automated detection）] > [設定（Configuration）]** に移動します。

ステップ 2 調査するカテゴリの名前をクリックします。

ステップ 3 [このカテゴリについて一致するすべての侵入からの保護のトリガーを表示する（View all matching intrusion protection triggers for this category）] をクリックします。

そのカテゴリのすべての関連イベントが表示されます。その後、トリガー中のイベントのリストを検索すると、ユーザ名、アドレス、またはエイリアスなど、関連イベントの詳細を確認できます。

自動保護サービスおよびクラスタ化システム

自動保護サービスがクラスタ化システムで有効の場合、以下のように動作します。

- ピアでごとにそれぞれの接続の失敗数が維持され、それぞれのピアでトリガーしきい値に達したときに初めて、侵入者のアドレスはそれぞれのピアによりブロックされます。
- アドレスは、アクセスの失敗が発生したピア対してのみブロックされます。つまり、アドレスがあるピアでブロックされた場合でも、（やはりブロックされる可能性がある）他のピアへアクセスを試行することができます。
- ブロックされているアドレスは、現在のピアに対してのみブロック解除できます。アドレスが他のピアによりブロックされている場合は、そのピアにログインしてから解除する必要があります。
- カテゴリの設定および例外リストは、クラスタ全体に適用されます。
- 「**自動検出の概要（Automated detection overview）**」ページには、現在のピアの統計情報のみが表示されます。

MRA 導入での自動保護

Expressway-C を Mobile & Remote Access に使用すると、Unified CM と Expressway-E から多くのインバウンド トラフィックを受信します。

Expressway-C の自動保護を使用するには、自動的に作成されたネイバー ゾーンとユニファイド コミュニケーションのセキュアなトラバーサル ゾーンを使用するすべてのホストについて免除を追加する必要があります。Expressway は、検出された Unified CM または関連ノードの免除を自動では作成しません。

その他の情報

- ブロックされているホストアドレスがシステムにアクセスしようとすると、要求はドロップされます（ホストは応答を受信しません）。
- 複数のカテゴリでホストアドレスを同時にブロックすることは可能ですが、すべてのカテゴリでブロックされるとは限りません。それぞれのブロックが異なるタイミングで期限切れになる可能性があります。
- （手動で、またはブロック期限が終了して）アドレスがブロック解除された場合は、カテゴリのトリガー レベルで指定した数の失敗が消化されて初めて、そのカテゴリによる2回目のブロックを設定できます。

- カテゴリは、有効になるたびにリセットされます。システムが再起動した場合、または自動保護サービスがシステム レベルで有効になると、すべてのカテゴリがリセットされます。カテゴリがリセットされると、以下のように動作します。
  - 現在ブロックされているアドレスがあれば、ブロック解除されます。
  - 失敗およびブロックの現在の合計はゼロにリセットされます。
- 「**自動検出の概要（Automated detection overview）**」ページで **[すべての侵入からの保護イベントを表示（View all intrusion protection events）]** をクリックすると、自動保護サービスに関連付けられているすべてのイベント ログが表示されます。
- アップグレード元 X14.0 リリース：
  - SIP 登録の失敗は、新しいインストールと工場出荷時のリセットケースでデフォルトで有効になっています。アップグレードのシナリオでは、前の値が保持されます。
  - SIP 認証の失敗は、新しいインストールと工場出荷時のリセットケースでデフォルトで有効になっています。アップグレードのシナリオでは、前の値が保持されます。
  - Expressway-C がサービスに影響を与えている場合は、SIP 認証失敗ジェイルルールを無効にします。

レート制限の設定

レート制限の概要ページ（**[システム（System）]** > **[保護（Protection）]** > **[レートの制限（Rate limits）]** > **[設定（Configuration）]**）は、クラッシュ、CPU 使用率が高い、メモリ使用量が多いなどの問題なく Expressway が実行できる SIP トラフィック レートを制限するために使用されます。

X14.0 リリースから、SIP トラフィックのレート制限はデフォルトで有効になっています。

1. デフォルトでは、1 秒あたり 100 の接続が許可され、SIP ポート 5060、5061、& 5062 に設定されている場合は 20 の制限があります。
2. 1 秒あたりの接続数および制限速度を有効または無効にするか、変更できます。
3. 秒の範囲の値あたりの接続数は 1 ~ 150 で、デフォルト値は 100 です。
4. 限界範囲の値は 15 ~ 30 で、デフォルト値は 20 です。
5. バーグラフには、確立された接続数とドロップされた接続数が表示されます。

重要

- TCP プロトコルの場合にのみ 「新規」 の状態が新しい接続と見なされます。関連した接続および確立された接続はすべて同じ接続として扱われるため、パケットが既存の接続からドロップされません。
- UDP プロトコルの場合は、関連した接続および確立された接続すべてが 「新規」 接続として実行されます。

レート制限ルールの設定

レート制限ルールを設定するには、次の手順を実行します。

1. **[システム（System）]** > **[保護（Protection）]** > **[レートの制限（Rate limits）]** > **[設定（Configuration）]** へ移動します。
2. 設定するカテゴリの名前をクリックします。

   このカテゴリの設定ページが表示されます。
3. 必要に応じて、カテゴリの以下の項目を設定します。
   1. **[ステータス（Status）]**：レート制限モードが有効か無効かを示します。
   2. **接続（1 秒毎）**：1 秒あたりの接続数を変更します。
   3. **[限界値（Burst limit）]**：一致する接続/パケットの最大初期数で、この数値は、上記の制限に達するたびに、この数値まで 1 ずつ再充電されます。
4. [保存（Save）] をクリックします。

ネットワーク サービス

システム名とアクセス設定値の設定

「システム管理（System administration）」ページ（**[システム（System）]** > **[管理（Administration）]**）は、次の設定に使用します。

- Cisco Expressway システムの名前。
- 管理者が使用できるシステムへのアクセス方法。シリアルケーブルでユニットに直接接続された PC を使用して Expressway を管理できますが、IP を使用してリモートからシステムにアクセスしなければならない場合もあります。それには、HTTPS を介して Web インターフェイスを使用するか、SSH を介してコマンド ライン インターフェイスを使用します。
- FindMe または Cisco Telepresence Management Suite Provisioning Extension に含まれる他のプロビジョニング サービスを使用するかどうか。

- 管理サービス（Web ユーザインターフェイス、REST API、CLI）が LAN3 上で Expressway の専用管理インターフェイス（DMI）を使用するために、オプションで管理サービスの直接管理トラフィック。

表 *12 : [*システム管理（***System Administration***）*]* ページの設定

フィールド	説明	使用方法のヒント
システム名（System name）	Expressway を識別するために使用します。システム名は、Web インターフェイスのさまざまな場所、および（ラック内の他のシステムと識別できるように）ユニットの前面パネルに表示されます。	容易に、かつ一意的にシステムを識別できる名前を付けることを推奨します。
エフェメラル ポート範囲（Ephemeral port range）	Expressway コール処理によって制限されている場合を除き、**開始**値と**終了**値によって、エフェメラル アウトバウンド接続に使用するポート範囲が定義されます。	
Services		
シリアル ポート/コンソール（Serial port/console）	VMware コンソール経由でシステムにローカルでアクセスできるかどうか。 デフォルトは [On] です。	シリアル ポート/コンソール アクセスは、通常は無効になっていますが、再起動後の 1 分間は常に有効になります。
SSH サービス（SSH service）	SSH と SCP を使用して Expressway にアクセスできるかどうか。 デフォルトは [On] です。	
Web インターフェイス（HTTPS を使用）（Web interface (over HTTPS)）	Web インターフェイス経由で Expressway にアクセスできるかどうか。 デフォルトは [On] です。	

フィールド	説明	使用方法のヒント
プロビジョニング サービス（**Provisioning services**）	**[システム（System）]** > **[TMS プロビジョニング拡張サービス（TMS Provisioning Extension services）]**のページに、Expressway Web ユーザインターフェイスでアクセスさせるかどうかを指定します。アクセス可能な場合、このページから、Cisco TelePresence Management Suite Provisioning Extension（Cisco TMSPE）とユーザ、デバイス、FindMe、電話帳のプロビジョニング サービスに接続できます。 デフォルトは [オフ（Off）] です。	FindMe は、Expressway X12.5 で非推奨となり、以降のリリースではサポートが終了します。
専用管理インターフェイス（**DMI**）のみを使用	管理サービス（Web ユーザインターフェイス、REST API、CLI）が LAN3 上で Expressway の専用管理インターフェイス（DMI）を使用するために、オプションで管理サービスの管理トラフィックが必要です。 デフォルトは [いいえ（No）] です。	SNMP 管理トラフィックでは、**[システム > SNMP]** ページから同じ機能を使用できます。
セッション制限（**Session Limit**）		
セッション タイム アウト（**Session time out**）	セッションがタイムアウトするまでに管理セッション（シリアル ポート、HTTPS、または SSH）または FindMe セッションが非アクティブになる可能性がある分数。デフォルトは 30 分です。	
アカウント単位のセッションの制限（**Per-account session limit**）	個々の管理者アカウントが各 Expressway で許可される同時セッション数。	これには、Web セッション、SSH セッション、およびシリアル セッションが含まれます。セッション制限は、root アカウントには適用されません。 値を 0 にすると、セッション制限はオフになります。

フィールド	説明	使用方法のヒント
システム セッションの制限（System session limit）	各 Expressway で許可される同時管理者セッションの最大数。	これには、Web セッション、SSH セッション、およびシリアル セッションが含まれます。セッション制限は、root アカウントには適用されません。ただし、アクティブなルートアカウントセッションは、現在の管理者セッションの総数にカウントされます。 値を 0 にすると、セッション制限はオフになります。
システム保護（System protection）		
自動保護サービス（Automated protection service）	自動化された侵入からの保護の設定をアクティブにするかどうかを指定します。 デフォルトは [On] です。	サービスを有効にした後は、特定の保護カテゴリについてを設定する必要があります。
自動検出保護（Automatic discovery protection）	Cisco TMS などの管理システムがこの Expressway をどのように検出するかを制御します。 *[オフ（Off）]*：自動検出が許可されます。 *[オン（On）]*：この Expressway を検出するように Cisco TMS を手動で設定する必要があります。また、Cisco TMS が管理者アカウントのクレデンシャルを提供する必要があります。 デフォルトは [オフ（Off）] です。	システムを再起動して変更はすべて有効にします。
Web サーバの設定（Web server configuration）		
HTTP リクエストを HTTPS にリダイレクト（Redirect HTTP requests to HTTPS）	HTTP 要求を HTTPS ポートにリダイレクトするかどうかを指定します。 デフォルトは [オフ（Off）] です。	HTTP を使用したアクセスを機能させるには、HTTPS も有効にする必要があります。 プロトコルを前に付加しないでアドレスを入力すると、ブラウザでは HTTP（ポート 80）と想定します。この設定が *[オン（On）]* の場合、Expressway は Web ブラウザを **Web 管理者ポート** にリダイレクトします。

フィールド	説明	使用方法のヒント
HTTP Strict Transport Security (HSTS)	Webブラウザがこのサーバへのアクセスにセキュアな接続のみを使用するように指示するかどうかを決定します。この機能を有効にすると、中間者（MITM）攻撃に対する保護が強化されます。 *[オン（On）]*：Webサーバからのすべての応答は、有効期限が 1 年の Strict Transport Security ヘッダーが追加されて送信されます。 *[オフ（Off）]*：：Strict Transport Security ヘッダーは送信されず、ブラウザは通常どおりに動作します。 デフォルトは [オン（On）] です。	HSTS の詳細については、以下を参照してください。
Web 管理者ポート（Web administrator port）	管理者が Expressway Web インターフェイスにアクセスするための https リスニング ポートを設定します。 Meeting Server Web プロキシなどで TCP 443 を必要とする機能を有効にする場合は、Expressway-E で Web 管理にデフォルト以外のポートを使用することを強くお勧めします。 変更を有効にするために Expressway を再起動します。	デフォルト以外のポートを使用し、アドレスの前に `https://` プロトコルを付加する場合は、ポートを付加する必要があります。たとえば、ブラウザにアドレス *https://vcse.example.com:7443* を入力します。*https://vcse.example.com* を使用すると、ブラウザはポート 443 を想定し、Expressway はアクセスを拒否します。 ネットワーク要素が Web 管理ポートへのトラフィックをブロックすると、Expressway への Web アクセスが失われることがあります。この状態が発生した場合は、SSH またはコンソールを使用してポートを変更できます。

フィールド	説明	使用方法のヒント
クライアント証明書ベースのセキュリティ（Client certificate-based security）	クライアント システム（通常は Web ブラウザ）が HTTPS を使用して Expressway と通信するために必要なセキュリティ レベルを制御します。 *[*不要（*Not required*）*]*：クライアント システムはどのような形式の証明書も提示する必要はありません。 *[*証明書の検証（*Certificate validation*）*]*：クライアント システムは、信頼できる認証局（CA）が署名した有効な証明書を提示する必要があります。 （注） *[*不要（*Not required*）*]* から *[*証明書の検証（*Certificate validation*）*]* に変更する場合は、再起動が必要です。 *[*証明書ベースの認証（*Certificate-based authentication*）*]*：クライアント システムは、信頼できる CA が署名した有効な証明書を提示する必要があり、その証明書にはクライアントの認証クレデンシャルが含まれている必要があります。 デフォルト：[不要（Not required）]	

フィールド	説明	使用方法のヒント
		重要 • *[*証明書の検証（*Certificate validation*）*]* を有効にすると、ブラウザ（クライアント システム）は、Expressway の信頼できる CA 証明書リストの CA が署名した有効な（日付において有効であり、CRL により失効されていない）クライアント証明書がある場合にのみ、Expressway の Web インターフェイスを使用できます。 • この機能を有効にする前に、ブラウザに有効なクライアント証明書があることを確認してください。証明書をブラウザにアップロードする手順はブラウザのタイプによって異なります。また、証明書を有効にするにはブラウザの再起動が必要になる場合もあります。 • CA 証明書をアップロードするには信頼された CA 証明書リストの管理（ページ）ページを、クライアント証明書をテストするにはクライアント証明書のテストページを使用します。 • *[*証明書ベースの認証（*Certificate-based authentication*）*]* を有効にすると、標準のログインメカニズムが使用できなくなります。ブラウザ証明書が有効

フィールド	説明	使用方法のヒント
		で、提供されたクレデンシャルに適切な許可レベルがある場合にのみ、ログインできます。ブラウザ証明書から Expressway がクレデンシャルを取得する方法は、「証明書ベースの認証の設定」ページで設定できます。 • この設定は、Expressway のサーバ証明書のクライアント検証に影響しません。
証明書失効リスト（CRL）の確認中（Certificate revocation list (CRL) checking）	HTTPS クライアント証明書を証明書失効リスト（CRL）と照合して確認するかどうかを指定します。 *[なし（None）]*：CRL チェックは実行されません。 *[ピア（Peer）]*：クライアントの証明書を発行した CA に関連付けられた CRL のみを確認します。 *[すべて（All）]*：クライアントの証明書を発行した CA の信頼できる証明書チェーン内のすべての CRL を確認します。 デフォルト：[すべて（All）]	**[クライアント証明書ベースのセキュリティ（Client certificate-based security）]** が有効になっている場合にのみ適用されます。

フィールド	説明	使用方法のヒント
CRL のアクセス不可のフォールバック動作（CRL inaccessibility 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：[Treat as not revoked]	**[クライアント証明書ベースのセキュリティ（Client certificate-based security）]** が有効になっている場合にのみ適用されます。
展開設定（Deployment Configuration）		

フィールド	説明	使用方法のヒント
Configuration	システムのサイズを決定します。オプションは次のいずれかです。 *[*大（*Large*）*]*：8 個の CPU コア、6 GB のメモリ、1 Gbps または 10 Gbps の NIC。 *[*中（*Medium*）*]*：2 個の CPU コア、4 GB のメモリ、1 Gbps の NIC。	1 Gbps の NIC を使用する中規模システムをアップグレードすると、Expressway は**自動的にアプライアンスを大規模システムに変換します**。その結果、Expressway-E は大規模システムのデフォルトの逆多重化ポート（36000 ～ 36011）で多重化 RTP/RTCP トラフィックをリッスンします。この場合、これらのポートはファイアウォールで開かれないため、Expressway はコールをドロップします。 この問題が発生した場合は、次のいずれかの操作を行います。 • システムのデフォルト サイズを [中（Medium）] に変更し、多重化RTP/RTCP トラフィック用に設定されているポートを使用するには、[中（Medium）] を選択します。 • 大規模システムとして使用する場合は、大規模システムのデフォルトの逆多重化ポートをファイアウォールで開きます。 このオプションは、Expressway-Es として導入され、次の最小仕様でCE1200 以降のアプライアンスでのみ使用できます。 • サポートされる Expressway ソフトウェアバージョン（詳細については、アプライアンスの *Cisco Expressway CExxxx* インストール ガイドを参照） • CPU：8 コア • メモリ：6 GB • NIC：1 Gbps

デフォルトでは、HTTPS と SSH を使用したアクセスが有効になっています。セキュリティを最適化するには、HTTPS と SSH を無効にし、シリアル ポートを使用してシステムを管理しま

す。シリアル ポートへのアクセスではパスワードのリセットが許可されるため、Expressway は物理的にセキュアな環境にインストールすることを推奨します。

HTTP 厳重トランスポートセキュリティ

HTTP Strict Transport Security（HSTS）は、Web サーバがセキュアな接続のみを使用して通信するように Web ブラウザに強制するメカニズムです。バージョンによっては、一部のブラウザでサポートされていない場合があります。HSTS を有効にすると、HSTS をサポートするブラウザは以下のように動作します。

- Web サイトへのセキュアでないリンクは、サーバにアクセスする前に、自動的にセキュアなリンクに置き替えられます（たとえば、`http://example.com/page/` は、`https://example.com/page/` に変更されます）。
- 接続がセキュアである（たとえば、サーバーの TLS 証明書が有効かつ信頼でき、期限切れでない）場合のみアクセスを許可します。

HSTS をサポートしないブラウザは、Strict-Transport-Security ヘッダーを無視し、以前と同じように動作します。サーバには以前と同様にアクセスできます。

対応ブラウザは、完全修飾名で IP アドレスではなくサーバにアクセスする場合に、Strict-Transport-Security ヘッダーのみを尊重します。

SNMP 設定値の設定

[SNMP] ページ（**[システム（System）]** > **[SNMP]**）を使用して、Expressway の SNMP を設定します。

Cisco Telepresence Management Suite（Cisco TMS）や HP OpenView などのツールは SNMP ネットワーク管理システム（NMS）として機能することができます。これらのツールでは、Expressway などのネットワーク デバイスの管理上の注意が必要な状態をモニタできます。Expressway は RFC 1213 で定義されているように、最も基本的な MIB-II ツリー（.1.3.6.1.2.1）をサポートします。

Expressway によって次のような情報が使用可能になります。

- システムの動作期間
- システム名
- ロケーション
- 連絡先
- インターフェイス
- ディスク領域、メモリ、その他の機器固有の統計情報

SNMP は、デフォルトでディセーブルになっています。そのため、Expressway を SNMP NMS（Cisco TMS を含む）でモニタするには、代替の **SNMP モード**を選択する必要があります。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
SNMP モード（SNMP mode）	SNMP サポートのレベルを制御します。 *[*無効（*Disabled*）*]*：SNMP サポートなし。 *[v3* セキュア *SNMP*（*v3 secure SNMP*）*]*：認証および暗号化をサポート。 *[v3* および *TMS* サポート（*v3 plus TMS support*）*]*：セキュア SNMPv3 および、OID 1.3.6.1.2.1.1.2.0 にのみ非セキュア アクセス。 *[v2c]*：非セキュアなコミュニティベースの SNMP。	セキュア SNMPv3 を使用する際に外部マネージャとして Cisco TMS も使用する場合は、[v3 および TMS サポート（v3 plus TMS support）] を選択する必要があります。
説明	SNMP で表示したときのシステムのカスタム説明。デフォルトは、カスタムの説明なし（空のフィールド）です。	このフィールドを空にしておくと、デフォルトの SNMP の説明が使用されます。
コミュニティ名（Community name）	Expressway の SNMP コミュニティ名。 デフォルトは *public* です。	*[v2c]* や *[v3* および *TMS* サポート（*v3 plus TMS support*）*]* を使用している場合にのみ適用されます。
システム管理者（System contact）	Expressway の問題についての問い合わせが可能な担当者の名前。 デフォルトは [管理者（Administrator）] です。	**[システム管理者（System contact）]** および **[ロケーション（Location）]** は、クエリのフォローアップ時に管理者により参照用に使用されます。
[所在地（Location）]	Expressway の物理的な場所を指定します。	
ユーザ名（Username）	Expressway の SNMP ユーザ名。SNMP マネージャに対してこの SNMP エージェントを識別するために使用します。	*[v3* セキュア *SNMP*（*v3 secure SNMP*）*]* または *[v3* および *TMS* サポート（*v3 plus TMS support*）*]* を使用している場合にのみ適用されます。

フィールド	説明	使用方法のヒント
専用管理インターフェイス（DMI）のみを使用	必要に応じて、SNMP が LAN3 で Expressway の専用管理インターフェイス（DMI）を使用するために、管理トラフィックが必要です。 デフォルトは [いいえ（No）] です。	管理サービス（Web ユーザインターフェイス、REST API、CLI）に関連する管理トラフィックでは、**[システム（System）] > [管理の設定（Administration settings）]** ページからでも同じ機能を使用できます。
[v3 認証（v3 Authentication）] の設定（SNMPv3 にのみ適用可能）		
認証モード（Authentication Mode）	SNMPv3 認証を有効または無効にします。	
タイプ（Type）	認証クレデンシャルをハッシュするために使用されるアルゴリズム。X12.5.7 から、SHA（セキュアハッシュアルゴリズム）がサポートされている唯一のオプションです。MD5（メッセージダイジェストアルゴリズム 5）のパスワードはサポートされていません。	
[パスワード（Password）]	認証クレデンシャルの暗号化に使用するパスワード。	8 文字以上でなければなりません。
[v3 プライバシー（v3 Privacy）] の設定（SNMPv3 にのみ適用可能）		
プライバシー モード（Privacy Mode）	SNMPv3 暗号化を有効または無効にします。	
タイプ（Type）	メッセージの暗号化に使用されるセキュリティ モデル。 *[AES]*：Advanced Encryption Standard、128 ビット暗号化。 デフォルトかつ推奨される設定は *[AES]* です。	
[パスワード（Password）]	メッセージの暗号化に使用するパスワード。	8 文字以上でなければなりません。

Expressway は SNMP トラップや SNMP セットをサポートしません。したがって、SNMP を使用して Expressway を管理することはできません。

（注） SNMP は、関連する情報が潜在的に機密情報であるため、デフォルトでは無効になっています。パブリック インターネットまたは内部システム情報を公開したくないその他の環境では、Expressway で SNMP を有効にしないでください。

時刻の設定

[時間（Time）] ページ（**[システム（System）] > [時間（Time）]**）を使用して、Expressway の NTP サーバを設定し、ローカルタイムゾーンを指定します。

NTP サーバは、時刻の正確性を確保するために Expressway が同期するリモート サーバです。NTP サーバは Expressway に UTC 時刻を提供します。

正確なシステム動作を実現するには正確な時刻が必要です。

NTP サーバの設定

システム時刻を同期するときに使用する 1 台以上の NTP サーバで Expressway を設定するには、システムの DNS の設定に応じて（**[DNS]** ページ（**[システム（System）] > [DNS]**）でこれらの設定を確認できます）、次の形式のいずれかで最大 5 台のサーバの **[アドレス（Address）]** を入力します。

- **DNS サーバ**が設定されていない場合は、NTP サーバに IP アドレスを使用します。
- 1 つまたは複数の **DNS サーバ**が設定されている場合、NTP サーバに FQDN または IP アドレスを使用できます。
- 1 台以上の **DNS サーバ**に加えて DNS **ドメイン名**が設定されている場合、そのサーバ名、FQDN、または IP アドレスを NTP サーバに使用できます。

デフォルトでは、3 つの **[アドレス（Address）]** フィールドが、シスコが提供する NTP サーバに設定されます。

NTP サーバへの接続時に Expressway が使用する**認証**方式を設定できます。NTP サーバの接続に、次のオプションのいずれかを使用します。

認証方式	説明
Disabled	認証は使用されません。

認証方式	説明
対称キー（*Symmetric Key*）	対称キー認証。この方式を使用する場合は、**[キーID（Key ID）]**、**[ハッシュ（Hash）]** 方式、**[パスフレーズ（Pass phrase）]** を指定する必要があります。ここで入力した値は、NTP サーバ上での同等の設定値と完全に一致する必要があります。複数の NTP サーバに同じ対称キーの設定を使用できます。ただし、各サーバに異なるパス フレーズを使用して設定する場合は、各サーバに一意のキーIDがあることを確認する必要があります。
秘密キー（*Private key*）	秘密キー認証。この方式では、NTP サーバに送信されるメッセージの認証に、自動生成された秘密キーを使用します。

NTP ステータス情報の表示

[ステータス（Status）] エリアには、NTP サーバと Expressway 間の同期ステータスが次のように表示されます。

- *[起動中（Starting）]*：NTP サービスは起動中です。
- *[同期済み（Synchronized）]*：Expressway は NTP サーバから正確なシステム時刻を正常に取得しています。
- *[非同期（Unsynchronized）]*：Expressway が NTP サーバから正確なシステム時刻を取得できません。
- *[ダウン（Down）]*：Expressway の NTP クライアントは稼働していません。
- *[拒否（Reject）]*：NTP サービスが NTP 応答を受け入れていません。

（注） 更新内容がステータス テーブルに表示されるまで数分かかります。

入手可能なその他の情報は次のとおりです。

フィールド	説明
NTP サーバ	要求に応答した実際の NTP サーバ。これは、NTP サーバのアドレス フィールド内の NTP サーバと異なる場合があります。

フィールド	説明
条件	各 NTP サーバの相対的なランク付けが表示されます。正確な時刻を提供しているすべてのサーバには [候補（Candidate）] というステータスが付与されます。これらのサーバのうち、Expressway が最も正確な時刻を提供しているため、使用しているサーバには、[sys.peer] というステータスが表示されます。
フラッシュ（**Flash**）	サーバのステータスに関する情報を示すコード。`[00 ok]` は、問題がないことを意味します。コードの詳細なリストについては、フラッシュ ステータス ワード参照テーブルを参照してください。
認証	現在の認証方式のステータスを示します。*[正常（ok）]*、*[異常（bad）]*、*[なし（none）]* のいずれか。*[なし（none）]* 方式が [無効（Disabled）]**[認証（Authentication）]** に設定されている場合は *[切断（Disabled）]* に指定されます。
イベント	NTP が特定した最後のイベントを表示します（たとえば、*[reachable]* や *[sys.peer]* など）。
到達可能性（**Reachability**）	Expressway と NTP サーバ間の最新 8 件の接続試行の結果を示します。成功の場合はティック、失敗の場合は十字形が表示されます。最新の試行の結果は右端に表示されます。 NTP の設定が変更されるたびに NTP クライアントは再起動し、**[到達可能性（Reachability）]** フィールドはすべてバツに戻ります。ただし、右側のインジケータには、再起動後の最初の接続の試みの結果が示されます。ただし、再起動プロセス中に NTP サーバがコンタクト可能なままである場合もあります。
オフセット（**Offset**）	NTP サーバの時刻と Expressway の時刻との差。
遅延（**Delay**）	NTP サーバと Expressway とのネットワーク遅延。
ストラタム（**Stratum**）	Expressway とリファレンス クロック間の分離度。`1` は、NTP サーバが基準クロックであることを示します。
リファレンス ID（**Ref ID**）	基準クロックを識別するコード。
リファレンス時刻（**Ref time**）	NTP サーバが基準クロックと最後に通信した時刻。

このページの残りのフィールドの定義と NTP の詳細については、Network Time Protocol Web サイトを参照してください。

Expressway の時刻表示とタイム ゾーン

Webインターフェイス全体で現地時間が使用されます。時刻は画面の下部のシステム情報バーに表示され、イベントログの各行の先頭に表示されるタイムスタンプの設定に使用されます。

（注） UTC タイムスタンプは、イベントログの各イベントの末尾に組み込まれています。

Expressway は内部的にシステム時刻を UTC で維持します。システム時刻は Expressway のオペレーティング システムの時刻に基づいており、NTP サーバを設定する場合は、その NTP を使用して同期されます。NTP サーバが設定されていない場合は、Expressway は独自のオペレーティング システム時刻を使用して日時を決定します。

ローカルの **[タイムゾーン（Time zone）]** を指定すると、システムが存在するローカル時刻を Expressway が決定します。選択したタイムゾーンに関連付けられた時間数（または分数）で UTC 時刻を補正します。また、該当する場合は夏時間を考慮するようにローカル タイムを調整します。

ログイン ページの設定

「ログインページの設定（Login page configuration）」ページ（**[システム（System）]** > > **[ログイン ページ（Login page）]**）を使用して、ログインページに表示されるメッセージや画像を指定できます。管理者がCLIまたはWebインターフェイスを使用してログインすると、**ウェルカム メッセージのタイトル**と**テキスト**が表示されます。

Web インターフェイスを使用すると、ログイン ページのウェルカム メッセージの上に表示される画像をアップロードできます。

- サポートされている画像形式は、JPG、GIF、および PNG です。
- 200 x 200 ピクセルよりも大きな画像は縮小されます。

オプションで、ログインしている人が続行を許可される前にウェルカム メッセージを確認する必要があることを指定できます。この場合、システムは受諾ボタンを表示し、ユーザはこれをクリックしないと続行できません。

Expressway が TMS Provisioning Extension サービスのステータスを使用して FindMe アカウントのデータを提供する場合は、ユーザは Expressway ではなく、Cisco TMS から FindMe アカウントにログインします。

（注） この機能は CLI を使用して設定できません。

外部マネージャ設定値の設定

「外部マネージャ（External manager）」ページ（**[システム（System）] > [外部マネージャ（External manager）]**）を使用して、外部管理システムへのExpresswayの接続を設定します。

外部マネージャはCisco TelePresence Management Suite（Cisco TMS）などのリモート システムであり、たとえば、コール試行、接続および切断などExpresswayで発生するイベントをモニタするために、また、Expresswayがアラーム情報を送信できる場所として使用されます。外部マネージャの使用は任意です。

（注） Cisco TMSは「「TANDBERG VCS」」としてExpresswayを識別します。

Expresswayは、Cisco TMSへの接続が失敗した場合もサービスを失うことなく動作し続けます。これは、Expresswayがクラスタ化されている場合にも適用されます。特定のアクションは必要ありません。接続が再確立されると、ExpresswayとCisco TMSは互いへの通信を自動的に再開します。

フィールド	説明	使用方法のヒント
アドレス（Address）およびパス（path）	外部マネージャを使用するには、IPアドレスまたはホスト名と、使用する外部マネージャのパスでExpresswayを設定する必要があります。	Cisco TMSを外部マネージャとして使用する場合は、デフォルト パスの tms/public/external/management/SystemManagementService.asmx を使用します。
[Protocol]	外部マネージャとの通信に*[HTTP]*または*[HTTPS]*のどちらを使用するかを指定します。 デフォルトは*HTTPS*です。	
証明書検証モード（Certificate verification mode）	外部マネージャによって提供される証明書を確認するかどうかを制御します。	確認を有効にした場合は、外部マネージャの証明書の発行者の証明書を、Expresswayの信頼できるCA証明書を含むファイルに追加する必要があります。これは、信頼されたCA証明書リストの管理ページ（**[メンテナンス（Maintenance）] > [セキュリティ（Security）] > [信頼できるCA証明書（Trusted CA certificate）]**）から行います。

専用管理インターフェイス（DMI）の設定

X12.7 から、Expressway は専用管理インターフェイス（DMI）をサポートします。これは、管理関連のアクティビティのために Expressway にアクセスするために 3 番目の LAN ポート（LAN3）を使用する新しいネットワークインターフェイスです。ルーティングインターフェイスを他のトラフィックと共有する代わりに、管理トラフィックはLAN3経由で送信および受信され、他のトラフィックはこのポートを使用しません。

DMI はデフォルトで無効です。

（注） 物理 CE1200 アプライアンスを使用している場合は、物理アプライアンスに提供されている**ポート3a**（「図 2：Cisco Expressway の背面図を参照」）を接続し、「「背面パネルのレイアウト」」の章で説明されているように DMI アドレスを設定します。具体的な手順については、「『*Cisco Expressway CE1200* アプライアンス設置ガイド（*Cisco Expressway CE1200 Appliance Installation Guide*）』」を参照してください。

DMI の概要

DMI の有効化には、次の 2 つの側面があります。

1. DMI機能の有効化：管理トラフィックのLAN3ポートをオンにします。ただし、専用ではなく、LAN1（および、設定している場合はLAN2）も使用できます。Expresswayは、LAN3ポートだけでなく、LAN1/LAN2 上の管理トラフィックも引き続きリッスンします。
2. 管理トラフィック用のインターフェイスを LAN3 のみにする場合は、Expressway で DMI 専用に個々の管理サービスを設定する必要があります。

（注） LAN3 サブネット外に管理サーバがある場合は、現在、これらのトラフィックを LAN3 に送信するにはスタティック IP ルートを設定する必要もあります。

Expressway 管理トラフィックは、サーバベースまたはクライアントベースとして分類できます。

Expressway がサーバである管理トラフィックは、次のとおりです。

- HTTP(S)：Web UI 管理および REST API 用
- ssh：（MRA トンネル用ではなく）CLI 用
- SNMP

Expressway がクライアントである管理トラフィックの例には、次のものがあります。

- Cisco TMS などの外部マネージャへのフィードバックイベント用の HTTP(S)

- NTP
- ディレクトリ（LDAP、Active Directory）
- リモート syslog
- 収集されたシステムメトリック

DMI の設定方法

SSOをの有効化手順

始める前に

DMI インターフェイスの新しい DNS 名は、Expressway サーバ証明書にサブジェクト代替名（SAN）として入力する必要があります。IPアドレスを使用してインターフェイス（または証明書の SAN エントリではない DNS）にアクセスする場合、証明書検証警告が発行され、アクセスがブロックされる場合があります。

⚠

注意 DMI は Expressway 設定へのアクセスを提供するので、適切に保護することが重要です。

手順

ステップ 1 Go to **[システム（System）]** > **[ネットワークインターフェイス（Network Interfaces）]** > **[IP]** に進み、**[専用の管理インターフェイスを使用する（Use Dedicated Management Interface）]** を *[*はい（*Yes*）*]* に設定します。 に設定します。

ステップ 2 [LAN3 - DMI] セクションで、次を実行します。

1. LAN3 ポートの IPv4 アドレスまたは IPv6 アドレスを指定します。
2. IPv4 では、サブネットマスクも指定します。
3. IPv6 の場合は、静的なグローバルアドレスを使用します。リンクローカルまたはステートレスの SLAAC は使用できません。
4. 必要に応じて、ポートの**最大伝送ユニット（MTU）**を設定することで、DMI 経由で送信できるイーサネットパケットの最大サイズを変更します。デフォルト値は 1500 バイトです。

ステップ 3 システムを再起動します。これらの変更を有効にするには、再起動が必要です。

これで、DMIが管理トラフィック用のインターフェイスとしてLAN3でアクティブ化されました。DMIを管理用の唯一のインターフェイスとして使用する場合は、次のタスクに進みます。

（注） Expressway VM の場合、OVF テンプレートに、DMI IP アドレスを定義するカスタマイズオプションがあります。

（オプション）DMI 単独のインターフェイス作成

（オプション）DMI を唯一のインターフェイスにする - サーバ管理トラフィック

Expressway がサーバである場合に、このタスクを使用して、管理トラフィックに DMIを使用します。

注意 これを行う前に、LAN3 で必要なサービスがアクセス可能であることを確認してください。そうしないと、DMIのみへの変更後にこれらのサービスがアクセスできなくなります。回復する唯一の方法は、コンソール（シリアル/VMWare）を使用して DMI をオフにすることであるため、これは管理サービスにとって特に重要です。

1. これは、管理サービス（Web ユーザインターフェイス、REST API、CLI）または SNMP に対して実行できます。DMI 専用に設定するサービスに応じて、次の手順のいずれかまたは両方を実行します。
   - **[システム（System）]** > **[SNMP]** に進み、**[設定（Configuration）]** セクションで、**[専用管理インターフェイスのみを使用する（Use Dedicated Management Interface）]** を *[*はい（*Yes*）*]* に設定します。
   - **[システム（System）]** > **[管理設定（Administration settings）]** に進み、**[サービス（Services）]** セクションで、**[管理インターフェイスのみを使用する（管理用）（Use Dedicated Management Interface only (for administration)）]** を *[*はい（*Yes*）*]* に設定します。
2. 変更を Web ユーザインターフェイスと API に適用するにはシステムを再起動する必要があります。再起動するまでLAN1/LAN2からアクセスできる状態が維持されます。変更は、再起動に関係なく、コマンドラインインターフェイス（SSH）およびSNMP サービスに対して即時に有効になります。

指定された管理サービスに、DMI/LAN3 ポートからのみアクセスできるようになりました。

（注） Expressway では、管理サービスが DMI を唯一のインターフェイスとして使用するように設定されている間は、この DMI を無効にすることはできません。

（オプション）DMI を唯一のインターフェイスにする - サブネット外のクライアント管理トラフィック

Expressway ソフトウェアのバージョンに応じて、Expressway がクライアントとして動作する管理トラフィックでは、ターゲットサーバが DMI/LAN3 ポートと同じサブネット内にある場合にのみ、トラフィックを DMI に送信できます。LAN3 と同じサブネットにサーバを導入できない場合は、オプションで、サービスごとに LAN3 用のスタティック IP ルートを設定することで、Expressway 管理トラフィックに DMI の使用を強制できます。

例

この例では、次のサブネットを含む Expressway を想定しています。

- LAN3 サブネット範囲：a.b.128.0 ～ a.b.191.255
- LAN1 サブネット範囲：x.y.156.0 ～ x.y.159.255

Expressway で NTP を設定するとします。NTP サーバが LAN1 サブネット内にあります。Expressway からの発信 NTP トラフィックと NTP からの着信応答で DMI/LAN3 を使用します。これは、LAN3用のスタティックルートを次の設定で作成することで実現できます（**[システム（System）] > [ネットワーク インターフェイス（Network interfaces）] > [スタティックルート（Static routes）]**）。

- IP アドレス：*x.y.151.0*
- プレフィックス長：*24*
- ゲートウェイ：*172.22.128.1*（LAN3 サブネットのゲートウェイ）
- インターフェイス：*LAN3*

詳細については、スタティック ルートを参照してください。

TMS プロビジョニング拡張サービスの設定

Cisco TMSPE サービスは Cisco TMS でホストされます。これらのサービスは、Expressway の Expressway プロビジョニング サーバがエンドポイント デバイスからのプロビジョニング要求に対応するために使用するユーザ、デバイス、および電話帳のデータを提供します。また、FindMe サービスの FindMe アカウントの設定データも Expressway に提供します。

X8.11 以降、Cisco TMS でホストされるプロビジョニング サービスを有効にするには、Web ユーザ インターフェイスで **[システム（System）] > [管理設定（Administration settings）]** ページを使用するか、デバイス プロビジョニング CLI コマンド（*xconfiguration Administration DeviceProvisoning*）を使用します。これらのサービスは、特別なオプション キーやライセンスがなくても有効にできます。次のデバイスのプロビジョニング サービスを使用できます。

- ユーザ
- FindMe
- 電話帳

- デバイス

新規インストールでは、すべてのサービスがデフォルトで無効になっています。既存のシステムでは、アップグレード後も現在のサービス設定が維持されたままになります。

はじめる前に

プロビジョニングサービスをまだ有効にしていない場合は、**[システム（System）]** > **[管理（Administration）]** に移動して **[プロビジョニングサービス（Provisioning services）]** を *[オン（ON）]* に設定します。**[システム（System）]** > **[TMS プロビジョニング拡張サービス（TMS Provisioning Extension services）]** ページを使用して、Expressway が Cisco TMSPE サービスに接続する方法と使用するサービスを設定します。（サービス自体を設定するには、TMS を使用することをお勧めします。Expressway を使用して Cisco TMSPE サービス設定を変更した場合、それらの変更は **TMS に適用されません**）。

FindMe は、特殊なケースです。プロビジョニング サービスを有効にすると、次の設定警告アラームが表示されます。FindMe のみ を使用し、他のプロビジョニング サービスは使用しない予定である場合、これらのアラームは無視できます。

- 電話帳を正しく動作させるには、デフォルトサブゾーンとその他の関連サブゾーンで認証ポリシーを有効にする必要があります。また、エンドポイントが登録されていない場合は、デフォルトゾーンで認証を有効にする必要もあります（*For phone book requests to work correctly, authentication policy must be enabled on the Default Subzone and any other relevant subzone; authentication must also be enabled on the Default Zone if the endpoints are not registered*）。
- プロビジョニングを正しく動作させるには、デフォルトゾーンと、プロビジョニング要求を受信する関連ゾーンで認証ポリシーを有効にする必要があります（*For provisioning to work correctly, authentication policy must be enabled on the Default Zone and any other relevant zone that receives provisioning requests*）。

設定

次の表に、プロビジョニング サービスに設定可能なオプションを記載します。

表 *13*：プロビジョニングサービスに設定可能なオプション

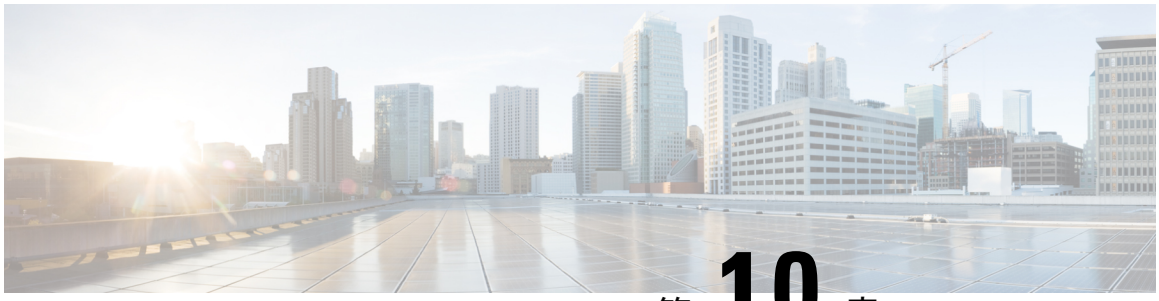
フィールド	説明	使用方法のヒント
デフォルトの接続設定 このセクションでは、Cisco TMSPE サービスにアクセスするためのデフォルトの接続設定値を指定します。各サービスでこれらの設定値を使用することも、サービスごとに固有の設定値を使用することもできます（たとえば、サービスごとに異なる Cisco TMSPE サーバを使用するなど）。		

フィールド	説明	使用方法のヒント
サーバアドレス（Server address）	IP アドレスまたはサービスの完全修飾ドメイン名（FQDN）。	
接続先ポート（Destination port）	Cisco TMSPE サービスのリスニング ポート。	
暗号化	Cisco TMSPE サービスを接続するための暗号化。詳細については、最小限 TLS バージョンと暗号スイートの設定を参照してください。 *[オフ（Off）]*：暗号化なし。 *TLS*：TLS 暗号化を提供します。 デフォルトは *[TLS]* です。	TLS 接続を推奨します。
証明書の確認（Verify Certificate）	Cisco TMSPE サービスによって提示される証明書を Expressway の現在の信頼できる CA リスト、および（存在する場合は）失効リストと照合して確認するかどうかを制御します。 デフォルトは [はい（Yes）] です。	検証が有効にされていない場合： • IIS（Cisco TMSPE サーバ上）が署名付きの証明書とともにインストールされており、SSL 接続を適用するように設定されている必要があります。 • Cisco TMSPE サーバの証明書の発行者の証明書を、Expressway の信頼できる CA 証明書を含むファイルに追加する必要があります。これは、信頼された CA 証明書リストの管理ページ（**[メンテナンス（Maintenance）]** > **[セキュリティ（Security）]** > **[信頼できる CA 証明書（Trusted CA certificate）]**）から行います。
証明書のホスト名の確認（Check certificate hostname）	Cisco TMSPE サービスによって提供される証明書に記載されているホスト名を Expressway で検証するかどうかを制御します。 デフォルトは [はい（Yes）] です。	これは、**[証明書の確認（Verify certificate）]** が *[はい（Yes）]* に設定されている場合に適用されます。 有効な場合、証明書のホスト名（共通名）と指定した**サーバ アドレス**が一致する必要があります。サーバアドレスが IP アドレスの場合、必要なホスト名は DNS ルックアップによって取得されます。

フィールド	説明	使用方法のヒント
基本グループ（Base Group）	この Expressway（または Expressway クラスタ）を Cisco TMSPE サービスで識別するために使用する ID。	TMS 管理者がこの値を提供します。 通常、**デバイス** サービスが使用する**基本グループ** ID は他のサービスが使用する ID とは違うため、明示的に指定する必要があります。
認証ユーザ名（Authentication username）と**パスワード（password）**	Cisco TMSPE サービスを使用して Expressway がそれ自体を認証するために使用するユーザ名と対応するパスワード。	TLS 暗号化が有効になっていない場合、認証パスワードはクリア テキストで送信されます。
サービス固有の設定 Cisco TMSPE サービスのそれぞれ（**ユーザ**、**FindMe**、**電話帳**、および**デバイス**）の接続の詳細を指定できます。		
このサービスに接続（Connect to this service）	Expressway を Cisco TMSPE サービスに接続するかどうかを制御します。 デフォルトは [いいえ（No）] です。	*[*はい（*Yes*）*]* の場合、接続のステータスがフィールドの横に表示されます。表示されるステータスは *[*チェック中（*Checking*）*]*、*[*アクティブ（*Active*）*]*、または *[*失敗（*Failed*）*]* です。（完全なステータス情報を表示するには、TMS Provisioning Extension サービスのステータスをクリックします）。
ポーリング間隔（Polling interval）	Expressway が Cisco TMSPE サービスのアップデートを確認する頻度。デフォルトは次のとおりです。 **[FindMe]**：*2* 分 **[ユーザ（Users）]**：*2* 分 **[電話帳（Phone books）]**：*1* 日 **[デバイス（Device）]** サービスのポーリング間隔は 30 秒に設定されています。これは変更できません。	ページの下部にある **[更新の確認（Check for updates）]** をクリックすると、すべてのサービスの即時更新を要求できます。

フィールド	説明	使用方法のヒント
デフォルトの接続設定を使用する（Use the default connection configuration）	サービスに Cisco TMSPE サービスのデフォルトの接続設定を使用するかどうかを制御します。 デフォルトは [はい（Yes）] です。	[いいえ（No）] を選択すると、追加の接続設定パラメータ一式が表示されます。別の接続詳細を指定して、サービスのデフォルトの接続設定をオーバーライドできます。

Expressway と Cisco TMS 間のデータの即時再同期は、いつでも行うことができます。それには、**「TMS プロビジョニング拡張サービス（TMS Provisioning Extension services）」**ページで **[完全同期の実行（Perform full synchronization）]** をクリックします。これにより、データが削除されて完全に更新されるまでの数秒間、Expressway 上でサービスが停止します。Cisco TMS 内での最近の更新のみを Expressway に適用する場合は、別の方法として、**[更新の確認（Check for updates）]** をクリックしてください。



第 10 章

ファイアウォール トラバーサル

ここでは、ファイアウォールを通過するための Expressway-C と Expressway-E の設定方法について説明します。

ファイアウォール トラバーサルについて

ファイアウォールは、ネットワークに着信する IP トラフィックを制御することを目的としています。ファイアウォールは一般に、未承諾の着信要求をブロックします。つまり、ネットワーク外から発信されたすべてのコールが阻止されます。ただし、信頼できる特定の宛先への発信要求を許可したり、それらの宛先からの応答を許可するようにファイアウォールを設定できます。これが、すべてのファイアウォールのセキュアなトラバーサルを可能にするためにシスコの Expressway テクノロジーが用いている原則です。

Expressway ソリューション

Expressway ソリューションは次のように構成されています。

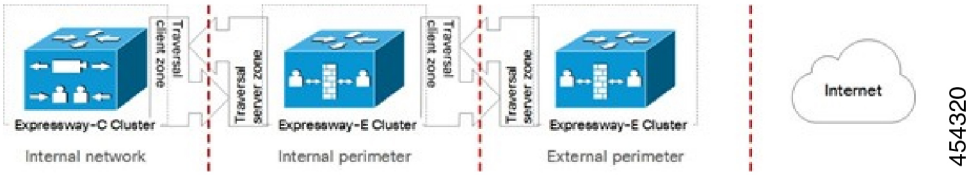
- ファイアウォール トラバーサル サーバとして機能し、パブリック ネットワーク上のファイアウォールの外側または DMZ 内にある Expressway-E。
- ファイアウォール トラバーサル クライアントとして機能し、プライベート ネットワーク内にある Expressway-C またはその他のトラバーサル対応のエンドポイント。

2つのシステムは連携して、2つの間のすべての接続が発信される環境を構築します。つまり、クライアントからサーバに確立されます。また、ファイアウォールを正常に通過することができます。

チェーン接続されたファイアウォール トラバーサル

企業間の Expressway 展開では、ファイアウォール トラバーサル チェーンを設定できます。Expressway-E は、トラバーサル サーバとして機能するだけでなく、別の Expressway-E へのトラバーサル クライアントとしても機能します。

図 *5 : 2* つのチェーン付き *Expressway-Es* の例



たとえば、（図に示すように）2つの Expressway-E をチェーン化した場合、最初の Expressway-E は Expressway-C のトラバーサル サーバです。その最初の Expressway-E は、2番目の Expressway-E のトラバーサル クライアントでもあります。2 番目の Expressway-E は最初の Expressway-E のトラバーサル サーバです。

（注）

- トラバーサル チェーンは、Mobile & Remote Access の展開ではサポートされていません。
- この機能は、バージョン X8.10 の Cisco Expressway シリーズで正式に導入されました。ファイアウォール トラバーサルが導入されたため Cisco TelePresence VCS で可能になっています。

推奨事項と前提条件

（注） Expressway-E と Expressway-C の両方で同じバージョンのソフトウェアを実行することを推奨します。

ファイアウォールが区別できないため、Expressway-E と Expressway-C に共有アドレスを使用しないでください。Expressway-E で IP アドレッシングにスタティック NAT を使用する場合は、Expressway-C 上の NAT が同じトラフィックの IP アドレスの解決を行わないことを確認します。Expressway-E と Expressway-C 間の共有 NAT アドレスはサポートされません。

動作の仕組み

トラバーサル クライアントは、トラバーサル サーバ上の指定ポートへの接続をファイアウォールを介して常に維持します。この接続は、クライアントがパケットを定期的にサーバへ送信することでアライブ状態が保持されます。トラバーサル サーバがトラバーサル クライアント宛の着信コールを受信すると、この既存の接続を使用して着信コール要求をクライアントに送信します。次に、クライアントはコール メディアまたは署名、あるいはその両方に必要なアウトバウンド接続を開始します。

この処理により、ファイアウォールの観点からはすべての接続がファイアウォール内部のトラバーサルクライアントからトラバーサル サーバに開始されることが保証されます。

ファイアウォール トラバーサルを正しく機能させるには、各クライアント システム用に Expressway-E 上で、Expressway-E に接続するクライアント システムごとに 1 つのトラバーサル サーバを設定する必要があります（これには、Expressway-E に直接登録するトラバーサル対応のエンドポイントは含まれません。これらの接続の設定値は別の方法で設定します）。同様に、各 Expressway クライアントには 1 つのトラバーサル クライアント ゾーンが必要です。これは、接続先のサーバごとに設定する必要があります。

クライアントとサーバ ゾーンの各ペアに設定するポートとプロトコルは同じである必要があります。各システムに必要な設定の概要については、トラバーサル クライアントとサーバの設定を参照してください。Expressway-E は特定のポート上のクライアントからの接続をリッスンするため、Expressway-C でトラバーサル クライアント ゾーンを作成する前に、Expressway-E でトラバーサル サーバ ゾーンを作成することを推奨します。

トラバーサルクライアントとトラバーサルサーバは両方とも Cisco Expressway システムである必要があります（どちらにも Cisco VCS は使用できません）。

エンドポイント トラバーサル テクノロジーの要件

ファイアウォールトラバーサルをサポートするための「遠端」（家庭やホテルなど）エンドポイントの要件の概要を以下に示します。

- H.323 の場合、エンドポイントで Assent、または H460.18 および H460.19 をサポートする必要があります。
- SIP の場合、エンドポイントは標準的な SIP のみをサポートする必要があります。
  - 登録メッセージで Expressway に対して「遠端」のファイアウォール ポートを開いたままにし、そのエンドポイントにメッセージを送信します。Expressway はファイアウォールの背後にあるエンドポイントからのメディアを待機してから、その同じポート上のエンドポイントにメディアを返します。つまり、エンドポイントは同じポートでのメディア転送や受信をサポートする必要がありません。
  - また、Expressway は SIP アウトバウンドもサポートしています。これは、登録メッセージ全体を使用するオーバーヘッドなしにファイアウォールを開いたままにする代替方法です。

- SIP エンドポイントと H.323 エンドポイントは Expressway-E に登録できます。または、SIP ポートや H.323 ポートを介して Expressway-E と通信できるようにローカル「DMZ」ファイアウォールで該当するポートを開いている場合、それらのエンドポイントは Expressway-E のみにコールを送信できます。

また、エンドポイントは ICE について を使用して、エンドポイント間のメディア通信に最適な（エンドポイントにとって最適な）パスを検出することもできます。メディアはエンドポイントからエンドポイントへと直接送信したり、エンドポイントから宛先のファイアウォールの外部 IP アドレスを経由して宛先のエンドポイントに送信したり、エンドポイントから TURN サーバを経由して宛先のエンドポイントに送信したりできます。

- Expressway がメディアを通過する必要がない場合（IPv4/IPv6 変換や SIP/H.323 変換の必要がないなど）、Expressway はコールの ICE をサポートします。通常これは、ICE をサポートできる 2 つのエンドポイントが Expressway-E クラスタと直接通信することを意味します。
- Expressway-E は独自の組み込み TURN サービスの設定を使用して ICE 対応のエンドポイントをサポートします。

H.323 ファイアウォール トラバーサル プロトコル

Expressway は、H.323 用の 2 つの異なるファイアウォール トラバーサル プロトコルである Assent と H.460.18/H.460.19 をサポートします。

- Assent はシスコ独自のプロトコルです。
- H.460.18 と H.460.19 は ITU 標準規格で、署名およびメディアのファイアウォール トラバーサルにそれぞれプロトコルを定義します。これらの標準規格は、元の Assent プロトコルに基づいています。

トラバーサル サーバとトラバーサル クライアントが通信するには、同じプロトコルを使用する必要があります。2 つのプロトコルはそれぞれが別の範囲のポートを使用します。

SIP ファイアウォール トラバーサル プロトコル

Expressway は、メディアの SIP ファイアウォール トラバーサル用の Assent プロトコルをサポートします。

クライアントからサーバへと確立された TCP/TLS 接続を通じてシグナリングが通過します。

メディアの逆多重化

Expressway-E は、次のようなシナリオでメディアの逆多重化を使用します。

- Assent を使用するように設定されたトラバーサル ゾーンを通じて Expressway-C が送受信する H.323 または SIP のコール レッグ

- 逆多重化モードでH460.19を使用するように設定されたトラバーサルサーバゾーンを通じて Expressway-C が送受信する H.323 のコールレッグ。
- Expressway-E と Assent または H.460.19 対応のエンドポイント間の H.323 のコールレッグ。

Expressway-E は SIP エンドポイント（Assent または H.460.19 をサポートしないエンドポイント）が直接送受信するコール レッグに対して、または、トラバーサル サーバ ゾーンが逆多重化モードでH.460.19を使用するように設定されていない場合は、非逆多重化メディアを使用します。

Expressway-E のメディア逆多重化ポートは、一般的な範囲の**トラバーサル メディア ポート**から割り当てられます。これは、H.323 か SIP かに関係なく、すべての RTP/RTCP メディアに適用されます。

デフォルトのメディアトラバーサルポートの範囲は 36000 ～ 59999 です。Expressway-C では **[設定（Configuration）] > [ローカルゾーン（Local Zones）] > [トラバーサルサブゾーン（Traversal Subzone）]** で設定できます。大規模 Expressway システムでは、その範囲の最初の 12 ポート（デフォルトでは、36000 ～ 36011）は多重化トラフィック用に常に予約されています。Expressway-E はそれらのポートでリッスンします。大規模システムでは逆多重化リスニング ポートの範囲を明示的に設定することはできません。常にメディア ポート範囲内の最初の 6 ペアが使用されます。小規模/中規模のシステムでは、Expressway-E で多重化 RTP/RTCP トラフィックをリッスンする 2 つのポートを明示的に指定できます（**[設定（Configuration）] > [トラバーサル（Traversal）] > [ポート（Ports）]**）。特定のペアのポートを設定しない場合（**[設定された逆多重化ポート**を使用する（Use configured demultiplexing ports）] が *[いいえ（No）]*）、Expressway-E はメディア トラバーサル ポート範囲内のポートの最初のペアでリッスンします（デフォルトでは 36000 と 36001）。

（注） **[設定済みの逆多重化ポートを使用（Use configured demultiplexing ports）]** 設定を変更するには、システムを再起動して変更を有効にする必要があります。

たとえば、Expressway-C と Expressway-E のペアを通じての企業内から自宅のエンドポイントへの SIP コールでは、発生する逆多重化のみが Expressway-C に対向する Expressway-E ポートで実行されます。

企業のエンドポイント	⟷	Expressway-C		⟷	Expressway-E		⟷	自宅のエンドポイント
		非逆多重化	非逆多重化		逆多重化	非逆多重化		
RTP ポート		36002	36004		36000	36002		
RTCP ポート		36003	36005		36001	36003		

ただし、同じ Expressway-C/Expressway-E を通じた企業内から自宅の Assent 対応の H.323 エンドポイントへの H.323 コールは、Expressway-E の両側で逆多重化を実行します。

企業のエンドポイント	⟷	Expressway-C		⟷	Expressway-E		⟷	自宅のエンドポイント
		非逆多重化	非逆多重化		逆多重化	逆多重化		
RTP ポート		36002	36004		36000	36000		
RTCP ポート		36003	36005		36001	36001		

Expressway-E で高度なネットワーキングを使用している場合も上記と同じポート番号を使用しますが、それらのポート番号は内部 IP アドレスと外部 IP アドレスに割り当てられます。

ファイアウォール トラバーサルの設定の概要

ここでは、Expressway がトラバーサル サーバまたはトラバーサル クライアントとしてどのように機能するかの概要を示します。

ファイアウォール トラバーサル クライアントとしての Expressway

Expressway は、VCS に登録された SIP エンドポイントと H.323 のエンドポイント、およびそれに隣接するシステムの代わりに、ファイアウォール トラバーサル クライアントとして機能します。ファイアウォール トラバーサル クライアントとして機能するには、ファイアウォール トラバーサル サーバとして機能するシステムに関する情報を使用して Expressway を設定する必要があります。

それには、Expressway クライアントのトラバーサルクライアント ゾーン（**[設定（Configuration）] > [ゾーン（Zones）] > [ゾーン（Zones）]**）を追加し、トラバーサルサーバの詳細を使用してそのゾーンを設定します。詳細については、トラバーサル クライアント ゾーンの設定を参照してください。複数のトラバーサル サーバに接続する場合は、複数のトラバーサル クライアント ゾーンを作成できます。

Expressway-C または Expressway-E？

- 通常、ファイアウォールトラバーサルクライアントとして Expressway-C を使用します。ただし、Expressway-E でもこの役割を果たします。
- Expressway クライアントが使用するファイアウォール トラバーサル サーバは Expressway-E でなければなりません。

ファイアウォール トラバーサル サーバとしての Expressway

Expressway-E には、Expressway-C のすべての機能（ファイアウォール トラバーサル クライアントとしての機能を含む）が備わっています。ただし、その主要機能は、他のシスコのシステム用のファイアウォール トラバーサル サーバおよびそれに直接登録されたトラバーサル対応のエンドポイントとして機能できることです。また、TURN リレー サービスも ICE 対応のエンドポイントに提供します。

トラバーサル サーバ ゾーンの設定

シスコのシステムのファイアウォールトラバーサルサーバとして機能する Expressway-E の場合は、Expressway-E でトラバーサルゾーンを作成し（**[設定（Configuration）]** > **[ゾーン（Zones）]** > **[ゾーン（Zones）]**）、トラバーサルクライアントの詳細を使用してそのゾーンを設定します。詳細については、トラバーサル サーバ ゾーンの設定を参照してください。

トラバーサル クライアントであるすべてのシステムに個別のトラバーサル サーバ ゾーンを作成する必要があります。

その他のトラバーサル サーバ機能の設定

- Expressway-E をトラバーサル対応のエンドポイント（Cisco MXP エンドポイントや、ITU H.460.18 および H.460.19 標準規格をサポートするその他のエンドポイントなど）のファイアウォール トラバーサル サーバとして機能させる場合、追加の設定は必要ありません。詳細については、Expressway-E とトラバーサル エンドポイントとの通信の設定を参照してください。
- TURN リレーサービスを有効にし、ICE に関する詳細な情報を取得するには、ICE および TURN サービスについてを参照してください。
- Expressway-E が使用するデフォルトのポートを設定するには、ファイアウォール トラバーサル用のポートの設定を参照してください。

ファイアウォール トラバーサルと高度なネットワーキング

高度なネットワーキングのオプション キーにより、Expressway-E の LAN 2 インターフェイスが有効になります（このオプションは Expressway-C では使用できません）。LAN 2 インターフェイスは、2 つの個別のネットワーク（内部 DMZ と 外部 DMZ）から構成される DMZ 内に Expressway-E があり、この 2 つのネットワーク間の直接通信を阻止するようにネットワークが構成されている場合に使用されます。

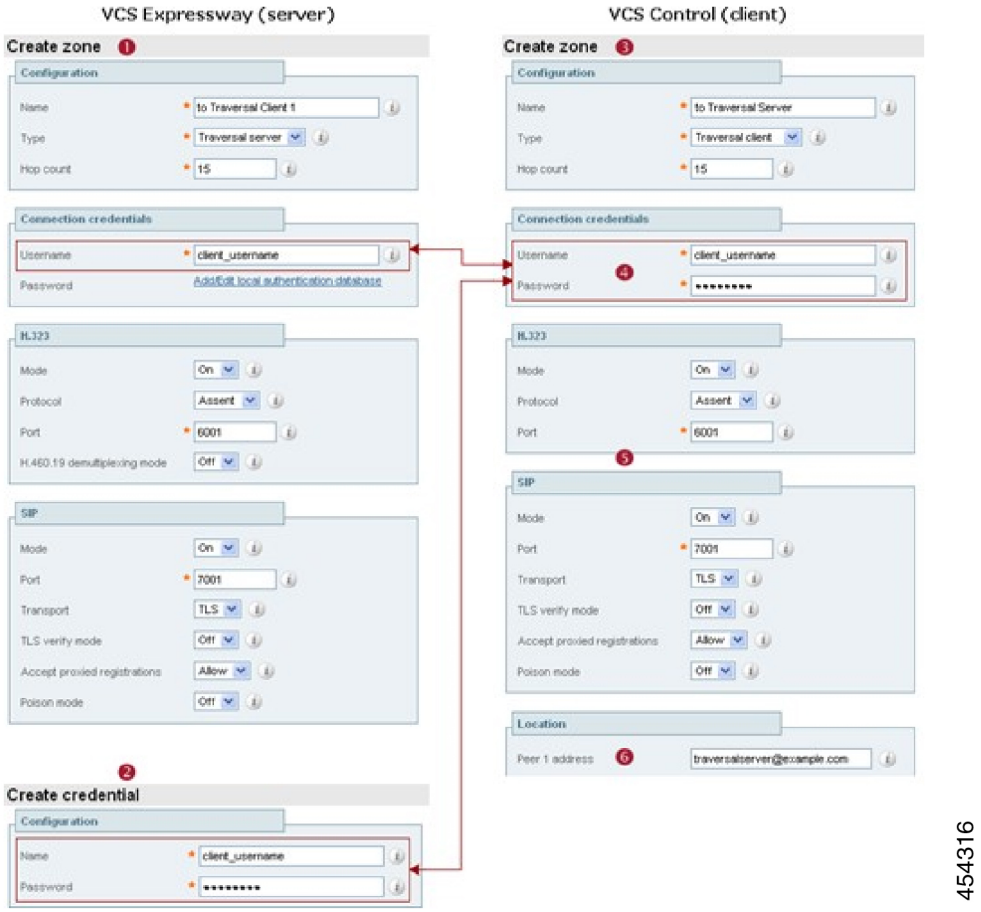
LAN 2 インターフェイスを有効にすると、2 つの個別の IP アドレス（DMZ 内のそれぞれのネットワークに 1 つずつ）を使用して Expressway を設定できます。そうすることで、Expressway は 2 つのネットワーク間でプロキシ サーバとして機能し、DMZ を構成する内部と外部のファイアウォール間でコールを渡すことができます。

高度なネットワーキングが有効になっていると、Expressway 上で設定された、ファイアウォール トラバーサルに関係するポートなどの全ポートが両方の IP アドレスに適用されます。IP アドレスごとにポートを個別に設定することはできません。

トラバーサル クライアントとサーバの設定

トラバーサル クライアントとサーバを設定する基本的な手順は、次のとおりです。

ステップ	説明
1	Expressway-E でトラバーサル サーバ ゾーンを作成します（これは、Expressway-C からの着信接続を表します）。**[ユーザ名（Username）]** フィールドに、Expressway-C の認証ユーザ名を入力します。
2	Expressway-E で、Expressway-C の認証ユーザ名とパスワードをクレデンシャルとしてローカル認証データベースに追加します。
3	Expressway-C でトラバーサル クライアント ゾーンを作成します（これは、Expressway-E への接続を表します）。
4	Expressway-E で指定したものと同じ認証用の**ユーザ名**と**パスワード**を入力します。
5	H.323 と SIP プロトコルのセクションのすべてのモードとポートを Expressway-E のトラバーサル サーバ ゾーンとまったく同じように設定します。
6	Expressway-E の IP アドレスまたは FQDN を **[ピア 1 アドレス（Peer 1 address）]** フィールドに入力します。



ファイアウォール トラバーサル用のポートの設定

（注） 具体的なポート情報は別のドキュメントに記載されています。Cisco Expressway シリーズ設定ガイドのページに用意されている、ご使用のバージョンに対応する『*Cisco Expressway IP Port Usage Configuration Guide*』を参照してください。

ポートはファイアウォール トラバーサル設定で重要な役割を果たします。接続が許可されるようにするには、正しいポートを Expressway-E、トラバーサル クライアントおよびファイアウォール上に設定する必要があります。

ポートは最初に Expressway-E 管理者が Expressway-E に設定します。次に、ファイアウォール管理者とトラバーサル クライアント管理者にそれらのポートが通知されます。管理者はサーバ上の特定のポートに接続するようにシステムを設定する必要があります。トラバーサル クライアント上で必要な唯一のポート設定は、発信接続に使用するポートの範囲です。ファイアウォー

ル管理者は、必要な場合にこれらのポートからの発信接続を許可するようにファイアウォールを設定できるよう、この情報を認識しておく必要があります。

ポートの使用ページ（**[メンテナンス（Maintenance）] > [ツール（Tools）] > [ポートの使用方法（Port usage）]**）に Expressway でインバウンドとアウトバウンドの両方で使用されるすべての IP ポートを示します。ファイアウォールを適切に設定できるようにファイアウォール管理者に提供することができます。

高度なネットワーキングが有効になっていると、Expressway 上で設定された、ファイアウォール トラバーサルに関係するポートなどの全ポートが両方の IP アドレスに適用されます。IP アドレスごとにポートを個別に設定することはできません。

Expressway ソリューションは次のように機能します。

1. 各トラバーサル クライアントは Expressway-E の一意のポートへファイアウォールを介して接続します。
2. サーバは、接続を受けるポートと、クライアントが提供する認証クレデンシャルで各クライアントを識別します。
3. 接続が確立されるとクライアントはプローブを Expressway-E に定期的に送信し、接続を有効に維持します。
4. Expressway-E がクライアント宛の着信コールを受信すると、この最初の接続を使用して着信コール要求をクライアントに送信します。
5. 次にクライアントが、1 つ以上のアウトバウンド接続を開始します。これらの接続に使用される宛先ポートは、シグナリングやメディアごとに異なり、使用されているプロトコルによっても違います（詳細については以降の項を参照してください）。

ファイアウォールの設定

Expressway のファイアウォール トラバーサルを正しく機能させるには、ファイアウォールを次のように設定する必要があります。

- クライアントから Expressway-E が使用するポートへの最初の発信トラフィックを許可する
- Expressway-E 上のこれらのポートから発信元のクライアントへのリターン トラフィックを許可する

（注） ファイアウォール上の H.323 および SIP プロトコルのサポートをすべてオフにすることをお勧めします。Expressway ソリューションでは不要なため、操作に支障をきたす可能性があります。

トラバーサル サーバ ポートの設定

Expressway-E にはファイアウォール トラバーサルに使用する特定のリスニング ポートがあります。これらのポートへの接続を許可するように、ファイアウォールにルールを設定する必要があります。ほとんどの場合はデフォルトのポートを使用します。ただし、必要に応じて**「ポート（Ports）」**ページ（**[設定（Configuration）] > [トラバーサル（Traversal）] > [ポート（Ports）]**）に移動して、これらのポートを変更することができます。

シグナリング用に設定可能なポートは次のとおりです。

- **H.323 Assent コール シグナリング ポート**
- **H.323 H.460.18 コール シグナリング ポート**

RTP と RTCP のメディア逆多重化ポート

ポート設定のオプションは、ハードウェア アプライアンスおよび仮想マシンのオプションによって異なります。

- **小規模/中規模システム**：1 ペアの RTP と RTCP メディア逆多重化ポートを使用します。これらは、明示的に指定するか、トラバーサル メディア ポートの一般的な範囲の最初から割り当てることができます。
- **大規模システム**：6 つのペアの RTP と RTCP メディア逆多重化ポートを使用します。これらは常に、トラバーサル メディア ポート範囲の最初から割り当てられます。

トラバーサル クライアントからの接続用のポートの設定

トラバーサル クライアントからの最初の接続に使用する H.323 ポートと SIP ポートを各トラバーサル サーバ ゾーンで指定します。トラバーサル サーバ ゾーンを Expressway-E に新たに設定するたびに、これらの接続にデフォルトのポート番号が割り当てられます。

- H.323 ポートは UDP/6001 から始まり、新たなトラバーサル サーバ ゾーンごとに 1 ずつ増えていきます。
- SHIP ポートは TCP/7001 から始まり、新たなトラバーサル サーバ ゾーンごとに 1 ずつ増えていきます。

これらのデフォルトのポートは必要に応じて変更できますが、各トラバーサル サーバ ゾーンで一意のポートであることを確認する必要があります。H.323 ポートと SIP ポートを Expressway-E に設定した後、対応するトラバーサル クライアントに一致するポートを設定する必要があります。

（注）

- MXP エンドポイントからの最初の接続に使用するデフォルトのポートは、標準 RAS メッセージに使用されるポートと同じ（UDP/1719）です。Expressway-E でこのポートを変更できますが、ほとんどのエンドポイントが UDP/1719 以外のポートへの接続をサポートしません。したがって、これはデフォルトのままにしておくことを推奨します。
- Expressway-E のトラバーサル サーバ ゾーンのそれぞれに設定された一意の SIP ポートと H.323 ポートそれぞれへのファイアウォールを通じたアウトバウンド接続を許可する必要があります。

コールシグナリングポートは **[設定（Configuration）]** > **[トラバーサル（Traversal）]** > **[ポート（Ports）]** で設定します。トラバーサルメディア ポートの範囲は **[設定（Configuration）]** > **[ローカル ゾーン（Local Zone）]** > **[サブゾーン（Subzone）]** で設定します。

Expressway-E に直接登録されているエンドポイントがない場合、Expressway-E がクラスタに含まれていなければ、UDP/1719 は必要ありません。したがって、Expressway-C と Expressway-E 間のファイアウォールを介してこのポートへのアウトバウンド接続を許可する必要はありません。

TURN ポートの設定

Expressway-E を ICE 対応の SIP エンドポイントで使用できる ICE および TURN サービスについて（Traversal Using Relays around NAT）を提供することができます。

これらのサービスで使用するポートは **[設定（Configuration）]** > **[トラバーサル（Traversal）]** > **[TURN]** で設定できます。

各 SIP エンドポイントの ICE クライアントは、DNS 内の SRV レコードを使用するか、直接設定のいずれかによって、これらのポートを検出できる必要があります。

パブリック インターネットへ接続するポートの設定

Expressway-E がパブリック インターネット上のエンドポイントに接続を試行する場合は、その接続が行われるエンドポイントのポートを正確に知ることはできません。使用するポートはエンドポイントによって決定され、パブリック インターネット上のエンドポイント上のサーバが見つかって初めて、Expressway-E に通知されるためです。これによって、Expressway-E が DMZ 内にある場合（Expressway-E とパブリック インターネット間にファイアウォールがある場合）は、そのエンドポイントのポートへの接続が許可されるルールを前もって指定することができないために問題が発生する場合があります。

ただし、ファイアウォール管理者がこれらのポートを介した接続を許可できるように、パブリック インターネット上のエンドポイントに送受信するコールに使用する Expressway-E 上のポートは指定できます。

Cisco Expressway シリーズ設定ガイドのページに用意されている、ご使用のバージョンに対応する『*Cisco Expressway IP Port Usage Configuration Guide*』を参照してください。

ファイアウォール トラバーサルと認証

Expressway-E では、認証されたクライアント システムのみがトラバーサル サーバとして使用できます。

最初の接続要求をトラバーサル クライアントから受け取ると、Expressway-E は、認証クレデンシャルを提供してそれ自体を認証するようクライアントに要求します。次に Expressway-E はクライアントのクレデンシャルを独自の認証データベースで検索します。一致が見つかると、Expressway-E はクライアントからの要求を受け入れます。

認証に使用する設定は、トラバーサル クライアントのタイプによって次のように異なります。

トラバーサル クライアント	Expressway-E トラバーサル サーバ
Expressway-C（または Expressway-E） Expressway クライアントは自身の**ユーザ名**と**パスワード**を提供します。これらは、**[接続認証情報（Connection credentials）]** セクションの **[設定（Configuration）]** > **[ゾーン（Zones）]** > **[ゾーン（Zones）]** > **[ゾーンの編集（Edit zone）]** を使用してトラバーサルクライアントゾーンで設定します。	Expressway クライアントのトラバーサル サーバ ゾーンは、クライアントの認証**ユーザ名**を使用して設定する必要があります。これは、**[接続クレデンシャル（Connection credentials）]** セクションの **[設定（Configuration）]** > **[ゾーン（Zones）]** > **[ゾーン（Zones）]** > **[ゾーンの編集（Edit zone）]** を使用して Expressway-E で設定します。 また、Expressway-E の認証データベースに対応するクライアント ユーザ名とパスワードでのエントリが必要です。
エンドポイント エンドポイント クライアントはその**認証 ID** と**認証パスワード**を提供します。	Expressway-E の認証データベースに対応するクライアント ユーザ名とパスワードでのエントリが必要です。

（注） Expressway-E がエンドポイントのデバイス認証を使用していないとしても、すべての Expressway トラバーサル クライアントを Expressway-E で認証する必要があります。

認証および NTP

H.323 をサポートするすべての Expressway のトラバーサル クライアントは Expressway-E で認証する必要があります。認証プロセスは、タイムスタンプを使用し、各システムが正確なシステム時刻を使用している必要があります。Expressway のシステム時刻はリモート NTP サーバによって提供されます。したがって、ファイアウォール トラバーサルが機能するには、関係するすべてのシステムを NTP サーバの設定の詳細情報を使用して設定する必要があります。

Expressway-E とトラバーサル エンドポイントとの通信の設定

トラバーサル対応の H.323 エンドポイントは Expressway-E に直接登録し、それをファイアウォール トラバーサルとして使用することができます。

「ローカルで登録済みのエンドポイント（Locally registered endpoints）」ページ（**[設定（Configuration）] > [トラバーサル（Traversal）] > [ローカルで登録済みのエンドポイント（Locally registered endpoints）]**）を使用して、Expressway-E とトラバーサル対応のエンドポイント間の通信方法を設定できます。

次のオプションを使用できます。

フィールド	説明
H.323 Assent モード（H.323 Assent mode）	ファイアウォール トラバーサルに Assent モードを使用する H.323 コールを許可するかどうかを決定します。
H.460.18 モード（H.460.18 mode）	ファイアウォール トラバーサルに H.460.18/19 モードを使用する H.323 コールを許可するかどうかを決定します。
H.460.19 逆多重化モード（H.460.19 demux mode）	Expressway-E がローカルで登録済みのエンドポイントからのコールに対して逆多重化モードで動作するかどうかを決定します。 *[オン（On）]*：すべてのコールにメディア逆多重化ポートを使用します。 *[オフ（Off）]*：各コールが個別のポート ペアをメディアに使用します。
H.323 優先（H.323 preference）	エンドポイントが Assent と H.460.18 の両方をサポートしている場合に Expressway-E が使用するプロトコルを指定します。
UDP プローブの再試行間隔（UDP probe retry Interval）	ローカルで登録済みのエンドポイントが UDP プローブを Expressway-E に送信する頻度（秒単位）です。
UDP プローブの再試行回数（UDP probe retry count）	ローカルで登録済みのエンドポイントが Expressway-E への UDP プローブ送信を試行する回数です。
UDP プローブのキープアライブ間隔（UDP probe keep alive interval）	コールが確立した後に、ファイアウォールの NAT バインドを有効にしておくために、ローカルで登録済みのエンドポイントが UDP プローブを Expressway-E に送信する間隔（秒単位）です。
TCP プローブの再試行間隔（UDP probe retry Interval）	ローカルで登録済みのエンドポイントが TCP プローブを Expressway-E に送信する頻度（秒単位）です。

フィールド	説明
TCP プローブの再試行回数（UDP probe retry count）	ローカルで登録済みのエンドポイントが Expressway-E への TCP プローブ送信を試行する回数です。
TCP プローブのキープアライブ間隔（UDP probe keep alive interval）	コールが確立した後に、ファイアウォールの NAT バインドを有効にしておくために、ローカルで登録済みのエンドポイントが TCP プローブを Expressway-E に送信する間隔（秒単位）です。

ICE および TURN サービスについて

ICE について

ICE（Interactive Connectivity Establishment）は SIP クライアントの NAT トラバーサル用のメカニズムを提供します。ICE はプロトコルではなく、TURN（Traversal Using Relays around NAT）や STUN（Session Traversal Utilities for NAT）など、数多くの異なるテクノロジをまとめるフレームワークです。

これにより、NAT デバイスの背後に存在するエンドポイント（クライアント）がメディアを通過できるパスを検出し、それらのパスのそれぞれを経由してピアツーピア接続を確認してから最適なメディア接続パスを選択することができます。通常、使用できるパスは、NAT デバイスに設定されたインバウンド接続とアウトバウンド接続の制約事項によって異なります。このような動作については、RFC 4787 を参照してください。

ICE の使用例として、インターネットを経由した 2 人の在宅ワーカーの通信があります。2 つのエンドポイントが ICE を経由して通信できる場合、Expressway-E は（NAT デバイスがどのように設定されているかに応じて）シグナリングのみを取得する必要があり、メディアは取得しない（そのため、これは非トラバーサル コールとなる）場合があります。送信元の ICE クライアントが非 ICE クライアントをコールしようとすると、Expressway もメディアを取得するためにメディアのラッチングによる NAT トラバーサルが必要な従来の SIP コールにコールの設定プロセスが戻ります。

ICE の詳細については、RFC 5245 を参照してください。

MRA 展開での ICE パススルー

X12.5 以降、Interactive Connectivity Establishment（ICE）パススルーがサポートされるようになっています。ICE パススルーにより、MRA 対応のエンドポイントが WAN および Cisco Expressway シリーズをバイパスして、エンドポイント間で直接メディアを渡すことができます。

ICE パススルーの設定の詳細と必要なバージョンについては、Expressway 設定ガイドのページに用意されている『*Mobile and Remote Access Through Cisco Expressway guide*』を参照してください。

TURN について

TURN サービスは、SIP クライアントが NAT デバイスの背後から UDP または TCP を介して通信できるようにする STUN ネットワーク プロトコルのリレー拡張機能です。

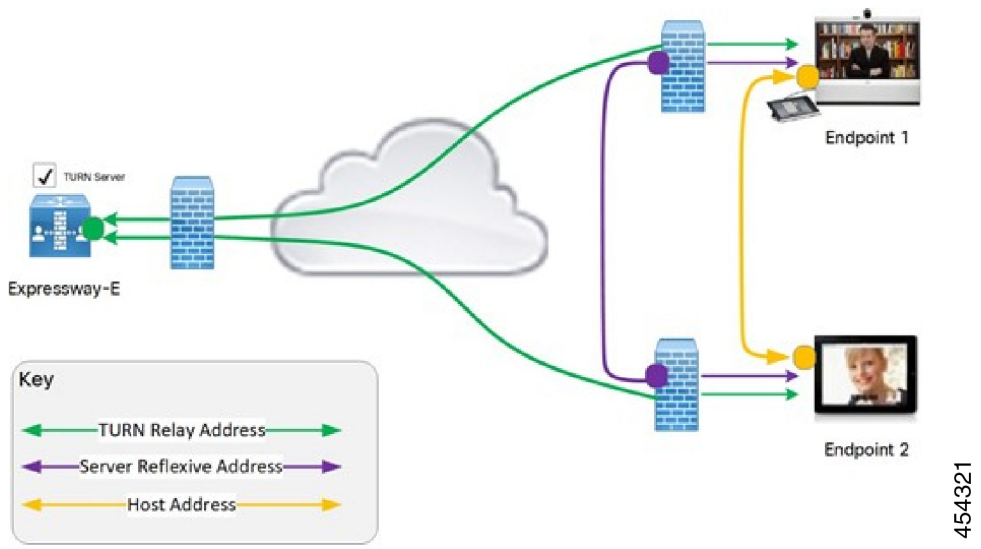
TURN の詳細については RFC 5766 を、基本の STUN プロトコルについては RFC 5389 を参照してください。

各 ICE クライアントはコールのメディア コンポーネントにリレーを割り当てるよう TURN サーバに要求します。各クライアント間のメディア ストリームの各コンポーネントに 1 つのリレーが必要です。

リレーが割り当てられると、各 ICE クライアントには、メディアの送受信が可能になる次の 3 つの潜在的な接続パス（アドレス）が備わります。

- NAT デバイスの背後にある（そのため、NAT の他方にあるエンドポイントからは到達できない）ホスト アドレス
- NAT デバイス上の公開形式でアクセス可能なアドレス
- TURN サーバ上のリレー アドレス

図 *6 : ICE* メディアの接続パス



次に、エンドポイントは ICE を通じて接続確認を実行して通信を行うかどうかを決定します。NAT デバイスがどのように設定されているかによっては、エンドポイントが NAT デバイス上の公開されているアドレス間で通信できることがありますが、そうでない場合は TURN サーバを介してメディアをリレーする必要があります。両方のエンドポイントが同じ NAT デバイスの背後にある場合は、内部ホスト アドレスを使用して、その 2 つのエンドポイント間にメディアを直接送信できます。

メディア ルートを選択した後は、選択した接続パスに TURN サーバを経由するルートが含まれていなければ、TURN リレーの割り当ては解放されます。エンドポイントが選択した最終的なメディア通信パスに関係なく、シグナリングは常に Expressway 経由になります。

（注） TURN サーバは、一方または両方が企業の内部ファイアウォール内にある場合でも、任意の 2 つの ICE クライアント間でメディアを中継できます。

機能と制限事項

- X12.6.1 以降では、セキュリティ強化により、Expressway-E TURN サーバは汎用 STUN サーバとして動作しなくなり、認証されていない STUN バインディング要求を受け入れません。その結果、以下のシナリオが考えられます。
  - シナリオ A：（『*Cisco Expressway* および *Microsoft* インフラストラクチャ導入ガイド』*[英語]*で説明されているように）Microsoft との相互運用性の目的で TURN クライアントとして B2BUA を使用する場合、B2BUA は、サーバが動作しているかどうかを確認するために STUN バインディング要求を TURN サーバに送信することはありません。つまり、Expressway X12.6.1 以降では、到達可能でない TURN サーバの使用を B2BUA が試みた結果、**コールが失敗する可能性があります**。
  - シナリオ B：導入された CMS のバージョンによっては、CMS WebRTC ソリューションが Expressway-E 上の TURN サーバに対して STUN バインド要求を使用する場合があり、これにより障害が発生します。Meeting Server WebRTC を使用する場合は、Expressway バージョン X12.6.1 以降のソフトウェアをインストールする前に、CMS のバージョンと互換性があることを確認してください。バグ ID CSCvv01243 を参照してください。（Expressway-E TURN サーバの設定の詳細については、『Cisco Meeting Server 版 Cisco Expressway Web プロキシ導入ガイド』を参照してください）。
- ハードウェア アプライアンスおよび仮想マシンのオプションまたはハードウェア アプライアンスおよび仮想マシンのオプションシステムでは、最大 1800 のリレー割り当てがサポートされます。通常、最大同時コール数の制限をサポートするにはこの数で十分ですが、ネットワーク トポロジと、コールに使用するメディア ストリーム コンポーネントの数によってはそうでない場合もあります。たとえば、コールの中にはデュオ ビデオを使用するものもあれば、音声のみを使用するものもあります。
- ハードウェア アプライアンスおよび仮想マシンのオプションシステムでは、最大 6000 のリレーがサポートされます。ポート多重化が有効になっている場合は、1 つの外部ポートでリレー容量のすべてを使用できます。ポート範囲が設定されている場合は、6 つの外部ポートにリレー容量が分配されます。ポート間で分配される場合、各ポートで処理できるリレー数は 1000 に制限されます。

  この制限は厳密に適用されるわけではありません。したがって、範囲内のポート アドレスごとに、6 つの A/AAAA エントリに同じアドレスを指定した DNS SRV レコードを作成することをお勧めします。このレコードを作成した上で、クライアントに Expressway-E TURN サーバの SRV レコードを設定します。TURN 多重化が有効にされている場合は、TURN 要求をリッスンする外部ポートにだけ SRV レコードを作成することをお勧めします。

- ハードウェア アプライアンスおよび仮想マシンのオプションシステムでは、ポートの範囲（デフォルトでは 3478 ～ 3483）で TURN 要求をリッスンする TURN サーバを設定できます。X8.11 以降、TURN 多重化が有効にされていると、Expressway-E はポート範囲の最初のポート（通常は UDP 3478）ですべての TURN 要求を受け入れます。Expressway は内部でこれらの要求をポート範囲に逆多重化します。TURN クライアントは設定済みの単一のポートで要求を送信する必要がありますが、大規模 Expressway-E TURN サーバの完全な容量を利用できます。

- X8.11 以降、Expressway-E は TCP ポート 443 で TURN 要求と Cisco Meeting Server 要求の両方をリッスンできます。Expressway-E は、ポート 443 経由で接続要求を受信すると、要求のタイプに応じて TURN サーバまたは Meeting Server Web プロキシに要求を転送します。したがって、外部ユーザは TURN サービスを使用することで、ファイアウォール ポリシーで制限された環境からでも Meeting Server スペースに参加できます。

  Web 管理者ポートがポート 443（**システム** > **管理設定**）でリッスンするように設定されている場合 、X12.7 以前の Expressway バージョンでは、443 から他の有効なポートに変更する必要があります。X12.7 から、Expressway が専用管理インターフェイスを唯一の管理インターフェイスとして使用するように設定されている場合は、これを行う必要があります。つまり、[**システム** > **管理設定**] ページで、**[専用管理インターフェイスのみを使用]** が *[はい]* に設定されます。

- ハードウェア アプライアンスおよび仮想マシンのオプションシステムでは、TCP 443 TURN サービスが有効で、TURN 多重機能も有効な場合 、6000 TCP TURN リレーがサポートされます。

- クラスタ化された Expressway：要求された TURN サーバのリレーが完全に割り当てられている場合、サーバは要求側のクライアントに対してクラスタ内の代替サーバの詳細情報で応答します（現在、使用可能なリソースが最大の TURN サーバ）。

- Expressway の TURN サービスは、単一のネットワーク インターフェイスまたはデュアル ネットワーク インターフェイスで（高度なネットワーキング オプションを介して）サポートされます。デュアル ネットワーク インターフェイスでは、TURN サーバは両方のインターフェイスでリッスンしますが、リレーは Expressway の外部に対向する LAN インターフェイスにのみ割り当てられます。

- Microsoft ICE（各種の標準規格に準拠していません）は Expressway-E の TURN サーバではサポートされていません。そのため、Microsoft Edge Server を通じて登録された Expressway と Microsoft クライアント間の通信を有効にするには、Microsoft の相互運用性についてを使用する必要があります。

- TURN サーバは帯域幅要求をサポートしません。トラバーサル ゾーンの帯域幅制限は適用されません。

- Expressway-E の TURN サーバは TCP と UDP で TURN メディアをサポートします。サポートされているプロトコルの設定は、CLI コマンド **xConfiguration Traversal Server TURN ProtocolMode** を通じてのみ行えます。

- Expressway-E の TURN サーバは、TCP で UDP リレーをサポートします。

内部インターフェイスで送信される STUN パケット

Expressway は、外部 LAN インターフェイスを介して受信した STUN パケットを、常にパケット送信元アドレスとして外部 LAN IP アドレスを使用して送信します。通常、パケットは外部インターフェイスから送信されます。そのため、IP アドレスは通常は一致します。ただし、次の場合、Expressway は内部 LAN インターフェイスから STUN パケットを 送信します。

- TURN クライアントがリレーセッションを使用して、Expressway-E の内部 IP と同じサブネット内のデバイスにメッセージを送信する場合、または
- TURN クライアントがリレーセッションを使用して、Expressway-E の内部ゲートウェイ IP を使用するスタティックルートと一致するサブネット内のデバイスにメッセージを送信する場合。

この動作により、IP アドレスに不一致があるように見える場合がありますが、実際にはシステムは設計どおりに機能しています。

TURN サービスの設定

TURN リレーサービスは、Expressway-E でのみ使用できます。(X8.11 以降は、TURN サービスの使用で TURN リレーオプションキーは不要です)。

「TURN」ページ（**[設定（Configuration）] > [トラバーサル（Traversal）] > [TURN]**）を使用して、Expressway-E の TURN 設定を構成します。Expressway-E を委任クレデンシャル チェック用に設定する場合は、**認証レルム**を介して、TURN サーバ 要求のクレデンシャル チェックが委任されるトラバーサル ゾーンも指定できます。

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
TURN サービス（TURN services）	Expressway が TURN サービスをトラバーサル クライアントに提供するかどうかを決定します。	**[TURNサービス（TURN services）]** がすでに *[オン（On）]* に設定されているときに、他の TURN 設定を変更する必要がある場合は、次の手順に従います。 1. **[TURNサービス（Turn services）]** を *[オフ（Off）]* に変更して **[保存（Save）]** します。 2. 必要に応じて TURN 設定を変更します。 3. **[TURNサービス（Turn services）]** を *[オン（On）]* に変更して **[保存（Save）]** します。 これは、他の TURN 設定を変更した場合、**TURN サービス**が再起動されるまでは、その変更が適用されないためです。
TCP 443 TURN サービス	TURN サーバが TCP ポート 443 で TURN クライアントからの TCP 要求をリッスンする必要があるかどうかを指定します。次のオプションがあります。 • *[オン（On）]*：TURN サーバは TCP ポート 443 で TURN クライアントからの TCP 要求をリッスンし、設定済みのポートで UDP 要求をリッスンします。 • *[オフ（Off）]*：TURN サーバは TCP ポート 443 で TURN クライアントをリッスンしません。ただし、この設定は TURN 要求をリッスンするように設定されたポートには影響しません。	この機能を有効にする前に、次のことを確認してください。 • **[TURNサービス（TURN services）]** が *[オン（On）]* に設定されていること。 • X12.7 以前は、Web 管理者ポートがポート 443 でリッスンするように設定されている場合（**[システム（System）] > [管理設定（Administration Settings）]**）、ポート 443 を他の有効なポートに変更する必要があります。X12.7 から、Expressway が専用管理インターフェイスを唯一の管理インターフェイスとして使用するように設定されている場合は、これを行う必要があります。つまり、[**システム > 管理設定**] ページで、**[専用管理インターフェイスのみを使用]** が *[はい]* に設定されます。

フィールド	説明	使用方法のヒント
TURN ポート多重化（TURN port multiplexing）	大規模システムで、Expressway TURN サーバの全容量を単一のリスニングポート上で有効にして、内部で要求をポート範囲に逆多重化します。 （注） このオプションは大規模システムでのみ使用できます。 オプションは次のいずれかです。 • *[オン（On）]*： • Expressway は、ポート範囲ではなく、単一の設定可能な外部ポートでリッスンします。 • **[TCP443TURN サービス（TCP 443 TURN services）]** が *[オン（On）]* に設定されている場合、設定可能な外部ポートのみが UDP TURN 要求を多重化します。 （注） **[TCP 443 TURN サービス（TCP 443 TURN services）]** が *[オン（On）]* に設定されている場合、技術的な制約により、外部ポートは TCP TURN 要求を多重化しません。 • *[オフ（Off）]*：TURN サーバは、ポート範囲で TCP 要求と UDP 要求をリッスンします。	この機能を有効にする前に、**[TURN サービス（TURN services）]** が *[オン（On）]* に設定されていることを確認してください。

フィールド	説明	使用方法のヒント
TURN要求ポート（TURN requests port）	TURN要求のリスニング ポート。デフォルト ポートは 3478 です。	大規模システムでは、このオプションは **[TURNポート多重化（TURN port multiplexing）]** が *[オン（On）]* に設定されている場合にのみ使用できます。 エンドポイントで TURN サービスを検出するには、**_turn._udp**. と **_turn._tcp** の DNS SRV レコードを作成する必要があります（必要に応じて、単一のポートでもポートの範囲でも可）。
TURN要求のポート範囲の開始（TURN requests port range start）	**[TURNポート多重化（TURN port multiplexing）]** が *[オフ（Off）]* の場合、このポートは大規模システム上の設定可能なポート範囲の最初のポートを表します。 デフォルトのポート範囲の開始は 3478 です。	このオプションは、大規模システムで **[TURNポート多重化（TURN port multiplexing）]** が *[オフ（Off）]* に設定されている場合にのみ使用できます。
TURN要求のポート範囲の終了（TURN requests port range end）	**[TURNポート多重化（TURN port multiplexing）]** が *[オフ（Off）]* の場合、このポートは大規模システム上の設定可能なポート範囲の上限ポートを表します。 デフォルトのポート範囲の終了は 3483 です。	このオプションは、大規模システムで **[TURNポート多重化（TURN port multiplexing）]** が *[オフ（Off）]* に設定されている場合にのみ使用できます。

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）	TURN サーバ要求のクレデンシャル チェックをトラバーサル ゾーンを介して別の Expressway に委任できるかどうかを制御します。関連付けられている**認証レルム**によって、どのトラバーサル ゾーンが使用されるかが決まります。 *[オフ（Off）]*：認証チャレンジを実行する Expressway 上の該当するクレデンシャル 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。	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。
認証レルム（Authentication realm）	認証チャレンジでサーバが送信するレルム。	クライアントのクレデンシャルがローカル認証データベースに保存されていることを確認します。
メディア ポート範囲の始端（Media port range start）	TURN リレーの割り当てに使用するポート範囲の下限ポート。 デフォルトの TURN リレー メディア ポートの範囲は 24000 ～ 29999 です。	
メディア ポート範囲の末尾（Media port range end）	TURN の割り当てに使用するポート範囲の上限ポート。	

TURN サーバ ステータス

TURN サーバのステータスの概要が **[TURN]** ページの下部に表示されます。TURN サーバがアクティブになっていると、この概要には、アクティブな TURN クライアントの数とアクティブなリレーの数も表示されます。

アクティブなリレーのリンクをクリックして「TURN リレーの使用状況」ページにアクセスします。このページには、Expressway 上で現在アクティブなすべての TURN リレーのリストが表示されます。また、アクセス許可、チャネル バインド、カウンタなどの TURN リレーの詳細も確認できます。

第 11 章

ユニファイドコミュニケーション

ここでは、Cisco Collaboration Edge Architecture の中心となる部分であるユニファイドコミュニケーションの機能を実現するための Expressway-C と Expressway-E の設定方法について説明します。

ユニファイドコミュニケーションの前提条件

ユニファイドコミュニケーションのためのセキュアなトラバーサル ゾーン接続の設定

ユニファイドコミュニケーション機能（Mobile & Remote Access、または Jabber Guest など）には、Expressway-C と Expressway-E 間にユニファイドコミュニケーション トラバーサル ゾーン接続が必要です。これには、以下が含まれます。

- Expressway-C と Expressway-E に適切なセキュリティ証明書をインストールする。
- Expressway-C と Expressway-E 間のユニファイドコミュニケーション トラバーサル ゾーンを設定する。

（注） ユニファイドコミュニケーショントラバーサルゾーンは Expressway のトラバーサルペアごとに 1 つだけ設定します。つまり、Expressway-C クラスタに 1 つのユニファイドコミュニケーション トラバーサル ゾーンと、Expressway-E クラスタに対応する 1 つのユニファイドコミュニケーション トラバーサル ゾーンです。

Expressway のセキュリティ証明書のインストール

Expressway-C と Expressway-E 間の信頼を設定する必要があります。

1. Expressway-C と Expressway-E の両方に適したサーバ証明書をインストールします。
   - 証明書には、**Client Authentication** 拡張子を含める必要があります。システムにより、ユニファイドコミュニケーション機能が有効になっている場合、この拡張子を指定せずにサーバ証明書をアップロードすることはできません。
   - Expressway には、証明書署名要求（CSR）を生成する機能が組み込まれており、CSR を生成する場合に推奨される方法です。
     - 要求に署名する CA がクライアント認証拡張子を除外していないことを確認します。
     - 生成した CSR には、クライアント認証要求と有効化されたユニファイド コミュニケーション機能に関連するサブジェクト代替名が含まれます（ユニファイドコミュニケーションのサーバ証明書要件を参照してください）。
   - CSR を生成するか Expressway にサーバ証明書をアップロードするには、**[メンテナンス（Maintenance）]** > **[セキュリティ（Security）]** > **[サーバ証明書（Server certificate）]** に移動します。新しいサーバ証明書を有効にするには、Expressway を再起動する必要があります。
2. 両方の Expressway に Expressway のサーバ証明書に署名した CA の信頼できる認証局（CA）証明書をインストールします。

   展開されるユニファイドコミュニケーション機能に基づいて、次のように信頼要件が追加されます。

   Mobile & Remote Access を導入する場合：
   - Expressway-C は Unified CM と IM&P の Tomcat 証明書を信頼する必要があります。
   - 状況に応じて、Expressway-C と Expressway-E の両方で、エンドポイントの証明書に署名した認証局を信頼する必要があります。

   Jabber Guest を導入する場合：
   - Jabber Guest サーバがインストールされると、自己署名証明書がデフォルトで使用されます。ただし、信頼できる認証局によって署名された証明書をインストールできます。Expressway-C に Jabber Guest サーバの自己署名証明書、または Jabber Guest サーバの証明書に署名した CA の信頼済み CA 証明書をインストールする必要があります。

   信頼できる認証局（CA）証明書を Expressway にアップロードするには、**[メンテナンス（Maintenance）]** > **[セキュリティ（Security）]** > **[信頼できる CA 証明書（Trusted CA certificate）]** を選択します。新しい信頼できる CA 証明書を有効にするには、Expressway を再起動する必要があります。

Expressway 構成ガイドページの『*Cisco Expressway* 証明書作成および使用導入ガイド』を参照してください。

暗号化された Expressway トラバーサル ゾーンの設定

Expressway-C と Expressway-E 間のセキュアなトラバーサル ゾーン接続によってユニファイド コミュニケーション機能をサポートするには、次の手順を実行します。

- Expressway-C、Expressway-E はユニファイド コミュニケーション トラバーサル のゾーン タイプで設定する必要があります。これは自動的に適切なトラバーサル ゾーン（Expressway-C 上で選択されたときは、トラバーサル クライアント ゾーン、Expressway-E 上で選択されたときは、トラバーサル サーバ ゾーン）を設定します。そのゾーンは、[TLS 検証モード（TLS verify mode）] が [オン（On）] かつ [メディア暗号化モード（Media encryption mode）] が [強制暗号化（Force encrypted）] の状態で SIP TLS を使用します。
- 両方の Expressway はサーバ証明書を相互に信頼する必要があります。各 Expressway がクライアントとサーバの両方として機能すると同時に各 Expressway の証明書がクライアントとサーバとして有効であることを確認する必要があります。
- Expressway は、CN（共通名）ではなく SAN 属性（サブジェクトの別名）を使用して、受信した証明書を検証することに注意してください。
- H.323 または暗号化されていない接続も必要な場合、別のトラバーサル ゾーン ペアを設定する必要があります。

安全なトラバーサルゾーンをセットアップするには

セキュアなトラバーサル ゾーンを設定するには、Expressway-C と Expressway-E を次のように設定します。

手順

ステップ 1 **[設定（Configuration）] > [ゾーン（Zones）] > [ゾーン（Zones）]** へ移動します。

ステップ 2 [新規（New）] をクリックします。

ステップ 3 次のようにフィールドを設定します（他のすべてのフィールドはデフォルト値のままにします）。

	Expressway-C	**Expressway-E**
名前（Name）	「「Traversal zone」」など	「「Traversal zone」」など
タイプ（Type）	*Unified Communications traversal*	*Unified Communications traversal*
[接続クレデンシャル（Connection credentials）] セクション		
ユーザ名（Username）	「「exampleauth」」など	「「exampleauth」」など

	Expressway-C	Expressway-E
[パスワード（Password）]	「「ex4mpl3.c0m」」など	**[ローカル認証データベースの追加/編集（Add/Edit local authentication database）]** をクリックし、ポップアップ ダイアログで **[新規（New）]** をクリックして、**[名前（Name）]** に名前（例：「「exampleauth」」）、**[パスワード（Password）]** にパスワード（例：「「ex4mpl3.c0m」」）を入力し、**[クレデンシャルの作成（Createcredential）]**をクリックします。
SIP セクション		
[ポート（Port）]	Expressway-E の設定に一致する必要があります。	**7001**（デフォルト）Cisco Expressway シリーズ設定ガイドのページに用意されている、ご使用のバージョンに対応する『*Cisco Expressway IP Port Usage Configuration Guide*』を参照してください）。
TLS サブジェクト名の確認（TLS verify subject name）	N/A	トラバーサル クライアントの証明書で、検索する名前を入力します（SAN（サブジェクトの別名）属性である必要があります）。トラバーサル クライアントのクラスタがある場合は、ここでクラスタ名を指定し、各クライアントの証明書に含まれることを確認します。
[認証（Authentication）] セクション		
[認証ポリシー（Authentication policy）]	*[クレデンシャルを確認しない（Do not check credentials）]*	*[クレデンシャルを確認しない（Do not check credentials）]*
[ロケーション（Location）] セクション		

	Expressway-C	Expressway-E
ピア 1 アドレス（Peer 1 address）	Expressway-E の FQDN を入力します。 （注） IP アドレスを使用する場合（推奨していません）、そのアドレスが Expressway-E サーバ証明書に含まれている必要があります。	**対象外**
ピア 2 ～ 6 アドレス（Peer 2...6 address）	Expressway-E のクラスタである場合は、追加ピアの FQDN を入力します。	**対象外**

ステップ 4 [ゾーンの作成（Create zone）] をクリックします。

ユニファイド コミュニケーションのサーバ証明書要件

Cisco Unified Communications Manager の証明書

Mobile & Remote Access で重要な Cisco Unified Communications Manager 証明書は、次の 2 つです。

- *CallManager* 証明書
- *tomcat* 証明書

これらの証明書は Cisco Unified Communications Manager に自動的にインストールされ、デフォルトで自己署名されて同じ一般名（CN）を持ちます。

CA によって署名された証明書を使用することを推奨します。ただし、自己署名証明書を使用する場合、2 つの証明書の一般名は異なる必要があります。Expressway では同じ CN を持つ 2 つの自己署名証明書は許可されません。そのため、Expressway の信頼される CA リストで *CallManager* と *tomcat* の自己署名証明書の CN が同じ場合、Expressway はそのうちの 1 つしか信頼できません。つまり、Expressway-C と Cisco Unified Communications Manager 間のセキュア HTTP またはセキュア SIP は失敗します。

また、シスコ コラボレーション システム リリース 10.5.2 内の製品に対して *tomcat* 証明書の署名要求を生成する場合、CSCus47235 に注意する必要があります。ノードの FQDN がサブジェクト代替名（SAN）エントリとして証明書に含まれるようにするため、この問題を回避する必要があります。「リリースノート」ページにある *Expressway X8.5.3* のリリースノートに回避策の詳細が記載されています。

IM and Presence Service の証明書

XMPP を使用する場合に重要となる IM and Presence Service 証明書は、次の 2 つです。

- *cup-xmpp* 証明書
- *tomcat* 証明書

CA によって署名された証明書を使用することを推奨します。ただし、自己署名証明書を使用する場合、2 つの証明書の一般名は異なる必要があります。Expressway では同じ CN を持つ 2 つの自己署名証明書は許可されません。*cup-xmpp* 証明書と *tomcat*（自己署名）証明書が同じ CN を持つ場合、Expressway はそのうちの 1 つしか信頼せず、Cisco Expressway サーバと IM and Presence Service サーバ間の一部の TLS 試行が失敗します。詳細については、CSCve56019 を参照してください。

Expressway 証明書

Expressway の証明書署名要求（CSR）ツールでは、Expressway でサポートされるユニファイド コミュニケーション機能に適した関連するサブジェクト代替名（SAN）について確認が求められ、組み込まれます。

次の表は、どのユニファイド コミュニケーションの機能にどの CSR 代替名の要素が適用されるかを示します。

サブジェクト代替名として次の項目を追加します ↓	これらの目的で CSR を生成する場合 ←			→
	モバイル & リモート アクセス	Jabber Guest	XMPP フェデレーション	ビジネス ツー ビジネス コール
Unified CM 登録ドメイン（ドメイン名にかかわらず、これらは Unified CM SIP 登録ドメインよりもサービス検出ドメインと共通点があります）	Expressway-E でのみ必要	-	-	-
XMPP フェデレーション ドメイン	-	-	Expressway-E でのみ必要	-
IM and Presence チャット ノード エイリアス（フェデレーテッド グループ チャット）	-	-	必須	-
Unified CM 電話セキュリティ プロファイル名	Expressway-C でのみ必要	-	-	-
（クラスタ化されたシステムのみ）Expressway クラスタ名	Expressway-C でのみ必要	Expressway-C でのみ必要	Expressway-C でのみ必要	-

（注）
- チャット ノード エイリアスを追加するか、名前を変更する場合、Expressway-C 用の新しいサーバ証明書の作成が必要になることがあります。つまり、IM and Presence ノードが追加されるか名前が変更される場合、または新しい TLS 電話セキュリティ プロファイルが追加される場合などです。
- 新しいチャット ノード エイリアスがシステムに追加される場合、または CM か XMPP フェデレーション ドメインが変更される場合は、新しい Cisco Expressway-E の証明書を作成する必要があります。
- 新しくアップロードされたサーバ証明書を有効にするには、Expressway を再起動する必要があります。

Expressway-C/Expressway-E の個々の機能要件についての詳細は、次のとおりです。

Expressway-C のサーバ証明書の要件

Expressway-E サーバ証明書には、そのサブジェクト代替名（SAN）のリストに次の要素が含まれる必要があります。

- Unified CM 電話セキュリティ プロファイル名：暗号化されたトランスポートライン（TLS）用に設定され、リモートアクセスを必要とするデバイスに使用される Unified CM の**電話セキュリティ プロファイル**の名前。完全修飾ドメイン名（FQDN）形式を使用し、複数のエントリをカンマで区切ります。

  Expressway-C の既存のクラスタに新しい Expressway-C ノードを追加する間は、新しいノードの証明書署名要求（CSR）を生成する必要があります。CUCM でモバイルおよびリモートアクセス（CUCM）クライアントの安全な登録が必要な場合、CUCM に安全なプロファイル名を付ける必要があります。「Unified CM Phone のセキュリティプロファイル名」が CUCM デバイスのセキュリティプロファイルの名前またはホスト名だけである場合、新しいノードでの CSR の作成は失敗します。これにより、管理者は **[安全な電話機プロファイル（Secure Phone Profile）]** ページの下で、CUCM で 「Unified CM Phone のセキュリティプロファイル名」の値を変更する必要があります。

  X12.6 から、Unified CM のセキュリティプロファイル名は完全修飾ドメイン名（FQDN）である必要があります。名前、ホスト名、または値だけでは使用できません。

  たとえば、`jabbersecureprofile.domain.com`、`DX80SecureProfile.domain.com`

  （注） FQDN は複数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。

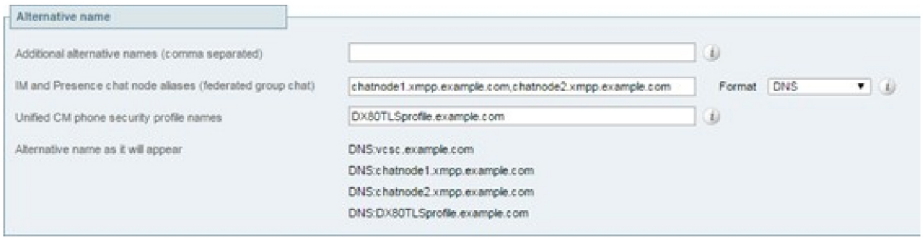
代替名としてセキュア電話プロファイルを持つことは、Unified CM がそのプロファイルを使用するデバイスからメッセージを転送する場合に、Expressway-C とトランスポートライン シグナリング（TLS）経由で通信できることを意味します。

- **IM and Presence チャット ノード エイリアス（フェデレーテッド グループ チャット）**：IM and Presence サーバで設定される**チャットノードエイリアス**（たとえば **`chatroom1.example.com`**）。これらは、フェデレーテッド連絡先との TLS を介したグループ チャットをサポートするユニファイド コミュニケーション XMPP フェデレーション導入にのみ必要です。

  Expressway-C は一連の IM&P サーバを検出すると、CSR にチャット ノード エイリアスを自動的に含めます。

  CSR を生成するときは、チャット ノード エイリアスに DNS 形式を使用することを推奨します。Expressway-E サーバ証明書の代替名には、同一のチャット ノード エイリアスを含める必要があります。

図 *7: Expressway-C* の *CSR* ジェネレータでのセキュリティ プロファイルおよびチャットノードエイリアスに対するサブジェクト代替名の入力



Expressway-E のサーバ証明書の要件

Expressway-E サーバ証明書には、そのサブジェクト代替名（SAN）のリストに次の要素が含まれる必要があります。Expressway-E が他の FQDN によって知られている場合は、**すべてのエイリアス**がサーバ証明書 SAN に含まれている必要があります。

- **Unified CM 登録ドメイン**：Unified CM の登録用に Expressway-C で設定されているすべてのドメイン。エンドポイント デバイスと Expressway-E 間のセキュアな通信に必要です。

  Expressway の設定と Expressway-E の証明書に使用される Unified CM 登録ドメインは、サービス検出時に **_collab-edge** DNS SRV レコードをルックアップするモバイルおよびリモート アクセス クライアントによって使用されます。これにより、Unified CM での MRA 登録が有効になり、サービス検出に役立ちます。

  これらのサービス検出ドメインは SIP 登録ドメインと一致することもしないこともあります。これは展開方法により異なるため、一致する必要はありません。たとえば、社内ネットワークの Unified CM で .local または類似するプライベート ドメインを使用し、Expressway-E FQDN とサービス検出にパブリック ドメイン名を使用する展開の場合、Expressway-E の証明書にパブリック ドメイン名を SAN として含める必要があります。

Unified CM で使用するプライベート ドメイン名を含める必要はありません。エッジ ドメインのみを SAN としてリストする必要があります。

DNS 形式を選択し、必要な FQDN を手動で指定します。複数のドメインが必要な場合は FQDN をカンマで区切ります。代わりに *CollabEdgeDNS* 形式を選択すると、入力したドメインにプリフィックス **collab-edge.** が追加されます。この形式は、トップ レベル ドメインを SAN として含めたくない場合に推奨されます（次のスクリーンショットの例を参照してください）。

- **XMPP フェデレーション ドメイン**：ポイントツーポイント XMPP フェデレーションに使用するドメイン。これらは、IM&P サーバで設定され、XMPP フェデレーション用のドメインとして Expressway-C でも設定する必要があります。

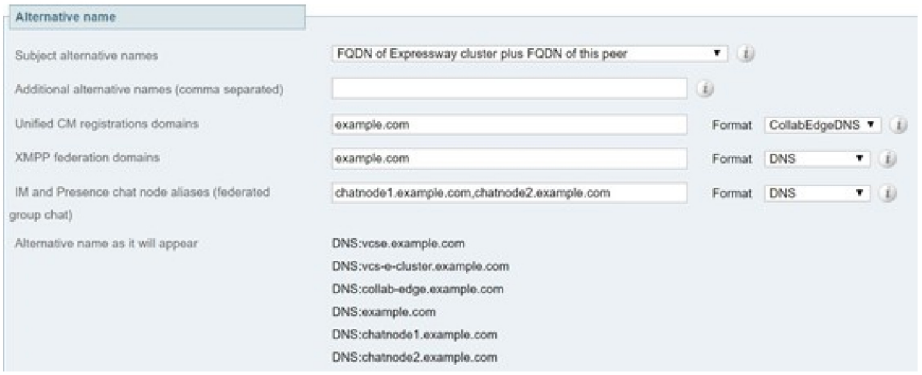
  DNS 形式を選択し、必要な FQDN を手動で指定します。複数のドメインが必要な場合は FQDN をカンマで区切ります。

  （注） *XMPPAddress* 形式を使用しないでください。この形式は CA によってサポートされない可能性があり、Expressway ソフトウェアの将来のバージョンでは廃止される可能性があります。

- **IM and Presence チャット ノード エイリアス（フェデレーテッド グループ チャット）**：Expressway-C の証明書で入力されたものと同じ**チャットノードエイリアス**のセット。フェデレーテッド連絡先との TLS を介したグループ チャットをサポートする音声とプレゼンスの導入にのみ必要です。

  （注） チャットノードエイリアスのリストは、Expressway-C 対応の「**CSR の作成（Generate CSR）**」ページからコピーできます。

図 *8: Expressway-E* の *CSR* ジェネレータでの *Unified CM* 登録ドメイン、*XMPP* フェデレーション ドメイン、およびチャット ノード エイリアスに対するサブジェクト代替名の入力



454312

詳細については、Expressway 構成ガイドページの『*Cisco Expressway* 証明書作成および使用導入ガイド』を参照してください。

MRA オンボードを使用する場合の mTLS 証明書

MRA 上でアクティベーション コード オンボードを有効にすると、相互 TLS に必要な CA 証明書が自動的に生成されます (相互 TLS はアクティベーション コード オンボードの必須要件です)。証明書は、信頼された CA 証明書のあるページからアクセスするための mTLS 用 CA 証明書ページで使用できます（**[メンテナンス（Maintenance）] > [セキュリティ（Security）] > [信頼された CA 証明書（Trusted CA certificate）]**）。

ドメイン証明書および Sever Name Indication の管理

Cisco Hosted Collaboration Solution（HCS）の一部であるマルチテナンシーにより、サービス プロバイダーは複数のテナント間で Expressway-E クラスタを共有できます。

TLS 内のサーバ名指定（SNI）プロトコル拡張を使用して、Expressway は、TLS ハンドシェイク中にクライアントに提供できるドメイン固有の証明書を保存および使用できるようになりました。この機能により、マルチテナント環境で MRA を介して登録したエンドポイントのシームレスな統合が可能になり、証明書のドメイン名がクライアントのドメインと一致するようになります。TLS ハンドシェイク中、クライアントは *ClientHello* 要求に SNI フィールドを含めます。Expressway は証明書ストアを検索し、SNI ホスト名との一致を探そうとします。一致が見つかった場合、ドメイン固有の証明書がクライアントに返されます。

（注） マルチテナントモードでは、Cisco Expressway-E の **[システム（System）] > [DNS]** ページで、DNS に設定されているホスト名と一致するようにシステムのホスト名を設定する必要があります（X8.10.1 より前では大文字と小文字が区別されます。X8.10.1 以降は大文字と小文字は区別されません）。このようにしなければ、Cisco Jabber クライアントを MRA に正常に登録できません。

Cisco Hosted Collaboration Solution ページの『マルチテナントおよび *Cisco Expressway*』を参照してください。

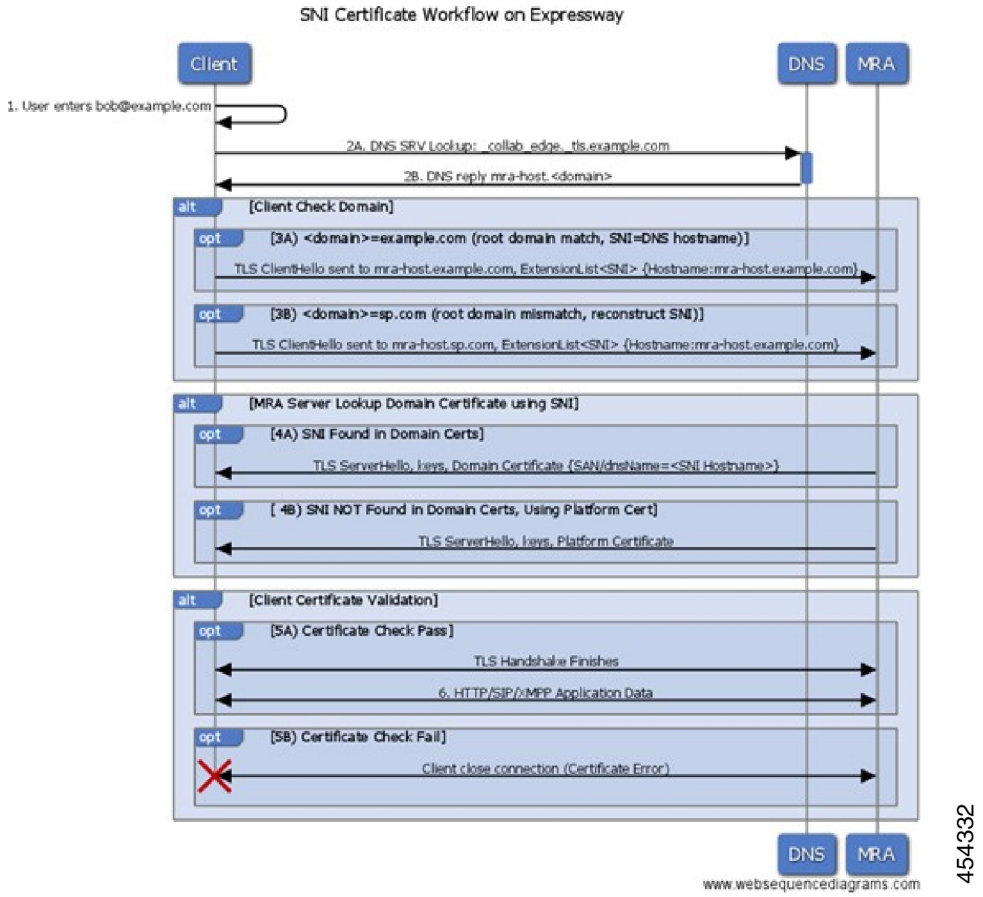
SNI のコール フロー

1. 登録されている MRA クライアントで、ユーザが **bob@example.com** と入力します。ここで、**example.com** はユーザのサービス ドメイン（クラスタ ドメイン）です。
2. クライアントが DNS 解決を行います。
    1. **_collab-edge._tls.example.com** に対して DNS SRV 要求を送信します。
    2. DNS が要求に応答します。
        - 単一のテナント設定の場合：通常、DNS 応答にはサービス ドメイン内のホスト名（たとえば、**mra-host.example.com**）が含まれます。

- マルチテナント設定の場合：DNS が代わりに、サービス プロバイダーのドメイン内のサービス プロバイダーの MRA ホスト名を返す場合があります。これは、ユーザのサービス ドメインとは異なります（たとえば、**mra-host.sp.com**）。

3. クライアントが SSL 接続を設定します。
   1. クライアントは、SSL ClientHello リクエストに SNI 拡張子を付けて送信します。
      - DNS によって返されたホスト名がユーザのサービス ドメインと同じドメインを持つ場合、DNS ホスト名は SNI server_name（変更なし）で使用されます。
      - それ以外の場合、ドメインが一致しなければ、クライアントは SNI server_name を DNS ホスト名とサービス ドメインに設定します（たとえば、DNS から **mra host.sp.com** が返されるのではなく、**mra-host.example.com** が返されます）。
   2. Expressway-E が証明書ストアを検索し、SNI ホスト名と一致する証明書を検索します。
      - 一致するものが見つかると、Expressway-E は証明書（SAN/dnsName=SNI ホスト名）を返信します。
      - それ以外の場合、MRA はプラットフォーム証明書を返します。
   3. クライアントがサーバの証明書を検証します。
      - 証明書が検証されると、SSL セットアップが続行され、SSL セットアップが正常に終了します。
      - それ以外の場合、証明書エラーが発生します。
4. アプリケーション データが開始されます。

（注） SIP と HTTPS の場合は、アプリケーションが SSL ネゴシエーションを即座に開始します。XMPP の場合は、クライアントが XMPP StartTLS を受信すると、SSL 接続が開始されます。



Expressway のドメイン証明書の管理

Expressway のドメイン証明書は、**「ドメイン証明書（Domain certificates）」**ページ（**[メンテナンス（Maintenance）] > [セキュリティ（Security）] > [ドメイン証明書（Domain certificates）]**）で管理します。これらの証明書は、マルチテナント環境で複数の顧客が TLS 暗号化と HTTPS 経由の Web ブラウザを使用してクライアントシステムと通信するために Expressway-E クラスタを共有している場合に、ドメインを識別するために使用されます。[ドメイン証明書（domain certificate）] ページを使用すると、次のことを実行できます。

- 現在ロードされている証明書に関する詳細の表示
- 証明書署名要求（CSR）を生成します。
- 新しいドメイン証明書のアップロード
- ACME（Automated Certificate Management Environment）サービスが自動的に CSR を ACME プロバイダーに送信して、生成された証明書を自動的に展開するように設定します。

（注） RSA キーに基づく証明書を使用することを強く推奨します。DSA キーに基づく証明書など他のタイプの証明書はテストされておらず、あらゆるシナリオで Expressway と連携するとは限りません。「**信頼できる CA 証明書（Trusted CA certificate）**」 ページを使用して、この Expressway で信頼されている認証局（CA）の証明書のリストを管理します。

現在アップロードされているドメイン証明書の表示

ドメインをクリックすると、ドメイン証明書データ セクションに、現在 Expressway にロードされている特定のドメイン証明書に関する情報が表示されます。

現在アップロードされているドメイン証明書ファイルを表示する場合、人間可読形式で表示するには **[表示（復号化）（Show (decoded)）]** をクリック、または RAW 形式でファイルを表示するには **[表示（PEM ファイル）（Show (PEM file)）]** をクリックします。

現在アップロードされているドメインを削除するには、**[削除（Delete）]** をクリックします。

（注） ドメイン証明書を期限切れにしないでください。期限が切れると他の外部システムが証明書を拒否し、Expressway がそれらのシステムに接続できなくなります。

新しいドメインの追加

手順

ステップ 1 **[メンテナンス（Maintenance）]** > **[セキュリティ（Security）]** > **[ドメイン証明書（Domain certificates）]** に移動します。

ステップ 2 **[新規（New）]** をクリックします。

ステップ 3 **[新しいローカルドメイン]**で、追加するドメインの名前を入力します。

例：

有効なドメインの例としては、`100.example-name.com` などがあります。

ステップ 4 [ドメインの作成（Create domain）] をクリックします。

ステップ 5 新しいドメインが **[ドメイン証明書（Domain certificates）]** ページに追加され、ドメインの証明書のアップロードに進むことができます。

証明書署名要求の生成

Expressway はドメイン CSR を生成可能で、これにより証明書要求を生成および取得するために外部メカニズムを使用する必要がなくなります。

（注）
- 1 回に 1 つの署名要求だけを進行させることができます。これは、Expressway が現在の要求に関連付けられた秘密キーファイルを追跡する必要があるためです。現在の要求を廃棄し、新しい要求を開始するには、[Discard CSR] をクリックします。
- ユーザインターフェイスにダイジェストアルゴリズムを設定するオプションがあります。デフォルトでは SHA-256 に設定されており、SHA-384 または SHA-512 に変更するオプションがあります。
- ユーザインターフェイスにキーの長さを設定するオプションがあります。Expressway は、1024、2048、および 4096 のキーの長さをサポートしています。

手順

ステップ 1 **[メンテナンス（Maintenance）] > [セキュリティ（Security）] > [ドメイン証明書（Domain certificates）]** に移動します。

ステップ 2 CSR を生成するドメインをクリックします。

ステップ 3 **[CSR の作成（Generate CSR）]** をクリックして **[CSR の作成（Generate CSR）]** ページに移動します。

ステップ 4 証明書に必要なプロパティを入力します。

Expressway がクラスタの一部である場合、145 ページのドメイン証明書とクラスタ化システムを参照してください。

ステップ 5 [Generate CSR] をクリックします。システムが署名要求と関連する秘密キーを生成します。秘密キーは、Expressway に安全に保存され、表示またはダウンロードすることはできません。

（注） 認証局に対しても秘密キーを開示してはなりません。

ステップ 6 「**ドメイン証明書（Domain certificate）**」ページに戻ります。グローバル設定に関して実行できることは次のとおりです。

- 認証局に送信できるように、要求をローカル ファイル システムにダウンロードします。ファイルを保存するよう求められます（実際の表現はブラウザによって異なります）。
- 現在の要求の表示（人間可読形式で表示するには **[Show (decoded)]** をクリック、または raw 形式でファイルを表示するには **[Show (PEM file)]** をクリックします）。

新しいドメイン証明書のアップロード

署名付きドメイン証明書が認証局から送り戻されたら、Expressway にアップロードする必要があります。**[新規証明書のアップロード（Upload new certificate）]** セクションを使用して、現在のドメイン証明書を新しい証明書に置き換えます。

手順

ステップ 1 **[メンテナンス（Maintenance）] > [セキュリティ（Security）] > [ドメイン証明書（Domain certificates）]** に移動します。

ステップ 2 **[新規証明書のアップロード（Upload new certificate）]** セクションの **[参照（Browse）]** ボタンを使用して、ドメイン証明書の PEM ファイルを選択し、アップロードします。

ステップ 3 外部システムを使用して CSR を生成する場合は、ドメイン証明書を暗号化するために使用した、サーバ秘密キー PEM ファイルもアップロードする必要があります。（Expressway を使用して、このドメイン証明書用の CSR が作成された場合、秘密キー ファイルは、前もって自動的に生成および保存されます）。

- サーバ秘密キー PEM ファイルはパスワードで保護しないでください。
- 証明書署名要求の進行中は、サーバ秘密キーをアップロードできません。

ステップ 4 [ドメイン証明書データのアップロード（Upload domain certificate data）] をクリックします。

自動証明書管理環境サービス

バージョン X12.5 から、Expressway-E の自動証明書管理環境（ACME）サービスは、（SNI で使用される）ドメイン証明書を要求して導入できます。

[メンテナンス（Maintenance）] > [セキュリティ（Security）] > [ドメイン証明書（Domain certificates）] に移動すると、ドメインのリストの **[ACME]** 列に、各ドメインの ACME サービスのステータスが示されます。

ACME サービスを有効にするドメイン名の横にある **[表示/編集（View/Edit）]** をクリックします。

ドメイン証明書用に ACME サービスを設定するプロセスは、サーバ証明書用に設定する場合と同じで、Expressway-E インターフェイスで使用する場所が異なるだけです。

Expressway 構成ガイドページの『*Cisco Expressway* 証明書作成および使用導入ガイド』を参照してください。

ドメイン証明書とクラスタ化システム

CSR の生成時には、1 つの要求および秘密キーの組み合わせがそのピア専用に生成されます。

Expressway のクラスタがある場合は、各ピアで個別の署名要求を生成する必要があります。これらの要求はその後、認証局に送信し、返されたドメイン証明書を関連する各ピアにアップロードする必要があります。

（注） 正しいドメイン証明書が適切なピアにアップロードされていることを確認する必要があります。そうでないと、各ピアに保存された秘密キーがアップロードされた証明書に対応しません。

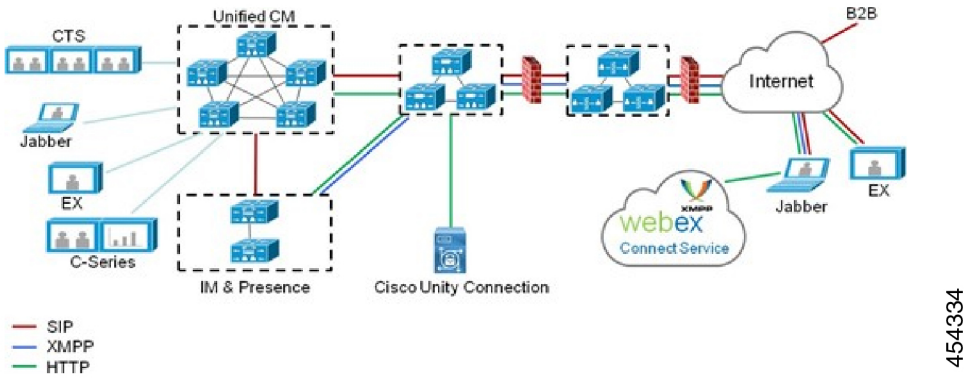
モバイルおよびリモート アクセスの概要

Cisco Unified Communications の Mobile & Remote Access は Cisco Collaboration Edge アーキテクチャの中核を成します。Cisco Jabber などのエンドポイントが企業ネットワーク外にある場合に、Cisco Unified Communications Manager（Unified CM）への登録、呼制御、プロビジョニング、メッセージング、およびプレゼンスの機能を使用することができるようになります。Expressway は、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。

ソリューション全体で、次の機能が提供されます。

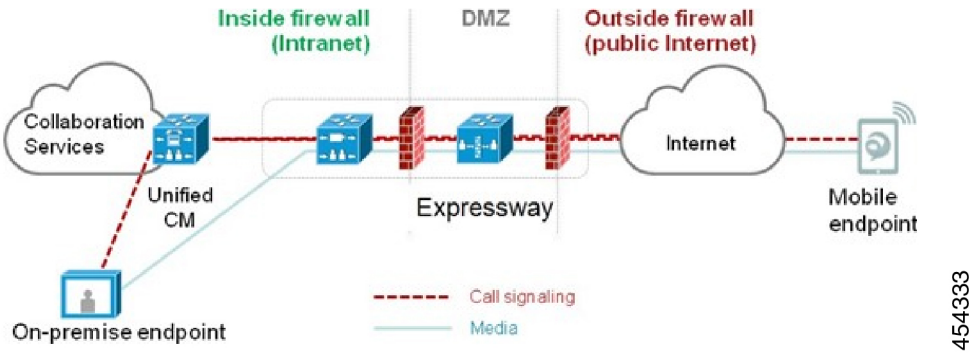
- **オフプレミスアクセス**：企業ネットワーク外においても、JabberおよびEX/MX/SXシリーズ クライアントで一貫したエクスペリエンスを提供。
- **セキュリティ**：セキュアな Business-to-Business（B2B）コミュニケーション
- **クラウドサービス**：エンタープライズクラスの柔軟性と拡張性に優れたソリューションにより、さまざまな Cisco Webex 統合およびサービス プロバイダ オファリングに対応。
- **ゲートウェイと相互運用性サービス**：メディアおよびシグナリングの正規化、非標準エンドポイントのサポート

図 *9 : Unified Communications*：モバイルおよびリモート アクセス



（注） サードパーティのSIPまたはH.323デバイスはExpressway-Cに登録でき、必要に応じてSIPトランクを介して統合されたCM登録デバイスと相互運用することもできます。

図 *10* : 一般的なコールフロー：シグナリングとメディアパス



Unified CM は、モバイルとオンプレミスの両方のエンドポイントにコール制御を提供します。

シグナリングは、モバイル エンドポイントと Unified CM の間で Expressway ソリューションを横断します。Expressway ソリューションをトラバースするメディアは、エンドポイント間で直接中継されます。

すべてのメディアは、Expressway-C とモバイル エンドポイント間で暗号化されます。

導入範囲

次の主要な Expressway ベースの導入は機能しません。これらを同じ Expressway（またはトラバーサル ペア）で一緒に実装することはできません。

- モバイル & リモート アクセス
- Expressway-C ベースの B2BUA を使用した Microsoft 相互運用性
- Jabber Guest サービス

モバイルおよびリモートアクセスポート

MRA のポートについては、Cisco Expressway シリーズ設定ガイドのページに用意されている『*Cisco Expressway IP Port Usage Configuration Guide*』を参照してください。このガイドに、内部ネットワーク（Expressway-C が配置されている）と DMZ（Expressway-E が配置されている）間、および DMZ とパブリック インターネット間のファイアウォールで使用できるポートが記載されています。

VPN を使用しない Jabber クライアント接続

MRA ソリューションでは、ハイブリッド オンプレミス サービス モデルとクラウドベースのサービス モデルをサポートしています。これは、社内および社外で一貫したエクスペリエンスを提供します。MRA は、VPN で企業ネットワークに接続せずに Jabber アプリケーション トラ

フィックのセキュアな接続を提供します。Windows、Mac、iOS および Android プラットフォームでデバイスとオペレーティング システムに依存しない Cisco Jabber クライアントのソリューションです。

MRA は、企業外の Jabber クライアントで以下を実現します。

- インスタント メッセージングおよびプレゼンス サービスの使用
- 音声/ビデオ通話
- 社内ディレクトリを検索する。
- コンテンツの共有
- Web 会議の開始
- ビジュアル ボイスメールへのアクセス

詳細な設定情報の取得場所

MRA 用に Expressway を使用する方法について詳しくは、「Expressway 設定ガイド」ページの『*Cisco Expressway* を使用したモバイルおよびリモートアクセス』を参照してください。このガイドでは、以下について説明します。

- Expressway-C と Expressway-E で MRA 機能を有効にして設定する方法。
- MRA サービスで使用する Unified CM サーバと IM&P サーバを検出する方法。
- MRA アクセス制御（認証の設定、SAML SSO、許可リストを含む）。
- プッシュ通知のサポートを有効にする方法

Expressway による XMPP フェデレーション

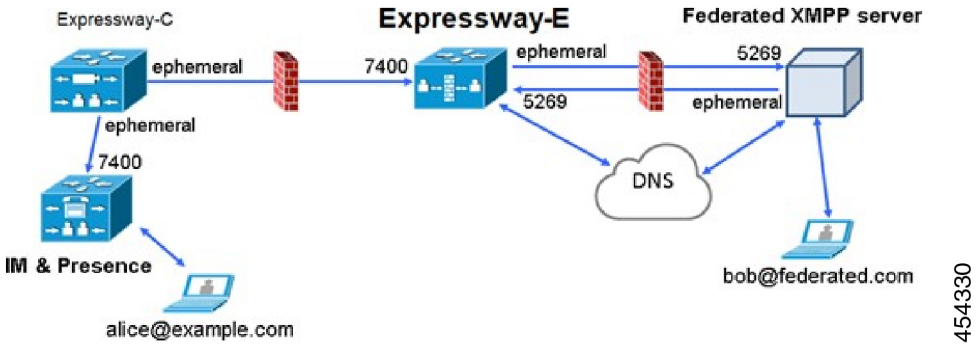
外部 XMPP フェデレーションでは、Cisco Unified Communications Manager IM and Presence Service に登録されたユーザが、異なる XMPP 導入環境からのユーザと Cisco Expressway-E を介して通信できます。

（注） このセクションでは、Expressway を使用して管理する XMPP フェデレーションについて説明しますが、このガイドで後述するように、IM and Presence Service を使用して管理することもできます。

次の図は、オンプレミス IM & Presence サーバから Expressway-C および Expressway-E コラボレーション エッジ ソリューションを介してフェデレーテッド XMPP サーバにルーティングされる XMPP メッセージを示しています。また、メッセージが DMZ ファイアウォールを通過するときに使用される接続とポートも示しています。「「example.com」」組織では Expressway

フェデレーション モデル（図の左側）を使用し、一方、「「federated.com」」組織（図の右側）では DMZ フェデレーション モデルの IM and Presence Service を使用しています。

図 *11 : XMPP* 連邦に対するメッセージのルーティング



サポートされるシステム

Expressway-E は次の製品との XMPP フェデレーションをサポートしています。

- Expressway X8.2 以降
- Cisco Unified Communications Manager IM and Presence Service 9.1.1 以降
- Cisco Webex Connect リリース 6.x
- Cisco Jabber 9.7 以降
- その他の XMPP 標準準拠サーバ

制限事項

- Expressway を XMPP フェデレーションに使用する場合、Expressway-E はリモート フェデレーション サーバへの接続を処理し、Jabber ID のみを使用して XMPP メッセージを管理できます。Expressway-E は（電子メール アドレスなどの）XMPP のアドレス変換をサポートしません。

  外部ユーザとして、フェデレーションを介して企業内のユーザとチャットを試みる場合は、エンタープライズユーザの Jabber ID を使用して XMPP を介してユーザと連絡をとる必要があります。エンタープライズ ユーザの Jabber ID が電子メール アドレスと一致しない場合（特に Jabber ID に内部ユーザの ID またはドメインを使用している場合）、エンタープライズ ユーザの電子メール アドレスがわからないため、フェデレーションを設定することはできません。このため、Expressway を XMPP フェデレーションに使用する場合、企業は Unified CM ノードを設定して、ユーザの Jabber ID と電子メールに同じアドレスを使用することを推奨します。この制限は、フェデレーションが Expressway-E で処理されているとしても、企業内で（フェデレーションを使用せず）互いに連絡を取り合うユー

ザには適用されません。このようなフェデレーションされていないユース ケースでは、Jabber ID またはディレクトリ URI（通常は電子メール）を使用するように IM and Presence Service を設定できます。

ユーザの Jabber ID をユーザの電子メール アドレスに似せて、フェデレーテッド パートナーがフェデレーション用に電子メールアドレスを近いものにできるようにするには、次のように設定します。

a. ユーザ ID がユーザの sAMAccountName になるように、Unified CM Lightweight Directory Access Protocol（LDAP）属性を設定。

b. 電子メール ドメインと同じになるように Unified CM IM and Presence Service プレゼンス ドメインを設定。

c. samaccountname@presencedomain と同じになるように電子メール アドレスを設定。

- IM and Presence Service によって管理される内部フェデレーションと Cisco Expressway によって管理される外部フェデレーションは同時にサポートされません。内部フェデレーションのみが必要な場合に、IM and Presence Service 上でドメイン間フェデレーションを使用する必要があります。使用可能なフェデレーション導入の設定オプションは次のとおりです。
  - 外部フェデレーションのみ（Expressway で管理）。
  - 内部フェデレーションのみ（IM and Presence Service によって管理）。
  - IM and Presence Service によって内部および外部フェデレーションが管理されますが、インバウンド接続を許可するようにファイアウォールを設定する必要があります。

前提条件

- Expressway 上で XMPP フェデレーションを有効にする前に、IM and Presence Service 上のドメイン間 XMPP フェデレーションが**無効**にされている必要があります。

  [Cisco Unified CM IM and Presence サービス管理（Cisco Unified CM IM and Presence Service Administration）] > [プレゼンス（Presence）] > [ドメイン間フェデレーション（Inter Domain Federation）] > [XMPP フェデレーション（XMPP Federation）] > [設定（Settings）] に移動して、**[XMPP フェデレーション ノードのステータス（XMPP Federation Node Status）]** が *[オフ（Off）]* に設定されていることを確認します。

- XMPP フェデレーションは単一の Expressway クラスタでのみサポートされます。
- Expressway-C（クラスタ）と Expressway-E（クラスタ）は、『*Mobile and Remote Access via Cisco Expressway Deployment Guide*』で説明されているように、ユニファイド コミュニケーション サービスに対するモバイルおよびリモート アクセス用に設定する必要があります。XMPP フェデレーションのみが必要となる場合（Unified CM へのビデオ コールとリモート登録は不要な場合）、次の項目を設定する必要はありません。
  - *Unified CM* 上での *SIP* 登録とプロビジョニングをサポートするドメイン、または *Unified CM* 上での *IM and Presence Service* をサポートするドメイン。

- Unified CM サーバ（IM&P サーバは設定する必要があります）。
- HTTP サーバ許可リスト。

（注） フェデレーテッドコミュニケーションは、オンプレミスクライアント（IM and Presence Service に直接接続）とオフプレミスクライアント（MRA を介して IM and Presence Service に接続）の両方で使用できます。

- SIP および XMPP フェデレーションは独立していて、相互に影響を与えません。たとえば、IM and Presence サービスの SIP フェデレーションと Expressway の外部 XMPP フェデレーションを展開することができます。
- Expressway を通じて外部 XMPP フェデレーションを導入する場合、IM and Presence Service に対して Cisco XCP XMPP Federation Connection Manager 機能サービスをアクティブ化しないでください。
- Transport Layer Security（TLS）とグループ チャットの両方を使用する場合は、Expressway-C および Expressway-E サーバ証明書のサブジェクト名代替名リストに、IM and Presence Service サーバで設定された**チャット ノード エイリアス**を含める必要があります。XMPPAddress または DNS の形式を使用します。

（注） Expressway-C は、一連の IM and Presence Service サーバを検出すると、その証明書署名要求（CSR）にチャット ノードエイリアスを自動的に含めることに注意してください。Expressway-E 用の CSR を生成する場合は、Expressway-C 対応の「**CSR の作成（Generate CSR）**」ページからチャット ノード エイリアスをコピー、ペーストすることを推奨します。

設定情報の詳細

IM and Presence Service で管理する XMPP フェデレーションの設定については、『Cisco Unified Communications Manager の IM and Presence Service 用インタードメインフェデレーション』を参照してください。

Expressway で管理する XMPP フェデレーションの設定については、Expressway 設定ガイド ページの『*XMPP* フェデレーションに関する *Expressway* または *IM and Presence Service* の使用方法』を参照してください。

Cisco XCP ルータの遅延再起動

Cisco Hosted Collaboration Solution（HCS）の一部である、Cisco XCP ルータの遅延再起動機能は、Expressway-E がマルチテナント モードの場合にのみ使用できます。新しい SIP ドメインを持つ 2 つ目の Unified CM トラバース ゾーンを追加すると、Expressway-E はマルチテナント モードに入ります。

（注） マルチテナントモードでは、Cisco Expressway-E の **[システム（System）]** > **[DNS]** ページで、DNS に設定されているホスト名と一致するようにシステムのホスト名を設定する必要があります（X8.10.1 より前では大文字と小文字が区別されます。X8.10.1 以降は大文字と小文字は区別されません）。このようにしなければ、Cisco Jabber クライアントを MRA に正常に登録できません。

マルチテナンシーにより、サービス プロバイダーは複数のテナント間で Expressway-E クラスタを共有できます。各テナントには、共有 Expressway-E クラスタに接続する専用の Expressway-C クラスタがあります。

Expressway-E クラスタ、または顧客の Expressway-C クラスタで特定の設定を変更すると、共有クラスタ内の各 Expressway-E で Cisco XCP ルータを再起動する必要があります。マルチテナント Expressway-E クラスタのすべてのノードにわたって Cisco XCP ルータの設定の変更が有効になるには、再起動が必要です。再起動は、すべての顧客のすべてのユーザに影響します。

この再起動の頻度およびユーザへの影響を軽減するには、Cisco XCP ルータの遅延再起動機能を使用できます。

（注） 遅延再起動機能が有効になっていない場合、再起動は自動的に行われ、Cisco XCP ルータに影響を与える構成変更を保存するたびに発生します。複数の設定変更が必要な場合に、Cisco XCP ルータを数回再起動すると、ユーザに悪影響を及ぼす可能性があります。マルチテナントのお客様は、Cisco XCP ルータの遅延再起動機能を有効にすることを強く推奨します。

詳細については、Expressway 構成ガイドページの『*Cisco Unified Communications XMPP Federation using IM and Presence Service or Expressway*』を参照してください。

Jabber Guest サービスの概要

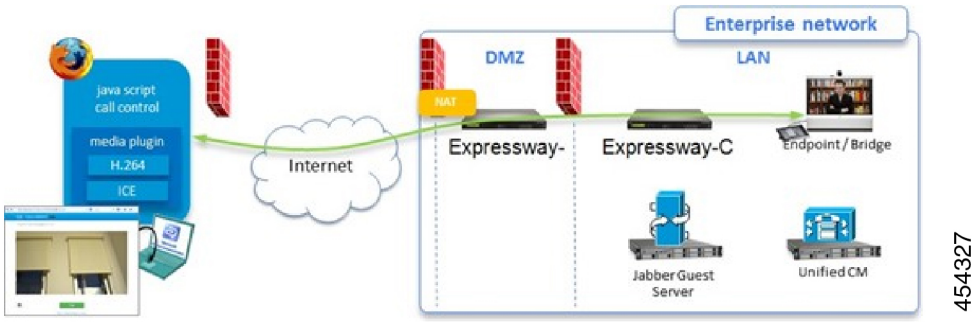
Cisco Jabber Guest は消費者企業間（C2B）ソリューションであり、電話機を Cisco Unified Communications Manager で登録していない企業のファイアウォール外の人々にシスコの企業テレフォニー範囲を拡張します。

これにより、外部ユーザはハイパーリンク（電子メールまたは Web ページ内）をクリックすると、H.264 プラグインをユーザのブラウザにダウンロードし、インストール（最初の使用時）

することができます。次に、ユーザは http ベースのコール制御を使用して URL を「「ダイヤル」」し、企業内に事前に定義された宛先にコールを発信します。ユーザがアカウントを開いたり、パスワードを作成したり、あるいは認証を行ったりする必要はありません。

コールを発信するには、インターネット内の Jabber Guest クライアントと企業内の Jabber Guest サーバ間のファイアウォールを通過して宛先のユーザエージェント（エンドポイント）に到達するために、Expressway ソリューションをユニファイド コミュニケーションのゲートウェイ（Expressway-C と Expressway-E 間のセキュアなトラバーサル ゾーン）として使用します。

図 *12 : Jabber Guest* のコンポーネント



情報の範囲

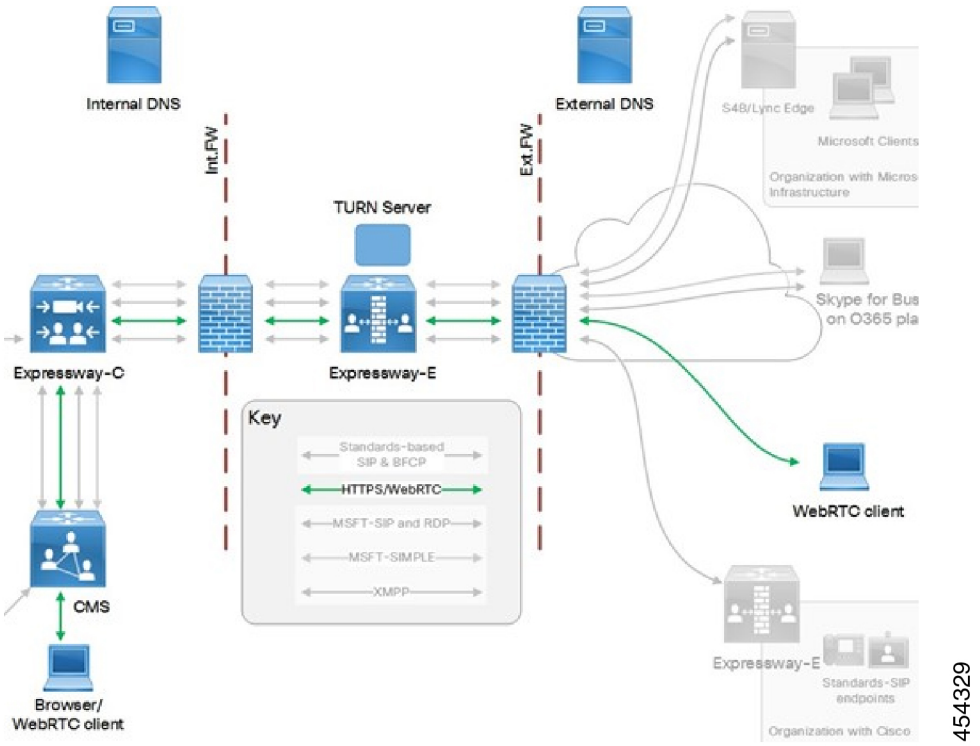
バージョン X8.7 以前では、Jabber Guest の導入に必要な Expressway のすべての設定項目は管理者ガイドに記載されていました。X8.8 以降から、この情報は個別の導入ガイドに記載されています。Jabber Guest の詳細については、次のドキュメントを参照してください。

- Expressway 設定ガイドのページに用意されている『*Cisco Expressway with Jabber Guest Deployment Guide*』。
- Jabber Guest インストールおよびアップグレードガイドのページに用意されている、ご使用のバージョンに応じた『*Cisco Jabber Guest Server Installation and Configuration Guide*』。
- Jabber Guest メンテナンスおよびオペレーションガイドのページに用意されている、ご使用のバージョンに応じた『*Cisco Jabber Guest Administration Guide*』。
- Jabber Guest リリースノートのページに用意されている、ご使用のバージョンに応じた『*Cisco Jabber Guest Release Notes*』。

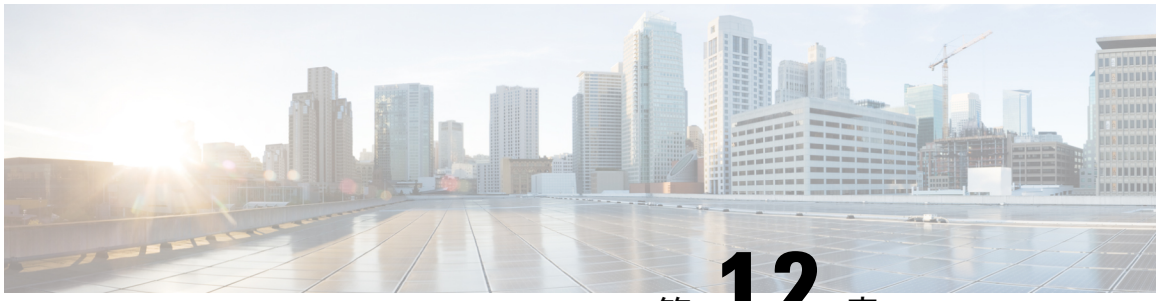
Expressway の Meeting Server Web プロキシ

このオプションにより、外部ユーザは各自のブラウザを使用して Meeting Server スペースに参加したり、管理したりすることができます。すべての外部ユーザには、Meeting Server スペースへの URL と Meeting Server にアクセスするためのクレデンシャルが必要です。

図 *13 : Expressway* の *Meeting Server Web* プロキシ



「Expressway 設定ガイド」ページの『*Cisco Meeting Server* および *Cisco Expressway* 導入ガイド』（旧称『*Cisco ExpresswayTraffic Classification* 導入ガイド』）。



第 12 章

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、登録についての設定によって異なります。

モバイルおよびリモートアクセスの概要導入環境では、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 の標準的な登録についての他に、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（デフォルト以外のゾーン）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、プレゼンスについて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 マッチングの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 をモバイルおよびリモート アクセスの概要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。

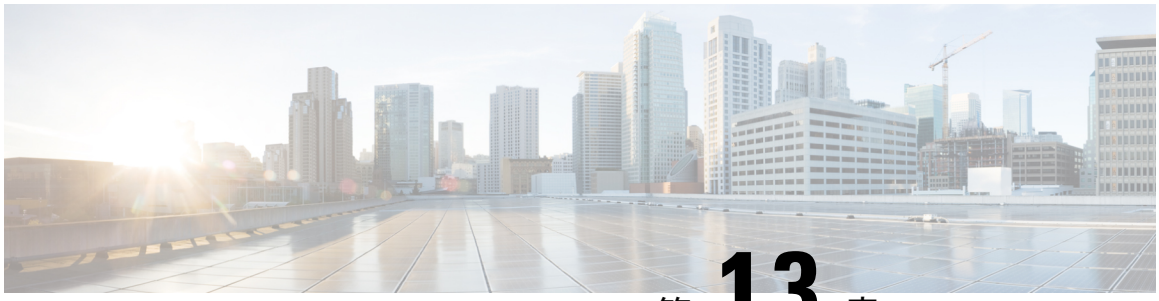
  事前検索トランスフォーメーションの設定方法については、検索前トランスフォーメーションについての項を、H.323 番号からドメイン名を取り除く方法については H.323 番号へのダイヤリングでの @domain の除去の項を参照してください。

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。



第 13 章

登録制御

ここでは、**[設定（Configuration）]**>**[登録（Registration）]** メニューに表示されるページについて説明します。

登録について

Expressway を H.323 ゲートキーパーまたは SIP レジストラとして使用するエンドポイントでは、そのエンドポイントを最初に Expressway に登録する必要があります。Expressway は、次のメカニズムを使用して登録を許可するデバイスを制御するように設定できます。

- エンドポイントが提供するユーザ名とパスワードに基づくデバイス認証についてプロセスです。
- 許可リストと拒否リストについてを使用した登録制限ポリシーの設定、または Expressway に登録できるエイリアスと登録できないエイリアスを指定するための外部ポリシーサービスです。
- サブゾーンメンバーシップ ルールとサブゾーンについてを指定した、IP アドレスおよびサブネット範囲に基づく制限です。

これらのメカニズムは併用できます。たとえば、社内ディレクトリからエンドポイントの ID を確認するために認証を使用し、これらの認証済みのエンドポイントのうちのどれが特定の Expressway に登録できるかを制御するために登録制限を使用できます。

また、次のようなプロトコル固有の一部の動作も制御できます。

- H.323 の設定 登録に対する **[登録競合モード（Registration conflict mode）]** 設定と **[自動検出（Auto discover）]** 設定
- **[SIP 登録プロキシ モード（SIP registration proxy mode）]**（SIP の設定 登録用）

クラスタ内のピア間での登録の管理方法に関する特定の情報については、ピア間での登録の共有の項を参照してください。

モバイルおよびリモートアクセスの概要導入環境では、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。

登録する Expressway の検出

エンドポイントを Expressway に登録する前に、登録できる、または登録が必要な Expressway を特定する必要があります。エンドポイントでこの設定を行いますが、プロセスは SIP の設定と H.323 の設定 で異なります。

MCU、ゲートウェイ、コンテンツサーバの登録

ゲートウェイ、MCU、コンテンツ サーバなどの H.323 システムも Expressway に登録できます。これらは、ローカルに登録されたサービスと呼ばれます。これらのシステムは、登録時に Expressway に提供する独自のプレフィックスを使用して設定されます。これにより、Expressway はそのプレフィックスで始まるすべてのコールを必要に応じてゲートウェイ、MCU、またはコンテンツ サーバにルーティングすることを認識します。また、これらのプレフィックスは登録の制御にも使用できます。

SIP デバイスはプレフィックスを登録できません。ダイヤル プランで SIP デバイスには特定のプレフィックスを介して到達するように指定している場合は、使用するプレフィックスと等しいパターン マッチを使用して、検索ルールを関連付けたネイバー ゾーンとしてデバイスを追加する必要があります。

登録制限ポリシーの設定

「登録設定（Registration configuration）」ページ（**[設定（Configuration）] > [登録（Registration）] > [設定（Configuration）]**）を使用して、Expressway による登録の管理方法を制御します。

[制限ポリシー（Restriction policy）] オプションは、Expressway に登録できるエンドポイントの決定時に使用するポリシーを指定します。次のオプションがあります。

- *[なし（None）]*：どのエンドポイントも登録できます。
- *[許可リスト（Allow List）]*：[許可リスト（Allow List）] 内のエントリに一致するエイリアスを持つエンドポイントのみが登録できます。
- *[拒否リスト（Deny List）]*：[拒否リスト（Deny List）] のエントリに一致しない限り、すべてのエンドポイントが登録できます。
- *[ポリシーサービス（Policy service）]*：外部ポリシーサービスで許可された詳細を使用して登録するエンドポイントのみが登録できます。

デフォルトは [なし（None）] です。

また、*[許可リスト（Allow List）]* または *[拒否リスト（Deny List）]* を使用する場合は、適切な [登録許可リスト（Registration Allow List）] の設定 または [登録拒否リスト（Registration Deny List）] の設定 の設定ページに移動してリストを作成する必要があります。

すべての登録制限ポリシーの決定を外部サービスに照会する場合は、*[ポリシーサービス（Policy service）]* オプションを使用します。このオプションを選択すると、外部サービスの接続の詳細情報を指定できる一連の設定フィールドが新たに表示されます。外部サービスを使用するための登録ポリシーの設定を参照してください。

エイリアスの登録

デバイス認証についてプロセス（必要な場合）が完了した後、エンドポイントはそのエイリアスを Expressway に登録しようと試みます。

H.323

登録時に H.323 エンドポイントは次のうちの 1 つ以上を Expressway に提供します。

- 1 つ以上の H.323 ID
- 1 つ以上の E.164 エイリアス
- 1 つ以上の URI

登録済みの他のエンドポイントのユーザは、これらのエイリアスのいずれかをダイヤルすることでそのエンドポイントをコールできます。

- URI を使用して H.323 エンドポイントを登録することを推奨します。これにより、SIP エンドポイントは標準として URI を使用して登録されるため、SIP と H.323 間のインターワーキングが促進されます。
- 機密情報を公開するエイリアスは使用しないでください。H.323 の特性上、コールセットアップ情報は暗号化されていない形式で交換されます。

SIP

登録時に SIP エンドポイントは、連絡先アドレス（IP アドレス）と論理アドレス（レコードのアドレス）を Expressway に提供します。論理アドレスは、そのエンドポイントのエイリアスと見なされ、一般的に URI の形式をとります。

H.350 ディレクトリの認証と登録

Expressway が H.350 ディレクトリ サービスを使用して登録要求を認証する場合、**[登録用エイリアスの送信元（Source of aliases for registration）]** の設定を使用して、エンドポイントによる登録の試行を許可するエイリアスを特定します。詳細については、「「LDAP 経由の H.350 ディレクトリ サービス ルックアップの使用」」を参照してください。

既存のエイリアスを使用した登録の試行

エンドポイントは、システム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場合があります。これをどのように管理するかは、Expressway がどのように設定されているかと、エンドポイントが SIP か H.323 かによって異なります。

- **H.323**：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。この場合に Expressway の動作を制御するには、H.323 の設定ページ（**[設定（Configuration）]** > **[プロトコル（Protocols）]** > **[H.323]**）で **[登録競合モード（Registration conflict mode）]** を設定します。
- **SIP**：SIP エンドポイントには、別の IP アドレスからすでに使用されているエイリアスを使用した登録が常に許可されます。このエイリアス宛のコールを受信すると、そのエイリアスを使用して登録されているすべてのエンドポイントが同時にコールされます。この SIP 機能は「「フォーキング」」と呼ばれます。

登録のブロック

[登録拒否リスト（Registration Deny List）] の設定 を使用するように Expressway を設定している場合は、登録をブロックするオプションがあります。このオプションはそのエンドポイントが使用するすべてのエイリアスを [拒否リスト（Deny List）] に追加します。

既存の登録の削除

制限ポリシーはアクティブになると、その時点以降のすべての登録要求を制御します。ただし、既存の登録は、新しいリストがブロックしても、そのまま残ります。したがって、制限ポリシーを実装した後は、既存の不要な登録すべてを手動で削除することを推奨します。

登録を手動で削除するには、**[ステータス（Status）]** > **[登録（Registrations）]** > **[デバイスごと（By device）]** に移動し、削除する登録を選択して **[登録解除（Unregister）]** をクリックします。

登録されているデバイスがアクティブ コールに参加しており、その登録を削除した（または期限が切れた）場合、コールへの影響はプロトコルによって次のように異なります。

- **H.323**：コールが停止します。
- **SIP**：デフォルトでは、コールは有効な状態のままになります。SIP の動作は変更できますが、CLI で `xConfiguration SIP Registration Call Remove` コマンドを使用する必要があります。

再登録

すべてのエンドポイントは定期的に Expressway に再登録し、登録を有効状態に維持する必要があります。手動で登録を削除しない場合は、エンドポイントが再登録をしようとした時点で削除されますが、これは、エンドポイントが使用しているプロトコルによって次のように異なります。

- H.323 エンドポイントは「「軽量の」」再登録を使用することがあります。これには、最初の登録で提供されたすべてのエイリアスは含まれておらず、再登録が制限ポリシーによってフィルタリングされない可能性があります。この場合、登録は登録タイムアウト期間の終了時に期限切れにならないため、手動で削除する必要があります。
- SIP の再登録には、最初の登録と同じ情報が含まれるため、制限ポリシーによってフィルタリングされます。つまり、リストがアクティブになった後にすべての SIP アプリケーションが登録タイムアウト期間の終了時点で表示されなくなります。

再登録の頻度は、SIP の設定（**[設定（Configuration）] > [プロトコル（Protocols）] > [SIP]**）の **[登録制御（Registration controls）]** の設定と、[H.323]（**[設定（Configuration）] > [プロトコル（Protocols）] > [H.323]**）の **[存続時間（Time to live）]** の設定で決まります。

（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。

許可リストと拒否リストについて

エンドポイントが Expressway への登録を試行するときに、エイリアスのリストを提供します。Expressway が提供する登録を許可するエンドポイントを制御するための方法の 1 つは、**[制限ポリシー（Restriction policy）]** ページ（「登録制限ポリシーの設定」）を *[*許可リスト（*Allow List*）*]* または *[*拒否リスト（*Deny List*）*]* に設定してから、必要に応じて [許可リスト（Allow List）] か [拒否リスト（Deny List）] のエンドポイントのエイリアスのいずれかを含めることです。各リストには、最大で 2,500 のエントリを含めることができます。

エンドポイントが登録を試行すると、エイリアスのそれぞれが関連リストのパターンと比較され、一致するかどうかが確認されます。登録を許可または拒否するために [許可リスト（Allow List）] または [拒否リスト（Deny List）] に表示されるエイリアスは 1 つのみである必要があります。

たとえば、**[制限ポリシー（Restriction policy）]** が *[Deny List*（拒否リスト）*]* に設定されており、エンドポイントが 3 つのエイリアスを使用して登録しようとした場合にそのうちの 1 つが [Deny List（拒否リスト）] のパターンに一致していれば、そのエンドポイントの登録は拒否されます。同様に、**[制限ポリシー（Restriction policy）]** が *[Allow List*（許可リスト）*]* に設定されている場合にそれらすべてのエイリアスを使用した登録が許可されるには、エンドポイントのエイリアスの 1 つのみが [Allow List（許可リスト）] のパターンに一致する必要があります。

[許可リスト（Allow List）] と [拒否リスト（Deny List）] は相互に排他的です。使用できるのは常にどちらか 1 つです。また、サブゾーンの設定 レベルでも登録を制御できます。各サブゾーンの登録ポリシーは、サブゾーン メンバーシップ ルールを介して割り当てられた登録を許可または拒否するように設定できます。

[登録許可リスト（Registration Allow List）] の設定

「登録許可リスト（Registration Allow List）」ページ（[設定（Configuration）] > [登録（Registration）] > [Allow List（許可リスト）]）には、Expressway への登録が許可されるエンドポイントのエイリアスとエイリアスパターンが表示されます。登録を許可するには、[許可リスト（Allow List）] のエントリにエンドポイントのエイリアスの 1 つが一致している必要があります。

[許可リスト（Allow List）] を使用するには、「登録制限ポリシーの設定」ページにある *[Allow List（許可リスト）]* の **[制限ポリシー（Restriction policy）]** を選択する必要があります。

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
Description	エントリの任意の自由形式の説明。	
パターン タイプ（Pattern type）	**[パターン文字列（Pattern string）]** とエイリアスを一致させる方法。 次のオプションがあります。 *[完全一致（Exact）]*：エイリアスはパターン文字列に正確に一致する必要があります。 *[プレフィックス（Prefix）]*：エイリアスはパターン文字列で開始される必要があります。 *[サフィックス（Suffix）]*：エイリアスはパターン文字列で終了する必要があります。 *[正規表現（Regex）]*：パターン文字列は正規表現です。	パターンが特定のエイリアスに一致するかどうかは、パターンの効果の確認 ツール（**[メンテナンス（Maintenance）] > [ツール（Tools）] > [パターンの確認（Check pattern）]**）を使用してテストできます。
パターン文字列（Pattern string）	エイリアスと比較するパターン。	

[登録拒否リスト（Registration Deny List）] の設定

「登録拒否リスト（Registration Deny List）」ページ（[設定（Configuration）] > [登録（Registration）] > [Deny List（拒否リスト）]）は、Expressway への登録が許可されないエンドポイントのエイリアスとエイリアスパターンが表示されます。登録を拒否するには、[拒否リスト（Deny List）] のエントリにエンドポイントのエイリアスの 1 つのみが一致している必要があります。

[拒否リスト（Deny List）] を使用するには、登録制限ポリシーの設定ページにある *[Deny List（拒否リスト）]* の **[制限ポリシー（Restriction policy）]** を選択する必要があります。

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
Description	エントリの任意の自由形式の説明。	
パターン タイプ（Pattern type）	**[パターン文字列（Pattern string）]** とエイリアスを一致させる方法。 次のオプションがあります。 *[完全一致（Exact）]*：エイリアスはパターン文字列に正確に一致する必要があります。 *[プレフィックス（Prefix）]*：エイリアスはパターン文字列で開始される必要があります。 *[サフィックス（Suffix）]*：エイリアスはパターン文字列で終了する必要があります。 *[正規表現（Regex）]*：パターン文字列は正規表現です。	パターンが特定のエイリアスに一致するかどうかは、パターンの効果の確認 ツール（**[メンテナンス（Maintenance）]** > **[ツール（Tools）]** > **[パターンの確認（Check pattern）]**）を使用してテストできます。
パターン文字列（Pattern string）	エイリアスと比較するパターン。	

外部サービスを使用するための登録ポリシーの設定

すべての登録制限ポリシーの決定を外部サービスを参照するように登録ポリシーを設定するには、次の手順を実行します。

手順

ステップ 1 **[設定（Configuration）]** > **[登録（Registration）]** > **[設定（Configuration）]** に移動します。

ステップ 2 *[ポリシー サービス（Policy service）]* の **[制限ポリシー（Restriction policy）]** を選択します。

ステップ 3 フィールドを次のように設定します。

フィールド	説明	使用方法のヒント
[Protocol]	ポリシー サービスに接続するために使用するプロトコル。 デフォルトは *HTTPS* です。	ポリシー サービス サーバと通信を行う場合、Expressway は HTTP から HTTPS へのリダイレクトを自動的にサポートします。

フィールド	説明	使用方法のヒント
証明書検証モード（Certificate verification mode）	HTTPS を使用して接続すると、この設定は、ポリシー サーバが提示する証明書を検証するかどうかを制御します。 設定が [オン（On）] の場合、Expressway で HTTPS を使用してポリシー サーバに接続するには、Expressway にそのサーバのサーバ証明書を承認するルート CA 証明書がロードされている必要があります。また、証明書のサブジェクトの共通名またはサブジェクト代替名は次の **[サーバ アドレス（Server address）]** フィールドの 1 つに一致する必要があります。	Expressway のルート CA 証明書は（**[メンテナンス（Maintenance）]** > **[セキュリティ（Security）]** > **[信頼できる CA 証明書（Trusted CA certificate）]**）を選択してロードします。
HTTPS 証明書失効リスト（CRL）による確認（HTTPS certificate revocation list (CRL) checking）	CRL による確認で証明書を保護する場合は、このオプションを有効にし、手動で CRL ファイルをロードするか、または、自動 CRL 更新を有効にします。	> **[セキュリティ（Security）]** > **[CRL 管理（CRL management）]** に移動して、Expressway が CRL ファイルを更新する方法を設定します。
サーバ アドレス 1 ～ 3（Server address 1 - 3）	サービスをホストしているサーバの IP アドレスまたは完全修飾ドメイン名（FQDN）を入力します。アドレスに **:<port>** を追加することでポートを指定できます。	FQDN を指定する場合は、Expressway に FQDN を解決できる適切な DNS 設定が指定されていることを確認します。 復元力のために、最大 3 つのアドレスを指定できます。
パス	サーバのサービスの URL を入力します。	
ステータス パス（Status path）	**[ステータス パス（Status path）]** は、Expressway がリモート サービスのステータスを取得できる場所からのパスを特定します。 デフォルトはステータス（status）です。	ポリシーサーバは戻りステータス情報を提供する必要があります。ポリシー サーバのステータスと復元力を参照してください。

フィールド	説明	使用方法のヒント
ユーザ名（Username）	サービスにログインし、問い合わせするために Expressway が使用するユーザ名。	
[パスワード（Password）]	サービスにログインし、問い合わせをするために Expressway が使用するパスワード。	プレーン テキストの最大長は 30 文字です（後で暗号化されます）。
デフォルト CPL（Default CPL）	これは、サービスが使用できない場合に Expressway が使用するフォールバック CPL です。	デフォルト CPL を、たとえば、応答サービスまたは録音メッセージにリダイレクトするように変更できます。 詳細については、ポリシー サービスのデフォルト CPLを参照してください。

ステップ 4 [保存（Save）] をクリックします。

Expressway はポリシー サービス サーバに接続し、登録ポリシーの決定に必要なサービスを使用して開始する必要があります。

接続の問題は、このページに報告されます。このページの下部の **[ステータス（Status）]** エリアを確認し、追加の情報メッセージを **[サーバ アドレス（Server address）]** フィールドと照合します。

第 14 章

デバイス認証

ここでは、Expressway の認証ポリシーと、**[設定（Configuration）] > [認証（Authentication）]** メニューに表示されるページについて説明します。

デバイス認証について

デバイス認証では、デバイスまたは外部システムから Expressway に届く着信要求のクレデンシャルを検証します。これは、特定の機能を既知のユーザと信頼できるユーザ用に予約できるようにするために使用されます。

Mobile & Remote Access デバイス

Expressway を介して Unified CM に登録するデバイスの認証について、Expressway 上で明示的に設定する必要はありません。（外部 IdP ではなく）Expressway がこれらのデバイスの認証エージェントである場合は、ホーム Unified CM クラスタに対してこれらのデバイスの認証を自動的に処理します。

リッチ メディア セッション

リッチ メディア セッションに参加して、Expressway と通信するデバイスは、Expressway の設定可能な認証ポリシーの対象となります。

デバイス認証が有効になっている場合、その Expressway との通信を試みるデバイスはすべて、クレデンシャル（通常はユーザ名とパスワードに基づく）の提示を要求されます。Expressway はそれらのクレデンシャルをローカル データベースを使用するための認証の設定と照合します。

Expressway 認証ポリシーは、各ゾーンにそれぞれ独立して設定できます。つまり、認証済みと未認証の両方のデバイスに対して同じ Expressway への通信を必要に応じて許可することが可

能です。後続のコールルーティングの決定には、デバイスが認証されているかどうかに基づいたさまざまなルールを設定できます。

認証ポリシー（Authentication policy）

認証ポリシーの設定オプション

認証ポリシーの動作は、H.323 メッセージ、ローカル ドメインから受信した SIP メッセージ、および非ローカル ドメインから受信した SIP メッセージであるかによって異なります。

プライマリ認証ポリシーの設定オプションおよびそれぞれに関連付けられている動作は以下のとおりです。

- **[クレデンシャルを確認する（Check credentials）]**：該当する認証方式を使用してクレデンシャルを検証します。

  （注） 一部のシナリオでは、メッセージはチャレンジされません。以下を参照してください。

- **[クレデンシャルを確認しない（Do not check credentials）]**：クレデンシャルを確認せずに、メッセージを処理します。
- **[認証済みとして扱う（Treat as authenticated）]**：クレデンシャルを確認せず、認証済みであるかのようにメッセージを処理します。このオプションは、それぞれの登録メカニズム内で認証をサポートしていないサードパーティ サプライヤからのエンドポイントに対応するために使用できます。

  （注） 一部のシナリオでは、メッセージは許可されても、未認証であるかのように扱われることがあります。以下を参照してください。

認証ポリシーは、メッセージを受信しているかどうかに基づき、ゾーン タイプごとに選択して設定できます。

- デフォルト ゾーン、ネイバー ゾーン、トラバーサル クライアント ゾーン、トラバーサル サーバ ゾーン、およびユニファイド コミュニケーション トラバーサル ゾーンはすべて、認証ポリシーを設定できます。
- DNS ゾーンと ENUM ゾーンはメッセージを受信しないため、認証ポリシーの設定はありません。

ゾーンの [認証ポリシー（Authentication policy）] を編集するには、**[設定（Configuration）]** > **[ゾーン（Zones）]** > **[ゾーン（Zones）]** に移動して、ゾーンの名前をクリックします。新しい

ゾーンを作成すると、ポリシーはデフォルトで *[クレデンシャルを確認しない（Do not check credentials）]* に設定されます。

以下の表に示されているように、H.323 メッセージと SIP メッセージの動作は異なります。

H.323

ポリシー	動作
クレデンシャルを確認する（Check credentials）	メッセージは、メッセージ内のいずれかのクレデンシャルを認証データベースで確認できるかどうかによって、認証済みまたは未認証として分類されます。 クレデンシャルが提供されていない場合、メッセージは常に未認証として分類されます。
クレデンシャルを確認しない（Do not check credentials）	メッセージのクレデンシャルはチェックされず、すべてのメッセージが未認証として分類されます。
認証済みとして扱う（Treat as authenticated）	メッセージのクレデンシャルはチェックされず、すべてのメッセージが認証済みとして分類されます。

SIP

ゾーン レベルでの SIP メッセージの動作は、SIP 認証信頼 の設定によって異なります。つまり、Expressway が受信メッセージに含まれている P-Asserted-Identity ヘッダーと呼ばれる既存の認証済みインジケータを信頼するかどうか、およびメッセージをローカル ドメイン（Expressway が信頼するドメイン）から受信したか、非ローカル ドメインから受信したかによって異なります。

ポリシー	信頼性	ローカル ドメイン内	ローカル ドメインの外
クレデンシャルを確認する（Check credentials）	オフ（Off）	メッセージは認証をチャレンジされます。 認証に失敗したメッセージは拒否されます。 認証に合格したメッセージは認証済みとして分類され、P-Asserted-Identity ヘッダーがメッセージに挿入されます。	メッセージは認証をチャレンジされません。 すべてのメッセージが未認証として分類されます。 既存の P-Asserted-Identity ヘッダーは削除されます。

ポリシー	信頼性	ローカル ドメイン内	ローカル ドメインの外
	オン（On）	既存の P-Asserted-Identity ヘッダーがあるメッセージは、追加のチャレンジなしに認証済みとして分類されます。P-Asserted-Identity ヘッダーは変更されずに渡されます（発信者の Asserted IDを保持）。 既存の P-Asserted-Identity ヘッダーがないメッセージはチャレンジされます。認証に合格すると、メッセージは認証済みとして分類され、P-Asserted-Identity ヘッダーがメッセージに挿入されます。認証に失敗すると、メッセージは拒否されます。	メッセージは認証をチャレンジされません。 既存の P-Asserted-Identity ヘッダーがあるメッセージは、認証済みとして分類され、ヘッダーは変更されずに渡されます。 既存の P-Asserted-Identity ヘッダーがないメッセージは未認証として分類されます。
クレデンシャルを確認しない（Do not check credentials）	オフ（Off）	メッセージは認証をチャレンジされません。 すべてのメッセージが未認証として分類されます。 既存の P-Asserted-Identity ヘッダーは削除されます。	メッセージは認証をチャレンジされません。 すべてのメッセージが未認証として分類されます。 既存の P-Asserted-Identity ヘッダーは削除されます。
	オン（On）	メッセージは認証をチャレンジされません。 既存の P-Asserted-Identity ヘッダーがあるメッセージは、認証済みとして分類され、ヘッダーは変更されずに渡されます。 既存の P-Asserted-Identity ヘッダーがないメッセージは未認証として分類されます。	メッセージは認証をチャレンジされません。 既存の P-Asserted-Identity ヘッダーがあるメッセージは、認証済みとして分類され、ヘッダーは変更されずに渡されます。 既存の P-Asserted-Identity ヘッダーがないメッセージは未認証として分類されます。
認証済みとして扱う（Treat as authenticated）	オフ（Off）	メッセージは認証をチャレンジされません。 すべてのメッセージが認証済みとして分類されます。 既存の P-Asserted-Identity ヘッダーは削除され、Expressway の発信者 ID を含む新しいヘッダーがメッセージに挿入されます。	メッセージは認証をチャレンジされません。 すべてのメッセージが未認証として分類されます。 既存の P-Asserted-Identity ヘッダーは削除されます。

ポリシー	信頼性	ローカル ドメイン内	ローカル ドメインの外
	オン（On）	メッセージは認証をチャレンジされません。 すべてのメッセージが認証済みとして分類されます。 既存の P-Asserted-Identity ヘッダーがあるメッセージは変更されずに渡されます。既存の P-Asserted-Identity ヘッダーがないメッセージにはヘッダーが挿入されます。	メッセージは認証をチャレンジされません。 既存の P-Asserted-Identity ヘッダーがあるメッセージは、認証済みとして分類され、ヘッダーは変更されずに渡されます。 既存の P-Asserted-Identity ヘッダーがないメッセージは未認証として分類されます。

認証済みデバイスおよび未認証デバイスに対するシステム動作の制御

認証済みデバイスおよび未認証デバイスからのコールおよびその他のメッセージの処理方法は、検索ルール、外部ポリシー サービス、および CPL の設定内容によって異なります。

検索ルール

検索ルールを設定する場合は、**[要求は認証が必要（Request must be authenticated）]** 属性を使用して、検索ルールが認証済みの検索要求にのみ適用されるのか、またはすべての要求に適用されるのかを指定します。

外部ポリシー サービス

外部ポリシー サービスは、通常、Expressway 自体にポリシー ルールを設定するのではなく、外部の集中型サービスによってポリシー決定が管理される導入で使用されます。次の領域でポリシー サービスを使用するように、Expressway を設定できます。

- 登録制限ポリシーの設定
- 検索ルールの設定
- コール ポリシーの設定
- FindMe の設定

Expressway は、ポリシー サービスを使用するときに、コール要求または登録要求に関する情報を POST メッセージでそのサービスに送信します。その際、名前と値のペアで構成される一連のパラメータを使用します。それらのパラメータには、要求の送信元が認証済みソースかどうかの情報が含まれています。

Cisco Expressway シリーズ構成ガイドページの『*Cisco Expressway* 外部ポリシー導入ガイド』を参照してください。

CPL

Expressway でコール ポリシー ルール ジェネレータを使用している場合、送信元の照合は、認証済みソースに対して実行されます。未認証のソースに対する照合を指定するには、空白フィールドを使用します。（送信元が認証されていない場合、その値は信頼できません）。

手作業で作成し、アップロードしたローカル CPL を使用してコール ポリシーを管理する場合は、認証済みと未認証のいずれの発信元を調べるかについて CPL を明確にすることを推奨します。

- CPL で未認証の送信元を調べる必要がある場合（たとえば、非認証の発信者をチェックする場合）は、「`unauthenticated-origin`」を使用する必要があります。（ただし、未認証のユーザは、自らを好きなように呼ぶことができるため、このフィールドでは、発信者は確認されません）。
- 認証済みの送信元（認証済みデバイスまたは「「認証済みとして扱う」」デバイスでのみ可能）をチェックするには、CPL で「`authenticated-origin`」を使用する必要があります。

（注） CPL スクリプトの記述は複雑なため、代わりに外部ポリシーサービスを使用することを推奨します。

SIP 認証信頼

デバイス認証についてを使用するように設定されている Expressway では、着信の SIP INVITE 要求が認証されます。その後、Expressway からネイバー ゾーン（別の Expressway など）に要求が転送されると、受信システムでもその要求が認証されます。このシナリオでは、すべてのホップでメッセージを認証する必要があります。

デバイスのクレデンシャルが（最初のホップで）一度だけ認証され、ネットワーク内の SIP メッセージの数が減るように簡素化する場合は、**[認証信頼モード（Authentication trust mode）]** の設定を使用するようにネイバー ゾーンを設定できます。

この設定は、ゾーンの認証ポリシーと組み合わせて使用されて、該当ゾーンから受信した事前認証済みの SIP メッセージが信頼されているかどうか、その後、Expressway 内で認証済みまたは未認証として扱われるかを制御します。事前認証済みの SIP 要求は、RFC 3326 で定義されている SIP メッセージ ヘッダー内の P-Asserted-Identity フィールドの存在によって識別されます。

[認証信頼モード（Authentication trust mode）] の設定は次のとおりです。

- *[オン（On）]*：事前認証済みメッセージは追加のチャレンジなしに信頼され、その後、Expressway内では認証済みとして扱われます。未認証メッセージは、**[認証ポリシー（Authentication policy）]** が *[クレデンシャルを確認する（Check credentials）]* に設定されている場合はチャレンジされます。
- *[オフ（Off）]*：既存の認証済みインジケータ（P-Asserted-Identityヘッダー）はすべてメッセージから削除されます。ローカル ドメインからのメッセージは、**[認証ポリシー**

（**Authentication Policy**）] が *[*クレデンシャルを確認する（*Check credentials*）*]* に設定されている場合はチャレンジされます。

（注）
- 認証信頼は、ネイバーゾーンが信頼できるSIPサーバのネットワークの一部である場合のみ有効にすることを推奨します。
- 認証信頼は、トラバーサル サーバ ゾーンとトラバーサル クライアント ゾーンの間では自動的に暗示されます。

デバイス プロビジョニングと認証ポリシー

プロビジョニング サーバが受信するプロビジョニング要求または電話帳要求は、Expressway へのゾーンまたはサブゾーン エントリ ポイントにおいて、すでに認証されている必要があります。プロビジョニング サーバは、自分自身で認証チャレンジを行うことはありません。未認証のメッセージはすべて拒否されます。

Expresswayには、適切なデバイス認証設定が行われている必要があります。そうでなければ、プロビジョニング関連のメッセージは拒否されます。

- （サブスクライブ メッセージ）の初期プロビジョニングの認証は、デフォルト ゾーンの認証ポリシーの設定によって制御されます（デバイスがまだ登録されていないので、デフォルト ゾーンが使用されます）。
- デフォルトゾーンおよびトラバーサルクライアントゾーンの認証ポリシーは、*[*クレデンシャルを確認する（*Check credentials*）*]* または *[*認証済みとして扱う（*Treat as authenticated*）*]* のいずれかに設定されている必要があります。そうでなければ、プロビジョニング要求は失敗します。

それぞれの場合に、Expressway はその認証をローカル データベースと照合して検査を実行します。これには Cisco TMS によって提供されるすべてのクレデンシャルが含まれます。

一般的なプロビジョニング設定の詳細については、『Cisco TMS Provisioning Extension 導入ガイド』を参照してください。

認証方式

ローカル データベースを使用するための認証の設定

ローカル認証データベースは、Expressway システムの一部として組み込まれているため、固有の接続設定は必要ありません。ユーザアカウントの認証クレデンシャルを保存するために使用されます。各クレデンシャルのセットは**名前**と**パスワード**で構成されます。

ローカル データベース内のクレデンシャルは、デバイス（SIP）、トラバーサル クライアント、および TURN クライアントの認証に使用できます。

ローカル データベースへのクレデンシャルの追加

デバイス クレデンシャルのセットを入力するには、次の手順を実行します。

1. **[設定（Configuration）]** > **[認証（Authentication）]** > **[デバイス（Devices）]** > **[ローカル データベース（Local Database）]** に移動し、**[新規（New）]** をクリックします。
2. デバイスのクレデンシャルを表す**名前**と**パスワード**を入力します。
3. **[クレデンシャルの作成（Create credential）]** をクリックします。

（注） 2 台以上のデバイスで同じクレデンシャルを使用することができます。

Cisco TMS 内で管理されるクレデンシャル（デバイス プロビジョニング用）

Expressway が TMS Provisioning Extension サービスを使用している場合、ユーザ サービスから提供されたクレデンシャルは、手動で設定されたエントリとともに、ローカル認証データベースに保存されます。**[ソース（Source）]** カラムにより、ユーザ アカウント名が **TMS** から提供されたものか、**ローカル** エントリであるかが識別されます。編集できるのは、**ローカル** エントリのみです。

ローカル データベース内に Cisco TMS のクレデンシャルを組み込むことで、Expressway は Cisco TMS 内で使用されている同一のクレデンシャルのセットと照合して（プロビジョニング要求だけではなく）すべてのメッセージを認証できます。

H.350 ディレクトリ認証と組み合わせたローカル データベース認証

Expressway は、ローカル データベースと H.350 ディレクトリの両方を使用するように設定できます。

H.350ディレクトリが設定されている場合、Expresswayは、提示されたダイジェストクレデンシャルを検証する際は常に、最初にローカルデータベースと照合してから、H.350ディレクトリと照合します。

Active Directory（直接）認証と組み合わせたローカル データベース認証

Active Directory（直接）認証が設定されていて、[NTLM プロトコル チャレンジ（NTLM protocol challenges）] が *[自動（Auto）]* に設定されている場合、NTLM をサポートするデバイスに NTLM 認証チャレンジが提供されます。

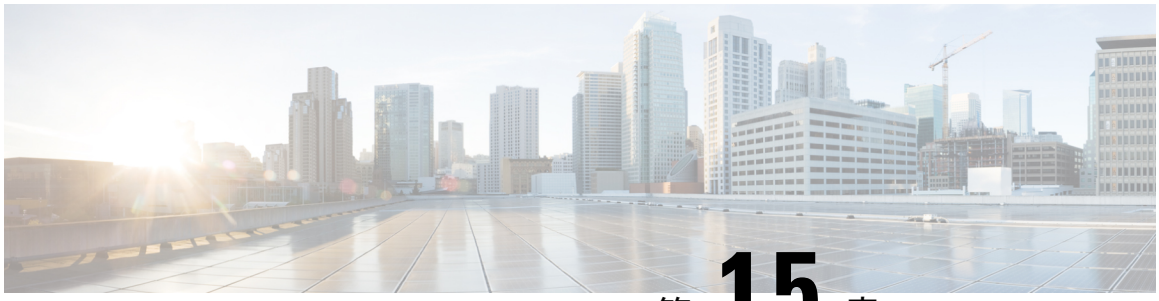
- NTLM チャレンジは標準のダイジェスト チャレンジに加えて提供されます。
- NTLM をサポートするエンドポイントは、ダイジェスト チャレンジに優先して NTLM チャレンジに応答します。Expressway は、その NTLM 応答の認証を試みます。

外部システムによる認証

「アウトバウンド接続クレデンシャル（Outbound connection credentials）」ページ（**[設定（Configuration）]>[認証（Authentication）]>[アウトバウンド接続クレデンシャル（Outbound connection credentials）]**）は、外部システムとの認証が必要な場合にExpresswayが常に使用するユーザ名とパスワードを設定するために使用します。

たとえば、Expressway がエンドポイントから他の Expressway に招待を転送している場合、その別のシステムで認証が有効になっているために、ローカルExpresswayがユーザ名とパスワードをそのシステムに提供する必要があることがあります。

（注） これらの設定はトラバーサルクライアントゾーンでは使用されません。接続前に、トラバーサル サーバと常に認証する必要があるトラバーサル クライアントでは、トラバーサル クライアント ゾーンごとに接続のクレデンシャルを設定します。



第 15 章

ゾーンとネイバー

ここでは、Expressway でゾーンとネイバーを設定する方法について説明します（**[設定（Configuration）] > [ゾーン（Zones）]**）。

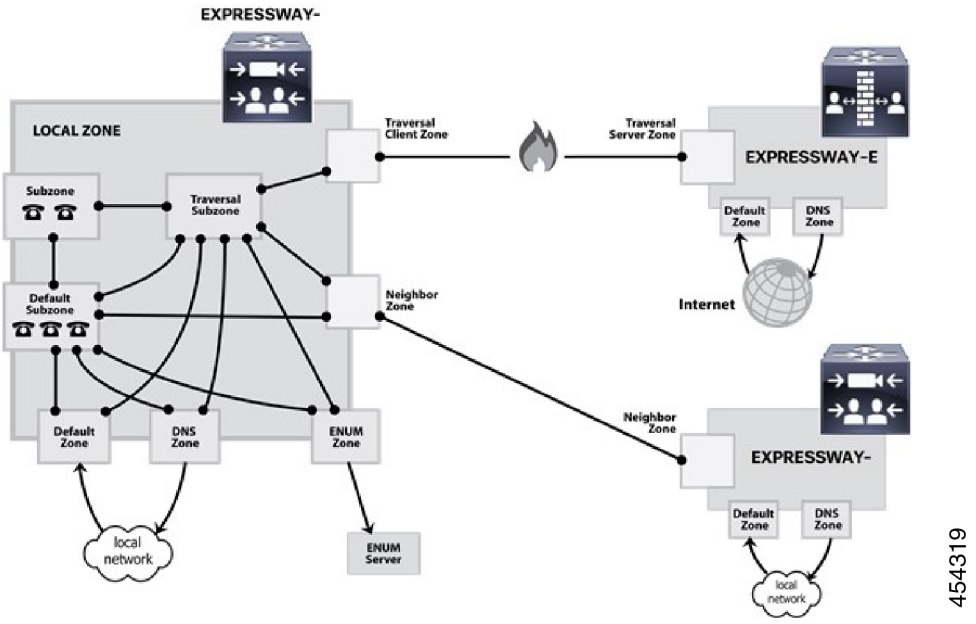
ビデオ ネットワークの基礎

このセクションでは、Expressway のビデオ通信ネットワークに関するさまざまな部分とその接続方法について概説します。

最も基本的な実装は、インターネットに接続する、1 つ以上のエンドポイントが登録された単一の Expressway です。企業の規模と複雑性に応じて、Expressway はエンドポイント ネットワーク、他の Expressway、および他のネットワーク インフラストラクチャ デバイスの一部となっており、Expressway とインターネットの間に 1 つ以上のファイアウォールがある場合があります。（そのような場合に、ネットワークの別の部分によって使用される、またはそれらの間で使用される帯域幅の量に制約を適用することができます。）

図は、Expressway の導入例に対応するさまざまなサブゾーンとゾーンを示しています。リンクによって接続されている複数のサブゾーンを設定する方法を示すために、ローカルゾーンの例として Expressway-C を使用しています。ローカル ゾーンは外部の Expressway およびインターネットと、特定のタイプのゾーンを通じて接続されています。

図 *14 :* ネットワーク構成図の例



ダイヤル プランの構築

複数の Expressway の導入を開始するにあたっては、登録済みのエンドポイントについて相互に照会できるようにシステムをまとめて隣接させると便利です。開始する前に、ダイヤルプランの構築方法を検討してください。これによって、エンドポイントに割り当てるエイリアスや、Expressway を隣接させる方法が決定します。選択するソリューションは、システムの複雑性によって異なります。以降の項では、考えられるオプションのいくつかを説明します。

フラット ダイヤル プラン

最もシンプルなアプローチは、各エンドポイントに一意のエイリアスを割り当ててエンドポイントの登録を Expressway 間で分割することです。各 Expressway は、他のすべての Expressway でネイバー ゾーンとして設定されます。1 つの Expressway が、その Expressway に登録されていないエンドポイント宛のコールを受信すると、ロケーション要求を他のすべてのネイバー Expressway に送信します。

概念的にはシンプルですが、このタイプのフラット ダイヤル プランの拡張性はあまり高くありません。Expressway の追加や移動には、すべての Expressway の設定を変更する必要があり、1 回のコール試行が多数のロケーション要求を発生させる可能性があります。したがって、このオプションは、1 つまたは 2 つの Expressway とそのピアのみでの導入に最も適しています。

構造化ダイヤル プラン

構造化ダイヤルプランを使用して導入することもできます。このプランでは、登録するシステムに基づいてエンドポイントにエイリアスが割り当てられます。

E.164エイリアスを使用している場合、各Expresswayにはエリア コードが割り当てられます。Expresswaysをまとめて隣接させると、ネイバー ゾーンには対応するエリア コードで設定された検索ルールがプレフィックスとして割り当てられます（*[エイリアス パターン マッチ（Alias pattern match）]* の **[モード（Mode）]** および *[プレフィックス（Prefix）]* の **[パターン タイプ（Pattern type）]**）。そのネイバーは、そのプレフィックスで開始する番号へのコールのみを照会します。

ダイヤルプランに基づくURIでは、必要なドメイン名に一致するサフィックスを持つネイバーごとに検索ルールを設定することによって同様の動作を得ることができます。

エンドポイントをサブスクライバ番号（E.164 番号の最後の部分）のみで登録すると有効な場合があります。その場合、そのゾーンにクエリを送信する前にプレフィックスを除去するように検索ルールを設定できます。

構造化ダイヤルプランは、コールを試行するときに発行するクエリの数を最小限に抑えます。ただし、この場合も、導入環境内のすべての Expressway による完全に接続されたメッシュが必要です。階層型ダイヤル プランはこれを簡略にします。

階層型ダイヤル プラン

このタイプの構造では、1 つの Expressway をその導入環境の中央ディレクトリ Expressway として指定し、他のすべての Expressway をその中央ディレクトリ Expressway と隣接させます。

- ディレクトリ Expresswayは、近傍ゾーンとしての各 Expressway を、*[エイリアスパターン マッチ（Alias pattern match）]* の **[モード（Mode）]**と**パターン文字列**としてターゲット Expresswayのプレフィックス（構造化ダイヤルプランの場合）を持つ各ゾーンに対応する検索ルールを設定します。
- 各 Expressway には、近傍ゾーンとしてのディレクトリ Expressway が設定されています。また、*[任意のエイリアス（Any alias）]* の **[モード（Mode）]** を使用する検索ルールとディレクトリ Expressway の **[ターゲット（Target）]** を設定します。

導入環境でデバイス認証を使用していない場合は、すべての Expressway をお互いに隣接させる必要はありません。この時点で新しい Expressway を追加するには、その新しい Expressway とディレクトリ Expressway で設定を変更する必要があります。デバイス認証（下記を参照）を使用している場合は、Expressway を互いに隣接させなければならない場合があります。

この場合、ディレクトリ Expressway に障害が発生すると、通信が大幅に途絶される可能性があります。復元力を引き上げるためにクラスタについての使用を検討してください。

階層型ダイヤル プラン（ディレクトリ Expressway）の導入とデバイス認証

階層型ダイヤルプラン内での認証ポリシーの設定方法に関する重要な情報については、「階層型ダイヤル プランと認証ポリシー」を参照してください。

ゾーンについて

ゾーンはエンドポイントの集合であり、1 つのシステムにすべて登録されているか、そうでない場合は ENUM や DNS ルックアップなどの特定の方法で見つかります。ゾーンには、次を含む多くの機能があります。

- コールをこれらのゾーンの間で使用できるかどうかに関するリンク経由での制御。
- ローカルサブゾーンと他のゾーンのエンドポイント間のコールの帯域幅の管理。
- ローカルに登録されていないエイリアスの検索。
- デバイス認証についての設定による、そのゾーン内のエンドポイントが使用できるサービスの制御。
- そのゾーンで送受信する SIP コールのメディア暗号化ポリシーの設定と ICE メッセージング サポートの設定 機能の制御。

最大 1,000 のゾーンを設定できます。各ゾーンは、次のゾーン タイプのいずれかとして設定します。

- ネイバー ゾーンの設定：ローカル Expressway のネイバー システムへの接続
- トラバーサル クライアント ゾーンの設定：ローカル Expressway は接続されているシステムのトラバーサル クライアントであり、それら 2 つの間にはファイアウォールがあります。
- トラバーサル サーバ ゾーンの設定：ローカル Expressway は接続されているシステムのトラバーサル サーバであり、それら 2 つの間にはファイアウォールがあります。
- ENUM ゾーンの設定：ゾーンには、ENUM ルックアップで検出されたエンドポイントが含まれています。
- DNS ゾーンの設定：ゾーンには、ENUM ルックアップで検出されたエンドポイントが含まれています。
- ユニファイドコミュニケーションの前提条件：モバイルおよびリモートアクセスや Jabber Guest などのユニファイドコミュニケーション機能に使用するトラバーサルクライアント ゾーンまたはトラバーサルサーバ ゾーン

また、Expressway には事前に設定されたデフォルト ゾーンの設定もあります。

- すべてのゾーン タイプに使用できる設定オプションについては、ゾーンの設定（デフォルト以外のゾーン）の項を参照してください。
- 検索ルールのターゲットとしてゾーンを含める方法については、検索ルールの設定の項を参照してください。

自動的に生成されたネイバー ゾーン

Expressway は設定できない一部のネイバー ゾーンを自動的に生成します。

- システムがモバイルおよびリモート アクセスの概要用に設定されている場合、Expressway-C は、自身と検出された各 Unified CM ノード間にネイバー ゾーンを自動的に生成します。
- Microsoft の相互運用性についてサービスが有効になっている場合、Expressway は「「To Microsoft destination via B2BUA」」というネイバー ゾーンを自動的に生成します。
- Unified CM 上で SIP OAuth モードが有効になっている場合、Expressway は、自身と検出された各 Unified CM ノード間に「「CEOAuth <Unified CM name>」」という名前のネイバー ゾーンを自動的に生成します。

ICE メッセージング サポートの設定

[ICE サポート（ICE support）] オプションはゾーン単位の設定であり、Expressway がそのゾーン内で SIP デバイスと送受信する ICE メッセージをサポートする方法を制御します。

この動作は、着信（入力）と発信（出力）ゾーンまたはサブゾーンの **[ICE サポート（ICE support）]** の設定によって異なります。設定の不一致（一方は *[オン（On）]*、もう一方は *[オフ（Off）]*）がある場合、Expressway はバック ツー バック ユーザ エージェント（B2BUA）を呼び出して、関連ホストと ICE ネゴシエーションを実行します。

すべてのゾーンはデフォルトで **[ICE サポート（ICE support）]** が *[オフ（Off）]* に設定されます。

B2BUA がホストと ICE ネゴシエーション を実行する際に TURN リレーの候補アドレスを提供することができます。これを行うには、TURN サーバのアドレスで設定する必要があります（**[アプリケーション（Applications）] > [B2BUA] > [B2BUA TURN サーバ（B2BUA TURN servers）]**）。

次のマトリックスで、たとえば、ゾーン A とゾーン B 間のコールを処理するときの **[ICE サポート（ICE support）]** 設定の考えられるさまざまな組み合わせでの Expressway 動作を示します。

ICE サポートの設定	ゾーン A	
	オフ（Off）	オン（On）

ゾーン B	**オフ**	標準的な Expressway のプロキシ動作。 B2BUA は通常は呼び出されません（ただし、メディア暗号化ポリシーについては下記の注を参照してください）。	B2BUA が呼び出されます。 B2BUA は、ゾーン A のホストへのメッセージ内に ICE 候補を組み込みます。
	オン	B2BUA が呼び出されます。 B2BUA は、ゾーン B のホストへのメッセージ内に ICE 候補を組み込みます。	標準的な Expressway のプロキシ動作。 B2BUA は通常は呼び出されません（ただし、メディア暗号化ポリシーについては下記の注を参照してください）。

ICE サポートと組み合わせた場合のメディア暗号化ポリシーの影響

Expressway は、メディア暗号化ポリシーの設定（253 ページ）（自動以外の暗号化設定）を適用する必要がある場合は、B2BUA も呼び出します。次の表に、入力ゾーンと出力ゾーンの ICE サポートとメディア暗号化モードに依存する ICE ネゴシエーションの動作への影響を示します。

ICE サポート（ICE support）	**メディア暗号化モード（Media encryption mode）**	**B2BUA の呼び出し**	**ICE ネゴシエーションへの影響**
両方のゾーン = [オフ（Off）]	少なくとも 1 つのゾーンは、*[自動（Auto）]* **ではありません。**	○	B2BUA はどのホストとも ICE ネゴシエーションを実行しません。
両方のゾーン = [オン（On）]	少なくとも 1 つのゾーンは、*[自動（Auto）]* **ではありません。**	○	B2BUA は両方のホストと ICE ネゴシエーションを実行します。
両方のゾーン = [オン（On）]	両方のゾーン = [自動（Auto）]	なし	Expressway は ICE 対応のどのホストにも TURN リレーの候補アドレスを提供しません。 **（注）** 各ホストのデバイスはすでに TURN リレー候補アドレスを使用してプロビジョニングされている場合があります。

（注）

- B2BUA でルーティングされたコールは、コンポーネント タイプ *B2BUA* としてコール履歴で識別されます。
- 登録されたエンドポイントでコールを発信する場合を除き、暗号化 B2BUA を介してコールが実行される場合は、1 つの RMS コールライセンスが使用されます。
- B2BUA を介してルーティングが可能な同時発生コールは 100（ハードウェア アプライアンスおよび仮想マシンのオプションでは 500 コール）の制限があります。

メディア暗号化ポリシーの設定

メディア暗号化ポリシーの設定では、Expressway を通過する SIP コールのメディア暗号化機能を選択的に追加または削除できます。これにより、たとえば、パブリック インターネットから Expressway-E に発着信するすべてのトラフィックを暗号化し、プライベート ネットワーク内では暗号化を解除するようにシステムを設定できます。

- ポリシーはゾーン/サブゾーン単位で設定され、そのゾーン/サブゾーンのコールの発着信のレッグにのみ適用されます。
- 暗号化は、他のレッグが H.323 の場合でも、コールの SIP レッグに適用されます。

メディア暗号化ポリシーは、各ゾーンとサブゾーンの**[メディア暗号化モード（Media encryption mode）]**設定を通じて設定されます。ただし、結果のコールの暗号化ステータスもターゲット システム（エンドポイントや別の Expressway など）の暗号化ポリシーの設定によって異なります。

暗号化モードのオプションは次のとおりです。

- *[*強制暗号化（*Force encrypted*）*]*：ゾーン/サブゾーンで送受信するすべてのメディアが暗号化されます。暗号化を使用しないようにターゲット システム/エンドポイントを設定している場合は、コールは破棄されます。
- *[*強制暗号化解除（*Force unencrypted*）*]*：すべてのメディアの暗号化が解除されます。暗号化を使用するようにターゲットシステム/エンドポイントが設定されている場合は、コールが破棄される可能性があります。*[*ベストエフォート（*Best effort*）*]* を使用するように設定されている場合は、コールは暗号化されていないメディアにフォールバックします。
- *Best Effort*：使用可能な場合は暗号化を使用します。使用できない場合は暗号化されていないメディアにフォールバックします。
- *[*自動（*Auto*）*]*：特定のメディア暗号化ポリシーが Expressway によって適用されることはありません。メディア暗号化は、ターゲット システム/エンドポイントの要求にのみ依存します。これはデフォルト動作で、この機能が導入される前の Expressway の動作と同等です。

暗号化ポリシー（[自動（Auto）]以外の暗号化の設定）は、Expressway でホストされるバックツーバック ユーザ エージェント（B2BUA）を通じてルーティングされたコールに適用されます。

（注） メディア暗号化を使用するためにシステムを設定する際は、次のことを覚えておいてください。

- 暗号化モードが *[強制暗号化（Force encrypted）]* または *[強制暗号化解除（Force unencrypted）]* のゾーンは、SIP 専用ゾーンとして設定する必要があります（そのゾーンでは H.323 を無効にする必要があります）。
- 暗号化モードを *[強制暗号化（Force encrypted）]* または *[ベスト エフォート（Best effort）]* にする必要がある場合は、TLS 転送を有効にする必要があります。
- B2BUA を通じてルーティングしたコール コンポーネントは、コンポーネント タイプが B2BUA であるため、コール履歴の詳細情報で特定できます。
- B2BUA がメディアを利用する必要がある場合、各コールはトラバーサルコールとして分類され、したがって、両方のエンドポイントがシスコのインフラストラクチャに登録されている場合を除き、Rich Media Session（RMS）ライセンスが使用されます。
- Expressway ごとに同時発生ビデオコールは 100（ハードウェア アプライアンスおよび仮想マシンのオプションでは 500 ビデオコール）という制限があり、これにはメディア暗号化ポリシーを適用できます。
- B2BUA は、ICE メッセージング サポートの設定が有効になっている場合でも呼び出せます。

メディア暗号化用の B2BUA の設定

暗号化（および ICE サポート）に使用する B2BUA は、Microsoft 相互運用性に使用する B2BUA とは異なるインスタンスです。Microsoft 相互運用性サービス B2BUA は手動で設定して有効にする必要がありますが、暗号化に使用する B2BUA は暗号化ポリシーが適用されている場合は常に自動で有効になります。

ローカル ゾーンとサブゾーンについて

Expressway に登録されているすべてのデバイスの集合は、その**ローカル ゾーン**を構成します。

ローカル ゾーンは**サブゾーン**に分割されます。これには、自動的に作成された**デフォルトのサブゾーン**と、最大 1,000 個の手動設定が可能なサブゾーンが含まれます。

エンドポイントを Expressway に登録すると、そのエンドポイントはサブゾーンのメンバーシップ ルールに基づいて適切なサブゾーンに割り当てられます。これらのルールは各サブゾーンの IP アドレスまたはエイリアスのパターンマッチの範囲を指定します。エンドポイントの IP ア

ドレスまたはエイリアスがメンバーシップルールのいずれにも一致しない場合は、デフォルトサブゾーンに割り当てられます。

ローカル ゾーンはネットワーク トポロジとは関係ない場合があり、複数のネットワーク セグメントを構成することがあります。また、Expressway には2つの特殊なタイプのサブゾーンがあります。

- トラバーサル サブゾーンについて。これは常に存在します。
- クラスタ サブゾーンについて。これは常に存在しますが、Expressway がクラスタの一部の場合にのみ使用されます。

帯域幅管理

ローカルゾーンのサブゾーンは帯域幅の管理に使用します。サブゾーンを設定した後に、帯域幅制限を次のコールに適用できます。

- サブゾーン内の 2 つのエンドポイント間の個々のコール。
- サブゾーン内のエンドポイントとそのサブゾーン外の別のエンドポイント間の個々のコール。
- サブゾーン内のエンドポイントで送受信するコールの総数。

サブゾーンの作成および設定方法、およびデフォルト サブゾーンとトラバーサル サブゾーンなどのサブゾーンに帯域幅制限を適用する方法の詳細については、帯域幅制御についての項を参照してください。

登録、認証、およびメディア暗号化のポリシー

帯域幅管理の他に、Expressway の登録、認証、およびメディア暗号化のポリシーを制御するためにもサブゾーンを使用します。

これらの設定方法の詳細については、サブゾーンの設定を参照してください。

ローカル ゾーンの検索

Expressway の機能の 1 つは、ローカルに登録したエンドポイントまたは外部ゾーンから受信したコールを適切な宛先にルーティングすることです。コールは宛先エンドポイントのアドレスまたはエイリアスに基づいてルーティングされます。

Expressway はローカル ゾーンと設定された外部ゾーンの宛先のエンドポイントを検索します。検索するアドレスやエイリアスに基づいて、これらのゾーンを検索する順序にプライオリティを設定したり、各ゾーンに送信された検索要求をフィルタリングしたりできます。これにより、ローカル ゾーンや外部ゾーンに送信する検索要求の潜在的な数を削減し、検索プロセスの速度を速めることができます。

ローカルゾーンの検索ルールの設定方法の詳細については、「検索ルールの設定」の項を参照してください。

デフォルト ゾーンの設定

デフォルト ゾーンは、登録されていないか、または認識されておらず、ローカル ゾーンまたは既存の設定済みのゾーンのいずれかに属しているエンドポイントまたはその他のデバイスからの着信コールを表します。

Expressway には、デフォルト ゾーンおよびデフォルト ゾーンとトラバーサル サブゾーン間のデフォルト リンクが事前に設定されています。デフォルト ゾーンは削除できません。

デフォルト ゾーンの設定

デフォルト ゾーンを設定することによって、認識されていないシステムやエンドポイントからのコールを Expressway がどのように処理するかを制御できます。**[設定（Configuration）]** > **[ゾーン（Zones）]** > **[ゾーン（Zones）]** に移動し、**[デフォルト ゾーン（DefaultZone）]** をクリックします。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
認証ポリシー（Authentication policy）	**[認証ポリシー（Authentication policy）]** の設定で、Expressway がデフォルト ゾーンへの着信メッセージにどのように対処するかを制御します。	詳細 については、認証ポリシー（Authentication policy）を参照してください。
メディア暗号化モード（Media encryption mode）	**[メディア暗号化モード（Media encryption mode）]** の設定では、デフォルト ゾーンを通過する SIP コール用のメディア暗号化機能を設定します。	詳細については、メディア暗号化ポリシーの設定を参照してください。
ICE サポート（ICE support）	このゾーン内のデバイスで ICE メッセージをサポートするかどうかを制御します。	詳細については、ICE メッセージング サポートの設定を参照してください。

フィールド	説明	使用方法のヒント
デフォルト ゾーンで相互 TLS を有効にする（Enable Mutual TLS on Default Zone）	*[オン（On）]* で、MTLS（Mutual Transport Layer Security）がデフォルト ゾーンを通じた着信接続に適用されます。 *[オフ（Off）]* は、MTLS が TLS ポートへの接続に適用されていないことを意味します。専用 MTLS ポートへの接続がある場合、そのポートが **[設定（Configuration）] > [プロトコル（Protocols）] > [SIP]** で有効にされていれば、MTLS は依然として適用されます。 デフォルト：[オフ（Off）]	この設定は、デフォルト ゾーンへの他の接続（H.323、SIP UDP、または SIP TCP）に影響しません。 （注） B2BUA はクライアント証明書の検査を実行できません。MTLS が TLS ポート 5061 で設定されているときに B2BUA を実行すると、コールは失敗します。TLS と MTLS をさまざまなポートで有効にすることを推奨します（**[プロトコル（Protocols）] > [SIP]** のページを使用）。 MTLS にポート 5061 を使用する必要がある場合、B2BUA の実行を避ける必要があります。そのためには、コール パスのすべてのゾーンで **[メディア暗号化モード（Media encryption mode）]** を *[自動（Auto）]* に切り替えます。

アクセスと帯域幅を管理するためのリンクとパイプの使用

認識されていないシステムやエンドポイントからのコールも、デフォルト ゾーンに関連付けられた「リンク」と「パイプ」を設定することで管理できます。たとえば、既定のリンクを削除して、認識されていないエンドポイントから着信コールが発信されないようにしたり、既定のリンクにパイプを適用したりすることで、認識されないエンドポイントからの着信コールに消費される帯域幅を制御できます。

デフォルト ゾーンのアクセス ルールの設定

デフォルト ゾーンのアクセス ルールを作成し（**[設定（Configuration）]> >[ゾーン（Zones）]> [デフォルト ゾーンのアクセス ルール（Default Zone access rules）]**）、デフォルト ゾーンを介して SIP TLS から Expressway への接続を許可する外部システムを制御します。

ルールごとに、パターンを指定し、外部システムから受信した証明書の CN（および SAN）と照合して比較します。次に、照合する証明書を提供するシステムへのアクセスを許可するか拒否するかを選択します。最大 10,000 のルールを設定できます。

表 *14*：デフォルトのゾーンアクセスルールパラメータ

フィールド	説明	使用方法のヒント
名前（Name）	ルールに割り当てられる名前。	
Description	ルールの任意の自由形式の説明	
優先度（Priority）	証明書名が複数のルールに一致する場合に適応するルールの順序を決定します。最も高いプライオリティ（1、2、3 の順）を持つルールが最初に適用されます。同じプライオリティの複数のルールが設定順序に適用されます。	
パターン タイプ（Pattern type）	**[パターン文字列（Pattern string）]** と証明書内に含まれる [サブジェクト共通名（Subject Common Name）] または [サブジェクト代替名（Subject Alternative Names）] を一致させる方法。 *[完全一致（Exact）]*：文字列全体が名前と 1 文字も違うことなく完全に一致する必要があります。 *[プレフィックス（Prefix）]*：文字列が名前の先頭に表示される必要があります。 *[サフィックス（Suffix）]*：文字列が名前の末尾に表示される必要があります。 *[正規表現（Regex）]*：文字列を正規表現として処理します。	パターンが特定の名前に一致するかどうかは、パターンの効果の確認 ツール（**[メンテナンス（Maintenance）] > [ツール（Tools）] > [パターンの確認（Check pattern）]**）を使用してテストできます。
パターン文字列（Pattern string）	名前を比較するパターン。	
アクション（Action）	証明書がこのアクセス ルールに一致する場合に実行するアクション。 *[許可（Allow）]*：外部システムがデフォルト ゾーンを介して接続することを許可します。 *[拒否（Deny）]*：外部システムから受信した接続要求を拒否します。	

フィールド	説明	使用方法のヒント
状態（State）	ルールが有効になっているかどうかを示します。	この設定を使用して設定変更をテストしたり、特定のルールを一時的に無効にします。ルール リストには無効にしたルールが表示されますが、無視されます。

ゾーンの設定（デフォルト以外のゾーン）

[ゾーン（Zones）]ページ（**[設定（Configuration）]**>**[ゾーン（Zones）]**>**[ゾーン（Zones）]**）には、Expressway で設定したすべてのゾーンのリストが表示されます。このページで、ゾーンの作成、編集、および削除を行えます。リスト内のゾーンで、コールの数、使用される帯域幅、プロキシ経由の登録の数、プロトコルのステータス、検索ルールのステータスに関する情報が表示されます。

H.323 または SIP ステータス オプションは次のとおりです。

- *[オフ（Off）]*：ゾーンまたはシステムのどちらかでプロトコルが無効になっています。
- *[アクティブ（Active）]*：そのゾーンに対してプロトコルが有効になっており、1 つ以上の接続がアクティブになっています。複数の接続を設定し、それらの接続の一部が失敗した場合は、アクティブな接続数が表示されます。
- *[オン（On）]*：そのゾーンに対してプロトコルが有効になっていることを示します（アクティブな接続がないゾーン タイプ（たとえば、DNS ゾーンや ENUM ゾーンなど）の場合）。
- *[失敗（Failed）]*：そのゾーンに対してプロトコルが有効になっていますが、接続に失敗しました。
- *[チェック中（Checking）]*：そのゾーンに対してプロトコルが有効になっており、現在、システムが接続を確立しようとしています。

ローカル Expressway にゾーンを設定して、別のシステム（別の Expressway やゲートキーパーなど）と隣接させる、ファイアウォールを越えてトラバーサル サーバまたはトラバーサル クライアントへの接続を作成する、あるいは ENUM または DNS ルックアップを使用してエンドポイントを検出します。使用できるゾーン タイプは次のとおりです。

- ネイバー ゾーンの設定：ローカル Expressway をネイバーシステムに接続します。
- トラバーサル クライアント ゾーンの設定：ローカル Expressway をトラバーサルサーバに接続します。
- トラバーサル サーバ ゾーンの設定：ローカル Expressway-E をトラバーサルクライアントに接続します。

- ENUM ゾーンの設定：ローカル Expressway を介して ENUM ダイヤリングを有効にします。
- DNS ゾーンの設定：ローカル Expressway を有効にし、DNS ルックアップを使用してエンドポイントやその他のシステムを見つけます。
- ユニファイドコミュニケーションの前提条件：モバイルおよびリモートアクセスや Jabber Guest などのユニファイドコミュニケーション機能に使用するトラバーサルクライアントゾーンまたはトラバーサルサーバゾーン
- Webex ゾーンの設定: Cisco Collaboration Cloud で使用するための具体的に設定されている DNS ゾーンを有効にします。

ゾーン タイプは接続の特性を示し、使用できる設定オプションを決定します。トラバーサル サーバ ゾーン、トラバーサルクライアント、およびネイバーゾーンの場合、これは、IP アドレスやポートなど、ネイバーシステムに関する提供情報を示します。ゾーンとゾーンタイプの詳細については、ゾーンについてを参照してください。

また、Expresswayには事前に設定されたデフォルト ゾーンの設定もあります。デフォルト ゾーンは、登録されていないか、または認識されておらず、ローカル ゾーンまたは既存の設定済みのゾーンのいずれかに属しているエンドポイントまたはその他のデバイスからの着信コールを表します。

Expressway とネイバー システム間の接続は、同じ SIP トランスポート タイプを使用するように設定する必要があります。つまり、どちらも TLS を使用するように設定するか、どちらも TCP を使用するように設定する必要があります。トランスポート タイプの不一致による接続の失敗はイベント ログに記録されます。

ゾーンを作成した後は、通常、1 つ以上のゾーンポリシー検索ルールにターゲットを作成します（検索ルールの設定**[設定（Configuration）] > [ダイヤル プラン（Dial plan）] > [検索ルール（Search rules）]**）。これを行わないと、検索要求がそのゾーンに送信されません。

ネイバー ゾーンの設定

ネイバー ゾーンは別のシステム（VCS や Expressway など）に登録されたエンドポイントの集合であるか、SIP デバイス（Cisco Unified Communications Manager など）です。別のシステムまたはSIPデバイスはネイバーと呼ばれます。ネイバーは固有のエンタープライズネットワークの一部か別のネットワークの一部、あるいは、スタンドアロン システムである場合があります。

別のシステムとのネイバー関係は、ローカル Expressway にネイバー ゾーンとしてその別のシステムを追加することによって構築します。ネイバーゾーンでは次の操作を行うことができます。

- ネイバーに対するエンドポイントのクエリ
- 送信前の要求に対するトランスフォーメーションの適用
- ローカル Expressway とネイバー ゾーン間のコールに使用する帯域幅の制御

（注）

- ネイバー ゾーン関係の定義は一方向です。Expressway にシステムをネイバーとして追加しても、Expressway は自動的にそのシステムのネイバーにはなりません。
- 設定されたネイバーからのインバウンドコールはそのネイバーからの着信として識別されます。
- クラスタ ピアとして設定されたシステム（以前は代替と呼ばれていました）は相互にネイバーとして設定しないでください。

次の表に、ネイバー ゾーンの設定可能なオプションを記載します。

表 *15*：ネイバーゾーンの設定

フィールド	説明	使用方法のヒント
[設定（Configuration）] セクション：		
名前（Name）	名前は一意の ID として機能し、同じタイプのゾーンを区別するために使用されます。	
タイプ（Type）	ローカル Expressway に関連する指定ゾーンの特性。[ネイバー（Neighbor）] を選択します。	ゾーンの作成後に**タイプ**を変更することはできません。
ホップ カウント（Hop count）	ホップ カウントは要求がネイバー ゲートキーパーまたはプロキシに転送される回数です（詳細については、ホップ カウントの設定の項を参照してください）。このフィールドで、この特定のゾーンに検索要求を送信するときに使用するホップ カウントを指定します。	別のゾーンから受信した検索要求にすでにホップ カウントが割り当てられている場合は、2つの値のうちの小さいほうが使用されます。
[H.323] セクション：		
モード（Mode）	ネイバー システムでH.323 コールを送受信するかどうかを決定します。	

フィールド	説明	使用方法のヒント
[ポート（Port）]	ローカル Expressway から発信された H.323 検索に使用するネイバー システムのポート。	これは、ネイバー システムでその H.323 UDP ポートで設定されたものと同じポート番号である必要があります。 ネイバーがゲートキーパーとして動作している Expressway の場合は、**[設定（Configuration）]** > **[プロトコル（Protocols）]** > **[H.323]** のページで設定されている **[登録 UDP ポート（Registration UDP port）]** の値と一致する必要があります。
SIP セクション：		
モード（Mode）	ネイバー システムで送受信する SIP コールを許可するかどうかを決定します。	
[ポート（Port）]	ローカル Expressway から発信された発信 SIP メッセージに使用するネイバー システムのポート。	これは、その SIP TCP、SIP TLS、または SIP UDP のリスニング ポート（使用する SIP **トランスポート** モードに依存）としてネイバー システムで設定されているものと同じポート番号である必要があります。
トランスポート（Transport）	ネイバー システムで送受信する SIP コールに使用するトランスポート タイプを決定します。デフォルトは、[TLS] です。	
TLS 検証モード（TLS verify mode）	TLS を使用して通信するときにネイバー システムに対して X.509 証明書チェックを Expressway が実行するかどうかを制御します。	ネイバー システムが別の Expressway である場合、両方のシステムが互いの証明書を確認できます（相互認証と呼ばれます）。詳細については、ネイバー システムの TLS 証明書の確認を参照してください。

フィールド	説明	使用方法のヒント
プロキシ経由の登録の許可（Accept proxied registrations）	このゾーンを通じてルーティングされたプロキシ経由で送信される SIP 登録を受け入れるかどうかを制御します。	この設定は、Expressway がレジストラとして機能するドメイン宛の登録要求にのみ適用されます。他のドメイン宛の要求の場合は、**[SIP 登録プロキシ モード（SIP registration proxy mode）]** の設定が適用されます。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。
メディア暗号化モード（Media encryption mode）	このゾーンで送受信される SIP コール（インターワーキング コールを含む）に Expressway によって適用されるメディア暗号化ポリシーを制御します。	詳細については、メディア暗号化ポリシーの設定を参照してください。
ICE サポート（ICE support）	このゾーン内のデバイスで ICE メッセージをサポートするかどうかを制御します。	詳細については、ICE メッセージング サポートの設定を参照してください。
ICE パススルー サポート（ICE Passthrough support）	このゾーン内で Expressway が ICE パススルーをサポートする方法を制御します。	ICE パススルー サポートは ICE サポートよりも優先されます。ベスト プラクティスとして、ICE パススルー サポートをオンにして ICE サポートをオフにすることをお勧めします。 ICE パススルーの設定の詳細と必要なバージョンについては、Expressway 設定ガイドのページに用意されている『*Mobile and Remote Access Through Cisco Expressway guide*』を参照してください。

フィールド	説明	使用方法のヒント
マルチストリーム モード（Multistream mode）	Expressway B2BUA が発呼側間でマルチストリーム コールをネゴシエートすることを許可するかどうかを制御します。 *[オン（On）]*：Expressway は、発呼側がこのゾーンを通じてマルチストリームコールをネゴシエートし、セットアップすることを許可します。 *[オフ（Off）]*：Expressway はこのゾーンを通じてマルチストリーム ネゴシエーションを拒否します。発呼側は標準コールのネゴシエーションをフォールバックする必要があります。	この切り替えは、コールが B2BUA を通過しない場合はコールに影響しません。 発呼側双方にマルチストリーム機能がない場合、相互に正しく応答することが予測されるため、デフォルトは *[オン（On）]* になっています。ただし、発呼側間のマルチストリームの設定に問題がある場合、マルチストリーム モードを無効にして、発呼側が標準コールをネゴシエートできるかどうか確認することができます。 TelePresence Server の場合、標準コールは、TelePresence Server が、複数のストリームをエンドポイントに送信して独自の方法で処理する代わりに、複数の参加者から 1 つの「会議ストリーム」を構成してエンドポイントに送信することを意味します。
プリロードされた SIP ルートのサポート（Preloaded SIP routes support）	**[プリロードされた SIP ルートのサポート（Preloaded SIP routes support）]** を *[オン（On）]* に切り替えて、Route ヘッダーを含んだ SIP INVITE 要求をこのゾーンで処理できるようにします。このヘッダーを含んでいる SIP INVITE 要求をゾーンで拒否するには、**[プリロードされた SIP ルートのサポート（Preloaded SIP routes support）]** を *[オフ（Off）]* に切り替えます。	
AES GCM のサポート	このゾーンを通過するメディアの AES GCM アルゴリズムによる暗号化/復号化を有効にします。	デフォルトでは、無効になっています。発呼側が AES GCM をネゴシエートしようとしている場合は、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
セッションのリフレッシュに対する SIP の更新	このゾーンで、セッション更新要求の送受信に SIP UPDATE メソッドをサポートするかどうかを指定します。	*[オン（On）]*：このゾーンでセッション更新リクエストの SIP UPDATE を送受信します。 *[オフ（Off）]*：このゾーンではセッション更新リクエストの SIP UPDATE の送受信を許可しません。 デフォルト：[オフ（Off）]
[認証（Authentication）] セクション：		
認証ポリシー（Authentication policy）	Expressway がこのゾーンからの着信メッセージをどのように認証するかを制御し、それらのメッセージを認証または未認証として処理するか、あるいは拒否するかを制御します。	H.323 メッセージ、ローカル ドメインから発信される SIP メッセージか非ローカル ドメインから発信される SIP メッセージかによって動作が異なります。詳細 については、認証ポリシー（Authentication policy）を参照してください。
SIP 認証信頼モード（SIP authentication trust mode）	このゾーンからの認証された SIP メッセージ（P-Asserted-Identity ヘッダーを含んでいるもの）はこれ以上のチャレンジをせずに処理されるかどうかを制御します。	詳細については、SIP 認証信頼を参照してください。
[ロケーション（Location）] セクション：		

フィールド	説明	使用方法のヒント
次の方法でピアを検索する（Look up peers by）	ピアをアドレスで検索するか、またはサービス（SRV）レコード ルックアップで検索するかを指定します。 • アドレス（デフォルト）を使用すると、最大6つのピアを追加できます。[保存（Save）] をクリックすると、Expresswayがアドレスの検索を行います。 • サービス レコードは、サービス ドメインに入るためのフィールドを生成します。[保存（Save）] をクリックすると、Expresswayは、入力されたドメインとそのゾーンで有効になっているプロトコルとトランスポートに基づいて、その DNS サーバにサービス レコードの照会を行います。 次にゾーン ページにアクセスすると、ピア アドレスが表示されているステータスが報告されます。プロトコル（SIP、SIPS、H323）、ピアが到達可能かどうか、およびピア アドレスの後にポートが表示されます。	**SRV レコード ルックアップに関する注記**： 有効なサービス ルックアップは次の 4 つです。 • _sip._udp.example.com. SIP over UDP（これは Expressway とそのゾーンではデフォルトで無効になっています） • _sip._tcp.example.com. SIP over TCP • _sips._tcp.example.com. SIP over TLS（セキュア SIP） • _h323._udp.example.com. H.323 over UDP（他のトランスポートはH.323 ではサポートされていません） SRV レコード ルックアップが設定されている所定のネイバー ゾーンでは、Expressway が登録できるピアの最大数はデフォルトで 15 に制限されます。 DNS サーバでルックアップを使用する場合は、ゾーンはゾーン ポートではなく、SRV レコードで指定されたポート経由で通信することに注意してください。ファイアウォールで、DNS 指定のポートを開いたままの状態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
ピア 1 ～ ピア 2 アドレス（Peer 1 to Peer 6 address）	ネイバー システムの IP アドレスまたは FQDN。 次の場合に追加ピアのアドレスを入力します。 • ネイバーが Expressway クラスタ。この場合は、クラスタ内のすべてのピアを指定する必要があります。 • ネイバーの復元力がある Expressway 以外のシステム。この場合は、そのシステム内の復元力のあるすべての要素のアドレスを入力する必要があります。	Expressway クラスタへのコールは、そのネイバー クラスタ内でリソース使用率が最も低いピアにルーティングされます。詳細については、Expressway クラスタ間の隣接化を参照してください。 Expressway 以外のシステムに接続する場合、リソース使用率の情報が使用できないときは Expressway はラウンドロビン選択プロセスを使用して通信するピアを決定します。
[詳細]セクション：		
ゾーン プロファイル（Zone profile）	ゾーンの詳細な設定方法を決定します。 *[デフォルト（Default）]*：工場出荷時のデフォルト プロファイルを使用します。 *[カスタム（Custom）]*：各設定を個別に行うことができます。 または、事前設定されたプロファイルのいずれかを選択して、そのタイプのシステムへの接続に必要な適切な設定を自動的に使用します。オプションは次のとおりです。 • *Default* • *Custom* • *Cisco Unified Communications Manager（8.6 以前）* • *Cisco Unified Communications Manager（8.6.1 または 8.6.2）* • *Cisco Unified Communications Manager（9.x 以降）* • *Nortel Communication Server 1000* • インフラストラクチャ デバイス（通常は MCU などの非ゲートキーパー デバイスに使用）	詳細設定について詳しくは、ゾーンの設定：詳細設定を参照してください。 シスコのカスタマー サポートのアドバイスがあった場合に個別の詳細設定を行うには、カスタム プロファイルのみを使用してください。 *Cisco Unified Communications Manager* のプロファイルについて詳しくは、『Cisco Unified Communications Manager with Expressway Deployment Guide』を参照してください。

トラバーサル クライアント ゾーンの設定

ファイアウォールを通過するには、トラバーサル サーバ（通常は Expressway-E）を使用して Expressway を接続する必要があります。この場合、ローカル Expressway がトラバーサル クライアントとなるため、ローカル Expressway にトラバーサル クライアント ゾーンを作成してトラバーサル サーバとの接続を確立します。次に、トラバーサル サーバの対応するゾーンの詳細を使用してクライアント ゾーンを設定します（トラバーサル サーバも Expressway クライアント ゾーンの詳細情報を使用して設定する必要があります）。

トラバーサル サーバと隣接させた後は、次のことが可能になります。

- トラバーサル サーバとしてネイバーを使用する
- トラバーサル サーバに対してエンドポイントをクエリする
- トラバーサル サーバに送信する前にクエリへトランスフォーメーションを適用する
- ローカル Expressway とトラバーサル サーバ間のコールに使用する帯域幅を制御する

（注） NTP サーバの設定は、トラバーサルゾーンで動作するように設定する必要があります。

詳細情報

ファイアウォールを通過するためにトラバーサルクライアントゾーンとトラバーサルサーバゾーンが連携する仕組みについて詳しくは、ファイアウォール トラバーサルについてを参照してください。

トラバーサル クライアント ゾーンの設定

次の表に、トラバーサル クライアント ゾーンの設計可能なオプションを記載します。

表 *16*：トラバーサル クライアント ゾーンの設定

フィールド	説明	使用方法のヒント
[設定（Configuration）] セクション：		
名前（Name）	名前は一意の ID として機能し、同じタイプのゾーンを区別するために使用されます。	
タイプ（Type）	ローカル Expressway に関連する指定ゾーンの特性。[トラバーサル クライアント（Traversal client）] を選択します。	ゾーンの作成後に**タイプ**を変更することはできません。

フィールド	説明	使用方法のヒント
ホップ カウント（Hop count）	ホップ カウントは要求がネイバー ゲートキーパーまたはプロキシに転送される回数です（詳細については、ホップ カウントの設定の項を参照してください）。このフィールドで、この特定のゾーンに検索要求を送信するときに使用するホップ カウントを指定します。	別のゾーンから受信した検索要求にすでにホップ カウントが割り当てられている場合は、2つの値のうちの小さいほうが使用されます。
[接続クレデンシャル（Connection credentials）] セクション		
[ユーザ名(Username)] と **[パスワード(Password)]**	トラバーサル クライアントは常に認証クレデンシャルを提供することによってトラバーサル サーバで認証される必要があります。各トラバーサル クライアント ゾーンは、トラバーサル サーバで認証を受けるために使用する**ユーザ名**と**パスワード**を指定する必要があります。	1 つ以上のサービス プロバイダに接続するために、それぞれ異なるクレデンシャルを使用して複数のトラバーサル クライアントを指定できます。
[H.323] セクション：		
モード（Mode）	トラバーサル サーバで H.323 コールを送受信するかどうかを決定します。	
[Protocol]	トラバーサルサーバへのコールに 2 つのファイアウォールトラバーサルプロトコル（*Assent* または *H.460.18*）のどちらを使用するかを指定します。	詳細については、ファイアウォール トラバーサル用のポートの設定を参照してください。
[ポート（Port）]	ローカル Expressway で送受信する H.323 コールに使用するトラバーサル サーバのポート。	H.323 を介してファイアウォール トラバーサルを動作するようにするには、トラバーサル サーバに、同じポート番号を使用してこの Expressway を表すために設定したトラバーサル サーバ ゾーンが必要です。
SIP セクション：		
モード（Mode）	トラバーサル サーバで SIP コールの送受信を許可するかどうかを決定します。	

フィールド	説明	使用方法のヒント
[ポート（Port）]	Expressway で送受信する SIP コールに使用するトラバーサル サーバのポート。 着信 SIP コールに使用するリスニング ポートとは異なっている必要があります。	SIP を介してファイアウォール トラバーサルを動作するようにするには、トラバーサル サーバに、同じトランスポート タイプとポート番号を使用してこの Expressway を表すために設定したトラバーサル サーバ ゾーンが必要です。
トランスポート（Transport）	トラバーサル サーバで送受信する SIP コールに使用するトランスポート タイプを決定します。デフォルトは、[TLS] です。	
TLS 検証モード（TLS verify mode）	TLS を使用して通信するときのこの Expressway とトラバーサル サーバ間での X.509 証明書チェックと相互認証を制御します。	詳細については、ネイバー システムの TLS 証明書の確認を参照してください。
プロキシ経由の登録の許可（Accept proxied registrations）	このゾーンを通じてルーティングされたプロキシ経由で送信される SIP 登録を受け入れるかどうかを制御します。	この設定は、Expressway がレジストラとして機能するドメイン宛の登録要求にのみ適用されます。他のドメイン宛の要求の場合は、**[SIP 登録プロキシ モード（SIP registration proxy mode）]** の設定が適用されます。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。
メディア暗号化モード（Media encryption mode）	このゾーンで送受信される SIP コール（インターワーキング コールを含む）に Expressway によって適用されるメディア暗号化ポリシーを制御します。	詳細については、メディア暗号化ポリシーの設定を参照してください。
ICE サポート（ICE support）	このゾーン内のデバイスで ICE メッセージをサポートするかどうかを制御します。	詳細については、ICE メッセージング サポートの設定を参照してください。

フィールド	説明	使用方法のヒント
ICE パススルー サポート（ICE Passthrough support）	このゾーン内で Expressway が ICE パススルーをサポートする方法を制御します。	ICE パススルー サポートは ICE サポートよりも優先されます。ベスト プラクティスとして、ICE パススルー サポートをオンにして ICE サポートをオフにすることをお勧めします。 ICE パススルーの設定の詳細と必要なバージョンについては、Expressway 設定ガイドのページ に用意されている『*Mobile and Remote Access Through Cisco Expressway guide*』を参照してください。
マルチストリーム モード（Multistream mode）	Expressway B2BUA が発呼側間でマルチストリーム コールをネゴシエートすることを許可するかどうかを制御します。 *[オン（On）]*：Expressway は、発呼側がこのゾーンを通じてマルチストリームコールをネゴシエートし、セットアップすることを許可します。 *[オフ（Off）]*：Expressway はこのゾーンを通じてマルチストリームネゴシエーションを拒否します。発呼側は標準コールのネゴシエーションをフォールバックする必要があります。	この切り替えは、コールが B2BUA を通過しない場合はコールに影響しません。 発呼側双方にマルチストリーム機能がない場合、相互に正しく応答することが予測されるため、デフォルトは*[オン（On）]* になっています。ただし、発呼側間のマルチストリームの設定に問題がある場合、マルチストリーム モードを無効にして、発呼側が標準コールをネゴシエートできるかどうか確認することができます。 TelePresence Server の場合、標準コールは、TelePresence Server が、複数のストリームをエンドポイントに送信して独自の方法で処理する代わりに、複数の参加者から 1 つの「会議ストリーム」を構成してエンドポイントに送信することを意味します。
SIP Poison モード（SIP poison mode）	このゾーンを介して見つかったシステムに送信される SIP 要求が、この Expressway が再度受信したときには拒否されるように「「ポイズニング」」されるかどうかを決定します。	

フィールド	説明	使用方法のヒント
プリロードされた SIP ルートのサポート（**Preloaded SIP routes support**）	**[プリロードされた SIP ルートのサポート（Preloaded SIP routes support）]** を *[オン（On）]* に切り替えて、Route ヘッダーを含んだ SIP INVITE 要求をこのゾーンで処理できるようにします。このヘッダーを含んでいる SIP INVITE 要求をゾーンで拒否するには、**[プリロードされた SIP ルートのサポート（Preloaded SIP routes support）]** を *[オフ（Off）]* に切り替えます。	
SIP パラメータの保持（SIP parameter preservation）	Expressway の B2BUA がこのゾーンを介してルーティングされた SIP 要求内のパラメータを保持するか、書き直すかを決定します。	*[オン（On）]*は、このゾーンと B2BUA の間でルーティングされる要求の SIP 要求 URI と連絡先パラメータを保持します。 *[オフ（Off）]*は、必要に応じて、このゾーンと B2BUA の間でルーティングされる要求の SIP 要求 URI と連絡先パラメータを B2BUA が書き直すことを許可します。 デフォルト：[オフ（Off）]
AES GCM のサポート	このゾーンを通過するメディアの AES GCM アルゴリズムによる暗号化/復号化を有効にします。	デフォルトでは、無効になっています。発呼側が AES GCM をネゴシエートしようとしている場合は、有効にする必要があります。
セッションのリフレッシュに対する SIP の更新	このゾーンで、セッション更新要求の送受信に SIP UPDATE メソッドをサポートするかどうかを指定します。	*[オン（On）]*：このゾーンでセッション更新リクエストの SIP UPDATE を送受信します。 *[オフ（Off）]*：このゾーンではセッション更新リクエストの SIP UPDATE の送受信を許可しません。 デフォルト：[オフ（Off）]
[認証（Authentication）] セクション：		

フィールド	説明	使用方法のヒント
認証ポリシー（Authentication policy）	Expresswayがこのゾーンからの着信メッセージをどのように認証するかを制御し、それらのメッセージを認証または未認証として処理するか、あるいは拒否するかを制御します。H.323メッセージ、ローカル ドメインから発信されるSIPメッセージか非ローカル ドメインから発信されるSIPメッセージかによって動作が異なります。	詳細については、認証ポリシー（Authentication policy）を参照してください。
[クライアントの設定（Client settings）] セクション：		
再試行間隔（Retry Interval）	トラバーサル サーバへの接続の確立に失敗した試行を再度試す秒単位の間隔。	
[ロケーション（Location）] セクション：		
ピア 1 ～ ピア 2 アドレス（Peer 1 to Peer 6 address）	トラバーサル サーバのIPアドレスまたはFQDN。 トラバーサル サーバがExpressway-Eのクラスタの場合は、そのすべてのピアを組み込む必要があります。	詳細については、Expressway クラスタ間の隣接化を参照してください。

トラバーサル サーバ ゾーンの設定

Expressway-E はトラバーサル サーバとして機能でき、トラバーサル クライアント（Expressway-C）に代わってファイアウォール トラバーサルを実装します。

ファイアウォール トラバーサルを動作させるには、トラバーサル サーバ（Expressway-E）に特殊なタイプの各トラバーサル クライアントとの双方向の関係が必要です。Expressway-E と Expressway-C 間にこの接続を作成するには、トラバーサル クライアントとサーバの設定を参照してください。ファイアウォールを通過するためにトラバーサル クライアント ゾーンとトラバーサル サーバ ゾーンが連携する仕組みについて詳しくは、ファイアウォール トラバーサルについてを参照してください。

（注） トラバーサル ゾーンを確実に機能させるには、NTP サーバの設定と同期させる必要があります。

トラバーサル クライアントと隣接させた後は、次のことが可能になります。

- トラバーサルクライアントへファイアウォールトラバーサルサービスを提供する

- トラバーサルクライアントにエンドポイントを照会する
- トラバーサルクライアントに送信する前にクエリへトランスフォーメーションを適用する
- ローカル Expressway とトラバーサルクライアント間のコールに使用する帯域幅を制御する
- 接続アドレスなどのゾーンステータス情報を表示する

（注） ステータス情報に示されている接続アドレスは、トラバーサル サーバ ゾーンと送信元のデバイス間で NAT 要素により変換されていることがあります。

表 *17*: トラバーサルサーバ ゾーンの設定リファレンス

フィールド	説明	使用方法のヒント
[設定（Configuration）] セクション：		
名前（Name）	名前は一意の ID として機能し、同じタイプのゾーンを区別するために使用されます。	
タイプ（Type）	ローカル Expressway に関連する指定ゾーンの特性。[トラバーサル サーバ（Traversal server）] を選択します。	ゾーンの作成後に**タイプ**を変更することはできません。
ホップ カウント（Hop count）	ホップ カウントは要求がネイバー ゲートキーパーまたはプロキシに転送される回数です（詳細については、ホップ カウントの設定の項を参照してください）。このフィールドで、この特定のゾーンに検索要求を送信するときに使用するホップ カウントを指定します。	別のゾーンから受信した検索要求にすでにホップ カウントが割り当てられている場合は、2 つの値のうちの小さいほうが使用されます。
[接続クレデンシャル（Connection credentials）] セクション		

フィールド	説明	使用方法のヒント
ユーザ名（Username）	トラバーサル クライアントは常に認証クレデンシャルを提供することによってトラバーサル サーバで認証される必要があります。 認証ユーザ名はトラバーサル クライアントが Expressway-E に提供する必要がある名前です。（トラバーサル クライアント ゾーンに接続クレデンシャルの **[ユーザ名（Username）]** として設定されています。）	また、クライアントの認証ユーザ名とパスワードについては、Expressway-E のローカル認証データベースにエントリがある必要があります。エントリのリストを確認し、必要に応じて追加するには、**[ローカル認証データベース（Local authentication database）]** ページに移動します。次のいずれかを行います。 • **[ローカル認証データベースの追加/削除（Add/Edit local authentication database）]** リンクをクリックします • **[設定（Configuration）]** > **[認証（Authentication）]** > **[ローカル データベース（Local database）]** に移動します
[H.323] セクション：		
モード（Mode）	トラバーサル クライアントで H.323 コールを送受信するかどうかを決定します。	
[Protocol]	ファイアウォールまたはNAT の通過に使用するプロトコル（*Assent* または *H.460.18*）を指定します。	詳細については、ファイアウォール トラバーサル用のポートの設定を参照してください。
[ポート（Port）]	トラバーサル クライアントで送受信する H.323 コールに使用するローカル Expressway-E のポート。	
H.460.19 逆多重化モード（H.460.19 demultiplexing mode）	2 つ以上のコールで同じ 2 つのポートをメディアに使用するかどうかを決定します。 *[オン（On）]*：トラバーサル クライアントからのすべてのコールで同じ 2 つのポートをメディアに使用します。 *[オフ（Off）]*：トラバーサル クライアントからの各コールで個別のポート ペアをメディアに使用します。	
SIP セクション：		

フィールド	説明	使用方法のヒント
モード（Mode）	トラバーサル クライアントで SIP コールを送受信するかどうかを決定します。	
[ポート（Port）]	トラバーサル クライアントで送受信する SIP コールに使用するローカル Expressway-E のポート。	これは、着信 TCP、TLS、および UDP SIP コールに使用するリスニング ポート（通常は 5060 と 5061）とは異なる必要があります。
トランスポート（Transport）	トラバーサル クライアントで送受信する SIP コールに使用するトランスポート タイプを決定します。デフォルトは、[TLS] です。	
ユニファイド コミュニケーション サービス（Unified Communications services）	このトラバーサル ゾーンが Mobile & Remote Access などのユニファイド コミュニケーション サービスを提供するかどうかを制御します。	有効にした場合、このゾーンも有効にし、**[TLS 検証モード（TLS verify mode）]** を有効にした状態で TLS を使用する必要があります。 この設定は [モバイルおよびリモート アクセスの概要] が *[モバイルとリモート アクセス（Mobile & Remote Access）]* に設定されているときにのみ適用されます。
TLS 検証モード（TLS verify mode）とサブジェクト名（subject name）	この Expressway とトラバーサル クライアント間での X.509 証明書チェックと相互認証を制御します。 **[TLS 検証モード（TLS verify mode）]** が有効になっている場合は、**[TLS 検証サブジェクト名（TLS verify subject name）]** を指定する必要があります。これは、トラバーサル クライアントの X.509 証明書内で検索する証明書の所有者の名前です。	トラバーサル クライアントがクラスタ化されている場合、**[TLS 検証サブジェクト名（TLS verify subject name）]** はクラスタの FQDN である必要があります。 詳細については、ネイバー システムの TLS 証明書の確認を参照してください。
プロキシ経由の登録の許可（Accept proxied registrations）	このゾーンを通じてルーティングされたプロキシ経由で送信される SIP 登録を受け入れるかどうかを制御します。	この設定は、Expressway がレジストラとして機能するドメイン宛の登録要求にのみ適用されます。他のドメイン宛の要求の場合は、**[SIP 登録プロキシ モード（SIP Registration Proxy Mode）]** の設定が適用されます。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。

フィールド	説明	使用方法のヒント
メディア暗号化モード（Media encryption mode）	このゾーンで送受信される SIP コール（インターワーキング コールを含む）に Expressway によって適用されるメディア暗号化ポリシーを制御します。	詳細については、メディア暗号化ポリシーの設定を参照してください。
ICE サポート（ICE support）	このゾーン内のデバイスでICEメッセージをサポートするかどうかを制御します。	詳細については、ICE メッセージング サポートの設定を参照してください。
ICE パススルー サポート（ICE Passthrough support）	このゾーン内で Expressway が ICE パススルーをサポートする方法を制御します。	ICE パススルー サポートは ICE サポートよりも優先されます。ベスト プラクティスとして、ICE パススルー サポートをオンにして ICE サポートをオフにすることをお勧めします。 ICE パススルーの設定の詳細と必要なバージョンについては、Expressway 設定ガイドのページ に用意されている『*Mobile and Remote Access Through Cisco Expressway guide*』を参照してください。
マルチストリーム モード（Multistream mode）	Expressway B2BUA が発呼側間でマルチストリーム コールをネゴシエートすることを許可するかどうかを制御します。 *[オン（On）]*：Expressway は、発呼側がこのゾーンを通じてマルチストリームコールをネゴシエートし、セットアップすることを許可します。 *[オフ（Off）]*：Expressway はこのゾーンを通じてマルチストリーム ネゴシエーションを拒否します。発呼側は標準コールのネゴシエーションをフォールバックする必要があります。	この切り替えは、コールが B2BUA を通過しない場合はコールに影響しません。 発呼側双方にマルチストリーム機能がない場合、相互に正しく応答することが予測されるため、デフォルトは*[オン（On）]* になっています。ただし、発呼側間のマルチストリームの設定に問題がある場合、マルチストリーム モードを無効にして、発呼側が標準コールをネゴシエートできるかどうか確認することができます。 TelePresence Server の場合、標準コールは、TelePresence Server が、複数のストリームをエンドポイントに送信して独自の方法で処理する代わりに、複数の参加者から 1 つの「会議ストリーム」を構成してエンドポイントに送信することを意味します。

フィールド	説明	使用方法のヒント
ポイズンモード（Poison mode）	このゾーンを介して見つかったシステムに送信される SIP 要求が、この Expressway が再度受信したときには拒否されるように「「ポイズニング」」されるかどうかを決定します。	
プリロードされた SIP ルートのサポート（Preloaded SIP routes support）	**[プリロードされた SIP ルートのサポート（Preloaded SIP routes support）]** を *[オン（On）]* に切り替えて、Route ヘッダーを含んだ SIP INVITE 要求をこのゾーンで処理できるようにします。このヘッダーを含んでいる SIP INVITE 要求をゾーンで拒否するには、**[プリロードされた SIP ルートのサポート（Preloaded SIP routes support）]** を *[オフ（Off）]* に切り替えます。	
SIP パラメータの保持（SIP parameter preservation）	Expressway の B2BUA がこのゾーンを介してルーティングされた SIP 要求内のパラメータを保持するか、書き直すかを決定します。	*[オン（On）]*は、このゾーンと B2BUA の間でルーティングされる要求の SIP 要求 URI と連絡先パラメータを保持します。 *[オフ（Off）]*は、必要に応じて、このゾーンと B2BUA の間でルーティングされる要求の SIP 要求 URI と連絡先パラメータを B2BUA が書き直すことを許可します。 デフォルト：[オフ（Off）]
AES GCM のサポート	このゾーンを通過するメディアの AES GCM アルゴリズムによる暗号化/復号化を有効にします。	デフォルトでは、無効になっています。発呼側が AES GCM をネゴシエートしようとしている場合は、有効にする必要があります。
セッションのリフレッシュに対する SIP の更新	このゾーンで、セッション更新要求の送受信に SIP UPDATE メソッドをサポートするかどうかを指定します。	*[オン（On）]*：このゾーンでセッション更新リクエストの SIP UPDATE を送受信します。 *[オフ（Off）]*：このゾーンではセッション更新リクエストの SIP UPDATE の送受信を許可しません。 デフォルト：[オフ（Off）]
[認証（Authentication）] セクション：		

フィールド	説明	使用方法のヒント
認証ポリシー（Authentication policy）	Expresswayがこのゾーンからの着信メッセージをどのように認証するかを制御し、それらのメッセージを認証または未認証として処理するか、あるいは拒否するかを制御します。H.323メッセージ、ローカル ドメインから発信されるSIPメッセージか非ローカル ドメインから発信されるSIPメッセージかによって動作が異なります。	詳細 については、認証ポリシー（Authentication policy）を参照してください。
[UDP/TCP プローブ（UDP / TCP probes）] セクション：		
UDP の再試行間隔（UDP retry interval）	キープ アライブ確認を受信していない場合にクライアントがUDPプローブをExpressway-E へ送信する頻度（秒単位）。	デフォルトの UDP および TCP プローブの再試行間隔はほとんどの場合に適しています。ただし、NAT バインドのタイムアウトに問題が発生した場合は、変更する必要がある場合があります。
UDP の再試行回数（UDP retry count）	コール セットアップ時にクライアントが UDP プローブの Expressway-E への送信を試行する回数。	
UDP のキープ アライブ間隔（UDP keep alive interval）	コールが確立した後に、ファイアウォールの NAT バインドを有効にしておくために、クライアントが UDP プローブを Expressway-E に送信する間隔（秒単位）。	
TCP の再試行間隔（TCP retry interval）	キープ アライブ確認を受信していない場合にトラバーサル クライアントが TCP プローブを Expressway-E へ送信する間隔（秒単位）。	
TCP の再試行回数（TCP retry count）	コール セットアップ時にクライアントが TCP プローブの Expressway-E への送信を試行する回数。	
TCP のキープ アライブ間隔（TCP keep alive interval）	コールが確立しているときに、ファイアウォールの NAT バインドを有効にしておくために、トラバーサル クライアントが TCP プローブを Expressway-E に送信する間隔（秒単位）。	

ENUM ゾーンの設定

ENUM ゾーンでは、ENUM ルックアップを使用してエンドポイントを見つけることができます。使用されている ENUM DNS サフィックスに基づき、またはエンドポイントのエイリアスのパターンマッチングにより、あるいはそれらの両方で、ENUM ゾーンに 1 つ以上の検索ルールを作成できます。

1 つ以上の ENUM ゾーンを設定した後で、次のことが可能になります。

- エンドグループのそのグループ宛のエイリアス検索要求にトランスフォーメーションを適用します。
- ローカル Expressway と ENUM エンドポイントの各グループ間でのコールに使用する帯域幅を制御します。

ENUM ゾーンの使用方法と設定方法の詳細については、ENUM ダイヤリングについてセクションを参照してください。

次の表に、ENUM ゾーンの設定可能なオプションを記載します。

表 *18 : ENUM* ゾーン設定

フィールド	説明	使用方法のヒント
名前（Name）	名前は一意の ID として機能し、同じタイプのゾーンを区別するために使用されます。	
タイプ（Type）	ローカル Expressway に関連する指定ゾーンの特性。[ENUM] を選択します。	ゾーンの作成後に**タイプ**を変更することはできません。
ホップ カウント（Hop count）	ホップ カウントは要求がネイバー ゲートキーパーまたはプロキシに転送される回数です（詳細については、ホップ カウントの設定の項を参照してください）。このフィールドで、この特定のゾーンに検索要求を送信するときに使用するホップ カウントを指定します。	別のゾーンから受信した検索要求にすでにホップ カウントが割り当てられている場合は、2 つの値のうちの小さいほうが使用されます。
DNS サフィックス（DNS suffix）	このゾーンを照会する ENUM ドメインを作成するために変換された E.164 番号に追加するドメイン。	
H.323 モード（H.323 Mode）	このゾーンについて H.323 レコードをルックアップするかを決定します。	

フィールド	説明	使用方法のヒント
SIP モード（SIP mode）	このゾーンについて SIP レコードをルックアップするかどうかを決定します。	

DNS ゾーンの設定

DNS ゾーンでは、DNSルックアップを使用してエンドポイントを見つけることができます。エンドポイント エイリアスのパターン マッチングに基づいて DNS ゾーンに 1 つ以上の検索ルールを作成できます。

1 つ以上の DNS ゾーンを作成した後、そのエンドポイント グループ宛のエイリアス検索要求にトランスフォームを適用できます。ローカル Expressway と DNS エンドポイントの各グループ間でのコールに使用する帯域幅を制御することもできます。DNS ゾーンの設定および仕様の詳細については、URI ダイヤリングについてを参照してください。

次の表に、DNS ゾーンの設定可能なオプションを記載します。

表 *19 : DNS* ゾーン設定

フィールド	説明	使用方法のヒント
名前（Name）	名前は一意の ID として機能し、同じタイプのゾーンを区別するために使用されます。	
タイプ（Type）	ローカル Expressway に関連する指定ゾーンの特性。[DNS] を選択します。	ゾーンの作成後に**タイプ**を変更することはできません。
ホップカウント（Hop count）	ホップ カウントは要求がネイバー ゲートキーパーまたはプロキシに転送される回数です（詳細については、ホップ カウントの設定の項を参照してください）。このフィールドで、この特定のゾーンに検索要求を送信するときに使用するホップ カウントを指定します。	別のゾーンから受信した検索要求にすでにホップ カウントが割り当てられている場合は、2 つの値のうちの小さいほうが使用されます。
[H.323] セクション		
H.323 モード（H.323 Mode）	このゾーンを介した DNS ルックアップを使用して見つかったシステムとエンドポイントに対する H.323 コールを許可するかどうかを決定します。	
SIP セクション		

フィールド	説明	使用方法のヒント
SIP モード（SIP mode）	このゾーンを介した DNS ルックアップを使用して見つかったシステムとエンドポイントに対する SIP コールを許可するかどうかを決定します。	
TLS 検証モード（TLS verify mode）とサブジェクト名（subject name）	DNS ルックアップにより返された宛先システム サーバに対して X.509 認証チェックを Expressway が実行するかどうかを制御します。 **[TLS 検証モード（TLS verify mode）]** が有効になっている場合は、**[TLS 検証サブジェクト名（TLS verify subject name）]** を指定する必要があります。これは、宛先システムのサーバの X.509 証明書内で検索する証明書の所有者の名前です。	この設定は、DNS ルックアップが必要なプロトコルとして TLS を指定している場合にのみ適用されます。TLS が不要であれば、設定は無視されます。詳細については、ネイバー システムの TLS 証明書の確認を参照してください。
TLS サブジェクト名の確認（TLS verify subject name）	宛先システムのサーバの X.509 証明書で検索する証明書の所有者の名前（SAN にあるサブジェクト代替名の属性に含まれている必要があります）。	
TLS 検証着信マッピング（TLS verify inbound mapping）	[着信TLSマッピング（Inbound TLS mapping）] を [オン（On）] に切り替えて、ピア証明書に TLS 検証サブジェクト名が含まれている場合に着信 TLS 接続をこのゾーンにマッピングします。受信した証明書に TLS検証サブジェクト名（共通名またはサブジェクト代替名）が含まれていない場合は、接続はこのゾーンにマッピングされません。	[着信 TLS マッピング（Inbound TLS mapping）] を [オフ（Off）] に切り替えて、Expressway が着信 TLS接続をこのゾーンにマッピングしようとしないようにします。
フォールバック トランスポート プロトコル（Fallback transport protocol）	DNS NAPTR レコードと SIP URI パラメータによって必要なトランスポート情報が得られないときに DNS ゾーンからの SIP コールに使用するトランスポートタイプ。 デフォルトは、*[UDP]* です（有効になっている場合）。	
メディア暗号化モード（Media encryption mode）	インターネットへの SIP コール（インターワーキング コールを含む）に Expressway によって適用されるメディア暗号化ポリシーを制御します。	詳細については、メディア暗号化ポリシーの設定を参照してください。

フィールド	説明	使用方法のヒント
ICE サポート（ICE support）	このゾーン内のデバイスで ICE メッセージをサポートするかどうかを制御します。	詳細については、ICE メッセージング サポートの設定を参照してください。
プリロードされた SIP ルートのサポート（Preloaded SIP routes support）	**[プリロードされた SIP ルートのサポート（Preloaded SIP routes support）]** を *[オン（On）]* に切り替えて、Route ヘッダーを含んだ SIP INVITE 要求をこのゾーンで処理できるようにします。このヘッダーを含んでいる SIP INVITE 要求をゾーンで拒否するには、**[プリロードされた SIP ルートのサポート（Preloaded SIP routes support）]** を *[オフ（Off）]* に切り替えます。	
DNS 要求の変更（Modify DNS request）	このゾーンからの発信 SIP コールをダイヤルした宛先内のドメインではなく、手動で指定した SIP ドメインにルーティングします。	このオプションは、コール サービス制御で使用することを主な目的としています。www.cisco.com/go/hybrid-services を参照してください。
検索対象のドメイン（Domain to search for）	発信 SIP URI のドメインを検索するのではなく、DNS にある完全修飾ドメイン名を入力します。元の SIP URI には影響しません。	
AES GCM のサポート	このゾーンを通過するメディアの AES GCM アルゴリズムによる暗号化/復号化を有効にします。	デフォルトでは、無効になっています。発呼側が AES GCM をネゴシエートしようとしている場合は、有効にする必要があります。
セッションのリフレッシュに対する SIP の更新	このゾーンで、セッション更新リクエストを送受信するための SIP UPDATE メソッドをサポートするかどうかを指定します。	*[オン（On）]*：このゾーンでセッション更新リクエストの SIP UPDATE を送受信します。 *[オフ（Off）]*：このゾーンではセッション更新リクエストの SIP UPDATE の送受信を許可しません。 デフォルト：[オフ（Off）]
[認証（Authentication）] セクション		

フィールド	説明	使用方法のヒント
SIP 認証信頼モード（SIP authentication trust mode）	**[認証ポリシー（Authentication Policy）]** と一緒に使用して、このゾーンから受信した事前に認証された SIP メッセージ（P-Asserted-Identity ヘッダーが含まれているもの）が信頼できるかどうかを制御、さらに、Expressway 内で認証済みまたは未認証として処理するかどうかを制御します。 *[オン（On）]*：事前認証済みメッセージは追加のチャレンジなしに信頼され、その後、Expressway内では認証済みとして扱われます。未認証メッセージは、**[認証ポリシー（Authentication Policy）]** が *[クレデンシャルを確認する（Check credentials）]* に設定されている場合はチャレンジされます。 *[オフ（Off）]*：既存の認証済みインジケータ（P-Asserted-Identityヘッダー）はすべてメッセージから削除されます。ローカルドメインからのメッセージは、**[認証ポリシー（Authentication Policy）]** が *[クレデンシャルを確認する（Check credentials）]* に設定されている場合はチャレンジされます。	DNS ゾーンの場合、認証済みとして処理するには、**[認証ポリシー（Authentication Policy）]** を常に設定します。
[詳細]セクション		

フィールド	説明	使用方法のヒント
アドレスレコードを含める（**Include address record**）	NAPTR（SIP）レコードまたは SRV（SIP と H.323）レコードがこのゾーンを介してダイヤルされたエイリアスで検出されなかった場合は、プライオリティが下位のゾーンの照会に進む前に、Expressway が A および AAAA DNS レコードを照会するかどうかを決定します。SIP または H.323 をサポートするシステム以外で A および AAAA レコードが同じドメインにある場合は、Expressway は検索が成功したと認識し、コールがこのゾーンに転送されて、コールが失敗する場合があります。 *[オン（On）]*：Expressway は A または AAAA レコードを照会します。検出された場合、Expressway はプライオリティが下位のゾーンは照会しません。 *[オフ（Off）]*：（デフォルト）Expressway は A および AAAA レコードを照会しません。その代わりに、検索を続行し、プライオリティが下位の残りのゾーンを照会します。	
ゾーン プロファイル（**Zone profile**）	ゾーンの詳細な設定方法を決定します。 *[デフォルト（Default）]*：工場出荷時のデフォルトプロファイルを使用します。 *[カスタム（Custom）]*：各設定を個別に行うことができます。	詳細設定について詳しくは、ゾーンの設定：詳細設定を参照してください。 シスコのカスタマー サポートのアドバイスがあった場合に個別の詳細設定を行うには、カスタム プロファイルのみを使用してください。

Webex ゾーンの設定

Webex ゾーンは、Expressway-E から Cisco Webex に接続するために事前設定された DNS ゾーンです。このゾーンを使用して、Cisco Webex ハイブリッド コール サービスまたは Webex Meetings、あるいはその両方を有効にすることができます。

このようにすると、Expressway-E は、Expressway-C を使用せずに Cisco Unified Communications Manager に接続します。このシナリオではトラバーサルまたはファイアウォールは必要ありません。また Expressway-E は、Webex クラウドを Cisco Unified Communications Manager に直接接続します。テスト済み設定では、Cisco Unified Communications Manager と Expressway-E 間のネイバーゾーンで、インターネット上の標準の Webex Edge Audio を使用します。

このシナリオでは、インバウンド接続を内部ファイアウォールで開く必要があります。そのため、通常のデュアルファイアウォール設定を使用した標準規格の導入ではサポートされて**いません**。

Webex ゾーンを有効にするには、次の方法を実行します。

1. **[設定（Configuration）]** > **[ゾーン（Zones）]** > **[ゾーン（Zones）]** へ移動します。
2. [新規（New）] をクリックします。
3. **[タイプ（Type）]** ドロップダウンから *[Webex]* を選択します。

   Expressway は、Cisco Webex への正しい接続を保証する事前設定された名前と事前設定されたパラメータを使用して新しいゾーンを作成します。

（注） このタイプのゾーンを複数作成することはできません。また、ゾーンを有効化した後で、ゾーンの 1 つのインスタンスを変更することはできません。

設定の詳細については、ハイブリッド コール サービスのドキュメントを参照してください。

デフォルト設定を変更する方法

Webex ゾーンのメディア暗号化モードは 「[自動（Auto）]」 です 。Webex ゾーンは事前設定された DNS ゾーンなので、シナリオによっては 「[オン（On）]」 である必要がある場合は、代わりに DNS ゾーンを作成することをお勧めします。その後、Expressway Web インターフェイスを介して DNS ゾーンを変更 します（**[設定（Configuration）]** > **[ゾーン（Zones）]** > **[ゾーン（Zones）]**を設定し、**[メディア暗号化モード（Media encryption mode）]** を *[オン（On）]*に設定します）。同じ回避策を使用して、**[SIP 認証信頼モード（SIP authentication trust mode）]** を *[オン（On）]* に変更できます。

ゾーンの設定：詳細設定

次の表に、カスタム ゾーン プロファイルの詳細なゾーン設定オプションを記載します。これらの設定の一部は、特定のゾーン タイプのみに適用されます。

設定	説明	デフォルト	ゾーン タイプ
アドレスレコードを含める（Include address record）	NAPTR（SIP）レコードまたは SRV（SIP と H.323）レコードがこのゾーンを介してダイヤルされたエイリアスで検出されなかった場合は、プライオリティが下位のゾーンの照会に進む前に、Expressway が A および AAAA DNS レコードを照会するかどうかを決定します。SIP または H.323 をサポートするシステム以外で A および AAAA レコードが同じドメインにある場合は、Expressway は検索が成功したと認識し、コールがこのゾーンに転送されて、コールが失敗する場合があります。 *[オン（On）]*：Expressway は A または AAAA レコードを照会します。検出された場合、Expressway はプライオリティが下位のゾーンは照会しません。 *[オフ（Off）]*：Expresswayは A および AAAA レコードを照会しません。その代わりに、検索を続行し、プライオリティが下位の残りのゾーンを照会します。	オフ（Off）	DNS
ピア ステータスのモニタ（Monitor peer status）	Expressway がゾーンのピアのステータスをモニタするかどうかを指定します。有効になっている場合は、H.323 LRQ または SIP OPTIONS、あるいはその両方が定期的にピアに送信されます。ピアが応答しない場合は、そのピアを非アクティブとマークします。すべてのピアが応答しない場合は、ゾーンを非アクティブとします。	○	ネイバー（Neighbor）
コール シグナリング ルーティング モード（Call signaling routed mode）	このネイバーで送受信するコールのシグナリングを Expressway がどのように処理するかを指定します。 *[自動（Auto）]*：シグナリングは**[コールシグナリングの最適化（Call signaling optimization）]（[設定（Configuration）]>[コール ルーティング（Call routing）]）**の設定に従って行われます。 *[常時（Always）]*：シグナリングは**[コールシグナリングの最適化（Call signaling optimization）]**の設定に関係なく、のネイバーで送受信するコールに応じて行われます。 トラバーサル ゾーンまたは B2BUA を介したコールは常にシグナリングを取得します。	Auto	ネイバー（Neighbor）

設定	説明	デフォルト	ゾーン タイプ
H.323 検索に自動的に応答（Automatically respond to H.323 searches）	Expressway がこのゾーン宛の H.323 検索を受信したときの動作を決定します。 *[オフ（Off）]*：LRQ メッセージがゾーンに送信されます。 *[オン（On）]*：検索をゾーンに転送せずに自動的に応答します。	オフ（Off）	ネイバー（Neighbor）
SIP 検索に自動的に応答（Automatically respond to SIP searches）	Expressway が H.323 検索として発信された SIP 検索を受信したときの動作を決定します。 *[オフ（Off）]*：SIP OPTIONS または SIP INFO メッセージが送信されます。 *[オン（On）]*：検索に自動的に応答します。検索が転送されることはありません。 通常はこれをデフォルトの [オフ（Off）] のままにしてください。ただし、SIP OPTIONS メッセージオプションを許可しないシステムもあります。そのため、これらのゾーンについては、設定を [オン（On）] にする必要があります。これを [オン（On）] に変更した場合はパターン マッチも設定し、このゾーン内で実際にエンドポイントに一致する検索のみに応答するよう設定する必要もあります。これを行わないと、プライオリティが下位の他のゾーンの検索が続行され、サポートできない場合でも、このゾーンにコールが転送されます。	オフ	ネイバー（Neighbor） DNS

設定	説明	デフォルト	ゾーン タイプ
相互運用されるコール用に空の INVITE を送信（Send empty INVITE for interworked calls）	Expressway がこのゾーンを介して送信する SDP なしに SIP INVITE メッセージを生成するかどうかを決定します。SDP を使用していない INVITE は、宛先デバイスがコーデックの選択を開始するよう求められることを意味し、コールが H.323 からローカルにインターワーキングされていた場合に使用されます。 *[オン（On）]*：SDP なしの SIP INVITE が生成されます。 *[オフ（Off）]*：SIP INVITE が生成され、事前設定された SDP が挿入されてから INVITE が送信されます。 ほとんどの場合、このオプションは通常はデフォルトの [オン（On）] のままにしてください。ただし、一部のデバイスは SDP なしの INVITE を許可しません。そのため、これらのゾーンについてはこの設定を [オフ（Off）] にする必要があります。 （注） 事前に設定された SDP の設定は、CLI で `xConfiguration Zones Zone [1..1000] [Neighbor/DNS] Interworking SIP` コマンドを使用して設定できます。これらの設定値は、シスコ カスタマー サポートのアドバイスがあった場合にのみ、変更してください。		

設定	説明	デフォルト	ゾーン タイプ
SIP パラメータの保持（SIP parameter preservation）	Expressway の B2BUA がこのゾーンを介してルーティングされた SIP 要求内のパラメータを保持するか、書き直すかを決定します。 *[オン（On）]*は、このゾーンと B2BUA の間でルーティングされる要求の SIP 要求 URI と連絡先パラメータを保持します。 *[オフ（Off）]*は、必要に応じて、このゾーンと B2BUA の間でルーティングされる要求の SIP 要求 URI と連絡先パラメータを B2BUA が書き直すことを許可します。 デフォルト：[オフ（Off）]	オフ（Off）	ネイバー（Neighbor） DNS UC トラバーサル（UC Traversal） トラバーサル サーバ（Traversal Server） トラバーサル クライアント（Traversal Client）
SIP Poison モード（SIP poison mode）	*[オン（On）]*：このゾーンを介して見つかったシステムに送信される SIP 要求が、この Expressway が再度受信したときには拒否されるように「「ポイズニング」」されます。 *[オフ（Off）]*：このゾーンを介して送信され、Expressway が再度受信する SIP 要求は拒否されません。これらの要求は通常どおりに処理されます。	オフ	ネイバー（Neighbor）トラバーサル クライアント（Traversal client）トラバーサル サーバ（Traversal server）DNS
SIP 暗号化モード（SIP encryption mode）	Expressway がこのゾーンで暗号化された SIP コールを許可するかどうかを決定します。 *Auto*：セキュア SIP トランスポート（TLS）が使用されている場合、SIP コールが暗号化されます。 *[Microsoft]*：SIP コールは MS-SRTP を使用して暗号化されます。 *[オフ（Off）]*：SIP コールは暗号化されません。 通常はこのオプションをデフォルトの *[自動（Auto）]* のままにしてください。	自動（Auto）	ネイバー（Neighbor）

設定	説明	デフォルト	ゾーン タイプ
SIP REFER モード（SIP REFER mode）	SIP REFER 要求の処理方法を決定します。 *[転送（Forward）]*：SIP REFER 要求がターゲットに転送されます。 *[終了（Terminate）]*：SIP REFER 要求は Expressway によって終了されます。	転送（Forward）	ネイバー（Neighbor）
Meeting Server ロードバランシング（Meeting Server load balancing）	X8.11 以降、Cisco Expressway シリーズではコールブリッジ グループに含まれる Meeting Server 間のコールのロードバランシングに使用されるメカニズムがサポートされています。 Cisco Meeting Server がコール ブリッジ グループに含まれている場合、容量のないサーバ上のスペースに参加者が参加しようとすると、コールは別のサーバーに再ルーティングされます。ルーティング先のサーバは、元のコールの詳細を使用して SIP INVITE をコール制御層に送信します。これにより、参加者は別の Meeting Server 上の適切なスペースに参加できます。「「2 番目」」のサーバに容量があるが、別の Meeting Server にそれよりも多い容量がある場合は、2 番目のサーバはその Meeting Server に SIP INVITE を送信するよう求めます。 *[オン（On）]*：Expressway B2BUA は Meeting Server からの INVITE を処理します。Unified CM またはこの Expressway に登録されているエンドポイント、あるいは隣接する VCS または Expressway に登録されているエンドポイントに対してロードバランシングを有効にする必要があります。 *[オフ（Off）]*：Expressway B2BUA は p ではありません	オフ（Off）	ネイバー（Neighbor）
SIP マルチパート MIME 削除モード（SIP multipart MIME strip mode）	複数の MIME ストリッピングをこのゾーンからの要求上で実行するかどうかを制御します。 通常はこのオプションをデフォルトの [オフ（Off）] のままにしてください。	オフ（Off）	ネイバー（Neighbor）

設定	説明	デフォルト	ゾーン タイプ
SIP UPDATE 削除モード（SIP UPDATE strip mode）	Expressway がこのゾーンで送受信するすべての要求と応答の Allow ヘッダーから UPDATE メソッドを削除するかどうかを制御します。 通常はこのオプションをデフォルトの [オフ（Off）] のままにしてください。ただし、Allow ヘッダーの UPDATE メソッドをサポートしていないシステムもあります。そのため、これらのゾーンについては設定を [オン（On）] にする必要があります。	オフ（Off）	ネイバー（Neighbor）
相互接続 SIP 検索戦略（Interworking SIP Search Strategy）	H.323 コールとインターワーキングするときに Expressway が SIP エンドポイントをどのように検索するかを決定します。 *[オプション（Options）]*：Expressway は OPTIONS 要求を送信します。 *[情報（Info）]*：Expressway は INFO 要求を送信します。 通常はこのオプションをデフォルトの *[オプション（Options）]* のままにしてください。ただし、OPTIONS 要求に応答できないエンドポイントもあります。そのため、これらのエンドポイントについては *[情報（Info）]* に設定する必要があります。	オプション（Options）	ネイバー（Neighbor）
SIP UDP/BFCP フィルタ モード（SIP UDP/BFCP filter mode）	このゾーンに送信された INVITE 要求から UDP/BFCP をフィルタリングにより除去するかどうかを決定します。UDP/BFCP プロトコルをサポートしない SIP デバイスとの相互運用性を有効にするためにこのオプションが必要な場合があります。 *[オン（On）]*：UDP/BFCP プロトコルを参照しているメディア回線が TCP/BFCP で置き換えられ、無効になります。 *[オフ（Off）]*：INVITE 要求は変更されません。	オフ	ネイバー（Neighbor） DNS

設定	説明	デフォルト	ゾーン タイプ
SIP UDP/IX フィルタ モード（SIP UDP/IX filter mode）	このゾーンに送信された INVITE 要求から UDP/UDT/IX または UDP/DTLS/UDT/IX をフィルタリングにより除去するかどうかを決定します。UDP/UDT/IX プロトコルまたは UDP/DTLS/UDT/IX プロトコルをサポートしない SIP デバイスとの相互運用性を有効にするためにこのオプションが必要な場合があります。 *[オン（On）]*：UDP/UDT/IX プロトコルまたは UDP/DTLS/UDT/IX プロトコルを参照するメディア回線を RTP/AVP に置き換えて無効にします。 *[オフ（Off）]*：INVITE 要求は変更されません。 次の場合は **[SIP UDP/IX フィルタ モード（SIP UDP/IX filter mode）]** を *[オン（On）]* に設定することを推奨します。 • 外部ネットワークまたはシスコ以外のインフラストラクチャに接続されているネイバーゾーンを通じてルーティングされている Business-to-Business（B2B）コール • Unified CM 8.x 以前に内部的に接続されているコール（9.x 以降の場合は *[オフ（Off）]* に設定）	Cisco Unified Communications Manager で事前設定されたゾーンプロファイルでは *[オフ（Off）]*。 それ以外の場合は *[オン（On）]*。	ネイバー（Neighbor） DNS
SIP レコード ルート アドレス タイプ（SIP record route address type）	Expressway がその IP アドレスを使用するか、このゾーンへの発信 SIP 要求のレコードルートまたはパスのヘッダーのホスト名を使用するかを制御します。 *[IP]*：Expressway の IP アドレスを使用します。 *[ホスト名（Hostname）]*：Expressway の**システム ホスト名**を使用します（空白の場合は、IP アドレスが使用されます）。	IP	ネイバー（Neighbor） DNS
SIP プロキシ - ヘッダー削除リストが必要（SIP Proxy-Require header strip list）	このゾーンから受信した SIP 要求の Proxy-Require ヘッダーを検索し、そのヘッダーから削除するオプション タグのカンマ区切りのリスト。	なし（None）	ネイバー（Neighbor）

ゾーンの設定：事前設定されたプロファイルの設定

次の表に、事前に設定されたプロファイルに自動的に適用される詳細なゾーン設定オプションを示します。

設定	Cisco Unified CM（9.x or 以降）	Cisco Unified CM（8.6.1 または 8.6.2）	Cisco Unified CM（8.6 以下）	Nortel Communication Server 1000	インフラストラクチャデバイス	デフォルト
ピア ステータスのモニタ（Monitor peer status）	はい	はい	はい	はい	いいえ	はい
コール シグナリング ルーティング モード（Call signaling routed mode）	常に（Always）	常に（Always）	常に（Always）	自動（Auto）	常に（Always）	自動（Auto）
H.323 検索に自動的に応答（Automatically respond to H.323 searches）	消灯	消灯	消灯	オフ	オン	オフ
SIP 検索に自動的に応答（Automatically respond to SIP searches）	消灯	消灯	消灯	オフ	オン	オフ
相互運用されるコール用に空の INVITE を送信（Send empty INVITE for interworked calls）	オン	オン	オン	オン	オン	オン

設定	Cisco Unified CM（9.x or 以降）	Cisco Unified CM（8.6.1 または 8.6.2）	Cisco Unified CM（8.6 以下）	Nortel Communication Server 1000	インフラストラクチャデバイス	デフォルト
SIP パラメータの保持（SIP parameter preservation）	消灯	消灯	消灯	消灯	消灯	消灯
SIP Poison モード（SIP poison mode）	消灯	消灯	消灯	消灯	消灯	消灯
SIP 暗号化モード（SIP encryption mode）	自動（Auto）	自動（Auto）	自動（Auto）	自動（Auto）	自動（Auto）	自動（Auto）
SIP REFER モード（SIP REFER mode）	転送（Forward）	転送（Forward）	転送（Forward）	転送（Forward）	転送（Forward）	転送（Forward）
Meeting Server ロードバランシング（Meeting Server load balancing）	消灯	消灯	消灯	消灯	オフ	オン
SIP マルチパート MIME 削除モード（SIP multipart MIME strip mode）	消灯	消灯	消灯	消灯	消灯	消灯
SIP UPDATE 削除モード（SIP UPDATE strip mode）	消灯	消灯	オフ	オン	オフ	消灯

設定	Cisco Unified CM（9.x or 以降）	Cisco Unified CM（8.6.1 または 8.6.2）	Cisco Unified CM（8.6 以下）	Nortel Communication Server 1000	インフラストラクチャデバイス	デフォルト
相互接続 SIP 検索戦略（Interworking SIP Search Strategy）	オプション	オプション	オプション	オプション	オプション	オプション
SIP UDP/BFCP フィルタモード（SIP UDP/BFCP filter mode）	消灯	オフ	オン	オフ	消灯	消灯
SIP UDP/IX フィルタモード（SIP UDP/IX filter mode）	オフ	オン	オン	オン	オン	オフ
SIP レコードルートアドレス タイプ（SIP record route address type）	IP	IP	IP	IP	IP	IP
SIP プロキシ - ヘッダー削除リストが必要（SIP Proxy-Require header strip list）	<空白>	<空白>	<空白>	[illegible]	<空白>	<空白>

Expressway と Unified CM 間の SIP トランクの設定詳細：

「Expressway 設定ガイド」 ページに用意されている『*Cisco Expressway and CUCM via SIP Trunk Deployment Guide*』を参照してください。

ネイバー システムの TLS 証明書の確認

SIP TLS 接続が Expressway とネイバー システム間で確立されている場合、ネイバー システムの ID を確認するためにそのシステムの X.509 証明書を確認するように Expressway を設定できます。これを行うには、ゾーンの [TLS 検証モード（TLS verify mode）] を設定します。

TLS 検証モードが有効にされている場合、ゾーン設定の **[ピア アドレス（Peer address）]** フィールドに指定されたネイバー システムの FQDN または IP アドレスがそのシステムで提示された X.509 証明書に含まれる証明書の所有者名と照合するために使用されます。(名前は、証明書のサブジェクト代替名属性に含める必要があります。) 証明書自体も有効であり、信頼された認証局によって署名されている必要があります。

（注） トラバーサル サーバと DNS ゾーンでは、接続元のトラバーサル クライアントの FQDN または IP アドレスは設定されないため、必須の証明書の所有者の名前を個別に指定する必要があります。

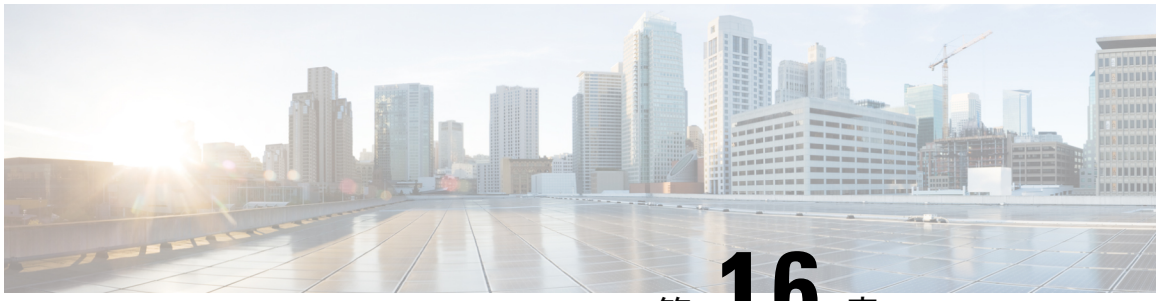
ネイバー システムが別の Expressway であるか、またはトラバーサル クライアントとトラバーサル サーバの関係がある場合、互いの証明書を認証するように 2 つのシステムを設定できます。これは相互認証と呼ばれ、この場合は各 Expressway がクライアントとサーバの両方として機能します。そのため、各 Expressway の証明書がクライアントとしてもサーバとしても有効であることを確認する必要があります。

証明書の確認についての詳細、および Expressway のサーバ証明書のアップロードと信頼できる認証局のリストのアップロードの手順については、セキュリティの基本を参照してください。

着信コール専用のゾーンの設定

エイリアス検索要求を送信しないように（このゾーンからの着信コールのみを受信する場合など）ゾーンを設定するには、ターゲットとしてそのゾーンが必要な検索ルールを定義しないでください。

このシナリオでは、ゾーンを表示するときに、検索ルールが設定されていないことを示す警告を無視できます。



第 16 章

クラスタリングとピア

ここでは、Expressway ピアのクラスタのセットアップ方法について説明します。Expressway の導入のキャパシティを高め、復元力を提供するためにクラスタリングを使用します。

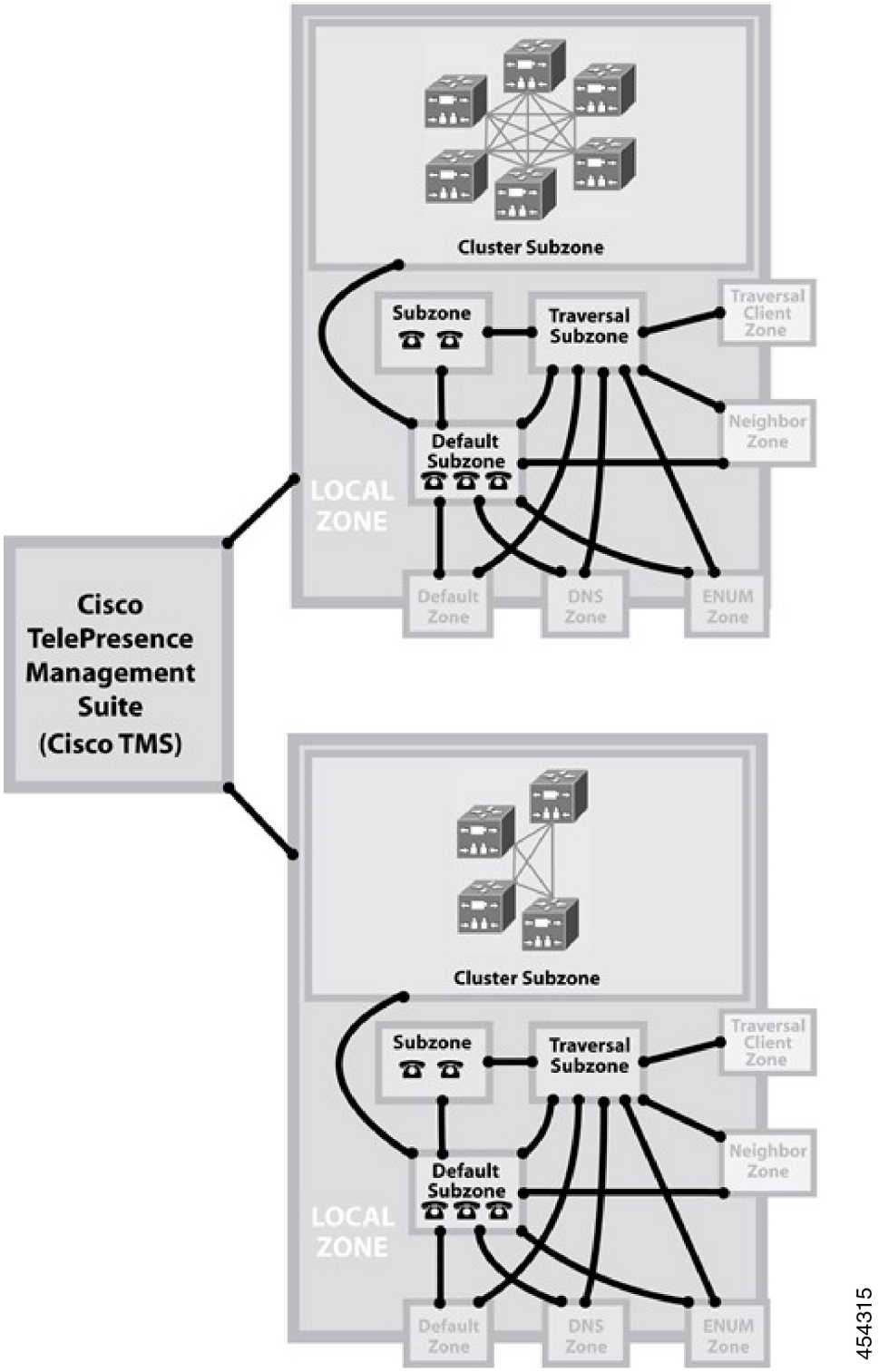
クラスタについて

Expressway は最大 6 つの Expressway で構成されるクラスタに含めることができます。クラスタ内の各 Expressway がクラスタ内の他のすべての Expressway のピアです。クラスタを作成する際は、クラスタ名を定義し、1 つのピアをプライマリとして指定します。このプライマリ ピアの設定が、他のピアに複製されます。クラスタを使用する目的は次のとおりです。

- **キャパシティ** 単一の Expressway と比べて、Expressway 導入環境のキャパシティを引き上げる。
- **復元力**。Expressway がメンテナンスモードを有効にするになっている間、あるいはネットワークの停止や停電またはその他の理由により万が一 Expressway にアクセスできなくなった場合に備え、冗長性を確保します。

（注） キャパシティの増加につながるのは、4 つのピアまでです。たとえば 6 つのピアからなるクラスタでは、5 番目と 6 番目の Expressways はクラスタにコール キャパシティを追加しません。復元力はキャパシティではなく、ピアの追加によって強化されます。

ピアは、帯域幅の使用や、登録数およびユーザ アカウント数に関して互いに情報を共有します。これにより、次に示す例のように、クラスタは 1 つの大規模な Expressway ローカル ゾーンとして機能できます。


Cisco TelePresence Management Suite (Cisco TMS)
Cluster Subzone
Subzone
Traversal Subzone
Traversal Client Zone
Neighbor Zone
Default Subzone
LOCAL ZONE
Default Zone
DNS Zone
ENUM Zone
Cluster Subzone
Subzone
Traversal Subzone
Traversal Client Zone
Neighbor Zone
Default Subzone
LOCAL ZONE
Default Zone
DNS Zone
ENUM Zone
454315

クラスタライセンスの使用方法とキャパシティのガイドライン

このセクションでは、クラスタ全体でライセンスを使用する方法とキャパシティのガイドラインについて説明しています。参照しやすいように、スタンドアロン システムに対応するキャパシティのガイドラインも含めています。

Cisco Expressway シリーズ（Cisco VCS 以外）でサポートされる最大容量とサイズは、次の表にリストされています。実際の導入でパフォーマンスに影響を与える要因が多いため、これらの図はガイドラインについてのみ掲載していますが動作を保証しているわけではありません。Expressway がサポートしているユース ケースが多いので、独自で行う特定の導入に対応する容量制限を実現することはできません。

Expressway のサイジングと容量の情報は、サポートされている同時登録またはコールの数に基づいて分類されています。

重要な警告

- ここで示す図は、必要なすべてのソフトウェアライセンスが適用されている場合を想定しています。
- この数値は、特定かつ専用の Expressway シナリオでテストされたものです。Expressway またはクラスタに基づいて、単一のサービスまたはシナリオに使用されます（たとえば、MRA または B2B コールに対する場合など）。マルチサービス導入のためのテスト済みキャパシティガイドラインを提供することはできません。
- 最大 6 つの Expressway システムをクラスタ化できますが、キャパシティは**最大で 4 つ**増加します（ゲインがないスモール VM を除く）。
- 小規模な VM の場合、クラスタリングは冗長性のためだけに使用され、スケーリングには使用されず、**クラスタリングによる容量の増加もありません**。
- ビデオコールと音声専用コールに提供される数字は選択肢です。指定されたキャパシティはビデオと音声のどちらでも使用できます。両方には使用できません。

依存関係

コールに対応する数は、同時コール数を表します。

同時コールとリッチ メディア セッション（RMS）ライセンスは、1 対 1 の関係がありません。さまざまな要因によって RMS ライセンスの使用が決定されます。つまり、いくつかのコールが「自由」に使用されており、他のコールは複数のライセンスを使用している場合があります。

6000 TURN リレーをサポートするには、大規模システム（大規模な VM または CE1200）に対して 「[大規模 Expressway の TURN ポートを多重化（TURN Port Multiplexing on Large Expressway）]」 を有効にする必要があります（**[設定 (Configuration)]** > **[トラバース（Traversal）]** > **[TURN]**）。

小規模 VM は、Cisco Business Edition 6000 プラットフォームまたは Cisco Business Edition 6000 仕様に一致する汎用ハードウェア / ESXi でサポートされています。小規模 VM の数字は、M5 ベースの BE6000 アプライアンスに対応しています。

スタンドアロン システムのキャパシティ数

次の表は、スタンドアロン Expressway の基本キャパシティを表しています。

表 *20 :* スタンドアロンキャパシティのガイドライン：シングル *Expressway*

プラットフォーム（**Platform**）	登録（ルーム/デスクトップ）	コール（ビデオまたは音声のみ）	**RMS** ライセンス	**MRA** 登録（プロキシ実施済み）	**TURN** リレー*
CE1200	5,000	500 ビデオまたは 1000 音声	500	5000	6000
大規模 VM	5,000	500 ビデオまたは 1000 音声	500	2500	6000
中規模 VM	2,500	100 ビデオまたは 200 音声	100	2,500	1800
小規模 VM	2000	40の 非 MRA ビデオ、または 20 MRA ビデオまたは 40 音声	75	200	1800

クラスタ システムのキャパシティ数

次の表は、4 つの Expressways（スケール ゲインの最大クラスタ サイズ）を搭載したクラスタ システムのキャパシティが増えた状態を示しています。

2 つまたは 3 つのノードを持つクラスタのキャパシティを決定するには、2 または 3 の因数をそれぞれスタンドアロンの数字に適用します。クラスタ化システムとスタンドアロンシステムの数値が常に同じ小規模VMを除きます（小規模VMのクラスタ化によってキャパシティゲインが得られるため）。

表 *21* : クラスタ化されたキャパシティのガイドライン：*4* つの機能を搭載したクラスタの例

プラットフォーム（**Platform**）	登録（ルーム/デスクトップ）	コール（ビデオまたは音声のみ）	**RMS** ライセンス	**MRA** 登録（プロキシ実施済み）	**TURN** リレー*
CE1200	20,000	2000 ビデオまたは 4000 音声	2000	20,000	24,000
大規模 VM	20,000	2000 ビデオまたは 4000 音声	2000	10,000	24,000
中規模 VM	10,000	400 ビデオまたは 800 音声	400	10,000	7200
小規模 VM	2000	40の 非 MRA ビデオ、または 20 MRA ビデオまたは 40 音声	75	200	1800

導入例

たとえば、デスクトップへの登録を最大 750 件同時に実施して 250 件のリッチメディアセッションを処理できる耐障害性クラスタを導入する必要があるとします。この場合は、次のようにして 4 つのピアを設定することができます。

	ピア 1	**ピア 2**	**ピア 3**	**ピア 4**	**総クラスタ容量**
デスクトップ登録ライセンス	250	250	250	0	750
リッチ メディア セッション	100	100	50	0	250

この例ではライセンスはすべてのピアで共有されるため、エンドポイントがどのピアに登録するかは問題になりません。ピアのいずれかが一時的にサービスを中断しても、一連のコールライセンスのすべてを、そのままクラスタ全体で使用できます。

クラスタ内のコール

エンドポイントが同じクラスタ内の異なるピアに登録されたライセンス使用状況は、クラスタ全体のコール メディア トラバーサルによって異なります。

- コールメディアがクラスタピアを通過しない場合、エンドポイント間のコールは RMS ライセンスを使用しません（「「登録済み」」のコールです）。
    - エンドポイントの 1 つがシスコインフラストラクチャに登録されていない場合、コールは RMS ライセンスを使用します。

- コールメディアがクラスタピアを通過する場合、エンドポイント間のコールでは、B2BUA が使用されている場合に、管理対象の RMS ライセンスが使用されます。
  - 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、コールは、実効的なライセンスを使用しません。

クラスタ化システムでのライセンスの使用方法の詳細については、このガイドの「ライセンス」セクションを参照してください。

クラスタとピアの管理

クラスタのセットアップ

始める前に

1. ご使用のバージョンに対応する『*Cisco Expressway* クラスタ作成および保守導入ガイド』（Cisco Expressway シリーズ設定ガイドページに用意されています）に記載されているすべての前提条件が満たされていることを確認してください。
2. クラスタをセットアップする前に Expressway データをバックアップすることを推奨します。手順については、『*Cisco Expressway* クラスタの制作および保守導入ガイド』を参照してください。

プロセス

クラスタを作成するには、最初にプライマリ ピアを設定してから、その他のピアを一度に 1 つずつクラスタに追加します。

クラスタの管理

「クラスタリング（Clustering）」ページ（**[システム（System）] > [クラスタリング（Clustering）]**）には、この Expressway が属するクラスタ内のすべてのピアの IP アドレスのリストが表示され、プライマリとして設定されているピアが識別されます。

クラスタ構成の基本

- **[クラスタ名（Cluster name）]** を使用して、Expressway の 1 つのクラスタを他のクラスタから識別します。この Expressway クラスタに対応する SRV レコードで使用する完全修飾ドメイン名（FQDN）に設定します（例：**cluster1.example.com**）。

  FQDN は複数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。クラスタ名は FindMe が有効になっている場合に必要です。

- すべてのピアが、**プライマリとして設定**するピアについて同意する必要があります。各ピアに同じ番号を使用し、すべてのピアで **[ピア N アドレス（Peer N addresses）]** リストを同じ順序にしておきます。
- すべてのピアは同じ IP バージョンを使用する必要があります。すべてのピアで [クラスタ IP バージョン（Cluster IP version）] を同じ値に設定します。
- すべてのピアで同じ [TLS 検証モード（TLS verification mode）] を使用する必要があります。セキュリティを強化するには、*[強制（Enforce）]* を選択しますが、ピアは信頼できる CA に対して互いの証明書を検証できる必要があることに注意してください。
- [クラスタ アドレス マッピング（Cluster Address Mapping）] オプションを使用すると、Cisco Expressway-E ピアの FQDN をプライベート IP アドレスにマッピングできます。クラスタ アドレス マッピングを使用すると、パブリック DNS とピアのパブリック IP アドレスを使用する必要がないため、隔離されたネットワークにピアの TLS クラスタリングを適用することができます。

詳細は、Expressway 設定ガイドページの『*Cisco Expressway* クラスタの作成とメンテナン導入ガイド』を参照してください。

クラスタのその他の設定

設定変更はプライマリ Expressway のみで行う必要があります。

注意 実行中のすべてのピアでクラスタが安定するまで、クラスタ全体の設定を変更しないでください。いずれかのピアがアップグレード中または再起動中である、あるいはサービスを使用できない状態でクラスタ設定の変更を行った場合、クラスタデータベースの複製により悪影響が及ぶ恐れがあります。

注意 Dbxsh は、ポート 4370 を使用してローカルループバックアドレス上のクラスタ データベースに接続するスクリプトです。Dbxsh は、コマンドを実行する前にデータベースを認証する必要がありません。ポートは接続用に開いており、内部使用のみを目的としています。これはルートからのみアクセスできます。

他のピアに対する変更がクラスタ全体に反映されることはなく、次にプライマリの設定がピア全体に複製された場合に上書きされます。一部のクラスタ化システムのピア固有の項目については例外です。

クラスタ内のすべてのピアに変更で更新されるまで、最大 1 分待つ必要があります。

クラスタに対するピアの追加と削除

クラスタをセットアップした後は、新しいピアをクラスタに追加したり、クラスタからピアを削除したりできます。詳細については 、「*Expressway* クラスタの作成およびメンテナンス導入ガイド」を参照してください 。

⚠

注意 クラスタリングページからすべてのピアアドレス フィールドをクリアして設定を保存した場合、Expressway を次に再起動したときに、自動的に Expressway が初期設定にリセットされます。つまり、LAN1 インターフェイスの基本的なネットワーク設定を除き、既存の設定のすべてを失うことになります。これには、フィールドをクリアしてから次に再起動するまでに行ったすべての設定も含まれます。

プライマリ ピアの変更

通常は、次の場合の **[プライマリ設定（Configuration primary）]** を変更する必要があります。

- 元のプライマリ ピアに障害が発生した場合（プライマリに障害が発生した場合、プライマリから設定をコピーできなくなり互いに同期できない状態になった場合を除き、残りのピアは通常どおりに機能し続けます。）
- プライマリ Expressway ユニットをサービスから外す必要がある場合

プライマリピアを変更する方法の詳細については、*Expressway* クラスタの作成とメンテナンス導入ガイドを参照してください。

クラスタ ステータスのモニタリング

「**クラスタリング（Clustering）**」ページの下部にあるステータスのセクションには、クラスタの現在のステータスと前回および次回の同期の時刻が表示されます。

クラスタ問題のトラブルシューティング

クラスタ レプリケーションの問題のトラブルシューティングを参照してください。

クラスタ化システムのピア固有の項目

設定のほとんどの項目は、プライマリ ピアを介してクラスタ内のすべてのピアに適用されます。ただし、次の項目（Web インターフェイスでは † でマークされます）は各クラスタ ピアで個別に指定する必要があります。

すべてのピアに適用される設定データは、プライマリピア上でのみ変更する必要があります。そうしないと、最良の場合、変更はプライマリから上書きされ、最悪の場合、クラスタの複製は失敗します。

セットアップウィザードを選択できます

サービスセットアップウィザードを使用して行った設定（タイプの選択、サービスの選択、それらのサービスのライセンス、および基本的なネットワーク設定）は、クラスタの各ピアで設定する必要があります。

クラスタ構成（[System] > [Clustering]）

クラスタを構成する**ピアNアドレス**（ピア自身のアドレスを含む）のリストは、各ピアで指定する必要があり、すべてのピアで同一である必要があります。

各ピアに**[クラスタ名（Cluster name）]**、**[設定プライマリ（Configuration primary）]**、および**[クラスタ IP バージョン（Cluster IP version）]**を指定し、すべてのピアでこれらの項目が一致する必要があります。

クラスタアドレスマッピングを有効にする必要がある場合は、最初にクラスタを IP アドレスで形成することをお勧めします。その後は、1 つのピアにマッピングを追加するだけで済みます。

イーサネット速度（[システム（System）] > [ネットワーク インターフェイス（Network interfaces）] > [イーサネット（Ethernet）]）

イーサネット速度は、各ピアに固有です。各ピアでは、イーサネットスイッチに接続するために多少異なる要件がある場合があります。

IP 設定（[System] > [Network interfaces] > [IP]）

LAN の設定は、各ピアで固有です。

- **IPv4 アドレス**、**IPv6 アドレス**、またはこの両方であるかにかかわらず、ピアごとに一意の IP アドレスが必要です。
- **IP ゲートウェイ**の設定はピアに固有です。各ピアで異なるゲートウェイを使用できます。

（注） 各ピアが同じプロトコルをサポートする必要があるので、IP プロトコルがすべてのピアに適用されます。

IP スタティック ルート（[システム（System）]> [ネットワーク インターフェイス（Network interfaces）] > [スタティック ルート（Static routes）]）

追加するスタティックルートはピアに固有なので、必要に応じて、異なるルートを異なるピアで作成できます。クラスタ内のすべてのピアが同じスタティックルートを使用できるようにする場合は、各ピアでルートを作成する必要があります。

システム名（[システム（System）] > [管理（Administration）]）

システム名はクラスタ内のピアごとに異なっている必要があります。

DNS サーバと DNS ホスト名（[System] > [DNS]）

DNS サーバは、各ピアに固有です。各ピアで異なる DNS サーバのセットを使用できます。

システム ホスト名と**ドメイン名**は各ピアに固有です。

NTP サーバとタイム ゾーン（[System] > [Time]）

NTP サーバは各ピアに固有です。各ピアで、1 つ以上の異なる NTP サーバを使用できます。

タイム ゾーンは各ピアに固有です。各ピアで異なる現地時間を設定できます。

SNMP（[System] > [SNMP]）

SNMP 設定は、各ピアに固有です。また、各ピアで異なることができます。

ロギング（[メンテナンス（Maintenance）] > [ロギング（Logging）]）

各ピアのイベント ログおよびコンフィグレーション ログは、特定の Expressway のアクティビティのみを報告します。**ログ レベル**と**リモート syslog サーバ**のリストは各ピアに固有です。すべてのピアのログを送信できるリモート syslog サーバを設定することを推奨します。これにより、クラスタ内のすべてのピア間でアクティビティの全体像を把握できます。

セキュリティ証明書（[メンテナンス（Maintenance）] > [セキュリティ（Security）]）

Expressway が使用する信頼できる CA 証明書とサーバ証明書および証明書失効リスト（CRL）は、ピアごとに個別にアップロードする必要があります。

管理アクセス（[システム（System）] > [管理（Administration）]）

次のシステム管理アクセス設定は各ピアに固有です。

- シリアル ポート/コンソール
- SSH サービス
- Web インターフェイス（HTTPS 経由）
- HTTP リクエストを HTTPS にリダイレクト
- 自動保護サービス

オプション キー（[メンテナンス（Maintenance）] > [オプション キー（Option keys）]）

このセクションは、PAK ベースのライセンスを使用するシステムにのみ適用されます（オプションキーは、システムでスマートライセンシングを使用している場合は適用されません）。オプションキーは、ライセンスまたは特定の機能を制御できます。Expressway 向けには段階的に切り分け、使用が減少しています。

ライセンスを制御するオプションキーは、クラスタ全体で使用するようにプールされています。

機能を制御するオプションキー（高度なアカウントセキュリティや Microsoft 相互運用性など）は、適用されるピアに固有のキーです。各ピアには同一の機能オプションキーがインストールされている必要がありるため、機能にオプションキーを使用する場合は、クラスタ内のピアごとにキーを購入する必要があります。

ライセンス オプション キーは、クラスタ内の 1 つ以上のピアに適用できます。インストール済みライセンスの合計がクラスタ全体で使用できます。ライセンス プーリング動作には次のオプション キーが含まれます。

- リッチ メディア セッション
- TelePresence Room システム
- デスクトップ システム

（注） クラスタ内でライセンスが使用できても、必要なライセンスを有効にするキーがないことを示すアラームがピアに表示される場合があります。必要なライセンスがインストールされたピアが 1 つだけで、サービスを中断していない限り、このカテゴリのアラームは確認して、無視できます。

Active Directory サービス（[設定（Configuration）] > [認証（Authentication）] > [デバイス（Devices）] > [Active Directory サービス（Active Directory Service）]）

デバイス認証のために Active Directory サービスへの接続を設定する場合、**[NetBIOS マシン名（上書き）（NetBIOS machine name (override)）]** とドメイン管理者の **[ユーザ名（Username）]** および **[パスワード（Password）]** は各ピアに固有です。

Conference Factory テンプレート（[アプリケーション（Applications）] > [Conference Factory]）

Conference Factory アプリケーションで会議サーバにコールをルーティングするために使用するテンプレートは、クラスタ内の各ピアに固有です。

ピア間での登録の共有

クラスタ ピアが検索要求（INVITE など）を受信すると、応答前にそれ自体の登録リストとそのピアの登録リストを確認します。これにより、クラスタ内のすべてのエンドポイントが単一の Expressway に登録されているかのように処理されます。

ピアは定期的に照会することで、機能し続けていることを確認します。

H.323 の登録

クラスタ内のすべてのピアは、H.323 エンドポイント コミュニティの責任を共有します。H.323 エンドポイントを 1 つのピアに登録すると、そのピアは代替ゲートキーパーのリストを含んだ登録応答を受信します。そのリストには、クラスタ内の他のすべてのピアの IP アドレスが無作為に示されています。

エンドポイントが最初のピアとの通信を失った場合、他のピアの 1 つに登録しようとします。代替ピアの無作為の順序で示されたリストによって、単一の代替ピアしか保存できないエンドポイントがクラスタに均一にフェールオーバーするようにします。

クラスタを使用すると、クラスタ内のすべてのピアの登録の **[存続時間（Time to live）]** をデフォルトの 30 分から短縮できます。この設定により、エンドポイントで Expressway への再登録が必要な頻度を決定します。これを短縮することによって、クラスタが使用できなくなった場合に、エンドポイントが使用できるピアにより迅速にフェールオーバーできるようになります。

（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。

この設定を変更するには、**[設定（Configuration）]** > **[プロトコル（Protocols）]** > **[H.323]** > **[ゲートキーパー（Gatekeeper）]** > **[存続時間（Time to live）]** に移動します。

SIP の登録

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。

また、DNS ラウンドロビンのテクニックを使用して登録フェールオーバー戦略を実装することもできます。Jabber Video などの一部の SIP UA は、FQDN である SIP サーバ アドレスを使用して設定できます。FQDN がクラスタ内のすべてのピアの IP アドレスで埋め込まれたラウンドロビン DNS レコードを解決した場合、エンドポイントは元のピアへの接続が失われたときに別のピアに再登録できます。

ピア間での帯域幅の共有

クラスタリングが設定されている場合、すべてのピアはクラスタに使用可能な帯域幅を共有します。

- ピアは、サブゾーン、リンク、パイプなど、帯域幅制御のすべての側面について同じに設定する必要があります。
- ピアはクラスタ内の他のすべてのピアと使用率情報を共有するため、1 つのピアが特定のサブゾーン内または特定のサブゾーンから、あるいは特定のパイプ上で使用可能なすべての帯域幅の一部を使用している場合、他のピアがこの帯域幅を使用できなくなります。

Expressway による帯域幅の管理方法の一般的な情報については、「帯域幅制御について」の項を参照してください。

クラスタのアップグレード、バックアップ、および復元

クラスタのアップグレード

ご使用のバージョンについては、Cisco Expressway シリーズ構成ガイドページの『*Cisco Expressway* クラスタ作成および保守導入ガイド』を参照してください。

（注） 以前のバージョンから X8.8 以降にアップグレードする場合、X8.8 では IPSec ではなくピア間の TLS 接続を使用するようにクラスタリング通信が変わりました。アップグレード後に TLS 検証は実行されません (デフォルト) 。TLS 検証の実行を促すアラームが表示されます。

クラスタのバックアップ

クラスタ設定情報を保存するには、Expressway データのバックアップと復元プロセスを使用します。バックアップ プロセスで、バックアップを行うために使用する Expressway にかかわらず、クラスタのすべての設定情報が保存されます。

注意 Cisco Expressway システムの VMware スナップショットは作成しないでください。このプロセスはデータベース タイミングに干渉し、パフォーマンスに悪影響を及ぼします。

クラスタの復元

以前にバックアップされているクラスタ設定データを復元するには、次のプロセスを実行します。

重要 クラスタの一部である Expressway にはデータを復元できません。本項で説明したように、最初にクラスタから Expressway ピアを削除します。次に復元を実行します。（復元後、新しいクラスタを構築する必要があります）。

1. スタンドアロン Expressway になるように、クラスタから Expressway ピアを削除します。
2. スタンドアロン Expressway に設定データを復元します。詳細については、以前のバックアップの復元を参照してください。
3. 復元されたデータがある Expressway を使用して新しいクラスタを構築します。
4. 他のピアそれぞれを以前のクラスタから取得し、それらを新しいクラスタに追加します。詳細については、クラスタのセットアップを参照してください。

（注） FQDN を使用していて、有効なクラスタアドレスマッピングが設定されている場合は、追加の手順は必要ありません。マッピングは、復元操作で構成されます。

Cisco TMS のクラスタリング

FindMe やデバイス プロビジョニングを使用するようにクラスタが設定されている場合は、Cisco TMS のバージョン 13.2 以降が必要です。

クラスタとプロビジョニングのサイズの制限

あらゆる規模の Expressway クラスタでサポートされる最大値は次のとおりです。

- 10,000 個の FindMe アカウント
- 10,000 人のプロビジョニングするユーザ
- 200,000 の電話帳エントリ

（注） システムのクラスタ ライセンスの使用方法とキャパシティのガイドラインが上記の設定よりも大きい場合でも、クラスタごとの FindMe アカウント/ユーザ数は 10,000、プロビジョニングできるデバイス数は 10,000 に制限されます。

10,000 を超えるデバイスをプロビジョニングする必要がある場合、ご使用のネットワークには、適切に設計され、ダイヤル プランが設定された追加の Expressway クラスタが必要になります。

ご使用のバージョンについては、Cisco Expressway シリーズ構成ガイドページの『*Cisco Expressway* クラスタ作成および保守導入ガイド』を参照してください。

クラスタ サブゾーンについて

複数の Expressways をまとめてクラスタ化すると、クラスタのローカル ゾーン内に新しいサブゾーンが作成されます。これがクラスタサブゾーンです（クラスタについての項に記載されている図を参照）。クラスタ内の 2 つのピア間のコールはコールのセットアップ時にこのサブゾーンを介して短時間で通過します。

クラスタ サブゾーン（トラバーサル サブゾーンなど）は、コール ルーティングのみに使用する仮想サブゾーンであり、エンドポイントはこのサブゾーンに登録できません。2 つのピア間にコールが確立されると、クラスタ サブゾーンはコール ルートには現れなくなり、コールがデフォルトのサブゾーンから着信したように（またはルーティングされたように）示されます。

クラスタ サブゾーンを通じてコールが通過するのは次の 2 つの場合です。

- 2 つのエンドポイント間のコールがクラスタ内の異なるピアに登録される。

  たとえば、エンドポイント A はデフォルトのサブゾーンでピア 1 に登録され、エンドポイント B はデフォルトのサブゾーンで、ピア 2 に登録されているなどです。A が B にコールすると、そのコール ルートがピア 1 には [**デフォルト サブゾーン -> クラスタ サブゾーン**（**Default Subzone -> Cluster Subzone**）] と表示され、ピア 2 には **[クラスタサブゾーン -> デフォルトサブゾーン**（Cluster Subzone -> Default Subzone）] と表示されます。

- 1 つのピアがクラスタの外部から受信した別のピアに登録されたエンドポイント宛のコール。

  たとえば、本社の 4 つの Expressway で構成されるクラスタに隣接する支店用の単一の Expressway があるとします。支店のユーザが本社のエンドポイント A をコールします。エンドポイント A はデフォルトのサブゾーンでピア 1 に登録されます。ピア 2 がコールを受信します。このコールはその時点でリソース使用率が最低でした。ピア 2 はクラスタ内のローカル ゾーン内のエンドポイント A を検索し、ピア 1 に登録されていることを検出します。ピア 2 はそのコールをピア 1 に転送し、ピア 1 はそのコールをエンドポイント A に転送します。この場合、ピア 2 では、コール ルートが [**支店 -> デフォルト サブゾーン -> クラスタサブゾーン**（Branch Office -> Default Subzone -> Cluster Subzone）] と表示され、ピア 1 では [**クラスタサブゾーン -> デフォルトのサブゾーン**（Cluster Subzone -> Default Subzone）] と表示されます。

（注） **[コール シグナリングの最適化（Call signaling optimization）]** が *[オン（On）]* に設定されており、コールが H.323 の場合、そのコールはピア 2 には表示されず、ピア 1 にはルートが **[支店（Branch Office）]>[デフォルトのサブゾーン（Default Subzone）]** と表示されます。

Expressway クラスタ間の隣接化

ローカルの Expressway（または Expressway クラスタ）をリモート Expressway クラスタに隣接することができます。リモートクラスタは、ローカルシステムへのネイバー、トラバーサルクライアント、またはトラバーサルサーバなどです。ローカルの Expressway でコールを受信し、関連するゾーンを経由してリモートクラスタに渡された場合、ネイバークラスタのリソース使用率が最も低いピア（メンテナンスモードのピアは考慮されません）にルーティングされます。そのピアは、コールを次のいずれかの方法に転送します。

- ローカルに登録されたエンドポイント（エンドポイントがそのピアに登録されている場合）。
- ピア（エンドポイントがクラスタ内の別のピアに登録されている場合）。
- エンドポイントが他の場所にある場合は、外部ゾーンです。

最も低いリソース使用率は、ピア上の使用可能なメディア セッション数（最大 - 現在の使用率）を比較して、最大数を持つピアを選択することで決定されます。

ピアとして設定されている Expressway は、**相互にネイバーとして設定することも、その逆を設定することもできません。**

ネイバークラスタへのプロセス

リモートクラスタへの接続を表す単一のゾーンをローカルシステムに作成し、リモートクラスタ内のすべてのピアの詳細を使用して設定します。ゾーンにこの情報を追加することで、個別のピアの状態に関係なく、コールがそのクラスタに確実に渡ります。

1. ローカルの Expressway（またはクラスタのプライマリピア）で、適切なタイプのゾーンを作成します。
2. [ロケーション（Location）] セクションで、[ピア 1（Peer 1）] から [ピア 6（Peer 6）] のアドレス フィールドにリモート クラスタ内の各ピアの IP アドレスまたは FQDN を入力します。**トラバーサル サーバ** ゾーンの場合は、これらの接続はリモート システムの IP アドレスを指定して設定されていないため、アドレスを入力することはありません。

   これらのフィールドで FQDN を使用するのが理想です。各 FQDN が異なっていて、各ピアに対して単一の IP アドレスに解決される必要があります。IP アドレスでは、TLS 検証を使用できない場合があります。CA の多くは IP アドレスを認証するための証明書を発行しないからです。

   リモート Expressway クラスタ内のピアがここでリストされる順序は重要ではありません。

（注） 追加の Expressway をクラスタに追加する場合は、そのクラスタに隣接する Expressway を変更して、新しいピアについてユーザに知らせる必要があります。

クラスタ レプリケーションの問題のトラブルシューティング

クラスタの複製は、さまざまな理由で失敗する可能性があります。ここでは、最も一般的な問題とそれらの解決方法について説明します。詳細の参照先は次のとおりです。

ご使用のバージョンについては、Cisco Expressway シリーズ構成ガイドページの『*Cisco Expressway* クラスタ作成および保守導入ガイド』を参照してください。

一部のピアに別のプライマリ ピアが定義されている

1. クラスタ内の各ピアを確認するには、**[システム（System）]>[クラスタリング（Clustering）]** ページに移動します。
2. 各ピアで同じ [プライマリ設定（Configuration primary）] を指定していることを確認します。

クラスタ設定のプライマリ ピアに到達できない

次を含むさまざまな理由で、プライマリ ピアとして動作している Expressway に到達できません。

- ネットワーク アクセスの問題
- Expressway ユニットの電源の切断
- アドレスの誤設定
- [TLS 検証モード（TLS verification mode）] は [強制（Enforce）] に設定されているが、一部のピアに無効または失効した証明書がある
- ピアにバージョンが異なるソフトウェアがある
- クラスタ内の DNS 設定が正しくない

「「設定を手動で同期させる必要があります（Manual synchronization of configuration is required）」」というアラームが下位のピア Expressway で発生する

1. CLI を使用してピアに **admin** としてログインします（CLI はデフォルトでは SSH で使用できます。また、各種ハードウェア バージョンのシリアル ポートを介して使用することもできます）。
2. 次に、**xCommand ForceConfigUpdate** と入力します。

これにより、下位 Expressway ピアの設定が削除され、設定を強制的にプライマリ Expressway から更新します。

注意 プライマリ Expressway では決してこのコマンドを実行しないでください。実行すると、クラスタのすべての設定が失われます。

Expressway ピアで 「クラスタの設定エラー」アラームが発生する

発生したアラームの説明に従って、クラスタリングページで新しい設定プライマリを指定できます。

（注） すべてのレプリケーションアラームが解除されたら、古い構成のプライマリに戻すことができます。

不正な IP から FQDN へのマッピング

1. 任意のピアで **[システム（System）]** > **[クラスタリング（Clustering）]** のページに移動します。
2. すべての FQDN と IP アドレスが正しく入力されていることを確認します。

クラスタ通信を妨げるファイアウォール

- パブリック IP アドレスを使用してクラスタリングする場合は、クラスタ通信ポートをブロックしてファイアウォールがクラスタ通信を妨げていないことを確認します。妨げている場合は、ファイアウォール ルールを変更できるかどうかを検討してください。
- プライベートアドレスを使用してクラスタリングする場合は、推奨事項に従ってクラスタを構成してください。つまり、IP アドレス マッピングを使用する FQDN と TLS 認証を使用してクラスタを形成します。

システムキーに関する問題のトラブルシューティング

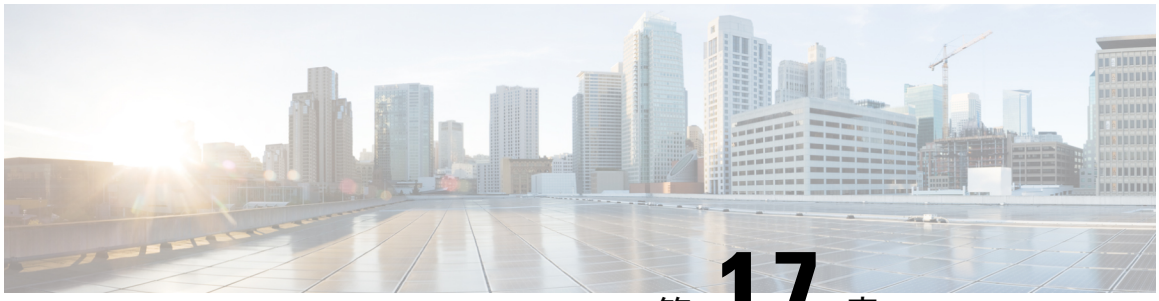
このセクションでは、システムキーに関連する最も一般的な問題と、それらを解決する方法について説明します。

「「キーファイルの更新に失敗しました」」アラームは、Expresswaysで発生します（単一ノードのシナリオ）

1. CLI を使用して admin としてログインします（CLI はデフォルトでは SSH で使用できます。また、各種ハードウェア バージョンのシリアル ポートを介して使用することもできます）。
2. **xCommand ForceSystemKeyUpdate** を入力します。

「「キーファイルの更新に失敗しました」」アラームは、Expresswaysで発生します（クラスタのシナリオ）

1. このアラームが発生しない CLI（SSH 経由およびハードウェアバージョンのシリアルポート経由でデフォルトで利用可能）を介して管理者としてノードにログインします。
2. **xCommand ForceSystemKeyUpdate** を入力します。



第 17 章

ダイヤル プランとコール処理

ここでは、[設定（Configuration）]のサブメニューの[コール（Calls）]、[ダイヤルプラン（Dial plan）]、[トランスフォーメーション（Transforms）]、および[コール ポリシー（Call Policy）]に表示されるページについて説明します。これらのページは、Expresswayがコールを受信して処理する方法を設定するために使用されます。

コール ルーティング プロセス

Expresswayの機能の1つに適切な宛先へのコールのルーティングがあります。これは、指定されたターゲットエイリアスを見つけるために着信検索要求を処理することで行われます。これらの検索要求は次の場所から送信されます。

- ローカルで登録済みのエンドポイント

- ネイバー、トラバーサルクライアント、トラバーサルサーバなどのネイバーシステム
- パブリックインターネットのエンドポイント

コールの宛先の特定には多くの手順があり、これらの手順の一部にはエイリアスの変換や他のエイリアスへのコールのリダイレクトが含まれています。

エイリアスを元の形式から別の形式に変換し、その後で元のエイリアスに戻す場合に循環参照を避けるには、ダイヤルプランの構築をセットアップする前にプロセスを理解していることが重要です。Expressway は循環参照を検出できます。循環参照を特定すると、VCS は検索のそのブランチを終了させ、「「ポリシーのループを検出しました（policy loop detected）」」というエラーメッセージを返します。

Expressway によるコールの宛先の決定方法

次に、宛先のエンドポイントを見つけようとするときに Expressway が従うプロセスについて説明します。

1. 発信者がエンドポイントに宛先エンドポイントのエイリアスまたはアドレスを入力します。このエイリアスまたはアドレスは、サポートされているアドレス形式をとることができます。
2. 宛先アドレスは、Expressway で受け取られます

   （アドレスは、登録済みのエンドポイントから Expressway へ直接送られるか、または導入の他のコール処理インフラストラクチャの結果として間接的に送られることもあります）。
3. エイリアスには、すべての検索前トランスフォーメーションについてが適用されます。
4. すべてのコール ポリシーの設定が（変換後の）エイリアスに適用されます。その結果、1 つ以上の新しいターゲットエイリアスとなった場合、その新しいエイリアスを検索前のトランスフォーメーションと照合してチェックすることからプロセスが再開されます。
5. すべてのユーザ ポリシー（FindMe についてが有効になっている場合）がエイリアスに適用されます。エイリアスが 1 つ以上の新しいエイリアスを解決する FindMe ID である場合、検索前のトランスフォーメーションとコールポリシーと照合して結果のすべてのエイリアスを確認することからプロセスが再開されます。
6. 次に、Expressway は検索ルールに従ってエイリアスを検索します。

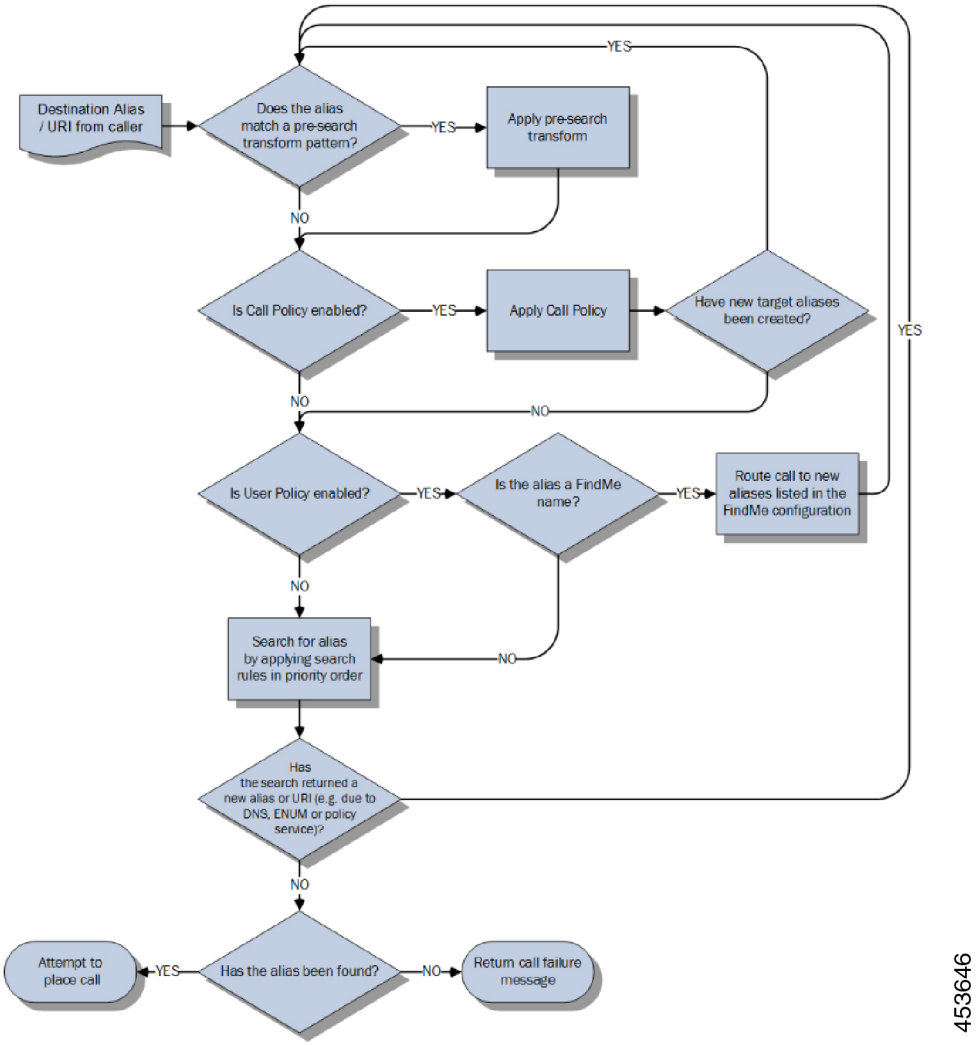
（注） Expressway は意図的に H.323 ロケーション要求から読み取った最初の宛先エイリアスのみを検索します。稀に、これによってコールが予想どおりにルーティングされないことがあります。

- マッチング ルールで、クエリを**ターゲット**に送信する前に、ゾーン トランスフォーメーションをエイリアスに適用する場合があります。**[ターゲット（Target）]** には、次のいずれかのタイプを指定できます。
  - **ローカルゾーン**：Expressway に登録されたエンドポイントとデバイス。

- **ネイバー ゾーン**：Expressway の設定済みの外部ネイバー ゾーンの 1 つ、あるいは DNS または ENUM のルックアップ ゾーン。
- **ポリシー サービス**：外部サービスやアプリケーション。サービスは、コールをルーティングする必要があるゾーンを指定するか、または新しい宛先エイリアスを指定するなどの CPL を返します。

7. 検索で新しいURIまたはエイリアスが返された場合（DNSまたはENUMのルックアップ、あるいはポリシー サービスからの応答などのため）、プロセスは再開され、検索前トランスフォーメーションに照合して新しい URI を確認し、コール ポリシーとユーザ ポリシーを適用してから、新しい Expressway 検索を実行します。
8. ローカル ゾーン内、外部ゾーンの 1 つでエイリアスが検出された、またはポリシー サービスによってルーティング先が返された場合、Expressway はコールを発信しようとします。
9. エイリアスが検出されなかった場合は、コールが失敗したことを通知するメッセージで応答します。

図 *15 :* コールルーティングのフローチャート



Cisco VCS のディレクトリサービスについて

ホップ カウントの設定

各検索要求には、その検索を開始したシステムによってホップ カウント値が割り当てられます。要求が別のネイバー ゲートキーパーまたはプロキシに転送されるたびに、ホップ カウント値は 1 ずつ減っていきます。ホップ カウントが 0 に達すると、要求はそれ以上は転送されず、検索は失敗します。

ローカル Expressway によって開始された検索要求では、要求に割り当てるホップ カウントをゾーンごとに設定できます。ゾーンのホップ カウントは、ローカル Expressway から開始され、そのゾーンに送信されたすべての検索要求に適用されます。

別のゾーンから受信した検索要求には、ホップ カウントがすでに割り当てられています。その要求をさらにネイバー ゾーンに転送すると、2 つの値（元のホップ カウントとそのゾーン用に設定されたホップ カウント）のどちらか小さいほうが使用されます。

H.323 では、ホップ カウントは検索要求のみに適用されます。SIP では、ホップ カウントはゾーンに送信されたすべての要求に適用されます（要求の [Max-Forwards] フィールドに影響します）。

ホップ カウント値には、1 ～ 255 を指定できます。デフォルトは 15 です。

（注） ホップカウントを必要以上に高く設定すると、ネットワークにループを発生させるリスクがあります。このような場合、検索要求は、ホップ カウントが 0 に到達するまでネットワークに送信され、リソースを不必要に消費します。これは、コール ルーティングとシグナリングの設定を *[オン（On）]* に設定することによって防ぐことができます。

URI または ENUM によるダイヤリングでは、使用するホップ カウントは、宛先エンドポイント（または 関連付けられた DNS あるいは中間の SIP プロキシまたはゲートキーパー）を介して検出された、関連 DNS ゾーンまたは ENUM ゾーンに対するものです。

ゾーンのホップ カウントの設定

ホップ カウントはゾーンごとに設定します。

重要 ネットワークが複雑な場合は、デフォルトのホップカウントが環境に対して低すぎる可能性があります。これにより、適切に設定された導入で予期しないコールエラーが発生する可能性があります。長いコール パスが予想される場合は、ホップ カウントを増やすことを検討してください。

その他のゾーンオプションの詳細については、ゾーンの設定（デフォルト以外のゾーン）の項を参照してください。

手順

ステップ 1 **[ゾーン（Zones）]** ページ（**[設定（Configuration）]** > **[ゾーン（Zones）]** > **[ゾーン（Zones）]**）に移動します。

ステップ 2 設定するゾーンの名前をクリックします。**[ゾーンの編集（Edit zone）]** ページが表示されます。

ステップ 3 **[設定（Configuration）]**セクションの**[ホップカウント（Hop count）]**フィールドに、このゾーンに使用するホップ カウント値を入力します。

ダイヤル プランの設定

「ダイヤル プランの設定（Dial plan configuration）」ページ（**[設定（Configuration）]** > **[ダイヤル プラン（Dial plan）]** > **[設定（Configuration）]**）を使用して、特定のコールシナリオでの Expressway によるコールルーティング方法を設定します。

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
不明 IP アドレスへのコール（Calls to unknown IP addresses）	Expressway またはそのネイバーの 1 つの登録されていないシステムに Expressway がコールを試行する方法を決定します。 *[直接（Direct）]*：Expressway がネイバーを照会することなく、エンドポイントが不明な IP アドレスにコールできます。端部がローカルシステムに直接登録されていたかのように、コール セットアップが実行されます。 *[間接（Indirect）]*：不明な IP アドレスへのコールを受信すると、Expressway はネイバーにそのリモート アドレスを照会し、許可されれば、ネイバーを通じてコールをルーティングします。 *[オフ（Off）]*：Expressway に直接登録されたエンドポイントが Expressway に直接登録されたシステムの IP アドレスのみをコールする可能性があります。 デフォルトは [間接（Indirect）] です。	この設定は、ゾーン トランスフォーメーションの前、かつ検索前のトランスフォーメーション、コール ポリシーまたはユーザ ポリシーのルールの適用後にコールの宛先アドレスに適用されます。 コール制御に加えて、SIP デバイスへのプロビジョニングメッセージとプレゼンスメッセージは IP アドレスにルーティングされるため、この設定はこれらのメッセージの動作も決定します。 詳細については、IP アドレスによるダイヤリングを参照してください。
フォールバック エイリアス（Fallback alias）	Expressway の IP アドレスまたはドメイン名が指定されていても、コール エイリアスが指定されていないコールの場合に、着信メッセージを発信するエイリアス。	フォールバック エイリアスが設定されていない場合、エイリアスを指定しないコールは切断されます。詳細については、以下を参照してください。

フォールバック エイリアスについて

Expresswayは、それ自体宛でも、エイリアスが指定されていないコールを受信できます。これは、次の理由のいずれかで発生することがあります。

- 発信者が Expressway の IP アドレスを直接ダイヤルした
- 発信者がプレフィックスとしてエイリアスを指定することなく、Expresswayに属するドメイン名（設定されている SIP ドメイン、または Expressway の IP アドレスを示す SRV レコードがあるドメインのいずれか）をダイヤルした

通常、このようなコールは切断されます。ただし、**[フォールバック エイリアス（Fallback alias）]** が指定されている場合、これらのコールはそのエイリアスにルーティングされます。

（注） ユーザがコールの発信先のエイリアスや IP アドレスを入力することを許可しないエンドポイントもあります。

使用例

フォールバックエイリアスを受付係として設定し、エイリアスを指定しないすべてのコールに個別に応答して、適切にリダイレクトするようにできます。

たとえば、ある会社のドメインが **example.com** だとします。受付のエンド ポイントのエイリアスは **reception@example.com** です。Expressway をフォールバック エイリアス、**reception@example.com** で設定します。つまり、**example.com** に直接行われたコール（つまり、エイリアスによるプレフィックスなし）はすべて **reception@example.com** に転送され、受付係がコールに応答して適切に転送されます。

トランスフォーメーションと検索ルールについて

Expressway は、コール ルーティング プロセスの一環として、トランスフォーメーションと検索ルールを使用するように設定できます。

トランスフォーメーション

トランスフォーメーションを使用して、特定の条件に一致した場合に検索要求内のエイリアスを変更します。プレフィックス、サフィックス、または文字列全体を削除または置換したり、正規表現を使用して、エイリアスを変換できます。

このトランスフォーメーションは、ルーティング プロセスの2つのポイントで、検索前のトランスフォーメーションとゾーン トランスフォーメーションとしてエイリアスに適用できます。

- **検索前トランスフォーメーション**は、コール ポリシーまたはユーザ ポリシーが適用される前と検索プロセスが実行される前に適用されます（詳細については、検索前トランスフォーメーションについてを参照してください）。

- **ゾーン トランスフォーメーション**は、検索プロセス時に、必要に応じて個別の検索ルールによって適用されます。検索ルールがエイリアスと一致すると、検索要求がターゲットゾーンまたはポリシーサービスに送信される前に、それを使用してターゲットエイリアスを変更できます（詳細については、検索とゾーン変換プロセスを参照してください。

検索ルール

検索ルールを使用して、適切なターゲット ゾーン（ローカル ゾーンを含む）またはポリシーサービスに着信検索要求を送信します。

Expressway の検索ルールは詳細な設定が可能です。次の操作を実行できます。

- 特定のゾーンまたはポリシーサービスへの検索をフィルタリングするエイリアス、IPアドレス、およびパターン マッチの定義。
- ルールを適用したり、一致が検出された後にプライオリティが下位の検索ルールの適用を中止するためのプライオリティの定義。これにより、送信する可能性がある検索要求の数を削減し、検索プロセスをスピードアップします。
- プロトコル（SIP または H.323）やクエリのソース（ローカルゾーンまたはサブゾーンの特定のゾーン）に応じた異なるルールのセットアップをします。
- 標準ベースの SIP または Microsoft SIP など、特定のタイプのトラフィックにのみ一致するルールのセットアップをします。
- 特定の検索ルールを認証ポリシー（Authentication policy）のみに適用可能にすることによる、未認証デバイスが使用できる宛先またはネットワーク サービスの範囲の制限します。
- クエリがターゲットゾーンまたはポリシーサービスに送信される前にエイリアスを変更するためのゾーントランスフォーメーションの使用します。

（注） 複数の検索ルールが同じターゲットゾーンまたはポリシーサービスを参照できます。つまり、ゾーンまたはポリシー サービスごとに異なる検索条件とゾーン トランスフォーメーションを指定できます。

Expresswayは、指定されたエイリアスを検出するためにゾーンを検索するときに着信コールのプロトコル（SIP または H.323）を使用します。検索が失敗すると、Expressway はその検索元と **[インターワーキング モード（Interworking mode）]**（**[設定（Configuration）]** > **[プロトコル（Protocols）]** > **[インターワーキング（Interworking）]**）に応じて代替プロトコルを使用し、同じゾーンを再度検索することがあります。

- 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。

検索前トランスフォーメーションについて

検索前トランスフォーメーション機能では、着信検索要求のエイリアスを変更できます。トランスフォーメーションは、コール ポリシーまたはユーザ ポリシーの適用前で、検索が実行される前に Expressway によって適用されます。

各検索前トランスフォーメーションはエイリアスを比較する文字列と、その文字列に一致する場合にエイリアスに加える変更を定義します。エイリアスが変換されると、そのエイリアスは変更された状態を維持し、その新しいエイリアスに対してその後のすべてのコール処理が適用されます。

（注） 1 つの検索で一致できる変換は 1 つのみです。

クラスタ化システム

クラスタ内のすべてのピアは、検索前トランスフォーメーションを含めて同じに設定する必要があります。各 Expressway は、任意のピアからの検索要求を Expressway 自体のローカル ゾーンから着信したものとして処理し、要求受信時には検索前トランスフォーメーションを再度適用することはありません。

変換が適用されるのはいつか

- これは、ローカルに登録されたエンドポイント、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のゾーン、ならびにパブリックインターネット上のエンドポイントから受信した着信検索要求すべてに適用されます。
- ピアから受信した要求に適用されません。これらは同じように設定されています。したがって、すでに同じ変換が適用されています。
- Expressway に登録されているエンドポイントから受信した GRQ メッセージまたは RRQ メッセージには適用されません。これらのメッセージに表示されるエイリアスには、エンドポイントが登録されます。

検索前トランスフォーメーションのプロセス

最大100の検索前トランスフォーメーションを設定できます。各トランスフォーメーションには、1 ～ 65534 の一意のプライオリティを付ける必要があります。

1. すべての着信エイリアスは、1に最も近いプライオリティのものから順に各トランスフォーメーションと比較されます。一致した場合、変換がエイリアスに適用され、それ以上の検

索前チェックと新しいエイリアスの変換は実行されません（検索ごとに 1 つの変換のみを一致させることができます）。残りの**コール ルーティング プロセス**には新しいエイリアスが使用されます。

2. これ以降のエイリアスのトランスフォーメーションは残りの検索プロセス中に実行される場合があります。これは、**コール ポリシー**（管理者ポリシーとも呼ばれる）またはユーザ ポリシー（**FindMe** が有効になっている場合）の結果によります。この場合、検索前トランスフォーメーションが新しいエイリアスに再度適用されます。

既存のトランスフォーメーションと同じプライオリティの新しい検索前トランスフォーメーションを追加する場合、それよりも下位のプライオリティ（大きい数値を持つ）のすべてのトランスフォーメーションには1ずつ増えるプライオリティがあり、新しいトランスフォーメーションは指定したプライオリティで追加されます。または、すべての優先順位を下に移動する「スロット」が不十分な場合にエラーメッセージが表示されます。

検索前トランスフォーメーションの設定

「トランスフォーメーション（Transforms）」ページ（**[設定（Configuration）] > [ダイヤル プラン（Dial plan）] > [トランスフォーメーション（Transformation）]**）には Expressway に現在設定されているすべての検索前トランスフォーメーションについてのリストが表示されます。これは、トランスフォーメーションの作成、編集、削除、有効化および無効化に使用します。

エイリアスは、パターンの **[タイプ（Type）]**で指定した方法でエイリアスが **[パターン（Pattern）]** と一致する場合にトランスフォーメーションが検出されるまで、**[プライオリティ（Priority）]**の順序で各トランスフォーメーションと比較されます。次に、エイリアスは、検索が（ローカルに、または外部ゾーンに対して）実行される前に **[パターン動作（Pattern behavior）]** と **[置換文字列（Replace string）]** のルールに従って変換されます。

エイリアスは変換された後は変更された状態が維持され、それ以降のすべてのコール処理は新しいエイリアスに適用されます。

（注） 変換はすべてのモバイルおよびリモート アクセスの概要 メッセージにも適用されます。

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
優先度（Priority）	トランスフォーメーションのプライオリティ。プライオリティは 1 ～ 65534 の範囲であり、1 が最も高いプライオリティになります。トランスフォーメーションはプライオリティ順に適用されるため、プライオリティは各トランスフォーメーションに一意である必要があります。	

フィールド	説明	使用方法のヒント
Description	トランスフォーメーションの任意の自由形式の説明。	リストのトランスフォーメーション上にマウス ポインタを置くと、ツールチップとして説明が表示されます。
パターン タイプ（Pattern type）	適用するルールで、**パターン文字列**をどのようにエイリアスと照合するか。次のオプションがあります。 *[*完全一致（*Exact*）*]*：文字列全体がエイリアスと1 文字も違うことなく完全に一致する必要があります。 *[*プレフィックス（*Prefix*）*]*：文字列がエイリアスの先頭に表示される必要があります。 *Suffix*：文字列がエイリアスの末尾に表示される必要があります。 *[*正規表現（*Regex*）*]*：文字列を正規表現として処理します。	パターンが特定の名前に一致するかどうか、および予想どおりに変換されているかどうかは、パターンの効果の確認 ツール（**[メンテナンス（Maintenance）] > [ツール（Tools）] > [パターンの確認（Check pattern）]**）を使用してテストできます。
パターン文字列（Pattern string）	エイリアスを比較するパターンを指定します。	Expressway には、特定の設定要素との照合に使用できる、事前に設定された一連のパターン マッチングの変数が備わっています。
パターン動作（Pattern behavior）	エイリアスの一致部分の変更方法を指定します。オプションは次のとおりです。 *[*除去（*Strip*）*]*：一致するプレフィックスまたはサフィックスが削除されます。 *[*置換（*Replace*）*]*：エイリアスの一致部分が [置換文字列（Replace string）] のテキストで置き換えられます。 *[*プレフィックスの追加（*Add Prefix*）*]*：エイリアスの前に**[追加テキスト（Additional text）]** の値を追加します。 *[*サフィックスの追加（*Add Suffix*）*]*：エイリアスの後ろに**[追加テキスト（Additional text）]** を追加します。	

フィールド	説明	使用方法のヒント
文字列の置換（Replace string）	パターンに一致するエイリアスの部分を置き換える文字列	**[パターン動作（Pattern behavior）]** が *[置換（Replace）]* の場合にのみ適用されます。 正規表現を使用できます。
追加テキスト（Additional text）	プレフィックスまたはサフィクスとして追加する文字列。	**[パターン動作（Pattern behavior）]** が *[プレフィックスの追加（Add Prefix）]* または *[サフィックスの追加（Add Suffix）]* の場合にのみ適用されます。
状態（State）	トランスフォーメーションが有効になっているかどうかを示します。	この設定を使用して設定変更をテストしたり、特定のルールを一時的に無効にします。ルール リストには無効にしたルールが表示されますが、無視されます。

設定するトランスフォームをクリックします（または**[新規（New）]**をクリックして新しいトランスフォーメーションを作成するか、**[削除（Delete）]** をクリックしてトランスフォーメーションを削除します）。

検索とゾーン変換プロセス

検索とゾーン トランスフォーメーションのプロセスは、すべての検索前トランスフォーメーションについて、コール ポリシーについて、およびFindMe についてが適用された後に適用されます。

そのプロセスは次のとおりです。

1. Expressway はプライオリティの順序で適用され（プライオリティ 1 のすべてのルールが最初に処理されてから、プライオリティ 2 以降のルールが処理されます）、指定したエイリアスがクエリの **[ソース（Source）]** ルールの **[モード（Mode）]** に基づいてルールの条件に一致しているかどうかを確認します。
2. 照合が成功すると、関連付けられたゾーン トランスフォーメーションがエイリアスに適用されます（**[モード（Mode）]** が *[エイリアス パターン マッチ（Alias pattern match）]* で、**[パターン動作（Pattern behavior）]** が *[置換（Replace）]* または *[除去（Strip）]* の場合）。
3. 検索ルールの**ターゲット**のゾーンまたはポリシー サービスは、着信コール要求と同じプロトコル（SIP または H.323）を使用して（ゾーン トランスフォーメーションが適用されている場合は変更されたエイリアスを使用して）照会されます。

（注） 同じプライオリティ レベルの複数のルールで多くの照合に成功した場合、該当するすべての**ターゲット**が照会されます。

- エイリアスが検出された場合、コールはそのゾーンに転送されます。エイリアスが複数のゾーンで検出された場合、最初に応答したゾーンにコールが転送されます。
- ネイティブのプロトコルを使用してエイリアスが検出されない場合は、[インターワーキング モード（interworking mode）]SIP および H.323 のインターワーキングの設定（224 ページ） に応じてインターワーキングしているプロトコルを使用してクエリが繰り返されます。
- 検索で新しいURIまたはエイリアスが返された場合（ENUMルックアップやポリシーサービスの応答などによる）、コール ルーティング プロセスが再度開始されます。

4. エイリアスが検出されなかった場合、プライオリティが次に高い検索ルールが次のことが発生するまで、適用されます（ステップ 1 に戻ります）。
   - エイリアスが検出されるか、または
   - 特定の条件を満たす検索ルールに関連付けられたすべてのターゲットゾーンまたはポリシーサービスが照会された、あるいは
   - 正常な一致がある検索ルールの **[正常に一致する場合（On successful match）]** が *[検索の停止（Stop searching）]* に設定されている

（注） 正常な一致（エイリアスが検索ルール条件に一致する場合）と検出するエイリアス（ターゲットゾーンに送信されたクエリに成功した場合）との違い。*[検索の停止（Stop searching）]* オプションは、ネットワークのシグナリングインフラストラクチャの制御を向上させます。たとえば、特定のドメインの検索を常に特定のゾーンにルーティングしなければならない場合、このオプションを使用すると、検索プロセスの効率が向上し、Expressway がほかのゾーンを不必要に検索しなくなります。

検索ルールの設定

「検索ルール（Search rules）」ページ（**[設定（Configuration）] > [ダイヤルプラン（Dial plan）] > [検索ルール（Search rules）]**）を使用して、Expressway による適切なターゲットゾーン（ローカルゾーンを含む）またはポリシーサービスへの着信検索要求のルーティング方法を設定します。

このページには、現在設定されているすべての検索ルールが表示されるため、ルールの作成、編集、削除、および有効化と無効化が行えます。列の見出しをクリックすると、**ターゲット**別または**プライオリティ**別にリストを並べ替えることができます。検索ルール上にマウスポインタを置くと、ルールの説明（定義されている場合）がツールチップとして表示されます。

また、既存の検索ルールは、**[アクション（Actions）]** 列の **[クローン（Clone）]** をクリックすると、コピーしてから編集することもできます。

最大 2000 の検索ルールを設定できます。プライオリティ 1 の検索ルールが最初に適用され、次にプライオリティ 2 のすべての検索ルールが適用されます。

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
ルール名	検索ルールの記述名。	
Description	検索ルールの任意の自由形式の説明。	リストのルールの上にマウス ポインタを置いた場合に説明がツールチップとして表示されます。
優先度（Priority）	他の検索ルールのプライオリティと比較したときに、このルールを適用する検索プロセスの順序。プライオリティ 1 のすべてのルールが最初に適用され、次にプライオリティ 2 のすべてのルールが適用されます。複数のルールに同じプライオリティを割り当てることができます。この場合、照合するターゲット ゾーンは同時に照会されます。デフォルトは 100 です。	デフォルト設定では、すべてのエイリアスについてローカル ゾーンが最初に検索されます。ローカルでエイリアスが検出されなかった場合、すべてのネイバー、トラバーサル クライアントおよびトラバーサル サーバが検索されます。エイリアスが検出されなかった場合は、DNS ゾーンと ENUM ゾーンに要求が送信されます。
[Protocol]	ルールを適用するソース プロトコル。オプションは *[いずれか（Any）]*、*[H.323]* または *[SIP]* です。	

フィールド	説明	使用方法のヒント
トラフィック タイプ（Traffic type）	このルールを適用するソース トラフィック タイプ。オプションは次のとおりです。 *[いずれか（Any）]*：ルールではトラフィック タイプを検査しません。 *[標準（Standard）]*：ルールはトラフィックが標準ベースの SIP の場合に適用されます。 *[いずれかの Microsoft（Any Microsoft）]*：ルールはトラフィックが Microsoft SIP または Microsoft SIP-SIMPLE の場合に適用されます。 *[Microsoft SIP]*：ルールはトラフィックが Microsoft SIP の場合に適用されます。 *[Microsoft IM および Presence（Microsoft IM and Presence）]*：ルールはトラフィックが Microsoft SIP-SIMPLE の場合に適用されます。	このオプションにより、異なるタイプのコールをその処理に最適なインフラストラクチャにルーティングできます。 たとえば、2 つの検索ルールを使用して、標準の SIP を Unified CM のネイバー ゾーンへルーティングし、任意の Microsoft SIP を Cisco Meeting Server のネイバー ゾーンへルーティングできます。
ソース（Source）	このルールを適用する要求のソース。 *[いずれか（Any）]*：ローカル登録されたデバイス、ネイバーまたはトラバーサル ゾーン、および登録されていないデバイス。 *[All Zones]*：ローカルに登録されたデバイスとネイバーまたはトラバーサル ゾーン。 *[ローカル ゾーン（Local Zone）]*：ローカル登録されたデバイスのみ。 *[指定（Named）]*：ルールを適用する特定のソース ゾーンまたはサブゾーン。	指定ソースは、特定のサブゾーンとゾーンのダイヤル プラン ポリシーとして適用する検索ルールの機能を作成します。
ソース名（Source name）	ルールを適用する特定のソース ゾーンまたはサブゾーン。デフォルト ゾーン、デフォルト サブゾーン、あるいはその他の設定済みのゾーンまたはサブゾーンを選択します。	**[ソース（Source）]** が *[指定（Named）]* に設定されている場合にのみ適用されます。

フィールド	説明	使用方法のヒント
要求に認証が必要（Request must be authenticated）	検索ルールを認証された検索要求にのみ適用するかどうかを指定します。	これを Expressway の認証ポリシー（Authentication policy）と併用して、認証されていないデバイスが使用可能な一連のサービスを制限できます。
モード（Mode）	エイリアスを検索ルールに適用するかどうかをテストするための方法。 *[エイリアスパターンマッチ（Alias pattern match）]*：エイリアスは、指定された **[パターンタイプ（Pattern type）]** と **[パターン文字列（Pattern string）]** に一致する必要があります。 *[任意のエイリアス（Any alias）]*：（IP アドレスでない限り）どのエイリアスでもかまいません。 *[任意の IP アドレス（Any IP Address）]*：エイリアスは IP アドレスである必要があります。	
パターン タイプ（Pattern type）	適用するルールで、**パターン文字列**をどのようにエイリアスと照合するか。次のオプションがあります。 *[完全一致（Exact）]*：文字列全体がエイリアスと1文字も違うことなく完全に一致する必要があります。 *[プレフィックス（Prefix）]*：文字列がエイリアスの先頭に表示される必要があります。 *Suffix*：文字列がエイリアスの末尾に表示される必要があります。 *[正規表現（Regex）]*：文字列を正規表現として処理します。	**[モード（Mode）]** が *[エイリアス パターン マッチ（Alias Pattern Match）]* である場合にのみ適用されます。 パターンが特定の名前に一致するかどうか、および予想どおりに変換されているかどうかは、パターンの効果の確認 ツール（**[メンテナンス（Maintenance）]** > **[ツール（Tools）]** > **[パターンの確認（Check pattern）]**）を使用してテストできます。

フィールド	説明	使用方法のヒント
パターン文字列（Pattern string）	エイリアスと比較するパターン。	**[モード（Mode）]** が *[エイリアス パターン マッチ（Alias Pattern Match）]* である場合にのみ適用されます。 Expressway には、特定の設定要素との照合に使用できる、事前に設定された一連のパターン マッチングの変数が備わっています。
パターン動作（Pattern behavior）	ターゲット ゾーンまたはポリシー サービスに送信する前に、エイリアスの一致した部分を変更するかどうかを決定します。 *[変更しない（Leave）]*：エイリアスは変更されません。 *[除去（Strip）]*：一致するプレフィックスまたはサフィックスをエイリアスから削除します。 *[置換（Replace）]*：エイリアスの一致部分が **[置換文字列（Replace string）]** のテキストで置き換えられます。	**[モード（Mode）]** が *[エイリアス パターン マッチ（Alias Pattern Match）]* である場合にのみ適用されます。 検索ルールの適用前にエイリアスを変換する場合は、検索前トランスフォーメーションについてを使用します。
文字列の置換（Replace string）	パターンに一致するエイリアスの部分を置き換える文字列	**[パターン動作（Pattern behavior）]** が *[置換（Replace）]* の場合にのみ適用されます。 正規表現を使用できます。
正常に一致する場合（On successful match）	エイリアスが検索ルールに一致する場合の進行中の検索動作を制御します。 *[続行（Continue）]*：エイリアスが特定したエンドポイントが検出されるまで、残りの検索ルールを（プライオリティ順に）適用します。 *[停止（Stop）]*：エイリアスで特定されたエンドポイントがターゲットゾーンで検出されない場合でも、これ以上は検索ルールを適用しません。	*[停止（Stop）]* を選択した場合、このルールと同じプライオリティのルールは適用されます。

フィールド	説明	使用方法のヒント
Target	エイリアスが検索ルールと一致するかどうかを照会するゾーンまたはポリシー サービス。	検索ルールのターゲットとして使用するように外部外部サービスを使用するための検索ルールの設定を設定できます。たとえば、外部サービスや TelePresence Conductor などのアプリケーションをコールアウトするために使用できます。サービスは、検索プロセスをもう一度開始する新しい宛先エイリアスを指定するなど、一部の CPL を返します。
状態（State）	検索ルールが有効になっているかどうかを示します。	この設定を使用して設定変更をテストしたり、特定のルールを一時的に無効にします。ルール リストには無効にしたルールが表示されますが、無視されます。

設定するルールをクリックします（または**[新規（New）]**をクリックして新しいルールを作成するか、**[削除（Delete）]** をクリックしてルールを削除します）。

検索ルールの設定を支援する便利なツール

- エンドポイントに実際に発信せずに、指定したエイリアスにより特定したエンドポイントを Expressway が検出できるかどうかは、エイリアスの検出 ツール（**[メンテナンス（Maintenance）] > [ツール（Tools）] > [検索（Locate）]**）でテストできます。
- パターンが特定の名前に一致するかどうか、および予想どおりに変換されているかどうかは、パターンの効果の確認 ツール（**[メンテナンス（Maintenance）]>[ツール（Tools）]> [パターンの確認（Check pattern）]**）を使用してテストできます。

検索とトランスフォーメーションの例

検索前のトランスフォーメーションと検索ルールは別々にも一緒にも使用できます。また、**[任意のエイリアス（Any alias）]** モードと **[エイリアスパターンマッチ（Alias pattern match）]** モードの組み合わせを使用する複数の検索ルールを定義することも、各ルールに同じプライオリティや別のプライオリティを適用することもできます。これによって、ターゲットゾーンをいつどのような場合に照会するか、およびトランスフォーメーションを適用するかどうかを決定する際に柔軟に対応できるようになります。

ここでは、導入環境における特定の使用例を解決するために検索前トランスフォーメーションや検索ルールをどのように使用できるかについて次の例を示します。

ゾーンへのクエリの変換なしのフィルタリング

特定の条件に一致するエイリアスのみを照会するように、ゾーンに送信する検索要求をフィルタリングできます。たとえば、地域の営業オフィスのすべてのエンドポイントがサフィックスの **@sales.example.com** を使用してローカルの Cisco VCS に登録されているとします。この場合は、本社の Expressway にはサフィックスの **@sales.example.com** を持つエイリアスに対する検索要求を受信したときにのみ、営業オフィスの VCS を照会することが適切です。別の検索要求をこの特定の VCS に送信するとリソースを不必要に消費することになります。また、このパターンに一致するエイリアスに対する検索要求を別のゾーンに送信してもリソースが無駄になります（これらのエイリアスに適用される、プライオリティの低い検索ルールも定義されている場合があります）。その場合、**[正常に一致する場合（On successful match）]** を *[*停止（*Stop*）*]* に設定すると、Expressway はそれ以上の（プライオリティの低い）検索ルールを適用しません。

上記の例を実現するには、本社の Expressway で営業オフィスの VCS を表すゾーンを作成し、**「検索ルールの作成（Create search rule）」**ページ（**[設定（Configuration）]** > **[ダイヤル プラン（Dial plan）]** > **[検索ルール（Search rules）]** > **[新規（New）]**）から関連する検索ルールを次のようにセットアップします。

フィールド	値
ルール名	地域営業オフィス（Regional sales office）
Description	サフィックスが @sales.example.com のエイリアスをコールする（Calls to aliases with a suffix of @sales.example.com）
優先度（**Priority**）	100
ソース（**Source**）	任意（Any）
要求に認証が必要（**Request must be authenticated**）	いいえ（No）
モード（**Mode**）	エイリアスのパターン マッチ（Alias pattern match）
パターン タイプ（**Pattern type**）	サフィックス（Suffix）
パターン文字列（**Pattern string**）	@sales.example.com
パターン動作（**Pattern behavior**）	変更なし（Leave）
正常に一致する場合（**On successful match**）	停止（Stop）
Target	営業オフィス（Sales office）
状態（**State**）	有効（Enabled）

常に元のエイリアス（変換なし）でゾーンを照会する

元のエイリアスを使用して検索要求が送信されるようにゾーンを設定するには、**「検索ルールの作成（Create search rule）」**ページ（**[設定（Configuration）] > [ダイヤル プラン（Dial plan）] > [検索ルール（Search rules）] > [新規（New）]**に*[*任意のエイリアス（*Any alias*）*]*の**モード**を使用してそのゾーンに検索ルールをセットアップします。

フィールド	値
ルール名	常に元のエイリアスを使用して照会する（Always query with original alias）
Description	元のエイリアスを使用して検索要求を送信する（Send search requests using the original alias）
優先度（**Priority**）	100
ソース（**Source**）	任意（Any）
要求に認証が必要（**Request must be authenticated**）	いいえ（No）
モード（**Mode**）	任意のエイリアス（Any alias）
正常に一致する場合（**On successful match**）	続行（Continue）
Target	本社（Head office）
状態（**State**）	有効（Enabled）

変換されたエイリアスに関するゾーンの照会

（注） エイリアスモードではエイリアス変換がサポートされません。受信した異なるエイリアスを使用してゾーンを常に照会する場合は、モードを *[*エイリアスのパターン マッチ（*Alias pattern match*）*]* にして正規表現と組み合わせて使用する必要があります。

ユーザが **name@example.com** の形式のエイリアスをダイヤルしたときに、Expressway が代わりに **name@example.co.uk** についてゾーンを照会するようにダイヤルプランを設定できます。

これを行うには、**[検索ルールの作成（Create search rule）]** ページ（**[設定（Configuration）] > [ダイヤル プラン（Dial plan）] > [検索ルール（Search rules）] > [新規（New）]**）から検索ルールを次のようにセットアップします。

フィールド	値
ルール名	example.co.uk へ変換（Transform to example.co.uk）
Description	example.com から example.co.uk へ変換（Transform example.com to example.co.uk）
優先度（**Priority**）	100
ソース（**Source**）	任意（Any）
要求に認証が必要（**Request must be authenticated**）	いいえ（No）
モード（**Mode**）	エイリアスのパターン マッチ（Alias pattern match）
パターン タイプ（**Pattern type**）	サフィックス（Suffix）
パターン文字列（**Pattern string**）	example.com
パターン動作（**Pattern behavior**）	置換（Replace）
文字列の置換（**Replace string**）	example.co.uk
正常に一致する場合（**On successful match**）	続行（Continue）
転送先ゾーン（**Target zone**）	本社（Head office）
状態（**State**）	有効（Enabled）

元のエイリアスと変換後のエイリアスに関するゾーンの照会

変換後のエイリアスをゾーンに照会すると同時に元のエイリアスをゾーンに照会できます。これを行うには、適用するトランスフォーメーションの詳細とともに、**[モード（Mode）]** を *[任意のエイリアス（Any alias）]* に設定した検索ルールを 1 つと、**[モード（Mode）]** を *[エイリアスのパターン マッチ（Alias pattern match）]* に設定した検索ルールをもう 1 つ作成します。両方の検索に同じ**プライオリティ** レベルを指定する必要があります。

たとえば、完全な URI と名前のみ（ドメインを除いた URI）の両方をネイバー ゾーンに照会することができます。これを行うには、ローカル Expressway で**「検索ルールの作成（Create**

search rule）」ページ（**[設定（Configuration）]** > **[ダイヤル プラン（Dial plan）]** > **[検索ルール（Search rules）]** > **[新規（New）]**）から 2 つの検索ルールを次のようにセットアップします。

ルール #1

フィールド	値
ルール名	海外オフィス - 元のエイリアス（Overseas office - original alias）
Description	元のエイリアスを持つ海外オフィスの照会（Query overseas office with the original alias）
優先度（**Priority**）	100
ソース（**Source**）	任意（Any）
要求に認証が必要（**Request must be authenticated**）	いいえ（No）
モード（**Mode**）	任意のエイリアス（Any alias）
正常に一致する場合（**On successful match**）	続行（Continue）
転送先ゾーン（**Target zone**）	海外オフィス（Overseas office）
状態（**State**）	有効（Enabled）

ルール #2

フィールド	値
ルール名	海外オフィス - ドメインの除去（Overseas office - strip domain）
Description	ドメインを除去した海外オフィスの照会（Query overseas office）
優先度（**Priority**）	100
ソース（**Source**）	任意（Any）
要求に認証が必要（**Request must be authenticated**）	いいえ（No）
モード（**Mode**）	エイリアスのパターン マッチ（Alias pattern match）

フィールド	値
パターン タイプ（**Pattern type**）	サフィックス（Suffix）
パターン文字列（**Pattern string**）	@example.com
パターン動作（**Pattern behavior**）	除去（Strip）
正常に一致する場合（**On successful match**）	続行（Continue）
転送先ゾーン（**Target zone**）	海外オフィス（Overseas office）
状態（**State**）	有効（Enabled）

複数の変換後のエイリアスに関するゾーンの照会

ゾーンに対して設定された検索ルールのプライオリティ順にゾーンが照会されます。

同じゾーンに複数の検索ルールを設定できます。たとえば、照合する**プライオリティ**と**パターン文字列**は同じにし、置換文字列は異なるものをそれぞれに設定できます。この場合、Expressway は新しいエイリアスのそれぞれについて、そのゾーンを同時に照会します（トランスフォーメーションによって重複するエイリアスが作成された場合は、検索要求が送信される前にそれらは削除されます）。新しいエイリアスのいずれかがそのゾーンで検出されると、コールはそのゾーンに転送されます。コールが転送されるエイリアスは、制御システムによって決定されます。

たとえば、ユーザが **name@example.com** 形式のエイリアスをダイヤルしたときに Expressway が **name@example.co.uk** と **name@example.net** の両方について同時にゾーンに照会するようにダイヤル プランを設定できます。

これを行うには、**「検索ルールの作成（Create search rule）」**ページ（**[設定（Configuration）]** > **[ダイヤル プラン（Dial plan）]** > **[検索ルール（Search rules）]** > **[新規（New）]**）から 2 つの検索ルールを次のようにセットアップします。

ルール #1

フィールド	値
ルール名	example.co.uk へ変換（Transform to example.co.uk）
Description	example.com から example.co.uk へ変換（Transform example.com to example.co.uk）

フィールド	値
優先度（**Priority**）	100
ソース（**Source**）	任意（Any）
要求に認証が必要（**Request must be authenticated**）	いいえ（No）
モード（**Mode**）	エイリアスのパターン マッチ（Alias pattern match）
パターン タイプ（**Pattern type**）	サフィックス（Suffix）
パターン文字列（**Pattern string**）	example.com
パターン動作（**Pattern behavior**）	置換（Replace）
文字列の置換（**Replace string**）	example.co.uk
正常に一致する場合（**On successful match**）	続行（Continue）
転送先ゾーン（**Target zone**）	本社（Head office）
状態（**State**）	有効（Enabled）

ルール #2

フィールド	値
ルール名	example.net へ変換（Transform to example.net）
Description	example.net example.com へ変換
優先度（**Priority**）	100
ソース（**Source**）	任意（Any）
要求に認証が必要（**Request must be authenticated**）	いいえ（No）
モード（**Mode**）	エイリアスのパターン マッチ（Alias pattern match）

フィールド	値
パターン タイプ（**Pattern type**）	サフィックス（Suffix）
パターン文字列（**Pattern string**）	example.com
パターン動作（**Pattern behavior**）	置換（Replace）
文字列の置換（**Replace string**）	example.net
正常に一致する場合（**On successful match**）	続行（Continue）
転送先ゾーン（**Target zone**）	本社（Head office）
状態（**State**）	有効（Enabled）

H.323 番号へのダイヤリングでの @domain の除去

SIP エンドポイントは URI の形式（たとえば **name@domain**）でのみコールを作成できます。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。

1 つの番号を使用して登録した SIP エンドポイントと H.323 エンドポイントの両方が含まれている導入環境の場合、次の検索前トランスフォーメーションとローカルゾーンの検索ルールをセットアップする必要があります。これらの両方によって、ユーザは SIP エンドポイントと H.323 エンドポイントの両方から、H.323 E.164 番号のみを使用して登録した H.323 エンドポイントにコールできます。

検索前トランスフォーメーション

「トランスフォーメーションの作成（**Create transforms**）」ページ（**[設定（Configuration）]**>**[ダイヤルプラン（Dial plan）]**>**[トランスフォーメーション（Transforms）]**>**[新規（New）]**）で、次のようにセットアップします。

フィールド	値
優先度（**Priority**）	1

フィールド	値
Description	数字のみのダイヤル文字列を使用し @domain を追加（Take any number-only dial string and append @domain）
パターン タイプ（**Pattern type**）	正規表現（Regex）
パターン文字列（**Pattern string**）	(\d+)
パターン動作（**Pattern behavior**）	置換（Replace）
文字列の置換（**Replace string**）	\1@domain
状態（**State**）	有効（Enabled）

この検索前トランスフォーメーションでは、数字のみのダイヤル文字列（**123** など）を使用して、導入環境内のエンドポイントの AOR と URI に使用したドメインを追加します。これによって、SIP エンドポイントと H.323 エンドポイントが発信したコールが同じ URI になるようにします。

ローカル ゾーンの検索ルール

「検索ルールの作成（Create search rule）」ページ（**[設定（Configuration）] > [ダイヤルプラン（Dial plan）] > [検索ルール（Search rules）] > [新規（New）]**）で 2 つの新しい検索ルールを次のように作成します。

ルール #1

フィールド	値
ルール名	H.323 番号をダイヤル（Dialing H.323 numbers）
Description	number@domain 形式のエイリアスを番号に変換（Transform aliases in format number@domain to number）
優先度（**Priority**）	50
ソース（**Source**）	任意（Any）
要求に認証が必要（**Request must be authenticated**）	いいえ（No）
モード（**Mode**）	エイリアスのパターン マッチ（Alias pattern match）

フィールド	値
パターン タイプ（**Pattern type**）	正規表現（Regex）
パターン文字列（**Pattern string**）	(\d+)@domain
パターン動作（**Pattern behavior**）	置換（Replace）
文字列の置換（**Replace string**）	\1
正常に一致する場合（**On successful match**）	続行（Continue）
転送先ゾーン（**Target zone**）	ローカル ゾーン（Local Zone）
状態（**State**）	有効（Enabled）

ルール #2

フィールド	値
ルール名	H.323 番号をダイヤル（Dialing H.323 numbers）
Description	エイリアスを変換せずに number@domain をコール（Place calls to number@domain with no alias transform）
優先度（**Priority**）	60
ソース（**Source**）	任意（Any）
要求に認証が必要（**Request must be authenticated**）	いいえ（No）
モード（**Mode**）	エイリアスのパターン マッチ（Alias pattern match）
パターン タイプ（**Pattern type**）	正規表現（Regex）
パターン文字列（**Pattern string**）	(\d+)@domain

フィールド	値
パターン動作（**Pattern behavior**）	変更なし（Leave）
正常に一致する場合（**On successful match**）	続行（Continue）
転送先ゾーン（**Target zone**）	ローカル ゾーン（Local Zone）
状態（**State**）	有効（Enabled）

これらの検索ルールによって、E.164 番号と完全な URI の両方が確実に検索されるため、エンドポイントが H.323 番号（**123**）で登録されているか、完全な URI（**123@domain**）で登録されているかに関係なくエンドポイントに到達できます。

- 最初の検索ルールの形式は **number@domain** で、これらが **number** の形式に変換されます。
- エイリアスを実際に **number@domain** の形式で登録したエンドポイントにも確実に到達させるには、プライオリティが低い 2 番目の検索ルールでエイリアスを変換せずに **number@domain** をコールします。

英数字の H.323 ID のダイヤル文字列の変換

次に、H.323 番号へのダイヤリングでの @domain の除去に基づく例を示します。この例は数字のみのダイヤル文字列を考慮したものですが、H.323 ID は完全に数字のみである必要はありません。これらの ID には英数字（英字と数字）を含めることができます。

この例は、上記の例と同じモデルに従っています。つまり、検索前トランスフォーメーションとローカル ゾーンの検索ルールを使用して、エンドポイントが H.323 ID で登録されているか、完全な URI で登録されているかにかかわらず到達できるようにしています。ただし、英数字をサポートする別の正規表現を使用しています。

検索前トランスフォーメーション

「トランスフォーメーションの作成（Create transforms）」ページ（**[設定（Configuration）]**>**[ダイヤルプラン（Dial plan）]**>**[トランスフォーメーション（Transforms）]**>**[新規（New）]**）で、次のようにセットアップします。

フィールド	値
優先度（**Priority**）	1
Description	英数字のダイヤル文字列に @domain を追加（Append @domain to any alphanumeric dial string）

フィールド	値
パターン タイプ（**Pattern type**）	正規表現（Regex）
パターン文字列（**Pattern string**）	([^@]*)
パターン動作（**Pattern behavior**）	置換（Replace）
文字列の置換（**Replace string**）	\1@domain
状態（**State**）	有効（Enabled）

この検索前の変換は英数字のダイヤル文字列（**123abc**）を使用し、導入環境に使用されているドメインを追加することで、SIP のエンドポイントと H.323 のエンドポイントによって行われたコールが同じ URI になることを保証します。

ローカル ゾーンの検索ルール

「検索ルールの作成（Create search rule）」ページ（**[設定（Configuration）] > [ダイヤル プラン（Dial plan）] > [検索ルール（Search rules）] > [新規（New）]**）で 2 つの新しい検索ルールを次のように作成します。

ルール #1

フィールド	値
ルール名	H.323 文字列をダイヤル（Dialing H.323 strings）
Description	string@domain 形式のエイリアスを文字列に変換（Transform aliases in format string@domain to string）
優先度（**Priority**）	40
ソース（**Source**）	任意（Any）
要求に認証が必要（**Request must be authenticated**）	いいえ（No）
モード（**Mode**）	エイリアスのパターン マッチ（Alias pattern match）
パターン タイプ（**Pattern type**）	正規表現（Regex）

フィールド	値
パターン文字列（**Pattern string**）	(.+)@domain
パターン動作（**Pattern behavior**）	置換（Replace）
文字列の置換（**Replace string**）	\1
正常に一致する場合（**On successful match**）	続行（Continue）
転送先ゾーン（**Target zone**）	ローカル ゾーン（Local Zone）
状態（**State**）	有効（Enabled）

ルール #2

フィールド	値
ルール名	ドメインを使用した H.323 文字列をダイヤル（Dialing H.323 strings with domain）
Description	エイリアスを変換せずに string@domain をコール（Place calls to string@domain with no alias transform）
優先度（**Priority**）	50
ソース（**Source**）	任意（Any）
要求に認証が必要（**Request must be authenticated**）	いいえ（No）
モード（**Mode**）	エイリアスのパターン マッチ（Alias pattern match）
パターン タイプ（**Pattern type**）	正規表現（Regex）
パターン文字列（**Pattern string**）	(.+)@domain
パターン動作（**Pattern behavior**）	変更なし（Leave）

フィールド	値
正常に一致する場合（**On successful match**）	続行（Continue）
転送先ゾーン（**Target zone**）	ローカル ゾーン（Local Zone）
状態（**State**）	有効（Enabled）

これらの検索ルールによって、E.164 番号と完全な URI の両方が確実に検索されるため、エンドポイントが H.323 ID（**123abc**）で登録されているか、完全な URI（**123abc@domain**）で登録されているかに関係なくエンドポイントに到達できます。

- 最初の検索ルールでは **string@domain** 形式のエイリアスをとり、それらを **string** の形式に変換します。
- エイリアスを実際に **string@domain** の形式で登録したエンドポイントにも確実に到達させるには、プライオリティが低い 2 番目の検索ルールでエイリアスを変換せずに **string@domain** をコールします。

既知のゾーンから着信した場合にのみ IP アドレスへのコールを許可

エイリアスへのコールの他に、指定した IP アドレスにコールを発信することができます。このようなコールを適切なターゲット ゾーンまで通過させるには、**[モード（Mode）]** を *[任意の IP アドレス（Any IP address）]* に設定した検索ルールをセットアップする必要があります。セキュリティを強化するには、ルールの **[ソース（Source）]** オプションを *[すべてのゾーン（All zones）]* に設定する必要があります。これにより、設定済みのゾーンまたはローカル ゾーンのいずれかからクエリが発信されている場合、そのクエリはターゲット ゾーンにのみ送信されます。

上記に示した例を実現するには、**「検索ルールの作成（Create search rule）」** ページ（**[設定（Configuration）] > [ダイヤル プラン（Dial plan）] > [検索ルール（Search rules）] > [新規（New）]**）から検索ルールを次のようにセットアップします。

フィールド	値
ルール名	既知のゾーンからの IP アドレス（IP addresses from known zones）
Description	既知のゾーンからの IP アドレスへのコールのみを許可（Allow calls to IP addresses only from a known zone）
優先度（**Priority**）	100
ソース（**Source**）	全ゾーン（All zones）

フィールド	値
要求に認証が必要（**Request must be authenticated**）	いいえ（No）
モード（**Mode**）	任意の IP アドレス
正常に一致する場合（**On successful match**）	続行（Continue）
転送先ゾーン（**Target zone**）	海外オフィス（Overseas office）
状態（**State**）	有効（Enabled）

Microsoft SIP コールを Cisco Meeting Server へ転送する

Cisco Meeting Server を使用して Microsoft ユーザがスペース内で会議できるようにする場合、次のような検索ルールを使用して、このタイプの着信コールをミーティングサーバのネイバーゾーンへ転送します。

フィールド	値
ルール名	すべて Meeting Server にルーティング（Route all to Meeting Server）
Description	すべてのインバウンドMS トラフィックを Meeting Server に送信（Send all inbound MS traffic to Meeting Server）
優先度（**Priority**）	100
[Protocol]	SIP
トラフィックのタイプ	いずれかの Microsoft（Any Microsoft）
ソース（**Source**）	任意（Any）
要求に認証が必要（**Request must be authenticated**）	いいえ（No）
モード（**Mode**）	任意のエイリアス（Any alias）
正常に一致する場合（**On successful match**）	停止（Stop）
Target	Cisco Meeting Server

フィールド	値
状態（State）	有効（Enabled）

Kari の法律の 911 コール（Expressway をコール制御および PSTN ゲートウェイとして使用）

このセクションでは、Cisco Expressway 経由で直接 911 緊急コールをサポートするダイヤルプランを設定するための推奨事項を提供します。Federal Communications Commission によって義務付けされた「Kari の法律」は、米国内の**直通** 911 コールをサポートするため、複数回線電話システム（MLTS）を必要とします。つまり、緊急電話をかける人は、プレフィックスやその他の追加の数字をダイヤルする必要もありません。

Kari の法律が Expressway に適用される時期

Kari の法律は、音声を扱います。この法律は、次のすべての条件が適用される場合に、**米国の** Expressway 導入に適用されます。

- Expressway は、呼制御を管理し、緊急コールを Expressway-C に直接登録するエンドポイントを管理しています。
- ゲートウェイは、PSTN コールを有効にする Expressway で設定されます。
- 展開用の PSTN 通話機能には、911 の緊急コールが含まれます。
- 関係するエンドポイントは、PSTN 番号をダイヤルして基本的な音声通話を発信できます。

はじめる前に

- Cisco Expressway バージョン X12.5.7 以降が必要です。
- 北米番号計画（INGP）に関する情報を保持している必要があります。
- X12.5.7 から、コールを開始する前に少なくとも 1 つの RMS ライセンスをインストールする通常の要件は、直接 911 コールには適用されません。
- 料金の不正なリスクを最小限に抑えるために、送信元設定には「任意の」ワイルドカードを使用しないようにしてください。
- また、プレフィックスなしで 911 コールをルーティングするように PSTN ゲートウェイを設定する必要があります。
- エンドポイントとは異なる場所にゲートウェイが地理的に広がる導入の場合は、911 コールの実際のルーティング要件と、発信者が自分の場所とは異なる場所の緊急エージェントに接続している可能性があります。

検索ルールの設定

[検索ルール の作成（Create search rule）] ページ (**[設定（Configuration）]** > **[ダイヤルプラン（Dial plan）]** > **[検索ルール（Search rules）]** > **[新規（New）]** で、必要な検索ルールを作成します。このセクションでは、次の導入タイプの例を示します。

1. スタンドアロン PSTN ゲートウェイ（冗長性なし）
2. 複数の PSTN ゲートウェイ。

例 1：スタンドアロンゲートウェイの検索ルール

これらのルール例は、次のことを前提にしています。

- PSTN コール用の ISDN ゲートウェイは、Expressway 上でネイバーゾーン（「PSTNGateway」という名前）として設定されます。
- 911 の緊急コールは、Expressway-C にローカルに登録されている SIP ユーザエージェントまたは H.323 エンドポイントからのみ許可されます。

例 1：ルール #1

フィールド	値
ルール名	緊急コール - 911
Description	PSTNGateway 経由で 911 緊急コールのルーティング
優先度（**Priority**）	1
[Protocol]	任意（Any）
ソース（**Source**）	ローカル ゾーン（Local Zone）
要求に認証が必要（**Request must be authenticated**）	いいえ（No）
モード（**Mode**）	エイリアスのパターン マッチ（Alias pattern match）
パターン タイプ（**Pattern type**）	正規表現（Regex）

フィールド	値
パターン文字列（**Pattern string**）	911|(911@%localdomains%)
パターン動作（**Pattern behavior**）	変更なし（Leave）
正常に一致する場合（**On successful match**）	停止（Stop）
転送先ゾーン（**Target zone**）	PSTNGateway
状態（**State**）	有効

例 1：ルール #2

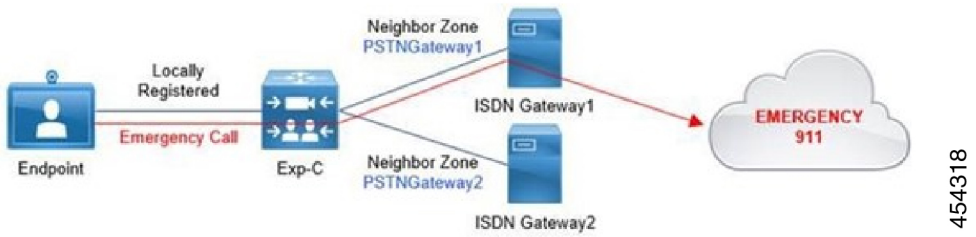
フィールド	値
ルール名	緊急コール - プレフィックス 00 と 911
Description	PSTNGateway 経由で 911 緊急コールのルーティング
優先度（**Priority**）	2
[Protocol]	任意（Any）
ソース（**Source**）	ローカル ゾーン（Local Zone）
要求に認証が必要（**Request must be authenticated**）	いいえ（No）
モード（**Mode**）	エイリアスのパターン マッチ（Alias pattern match）
パターン タイプ（**Pattern type**）	正規表現（Regex）
パターン文字列（**Pattern string**）	00(911|911@%localdomains%)
パターン動作（**Pattern behavior**）	置換（Replace）
文字列の置換（**Replace string**）	\1

フィールド	値
正常に一致する場合（**On successful match**）	停止（Stop）
転送先ゾーン（**Target zone**）	PSTNGateway
状態（**State**）	有効

例 2：複数のゲートウェイの検索ルール

これらのルール例は、次のことを前提にしています。

- PSTN コール用の 2 つの ISDN ゲートウェイを、冗長性を確保するためにライブネットワークで使用できます。
- 各ゲートウェイは、ネイバーゾーン（「PSTNGateway1」 と 「PSTNGateway2」 という名前）として Expressway 上で設定されます。
- 911 の緊急コールは、Expressway-C にローカルに登録されている SIP ユーザエージェントまたは H.323 エンドポイントからのみ許可されます。



ここで、ルールは、プライマリゲートウェイに対して一致に成功した場合＝「続行」、.backup one に対して*On successful match* ＝ 「停止」を指定します。

例 2：ルール #1

フィールド	値
ルール名	緊急コール - PSTNGateway1 経由の 911
Description	PSTNGateway 経由で 911 緊急コールのルーティング
優先度（**Priority**）	1
[Protocol]	任意（Any）

フィールド	値
ソース（**Source**）	ローカル ゾーン（Local Zone）
要求に認証が必要（**Request must be authenticated**）	いいえ（No）
モード（**Mode**）	エイリアスのパターン マッチ（Alias pattern match）
パターン タイプ（**Pattern type**）	正規表現（Regex）
パターン文字列（**Pattern string**）	911|(911@%localdomains%)
パターン動作（**Pattern behavior**）	変更なし（Leave）
正常に一致する場合（**On successful match**）	続行（Continue）
転送先ゾーン（**Target zone**）	PSTNGateway1
状態（**State**）	有効

例 2：ルール **#2**

フィールド	値
ルール名	緊急コール - PSTNGateway2 経由の 911
Description	PSTNGateway 経由で 911 緊急コールのルーティング
優先度（**Priority**）	2
[Protocol]	任意（Any）
ソース（**Source**）	ローカル ゾーン（Local Zone）
要求に認証が必要（**Request must be authenticated**）	いいえ（No）
モード（**Mode**）	エイリアスのパターン マッチ（Alias pattern match）
パターン タイプ（**Pattern type**）	正規表現（Regex）

フィールド	値
パターン文字列（**Pattern string**）	911|(911@%localdomains%)
パターン動作（**Pattern behavior**）	変更なし（Leave）
正常に一致する場合（**On successful match**）	停止（Stop）
転送先ゾーン（**Target zone**）	PSTNGateway2
状態（**State**）	有効

例 2：ルール **#3**

フィールド	値
ルール名	緊急コール - PSTNGateway1 経由のプレフィックス 00 で 911
Description	PSTNGateway 経由で 911 緊急コールのルーティング
優先度（**Priority**）	3
[Protocol]	任意（Any）
ソース（**Source**）	ローカル ゾーン（Local Zone）
要求に認証が必要（**Request must be authenticated**）	いいえ（No）
モード（**Mode**）	エイリアスのパターン マッチ（Alias pattern match）
パターン タイプ（**Pattern type**）	正規表現（Regex）
パターン文字列（**Pattern string**）	00(911|911@%localdomains%)
パターン動作（**Pattern behavior**）	置換（Replace）
文字列の置換（**Replace string**）	\1

フィールド	値
正常に一致する場合（**On successful match**）	続行（Continue）
転送先ゾーン（**Target zone**）	PSTNGateway1
状態（**State**）	有効

例 2：ルール **#4**

フィールド	値
ルール名	緊急コール - PSTNGateway2 経由のプレフィックス 00 で 911
Description	PSTNGateway 経由で 911 緊急コールのルーティング
優先度（**Priority**）	4
[Protocol]	任意（Any）
ソース（**Source**）	ローカル ゾーン（Local Zone）
要求に認証が必要（**Request must be authenticated**）	いいえ（No）
モード（**Mode**）	エイリアスのパターン マッチ（Alias pattern match）
パターン タイプ（**Pattern type**）	正規表現（Regex）
パターン文字列（**Pattern string**）	00(911|911@%localdomains%)
パターン動作（**Pattern behavior**）	置換（Replace）
文字列の置換（**Replace string**）	\1
正常に一致する場合（**On successful match**）	停止（Stop）
転送先ゾーン（**Target zone**）	PSTNGateway2

フィールド	値
状態（**State**）	有効

外部サービスを使用するための検索ルールの設定

検索ルール（ダイヤル プラン）に外部ポリシー サービスを使用するよう Expressway を設定する設定手順は以下のステップに分かれます。

- 検索ルールで使用するポリシー サービスを設定します。
- ポリシー サービスに検索を指定するための関連の検索ルールを設定します。

検索ルールが使用するポリシー サービスの設定

手順

ステップ 1 **[設定（Configuration）]**>**[ダイヤル プラン（Dial plan）]**>**[ポリシー サービス（Policy services）]** に移動します。

ステップ 2 **[新規（New）]** をクリックします。

ステップ 3 コールポリシーの場合と同じようにサーバアドレスと接続プロトコルを設定します。

ステップ 4 「**ポリシー サービスの作成（Create policy service）**」ページのフィールドを次のように設定します。

フィールド	説明	使用方法のヒント
名前（Name）	ポリシー サービスの名前。	
Description	オプションの自由形式のポリシー サービスの説明。	リストのポリシー サービスの上にマウス ポインタを置いた場合に説明がツールチップとして表示されます。
[Protocol]	ポリシー サービスに接続するために使用するプロトコル。 デフォルトは *HTTPS* です。	ポリシー サービス サーバと通信を行う場合、Expressway は HTTP から HTTPS へのリダイレクトを自動的にサポートします。

フィールド	説明	使用方法のヒント
証明書検証モード（Certificate verification mode）	HTTPS を使用して接続すると、この設定は、ポリシーサーバが提示する証明書を検証するかどうかを制御します。 設定が [オン（On）] の場合、Expressway で HTTPS を使用してポリシー サーバに接続するには、Expressway にそのサーバのサーバ証明書を承認するルート CA 証明書がロードされている必要があります。また、証明書のサブジェクトの共通名またはサブジェクト代替名は次の **[サーバ アドレス（Server address）]** フィールドの 1 つに一致する必要があります。	Expressway のルート CA 証明書は（**[メンテナンス（Maintenance）]** > > **[セキュリティ（Security）]** > **[信頼できる CA 証明書（Trusted CA certificate）]**）を選択してロードします。
HTTPS 証明書失効リスト（CRL）による確認（HTTPS certificate revocation list (CRL) checking）	CRL による確認で証明書を保護する場合は、このオプションを有効にし、手動で CRL ファイルをロードするか、または、自動 CRL 更新を有効にします。	**[メンテナンス（Maintenance）]** > **[セキュリティ（Security）]** > **[CRL 管理（CRL management）]** に移動して、Expressway が CRL ファイルを更新する方法を設定します。
サーバ アドレス 1 ～ 3（Server address 1 - 3）	サービスをホストしているサーバの IP アドレスまたは完全修飾ドメイン名（FQDN）を入力します。アドレスに **:<port>** を追加することでポートを指定できます。	FQDN を指定する場合は、Expressway に FQDN を解決できる適切な DNS 設定が指定されていることを確認します。 復元力のために、最大 3 つのアドレスを指定できます。
パス	サーバのサービスの URL を入力します。	
ステータス パス（Status path）	**[ステータス パス（Status path）]** は、Expressway がリモート サービスのステータスを取得できる場所からのパスを特定します。 デフォルトはステータス（status）です。	ポリシーサーバは戻りステータス情報を提供する必要があります。ポリシーサーバのステータスと復元力を参照してください。

フィールド	説明	使用方法のヒント
ユーザ名（Username）	サービスにログインし、問い合わせするために Expressway が使用するユーザ名。	
[パスワード（Password）]	サービスにログインし、問い合わせをするために Expressway が使用するパスワード。	プレーン テキストの最大長は 30 文字です（後で暗号化されます）。
デフォルト CPL（Default CPL）	これは、サービスが使用できない場合に Expressway が使用するフォールバック CPL です。	デフォルト CPL を、たとえば、応答サービスまたは録音メッセージにリダイレクトするように変更できます。 詳細については、ポリシー サービスのデフォルト CPL を参照してください。

ステップ 5 [ポリシー サービスの作成（Create policy service）] をクリックします。

ポリシー サービスに検索を指定するための検索ルールの設定

Expressway は、指定したパターンに一致するすべての検索をポリシー サービス サーバに指定します。

最初のエイリアスでは一致し、次にポリシー サーバがコールをルーティングしたエイリアスについては一致しない、または拒否を返信しないように検索ルールを設定する必要があります。

手順

ステップ 1 **[設定（Configuration）] > [ダイヤル プラン（Dial plan）] > [検索ルール（Search rules）]** に移動します。

ステップ 2 [新規（New）] をクリックします。

ステップ 3 外部ポリシー サーバに指定する検索に応じて、「**検索ルールの作成（Create search rule）**」ページのフィールドを設定します。

この例は、.meet で終わっているエイリアスへのコールを外部ポリシー サーバに転送する方法を示しています。

フィールド	値
ルール名	ルールを説明する短い名前。
Description	フリー形式のルールの説明。
優先度（Priority）	必要に応じて、10 など。

フィールド	値
[Protocol]	必要に応じて、[すべて（Any）] などにします。
ソース（**Source**）	必要に応じて、[すべて（Any）] などにします。
要求に認証が必要（**Request must be authenticated**）	この設定は認証ポリシーに従って設定します。
モード（**Mode**）	必要に応じて、[エイリアスのパターンの一致（Alias pattern match）] などにします。
パターン タイプ（**Pattern type**）	必要に応じて、[正規表現（Regex）] などにします。
パターン文字列（**Pattern string**）	必要に応じて、「.*\.meet@example.com」などにします。
パターン動作（**Pattern behavior**）	必要に応じて、[許可（Leave）] などにします。
正常に一致する場合（**On successful match**）	必要に応じて入力 （注） [停止（Stop）] が選択された場合、Expressway は元のエイリアスに対して、それ以上検索ルールを処理しませんが、新しいエイリアスが CPL で返される場合は、完全なコール処理シーケンスが再起動されます。
Target	前の手順で作成したポリシー サービスを選択します。
状態（**State**）	有効（*Enabled*）

ポリシー サーバにすべての検索を転送するには、どちらもポリシー サービスを対象とする 2 つの検索ルールを設定できます。

- **[モード（Mode）]** を *[*任意のエイリアス（*Any alias*）*]* に設定した最初の検索ルール。
- **[モード（Mode）]** を *[*すべての *IP* アドレス（*Any IP address*）*]* に設定した 2 番目の検索ルール。

ステップ 4 [検索ルールの作成（Create search rule）] をクリックします。

コール ポリシーについて

許可するコール、拒否するコール、および別の宛先に転送するコールを制御するルールをセットアップできます。これらのルールをコールポリシー（または管理者ポリシー）と呼びます。

コール ポリシーが有効になっており、設定されている場合は、コールが行われるたびに、Expresswayはそのコールの送信元と宛先に基づいて次のことを決定するためにポリシーを実行します。

- 元の宛先へのコールのプロキシ経由での送信します。
- 別の宛先または別の一連の宛先へのコールの転送します。
- 着信を拒否します。

（注） 有効になっている場合、Expressway を通過するすべてのコールにコール ポリシーが実行されます。

次の操作を実行する必要があります。

- コールポリシーを使用し、Expressway を介してコールを送受信できる発信者を決定する
- 許可リストと拒否リストについてを使用し、Expresswayに登録できるエイリアス、または登録できないエイリアスを決定する

コール ポリシーの設定

「コール ポリシーの設定（Call Policy configuration）」ページ（**[設定（Configuration）]** > >**[コール ポリシー（Call Policy）]** > **[設定（Configuration）]**）を使用してExpresswayのコールポリシーについてモードを設定し、ローカルポリシーファイルをアップロードします。

コール ポリシー モード

コール ポリシー モードは、コール ポリシーの設定を Expressway が取得する場所を制御します。次のオプションがあります。

- *[ローカル CPL（Local CPL）]*：ローカルで定義したコール ポリシーを使用します。
- *[ポリシー サービス（Policy service）]*：外部ポリシー サービスを使用します。
- *[オフ（Off）]*：コール ポリシーを使用しません。

次に、これらのオプションを詳しく説明します。

ローカル CPL（Local CPL）

[ローカル CPL（Local CPL）] オプションでは Expressway 上でローカルに設定されたコール ポリシーを使用します。*[ローカル CPL（Local CPL）]* を選択した場合は、次のいずれかを実行する必要があります。

- **コールポリシールール**ページで（**[設定（Configuration）]** > **[コールポリシー（Call Policy）]** > **[ルール（Rules）]**）ページで 、Web インターフェイスを使用したコール ポリシー ルールの設定します。

（注） これにより、指定したコールのみを許可または拒否できます。

- CPL スクリプトを使用したコール ポリシーの設定を行います。このファイルには CPL スクリプトが含まれています。ただし、CPL スクリプトの作成は複雑であるため、代わりに外部ポリシーサービスを使用することを推奨します。

コール ポリシーの指定に一度に使用できるのは、これらの 2 つの方法のいずれかのみです。CPL スクリプトがアップロードされている場合は、そのスクリプトが優先されるため、「**コール ポリシー ルール（Call Policy rules）**」ページを使用できません。このページを使用するには、アップロードされている CPL スクリプトを最初に削除する必要があります。

[ローカル CPL（Local CPL）] が有効になっていても、ポリシーが設定されていないか、またはアップロードされていない場合は、デフォルトのポリシーが適用されます。これにより、送信元や宛先に関係なく、すべてのコールが許可されます。

すべてのコール ポリシーの決定を外部サービスに照会する場合は、*[ポリシー サービス（Policy service）]* オプションを使用します。このオプションを選択すると、外部サービスの接続の詳細情報を指定できる一連の設定フィールドが新たに表示されます。外部サービスを使用するためのコール ポリシーの設定を参照してください。

Web インターフェイスを使用したコール ポリシー ルールの設定

「コールポリシー ルール（Call Policy rules）」ページ（**[設定（Configuration）]** > **[コールポリシー（Call Policy）]** > **[ルール（Rules）]**）には、現在導入されている（CPL ファイル経由でアップロードされたのではなく）Web で設定されたコールポリシー ルールのリストが表示されます。また、このページでは、ルールを作成、編集、削除できます。このページには基本的なコール ポリシー ルールをセットアップするメカニズムが備わっており、CPL スクリプトを作成したりアップロードしたりする必要はありません。

CPL ファイルがすでに導入されている場合は、**[コールポリシー ルール（Call Policy rules）]** ページを使用してコールポリシーを設定できません。この場合は、**「コールポリシーの設定（Call Policy configuration）」**ページ（**[設定（Configuration）]** > **[コール ポリシー（Call Policy）]** > **[設定（Configuration）]**）の **[アップロード済みのファイルの削除（Delete uploaded file）]** オプションを使用します。このオプションで CPL スクリプトを使用して導入された既存のポリシーを削除して「**コール ポリシー ルール（Call Policy rules）**」ページを使用できるようにし、コール ポリシーを設定します。

各ルールで、特定の**送信元**から特定の**宛先**エイリアスへのコールに実行する**アクション**を指定します。複数のルールがある場合は、それらのルールを適用するプライオリティ順に**並べ替える**こともできます。

コール ポリシー ルールが設定されていない場合は、デフォルトのポリシーで送信元や宛先に関係なく、すべてのコールが許可されます。

設定するルールをクリックします（または**[新規（New）]**をクリックして新しいルールを作成するか、**[削除（Delete）]** をクリックして選択したルールを削除します）。

各ルールの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
送信元のタイプ（Source type）	このフィールドでは、コールの送信元をゾーンまたは送信元アドレス の 2 つのタイプから選択できます。この選択は、ルールの設定に使用するそのほかのフィールドに影響します。	異なる送信元のタイプを使用してルールの組み合わせを設定できます。コール ポリシーを実装するため、または電話料金の詐欺行為から会議リソースを保護するために、これらを定義し、順序付けます。
発信側ゾーン（Originating Zone）	**[送信元のタイプ（Source type）]** が *[ゾーン（Zone）]* に設定されたルールに対してのみ表示されます。 ドロップダウンには、この Expressway に設定されたすべてのゾーンが表示されるため、このルールによって検査されたコールの送信元を選択できます。 ルールは、選択されたゾーンから発信されるすべてのコールを検査します。	
ルールの適用先（Rule applies to）	**[送信元のタイプ（Source type）]** が *[送信元アドレス（From address）]* に設定されたルールに対してのみ表示されます。 このフィールドでは、ルールが認証済みの発信者または非認証の発信者からのコールを検査するかどうかを選択できます。 認証済みの発信者は次のデバイスです。 • Expressway にローカルに登録され、認証されている、または • ネイバーに登録され、認証されてから、ローカル Expressway に認証されている	詳細については、デバイス認証についてを参照してください。

フィールド	説明	使用方法のヒント
送信元パターン（Source pattern）	**[送信元のタイプ（Source type）]** が *[送信元アドレス（From address）]* に設定されたルールに対してのみ表示されます。 ルールは、このフィールドへの入力値と、発信側エンドポイントが自身を特定するために使用する送信元アドレスの一致を試みます。 このフィールドが空白の場合、ポリシー ルールは、選択した発信者のタイプ（認証済みまたは非認証）からのすべての着信コールに適用されます。	より一般的なルール用のパターンを使用する、または明示的に特定の発信者を許可または拒否する必要がある場合には 1 つのエイリアス用のパターンを使用することができます。 このフィールドは、正規表現をサポートします。
宛先パターン（Destination pattern）	すべてのルールに必要です。 ルールは、このフィールドへの入力値と、着信コールからの宛先アドレスの一致を試みます。	より一般的なルール用のパターンを使用する、または明示的に特定の宛先を許可または拒否する必要がある場合には 1 つのエイリアス用のパターンを使用することができます。 このフィールドは、正規表現をサポートします。
アクション（Action）	検査したコールが、送信元と宛先に指定したものと一致したときの、ルールの動作を定義します。*[許可（Allow）]* または *[却下（Reject）]* を選択できます。 *[許可（Allow）]*：送信元アドレスまたは発信側ゾーンがルールのソースパラメータと一致した場合、およびコールの宛先がルールの宛先パターンに一致した場合、Expressway はコールを処理し続けます。 *[却下（Reject）]*：送信元アドレスまたは発信側ゾーンがルールのソースパラメータと一致した場合、およびコールの宛先がルールの宛先パターンに一致した場合、Expressway はコールを拒否します。	

フィールド	説明	使用方法のヒント
並べ替え（Rearrange）	このフィールドは、コール ポリシー ルールのリストでのみ表示されます（[コール ポリシー ルール（Call Policy rules）] ページ）。 ルールの順序を変更し、相対的な優先順位を変更するには、↑ および ↓ アイコンをクリックします。	各ルールは、コールに一致するまで、上から順に着信コールの詳細と比較されます。 ルールが一致すると、ルールのアクションがコールに適用されます。

CPL スクリプトを使用したコール ポリシーの設定

高度なコール ポリシーを設定するには、CPL スクリプトを使用します。これを行うには、まず、CPL スクリプトをテキスト ファイルとして作成して保存し、その後で Expressway にアップロードします。ただし、CPL スクリプトの記述は複雑なため、代わりに外部外部ポリシーの概要を使用することを推奨します。

Expressway でサポートされている CPL 構文とコマンドについては、CPL リファレンスのセクションを参照してください。

既存の CPL スクリプトの表示

XML ベースの CPL スクリプトとして現在導入されているコール ポリシーを表示するには、コール ポリシーの設定ページ（**[設定（Configuration）]** > **[コール ポリシー（Call Policy）]** > **[設定（Configuration）]**）に移動し、**[コールポリシーファイルの表示（Show Call Policy file）]** をクリックします。

- CPL スクリプトを使用するようにコール ポリシーを設定した場合は、アップロードしたスクリプトが表示されます。
- 「**コール ポリシー ルール（Call Policy rules）**」ページでコール ポリシーを設定した場合は、CPL バージョンのコール ポリシー ルールが表示されます。
- **[コール ポリシー モード（Call Policy mode）]** が *[オン（On）]* になっていてもポリシーが設定されていない場合は、すべてのコールを許可するデフォルトの CPL スクリプトが表示されます。

コール ポリシーのバックアップ コピーを取得するファイルを表示したり、コール ポリシーが [コール ポリシー ルール（Call Policy rules）] ページを使用して設定されている場合は、この CPL ファイルのコピーを取得し、より高度な CPL スクリプトを作成するための開始点として使用できます。

コール ポリシーを「**コール ポリシー ルール（Call Policy rules）**」ページを使用して設定した後に、CPL ファイルをダウンロードした後に編集せずに Expressway へアップロードした場合は、Expressway がそのファイルを認識して、各ルールを「**コール ポリシー ルール（Call Policy rules）**」ページに自動的に追加します。

CPL XSD ファイルについて

CPL スクリプトは Expressway によってサポートされている形式である必要があります。「**コール ポリシーの設定（Call Policy configuration）**」ページでは、Expressway へアップロードしたスクリプトの確認に使用する XML スキーマをダウンロードできます。XSD ファイルを使用して、CPL スクリプトが有効であることを事前に確認できます。2 つのダウンロード オプションから選択できます。

- **[CPL XSD ファイルの表示（Show CPL XSD file）]**：CPL スクリプトが使用する XML スキーマをブラウザに表示します。
- **[CPL 拡張 XSD ファイルの表示（Show CPL Extensions XSD file）]**：Expressway がサポートする追加の CPL 要素に使用する XML スキーマをブラウザに表示します。

CPL スクリプトのアップロード

CPL スクリプトの Expressway ポールは 5 秒ごとに変更されます。そのため、Expressway はほぼ即時にアップロードされた CPL スクリプトの使用を開始します。CPL スクリプトはコマンド ライン インターフェイスを使用してアップロードできません。新しい CPL ファイルをアップロードするには、次の手順を実行します。

手順

ステップ 1 **[設定（Configuration）] > [コールポリシー（Call Policy）] > [設定（Configuration）]** に移動します。

ステップ 2 **[ポリシー ファイル（Policy files）]** セクションの **[新しいコール ポリシー ファイルの選択（Select the new Call Policy file）]** フィールドで、ファイル名を入力するか、アップロードする CPL スクリプトを**参照**します。

ステップ 3 [ファイルのアップロード（Upload file）] をクリックします。

既存の CPL スクリプトの削除

CPL スクリプトがすでにアップロードされている場合は **[アップロード済みのファイルの削除（Delete uploaded file）]** ボタンが表示されます。ファイルを削除するには、そのボタンをクリックします。

外部サービスを使用するためのコール ポリシーの設定

すべてのポリシー決定を外部サービスに委託するようコール ポリシーを設定するには、次の手順を実行します。

手順

ステップ 1 **[設定（Configuration）]** > **[コールポリシー（Call Policy）]** > **[設定（Configuration）]** に移動します。

ステップ 2 **[コール ポリシー モード（Call Policy mode）]** に *[ポリシー サービス（Policy service）]* を選択します。

ステップ 3 フィールドの設定は以下のとおりです。

フィールド	説明	使用方法のヒント
[Protocol]	ポリシーサービスに接続するために使用するプロトコル。 デフォルトは *HTTPS* です。	ポリシー サービス サーバと通信を行う場合、Expressway は HTTP から HTTPS へのリダイレクトを自動的にサポートします。
証明書検証モード（Certificate verification mode）	HTTPS を使用して接続すると、この設定は、ポリシーサーバが提示する証明書を検証するかどうかを制御します。 設定が [オン（On）] の場合、Expressway で HTTPS を使用してポリシー サーバに接続するには、Expresswayにそのサーバのサーバ証明書を承認するルート CA 証明書がロードされている必要があります。また、証明書のサブジェクトの共通名またはサブジェクト代替名は次の [サーバ アドレス（Server address）] フィールドの 1 つに一致する必要があります。	Expressway のルート CA 証明書は（**[メンテナンス（Maintenance）]** > **[セキュリティ（Security）]** > **[信頼できる CA 証明書（Trusted CA certificate）]**）を選択してロードします。
HTTPS 証明書失効リスト（CRL）による確認（HTTPS certificate revocation list (CRL) checking）	CRL による確認で証明書を保護する場合は、このオプションを有効にし、手動で CRL ファイルをロードするか、または、自動 CRL 更新を有効にします。	> **[セキュリティ（Security）]** > **[CRL 管理（CRL management）]** に移動して、Expressway が CRL ファイルを更新する方法を設定します。

フィールド	説明	使用方法のヒント
サーバ アドレス 1 ～ 3（Server address 1 - 3）	サービスをホストしているサーバの IP アドレスまたは完全修飾ドメイン名（FQDN）を入力します。アドレスに **:<port>** を追加することでポートを指定できます。	FQDN を指定する場合は、Expressway に FQDN を解決できる適切な DNS 設定が指定されていることを確認します。 復元力のために、最大 3 つのアドレスを指定できます。
パス	サーバのサービスの URL を入力します。	
ステータス パス（Status path）	**[ステータス パス（Status path）]** は、Expressway がリモート サービスのステータスを取得できる場所からのパスを特定します。 デフォルトはステータス（status）です。	ポリシーサーバは戻りステータス情報を提供する必要があります。ポリシーサーバのステータスと復元力を参照してください。
ユーザ名（Username）	サービスにログインし、問い合わせするために Expressway が使用するユーザ名。	
[パスワード（Password）]	サービスにログインし、問い合わせをするために Expressway が使用するパスワード。	プレーン テキストの最大長は 30 文字です（後で暗号化されます）。
デフォルト CPL（Default CPL）	これは、サービスが使用できない場合に Expressway が使用するフォールバック CPL です。	デフォルト CPL を、たとえば、応答サービスまたは録音メッセージにリダイレクトするように変更できます。 詳細については、ポリシーサービスのデフォルト CPL を参照してください。

ステップ 4 フィールドの設定は以下のとおりです。

フィールド	説明	使用方法のヒント
[Protocol]	ポリシーサービスに接続するために使用するプロトコル。 デフォルトは *HTTPS* です。	ポリシー サービス サーバと通信を行う場合、Expressway は HTTP から HTTPS へのリダイレクトを自動的にサポートします。

フィールド	説明	使用方法のヒント
証明書検証モード（Certificate verification mode）	HTTPS を使用して接続すると、この設定は、ポリシーサーバが提示する証明書を検証するかどうかを制御します。 設定が [オン（On）] の場合、Expressway で HTTPS を使用してポリシー サーバに接続するには、Expressway にそのサーバのサーバ証明書を承認するルート CA 証明書がロードされている必要があります。また、証明書のサブジェクトの共通名またはサブジェクト代替名は次の **[サーバ アドレス（Server address）]** フィールドの 1 つに一致する必要があります。	Expressway のルート CA 証明書は（**[メンテナンス（Maintenance）] > > [セキュリティ（Security）] > [信頼できる CA 証明書（Trusted CA certificate）]**）を選択してロードします。
HTTPS 証明書失効リスト（CRL）による確認（HTTPS certificate revocation list (CRL) checking）	CRL による確認で証明書を保護する場合は、このオプションを有効にし、手動で CRL ファイルをロードするか、または、自動 CRL 更新を有効にします。	**[メンテナンス（Maintenance）] > [セキュリティ（Security）] > [CRL 管理（CRL management）]** に移動して、Expressway が CRL ファイルを更新する方法を設定します。
サーバ アドレス 1 ～ 3（Server address 1 - 3）	サービスをホストしているサーバの IP アドレスまたは完全修飾ドメイン名（FQDN）を入力します。アドレスに **:<port>** を追加することでポートを指定できます。	FQDN を指定する場合は、Expressway に FQDN を解決できる適切な DNS 設定が指定されていることを確認します。 復元力のために、最大 3 つのアドレスを指定できます。
パス	サーバのサービスの URL を入力します。	
ステータス パス（Status path）	**[ステータス パス（Status path）]** は、Expressway がリモート サービスのステータスを取得できる場所からのパスを特定します。 デフォルトはステータス（status）です。	ポリシーサーバは戻りステータス情報を提供する必要があります。ポリシーサーバのステータスと復元力を参照してください。

フィールド	説明	使用方法のヒント
ユーザ名（Username）	サービスにログインし、問い合わせするために Expressway が使用するユーザ名。	
[パスワード（Password）]	サービスにログインし、問い合わせをするために Expressway が使用するパスワード。	プレーン テキストの最大長は 30 文字です（後で暗号化されます）。
デフォルト CPL（Default CPL）	これは、サービスが使用できない場合に Expressway が使用するフォールバック CPL です。	デフォルト CPL を、たとえば、応答サービスまたは録音メッセージにリダイレクトするように変更できます。 詳細については、ポリシー サービスのデフォルト CPL を参照してください。

ステップ 5 [保存（Save）] をクリックします。

Expressway はポリシー サービス サーバに接続し、コール ポリシーの決定に必要なサービスを使用して開始する必要があります。

接続の問題は、このページに報告されます。このページの下部の **[ステータス（Status）]** エリアを確認し、追加の情報メッセージを **[サーバ アドレス（Server address）]** フィールドと照合します。

サポートされているアドレス形式

発信者のエンドポイントを使用して入力する宛先アドレスにはさまざまな形式を使用できますが、これは、宛先エンドポイントを見つけようとしたときに Expressway が従う特定のプロセスに影響します。Expressway でサポートされるアドレス形式は次のとおりです。

- IP アドレス。例：`10.44.10.1` または `3ffe:80ee:3706::10:35`
- H.323 ID、例えば `john.smith` または `john.smith@example.com`

（注） H.323 ID は URI 形式で使用できます。

- E.164 エイリアス。例：`441189876432` または `6432`
- URI。例：`john.smith@example.com`
- ENUM。例：`441189876432` または `6432`

これらのアドレス形式それぞれをサポートするには、Expressway での設定が必要な場合があります。次の表に、それらの設定要件を示します。

IP アドレスによるダイヤリング

宛先エンドポイントがシステムに登録されていない場合は、IP アドレスによるダイヤリングが必要です。詳細については、IP アドレスによるダイヤリングの項を参照してください。

H.323 ID または E.164 エイリアスによるダイヤリング

H.323 ID または E.164 エイリアスを使用してコールするための特別な設定は不要です。

Expressway は通常のコール ルーティング プロセスに従い、トランスフォーメーションを適用してから、検索ルールに従ってローカル ゾーンと外部ゾーンでエイリアスを検索します。

（注） SIP エンドポイントは常に、UIR の形式の AOR を使用して登録されます。インターワーキングを容易にするように、H.323 エンドポイントも 必ず URI の形式の H.323 ID を使用して登録することを推奨します。

H.323 または SIP URI によるダイヤリング

ユーザが URI ダイヤリングを使用してコールを発信するときは、通常 **name@example.com** をダイヤルします。

宛先エンドポイントがローカルに登録されている、またはネイバー システムに登録されている場合は、コールを発信するために必要な特別な設定はありません。Expressway は通常のコール ルーティング プロセスに従い、トランスフォーメーションを適用してから、検索ルールに従ってローカル ゾーンと外部ゾーンでエイリアスを検索します。

宛先エンドポイントがローカルに登録されていない場合、URI ダイヤリングは DNS を使用して宛先エンドポイントを見つけます。DNS を介して URI ダイヤリングをサポートするには、1 つ以上の DNS サーバと 1 つ以上の DNS ゾーンを使用して Expressway を設定する必要があります。

DNS を介した URI ダイヤリング（アウトバウンドとインバウンドの両方）をサポートする Expressway の設定方法の詳細については、URI ダイヤリングについての項を参照してください。

ENUM によるダイヤリング

ENUM ダイヤリングでは、そのエンドポイントが異なる形式のエイリアスを使用して登録されていても、E.164 番号（電話番号）にダイヤリングした発信者がエンドポイントに接続できます。E.164 番号が DNS システムによって URI に変換された後に、URI ダイヤリングのルールによりコールが発信されます。

ENUM ダイヤリング機能を使用すると、URI ダイヤリングの柔軟性は保ちながら、コールするために使用するのは番号だけというシンプルさが得られます。これは、発信者がテンキーを使用してのダイヤリングに限られている場合は特に重要です。

Expressway で ENUM ダイヤリングをサポートするには、1 つ以上の DNS サーバと適切な ENUM ゾーンを使用して設定する必要があります。

ENUM ダイヤリング（アウトバウンドとインバウンドの両方）をサポートする Expressway の設定方法の詳細については、「ENUM ダイヤリングについて」の項を参照してください。

IP アドレスによるダイヤリング

宛先エンドポイントがシステムに登録されていない場合は、IP アドレスによるダイヤリングが必要です。

宛先エンドポイントが登録されている場合は、IP アドレスを使用してコールすることも可能ですが、エンドポイントがプライベート ネット上にあるか、またはファイアウォールの背後にある場合は失敗する場合があります。このため、AOR や H.323 ID など、別のアドレス形式を介して登録されたエンドポイントにコールを発信することを推奨します。同様に、ネットワーク外の発信者が IP アドレスを使用してネットワーク内のエンドポイントと通信しないようにしてください。

既知の IP アドレスへのコール

IP アドレスがローカルに登録されたエンドポイントである場合、または Expressway で設定されているいずれかのサブゾーンメンバーシップルールの IP アドレス範囲内にある場合、Expressway はその IP アドレスを「「既知」」のものと見なします。

SIP ユーザ エージェント（および H.323 エンドポイント）は、メンバーシップ ルールに基づき、デフォルトのサブゾーンまたはカスタマイズされたサブゾーンに登録します。インターワーキングのタイミングは、コール フローによって異なります。

SIP IP ダイヤルは、常に UDP として扱われるなど、Expressway 上で期待される動作になります。Expressway サーバは次のとおりです。

1. デフォルト サブゾーンからカスタム Subzone1 へのコール -> SIP 間ネイティブ コールに進みます。Subzone1 で登録されているユニットが SIP UDP として登録されていない場合、ネイティブ プロトコルは失敗するため、サーバがインターワーキングを行うまでに遅延が発生します。
2. Subzone1 からデフォルト サブゾーンへのコール -> ただちに SIP-to-H.323 インターワーキング コールにフォールバックします。
3. Subzone1 から Subzone1 へのコール -> SIP 間ネイティブ コールに進みます。Subzone1 で登録されているユニットが SIP UDP として登録されていない場合、ネイティブ プロトコルは失敗するため、サーバがインターワーキングを行うまでに遅延が発生します。

4. Subzone1 から Subzone2 へのコール -> SIP 間ネイティブ コールに進みます。Subzone2 で登録されているユニットが SIP UDP として登録されていない場合、ネイティブ プロトコルは失敗するため、サーバがインターワーキングを行うまでに遅延が発生します。
5. デフォルト サブゾーンからデフォルト サブゾーンへのコール -> ただちに SIP-to-H.323 インターワーキング コールにフォールバックします。

不明 IP アドレスへのコール（Calls to unknown IP addresses）

Expressway は IP アドレスによるダイヤリングをサポートしていますが、Expressway がローカルではない IP アドレスにコールを発信できることが望ましくない場合もあります。Expressway の代わりにネイバーにコールを発信させたり、そのようなコールをまったく許可しないようにすることもできます。**[不明 IP アドレスへのコール（Calls to unknown IP addresses）]** の設定（「ダイヤル プランの設定」ページ）で、ローカル ネットワークになく、Expressway またはそのネイバーの 1 つに登録されていない IP アドレスに発信されたコールを Expressway がどのように処理するかを設定します。

Expressway は既知の IP アドレスに常にコールを発信しようとします（ローカル ゾーンに *[任意の IP アドレス（Any IP Address）]* の検索ルールがある場合）。

ほかのすべての IP アドレスは「「不明」」と見なし、**[不明 IP アドレスへのコール（Calls to Unknown IP addresses）]** の設定に従って Expressway が処理します。

- *[直接（Direct）]*：Expressway は、ネイバーに照会することなく、不明 IP アドレスにコールを直接発信しようとします。
- *[間接（Indirect）]*：Expressway は通常の検索プロセスに従ってネイバーに、つまり、*[任意の IP アドレス（Any IP Address）]* モードの検索ルールのターゲットであるゾーンに検索要求を転送します。一致が検出され、ネイバーの設定でその IP アドレスへのコールが許可されている場合は、Expressway はコールをそのネイバーに渡して完了します。これがデフォルトの設定です。
- *[オフ（Off）]*：Expressway はネイバーのいずれにも直接的にも間接的にもコールを発信しようとしません。

この設定は、ゾーン トランスフォーメーションの前、かつ検索前のトランスフォーメーション、コール ポリシーまたはユーザ ポリシーのルールの適用後にコールの宛先アドレスに適用されます。

（注） コールの制御のほかに、SIP デバイスのプロビジョニングメッセージとプレゼンスメッセージは IP アドレスにルーティングされることから、この設定ではそれらのメッセージの動作も決定します。

未登録エンドポイントへのコール発信

登録されていないエンドポイントとは、H.323 ゲートキーパーまたは SIP レジストラに登録されていないデバイスのことです。ほとんどのコールは、このようなシステムに登録されている

エンドポイント間で行われますが、未登録エンドポイントへコールを発信する必要が生じる場合があります。未登録エンドポイントにコールする方法は次の 2 つです。

- URI をダイヤルする。これには、URI ダイヤリングをサポートするようにローカル Expressway を設定し、未登録のエンドポイントの IP アドレスを解決するその URI の DNS レコードが存在している必要があります。
- IP アドレスをダイヤルする。

ファイアウォールを通過するための推奨設定

ファイアウォール トラバーサルのために Expressway-E が Expressway-C と隣接している場合、通常は、**[不明な IP アドレスへのコール（Calls to unknown IP addresses）]** を Expressway-C では *[間接（Indirect）]* に、Expressway-E では *[直接（Direct）]* に設定する必要があります。ファイアウォール内の発信者がファイアウォール外の IP アドレス コールの発信を試みると、次のようにルーティングされます。

1. コールはエンドポイントから、そのエンドポイントが登録されている Expressway-C に進みます。
2. コールされた IP アドレスがその Expressway に登録されておらず、**[不明な IP アドレスへのコール（Calls to unknown IP addresses）]** の設定が *[間接（Indirect）]* であるため、Expressway はコールを直接発信できません。代わりに、この Expressway は隣接する Expressway-E を照会し、そのシステムが Expressway-C の代わりにコールを発信できるかどうかを確認します。トラバーサル サーバ ゾーンに対して検索ルールを *[任意の IP アドレス（Any IP Address）]* に設定する必要があります。
3. Expressway-E がコールを受信すると、**[不明な IP アドレスへのコール（Calls to unknown IP addresses）]** 設定が *[直接（Direct）]* であるため、そのコールはコールされた IP アドレスに直接発信されます。

URI ダイヤリングについて

URI アドレスの形式は通常、**name@example.com** です。ここで、**name** はエイリアス、**example.com** はドメインです。

URI ダイヤリングは DNS を利用して、さまざまなシステムに登録されているエンドポイントを互いに見つけ出せるようにし、コールし合えるようにします。DNS がない場合、エンドポイントを互いに見つけ出せるようにするには、同じシステムまたは隣接するシステムにエンドポイントを登録する必要があります。

DNS を使用しない URI ダイヤリング

DNS を使用しない場合、URI ダイヤリングを使用してローカルに登録されたエンドポイントが行ったコールは、宛先エンドポイントもローカルに登録されている場合、またはネイバーシス

テムを介してアクセスできる場合にのみ、発信されます。これらのエンドポイントは、DNS クエリではなく、検索とゾーン変換プロセスを使用して見つけることができるためです。

DNS を使用せずにネットワークから URI ダイヤリングを使用する場合、ネットワーク内のすべてのシステムが互いに、直接または間接的ではなく、ネイバー関係で接続されていることを確認する必要があります。これによって、エンドポイントの URI を検索することで、いずれかのシステムがそのシステム自体または他のシステムに登録されているエンドポイントを確実に見つけられるようにします。

これは、システムの数が増えても十分に拡張されません。また、特に実用的でもありません。つまり、ネットワーク内のエンドポイントは、2 つのシステム間にネイバー関係がなければ、そのネットワーク外のシステムに登録されているエンドポイントにはダイヤルできません（別の会社へのコールの発信など）。

DNS ゾーンと DNS サーバがローカル Expressway 上に設定されていない場合、ローカルに登録されていないエンドポイントまたはネイバー システムへのコールは、ローカル Expressway が DNS を介した URI ダイヤリング用に設定された別の Expressway に（直接または間接的に）隣接していれば、発信されます。この場合、そのネイバーゾーンを参照する検索ルールによってピックアップされた URI でダイヤリングされたコールは、そのネイバーを経由し、DNS ルックアップが実行されます。

この設定は、すべての URI ダイヤリングを Expressway-E などの特定の 1 つのシステムを介して実行する場合に役に立ちます。

ネットワーク内での URI ダイヤリングの一環として DNS を使用しない場合は、特別な設定は不要です。エンドポイントが URI 形式のエイリアスを使用して登録され、コールがその URI に対して実行されたときに、Expressway がローカル ゾーンとネイバーにその URI について照会します。

Expressway に DNS が設定されておらず、ネットワークに H.323 エンドポイントが含まれている場合、これらのエンドポイントに URI ダイヤリングを使用して到達するには、次のいずれかが必要です。

- H.323 の登録で使用される形式に URI を変換するために適切なトランスフォーメーションを作成する。たとえば、H.323 エンドポイントを**エイリアス**を使用して登録し、**alias@domain.com** に対して着信コールを実行するという導入方法があります。この場合はローカル トランスフォーメーションを設定して **@domain**, を除去し、ローカルで **alias** を検索します。これを実行する方法の例については、H.323 番号へのダイヤリングでの @domain の除去を参照してください。

SIP エンドポイントは常に URI 形式の AOR で登録されるため、特別な設定は不要です。

DNS を使用した URI ダイヤリング

URI ダイヤリングの一環として DNS を使用することで、不明なシステムに登録されている可能性がある場合でも、エンドポイントを検出できます。Expressway は DNS ルックアップを使用して URI アドレス内のドメインを見つけ、そのドメインにエイリアスを照会します。詳細については、DNS を使用した URI の解決プロセスのセクションを参照してください。

DNS を介した URI ダイヤリングは、発信コールと着信コールに別々に有効にできます。

発信コール

URI ダイヤリングを使用し、DNS を介して Expressway がエンドポイントを見つけられるようにするには、次の手順を実行します。

- 少なくとも 1 つの DNS ゾーンと関連する検索ルールを設定します。
- 少なくとも 1 つの DNS サーバを設定します。

この詳細については、発信コールでの DNS を介した URI ダイヤリングのセクションを参照してください。

着信コール

Expressway に登録されているエンドポイントで、ローカルに登録されていないエンドポイントからのコールを URI ダイヤリングを使用し、DNS を介して受信できるようにするには、次の手順を実行します。

- すべてのエンドポイントが AOR（SIP）または URI 形式の H.323 ID で登録されていることを確認する
- 使用するプロトコルとトランスポートタイプとに応じて適切な DNS レコードを設定する

この詳細については、着信コールでの DNS を介した URI ダイヤリングのセクションを参照してください。

ファイアウォール トラバーサル コール

URI を使用したコールをファイアウォールを通じて送受信できるようにシステムを設定するには、URI ダイヤリングとファイアウォール トラバーサルのセクションを参照してください。

DNS を使用した URI の解決プロセス

Expressway が DNS システムを使用して宛先 URI アドレスを見つけようとする場合の一般的なプロセスは次のとおりです。

H.323

1. Expressway は URI 内のドメインに関する SRV レコードについて DNS サーバにクエリを送信します（複数の DNS サーバを Expressway に設定している場合、クエリはすべてのサーバに同時に送信されますが、すべての応答は Expressway が使用している SRV レコードで最も関連性の高いもののみを使用して優先順位付けが行われます）。使用可能な場合、この SRV レコードは、デバイス自体や、そのドメインに権限を持つ H.323 ゲートキーパーに関する情報（FQDN やリスニング ポートなど）を返します。
   - URI アドレスのドメインの部分が H.323 ロケーション SRV レコード（_h323ls の部分）を使用して正常に解決された場合、Expressway は返された名前レコードごとに A/AAAA レコードクエリを送信します。これらは 1 つ以上の IP アドレスに解決され、

Expressway がそれらの IP アドレスへの完全 URI の LRQ をプライオリティ順に送信します。

- URI アドレスのドメインの部分が H.323 コール シグナリング SRV レコード（_h323cs の部分）を使用して解決された場合、Expressway は返された名前レコードごとに A/AAAA レコードクエリを送信します。これらは1つ以上の IP アドレスに解決され、Expressway がこれらのレコードで返された IP アドレスへプライオリティ順にコールをルーティングします（例外として、**user@example.com:1719** など元のダイヤル文字列にポートが指定されていない場合があります。この場合、返されるアドレスで完全 URI アドレスが LRQ を介して照会されます）。

2. 関連する SRV レコードが見つからなかった場合は、次のようになります。
   - 照会する DNS ゾーンの [アドレス レコードを含める（Include address record）] の設定が [オン（On）] の場合、システムは URI 内のドメインの A レコードまたは AAAA レコードの検索にフォールバックします。このようなレコードが検出された場合、コールはその IP アドレスにルーティングされ、検索が終了します。

     （注） このドメイン内で検出された A レコードと AAAA レコードが SIP または H.323 をサポートするシステム以外のものである場合でも、Expressway はこのゾーンにコールを転送するため、コールは失敗します。そのため、デフォルト設定の [オフ（Off）] を使用することを推奨します。

   - 照会する DNS ゾーンの [アドレス レコードを含める（Include address record）] の設定が [オフ（Off）] の場合、Expressway は A レコードも AAAA レコードも照会しません。その代わりに検索を続行して、残りの下位のゾーンを照会します。

SIP

Expressway は、RFC 3263 で説明されているように、SIP 解決プロセスをサポートします。次に、Expressway がこのプロセスを実装する例を示します。

1. Expressway が URI のドメインについての NAPTR クエリを送信します。使用可能な場合、このクエリの結果セットは、そのドメインへの接続に使用する必要がある SRV レコードとトランスポートプロトコルの優先順位の高いリストを説明します。このドメイン名の DNS に NAPTR レコードが存在しない場合、Expressway は、NAPTR クエリから返された場合と同じ方法で、そのドメインに対してデフォルトの リスト `_sips._tcp.<domain>`, `_sip._tcp.<domain>` and `_sip._udp.<domain>` を使用します。
   - Expressway は NAPTR レコードのルックアップから返された結果それぞれに SRV クエリを送信します。返された A/AAAA レコードが優先順位付けられたリストが構築されます。
   - Expressway は、SRV レコード ルックアップによって返された名前ごとに A/AAAA レコード クエリを送信します。

上記の手順によって、ターゲット ドメインとの通信に使用される IP アドレス、ポート、およびトランスポート プロトコルのツリーが構築されます。このツリーは NAPTR レコードのプライオリティ、次に SRV レコードのプライオリティによってさらに分割されます。場所のツリーを使用すると、検索プロセスが最初の場所で停止し、ターゲットの宛先と通信したことを示す応答が返されます。

2. 検索プロセスが関連する SRV レコードを返さない場合は次のようになります。
   - 照会する DNS ゾーンの [アドレス レコードを含める（Include address record）] の設定が [オン（On）] の場合、システムは URI 内のドメインの A レコードまたは AAAA レコードの検索にフォールバックします。このようなレコードが検出された場合、コールはその IP アドレスにルーティングされ、検索が終了します。

     （注） このドメイン内で検出された A レコードと AAAA レコードが SIP または H.323 をサポートするシステム以外のものである場合でも、Expressway はこのゾーンにコールを転送するため、コールは失敗します。そのため、デフォルト設定の [オフ（Off）] を使用することを推奨します。

   - 照会する DNS ゾーンの [アドレス レコードを含める（Include address record）] の設定が [オフ（Off）] の場合、Expressway は A レコードも AAAA レコードも照会しません。その代わりに検索を続行して、残りの下位のゾーンを照会します。

発信コールでの DNS を介した URI ダイヤリング

ユーザが URI ダイヤリングを使用してコールを発信すると、通常は **name@example.com** の形式でエンドポイントからアドレスをダイヤルします。次に、Expressway に登録されたエンドポイントから URI をダイヤルした場合、またはネイバー システムからクエリとして URI アドレスを受信した場合に従うプロセスを示します。

1. Expressway は検索ルールの設定をチェックし、それらのルールの **[モード（Mode）]** が次のいずれかに設定されているかどうかを確認します。
   - *[任意のエイリアス（Any alias）]* または
   - URI アドレスに一致するパターンの *[エイリアス パターン マッチ（Alias pattern match）]*

2. 関連付けられたターゲット ゾーンで URI がプライオリティ順に照会されます。
   - ターゲット ゾーンのいずれかが DNS ゾーンである場合、Expressway は DNS ルックアップを通じてエンドポイントを見つけます。これは、Expressway に設定されている DNS サーバにドメインの場所を DNS を使用した URI の解決プロセスに従って照会することで実行されます。URI アドレスのドメインの部分が正常に解決されると、それらのアドレスに要求が転送されます。

- ターゲット ゾーンのいずれかがネイバー、トラバーサル クライアント、またはトラバーサル サーバである場合、URIについてそれらのゾーンが照会されます。そのシステムが DNS を介して URI ダイヤリングをサポートする場合、コール自体をルーティングする場合があります。

DNS ゾーンの追加と設定

DNS を介して URI ダイヤリングを有効にするには、1 つ以上の DNS ゾーンを設定する必要があります。手順は次のとおりです。

手順

ステップ 1 **[設定（Configuration）] > [ゾーン（Zones）] > [ゾーン（Zones）]** へ移動します。

ステップ 2 [新規（New）] をクリックします。**[ゾーンの作成（Create zone）]** ページが表示されます。

ステップ 3 ゾーンの**名前**を入力し、[タイプ（Type）] として [DNS] を選択します。

ステップ 4 DNS ゾーンを次のように設定します。

フィールド	ガイドライン
ホップ カウント（Hop count）	DNS を介し、URI を使用してダイヤリングすると、使用されるホップ カウントは、UIRアドレスに一致する検索ルールに関連付けられたDNS ゾーンに対して設定されたものになります（これがコールに現在関連付けられているホップ カウントよりも少ない場合）。 URI アドレスが DNS ゾーンと一致しない場合、ネイバーにクエリが送信されます。この場合、使用するホップ カウントは、ネイバー ゾーンに対して設定されたものになります（コールに現在関連付けられているホップ カウントよりも小さい場合）。
H.323 と SIP modes	[H.323] セクションと [SIP] セクションでは、コールが SIP または H.323 の SRV ルックアップを使用して見つかるかどうかに基づき、このゾーンを介して見つかったシステムとエンドポイントへのコールをフィルタリングすることができます。

フィールド	ガイドライン
アドレスレコードを含める（Include address record）	この設定によって、このゾーンを介してダイヤルされたエイリアスについての NAPTR（SIP）レコードまたは SRV（SIP と H.323）レコードが検出されなかった場合、Expressway はプライオリティが低いゾーンの照会に移る前に、A および AAAA の DNS レコードを照会します。 デフォルト設定の [オフ（Off）] を使用することを推奨します。つまり、Expressway は A レコードと AAAA レコードは照会せず、その代わりに検索を続行して残りのプライオリティが低いゾーンを検索します。これは、NAPTR レコードや SRV レコードとは異なり、A/AAAA レコードが関連する SIP メッセージまたは H.323 メッセージ（LRQ、Setup など）を処理できるシステムを示す保証がないためです。システムが、http メッセージを処理する Web サーバであったり、メール メッセージを処理するメール サーバであったりする可能性があります。システムが A/AAAA ルックアップをしている場合にこの設定が [オン（On）] になっていると、Expressway はその宛先にシグナリングを送信することになり、検索プロセスを続行しません。システムが SIP や H.323 をサポートしない場合、コールは失敗します。
ゾーン プロファイル（Zone profile）	ほとんどの導入環境について、この設定は [デフォルト（Default）] のままにする必要があります。

ステップ 5 [ゾーンの作成（Create zone）] をクリックします。

DNS ゾーンの検索ルールの設定

ローカル Expressway で DNS を使用し、ネットワーク外のエンドポイントを見つける場合は、次の手順を実行します。

- ENUM ダイヤリングと URI ダイヤリング用の DNS サーバの設定（DNS クエリに Expressway が使用するもの）
- DNS ゾーンを作成し、DNS クエリをトリガーするエイリアスを定義するために **[パターン文字列（Pattern string）]** フィールドと **[パターン タイプ（Pattern type）]** フィールドを使用する、関連付けられた検索ルールをセットアップする

たとえば、次のように設定します。

- **[パターン文字列（Pattern string）]** に .*@.*、**[パターンタイプ（Pattern type）]** に *[*正規表現（*Regex*）*]* を設定し、通常の URI アドレスの形式のすべてのエイリアスを DNS に照会する
- **[パターン文字列（Pattern string）]** に *(?!.*@example.com$).**、[パターンタイプ（Pattern type）] に *[*正規表現（*Regex*）*]* を設定し、ドメイン *example.com* 以外の通常の URI アドレスの形式のすべてのエイリアスを DNS に照会する

さらに詳細なフィルタをセットアップするには、同じDNSゾーンをターゲットとする検索ルールを追加して設定します。プロトコル（SIPまたはH.323）に基づいてフィルタリングしたり、異なるホップ カウントを使用したりしない限り、ルールごとに新しい DNS ゾーンを作成する必要はありません。

（注） DNS ゾーンに対して **[モード（Mode）]** を *[任意のエイリアス（Any alias）]* に設定した検索ルールは設定しないでください。このような検索ルールは、ローカルに登録されているものや、URI アドレスの形式でないものも含めてすべてのエイリアスについて DNS が常に照会されることになります。

着信コールでの DNS を介した URI ダイヤリング

DNS レコード タイプ

URI ダイヤリングを使用し、DNS を介して行われたコール（および登録などのその他のメッセージ）を受信するための Expressway の機能は、Expressway がホストしている各ドメインに DNS レコードがあるかないかに依存します。

これらのレコードには、次のようなさまざまなタイプがあります。

- Expressway の IPv4 アドレスを提供する A レコード
- Expressway の IPv6 アドレスを提供する AAAA レコード
- 特定のプロトコルやトランスポート タイプについて照会される Expressway の FQDN やそのポートを指定するサービス（SRV）レコード
- SIP ドメインの SRV レコードやトランスポートの設定を指定する NAPTR レコード

ホストしているドメインと、Expresswayで有効になっているプロトコルおよびトランスポートタイプの組み合わせごとにSRVレコードまたはNAPTRレコードを指定する必要があります。

着信コール プロセス

URIダイヤリングを使用し、DNSを介して着信コールが実行された場合、発信側のシステムは上述の DNS レコード ルックアップのいずれかを使用して Expressway を検出しています。Expressway は、ダイヤルされた user@example.com 形式の URI を含む要求を受信します。これは、デフォルト ゾーンから着信したように見えます。この場合、Expressway は通常のコール ルーティング プロセスに従って、検索前トランスフォーメーション、コールポリシーとFindMeポリシーを適用した後、ローカルゾーンとその他の設定済みのゾーンを検索ルールのプライオリティ順に検索して、URI を検索します。

SRV レコードの形式

SRV レコードの形式は RFC 2782 により、次のように定義されます。

_Service._Proto.Name TTL Class SRV Priority Weight Port Target

Expressway では、次のようになります。

- **_Service**と**_Proto**は異なり、使用するプロトコルとトランスポートタイプに依存します。
- **Name**は、Expressway がホストしている URI 内のドメイン（**example.com**）です。
- **Port**はその特定のサービスとプロトコルの組み合わせをリッスンするように設定された Expressway 上の IP ポートです。
- **Target**は、Expressway の FQDN です。

H.323 SRV レコードの設定

『ITU 仕様書：H.323』の「Annex O」に、DNS を使用してゲートキーパーとエンドポイントを見つけ、H.323 URL エイリアスを解決する手順が定義されています。また、H.323 URL で使用するパラメータも定義されています。

Expressway はこの付録で定義されている SRV レコードのロケーション、コール、および登録のサービス タイプをサポートします。

ロケーション サービスの SRV レコード

コールを Expressway にルーティングするゲートキーパーには、ロケーションレコードが必要です。Expressway がホストするドメインごとにロケーション サービスの SRV レコードを次のように設定する必要があります。

- **_Service** は **_h323ls**
- **_Proto** は **_udp**
- Port は、**[設定（Configuration）] > [プロトコル（Protocols）] > [H.323]** で**登録 UDP ポート**として設定したポート番号。

コール シグナリングの SRV レコード

コール シグナリングの SRV レコード（および A/AAAA レコード）は、LRQ と LCF を交換するロケーション トランザクションに参加できない未登録のエンドポイントによって主に使用されます。Expressway がホストするドメインごとにコール シグナリングの SRV レコードを次のように設定する必要があります。

- **_Service** は **_h323cs**
- **_Proto** は **_tcp**
- Port は、**[設定（Configuration）] > [プロトコル（Protocols）] > [H.323]** > でとして設定したポート番号。

登録サービスの SRV レコード

登録レコードは、Expressway の登録を試行するデバイスが使用します。Expressway がホストするドメインごとに登録サービスの SRV レコードを次のように設定する必要があります。

- **_Service** は **_h323rs**
- **_Proto** は **_udp**
- Port は、**[設定（Configuration）] > [プロトコル（Protocols）] > [H.323]** で**登録 UDP ポート**として設定したポート番号。

SIP SRV レコードの設定

RFC 3263 に、SIP URI を通信する次のホップの IP アドレス、ポート、トランスポート プロトコルに解決するために使用する DNS のプロシージャが示されています。

SIP URI ダイヤリングを使用して Expressway に接続できるようにするには、Expressway で有効になっている SIP トランスポート プロトコル（UDP、TCP、または TLS）ごとに SRV レコードを次のように設定する必要があります。

- **_Service**および**_Proto**の有効な組み合わせは次のとおりです。
  - **_sips._tcp**
  - **_sip._tcp**
  - **_sip._udp** （推奨されていません）
- Port はその特定のトランスポートプロトコル用のポートとして **[設定（Configuration）] > [プロトコル（Protocols）] > [SIP]** で設定した IP ポート番号

_sip._udp は、ビデオストリームの SIP メッセージが大きすぎて（ストリームベースでなく）パケットベースの転送では伝送できないため、推奨されません。UDP は、通常、オーディオ専用デバイスに使用されます。また、UDP は TCP や TLS よりもスパムが多発する傾向があります。

DNS レコードの設定例

ドメイン名を持つ企業は、**example.com**次の形式の URI アドレスを使用して H.323 および SIP の着信コールを有効にしたいと考えています。**user@example.com** ドメインをホストしている Expressway には、FQDN **expressway.example.com**があります。

通常、DNS レコードは次のようになります。

- **_h323ls._udp.example.com**リターンの SRV レコード**expressway.example.com**
- **_h323cs._tcp.example.com**リターンの SRV レコード**expressway.example.com**
- **_h323rs._tcp.example.com**リターンの SRV レコード**expressway.example.com**
- **example.com**リターンの NAPTR レコード
  - **_sip._tcp.example.com** および
  - **_sips._tcp.example.com**
- **_sip._tcp.example.com**リターンの SRV レコード**expressway.example.com**

- **_sips._tcp.example.com**リターンの SRV レコード**expressway.example.com**
- Expressway の IPv4 アドレスを返す**expressway.example.com**レコード。
- Expressway の IPv6 アドレスを返す**expressway.example.com** AAAA レコード。

DNS レコードの追加方法は、使用している DNS サーバのタイプによって異なります。2 つの共通DNSサーバをセットアップする手順については、「DNS設定」の項を参照してください。

URI ダイヤリングを使用してローカルに登録された H.323 エンドポイントに到達するには、次のいずれかを実行します。

- URI 形式のアドレスを使用して H.323 エンドポイントを Expressway に登録する
- H.323 の登録で使用される形式に URI を変換するために適切なトランスフォーメーションを作成する。たとえば、H.323 エンドポイントをエイリアスを使用して登録し、alias@domain.com に対して着信コールを実行するという導入方法があります。この場合はローカル トランスフォーメーションを設定して @domain を除去し、ローカルで alias を検索します。これを実行する方法の例については、H.323 番号へのダイヤリングでの @domain の除去を参照してください。

SIP エンドポイントは常に URI 形式の AOR で登録されるため、特別な設定は不要です。

Expressway を見つけるために複数のメカニズムが使用されていた可能性があります。**user@<IP_address>**に発信されたコールを**user@example.com**の既存の登録にルーティングできるようにすることができます。この場合は、検索前トランスフォーメーションについてを設定して着信 URI からサフィックスの IP_address を除去して**example.com**のサフィックスで置き換えます。

URI ダイヤリングとファイアウォール トラバーサル

DNS を介した URI ダイヤリングをファイアウォール トラバーサルと一緒に使用する場合、DNS ゾーンを Expressway-E とパブリック ネットワークの Expressway のみに設定する必要があります。ファイアウォールの背後にある Expressway には DNS ゾーンを設定しないでください。これにより、Expressway に登録されているエンドポイントからの発信 URI コールが Expressway-E を通じてルーティングされるようになります。

さらに、着信コールの DNS レコードは、その企業の権限のあるプロキシとして Expressway-E のアドレスを使用して設定する必要があります（詳細については、「DNS設定例」の項を参照してください）。これにより、URI ダイヤリングを使用して処理された着信コールが Expressway-E を通じて企業内に入るため、ファイアウォールのトラバーサルが成功するようになります。

ENUM ダイヤリングについて

ENUM ダイヤリングでは、そのエンドポイントが異なる形式のエイリアスを使用して登録されていても、E.164 番号（電話番号）にダイヤリングした発信者がエンドポイントに接続できます。

ENUM ダイヤリングを使用し、E.164 番号をダイヤルすると、DNS に保存された情報を使用して URI に変換されます。次に Expressway が返された URI に基づいてエンドポイントを検索しようとします。

ENUM ダイヤリング機能を使用すると、URI ダイヤリングの柔軟性は保ちながら、コールするために使用するのは番号だけというシンプルさが得られます。これは、発信者がテンキーを使用してのダイヤリングに限られている場合は特に重要です。

Expressway 上の ENUM ゾーンを設定できるため、Expressway は発信 ENUM ダイヤリングをサポートします。ENUM ゾーンを照会することによって、ENUM ドメインにダイヤルされ、その後で DNS を使用して照会される E.164 番号の Expressway による変換がトリガーされます。

（注） ENUM ダイヤリングは照会される ENUM ドメインの関連する DNS NAPTR レコードの有無に依存します。これは、そのドメインの管理者が担当します。

ENUM ダイヤリング プロセス

Expressway が ENUM を使用してエンドポイントを見つけようとする場合の一般的なプロセスは次のようになります。

1. ユーザがエンドポイントから E.164 番号をダイヤルします。
2. Expressway が E.164 番号を ENUM ドメインに次のように変換します。
    1. 数字を反転し、ドットで区切ります。
    2. E.164 番号の NAPTR レコードをホストするドメインの名前がサフィックスとして追加されます。
3. 次に、結果の ENUM ドメインを DNS に照会します。
4. その ENUM ドメインの NAPTR レコードがある場合は、1 つ（場合によっては複数）の H.323/SIP URI への番号の変換方法が示されます。
5. Expressway が再度検索を開始しますが、ここでは、変換した URI を 発信コールでの DNS を介した URI ダイヤリングに従って検索します。

（注） これは、まったく新しい検索と見なすことができるため、検索前トランスフォーメーションとコール ポリシーが適用されます。

ENUM ダイヤルの有効化

ENUM ダイヤリングは着信コールと発信コールに別々に有効にできます。

発信コール

ENUM を使用するエンドポイントへの発信コールを可能にするには、次の手順を実行する必要があります。

- 少なくとも 1 つの ENUM ゾーンを設定する、および
- 少なくとも 1 つの DNS サーバを設定します。

この詳細については、発信コールの ENUM ダイヤリングのセクションを参照してください。

着信コール

企業内のエンドポイントが ENUM ダイヤリングを介して他のエンドポイントからの着信コールを受信できるようにするには、エンドポイントの E.164 番号を SIP/H.323 URI にマッピングする DNS NAPTR レコードを設定する必要があります。これを実行する方法については、着信コールの ENUM ダイヤリングセクションを参照してください。

（注） ENUM ゾーンと DNS サーバがローカル Expressway 上に設定されていない場合も、ローカル Expressway が ENUM ダイヤリングに適切に設定された別の Expressway と隣接していれば、ENUM ダイヤリングを使用して発信されたコールは処理されます。ENUM ダイヤリングされたコールはネイバーを経由します。この設定は、自社からのすべての ENUM ダイヤリングを特定の 1 つのシステム上に設定する場合に便利です。

発信コールの ENUM ダイヤリング

ローカル エンドポイントを ENUM を使用して別のエンドポイントに Expressway を介してダイヤルできるようにするには、次の条件を満たす必要があります。

- 着信側のエンドポイントの E.164 番号を URI にマッピングするために使用できる NAPTR レコードが NDS に存在する必要があります。このレコードを提供する役割は着信側のエンドポイントが属する企業の管理者が担い、企業内のエンドポイントを ENUM ダイヤリングを介して接続可能にする場合にのみ、そのレコードを使用可能にします。

- ローカル Expressway 上に ENUM ダイヤリングのゾーンと検索ルールの設定する必要があります。この ENUM ゾーンには、着信側のエンドポイントの NAPTR レコードを保持しているドメインと同じ DNS サフィックスが必要です。
- NAPTR レコード（および、必要な場合は結果の URI）を照会できる、少なくとも 1 つ以上の ENUM ダイヤリングと URI ダイヤリング用の DNS サーバの設定のアドレスを使用してローカル Expressway を設定する必要があります。

ENUM プロセスが 1 つまたは複数の URI が返された後、発信コールでの DNS を介した URI ダイヤリングに従って、これらの URI のそれぞれについての新しい検索が開始されます。URI がローカルに登録されたエンドポイントに属している場合は、それ以上の設定は不要です。ただし、少なくとも 1 つの URI がローカルに登録されていない場合、DNS ルックアップを使用してそれらの URI を検索するのであれば、DNS ゾーンを設定する必要もあります。

コール処理

Expressway はこのプロセスに従って ENUM（E.164）番号を検索します。

1. Expressway は、ダイヤルされたとおりに受信した E.164 番号の検索を開始します。これは通常のコール ルーティング プロセスに従います。
2. 検索前トランスフォーメーションを適用した後、Expressway は検索ルールの設定をチェックして、それらのルールのいずれかが、次のいずれかの**モード**で設定されていることを確認します。
   - *[任意のエイリアス（Any alias）]* または
   - E.164 番号に一致するパターンによる *[エイリアス パターン マッチ（Alias pattern match）]*
3. 一致する検索ルールに関連付けられたターゲット ゾーンがルールのプライオリティ順に照会されます。
   - ターゲット ゾーンがネイバー ゾーンである場合、ネイバーで E.164 番号が照会されます。ネイバーが ENUM ダイヤリングをサポートする場合、コール自体をルーティングできます。
   - ターゲット ゾーンが ENUM ゾーンである場合、Expressway は ENUM を通じてエンドポイントを検出しようとします。Expressway に設定されている 各 ENUM ゾーンを照会する限り、E.164 番号が次のように ENUM ドメインに変換されます。
     1. 数字を反転し、ドットで区切ります。
     2. ENUM ゾーンに設定された **DNS サフィックス**が追加されます。
4. 次に、結果の ENUM ドメインを DNS に照会します。
5. DNS サーバがその ENUM ドメインで変換後の E.164 番号（反転され、ドットで区切られた後の番号）に一致する NAPTR レコードを検出した場合、関連付けられた URI を Expressway に返します。

6. その後、Expressway はその URI の新しい検索を開始します（既存のホップ カウントは維持されます）。検索プロセス（検索前トランスフォーメーションを適用してからローカルゾーンと外部ゾーンをプライオリティ順に検索）の開始時に Expressway が起動します。SIP/H.323 URI を検索しているこの時点から、URI ダイヤリングについてのプロセスに進みます。

この例では Example Corp の Fred をコールします。Fred のエンドポイントは実際には URI の **fred@example.com** を使用して登録されていますが、もっと簡単に Fred と接続するために、Fred のシステム管理者がこのエイリアスを Fred の E.164 番号である **+44123456789** にマッピングする DNS NAPTR レコードを設定しました。

example.comの NAPTR レコードが**e164.arpa**の DNS ドメインを使用することを分かっています。

1. ローカル Expressway に、**e164.arpa**の**DNS サフィックス**を使用して 、2 つのゾーンに 1 つの 2 つのゾーンを作成します。
2. **[パターン マッチ モード（Pattern match mode）]** を *[任意のエイリアス（Any alias）]* に、また、**[ターゲット（Target）]** を ENUM ゾーンに設定した検索ルールを設定します。つまり、検索されるエイリアスの形式に関係なく、常に ENUM が照会されます。
3. エンドポイントから **44123456789** をダイヤルします。
4. Expressway が **44123456789** の登録の検索を開始します。また、*[任意のエイリアス（Any alias）]* の検索ルールは ENUM ゾーンを照会することを意味します。

（注） 最初に他のプライオリティの高い検索が番号に一致する可能性があります。

5. 照会するゾーンが ENUM ゾーンであるため、Expressway が自動的にトリガーされ、番号を次のように ENUM ドメインに変換します。
   1. 数字を反転し、ドットで区切って **9.8.7.6.5.4.3.2.1.4.4** にします。
   2. ENUM ゾーン**e164.arpa**に設定された **DNS サフィックス**が追加されます。この結果、**9.8.7.6.5.4.3.2.1.4.4.e164.arpa**のドメインが変換されます。
6. 次に DNS で ENUM ドメインを照会します。
7. DNS サーバがドメインを検出し、関連付けられた NAPTR レコードの情報を返します。これは、ダイヤルした E.164 番号が**fred@example.com**の SIPURI にマップされていることを Expressway に通知します。
8. Expressway はその後、**fred@example.com**のこの時間に関する別の検索を開始します 。この時点から URI ダイヤリング プロセスに進み、コールは Fred のエンドポイントに転送されます。

ENUM ダイヤリングのゾーンと検索ルールの設定

ENUM ダイヤリングをサポートするには、リモート エンドポイントで使用する各 ENUM サービス用の ENUM ゾーンと関連する検索ルールを設定する必要があります。

ENUM ゾーンの追加と設定

（注）

- ENUM ゾーンは Expressway 上にいくつでも設定できます。エンドポイントが使用する各 DNS サフィックスに少なくとも 1 つの ENUM ゾーンを設定する必要があります。
- 通常の検索ルールのパターンマッチングと優先順位付けのルールが ENUM ゾーンに適用されます。
- また、NAPTR レコードの検索時に使用する ENUM ダイヤリングと URI ダイヤリング用の DNS サーバの設定必要もあります。

ENUM ゾーンをセットアップするには、次の手順を実行します。

手順

ステップ 1 **[設定（Configuration）] > [ゾーン（Zones）] > [ゾーン（Zones）]** へ移動します。

ステップ 2 [新規（New）] をクリックします。**[ゾーンの作成（Create zone）]** ページが表示されます。

ステップ 3 ゾーンの**名前**を入力し、**[タイプ（Type）]** として *[ENUM]* を選択します。

ステップ 4 ENUM ゾーンを次のように設定します。

フィールド	ガイドライン
ホップ カウント（Hop count）	ほかのゾーン タイプのホップ カウントと同じ方法で、ENUM ゾーンに指定したホップ カウントの設定を適用します。DNS ルックアップで戻されたエイリアスの新しい検索プロセスを Expressway が開始した時点で現在適用可能なホップ カウントが維持されます。
DNS サフィックス（DNS suffix）	ENUM のホスト名を作成するための変換後の E.164 番号に追加するサフィックス。これは NAPTR レコードを照会する（ドメイン ネームスペース内の）DNS ゾーンを表します。
H.323 モード（H.323 Mode）	このゾーンを H.323 レコードでルックアップするかどうかを制御します。
SIP モード（SIP mode）	このゾーンを SIP レコードでルックアップするかどうかを制御します。

ステップ 5 [ゾーンの作成（Create zone）] をクリックします。

ENUM ゾーンの検索ルールの設定

ローカルに登録されたエンドポイントが Expressway を介して ENUM コールをできるようにするには、少なくとも次の情報を使用して ENUM ゾーンと関連する検索ルールを設定する必要があります。

- **e164.arpa** の **DNS サフィックス**（この 2 つのドメインは、この 2 つのドメインの 1 つで指定されます)。
- **[モード（Mode）]** が *[任意のエイリアス（Any alias）]* に設定された関連する検索ルール。

これにより、ENUM だけでなく、常にすべてのタイプのエイリアスが DNS で照会されることになります。また、ダイヤルされる企業が **e164.arpa** ドメインを使用している場合にのみ、ENUM ダイヤリングが成功することも意味します。ENUM ダイヤリングが確実に成功するようにするには、企業内の発信者がダイヤルするエンドポイントの NAPTR レコードを保持しているドメインごとに ENUM ゾーンを設定する必要があります。

各 ENUM に送信するクエリをフィルタリングする検索ルールを次のように設定します。

- **[モード（Mode）]** に *[エイリアス パターン マッチ（Alias pattern match）]* を使用する
- **[パターン文字列（Pattern string）]** フィールドと **[パターン タイプ（Pattern type）]** フィールドを使用して ENUM ルックアップをトリガーするドメインごとにエイリアスを定義する

たとえば、自社のネットワークからエンドポイントの E.164 番号が **44** で始まる英国内のリモートオフィスへの ENUM ダイヤリングを有効にすることができます。これを行うには、Expressway 上に ENUM ゾーンと、それに関連付ける検索ルールを次のように設定します。

- **[モード（Mode）]** を *[エイリアス パターン マッチ（Alias pattern match）]* に設定する
- **[パターン文字列（Pattern string）]44**
- **[パターン タイプ（Pattern type）]** を *[プレフィックス（Prefix）]* に設定する

これにより、**44** で始まる番号を誰かがダイヤルした場合にのみ、ENUM クエリがそのゾーンに送信されるようになります。

ENUM ゾーンのトランスフォーメーションの設定

他のゾーンと同じ方法で、ENUM ゾーン用のトランスフォーメーションを設定できます（詳細については、検索とゾーン変換プロセスの項を参照してください）。

ENUM ゾーンのトランスフォーメーションは、番号が ENUM ドメインに変換される前に適用されます。

たとえば、自社のネットワークからプレフィックスに 8 と、その後にリモートのエンドポイントの E.164 番号の最後の 4 桁を使用してリモート サイトのエンドポイントへの ENUM ダイヤ

リングを有効にすることができます。これを行うには、Expressway 上に ENUM ゾーンと、それに関連付ける検索ルールを次のように設定します。

- **[モード（Mode）]** を *[エイリアス パターン マッチ（Alias pattern match）]* に設定する
- **[パターン文字列（Pattern string）]8(\d{4})**
- **[パターン タイプ（Pattern type）]** を *[正規表現（Regex）]* にする
- **[パターン動作（Pattern behavior）]** を *[置換（Replace）]* にする
- **[置換文字列（Replace string）]44123123(\1)**

この設定により、ENUM ドメインに変換され、DNS を介して照会された文字列は（**44123123xxxx**）になります。

発信 ENUM ダイヤリングを正しく設定したことを確認するには、エイリアスの検出（**[メンテナンス（Maintenance）]** > **[ツール（Tools）]** > **[検索（Locate）]**）を使用して E.164 エイリアスの解決を試行します。

着信コールの ENUM ダイヤリング

ENUM ダイヤリングを使用してローカルに登録したエンドポイントに到達するようにするには、エンドポイントの E.164 番号を UIR にマッピングする DNS NAPTR レコードを設定する必要があります。このレコードは、ENUM ダイヤリングを使用して到達しようとしているシステムが検出できる、適切な DNS ドメインに配置する必要があります。

ENUM の DNS ドメインについて

ENUM が E.164 番号と URI との間でマッピングを行うには、NAPTR レコードの有無に依存します。

RFC 3761 は、ENUM の標準規格を定義する一連のドキュメントの一部であり、NAPTR レコードが公共の ENUM 導入環境用として検出されるべき ENUM ドメインは**e164.arpa** であると明示しています。ただし、このドメインを使用するには、適切な国の規制機関によって E.164 番号が割り当てられている必要があります。すべての国が ENUM に参加しているわけではないため、NAPTR レコードに代替ドメインを使用することができます。このドメインは会社のネットワーク内に存在するか（ENUM を社内で使用する場合）、または http://www.e164.org などの公共の ENUM データベースを使用することも可能です。

DNS NAPTR レコードの設定

ENUM は RFC 2915 に定義されているように、NAPTR レコードの有無に依存します。これらのレコードを使用して、E.164 番号から H.323 や SIP URI が取得されます。

Expressway がサポートするレコード形式は次のとおりです。

order preference flag service regex replacement

値は次のとおりです。

- **order** および**preference** を選択して、NAPTR レコードが処理される順序を決定します。最下位のレコードが最初に処理され、照合順の場合は最下位の優先度を持つレコードが最初に処理されます。
- **flag** によってこのレコード内の他のフィールドの解釈が決まります。値 **u**（これが終端ルールであることを示す）のみが現在サポートされており、必須となっています。
- **service** はこのレコードが E.164 から H.323 または SIP の URI 変換を記述するためのものであることを示します。その値は、**E2U+h323 or E2U+SIP** のいずれかである必要があります。
- **regex** は指定された E.164 番号から H.323 または SIP URI への変換を記述する正規表現です。
- **replacement** は、Expressway で現在使用されていないので、**.**（句点）に設定する必要があります。

ENUM の非終端ルールは現在 Expressway ではサポートされていません。これらの詳細については、『RFC 3761』の 2.4.1 項を参照してください。

たとえば、次のレコードがあります。

IN NAPTR 10 100 "u" "E2U+h323" "!^(.*)$!h323:\1@example.com!"を使用して無効にすることができます。

この例は次のように解釈されます。

- **10** は **order**
- **100** は **preference**
- **u** は **flag**
- **E2U+h323** はこのレコードが H.323 URI 用であるとしています。
- **!^(.*)$!h323:\1@example.com!** は変換について説明します。
  - **!** はフィールド区切り文字
  - 最初のフィールドが変換する文字列であることを表します。この例では、**^(.*)$** は E.164 番号全体を表します。
  - 2 番目のフィールドは生成される H.323 URI を表します。この例では 、**h323:\1@example.com** が E.164番号が**@example.com** と連結されることを示しています。たとえば 、**1234** は**1234@example.com** にマッピングされます。
- 置換フィールドが使用されていないことを示します。

ENUM ダイヤリングと URI ダイヤリング用の DNS サーバの設定

DNS サーバは次のように ENUM ダイヤリングと URI ダイヤリングをサポートする必要があります。

- **ENUM ダイヤリング**：E.164 番号を URI にマッピングする NAPTR レコードを照会する
- **URI ダイヤリング**：ローカルに登録されていないか、またはネイバー システムを介してアクセスできないエンドポイントをルックアップする

DNS サーバ（DNS クエリに Expressway が使用するもの）を設定するには、次の手順を実行します。

手順

ステップ 1 **[DNS]** ページ（**[システム（System）]** > **[DNS]**）に移動します。

ステップ 2 **[アドレス 1（Address 1）]** フィールドから **[アドレス 5（Address 5）]** フィールドに、ドメインの検出を試行する際に Expressway を照会する最大 5 台の DNS サーバの IP アドレスを入力します。これらのフィールドには FQDN ではなく、IP アドレスを使用する必要があります。

コール ルーティングとシグナリングの設定

「コールルーティング（Call routing）」ページ（**[設定（Configuration）]** > **[コールルーティング（Call routing）]**）を使用して、Expressway のコールルーティングとシグナリングの機能を設定します。

コール シグナリングの最適化

コールは、シグナリングとメディアの2つのコンポーネントから構成されています。トラバーサル コールの場合、Expressway は常にメディアとシグナリングの両方を処理します。非トラバーサル コール場合は、Expressway はメディアを処理しません。またシグナリングの処理は必要な場合も不要な場合もあります。

[コール シグナリングの最適化（Call signaling optimization）] の設定では、コールがセットアップされた後にコール シグナリング パスから Expressway がそれ自体を（可能な場合は）削除するかどうかを指定します。この設定のオプションは次のとおりです。

- *[オフ（Off）]*：Expressway は常にコールシグナリングを処理します。

- コールは RMS コールライセンス、または Expressway 上の登録済みコールライセンスのいずれかを消費します。

- *[オン（On）]*：Expressway はコールが次のいずれかである場合にコールシグナリングを処理します。
  - トラバーサルコール
  - コールポリシーまたは FindMe によって次のように変更された H.323 コール
    - コールが複数のエイリアスに解決される
    - コールの送信元エイリアスが関連付けられた FindMe ID を表示するように変更された
    - FindMe に「応答なし」または「ビジー」のデバイスが設定されていない
  - コール内のいずれかのエンドポイントがローカルに登録されている
  - 着信トランスポート プロトコル（UDP、TCP、TLS）が発信プロトコルと異なっている場合の SIP コール

    その他の場合はすべて、Expressway はコールがセットアップされた後にコール シグナリング パスからそれ自体を削除します。Expressway はそのようなコールについてはコール ライセンスを消費しません。また、コール シグナリング パスが簡略化されます。この設定は、ディレクトリ Expressway で使用する場合の階層型ダイヤル プランに役立ちます。そのような導入環境では、ディレクトリ Expressway を使用してエンドポイントをルックアップして検出します。また、どのエンドポイントもその Expressway に登録させません。

コール ループ検出モード

ダイヤル プランまたは隣接するネットワークのダイヤル プランは、シグナリング ループが発生することを想定して設定できます。この例は構造化ダイヤルプランであり、すべてのシステムがメッシュ内にまとめて隣接化されています。このような設定では、ホップカウントの設定の設定が大きすぎると、ホップ カウントが 0 に到達するまで単一の検索要求がネットワークに繰り返し送信されることがあり、リソースを不必要に消費します。

Expressway はネットワーク内のループを検出し、そのような検索を **[コール ループ検出モード（Call loop detection mode）]** の設定で終了させて、ネットワーク リソースを節約することができます。この設定のオプションは次のとおりです。

- *[オン（On）]*：Expressway はループを含んでいる検索のブランチを実行せず、レベル 2 の「「ループを検出（loop detected）」」イベントとして記録します。次の条件のすべてを満たしている場合、2 つの検索がループしていると見なされます。
  - 同じコールタグがある
  - 同じ宛先エイリアス宛である

- 同じプロトコルを使用している
- 同じゾーンから発信されている

- *[オフ（Off）]*：Expresswayは検索ループを検出せず、検索ループは失敗します。この設定は高度な導入にのみ使用することを推奨します。

コールの識別

Expressway を通過する各コールにはコール ID とコール シリアル番号が割り当てられます。また、まだ行われていない場合には、コール タグも割り当てられます。

コール ID

Expressway は現在進行中の各コールに異なるコール ID を割り当てます。コール ID 番号は 1 から始まり、そのシステムで許可されるコールの最大数までになります。

コールが発信されるたびに、Expressway はそのコールに使用可能な最も小さいコール ID 番号を割り当てます。たとえば、すでにコール ID が 1 の進行中のコールがある場合、次のコールにはコール ID 2 が割り当てられます。コール 1 が切断されると、発信される 3 番目のコールにはコール ID 1 が割り当てられます。

したがって、コール ID は一意の識別子ではありません。同時に進行中の 2 つのコールが同じコール ID を持つことはありませんが、時間の経過とともに、同じコール ID が複数のコールに割り当てられます。

（注） Expressway の Web インターフェイスにはコール ID は表示されません。

コール シリアル番号

Expressway は、通過するすべてのコールに一意のコール シリアル番号を割り当てます。Expressway 上の 2 つのコールが同じコール シリアル番号を持つことはありません。複数の Expressway 間を通過する単一のコールは、システムごとに異なるコール シリアル番号によって識別されます。

コール タグ

コール タグは、多くの Expressway を通過するコールの追跡に使用されます。Expressway がコールを受信すると、そのコールにコール タグがすでに割り当てられているかどうかを確認します。割り当てられている場合は Expressway は既存のタグを使用します。割り当てられていない場合はそのコールに新しいコール タグを割り当てます。このコール タグは、コールが転送されるときにそのコールの詳細情報に組み込まれます。複数の Expressway 間を通過する単一のコールには、（すでの通過したものも含め）Expressway に着信するたびに異なるコール シリアル番号が割り当てられますが、コール タグを使用することで同じコールであると識別でき

ます。これは、ロギングの設定を使用してネットワーク内の多くの Expressway のイベントを照合している場合に特に役に立ちます。

また、コール タグは、ネットワーク内のループの識別にも役立ちます。自動コール ルーティングとシグナリングの設定の一部として使用されているため、単一のコール タグに関連するすべてのイベントをイベント ログで検索することができます。クエリをネイバー ゾーンに送信し、元の Expressway に再度ルーティングされる前に 1 つ以上のシステムを通過する場合にループが発生します。この場合、発信クエリと着信クエリは異なるコール シリアル番号を持ち、さらに、（トランスフォーメーションが割り当てられたかどうかに応じて）異なる宛先エイリアス宛となる場合があります。ただし、この場合もそのコールのコール タグは同じです。

（注） Expressway または TelePresence Conductor ではないシステムをコールが通過する場合は、コールタグの情報は失われます。

CLI でのコールの識別

CLI を使用してコールを制御するには、コール ID かコール シリアル番号のいずれかを使用してコールを参照する必要があります。これらは、次のコマンドを使用して取得できます。

xStatus Calls

このコマンドは、現在進行中の各コールの詳細情報をコール ID 順に返します。各エントリの 2 番目の行にはコール シリアル番号が表示され、3 番目の行にはコール タグが表示されます。

コールの切断

Web インターフェイスを使用したコールの切断

（注） Expressway がクラスタの一部である場合は、コールが関連付けられているピアにログインし、コールを切断できるようにする必要があります。

Web インターフェイスを使用して既存の 1 つ以上のコールを切断するには、次の手順を実行します。

手順

ステップ 1 「コール（Calls）」ページ（**[ステータス（Status）]** > **[コール（Calls）]**）に移動します。

ステップ 2 コール シリアル番号やコール タグなどのコールの詳細情報を確認するには、[表示（View）] をクリックします。ブラウザの [戻る（back）] ボタンをクリックして「**コール（Calls）**」ページに戻ります。

ステップ 3 終了するコールの横にあるボックスをオンにし、[切断（Disconnect）] をクリックします。

CLI を使用したコールの切断

CLI を使用して既存のコールを終了するには、まずコール ID 番号か、またはコールのシリアル番号を取得する必要があります（コールの識別を参照してください）。次に、必要に応じて次のコマンドのいずれかを使用します。

- **xCommand DisconnectCall Call: <ID number>**
- **xCommand DisconnectCall CallSerialNumber: <serial number>**

切断するコールの参照にコール ID 番号を使用するほうが簡単ですが、その間にそのコールが切断され、コール ID が新しいコールに割り当てられているというリスクがあります。そのため、Expressway では、より長くても一意のコール シリアル番号を使用してコールを照会することもできます。

（注） コールを切断すると、そのコール シリアル番号のコールのみが切断されます。コール タグが同じでコール シリアル番号が異なる他のコールは影響されない場合があります。

SIP コールの切断時の制限

コールの切断は、プロトコルの動作の違いにより、H.323 コールと SIP コールでは異なる方法で動作します。

H.323 コールでインターワーキングしているコールでは、**Disconnect**コマンドでコールが実際に切断されます。

SIP コールでは、**Disconnect**コマンドによって Expressway はそのコールに使用したすべてのリソースを解放します。これで、コールはExpressway 上で切断されたように見えます。ただし、この時点でも、エンドポイントはコール中であると見なします。SIP コールはピアツーピアであり、Expresswayは SIP プロキシであるため、エンドポイントに権限がありません。Expressway 上のリソースを解放すると、次にエンドポイントから Expressway へのシグナリングが発生した場合は、Expressway は「「481 コール/トランザクションは存在しません（481 Call/Transaction Does Not Exist）」」と応答してエンドポイントがコールをクリアします。

（注） SIP セッション タイマーをサポートするエンドポイント（RFC 4028 を参照）にはコールリフレッシュタイマーがあり、切断されたコール（エンドポイント間でのシグナリングの消失）を検出することができます。エンドポイントは、次のセッションタイマーメッセージの交換後にリソースを解放します。

第 18 章

帯域幅制御

ここでは、ローカルゾーン内のコールとほかのゾーンへのコールに使用する帯域幅の制御方法について説明します（**[設定（Configuration）] > [ローカルゾーン（Local Zone）]** と **[設定（Configuration）] > [帯域幅（Bandwidth）]**）。

帯域幅制御について

Expressway では、ネットワーク上のエンドポイントが使用する帯域幅の量を制御できます。それには、エンドポイントをサブゾーンにグループ化し、リンクの設定とパイプの設定を使用して、次で使用できる帯域幅の制限を適用します。

- 各サブゾーン内
- サブゾーンと別のサブゾーン間
- サブゾーンとゾーン間

帯域幅の制限は、コール単位や総同時使用量ベースで設定できます。この柔軟性によって、ネットワーク内の個々のコンポーネントの帯域幅制御を適切に設定することができます。

リンクが正しく設定されていないと、コールは失敗します。コールが成功するかどうか、およびどのような帯域幅がそのコールに割り当てられるかについては、コマンドの**xCommand CheckBandwidth**を使用して確認できます。

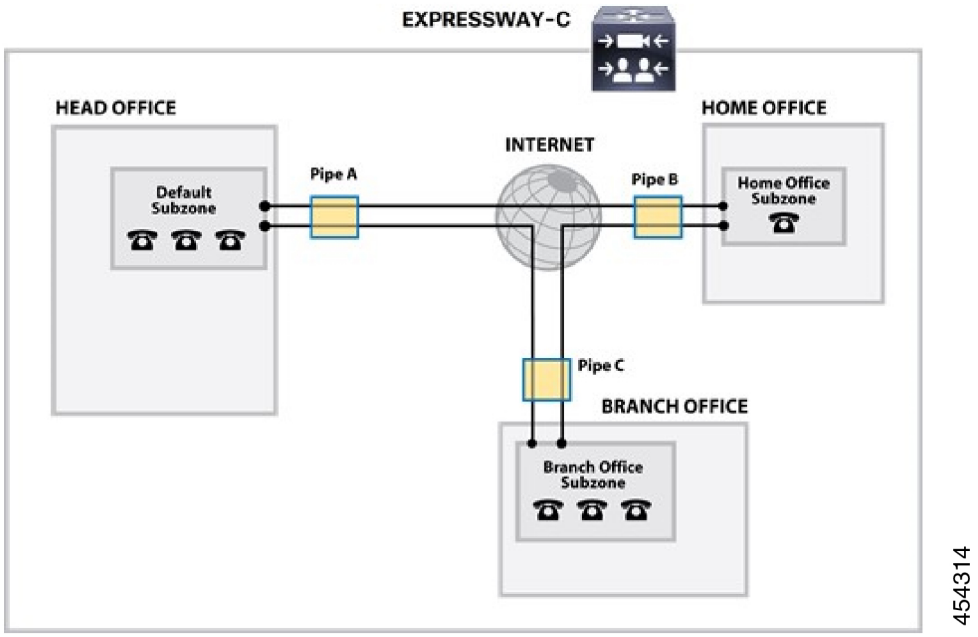
クラスタ内のピア間での帯域幅の管理方法に関する特定の情報については、ピア間での帯域幅の共有を参照してください。

ネットワークの配置例

次の図に、通常のネットワークの配置例を示します。

- 高帯域幅コールが許可される場合の企業とインターネット間のブロードバンド LAN
- インターネットへの帯域幅が制限されたパイプ（パイプ A）
- それぞれが独自のインターネット接続と制限付きのパイプを持つ2つのサテライトオフィスである支社とホーム。

この例では、エンドポイントの各プールには異なるサブゾーンが割り当てられています。そのため、各サブゾーン内およびサブゾーン間で使用される帯域幅には、インターネット接続を介して使用可能な帯域幅の量に基づいて適切な制限を適用することができます。



帯域幅制御の設定

[帯域幅の設定（Bandwidth configuration）] ページ（**[設定（Configuration）]** > **[帯域幅（Bandwidth）]** > **[設定（Configuration）]**）を使用して、帯域幅の指定がないコールを受信した場合と、現在使用可能な帯域幅以上を要求するコールを受信した場合の Expressway の動作を指定します。

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
デフォルトのコール帯域幅（kbps）（Default call bandwidth (kbps)）	帯域幅の値がコールを発信したシステムによって指定されていないコールに使用する帯域幅。 また、H.323インターワーキング コールにSIPで使用する最小帯域幅も定義します。 この値は空にできません。デフォルト値は384 kbps です。	通常、コールが発信されると、エンドポイントはそのコールが使用する帯域幅の量を要求に組み込みます。
コール モード単位のダウンスピード（Downspeed per call mode）	サブゾーンまたはパイプでの**コール単位**の帯域幅の制限が要求されたレートでコールを発信するために使用できる帯域幅が不足していることが示された場合にどのように動作するかを決定します。 *[オン（On）]*：コールはダウンスピードされます。 *[オフ（Off）]*：コールは発信されません。	
Downspeed トータル モード（Downspeed total mode）	サブゾーンまたはパイプでの**総**帯域幅の制限が要求されたレートでコールを発信するために使用できる帯域幅が不足していることが示された場合にどのように動作するかを決定します。 *[オン（On）]*：コールはダウンスピードされます。 *[オフ（Off）]*：コールは発信されません。	

ダウンスピード機能について

帯域幅制御を使用している場合、要求されたレートでコールを発信するために使用できる帯域幅が不足している場合があります。デフォルトでは（および一部の帯域幅がまだ使用できることを想定すると）、Expresswayは帯域幅を縮小してコールの接続を試行します。これを**ダウンスピード**と呼びます。

ダウンスピードは、次のシナリオのいずれか、または両方に適用できるように設定できます。

- コールが要求する帯域幅がサブゾーンまたはパイプのコール単位の最低限度を超過している。
- 要求された帯域幅でコールを発信すると、そのサブゾーンまたはパイプの総帯域幅の制限を超過する。

ダウンスピードはオフにできます。オフにすると、元々要求されたレートでコールを発信するには帯域幅が不足している場合、コールはまったく発信されません。ネットワークのキャパシ

ティに近づいている場合に、要求よりも遅い速度で接続するよりも、コールの接続を全面的に失敗させるためにこれを使用することができます。このような場合、エンドポイントユーザは検索を開始したシステムに応じて、次のメッセージのいずれかを受け取ります。

- 「コール キャパシティを超過している」
- 「ゲートキーパーにリソースが使用できない」

サブゾーンについて

ローカルゾーンはサブゾーンから構成されています。サブゾーンを使用してネットワークのさまざまな部分で使用される帯域幅を制御し、Expresswayの登録、認証、およびメディア暗号化のポリシーを制御します。

エンドポイントがExpresswayに登録されると、エンドポイントのIPアドレス範囲またはエイリアス パターン マッチに基づき、サブゾーン メンバーシップ ルールの設定によって決定された適切なサブゾーンに割り当てられます。

サブゾーンは、サブゾーンの設定ページ（**[設定（Configuration）]** > **[ローカル ゾーン（Local Zone）]** > **[サブゾーン（Subzones）]**）で作成し、設定できます。

Expresswayは、次の削除できない特別なサブゾーンを自動的に作成します。

- デフォルトサブゾーン
- トラバーサルサブゾーン
- クラスタサブゾーン（Expresswayがクラスタ内にある場合のみ適用されます）

サブゾーン間のデフォルト リンク

Expresswayは、デフォルト サブゾーンとトラバーサル サブゾーン（およびデフォルト ゾーン）が作成され、それらの間にリンクが設定されて出荷されます。Expresswayをクラスタに追加した場合、クラスタ サブゾーンへのデフォルトのリンクも自動的に確立されます。これらのデフォルトリンクは、ネットワークの制限のモデル化が必要な場合に、削除したり、修正したりできます。

トラバーサル サブゾーンについて

トラバーサル サブゾーンは概念的なサブゾーンです。トラバーサル サブゾーンにはエンドポイントを登録できません。このゾーンはトラバーサル コールが使用する帯域幅を制御する目的のみに使用します。

「トラバーサルサブゾーン（Traversal Subzone）」ページ（**[設定（Configuration）]** > **[ローカル ゾーン（Local Zone）]** > **[トラバーサルサブゾーン（Traversal Subzone）]**）では、トラバーサルサブゾーンで処理するコールに帯域幅の制限を適用したり、トラバーサルコールのメディアに使用するポートの範囲を設定したりできます。

帯域幅の制限の設定

すべてのトラバーサル コールがトラバーサル サブゾーンを通過します。そのため、トラバーサル サブゾーンに帯域幅の制限を適用することで、常時 Expressway によって実行されるメディアの処理量を制御できます。これらの制限は、同時総使用量ベースとコール単位ベースで適用できます。

詳細については、サブゾーンへの帯域幅の制限の適用を参照してください。

トラバーサル サブゾーン ポートの設定

[設定（Configuration）]>[ローカルゾーン（Local Zone）]>[トラバーサルサブゾーン（Traversal Subzone）]）で、トラバーサルコール内のメディアに使用するポートの範囲を設定できます。

使用可能な範囲

1024 ～ 65533 の範囲内であればメディア ポートの範囲をどこにでも定義できます[トラバーサル メディア ポートの開始（Traversal media port start）] は偶数、[トラバーサル メディア ポートの終了（Traversal media port end）] は奇数にする必要があります。これは、ポートはペアで割り当てられており、各ペアに最初に割り当てられるポートが偶数であるためです。

範囲の広さ

単一のトラバーサル コールには最大 48 のポートが必要です。そうすることで、小規模/中規模システムでは最大 75 の同時発生トラバーサル コール（M5 ベース）、中規模システムで 100、大規模システムで最大 500 の同時発生コールを処理できます。デフォルトの範囲は 48*500 = 24000 ポートになります。

範囲を縮小する場合は、ライセンス供与済みのリッチ メディア セッション数ごとに公称 48 のポートを満たすには範囲が十分でない場合は、Expressway のアラームが発生することに注意してください。新しいライセンスを追加した場合は、再度範囲の拡大が必要になる場合があります。

各コールに 48 のポートが必要な理由

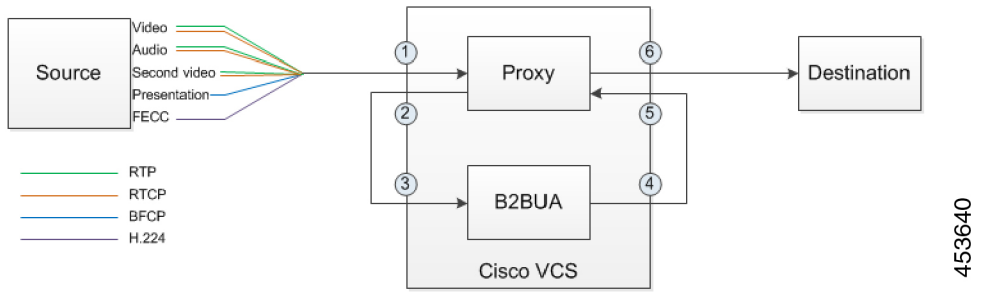
コール単位の最大割り当て済みポートの公称数は、割り当てごとのポートの最大数 x 割り当てインスタンスの最大数として計算します。これにより 8 * 6 = 48 となり、これらの数は次のように導くことができます。

各コールには最大で 5 つのタイプ（ビデオ（RTP/RTCP）、音声（RTP/RTCP）、セカンド/デュオ ビデオ（RTP/RTCP）、プレゼンテーション（BFCP）、相手側のカメラ制御（H.224））のメディアがあります。これらすべてのメディア タイプがコールに含まれている場合、コールには 8 つのポート、つまり、3 つの RTP/RTCP ペアのポート、BFCP 用に 1 つのポート、H.224 用に 1 つのポートが必要です。

各コールには少なくとも 2 つのレッグ（Expressway へのインバウンドと Expressway からのアウトバウンド）があり、2 つのポート割り当てのインスタンスが必要です。コールが B2BUA を介してルーティングされる場合は、さらに 4 つの割り当てのインスタンスが必要になります。この場合、ポートは次のポイントで割り当てられます。

1. 送信元からローカル プロキシへのインバウンド
2. ローカル プロキシからローカル B2BUA へのアウトバウンド
3. ローカル プロキシからローカル B2BUA へのインバウンド
4. ローカル B2BUA からローカル プロキシへのアウトバウンド
5. ローカル B2BUA からローカル プロキシへのインバウンド
6. ローカル プロキシから宛先へのアウトバウンド

図 *16 :* メディアトラバーサルコールの最大ポート割り当て



実際には、同時発生トラバーサル コールの最大数に到達せず、すべてのコールを B2BUA を通じてルーティングせず、すべてのコールに可能なタイプのすべてのメディアを含めることはないと考えられます。ただし、この極端なケースに対応するデフォルトの範囲を定義して、総ポート要件が指定したポート範囲を超える可能性がある場合に Expressway はアラームを生成します。

デフォルトの範囲

デフォルトのメディアトラバーサルポートの範囲は 36000 ～ 59999 です。Expressway-C では **[設定（Configuration）] > [ローカルゾーン（Local Zones）] > [トラバーサルサブゾーン（Traversal Subzone）]** で設定できます。大規模 Expressway システムでは、その範囲の最初の 12 ポート（デフォルトでは、36000 ～ 36011）は多重化トラフィック用に常に予約されています。Expressway-Eはそれらのポートでリッスンします。大規模システムでは逆多重化リスニング ポートの範囲を明示的に設定することはできません。常にメディア ポート範囲内の最初の 6 ペアが使用されます。小規模/中規模のシステムでは、Expressway-E で多重化 RTP/RTCP トラフィックをリッスンする 2 つのポートを明示的に指定できます（**[設定（Configuration）] > [トラバーサル（Traversal）] > [ポート（Ports）]**）。特定のペアのポートを設定しない場合（**[設定された逆多重化ポートを使用する（Use configured demultiplexing ports）]** が *[いいえ（No）]*）、Expressway-Eはメディア トラバーサル ポート範囲内のポートの最初のペアでリッスンします（デフォルトでは 36000 と 36001）。

（注） **[設定済みの逆多重化ポートを使用（Use configured demultiplexing ports）]** 設定を変更するには、システムを再起動して変更を有効にする必要があります。

デフォルト サブゾーンの設定

「デフォルト サブゾーン（Default Subzone）」ページ（**[設定（Configuration）] > [ローカル ゾーン（Local Zone）] > [デフォルトサブゾーン（Default Subzone）]**）を使用して、デフォルトサブゾーン内のエンドポイントを含むコールに帯域幅の制限を適用したり、デフォルトサブゾーンの登録、認証、およびメディア暗号化のポリシーを指定したりできます。

エンドポイントを Expressway に登録すると、その IP アドレスとエイリアスがサブゾーンのメンバーシップと照合して確認されて、適切なサブゾーンに割り当てられます。サブゾーンを作成していない場合、あるいはエンドポイントの IP アドレスまたはエイリアスがサブゾーンのメンバーシップ ルールに一致しない場合は、デフォルト サブゾーンに割り当てられます（これは、デフォルト サブゾーンの**登録ポリシー**と**認証ポリシー**によります）。

すべてのエンドポイント間で帯域幅を均等に使用できる場合にのみ、（手動で作成された他のサブゾーンがない）デフォルト サブゾーン自体を使用してください。

（注） ローカルゾーンに異なる帯域幅の制限を持つ複数の異なるネットワークが含まれている場合は、ネットワークの異なる部分ごとに個別にサブゾーンを設定する必要があります。

デフォルト サブゾーンの設定オプション

デフォルト サブゾーンは他のサブゾーンの設定と同様に設定できます。

サブゾーンの設定

「サブソーン（Subzones）」ページ（**[設定（Configuration）] > [ローカル ゾーン（Local Zones）] > [サブゾーン（Subzones）]**）には、Expressway に設定したすべてのサブゾーンのリストが表示されます。このページでは、サブゾーンを作成、編集、削除できます。各サブゾーンについては、設定されているメンバーシップ ルールの数、現在登録されているデバイスの数、および現在使用中のコールの数と帯域幅が表示されます。最大 1000 のサブゾーンを設定できます。

サブゾーンを設定した後、サブゾーン メンバーシップ ルールの設定をセットアップして、デフォルト サブゾーンの設定にデフォルトで設定されるのではなく、Expressway への設定時にエンドポイント デバイスを割り当てるサブゾーンを制御します。

設定可能なオプションは次のとおりです。

フィールド/セクション	説明
登録ポリシー（**Registration policy**）	エンドポイントを Expressway に登録すると、その IP アドレスとエイリアスがサブゾーンのメンバーシップと照合して確認されて、適切なサブゾーンに割り当てられます。サブゾーンを作成していない、あるいはエンドポイントの IP アドレスまたはエイリアスがメンバーシップ ルールのいずれにも一致しない場合は、デフォルト サブゾーンに割り当てられます。 エンドポイントを Expressway に登録可能かどうかを制御するために登録についてを使用するほかに、サブゾーン メンバーシップ ルールを使用して割り当てられた登録を受け入れるかどうかについて、サブゾーンの**登録ポリシー**も設定する必要があります。 これにより、登録ポリシーを設定するときの柔軟性が高まります。たとえば、次のことを実行できます。 • IP アドレスのサブネットに基づく登録の拒否。これを行うには、IP アドレスのサブネット範囲に基づいて関連するメンバーシップでサブゾーンを作成してから、登録を拒否するようにそのサブゾーンを設定します。 • 登録を拒否するようにデフォルト サブゾーンを設定する。これにより、サブゾーン メンバシップ ルールのいずれにも一致しないためにデフォルト サブゾーンに分類される登録要求が拒否されます。 （注） 登録要求は、サブゾーンメンバーシップとサブゾーン登録ポリシーのルールが適用される前に、登録制限ポリシールールを満たす必要があります。
認証ポリシー（**Authentication policy**）	[認証ポリシー（Authentication policy）] の設定は、デフォルト サブゾーンへの着信メッセージを Expressway がどのように処理するかを制御します。詳細については、認証ポリシー（Authentication policy）を参照してください。
メディア暗号化モード（**Media encryption mode**）	[メディア暗号化モード（Media encryption mode）] の設定では、サブゾーンを通過する SIP コール用のメディア暗号化機能を設定します。詳細については、メディア暗号化ポリシーの設定を参照してください。 （注） H.323 が有効になっていて、サブゾーンのメディア暗号化モードが *[強制暗号化（Force encrypted）]* または *[強制暗号化解除（Force unencrypted）]* の場合、このサブゾーンを通過する H.323 コールおよび SIP から H.323 のインターワーキングコールはこのモードを無視します。

フィールド/セクション	説明
メディアに対する ICE サポート（ICE support for media）	ICE メッセージをこのサブゾーンのデバイスがサポートするかどうかを制御します。
帯域幅制御（Bandwidth controls）	サブゾーンを設定するときに帯域幅の制限を次のように適用できます。 • サブゾーン内の 2 つのエンドポイント間の個々のコール。 • サブゾーン内のエンドポイントとそのサブゾーン外の別のエンドポイント間の個々のコール。 • サブゾーン内のエンドポイントで送受信するコールの総数。 帯域幅の制限の設定方法と管理方法については、サブゾーンへの帯域幅の制限の適用を参照してください。

サブゾーン メンバーシップ ルールの設定

「**サブゾーン メンバーシップ ルール（Subzone membership rules）**」ページ（**[設定（Configuration）] > [ローカル ゾーン（Local Zone）] > [サブゾーン メンバーシップ ルール（Subzone membership rules）]**）を使用して、Expressway に登録するときにエンドポイントに割り当てるサブゾーンをデバイスのアドレスに基づいて決定するルールを設定しますサブゾーンの設定 （405 ページ）。

このページには、Expressway に設定されているすべてのサブゾーン メンバーシップ ルールのリストが表示されるため、ルールを作成、編集、削除、有効化、および無効化することができます。ルールのプロパティは次のとおりです。

- ルールの名称と説明
- プライオリティ
- サブネットまたはエイリアスのパターンマッチング設定
- このルールを満たすアドレスを持つエンドゾーンに割り当てられるサブゾーン

（注） エンドポイントの IP アドレスまたは登録エイリアスがメンバーシップ ルールのいずれにも一致しない場合は、デフォルト サブゾーンの設定に割り当てられます。

最大 3000 のサブゾーン メンバーシップ ルールを設定できます。

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
ルール名	メンバーシップ ルールの記述名。	
Description	ルールの任意の自由形式の説明	リストのルールの上にマウス ポインタを置いた場合に説明がツールチップとして表示されます。
優先度（**Priority**）	エンドポイントのアドレスが複数のルールを満たす場合に、ルールを適用する順序（および、そのために、エンドポイントを割り当てるサブゾーン）。	最も高いプライオリティ（1、2、3の順）を持つルールが最初に適用されます。複数のサブネット ルールが同じプライオリティの場合、最も大きなプレフィックス長を持つルールが最初に適用されます。エイリアス パターン マッチ ルールで同じプライオリティのものは、設定順に検索されます。
タイプ（**Type**）	デバイスのアドレスの確認方法を決定します。 *[*サブネット（*Subnet*）*]*：IP アドレスが設定した IP アドレス サブネットに含まれる場合は、デバイスを割り当てます。 *[*エイリアス パターン マッチ（*Alias pattern match*）*]*：エイリアスが設定したパターンと一致する場合は、デバイスを割り当てます。	たとえば、ダイナミック IP アドレスの在宅ワーカーにとってパターン マッチングは便利です。継続的にサブネットを更新して割り当てられているものと一致させるのではなく、在宅ワーカーのエイリアスと一致させることができます。
サブネット アドレス（**Subnet address**）とプレフィックス長（**Prefix length**）	これら2つのフィールドで、このサブゾーンに属する IP アドレスの範囲を決定します。 [アドレス範囲（Address range）] フィールドには、[サブネット アドレス（Subnet address）] と [プレフィックス長（Prefix length）] の組み合わせに基づいてこのサブゾーンに割り当てる IP アドレスの範囲が表示されます。	[タイプ（Type）] が [サブネット（Subnet）] の場合にのみ適用されます。

フィールド	説明	使用方法のヒント
パターン タイプ（Pattern type）	適用するルールで、**パターン文字列**をどのようにエイリアスと照合するか。次のオプションがあります。 *[*完全一致（*Exact*）*]*：文字列全体がエイリアスと1文字も違うことなく完全に一致する必要があります。 *[*プレフィックス（*Prefix*）*]*：文字列がエイリアスの先頭に表示される必要があります。 *Suffix*：文字列がエイリアスの末尾に表示される必要があります。 *[*正規表現（*Regex*）*]*：文字列を正規表現として処理します。	**[タイプ（Type）]**が*[*エイリアス パターン マッチ（*Alias pattern match*）*]* の場合にのみ適用されます。
パターン文字列（Pattern string）	エイリアスと比較するパターン。	**[タイプ（Type）]** が *[*エイリアス パターン マッチ（*Alias pattern match*）*]* の場合にのみ適用されます。
ターゲット サブゾーン（Target subzone）	アドレスがこのルールを満たす場合にエンドポイントを割り当てるサブゾーン。	
状態（State）	ルールが有効になっているかどうかを示します。	この設定を使用して設定変更をテストしたり、特定のルールを一時的に無効にします。ルール リストには無効にしたルールが表示されますが、無視されます。

サブゾーンへの帯域幅の制限の適用

帯域幅の制限は、デフォルト サブゾーン、トラバーサル サブゾーン、および手動で設定されたすべてのサブゾーンに適用できます。適用する制限はサブゾーンのタイプに応じて、次のように異なります。

制限事項	説明	適用対象
合計（Total）	サブゾーン内のすべてのエンドポイントが常に使用する総同時帯域幅を制限します。トラバーサル サブゾーンの場合、これはすべての同時発生トラバーサル コールに使用できる最大帯域幅になります。	デフォルト サブゾーン トラバーサル サブゾーン 手動で設定されたサブゾーン
完全に内部のコール（Calls entirely within...）	サブゾーン内の2つのエンドポイント間の個々のコールの帯域幅を制限します。	デフォルト サブゾーン 手動で設定されたサブゾーン
送受信コール（Calls into or out of...）	サブゾーン内のエンドポイントと別のサブゾーンまたはゾーン内のエンドポイント間の個々のコールの帯域幅を制限します。	デフォルト サブゾーン 手動で設定されたサブゾーン
処理対象のコール（Calls handled by...）	個々のトラバーサル コールに使用できる最大帯域幅。	トラバーサル サブゾーン

上記のすべての制限に対して、**[帯域幅の制限（Bandwidth restriction）]** の設定には次の影響があります。

- *[帯域幅なし（No bandwidth）]*：帯域幅を割り当てず、そのためにコールは発信されません。
- *[制限付き（Limited）]*：制限が適用されます。対応する帯域幅（kbps）フィールドに値を入力する必要があります。
- *[無制限（Unlimited）]*：使用される帯域幅の量に制限は適用されません。

1 つの特定のサブゾーンと**そのほかすべて**のサブゾーンまたはゾーン間で使用できる帯域幅を設定する場合は、サブゾーンの帯域幅の制限を使用します。

1 つの特定のサブゾーンと**別の特定の**サブゾーンまたはゾーン間で使用できる帯域幅を設定する場合は、パイプを使用します。

帯域幅の設定で複数のタイプの帯域幅の制限がコールに適用されている場合（たとえば、サブゾーンの帯域幅の制限とパイプの制限がある場合）、そのコールには常に最も低い制限値が適用されます。

帯域幅のさまざまな制限の管理方法

同じリンクにさまざまな帯域幅の制限が適用されている場合、コールのルーティングや帯域幅の制限を考慮すると、常に最も低い制限値が使用されます。

たとえば、サブゾーンAのコール単位の相互帯域幅は128であるとします。これは、サブゾーンAと他のサブゾーンまたはゾーン間のコールは128 kbpsに制限されることを意味します。

ただし、サブゾーンAにはそのゾーンとサブゾーンBとの間に設定されたリンクがあります。このリンクは制限が512kbpsのパイプを使用しています。この場合、パイプのキャパシティのほうが大きくても、低いほうの制限値の 128 kbps がこの 2 つの間のコールに適用されます。

この逆の場合で、サブゾーン A のコール単位の相互帯域幅制限が 512 kbps で、サブゾーン B へのリンクに 128 kbps のパイプがある場合、この 2 つのサブゾーン間のコールも 128 kbps に制限されます。

トラバーサル コールの帯域幅消費

同じサブゾーン内の2つのエンドポイント間の非トラバーサル コールは、そのサブゾーンからそのコールの帯域幅の量を消費します。

同じサブゾーン内の2つのエンドポイント間のトラバーサルコールは、すべてのトラバーサル コールと同様に、トラバーサル サブゾーンを通過する必要があります。これは、このようなコールは発信元のサブゾーンの同時割り当ての合計、つまり、サブゾーンからトラバーサルサブゾーンへのコールで1回と、トラバーサルサブゾーンから発信元のサブゾーンへのコールにもう1回で、コールの帯域幅の2倍に等しくなる帯域幅の量を消費します。さらに、このコールはトラバーサル サブゾーンを通過するため、コールと等しい量の帯域幅をトラバーサル サブゾーンから消費します。

リンクとパイプ

リンクの設定

リンクはローカル サブゾーンを他のサブゾーンやゾーンと接続します。コールを発信するには、関与するエンドポイントがそれらの間にリンクのあるサブゾーンまたはゾーンにそれぞれ存在している必要があります。リンクは直接である必要はありません。2 つのエンドポイントが 1 つ以上の中間サブゾーンを介してリンクされている場合もあります。

リンクを使用して、ネット上へのコールのルーティング方法や、どのゾーンおよびサブゾーンが関与するか、および使用可能な帯域幅の量を計算します。複数のルートが考えられる場合、Expressway はもっとのリンクの少ないルートを使用して、帯域幅計算を実行します。

「リンク（Links）」ページ（**[設定（Configuration）] > [帯域幅（Bandwidth）] > [リンク（Links）]**）に既存のすべてのリンクのリストが表示されます。このページでは、リンクを作成、編集、削除できます。

次の情報が表示されます。

フィールド	説明
名前（Name）	各リンクの名前。自動的に作成されたリンクは、リンクが間にあるノードに基づいて名前が付けられます。

フィールド	説明
ノード 1（Node 1）と**ノード 2（Node 2）**	トラバーサル サブゾーンとリンクが間にあるゾーン。 2 つのサブゾーン、またはリンクが間にある 1 つのサブゾーンと 1 つのゾーン。
パイプ 1（Pipe 1）と**パイプ 2（Pipe 2）**	帯域幅の制限をリンクに適用するために使用したパイプ。詳細については、リンクへのパイプの適用を参照してください。 （注） パイプを適用するには、パイプの設定 ページを使用して、最初にパイプを作成する必要があります。
コール（Calls）	現在リンクを通過しているコールの総数を表示します。
使用済み帯域幅（Bandwidth used）	リンクを通過しているすべてのコールによって現在消費されている帯域幅の総量を表示します。

最大 3000 のリンクを設定できます。一部のリンクはサブゾーンまたはゾーンが作成されたときに自動的に作成されます。

デフォルト リンク

サブゾーンにリンクが設定されていない場合、そのサブゾーン内のエンドポイントは同じサブゾーン内の他のエンドポイントにのみコールできます。そのため、Expressway は一連のリンクを事前に設定して出荷されており、また、新しいサブゾーンを作成するたびに新しいリンクが自動的に作成されます。

事前設定されているリンク

Expressway はデフォルト サブゾーン、トラバーサル サブゾーン、およびデフォルト ゾーンがすでに作成された状態で出荷され、それらの間にデフォルトのリンクの *DefaultSZtoTraversalSZ*、*DefaultSZtoDefaultZ*、および *TraversalSZtoDefaultZ* も設定されています。Expressway がクラスタ内にある場合は、デフォルト サブゾーンとクラスタ サブゾーンの間に追加のリンクである *DefaultSZtoClusterSZ* も確立されています。

これらのデフォルト リンクは、設定済みのリンクを手動で編集するのと同じように編集できます。これらのリンクのいずれかが削除されていた場合は、次のいずれかで再度作成できます。

- Web インターフェイスを使用して手動で作成
- CLI コマンドを使用して自動的に作成**xCommand DefaultLinksAdd**

自動的に作成されたリンク

新しいサブゾーン、またはゾーンが作成されるたびに、リンクは次のように自動的に作成されます。

新しいゾーン/サブゾーンのタイプ	デフォルト リンクの作成先
サブゾーン	デフォルト サブゾーンとトラバーサル サブゾーン
ネイバー ゾーン	デフォルト サブゾーンとトラバーサル サブゾーン
DNS ゾーン	デフォルト サブゾーンとトラバーサル サブゾーン
ENUM ゾーン	デフォルト サブゾーンとトラバーサル サブゾーン
トラバーサル クライアント ゾーン	トラバーサル サブゾーン
トラバーサル サーバ ゾーン	トラバーサル サブゾーン

事前に設定されたデフォルトのリンクとともに、これらのリンクによって、デフォルトでは新しいサブゾーンまたはゾーンには他のすべてのサブゾーンやゾーンとの接続が保証されます。これらのデフォルト リンクはいずれも、名前を変更したり、削除したり、修正したりできます。

（注） リンクが正しく設定されていないと、コールは失敗します。コールが成功するかどうか、およびどのような帯域幅がそのコールに割り当てられるかについては、CLI コマンドの**xCommand CheckBandwidth**を使用して確認できます。

パイプの設定

パイプを使用して、特定のサブゾーンとゾーン間のコールで使用する帯域幅の量を制御します。常に使用される総同時帯域幅や、個々のコールに使用される帯域幅に制限を適用できます。

これらの制限を適用するには、まずパイプを作成してから、必要な帯域幅の制限を使用して設定します。次に、リンクを設定するときに、1 つ以上のリンクにパイプを割り当てます。リンクを使用したコールには、それらに適用されたパイプの帯域幅の制限が適用されます。詳細については、リンクへのパイプの適用を参照してください。

「パイプ（Pipes）」ページ（**[設定（Configuration）] > [帯域幅（Bandwidth）] > [パイプ（Pipes）]**）には、Expressway に設定したすべてのパイプのリストが表示されます。このページでは、パイプを作成、編集、削除できます。

次の情報が表示されます。

フィールド	説明
名前（Name）	パイプの名前。

フィールド	説明
総帯域幅（Total bandwidth）	このパイプが適用されるすべてのリンク上のすべてのコールによって常に使用される総帯域幅の上限値。
コール単位の帯域幅（Per call bandwidth）	このパイプが適用されるリンクでの 1 回のコールの最大帯域幅。
コール（Calls）	パイプが適用されるすべてのリンクを現在通過しているコールの総数を表示します。
使用済み帯域幅（Bandwidth used）	パイプが適用されるすべてのリンクを通過しているすべてのコールによって現在消費されている帯域幅の総量を表示します。

最大 1000 のパイプを設定できます。

帯域幅の制限の設定方法と管理方法については、サブゾーンへの帯域幅の制限の適用を参照してください。

リンクへのパイプの適用

パイプを使用して、リンクの帯域幅を制限します。パイプをリンクに適用すると、リンクの 2 つのノード間で実行されているコールの帯域幅を制限します。この制限はコールに双方向で適用されます。通常、単一のパイプが単一のリンクに適用されます。ただし、ネットワークをどのようにモデル化するかによっては、1 つ以上のパイプを 1 つ以上のリンクに適用することもできます。

1 つのパイプ、1 つのリンク

単一のパイプを単一のリンクに適用すると、サブゾーンと別の特定の座部ゾーンまたはゾーン間のコールに特定の制限を適用する場合に便利です。

1 つのパイプ、複数のリンク

各パイプを複数のリンクに適用できます。あるサイトが別の複数のサイトとインターネットへの同じブロードバンド接続を通じて通信する状況のモデル化にこれを使用します。パイプはブロードバンド接続を表すように設定してから、すべてのリンクに適用する必要があります。これにより、そのサイトで発着信するコールに帯域幅のオプションを設定できます。

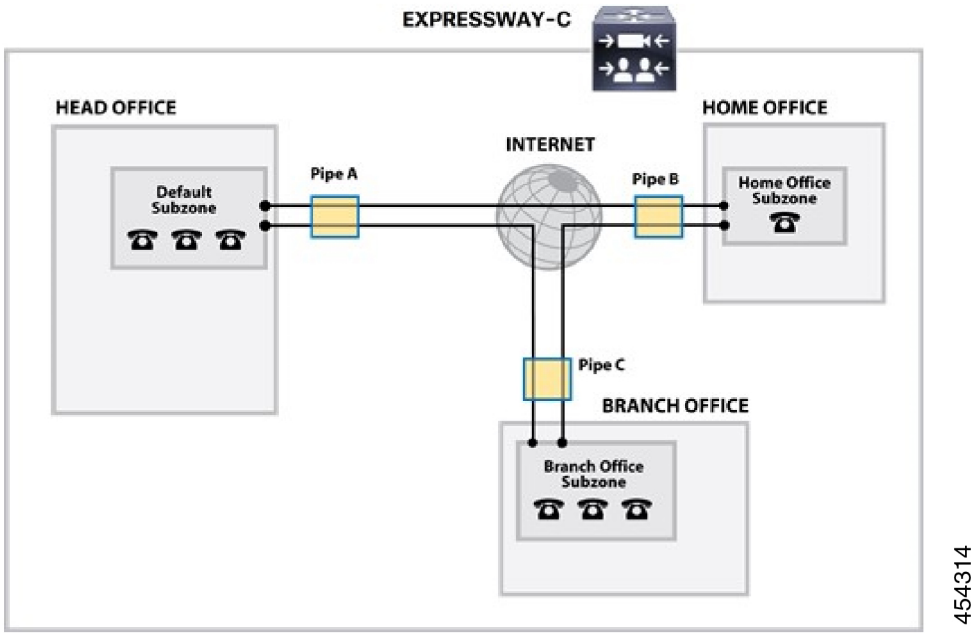
次の図では、パイプ A が 2 つのリンクが適用されています。1 つはデフォルト サブゾーンとホーム オフィス サブゾーン間のリンクで、もう 1 つはデフォルト サブゾーンと支社のサブゾーン間のリンクです。この場合、パイプ A は本社のインターネットへのブロードバンド接続を表し、総量とコール単位の制限が適用されることになります。

2 つのパイプ、1 つのリンク

各リンクにはそれに関連付けられた最大 2 つのパイプがある場合があります。たとえば、インターネットへの独自のブロードバンド接続をそれぞれ持っている 2 つのサイトなど、リンクの

2 つのノードが直接接続されていない場合に、これを使用します。各接続には独自のパイプが必要です。つまり、2つのノード間のリンクは、両方のパイプの帯域幅制限の対象となります。

次の図では、デフォルトのサブゾーンとホーム オフィスのサブゾーン間のリンクには、関連付けられている2つのパイプがあります。パイプ A はインターネットへの本社のブロードバンド接続を表し、パイプ B はインターネットへのホーム オフィスのダイヤルアップ接続を表しています。各パイプには最大キャパシティを表すために適用されている帯域幅の制限があります。このリンクを介して行われるコールには、2 つの帯域幅の制限のうち低いほうが適用されます。



帯域幅制御の例

ファイアウォールなし

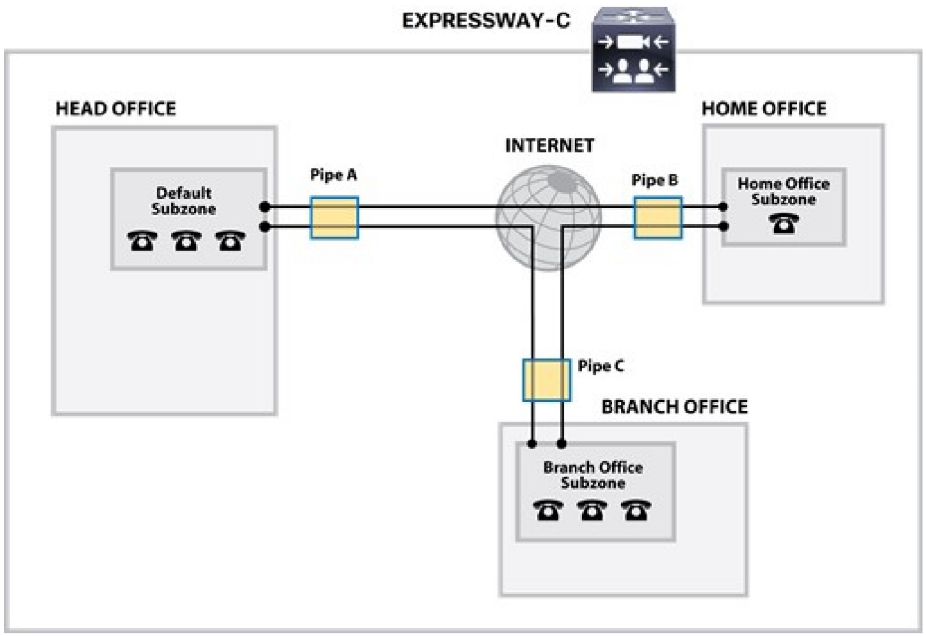
次の例では、地理的に離れた3つのオフィス、本社、支社、ホーム オフィスがあります。本社のすべてのエンドポイントは Expressway-C に登録されており、支社とホーム オフィスも同様です。

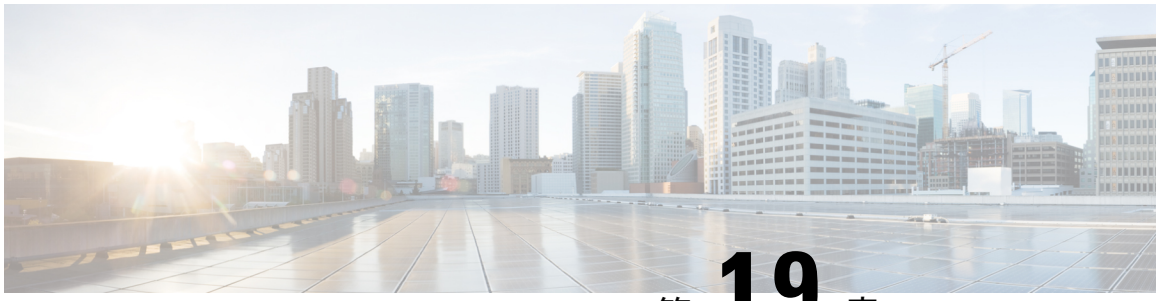
3つのオフィスそれぞれは、Expressway 上では、ローカル ポリシーに従って設定された帯域幅を持つ個別のサブゾーンとして示されます。

企業のインターネットへのリース回線接続と、リモート オフィスへの DLS 接続は個別のパイプとしてモデル化されています。

このシナリオではファイアウォールは含まれていません。したがって、それぞれのオフィス間に直接リンクを設定できます。次に、各リンクには、リンクの両端のオフィスのインターネット接続を表す 2 つのパイプを割り当てます。

このシナリオでは、ホーム オフィスと支社間のコールはホームと支社のサブゾーンの帯域幅と、本社と支社のパイプ（パイプ B とパイプ C）の帯域幅を消費します。本社の帯域幅予算にはこのコールによる影響はありません。





第 19 章

アプリケーション

ここでは、Expressway の **[アプリケーション（Applications）]** メニューで使用できる追加サービスのそれぞれについて説明します。

Conference Factory の設定

「Conference Factory」ページ（**[アプリケーション（Applications）]** > **[Conference Factory]**）では、Conference Factory アプリケーションを有効化または無効化することができ、使用するエイリアスとテンプレートを設定できます。

Conference Factory アプリケーションを使用して、Expressway は Multiway 対応のエンドポイントと会議ブリッジに従って Multiway 機能をサポートします（『Cisco TelePresence Multiway 導入ガイド』を参照してください）。Multiway は、エンドポイントにこの機能が組み込まれていない場合でも、コール中にエンドポイントのユーザが会議を作成できます。

Multiway をサポートするシスコのエンドポイントとインフラストラクチャ製品の最新のリストについては、シスコの担当者にお問い合わせください。

会議の作成プロセス

Multiway 機能をエンドポイントからアクティブ化すると、次のプロセスが行われます。

1. エンドポイントが Expressway 上の Conference Factory にルーティングするように事前に設定されたエイリアスをコールします。
2. Expressway はエンドポイントが Multiway 会議に使用する必要があるエイリアスでエンドポイントに応答します。このエイリアスは MCU にルーティングします。

3. 次に、エンドポイントは指定されたエイリアスを使用して MCU をコールし、他の参加エンドポイントに同じことを実行するように通知します。

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
モード（**Mode**）	Conference Factory アプリケーションを有効または無効にします。	
エイリアス（**Alias**）	Multiway 機能がアクティブになったときにエンドポイントがダイヤルするエイリアス。これも、Multiway 機能の開始に使用できるすべてのエンドポイントに設定する必要があります。例：**multiway@example.com**	
テンプレート **(Template)**	Multiway 会議を MCU に作成するためにダイヤルするよう Expressway がエンドポイントに通知するエイリアス。	会議ごとに異なるエイリアスを指定するには、テンプレートの一部として %% を使用する必要があります。%% は、Expressway が新しい会議要求を受信するたびに一意の番号によって置換されます。
番号範囲の開始/終了（**Number range start/end**）	会議エイリアスの生成に使用するテンプレートの %% を置換する範囲の最初と最後の数値。	たとえば、**テンプレート** 10 ~ 999 の歯にの**563%%@example.com**です。最初の会議はエイリアス**563010@example.com**を使用し、次の会議は**563011@example.com**を使用して**563999@example.com**まで続きます。その後、ループして**563010@example.com**から再開します。 （注） %% は、範囲の上限値の長さに基づき一定の桁数を表し、必要に応じて先行ゼロが付きます。

（注）

- Conference Factory アプリケーションが有効になっているネットワーク内の VCS のそれぞれで異なる**テンプレート**を使用する必要があります。Expressway がクラスタの一部である場合、クラスタ内のピアごとに異なるテンプレートを使用する必要があります。
- テンプレートが生成するエイリアスは完全修飾 SIP であり、MCU にルーティングする必要があります。MCU はこのエイリアスを処理するように設定する必要があります。MCU では、Conference Factory アプリケーションをサポートするためのその他の特別な設定は必要ありません。
- **[SIP モード（SIP mode）]** を *[オン（On）]*（**[設定（Configuration）]** > **[プロトコル（Protocols）]** > **[SIP]**）に設定する必要があります。H.323 エンドポイントから Conference Factory へのコールを発信するには、**[H.323 モード（H.323 mode）]** も *[オン（On）]* にし（**[設定（Configuration）]** > **[プロトコル（Protocols）]** > **[H.323]**）、**[H.323 <-> SIP 間のインターワーキングモード（H.323 <-> SIP interworking mode）]** が *[登録済みのみ（Registered only）]* または *[オン（On）]* に設定されていることを確認します（**[設定（Configuration）]** > **[プロトコル（Protocols）]** > **[インターワーキング（Interworking）]**）。

Multiway を導入環境で使用するようにネットワークの個々のコンポーネント（エンドポイント、MCU、および Expressway）を設定する方法の詳細については、『Cisco TelePresence Multiway 導入ガイド』を参照してください。

プレゼンスについて

プレゼンスは、エンドポイントの現在のステータス（オフラインか、オンラインか、コール中かなど）について他のユーザに情報を提供するためのエンドポイントの機能です。プレゼンス情報を提供するエンティティやプレゼンス情報を要求できるエンティティをプレゼンティティと呼びます。プレゼンティティは、それ自体のプレゼンス ステータスに関する情報をパブリッシュするとともに、他のプレゼンティティや FindMe ユーザがパブリッシュしている情報をサブスクライブします。

Jabber Video などのプレゼンスをサポートするエンドポイントは、独自のステータス情報をパブリッシュできます。また、Expressway は、H.323 エンドポイントなどプレゼンスをサポートしないエンドポイントが URI 形式のエイリアスで登録されている限り、それらに代わって基本的なプレゼンス情報を提供します。

FindMe を有効になっている場合、Expressway は、FindMe ユーザに設定された各プレゼンティティが提供する情報を集約することによって、その FindMe ユーザに関するプレゼンス情報も提供できます。

Expressway 上のプレゼンス アプリケーションは SIP ベースの SIMPLE 標準規格をサポートします。このアプリケーションは、2 つの個別のサービスから構成されます。具体的には、プレゼンス サーバとプレゼンス ユーザ エージェント（PUA）の 2 つです。これらのサービスは個別にプレゼンスの設定できます。

プレゼンスのステータス ページには、プレゼンス情報を提供するプレゼンティティと、他のユーザに関するプレゼンス情報を要求するユーザの情報が表示されます。ステータスページは次のように構成されています。

- パブリッシャ（Publishers）
- プレゼンティティ（Presentities）
- サブスクライバ（Subscribers）

（注） 1つのプレゼンティティがサブスクライブできるのは最大100の他のプレゼンティのみであり、そのプレゼンティティをサブスクライブできる他のプレゼンティティは最大 100 のみです。

プレゼンスは、クラスタリングによってサポートされます。

プレゼンス サーバ

Expressway 上のプレゼンス サーバは、その VCS が権限を持つ ドメインの設定のすべてのプレゼンティティのプレゼンス情報の管理を担います。プレゼンス サーバはローカルに登録されているエンドポイントと、SIP プロキシ（別の Expressway など）を介して情報を受信したプレゼンティティの情報を管理できます。

プレゼンス サーバは次のサービスから構成されますが、それらのすべてのサービスは、プレゼンス サーバが有効（または無効）になったときに同時に有効（または無効）になります。

- **パブリケーションマネージャ**：プレゼンティティに関するステータス情報を含むPUBLISHメッセージを受信し、その情報をプレゼンス データベースに書き込みます。PUBLISH はプレゼンス対応のエンドポイントとプレゼンス ユーザ エージェントによって生成されます。
- **サブスクリプションマネージャ**：プレゼンティティのステータスに関する情報を要求する SUBSCRIBE を処理します。SUBSCRIBE メッセージを受信すると、サブスクリプション マネージャはそのプレゼンティティに関する情報の要求をプレゼンティティ マネージャに送信し、返された情報をサブスクライバに転送します。また、サブスクリプション マネージャは、プレゼンティティのステータスが変更されたときにプレゼンティティ マネージャから通知を受信し、その情報をすべてのサブスクライバに送信します。
- **プレゼンティティ マネージャ**：プレゼンス データベースへのインターフェイス。さまざまなデバイスによって提供されたプレゼンス情報を集約して1つの特定のプレゼンティティに関する全体的なプレゼンス ステータスを提供する必要がある場合に、FindMe や PUA などの Expressway 機能をサポートするために使用されます。プレゼンティティに関する情報を求める要求をサブスクリプション マネージャから受信した場合、プレゼンティティ マネージャはその特定のプレゼンティティに関連付けられたすべてのエンドポイントで使用可能な情報をプレゼンス データベースに照会します。次に、プレゼンティティ マネージャはこの情報を集約してプレゼンティティの現在のステータスを決定し、それをサブスクリプション マネージャに返します。

- **プレゼンス データベース**：PUBLISH メッセージの形式で受信した現在のプレゼンス情報を格納します。また、NOTIFY メッセージをプレゼンティティ マネージャに送信し、変更があった場合にそれを通知します。

プレゼンスとデバイスの認証

プレゼンス サーバは、すでに認証されているプレゼンス PUBLISH メッセージのみ受け入れます。

- Expressway によるプレゼンス メッセージの認証は、エンドポイントが登録されている場合にはデフォルト サブゾーン（または関連する代替サブゾーン）上の認証ポリシー設定によって制御され（通常のケース）、エンドポイントが登録されていない場合はデフォルト ゾーン上の認証ポリシー設定によって制御されます。
- 関連する **[認証ポリシー（Authentication policy）]** は、*[クレデンシャルを確認する（Check credentials）]* または *[認証済みとして扱う（Treat as authenticated）]* のいずれかに設定されている必要があります。そうでなければ、PUBLISH メッセージは失敗し、エンドポイントはそれぞれのプレゼンス ステータスをパブリッシュできなくなります。

詳細については、「プレゼンスと認証ポリシー」を参照してください。

プレゼンス ユーザ エージェント

プレゼンスをサポートしないエンドポイントは、Expressway の代わりにパブリッシュされたステータスを持つことができます。この情報をパブリッシュするサービスをプレゼンス ユーザ エージェント（PUA）と呼びます。

PUA はローカル登録データベースとコール マネージャから情報を取得し、現在ローカルに登録されている各エンドポイントについて、それらがコール中かどうかを決定します。次に PUA はこのステータス情報を PUBLISH メッセージを介して提供します。

PUA がローカルに登録されているエンドポイントに関するプレゼンス情報を正常に提供するには、次のことが必要です。

- エンドポイントが URI 形式のエイリアスを使用して登録されている必要があります。
- プレゼンス サーバが有効になっている SIP レジストラに URI のドメインの部分のルーティングが可能である必要があります（これは、有効になっている場合にはローカル プレゼンス サーバか、リモート システムの別のプレゼンス サーバかのいずれかです）。

PUA は有効になっている場合は、プレゼンスをすでにサポートしているエンドポイントを含め、Expressway に登録されているすべてのエンドポイントについてのプレゼンス情報を生成します。PUA が提供するステータス情報は次のいずれかです。

- オンライン（*online*）：登録されているが、コール中ではない
- コール中（*in call*）：登録されており、現在コール中

プレゼンス情報の集約

PUA は有効になっている場合は、プレゼンスをすでにサポートしているエンドポイントを含め、Expresswayに登録されているすべてのエンドポイントについてのプレゼンス情報を生成します。ただし、プレゼンスをサポートするエンドポイントは、退席中や応答不可など、より詳細な別のステータスも提供できます。そのため、プレゼンティティ マネージャは PUA が提供する情報を次のように使用します。

- プレゼンス情報が PUA と別のもう 1 つのソースから提供される場合、PUA でないプレゼンス情報を常にPUAプレゼンス情報よりも優先して使用します。これは、情報の別のソースがプレゼンティティ自体であり、その情報のほうがより正確であると考えられるためです。
- プレゼンス情報が PUA と複数の別のソースから提供される場合、プレゼンス サーバはすべてのプレゼンティティからのプレゼンス情報を集約し、*[*オフライン（*offline*）*]* よりも *[*オンライン（*online*）*]*、*[*退席中（*away*）*]* よりも *[*コール中（*in call*）*]* のほうに「「高い関心」」を示します。
- エンドポイントに関する情報が、エンドポイント自体からも、PUAからもパブリッシュされていない場合、エンドポイントのステータスは [オフライン（offline）] になります。PUA が有効になっている場合、*[*オフライン（*offline*）*]* のステータスは、エンドポイントが現在登録されていないことを示します。

FindMe プレゼンス

プレゼンティティ マネージャが FindMe エイリアスの存在についての情報の要求を受信すると、その FindMe エイリアスを構成している各エンドポイントのプレゼンス情報をルックアップします。次に、この情報を次のように集約します。

- FindMe エイリアスが *[*個別（*Individual* ）*]*モードに設定され、その FindMe を構成しているエンドポイントのいずれかがコール中の場合、FindMe プレゼンティティのステータスは *[*コール中（*in call*）*]* と報告されます。
- FindMeエイリアスが *[*グループ（*Group*）*]*モードに設定され、エンドポイントにいずれかがオンライン（コール中でもオフラインでもない）場合、FindMe プレゼンティティのステータスは *[*オンライン（*online*）*]* と報告されます。

再登録更新期間

PUA は、次を受信した時点でプレゼンス情報を更新し、パブリッシュします。

- 登録要求（新規登録の場合）
- 際登録更新（既存の登録の場合）
- 再登録要求
- コールセットアップとクリアダウン情報

非トラバーサル H.323 登録では、デフォルトの登録更新期間は 30 分です。つまり、PUA が既存の登録でVCS上で有効になっている場合は、H.323登録更新を受信し、*[*使用可能（*available*）*]* プレゼンス情報がそのエンドポイントにパブリッシュされるまでに 30 分かかることがあります。

また、H.323 エンドポイントが再登録メッセージを送信せずに使用できなくなった場合、そのステータスが [オフライン（offline）] に変化するのに 30 分かかることがあります。H.323 エンドポイントのプレゼンス情報のパブリケーションをよりタイムリーに行うには、H.323 登録更新期間を短縮する必要があります（**[設定（Configuration）]** > > **[プロトコル（Protocols）]** > **[H.323]** > **[ゲートキーパー（Gatekeeper）]** > **[存続期間（Time to live）]** を使用します）。

SIP のデフォルトの登録更新期間は 60 秒です。したがって、PUA が更新されたプレゼンス情報を SIP エンドポイントの代わりにパブリッシュするのに 1 分もかかりません。

プレゼンスの設定

[プレゼンス（Presence）] ページ（**[アプリケーション（Applications）]** > **[プレゼンス（Presence）]**）を使用して、Expressway 上のプレゼンス サービスを有効にし、設定できます。

これらのサービスは、導入の特性に応じて、それぞれ個別に有効にしたり、無効にしたりできます。デフォルトでは両方とも無効になっています。

（注） プレゼンスサービス が機能するには、**SIP モード**を有効にする必要があります。

プレゼンス ユーザ エージェント

PUA は、登録されているエンドポイントの代わりにプレゼンス情報を提供します。

- *[*有効（*Enabled*）*]*：PUA が有効になっている場合、ローカルに登録されているすべてのエンドポイントがそれら自体のプレゼンス情報もパブリッシュしているかどうかにかかわらず、それらのプレゼンス情報をパブリッシュします。PUAによってパブリッシュされた情報は、エンドポイントのドメインとして機能しているプレゼンス サーバにルーティングされます。これは、ローカル プレゼンス サーバか、（これが無効になっている場合は、そのドメインに権限を持つ別のシステムのプレゼンス サーバである可能性があります。
- *[*無効（*Disabled*）*]*：PUA が無効になっている場合、プレゼンスをサポートするエンドポイントのみがプレゼンス情報をパブリッシュします。プレゼンスをサポートしないエンドポイントの情報は入手できません。

また、[登録済みエンドポイントのデフォルトで公開されるステータス（Default published status for registered endpoints）] も設定できます。これは、「「通話中」」でないときの登録済みエンドポイントについてプレゼンスユーザ エージェントがパブリッシュしたプレゼンティティス テータスです。オプションは [オンライン（Online）] と [オフライン（Offline）] です。

（注）
- これが *[オンライン（Online）]* に設定されている場合、永続的に登録されているビデオエンドポイントと、それらのエンドポイントが含まれている FindMe エンティティは永続的に 「[オンライン（Online）]」 と表示されます。
- 登録されていないエンドポイントのステータスは常に 「[オフライン（Offline）]」 と表示されます。
- Lync クライアントでは 「[オンライン（Online）]」 ステータスは 「[使用可能（Available）]」 と表示されます。

プレゼンス サーバ

プレゼンス サーバは、Expressway が権限を持つ SIP ドメイン内のすべてのプレゼンティティのプレゼンス情報を管理します。

- *[有効（Enabled）]*：ローカル プレゼンス サーバが有効になっている場合、ローカル Expressway が権限を持つ SIP ドメインを対象とする PUBLISH メッセージを処理します。ほかのすべての PUBLISH メッセージが、Expressway の SIP ルーティング ルールに従ってプロキシ経由で送信されます。

  （注） SIP ルートは CLI のみを使用して設定されます。

  - プレゼンスサーバは、受信したメッセージが事前認証されている必要があります（プレゼンスサーバは独自の認証チャレンジを実行しません）。PUBLISH メッセージを受信するサブゾーンの**認証ポリシー**が *[クレデンシャルのチェック]* または *[認証済みとして扱われる]* に設定されている場合は、メッセージが拒否されます。

- *[無効（Disabled）]*：ローカルプレゼンスサーバが無効になっている場合、Expressway はローカルに設定されているコール ルーティング プロセス ルールに従って、1 つ以上のネイバーゾーンにすべての PUBLISH メッセージをプロキシ送信します。ローカル Expressway は、プレゼンティティのドメインに権限があるかどうかに関係なく、これを実行します。これらのネイバーのいずれかにそのドメインの権限があり、そのネイバーでプレゼンスサーバが有効になっている場合、そのネイバーがプレゼンティティのプレゼンス情報を提供します。

プレゼンス サーバが有効になっているかどうかに関係なく、Expressway は次の送信元のいずれかから送信されている場合は PUBLISH メッセージを受信し続けます。

- プレゼンスをサポートするローカルに登録されたエンドポイント
- ローカル PUA（有効になっている場合）
- リモートの SIP プロキシ

（注） プレゼンスサーバは、**Starter Pack** のオプションキーがインストールされている場合は自動的に有効になります。

推奨事項

- **Expressway-E と Expressway-C**：Expressway-E が Expressway-C のトラバーサル サーバとして機能する場合に推奨される設定は、Expressway-E 上で PUA を有効にしてプレゼンス サーバを無効にし、Expressway-C 上でプレゼンス サーバを有効にすることです。これにより、PUA によって生成されるすべての PUBLISH メッセージが確実に Expressway-C にルーティングされます。
- **Expressway ネイバー**：複数の Expressway が互いに隣接する導入環境では、ドメインごとに 1 つのプレゼンス サーバのみを有効にすることを推奨します。これにより、ネットワーク内のすべてのプレゼンティティの情報の中心的なソースが確保されます。
- **Expressway クラスタ**：クラスタ内でのプレゼンスの機能についての情報。

（注） 定義されている検索前トランスフォーメーションについても、プレゼンス サーバが処理するパブリケーション、サブスクリプション、および通知の URI に適用されます。

B2BUA（バックツーバック ユーザ エージェント）の概要

B2BUA は SIP コールの両方のエンドポイントの間で動作し、2 つの独立したコール レッグに通信チャネルを分離します。プロキシ サーバとは異なり、B2BUA は処理するコール状態を完全に維持します。コールの両方のレッグは「**コール ステータス（Call status）**」ページと「**コール履歴（Call history）**」ページ上に別個のコールとして表示されます。

B2BUA インスタンスは Expressway でホストされます。これらは次のシナリオで使用されます。

- メディア暗号化ポリシーの設定を適用する場合。この用途では、明示的な B2BUA 設定は必要ではありません。
- ICE メッセージング サポートの設定をサポートする場合。必要になる B2BUA 関連の設定は、ICE コールをサポートするために必要な一連の B2BUA TURN サーバの設定を定義することだけです。
- Expressway と Microsoft SIP ドメインの間の SIP コールをルーティングする場合。これには、Microsoft 相互運用性の設定と B2BUA で使用可能な B2BUA TURN サーバの設定のセットの手動設定が必要です。

B2BUA TURN サーバの設定

[アプリケーション（Applications）] > [B2BUA] > [B2BUA TURN サーバ（B2BUA TURN servers）] の順に移動し、Expressway B2BUA インスタンスに必要な TURN サーバの詳細を入力します。このページには、現在設定されている TURN サーバのリストが表示されます。このページで TURN サーバを作成、編集、削除できます。

B2BUA は、使用可能なすべてのサーバ間でのランダムなロード バランシングを介して提供する TURN サーバを選択します。B2BUA が選択できるように設定できるサーバの数に制限はありません。

TURN サーバは、ゾーンまたはサブゾーンで有効になっているときに ICE メッセージング サポートの設定用の B2BUA インスタンスによって自動的に使用されます。

Microsoft 相互運用性に TURN サーバを使用するには、**[TURN サービスを提供（Offer TURN services）]** を有効にする必要があります（Microsoft 相互運用性の設定を参照してください）。

表 *22 : TURN* サーバ設定の詳細

フィールド	説明
TURN サーバ アドレス（TURN server address）	ICE コールを確立する（Microsoft Edge などで）ときに提供する TURN サーバの IP アドレス。 TURN サーバは、Expressway-E TURN など、RFC 5245 対応である必要があります。
TURN サーバ ポート（TURN server port）	TURN サーバのリスニング ポート。
Description	自由形式の TURN サーバの説明。
TURN サービス ユーザ名（TURN services username）と TURN サービス パスワード（TURN services password）	TURN サーバへのアクセスに必要なユーザ名とパスワード。

Microsoft の相互運用性について

Expressway の Microsoft との相互運用性は、Expressway と Microsoft Skype for Business の間の SIP コールを処理するバックツーバック ユーザ エージェント（B2BUA）に基づいています。

（注） バージョン X8.9 では、Expressway の B2BUA を使用せずに Microsoft のインフラストラクチャと相互運用できます。代わりに、セッション分類検索ルールを使用して、トランスコードをする Cisco Meeting Server にコールをルーティングできます。Expressway 設定ガイドのページに用意されている『*Cisco Meeting Server with Cisco Expressway Deployment Guide*』（旧称『*Cisco ExpresswayTraffic Classification Deployment Guide*』）。

機能

- Microsoft ICE と、シスコのコラボレーション エンドポイントとブリッジの標準ベースのメディアとの間のインターワーク。
- Microsoft クライアントを使用したコールに対するコール保留、コール転送、Multiway のサポート。また、FindMe プレゼンス情報を Microsoft インフラストラクチャと共有できます。
- Microsoft クライアントの画面共有（RDP）の H.264 へのトランスコーディング
- Microsoft SIP からのメッセージングおよびプレゼンスのトラフィックをフィルタリングし、Expressway の音声/ビデオ トラフィックを処理しながら、適切なサーバ、たとえば IM and Presence Service ノードへリダイレクトします。

設定の概要

- 専用の Expressway の Microsoft 相互運用性サービスの選択。
- *Microsoft* 相互運用性キーの追加。
- Microsoft 相互運用性の設定。
- B2BUA の信頼できるホストの設定（シグナリング メッセージを B2BUA に送信できるデバイス）
- B2BUA TURN サーバの設定。（ICE コールを確立するときに B2BUA が使用可能な TURN サーバ）。
- 自動的に設定の設定されたゾーンを介して、Microsoft ドメイン、B2BUA にコールをルーティングするための検索ルールの設定。

  B2BUA を有効にすると、Expressway は自動的に **To Microsoft destination via B2BUA** と呼ばれる構成不可能なネイバーゾーンを作成します。このゾーンは検索ルールの対象にする必要があります。

  このゾーンは B2BUA を無効にしても自動的に削除されません。また、X8.8 へのアップグレード時にこのゾーンがあると古いゾーン名（To Microsoft Lync Server via B2BUA）が存続されます。
- 必要に応じて、Microsoft 相互運用性サービスの再起動サービスを再起動する必要がある場合にシステムが通知します。

Microsoft 相互運用性オプション キーが必要になる理由

Expressway を使用して Microsoft コラボレーションのインフラストラクチャと標準ベースのインフラストラクチャ間のトラフィックを変更する場合に、Expressway-C で（Expressway-C がクラスタ化されている場合は各ピアで）このキーが必要です。次の内容が含まれています。

- Microsoft SIP から標準 SIP コールへのインターワーキング
- 画面共有のトランスコーディング（RDP から BFCP の H.264）
- Microsoft SIP メッセージとプレゼンスの転送（SIP ブローカ）

変更せずに Microsoft のトラフィックをルーティングするために Expressway を使用する場合はこのキーは不要です。たとえば、Cisco Meeting Server がインターワーキングする Microsoft のさまざまな SIP トラフィックを送信するために Expressway の検索ルールを使用する場合です。

機能および制限事項

- 最大同時コール能力は 100 コールです（大規模システムを含む）。コール数が 75 に制限される M5 ベースの小規模システムについては、例外となります。
- 外部トランスコーダ経由でルーティングされたコールは 2 つのコールとしてカウントします。
- コールが Microsoft 相互運用性 B2BUA を通じてルーティングされる場合、B2BUA は常にメディアを取得し、常にシグナリング パスに留まります。B2BUA を通じてルーティングしたコール コンポーネントは、コンポーネント タイプが *Microsoft* 相互運用性であるため、コール履歴の詳細情報で特定できます。
- Microsoft 相互運用性サービスは、エンドポイントと Expressway 間のコール レッグが必要とする追加コール ライセンスを超えて消費しません。
- 設定されたすべての外部トランスコーダがそれらのキャパシティの上限に達した場合、通常はトランスコーダを介してルーティングされるコールが失敗します。コールは通常に接続されますが、トランスコードされません。
- 複数の TURN サーバを Microsoft 相互運用性サービスと共に使用できます。TURN サーバは、Microsoft Edge サーバを通過するコールに必要です。
- エンドポイントと B2BUA 間のコール レッグを制御するために帯域幅を適用できますが、B2BUA と Microsoft のインフラストラクチャ間のコール レッグにはできません。ただし、B2BUA は受信したメディアを何の操作せずに転送するため、Expressway から B2BUA のレッグに適用する帯域幅制御が暗黙的に B2BUA から Microsoft のレッグに適用されます。
- （「**「To Microsoft destination via B2BUA」**」という名前の）構成不可能なネイバーゾーンは、*Microsoft* 相互運用性の特殊なゾーンプロファイルを使用します。手動で設定されたゾーンにこのプロファイルを選択することはできません。

Microsoft 相互運用性の Expressway の設定に関する詳細情報

- Cisco Expressway シリーズ設定ガイドのページに用意されている、ご使用のバージョンに対応する『*Cisco Expressway IP Port Usage Configuration Guide*』を参照してください。
- Expressway 構成ガイドページの『*Cisco Expressway* および *Microsoft* インフラストラクチャ導入ガイド』を参照してください。

Microsoft 相互運用性の設定

[アプリケーション（Applications）] > **[B2BUA]** > **[Microsoft 相互運用性（Microsoft Interoperability）]** > **[設定（Configuration）]** の順に移動し、Microsoft 環境への B2BUA の接続を設定して有効にします。

次の表に、設定可能なオプションを記載します。

フィールド	説明	使用方法のヒント
[設定（Configuration）] セクション：		
Microsoft 相互運用性（Microsoft interoperability）	Microsoft 相互運用性サービスを有効または無効にします。	
接続先アドレス（Destination address）	ハードウェア ロード バランサ、ディレクタ、または Expressway がシグナリング メッセージを送信するフロントエンドプロセッサの IP アドレスまたは完全修飾ドメイン名（FQDN）。	また、B2BUA の信頼できるホストの設定の IP アドレスも設定する必要があります。これらはシグナリング メッセージを Expressway に送信する可能性がある Microsoft システムです。
リスニング ポート（Listening port）	ハードウェア ロード バランサ、ディレクタ、または Expressway がシグナリング メッセージを送信するフロントエンドプロセッサの IP ポート。	
シグナリング トランスポート（Signaling transport）	Microsoft インフラストラクチャへの接続に使用するトランスポート タイプ。デフォルトは、[TLS] です。	
[FindMe 統合（FindMe integration）] セクション：		

フィールド	説明	使用方法のヒント
FindMe ユーザをクライアントとして Microsoft サーバに登録（Register FindMe users as clients to Microsoft server）	コールを FindMe エイリアスに転送したり、FindMe プレゼンス情報を共有したりできるように FindMe ユーザを Microsoft レジストラに登録するかどうかを制御します。デフォルトは [はい（Yes）] です。	この機能は FindMe が有効になっている場合にのみ適用されます。 （注） FindMe ID が Active Directory で有効なユーザである場合のみ FindMe ユーザを Microsoft インフラストラクチャに登録できます（同様に Microsoft クライアントが登録できるのは、所有している有効なアカウントが AD で有効な場合に限ります）。
Microsoft ドメイン（Microsoft domain）	Microsoft サーバで 使用されている SIP ドメイン。Expressway 上にすでに設定されている ドメインの設定のいずれかを選択する必要があります。	このドメインの FindMe の名前のみが Microsoft サーバに登録されます。
[リモート デスクトップ プロトコル（Remote Desktop Protocol）] セクション：		
この B2BUA に対して RDP トランスコーディングを有効化	B2BUA がリモートデスクトッププロトコルのトランスコーディングを提供するかどうかを制御します。 この機能には **Microsoft 相互運用性**のオプション キーが必要です。 デフォルトは [いいえ（No）] です。	Microsoft クライアント ユーザにシスコ コラボレーション エンドポイント/会議の参加者との画面共有を可能にするには、このオプションを有効にする必要があります。
[SIP ブローカ（SIP broker）] セクション：		
着信 SIP のブローカを有効化（Enable broker for inbound SIP）	SIP ブローカを切り替え、宛先プレゼンスサーバのリストを開きます。 ブローカは Microsoft SIP を検査し、SIP SIMPLE をユーザが入力する IM and Presence Service ノードにルーティングします。	ブローカが有効でない場合、B2BUA は Microsoft からのすべての着信 SIP の処理を試行します。SIP SIMPLE を受信すると、SIP 音声/ビデオ トラフィックであるかのようにルーティングしようとします。この状況ではおそらく、SIP SIMPLE はコール制御インフラストラクチャによって拒否されます。

フィールド	説明	使用方法のヒント
プレゼンスの宛先サーバのリスニングポート（Listening port on presence destination servers）	これは IM and Presence Service ノードに設定されているポートです。	
宛先プレゼンス サーバ 1 ～ 6（Destination presence server 1..6）	IM and Presence Service ノードの IP アドレス、ホスト名、または FQDN。	最大 6 つ入力します。Expressway は活性状態を判別するためにこれらを定期的にポーリングし、ラウンドロビン アルゴリズムを使用してこれらにトラフィックをルーティングします。
TURN セクション：		
TURN サービスを提供（Offer TURN services）	B2BUA が TURN サービスを提供するかどうかを制御します。デフォルトは [いいえ（No）] です。	Microsoft Edge サーバを通過するコールに推奨されます。 関連付けられた TURN サーバを設定するには、[B2BUA TURN サーバの設定（Configure B2BUA TURN servers）]B2BUA TURN サーバの設定 をクリックします。
[詳細設定（Advanced settings）]：シスコ カスタマー サポートのアドバイスがあった場合にのみ、高度な設定を変更してください。		

フィールド	説明	使用方法のヒント
暗号化	B2BUA が暗号化されたコール レッグと暗号化されていないコール レッグをどのように処理するかを制御します。 *[必須（Required）]*：コールの両方のレッグを暗号化する必要があります。 *[自動（Auto）]*：暗号化と非暗号化の組み合わせをサポートします。 デフォルトは [自動（Auto）] です。	B2BUA を介したコールには 2 つのレッグがあります。1 つは B2BUA から標準的なビデオ エンドポイントへのレッグ、もう 1 つは B2BUA から Microsoft クライアントへのレッグです。コールのどちらのレッグも暗号化することも、暗号化しないこともできます。 *[自動（Auto）]* に設定すると、暗号化されたコール レッグと暗号化されていないコール レッグのどのような組み合わせでもコールは確立できます。したがって、コールの一方のレッグを暗号化し、もう一方は暗号化しないこともできます。
B2BUA メディア ポート範囲の開始/終了（B2BUA media port range start/end）	メディアを処理するために B2BUA が使用するポート範囲。	このポート範囲は、この Expressway またはこの Expressway の TURN サーバが使用する他のポート範囲と重複しないことを確認してください。 デスクトップの共有によってコールごとに必要となるメディア ポートの数が増えるため、[この B2BUA に対して RDP トランスコーディングを有効化する（Enable RDP transcoding for this B2BUA）] を有効にしている場合はこの範囲も拡大する必要があります。
ホップ カウント（Hop count）	SIP メッセージに使用する最大転送値を指定します。デフォルトは 70 です。	
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。

フィールド	説明	使用方法のヒント
最小セッション更新間隔（Minimum session refresh interva）	B2BUA コールのセッション更新間隔を VCS 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。
Expressway 通信用の B2BUA のポート（Port on B2BUA for Expressway communications）	Expressway と通信するために B2BUA で使用するポート。	
Microsoft コール通信用の B2BUA のポート（Port on B2BUA for Microsoft call communications）	Microsoft サーバとのコール通信に B2BUA で使用するポート。デフォルトは 65072 です。	
RDP TCP ポート範囲の開始/終了（RDP TCP port range start/end）	トランスコーダ インスタンスが RDP メディアをリッスンする TCP ポートの範囲を定義します。デフォルトは 6000 ～ 6099 です。 （注） ページを保存し、Microsoft 相互運用性サービスを再起動して変更を適用します。	B2BUA で作成された各同時 RDP トランスコーディング セッションには受信ポートが必要です。考えられる同時トランスコード セッションの最大数が 100 であるため、範囲は 100 までに制限されます。
RDP UDP ポート範囲の開始/終了（RDP UDP port range start/end）	トランスコーダ インスタンスが H.264 メディアを送信する UDP ポートの範囲を定義します。デフォルトは 6100 ～ 6199 です。 （注） ページを保存し、Microsoft 相互運用性サービスを再起動して変更を適用します。	B2BUA で作成された各同時 RDP トランスコーディング セッションには、結果の H.264 メディアを送信するためのポートが必要です。考えられる同時トランスコード セッションの最大数が 100 であるため、範囲は 100 までに制限されます。

フィールド	説明	使用方法のヒント
最大 RDP トランスコードセッション数（Maximum RDP transcode sessions）	この Expressway 上での同時 RDP トランスコーディングセッション数を制限します。デフォルト値は 10 です。 （注） ページを保存し、Microsoft 相互運用性サービスを再起動して変更を適用します。	値が高いほど TDP トランスコーディングによってより多くのシステム リソースが消費され、他のサービスに影響が及ぶ可能性があります。最大値は 100 です。 推奨される最大 RDP トランスコードセッション： • 中規模の OVA システム：10 • 大型の OVA/CE1200 システム：20（X8.10 では、大規模システム用に 10 ギガビット NIC を使用する必要がなくなりました。帯域幅制約によっては、1 Gbps の NIC で大規模システムの容量を達成することが可能です。）

B2BUA の信頼できるホストの設定

[アプリケーション（Applications）] > [B2BUA] > [Microsoft 相互運用性（Microsoft Interoperability）] > [信頼できるホスト（Trusted hosts）] に移動し、Expressway が SIP シグナリングを信頼する Microsoft ホストを指定します。

相互運用性サービスは、信頼できるホストのリストにないアドレスからのメッセージは受け入れません。

（注） 信頼できるホスト検証は、Expressway ビデオ ネットワークにインバウンドされる Microsoft クライアントによって開始されるコールにのみ適用されます。コールの開始が Expressway のビデオ ネットワークからのみの場合は、信頼できるホストを設定する必要はありません。

Expressway には現在、25 という信頼できるホスト数の公称制限があります。信頼できるホストが 25 を超えていると、Expressway でアラームが発生します。

実際には、導入環境に必要な場合、25 を超えて信頼できるホストを設定できます。この数を 50 未満に保って、アラームを安全に無視できるようにすることを推奨します。50 を超える必要がある場合は、異なる Gateway Expressway を追加することを推奨します。

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
名前（Name）	オプションの自由形式の信頼できるホストの説明。	名前は「「信頼」」条件の一部としては使用されません。IP アドレスに依存せず複数のホストを区別しやすくするためだけのものです。
IP address	信頼できるホストの IP アドレス。	
タイプ（Type）	B2BUA にシグナリング メッセージを送信するデバイスのタイプ。 *[Microsoft インフラストラクチャ（Microsoft infrastructure）]*：ハードウェ ロードバランサ、ディレクタ、およびフロントエンド プロセッサなど	

Microsoft 相互運用性サービスの再起動

再起動を行い、Microsoft 相互運用性サービスに変更を適用する必要があることがあります。再起動を必要とするとシステムによってアラームが表示されます。

このサービスを再起動すると、Expressway は再起動しませんが、B2BUA によって管理されているコールはすべてドロップします。

手順

ステップ 1 **[アプリケーション（Applications）] > [B2BUA] > [Microsoft 相互運用性（Microsoft Interoperability）] > [サービスの再起動（Restart service...）]** に移動します

ステップ 2 現在実行されているアクティブなコールの数を確認します。

ステップ 3 [再起動（Restart）] をクリックします。

数秒後にサービスが再起動します。Microsoft 相互運用性の設定ページでサービス ステータスを確認できます。

クラスタ化された Expressway システム

すべてのピアの Microsoft 相互運用性サービスを再起動する必要があります。他のピアのサービスを再起動する前に、プライマリのサービスを設定し、再起動し、確認します。

FindMe について

FindMe はユーザ ポリシーの形式を取り、Expressway がコールを受信したときに特定のユーザまたはグループ宛のコールがどうなるかを決定する一連のルールです。

FindMe 機能によって、企業内の個人またはチームに単一の FindMe ID を割り当てることができます。FindMe アカウントにログインすることで、ユーザは「在宅中」や「社内」などのロケーションのリストをセットアップしてユーザのデバイスとそれらの場所とを関連付けることができます。次に、ユーザは FindMe ID をダイヤルしたときにどのデバイスをコールするかを指定し、それらのデバイスがビジーであったり、応答がない場合にどうするかを指定できます。各ユーザは最大 15 台のデバイスと 10 か所の場所を指定できます。

つまり、コールをする可能性がある発信者には単一の FindMe エイリアスを付与し、そのエイリアスで企業内の個人またはグループに接続できます。発信者は個人またはグループが応答できるすべてのデバイスの詳細を知る必要はありません。

この機能を有効にするには、デスクトップ システムまたは TelePresence Room システム登録ライセンスを購入し、インストールする必要があります。

エンドユーザの FindMe アカウント設定

ユーザは、Cisco TMS プロビジョニングを使用して FindMe の設定を構成できます。TMS プロビジョニングが有効な場合、ユーザは FindMe アカウントを使用して Cisco TMS にログインして、FindMe の設定を管理します。ユーザ アカウントと FindMe データは、TMS プロビジョニング拡張サービスの設定 サービスによって Cisco TMS から Expressway に提供されます。

FindMe アカウントのセットアップに関する詳細については『FindMe 導入ガイド』を参照してください。

デバイスの指定方法

FindMe アカウントの設定時に、ユーザは FindMe ID へのコールをルーティングするデバイスを指定するように求められます。

エイリアスを指定したり、他の FindMe ID を 1 つ以上のデバイスとして指定することもできます。ただし、このような場合は循環設定を回避するように注意する必要があります。

そのため、デバイスを登録したエイリアスを入力して FindMe ID をコールしたときに呼び出す物理的なデバイスをユーザが指定することを推奨します。

プリンシパル デバイス

FindMe ユーザのアカウントは 1 つ以上のプリンシパル デバイスで設定する必要があります。これらは、そのアカウントに関連付けられたメイン デバイスになります。

ユーザは、プリンシパルデバイスのアドレスを削除または変更できません。これは、基本的な FindMe 設定をユーザが誤って変更することがないようにするためです。

また、プリンシパルデバイスは Expressway が使用し、同じデバイス アドレスが複数の FindMe ID に関連付けられている場合に、どの FindMe ID を**発信者 ID** として表示するかを決定します。管理者（FindMe ユーザ自身ではない）のみが、FindMe ユーザのどのデバイスがプリンシパル デバイスかを設定できます。

FindMe プロセスの概要

Expressway が特定のエイリアス宛のコールを受信すると、ユーザ ポリシーを次のように適用します。

- 最初に、FindMe が有効になっているかどうかを確認します。有効になっている場合は、エイリアスが FindMe ID であるかを確認します。そうであった場合は、そのユーザの FindMe 設定のアクティブな場所に関連付けられたエイリアスにコールを転送します。
- FindMe が有効になっていないか、またはエイリアスが FindMe ID でなかった場合は、Expressway は通常の方法でエイリアスの検索を続行します。

（注） ユーザポリシーは Expressway に設定されているコールポリシーが適用された後に呼び出されます。詳細については 、コール ルーティング プロセスを参照してください。

FindMe 導入時の推奨事項

- FindMe ID は URI 形式であり、個人のプライマリ URI である必要があります。
- エンドポイントは既存の FindMe ID と同じエイリアスで登録しないでください。これを防ぐには、拒否リストのすべての FindMe ID を含めます。

例

Example Corp. のユーザは、FindMe ID の形式**john.smith@example.com**を使用しています。ユーザの各エンドポイントは、その物理的な場所を特定するために若干異なるエイリアスで登録されています。たとえば、オフィス エンドポイントは形式**john.smith.office@example.com**でエイリアスに登録され、ホームエンドポイントは**john.smith.home@example.com**として登録されます。

両方のエンドポイントが、FindMe ID がダイヤルされたときに呼び出すデバイスのリストに含まれています。エイリアス**john.smith@example.com**が拒否リストに追加され、個々のエンドポイントがそのエイリアスに登録されるのを防ぐためです。

FindMe の設定

「FindMe の設定（FindMe configuration）」ページ（**[アプリケーション（Applications）] > [FindMe]**）を使用して FindMe についてを有効にして設定します。

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
FindMe モード（FindMe mode）	FindMeが有効かどうかと、サードパーティ製のマネージャを使用するかどうかを決定します。 *Off*：FindMe を無効にします。 *[リモートサービス（Remote service）]*：FindMe を有効にし、オフボックスシステム（TMS など）にある FindMeマネージャを使用します。	コール ポリシーの設定は、FindMe モードに関係なく、常に適用されます。 FindMe を有効にした場合、**クラスタ名**が指定されていることを確認する必要があります（これは、クラスタの管理 ページで行います）。
発信者 ID（Caller ID）	着信コールの発信元が呼び出し先にどのように表示されるかを決定します。 *[着信 ID（Incoming ID）]*：コールが発信されたエンドポイントのアドレスを表示します。 *[FindMe ID]*：発信エンドポイントのアドレスに関連付けられた FindMe ID を表示します。	*FindMe ID* を使用すると、受信者が受信後にそのコールを返した場合は FindMe デバイス アカウントに関連付けられたすべてのデバイスがコールされます。 FindMe ID は送信元エンドポイントが認証されている（または認証済みとして処理されている）場合にのみ表示されます。認証されていない場合、着信 ID が表示されます。詳細については、デバイス認証について（237ページ）を参照してください。

次のオプションは、**[FindMe モード（FindMe mode）]** が *[リモート サービス（Remote service）]* の場合に適用されます。

フィールド	説明
プロトコル（Protocol）	リモート サービスに接続するために使用するプロトコル。
アドレス（Address）	リモート サーバの IP アドレスまたはドメイン名。
パス	リモート サービスの URL。
ユーザ名（Username）	リモート サービスにログインして照会するために Expressway が使用するユーザ名。
[パスワード（Password）]	リモート サービスにログインして照会するために Expressway が使用するパスワード。

FindMe データの管理とストレージ

FindMe を使用し、FindMe データの管理には Cisco TMS を使用する場合は、Cisco TMSPE サービスを設定して Expressway に FindMe データを提供する必要があります。

Cisco TMS プロビジョニング（FindMe を含む）

Cisco TMS プロビジョニングは、Expressway がプロビジョニング データを取得するためのメカニズムです。

- 具体的には、Expressway はこのメカニズムを使用して、エンドポイント デバイスからの Expressway プロビジョニング サーバに対し、ユーザ アカウント、デバイス、電話帳のデータを提供します。
- また、Expressway は FindMe についてを提供するために使用する FindMe アカウントの設定データもこのメカニズムによって取得します。

TMS プロビジョニング サービスを有効にする方法

X8.11 以降、新しいシステムでは Expressway 内の TMS プロビジョニング サービスはデフォルトで無効にされます（既存のシステムを X8.11 以降にアップグレードする場合は、現在の設定が保持されます）。TMS プロビジョニング サービスを有効にするには、次の手順に従います。

（注） プロビジョニングは Cisco Expressway-C と Cisco Expressway-E の両方でサポートされていますが、Cisco Expressway-C と Cisco Expressway-E をペアにした導入環境では Cisco Expressway-C 上で使用することを推奨します。

1. （1 回限り）プロビジョニング サービスがまだ有効にされていない場合、Expressway で次の操作を行って、プロビジョニング サービスを有効にする必要があります。
   1. **[システム（System）]** > **[管理（Administration）]** に移動します。
   2. **[サービス（Services）]** エリアで、**[プロビジョニング サービス（Provisioning services）]** を *[オン（On）]* に設定します。

      これにより、インターフェイスで **[システム（System）]** > **[TMS プロビジョニング拡張サービス（TMS Provisioning Extension services）]** のページにアクセスできるようになります。このページから、Cisco TelePresence Management Suite Provisioning Extension（Cisco TMSPE）とユーザ、デバイス、FindMe、電話帳のプロビジョニング サービスに接続できます。
2. **[システム（System）]** > **[TMS プロビジョニング拡張サービス（TMS Provisioning Extension services）]** に移動します。
3. Cisco TMSPE の接続詳細を指定します（詳細については、TMS プロビジョニング拡張サービスの設定を参照してください）。

4. 1 つ以上のプロビジョニング サービス（ユーザ、デバイス、FindMe、電話帳）を有効にします。各サービスについて、次の操作を行います。
   1. **[このサービスに接続（Connect to this service）]** を *[はい（Yes）]* に設定します。
   2. **[ポーリング間隔（Polling interval）]** または **[接続（Connection）]** のデフォルト値を使用しない場合は、必要に応じて値を設定します。

      [デバイス（Devices）] には、[基本グループ（Base Group）] を指定する必要があります。Cisco TMSPE 内で Expressway またはクラスタを識別する ID を入力します。

クラスタとプロビジョニングのサイズの制限

あらゆる規模の Expressway クラスタでサポートされる最大値は次のとおりです。

- 10,000 個の FindMe アカウント
- 10,000 人のプロビジョニングするユーザ
- 200,000 の電話帳エントリ

（注） システムのクラスタ ライセンスの使用方法とキャパシティのガイドラインが上記の設定よりも大きい場合でも、クラスタごとの FindMe アカウント/ユーザ数は 10,000、プロビジョニングできるデバイス数は 10,000 に制限されます。

10,000 を超えるデバイスをプロビジョニングする必要がある場合、ご使用のネットワークには、適切に設計され、ダイヤル プランが設定された追加の Expressway クラスタが必要になります。

Cisco TMS と Expressway でのプロビジョニングの設定方法の詳細については、『Cisco TMS プロビジョニング拡張導入ガイド』を参照してください。

プロビジョニングに使用される Cisco TMSPE サービス

TMS プロビジョニングが有効になっている場合、Expressway は（Cisco TMS 上でホストされる）次の Cisco TMSPE サービスを使用して Expressway または Expressway クラスタにデータを提供します。

サービス	説明
ユーザ設定	Expressway が特定のユーザに適用される設定値を使用してデバイスを設定するためのデータを提供します（ユーザは基本的に SIP URI です）。Jabber Video などのデバイスはこのサービスを使用して完全に設定されます。また、TURN サーバ（通常は Expressway-E）への接続詳細も提供します。

サービス	説明
FindMe	各 FindMe ID に関連付けられているロケーションとデバイスをはじめ、ユーザの FindMe アカウントの詳細を提供します。これにより、Expressway はユーザ ポリシーを適用したり、発信者の送信元アドレスを対応する FindMe ID に変更したりできます。
電話帳	ユーザが電話帳で連絡先を検索するために使用するデータを提供します。電話帳へのアクセスは、（Cisco TMS 内に）定義されているアクセス コントロール リストに従ってユーザ単位で制御されています。
デバイス	Expressway と Cisco TMS 間でプロビジョニング ランセンス情報を交換します。情報は 30 秒ごとに交換されます。Cisco TMS が管理している Expressway クラスタの範囲で使用可能な無償ライセンスの現在の数が Expressway に提供され、Expressway はその Expressway（または Expressway クラスタ）が使用しているプロビジョニング ライセンスのステータスで Cisco TMS を更新します。 デバイス サービスがアクティブになっていない場合は、Expressway のプロビジョニング サーバはデバイスをプロビジョニングできません。

Cisco TMSPE サービスのステータス情報

サービスのステータス情報は、TMS Provisioning Extension サービスのステータス ページに表示されます。

- Expressway は定期的に Cisco TMSPE サービスをポーリングし、Expressway に保持されているデータが最新の状態に維持されるようにします。ポーリング間隔はサービスごとに定義できます。通常の導入環境では、FindMe とユーザ プロビジョニングのデータを頻繁（2 分ごと）に更新し、電話帳のデータを毎日更新するデフォルトの設定を使用することを推奨します。

  クラスタ化された Expressway では、クラスタ ピアのいずれか 1 つのみが Cisco TMS との物理接続を維持します。Cisco TMS から取得されたデータは Expressway クラスタの複製メカニズムを通じてクラスタ内の他のピア間で共有されます。

- Expressway と Cisco TMS 間のデータの即時再同期は、いつでも行うことができます。それには、**「TMS プロビジョニング拡張サービス（TMS Provisioning Extension services）」** ページで **[完全同期の実行（Perform full synchronization）]** をクリックします。これにより、データが削除されて完全に更新されるまでの数秒間、Expressway 上でサービスが停止します。Cisco TMS 内での最近の更新のみを Expressway に適用する場合は、別の方法として、**[更新の確認（Check for updates）]** をクリックしてください。

Cisco TMSPE サービスの設定の変更

Cisco TMSPE サービスの設定を変更するには、Cisco TMS を使用することを強く推奨します。Expressway でもサービスを設定できますが（**「TMS プロビジョニング拡張サービス**

（**TMS Provisioning Extension services**）」ページ）、このページで行った変更は **Cisco TMS** で適用されません。

Expressway プロビジョニング サーバ

デバイス プロビジョニングが有効にされている場合、Expressway プロビジョニング サーバは Cisco TMS プロビジョニング（FindMe を含む）メカニズムを通じて Cisco TMS が提供したデータを使用して、プロビジョニング関連のサービスをプロビジョニング済みのデバイスに提供します。

Expressway はプロビジョニング データと FindMe データの Expressway への提供に Cisco TelePresence Management Suite Provisioning Extension（Cisco TMSPE）サービスのみをサポートしています。このモードでは、すべてのプロビジョニング データと FindMe データは、Cisco TMS 内のみで管理、維持されます。

プロビジョニング ライセンス

プロビジョニング サーバが同時にプロビジョニングできるデバイスの数には制限があります。Expressway と Cisco TMS は、Cisco TMSPE デバイス サービスを通じて情報を交換することで使用可能なプロビジョニング ライセンスの数を管理します。デバイス サービスがアクティブになっていない場合は、Expressway のプロビジョニング サーバはデバイスをプロビジョニングできません。

Cisco TMS が管理している Expressway クラスタの範囲で使用可能な無償ライセンスの現在の数が Expressway に提供され、Expressway はその Expressway（または Expressway クラスタ）が使用しているプロビジョニング ライセンスのステータスで Cisco TMS を更新します。ライセンスの制限は、デバイス タイプごとに管理できます。

Jabber Video 4.x など、一部のデバイスはプロビジョニングをサインアウト（登録解除）するタイミングを Expressway に通知しません。Expressway は、ライセンスを解放する前に 1 時間のタイムアウト間隔を適用することで、これらのデバイスを管理します。

プロビジョニングとデバイスの認証

プロビジョニング サーバが受信するプロビジョニング要求または電話帳要求は、Expressway へのゾーンまたはサブゾーン エントリ ポイントにおいて、すでに認証されている必要があります。プロビジョニング サーバは、自分自身で認証チャレンジを行うことはありません。未認証のメッセージはすべて拒否されます。

詳細については、デバイス プロビジョニングと認証ポリシーを参照してください。

ハイブリッド サービスとコネクタの管理

ハイブリッド サービス用に Expressways を登録する場合は、ハイブリッド サービスのドキュメントを参照して、ハイブリッド サービスを初めて導入する方法を含め、詳細情報を確認してください。

ハイブリッド サービスとは何か、また、何を実行するか。

Cisco Webex ハイブリッド サービスは、内部施設ベースのソリューションを Cisco Collaboration cloud に結び付け、より優れ、より緊密に統合されたコラボレーション ユーザ エクスペリエンスを実現します。

使用できるサービス

ハイブリッドサービスを購入すると、Cisco Webex Control Hub（Cisco Webex に対する管理インターフェイス）にアクセスできるようになります。Control Hub から、各ハイブリッド サービスの導入サポートに従って、ユーザに対して機能を有効にすることができます。

必要なソフトウェア

ハイブリッドサービスのオンプレミスコンポーネントは「「コネクタ」」と呼ばれ、Expressway ソフトウェアには登録を管理する管理コネクタとその他のコネクタが含まれています。

Expressway をクラウドに登録するまでは、管理コネクタは休止状態になっています。登録すると、新しいバージョンが使用できる場合は、管理コネクタが自動的にダウンロード、インストール、アップグレードされます。

その後で、Control Hub で選択したほかのコネクタが Expressway によってダウンロードされます。これらはデフォルトでは起動しないため、動作させる前に設定する必要があります。

設定が完了すると、Control Hub で設定したソフトウェア アップグレード スケジュールに従って、コネクタが自動的にダウンロードおよびアップグレードを行います。手動による作業は必要ありません。

インストール、アップグレード、またはダウングレードの方法

コネクタは、デフォルトではアクティブ化されていないため、設定し、起動するまでは何も実行しません。これを行うには Expressway にコネクタをインストールした新しいインターフェイスのページを使用します。

コネクタのアップグレードは、Control Hub からも実行でき、アップグレードを承認したときに管理コネクタが新しいバージョンを Expressway にダウンロードします。

また、登録解除もできますが、これを行うことによって Cisco Webex から Expressway が切断され、コネクタと関連設定がすべて削除されます。

（注） 新しいフィーチャと機能を提供するために、クラウドにより提供されるサービスの開発は常に継続されていることから、ハイブリッドサービスでサポートされる Expressway の最小バージョンも変更される場合があります。ハイブリッドサービス展開が機能し続け、公式にサポートされるよう、登録している Expressways を最新の状態を維持するようにしてください。詳細については、Expressway サポート バージョンの説明を参照してください。

ハイブリッド サービスに関する詳細情報の入手先

ハイブリッド サービスは開発が進められており、Expressway よりも頻繁にパブリッシュされる場合があります。そのため、ハイブリッド サービスに関する情報はハイブリッド サービスのドキュメントで維持されており、いくつかの Expressway インターフェイス ページにはそのサイトへのリンクが備わっています。

コネクタ プロキシ

ハイブリッドサービス用にExpresswaysを登録する場合は、ハイブリッドサービスのドキュメントを参照して、ハイブリッドサービスを初めて導入する方法を含め、詳細情報を確認してください。

このプロキシの目的

この Expressway を Cisco Webex に接続するにはプロキシが必要となる場合、**[アプリケーション（Applications）]** > **[ハイブリッド サービス（Hybrid Services）]** > **[コネクタ プロキシ（Connector Proxy）]** にあるページを使用します。Expressway はこのプロキシをその他の目的には使用しません。

このプロキシを通過するトラフィックの種類

このプロキシには、アウトバウンド HTTPS とセキュアな Web ソケット接続を処理する能力が必要です。また、これらの接続は基本認証を使用するか、認証なしで Expressway が発信できる必要があります。

プロキシの設定に必要な詳細情報

プロキシのアドレス、リッスンするポート、および基本認証のユーザ名とパスワード（プロキシが認証を必要とする場合）が必要です。

Expressway-E 上の Cisco Webex CA ルート証明書

Cisco Webex クラウド CA ルート証明書は Expressway ソフトウェアにパッケージ化されています。**[証明書の取得（Get certificates）]** をクリックすると、これらの詳細書を使用して着信証明書を検証できるようになります。この決定は、**[証明書の削除（Remove certificates）]** をクリックすることで必要に応じて撤回できます。

Expressway-E はこれらの CA を信頼することで、コラボレーション クラウドのサーバ 証明書を認証して一部の Expressway ベースのハイブリッド サービスに必要な暗号化された接続を確立できます。

（注） ハイブリッドサービス用に Expressway-E を登録することはできません。Cisco Webex クラウドに登録されている Expressway（またはクラスタ）へはセキュアなトラバーサル ゾーンによって接続される必要があります。

[証明書の取得（Get certificates）] をクリックすると、次の CA のルート証明書がインストールされます。

- O = The Go Daddy Group, Inc、OU = Go Daddy Class 2 Certification Authority
- O=GoDaddy.com, Inc., CN=Go Daddy Root Certificate Authority - G2
- O = QuoVadis Limited、CN = QuoVadis Root CA 2
- O = VeriSign, Inc.、OU = Class 3 Public Primary Certification Authority
- O=thawte, Inc., OU=Certification Services Division, OU=(c) 2006 thawte, Inc. - For authorized use only, CN=thawte Primary Root CA
- O=Baltimore, OU=CyberTrust, CN=Baltimore CyberTrust Root
- O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert Global Root CA

信頼できる CA のリストを手動で管理する場合は、**[メンテナンス（Maintenance）] > [セキュリティ（Security）] > [信頼できる CA 証明書（Trusted CA certificate）]** に移動します。詳細については、信頼された CA 証明書リストの管理を参照してください。

関連資料

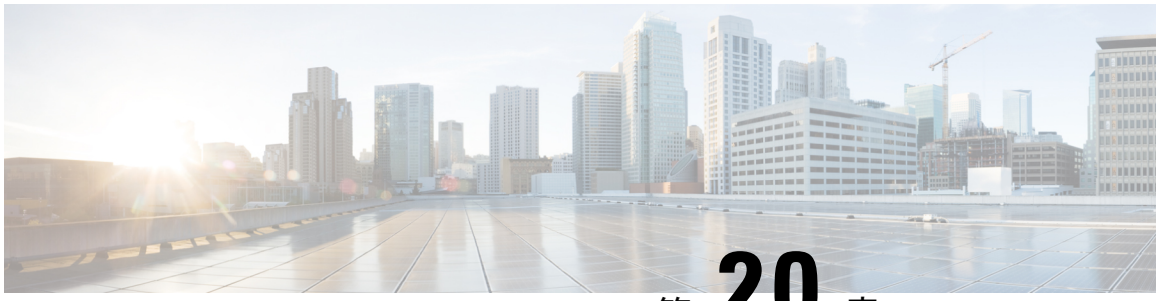
- Cisco Webex 署名 CA
- Cisco Webex でサポートされている認証局

Cisco Webex エッジ

Webex Edge Connect の使用（Expressway-C なし）

X 12.5.5 からのビジネス間のケース（MRA ではない）については、Cisco Webex Edge Audio と Webex Edge Connect 製品を使用し、Expressway-C を使用せずに正常にテストされました。したがって、Expressway-E は、Expressway-C を使用せずに Cisco Unified Communications Manager に接続します。このシナリオでは、トラバーサルやファイアウォールは必要ありません。また、Expressway E は Webex Cloud を Cisco Unified Communications Manager に直接接続します。テスト対象の構成では、Cisco Unified Communications Manager と Expressway -E の間にある近隣ゾーンで、インターネットを介した標準的な Webex Edge Audio を使用しています。Webex ゾーンのメディア暗号化モードは、「On」 である必要があります（デフォルトは「[自動（Auto）]」です）。

このシナリオでは、インバウンド接続を内部ファイアウォールで開く必要があります。そのため、通常のデュアル ファイアウォール構成の標準の Expressway デプロイはサポートされて**いません**。Webex Edge Connect で使用するためのみを目的としています。



第 20 章

ユーザ アカウント

ここでは、管理者アカウントと FindMe ユーザアカウントの設定方法と、アクティブなすべての管理者セッションと FindMe セッションの詳細の表示方法について説明します。

ユーザ アカウントについて

Expressway には通常運用用の 2 つのタイプのユーザアカウントがあります。

- **管理者アカウント**：Expressway を設定する際に使用します。
- **FindMe アカウント**：企業内の個人が FindMe プロファイルを設定する際に使用します。（Expressway が TMS プロビジョニング拡張サービスの設定を使用して FindMe データを提供している場合、Expressway を介した FindMe アカウントの構成は適用されません。）

アカウントの認証

管理者アカウントと FindMe アカウントは、Expressway へのアクセスが許可される前に認証されている必要があります。

Expressway はアカウントをローカルに、または LDAP を使用してリモート ディレクトリ サービスと照合して（現在は Windows Active Directory のみでサポート）認証することができます。また、ローカルとリモートで管理されているアカウントも使用できます。リモート オプション

を使用すると、企業内のすべての Expressway 用のディレクトリ サービスに管理者グループを設定できます。これにより、Expressway ごとに個別のアカウントを持つ必要がなくなります。

リモート認証の設定の詳細については、LDAP を使用したリモート アカウント認証の設定を参照してください。

リモートソースを管理者または FindMe アカウントのいずれかの認証に使用している場合は、Expressway を次のように設定する必要があります。

- 適切な LDAP サーバ接続の設定。
- この Expressway への管理者と FindMe のアクセスを管理するリモートディレクトリサービスにすでにセットアップ済みの対応するグループ名に一致する管理者グループまたは FindMe グループ、あるいはその両方（管理者グループの設定とユーザグループの設定を参照してください。）

また Expressway は証明書ベースの認証の設定を使用するように設定することもできます。これは通常、Expressway を安全性の高い環境に導入する場合に必要になります。

パスワードの複雑度

複雑度の要件は、パスワード セキュリティの設定 ページ（**[ユーザ（Users）]** > **[パスワードセキュリティ（Password security）]**）から、ローカルで管理されているパスワードに対して指定できます。

すべてのパスワードとユーザ名で大文字と小文字が区別されます。

アカウント タイプ

管理者アカウント

管理者アカウントを使用して Expressway を設定します。

Expressway には、完全な読み取り/書き込みアクセス権が付与されたデフォルトの **admin** アカウントがあります。これは、Web インターフェイス、API インターフェイスまたは CLI を使用して Expressway にアクセスするために使用できます。

（注） *[リモートのみ（Remote only）]* 認証ソースが使用中の場合は、デフォルトの **admin** アカウントを使用して Expressway にアクセスすることはできません。

Web インターフェイスと API インターフェイスのみを使用して Expressway にアクセスできるようにするには、新たにローカル管理者アカウントを追加します。

リモートで管理する管理者アカウントを使用すると、Web インターフェイスと API インターフェイスのみを使用して Expressway にアクセスすることもできます。

1つの管理者アカウントを緊急時アカウントに設定できます。この特殊なアカウントは、リモート認証ができない場合にローカル認証が許可されないときでも Expressway にアクセスできます。

設定ログ

設定ログには、すべてのログイン試行と、Webインターフェイスを使用して行われた設定変更が記録されます。これらは監査証跡に使用できます。これは、複数の管理者アカウントがあるときに特に役立ちます。

複数の管理セッション

複数の管理者セッションを同時に実行できます。これらのセッションは、Webインターフェイス、コマンド ライン インターフェイス、またはその両方を組み合わせて使用していることがあります。これにより、各管理者セッションで同じ設定を変更しようとすると、1つのセッションに加えた変更によりもう1つのセッションに加えた変更が上書きされることにご注意ください。

セッションの制限とタイムアウト

ネットワーク サービスの説明に従って、アカウントセッションの制限と非アクティブタイムアウトを設定できます。

ログイン履歴ページ（高度なアカウントセキュリティ）

システムが高度なアカウントセキュリティモードになっている場合はログインした直後に「**ログイン履歴（Login history）**」ページが表示されます。このページには、現在ログインしているアカウントの最新の履歴が示されます。

FindMe アカウント

企業内の個人が FindMe アカウントを使用して、それらの個人が FindMe ID を通じて接続できるデバイスと場所を設定します。

各 FindMe アカウントには、ユーザ名とパスワードを使用してアクセスします。

- リモート FindMe アカウント認証を選択した場合は、Expressway 管理者はリモート ディレクトリ サービスの対応するグループ名と照合するように FindMe グループをセットアップする必要があります。

  （注） ユーザ名とパスワードの詳細のみリモートで管理されます。

- FindMe ID、デバイス、および場所などの FindMe アカウントのその他プロパティはローカル Expressway データベースに保存されます。

FindMe アカウントの詳細と、関連付けられた FindMe デバイスと場所の定義の詳細については、FindMe の設定セクションを参照してください。

多くの FindMe アカウントのプロビジョニングが必要な場合は、Cisco TMS を使用することを推奨します。FindMe アカウントとユーザ アカウントの設定の詳細については、『Cisco TMS プロビジョニング拡張導入ガイド』を参照してください。

root アカウント

Expressway は Expressway オペレーティング システムへのログインに使用できる root アカウントを提供します。通常の運用では **root** アカウントを使用しないでください。特に、このアカウントを使用してシステム設定を行わないでください。代わりに管理者のアカウントを使用します。

詳細については、root アカウントの使用の項を参照してください。

注意 **admin** および **root** アカウントの X8.9 より前のデフォルトのパスワードはよく知られています。これらのアカウントには強力なパスワードを使用する必要があります。新しいシステムが X8.9 以降である場合は、スタートアップ時にデフォルト以外のパスワードを指定する必要があります。

詳細情報

管理者アカウントの設定を参照してください。

パスワード セキュリティの設定

「パスワード セキュリティ（Password security）」ページ（**[ユーザ（Users）]** > **[パスワード セキュリティ（Password security）]**）は、ローカルアカウントのパスワードが承認される前に最小レベルの複雑さを満たす必要があるかどうかを制御します。

- **[厳格なパスワードを適用（Enforce strict passwords）]** が *[オン（On）]* に設定されている場合、その後に設定される対象となるアカウントのパスワードはすべて、厳密なパスワードを構成するための以下のルールに従う必要があります。
- **[厳密なパスワードを強制する（Enforce strict passwords）]** が *[オフ（Off）]* に設定されている場合、パスワードに対して追加のチェックは行われません。デフォルトはオフです。

生成されたパスフレーズのエントロピーの最小ビット数も、このページで 0ー255 の範囲で構成できます（デフォルトは6）。

（注） この設定に関係なく、管理者アカウントに対して空のパスワードを設定することはできません。

厳格なパスワードの範囲

厳格なパスワードの適用設定は、Expressway で管理されているローカルアカウントにのみ適用されます。

- ローカル管理者アカウント
- ローカル FindMe ユーザアカウント
- ローカル認証データベース クレデンシャル（他のデバイスが Expressway での認証を求められている場合に使用する有効なユーザ名とパスワードのリスト）

Expressway で使用される他のパスワード（LDAP/リモートに保存されている管理者や FindMe のクレデンシャルなど）には影響はありません。

（注） すべてのパスワードとユーザ名で大文字と小文字が区別されます。

厳密なパスワードに関する設定不可能なルール

[厳密なパスワードを強制する（Enforce strict passwords）] が *[オン（On）]* に設定されている場合は、次のパスワード規則が常に適用され、構成できません。

- 同じ文字列の複数インスタンスを避ける（連続しないインスタンスもチェック）
- 3 文字以上の連続文字列を避ける（「「abc」」や「「123」」など）
- 辞書にある単語や辞書にある単語の反転を避ける
- 回文を避ける（「「risetovotesir」」など）

管理者アカウント、ローカル認証データベース、および FindMe ユーザのパスワードの作成または変更中に、**[厳格なパスワードを適用する (Enforce strict passwords]** がオンで、ユーザ名と同じ文字がストレートまたはリバースの順序（小文字または大文字）の場合、ページの上部にエラーメッセージが表示されます。

厳密なパスワードに関する設定可能なルール

パスワード ポリシーの以下のプロパティを設定できます。

[カスタム禁止パスワードディクショナリを有効にする（Enable custom forbidden password dictionary）] が *[オン（On）]* に設定されている場合、カスタム禁止パスワードディクショナリを使用して厳密なパスワードチェックを実行できます。

[カスタム禁止パスワードディクショナリを有効にする（Enable custom forbidden password dictionary）] が *[オフ（Off）]* に設定されている場合、厳密なパスワードチェックを実行するときにカスタムディクショナリは使用されません。デフォルトは [オフ（Off）] です。

- 長さは ASCII 文字で 6 文字以上、255 文字以下（デフォルトは 15）
- 数字 [0-9] の数は 0 ～ 255（デフォルトは 2）

- 大文字 [A-Z] の数は 0 ～ 255（デフォルトは 2）
- 小文字 [a-z] の数は 0 ～ 255（デフォルトは 2）
- 特殊文字 [7 ビット ASCII の印刷可能文字（例：スペース、@、$ など）] の数は 0 ～ 255（デフォルトは 2）
- 許容される連続繰り返し文字の数は 1 ～ 255（デフォルトの 0 ではチェックは無効になるため、連続繰り返し文字はデフォルトで許容されます。パスワードに連続繰り返しが含まれないようにするには、1 に設定します）
- 文字クラスの最小数は0～4（デフォルトの0はチェックを無効にします）文字クラスは、数字、小文字、大文字、および特殊文字です。

  必要な文字クラスの数とクラスあたりの文字数の間で優先順位の効果が現れる場合があります。

  例：各クラス 2 文字というデフォルトの要件のままにしておくと、4 つの文字クラスが必要であるという暗黙的なルールが存在します。この場合、**[文字クラスの最小数（Minimum number of character classes）]** の設定は無意味になります。または、文字クラスの最小数を 2 に設定し、各クラスから必要な文字の最小数を 0 に設定した場合、各クラスに必要な最小文字数を0にすると、任意の 2 つのクラスの文字を含むパスワードで十分になります（その他の条件を満たしていると見なします）。

パスワードの暗号化

Expresswayに設定されているすべてのパスワードが暗号化またはハッシュ形式のいずれかで安全に保存されます。これは、次の項目に適用されます。これらのすべての項目にはユーザ名とパスワードが関連付けられています。

- デフォルトの admin 管理者アカウント
- 追加の管理者アカウント
- ローカル認証データベース クレデンシャル（他のデバイスが Expressway での認証を求められている場合に使用する有効なユーザ名とパスワードのリスト）
- アウトバウンド接続クレデンシャル（別のシステムでの認証に必要な場合に Expressway が使用）
- LDAP サーバ（LDAP サーバにバインドする際に Expressway が使用）

ローカルの管理者アカウントのパスワードは、SHA512 を使用してハッシュされます。他のパスワードは暗号化された形式で保存されます。

Web インターフェイスと CLI の比較

Webインターフェイスを使用してパスワードを入力または表示する場合は、入力する文字の代わりにプレースホルダ文字が表示されます。

コマンドラインインターフェイスを使用してパスワードを入力する場合は、プレーンテキストでパスワードを入力します。ただし、コマンドを実行した後、パスワードは*{cipher}*プレフィックスを使用して暗号化された形式で表示されます。次に例を示します。

xConfiguration Authentication Password: "{cipher}xcy6k+4NgB025vYEgoEXXw=="

パスワードの最大長

次の表に、入力可能なプレーンテキスト文字の最大数をパスワードのタイプごとに示します。

パスワード タイプ	最大長
admin アカウント	1024
その他のローカル管理者アカウント	1024
ローカル データベース認証クレデンシャル	128
アウトバウンド接続クレデンシャル	128
LDAP サーバ	60
FindMe アカウント	1024

（注） パスワードが暗号化されて保存される場合は、プレーンテキストバージョンよりも多くの文字が使用されます。

禁止パスワード辞書

（注） 使用禁止パスワードディクショナリを設定していない場合は、それをクリックすると警告メッセージが表示されます。

□□ Expressway □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

禁止パスワード辞書のダウンロード

手順

ステップ 1 **[ユーザ（Users）]** > **[禁止されているパスワード（Forbidden password）]**に移動します。

ステップ 2 **[ディクショナリのダウンロード（Download dictionary）]** をクリックして、現在のバージョンのディクショナリをローカルドライブにダウンロードします。

禁止パスワード辞書のアップロード

（注） **.txt** ファイルのみサポートされています。

手順

ステップ 1 **[ユーザ（Users）]** > **[禁止されているパスワード（Forbidden password）]**に移動します。

ステップ 2 [Choose File] をクリックします。

ステップ 3 ローカルドライブからアップロードするディクショナリファイルを選択し、**[ディクショナリのアップロード（Upload dictionary）]** をクリックします。
結果：新しいディクショナリがアップロードされ、アプリケーションに統合されます。

禁止パスワード辞書のアップデート

手順

ステップ 1 **[ユーザ（Users）]** > **[禁止されているパスワード（Forbidden password）]**に移動します。

ステップ 2 **[ディクショナリのダウンロード（Download dictionary）]** をクリック します。

現在のバージョンのディクショナリをダウンロードし、必要な変更を行います。

ステップ 3 **[ファイルの選択（Choose File）]** をクリックして更新ファイルを選択します。

ステップ 4 **[ディクショナリのアップロード（Upload dictionary）]** をクリックします。

更新されたディクショナリがアップロードされ、アプリケーションに統合されます。

パスフレーズの生成

パスフレーズを生成すると、パスワードよりも長く、単語間にスペースが含まれるランダムなセキュアパスフレーズが提供されます。これにより、文字、数字、記号の不可解なシリーズがなく、セキュリティが向上し、使いやすさが向上します。許可されていないユーザーがそれらを復号化するのを防ぎます。生成されるパスフレーズのデフォルト長は 64 です。

手順

ステップ 1 **[メンテナンス（Maintenance）] > [ツール（Tools）] > [パスフレーズの生成（Generate Passphrase）]**に移動します。

ステップ 2 新しく**[生成されたパスフレーズ（Generated passphrase）]**が表示されます。

管理者アカウントの設定

「管理者アカウント（Administrator accounts）」ページ（**[ユーザ（Users）] > [管理者アカウント（Administrator accounts）] >**）ページには、Expressway 上のすべてのローカル管理者アカウントのリストが表示されます。

一般に、ローカル管理者アカウントは、WebインターフェイスまたはAPIインターフェイスの Expressway にアクセスするために使用されますが、CLI にアクセスすることはできません。

このページでは、次の操作を実行できます。

- 新しい管理者アカウントの作成
- 管理者パスワードの変更
- アカウントのアクセス レベルの変更：[読み取り/書き込み（Read-write）]、[読み取り専用（Read-only）]、または [オーディタ（Auditor）]
- アカウントのアクセス範囲の変更：[Web アクセス（Web access）]、[API アクセス（API access）]、またはこの両方
- 個別または複数の管理者アカウントの削除、有効化、または無効化
- 緊急時アカウントの指定

管理者アカウントの詳細情報の編集

デフォルトの管理者アカウントと追加したローカル管理者アカウントの詳細情報は編集できます。

手順

ステップ 1 **[ユーザ（Users）] > [管理者アカウント（Administrator accounts）]**に移動します。

ステップ 2 関連する管理者アカウントの **[アクション（Actions）]** で、**[ユーザの編集（Edit user）]** をクリックします。

新しいページが表示され、選択した管理者アカウントのパスワードを除くすべてのフィールドを編集できます。

パスワードの変更

手順

ステップ 1 **[ユーザ（Users）]** > **[管理者アカウント（Administrator accounts）]**に移動します。

ステップ 2 関連する管理者アカウントの **[アクション（Actions）]** で、**[パスワードの変更（Change password）]** をクリックします。

新しいページが表示され、選択した管理者アカウントのパスワードを変更できます。

ステップ 3 **[関連タスク（Related tasks）]** セクションに移動し、**[パスフレーズの生成（Related tasks）]** をクリックします。

[生成されたパスフレーズ（Generated passphrase）] ページに新しいパスフレーズが表示されます。

ステップ 4 **[新しいパスワード（New password）]** フィールドと **[新しいパスワードの確認（Confirm new password）]** フィールドのテキストボックスに、新しく生成されたパスフレーズを入力するかコピーして貼り付けます。

ステップ 5 **現在のパスワード**を入力 して、パスワード変更プロセスを承認します。

ステップ 6 [保存（Save）] をクリックします。

パスワードの変更が正常に表示されるメッセージ 。

管理者アカウントとフィールド参照について

このデフォルトのローカル管理者 「admin」 アカウントには完全な読み取り/書き込みのアクセス権があり、Web UI、API インターフェイス、または CLI を使用して Expressway にアクセスできます。

このアカウントのユーザ名は **admin** です（すべて小文字）。

X8.9 より前のデフォルトパスワードは**TANDBERG**（すべて大文字）です。X8.9以降では、新しいシステムはスタートアップ時にセキュアなインストール ウィザードを実行するため、システムがネットワークに接続される前に新しいパスワードを提供できます。

admin は、削除も名前の変更も、無効化も行えず、アカウント レベルを *[*読み取り/書き込み（*Read-write*）*]* から変更できませんが、Web アクセスと API アクセスを無効にすることはできます。

X8.9 より前のバージョンからシステムをアップグレードした場合、パスワードを変更する必要があることがあります。特に IP による管理が有効になっている場合は、強力なパスワードを選択してください。

admin アカウントのパスワードを忘れた場合は、読み取り/書き込みアクセス権を持つ別の管理者アカウントとしてログインして、**admin** アカウントのパスワードを変更することができます。ほかの管理者アカウントがない場合、またはそれらのパスワードも忘れた場合でも、Expressway への物理的なアクセスがあれば **admin** アカウントのパスワードをリセットできます。詳細については、忘れた場合のパスワードのリセットを参照してください。

管理者アカウントのフィールド リファレンス

フィールド	説明	使用方法のヒント
名前（Name）	管理者アカウントのユーザ名。	「「root」」などの一部の名前は予約されています。ローカル管理者アカウントのユーザ名では、大文字と小文字が区別されます。
アクセス レベル（Access level）	管理者アカウントのアクセス レベル： *[Read-write]*：すべての設定情報の表示と変更を許可します。これにより、デフォルトの **admin** アカウントと同じ権限が与えられます。 *[Read-only]*：ステータスおよび設定情報の表示のみを許可し、変更は許可しません。「**アップグレード（Upgrade）**」ページなどのいくつかのページは、読み取り専用アカウントに対してはブロックされています。 *[オーディタ（Auditor）]*：**[イベント ログ（Event Log）]** ページ、**[設定ログ（Configuration Log）]** ページ、**[ネットワーク ログ（Network Log）]** ページ、**[アラーム（Alarms）]** ページ、および **[概要（Overview）]** ページのみにアクセスできます。 デフォルト：[Read-write]	現在ログインしているユーザのアクセス権限は、各 Web ページの下部にあるシステム情報バーに表示されます。 デフォルトの **admin** アカウントのアクセス レベルは *[読み取り/書き込み（Read-write）]* から変更できません。

フィールド	説明	使用方法のヒント
[パスワード（Password）]	この管理者が Expressway へのログインに使用するパスワード。	Expressway のすべてのパスワードは暗号化されます。そのため、ここにはプレースホルダのみが表示されます。 パスワードを入力すると、**[パスワード（Password）]** フィールドの横にあるバーの色が変わり、パスワードの複雑さが示されます。パスワード セキュリティの設定ページ（**[ユーザ（Users）]** > **[パスワード セキュリティ（Password security）]**）で、ローカル管理者パスワードの複雑さ要件を設定できます。 ブランク パスワードは設定できません。 （注） 管理者アカウント、ローカル認証データベース、および FindMe ユーザのパスワードの作成または変更中に、「**[厳格なパスワードを適用する（Enforce strict passwords）]**」 が オンで、ユーザ名と同じ文字がストレートまたはリバースの順序（小文字または大文字）の場合、ページの上部にエラーメッセージが表示されます。
New password	アカウントの新しいパスワードを入力します。	このフィールドは、パスワードを変更するときにのみ表示されます。
パスワードの確認（Confirm Password）	アカウントのパスワードを再入力します。	このフィールドは、アカウントを作成するとき、またはそのパスワードを変更するときにのみ表示されます。

フィールド	説明	使用方法のヒント
緊急時アカウント（Emergency account）	*[*はい（*Yes*）*]* を選択すると、このアカウントを緊急時アカウントとして使用します。 読み取り/書き込みアクセスと Web アクセスが可能な有効になっているローカル管理者アカウントを使用する必要があります。	1 つの緊急時アカウントを許可でき、このアカウントを使用すると、ローカル認証が許可されない場合でも Expressway にアクセスできます。 このアカウントの目的は、リモート認証が使用できないときにシステムからロックアウトされるのを回避できるようにするためです。
Web アクセス（Web Access）	このアカウントが Web インターフェイスを使用してシステムにログインできるかどうかを選択します。 デフォルト：[Yes]	
パスワードの強制的なリセット（Force password reset）	[はい（Yes）]を選択する場合、新しいユーザする必要があります新しいパスワードを作成ログインするときにします。 デフォルト：[いいえ（No）]	
API アクセス（API access）	このアカウントがアプリケーション プログラミングインターフェイス（API）を使用してシステムのステータスおよび設定にアクセスできるかどうかを選択します。 デフォルト：[Yes]	Cisco TMS などのシステムによる XML および REST API へのアクセスを制御します。
状態（State）	アカウントが *[*有効（*Enabled*）*]* か *[*無効（*Disabled*）*]* かを選択します。無効なアカウントはシステムにアクセスできません。	
現在のパスワード（Your current password）	変更を承認する必要がある場合、ここに自身の現在のパスワードを入力します。	セキュリティを強化するため、システムはアカウントを作成したりパスワードを変更すると、管理者に自分自身のパスワードを入力するように求めます。

アクティブな管理者セッションの表示

「アクティブな管理者セッション（Active administrator sessions）」ページ（**[ユーザ（Users）]**> **[アクティブな管理者セッション（Active administrator sessions）]**）には、この Expressway に現在ログインしているすべての管理者アカウントのリストが表示されます。

これには、ログイン時刻、セッション タイプ、IP アドレスとポート、および最後にこの Expressway へアクセスした日時などのセッションの詳細が示されます。

必要なセッションを選択して [セッションの終了（Terminate session）] をクリックすることで、アクティブな Web セッションを終了できます。

[セッション タイム アウト（Session time out）] 値をゼロに設定している場合は、このページに多くのセッションが一覧表示されます。これは通常、管理者が Expressway からログアウトせずにブラウザを閉じてセッションを終了した場合に発生します。

LDAP を使用したリモート アカウント認証の設定

管理者アカウント認証のためのリモートディレクトリサービスへの LDAP 接続を設定するには、**「LDAP 設定（LDAP configuration）」**ページ（**[ユーザ（Users）]** > **[LDAP 設定（LDAP configuration）]**）を使用します。

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
[リモートアカウント認証（Remote account authentication）]：このセクションでは、リモートアカウント認証用の LDAP の使用を有効または無効にできます。		
管理者認証ソース（Administrator authentication source）	管理者のログイン クレデンシャルを認証する場所を定義します。 *[ローカルのみ（Local only）]*：システムに保存されているローカルデータベースと照合してクレデンシャルを確認します。 *[リモートのみ（Remote only）]*：外部クレデンシャルディレクトリと照合してクレデンシャルを確認します。 *[両方（Both）]*：最初にシステムに保存されているローカルデータベースと照合して確認し、一致するアカウントが見つからなかった場合は外部クレデンシャルディレクトリが代わりに使用されます。 デフォルトは [Local only] です。	*[Both]* を選択すると、ローカルで定義したアカウントを引き続き使用できます。これは、LDAP サーバとの接続や認証の問題をトラブルシューティングするときに役立ちます。 *[リモートのみ（Remote only）]* の認証が使用されている場合は、デフォルトの **admin** アカウントを含め、ローカルで設定した管理者アカウントを使用してログインできません。 （注） Expressway が Cisco TMS によって管理されている場合、*[リモートのみ（Remote only）]* は使用しないでください。

フィールド	説明	使用方法のヒント
[LDAP サーバ設定（LDAP server configuration）]：このセクションでは、LDAP サーバへの接続の詳細を指定します。		
FQDN アドレス解決（FQDN address resolution）	LDAP サーバアドレスを解決する方法を定義します。 *[SRV* レコード（*SRV record）]*：DNS SRV レコード ルックアップ。 *[*アドレス レコード（*Address record）]*：DNS A レコードまたは AAAA レコード ルックアップ。 *[IP* アドレス（*IP address）]*：IP アドレスとして直接入力。 デフォルトは *[Address record]* です。 SRV レコードを使用する場合は、*ldap._tcp.<domain> records* を標準 LDAP ポート 389 で使用していることを確認してください。Expressway は LDAP 用に他のポート番号をサポートしていません。 SRV として LDAPS を使用するには、AD サーバが STARTTLS 拡張機能をサポートしている必要があります。（ポート 636 を使用して LDAPS を実行する場合は、アドレスレコードを使用して FQDN を解決し、ポート 636 に直接接続する必要があります。）	SRV ルックアップは _ldap._tcp レコードです。複数のサーバが返された場合、各 SRV レコードの優先度とウェイトによって、サーバが使用される順序が決まります。
[ホスト名（Host name）] と **[ドメイン（Domain）]** または **サーバ アドレス（Server address）**	サーバ アドレスの指定方法は、**FQDN アドレス解決**の設定によって異なります。 *[SRV* レコード（*SRV record）]*：サーバ アドレスの**ドメイン**部分だけが必要です。 *[*アドレス レコード（*Address record）]*：**ホスト名**と**ドメイン**を入力します。これらは組み合わされて、DNS アドレス レコードを検索するための完全なサーバ アドレスになります。 *[IP* アドレス（*IP address）]*：**サーバ アドレス**を IP アドレスとして直接入力します。	TLS を使用する場合、ここに入力するアドレスは、LDAP サーバから提示される証明書に含まれる CN（コモン ネーム）と一致している必要があります。
[ポート（Port）]	LDAP サーバで使用する IP ポート。	

フィールド	説明	使用方法のヒント
暗号化	LDAP サーバへの接続を Transport Layer Security（TLS）を使用して暗号化するかどうかを決定します。 • *[TLS]*：LDAP サーバへの接続に TLS 暗号化を使用します。 • *[Off]*：暗号化は使用されません。 デフォルトは、[TLS] です。 詳細については、最小限 TLS バージョンと暗号スイートの設定を参照してください。	TLS が有効になっている場合は、Expressway の信頼済み CA 証明書ファイル内の認証局が LDAP サーバ証明書に署名する必要があります。 **[TLS 用の CA 証明書ファイルをアップロード（Upload a CA certificate file forTLS）]**（**[関連タスク（Related tasks）]** セクション内）をクリックし、信頼された CA 証明書リストの管理ページに移動します。
証明書失効リスト（CRL）の確認中（Certificate revocation list (CRL) checking）	LDAP サーバとの TLS 接続を確立するときに証明書失効リスト（CRL）を確認するかどうかを指定します。 *[なし（None）]*：CRL チェックは実行されません。 *[ピア（Peer）]*：LDAP サーバの証明書を発行した CA に関連付けられた CRL のみを確認します。 *[すべて（All）]*：LDAP サーバ証明書を発行した CA の信頼できる証明書チェーン内のすべての CRL を確認します。 デフォルトは [なし（None）] です。	失効リストを使用している場合は、必要な CRL データも CA 証明書ファイル内に含める必要があります。
[認証設定（Authentication configuration）]：このセクションでは、LDAP サーバにバインドするときに使用する Expressway の認証クレデンシャルを指定します。		
バインド DN（Bind DN）	LDAP サーバにバインドするときに Expressway で使用される識別名（大文字と小文字の区別なし）。 cn=、ou=、dc= の順に DN を指定する必要があります。 （注） LDAP ユーザに最小の権限を与える必要があります。	名前の中に含まれる特殊文字は、LDAP 標準（*RFC 4514*）に従ってバックスラッシュでエスケープする必要があります。名前と名前の間の区切り文字はエスケープしないでください。 通常、バインド アカウントは特別な権限を持たない読み取り専用のアカウントです。

フィールド	説明	使用方法のヒント
バインド パスワード（Bind Password）	LDAP サーバにバインドするときに Expressway で使用されるパスワード（大文字と小文字の区別あり）。	プレーンテキストの最大長は 60 文字で、暗号化されます。
SASL	LDAP サーバにバインドするときに使用する SASL（Simple Authentication and Security Layer）のメカニズム。 *None*：メカニズムを使用しません。 *[DIGEST-MD5]*：DIGEST-MD5 メカニズムを使用します。 デフォルトは *[DIGEST-MD5]* です。	企業のポリシーに応じて、Simple Authentication and Security Layer を有効にします。
バインド ユーザ名（Bind username）	Expressway が LDAP サーバにログインするときに使用するアカウントのユーザ名（大文字と小文字の区別あり）。 SASL が有効になっている場合にのみ必要です。	これは、sAMAccountName（セキュリティ アクセス マネージャ アカウント名）になるように設定します（AD では、これはアカウントのユーザ ログオン名です）。
[ディレクトリ設定（Directory configuration）]：このセクションでは、アカウントとグループ名を検索するときに使用する基本識別名を指定します。		
アカウントのベース DN（Base DN for accounts）	データベース構造においてユーザ アカウント検索の開始点となる識別名の ou= および dc= 定義（大文字と小文字の区別なし）。 ou=、dc= の順に DN を指定する必要があります。	アカウントとグループのベース DN は、dc レベル以下にする必要があります（必要に応じてすべての dc= 値と ou= 値を含めてください）。LDAP 認証では、サブ dc アカウントを確認しません。下の レベルの ou= および cn= レベルのみを確認します。
グループのベース DN（Base DN for groups）	データベース構造においてグループ検索の開始点となる識別名の ou= および dc= 定義（大文字と小文字の区別なし）。 ou=、dc= の順に DN を指定する必要があります。	**グループのベース DN** を指定しない場合は、アカウントのベース DN がグループおよびアカウントの両方に使用されます。
ネストされたサブグループの検索深度	LDAP 検索のグループの深さを制限するために使用されます。	最適な検索パフォーマンスのために、リモート管理者の上位レベルのグループを Expressway の（管理者）グループとして定義し、検索深さを 「「1」」に設定します。

フィールド	説明	使用方法のヒント
すべてのメンバーの検索をスキップ	認証検索プロセス中に管理者グループのメンバールックアップを無効または有効にするために使用されます。デフォルトは「*[*はい（*Yes*）*]*」で、メンバールックアップをスキップします。	設定されているグループのメンバー数が相対的に多い場合は、この設定を「*[*はい（*Yes*）*]*」のままにしておくことをお勧めします。ただし、設定されているグループのメンバーが相対的に少ない導入では、「*[*いいえ（*No*）*]*」（メンバールックアップを行う）に設定すると、認証の遅延が減少する 場合があります。

LDAP サーバの接続ステータスの確認

LDAP サーバへの接続のステータスはページの下部に表示されます。

状態 = 使用可能

エラー メッセージは表示されません。

[State] = [Failed]

次のエラー メッセージが表示されることがあります。

エラー メッセージ	理由/解決方法
DNSはリバース検索を実行できません（DNS unable to do reverse lookup）	SASL 認証にはリバース DNS 検索が必要です。 （注） 逆引きルックアップを容易にするために、152.50.10.in-addr.arpa（アドレスのサブネットは 10.50.152.0/24）とアドレス内のターゲット DNS サーバの形式にします。これにより、サブネット内のすべての要求がデフォルトサーバではなく、ターゲット DNS サーバに送信されます。
DNS で LDAP サーバアドレスを解決できません（DNS unable to resolve LDAP server address）	有効な DNS サーバが設定されていることと、LDAP サーバのアドレスのスペルを確認します。

エラー メッセージ	理由/解決方法
LDAP サーバへの接続に失敗しました。サーバのアドレスとポートを確認してください（Failed to connect to LDAP server. Check server address and port）	LDAP サーバの詳細が正しいことを確認します。
TLS 接続の設定に失敗しました。CA 証明書を確認してください（Failed to setup TLS connection. Check your CA certificate）	TLS には、CA 証明書、秘密キー、およびサーバ証明書が必要です。
サーバへの接続に失敗しました。コードが返されました <戻りコード>（Failure connecting to server. Returned code<return code>）	その他の一般的な問題。
無効なアカウントのベース DN です（Invalid Base DN for accounts）	**アカウントのベース DN** を確認してください。現在の値は、LDAP ディレクトリの有効な部分を記述したものではありません。
無効なサーバ名または DNS 障害（Invalid server name or DNS failure）	LDAP サーバ名の DNS 解決に失敗しました。
無効なバインドクレデンシャル（Invalid bind credentials）	**[バインド DN（Bind DN）]** および **[バインド パスワード（Bind password）]** を確認してください。このエラーは、SASL を *[なし（None）]* に設定する必要があるときに、*[DIGEST-MD5]* に設定した場合にも表示されることがあります。

エラー メッセージ	理由/解決方法
無効なバインド DN（Invalid bind DN）	[Bind DN] を確認してください。現在の値は LDAP ディレクトリ内の有効なアカウントを記述したものではありません。 **バインド DN** の長さが 74 文字以上ある場合に、この失敗した状態が誤って報告されることがあります。実際に失敗したかどうかを確認するには、有効なグループ名を使用して Expressway 上で管理者グループを設定します。Expressway から「「保存されました（saved）」」と報告された場合は問題ありません（Expresswayは指定されたグループが見つかるかどうかを確認します）。グループが見つからないと報告された場合は、**バインド DN** が誤っているか、グループが誤っているか、あるいはそのほかの設定項目が誤っている可能性があります。
インストールされた CA 証明書がありません（There is no CA certificate installed）	TLS には、CA 証明書、秘密キー、およびサーバ証明書が必要です。
設定を取得できません（Unable to get configuration）	LDAP サーバ情報がないか、誤っています。

管理者グループの設定

「管理者グループ（Administrator groups）」ページ（**[ユーザ（Users）] > [管理者グループ（Administrator groups）]**）には、Expressway で設定したすべての管理者グループのリストが表示されます。このページでは、グループを作成、編集、削除できます。

管理者グループは、LDAP を使用したリモート アカウント認証の設定が有効になっている場合にのみ適用されます。

Expressway の Web インターフェイスにログインすると、リモート ディレクトリ サービスと照合してクレデンシャルが認証され、所属するグループに関連付けられたアクセス権が割り当てられます。管理者アカウントが複数のグループに属している場合は、最も高いレベルの権限が割り当てられます。

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
名前（Name）	管理者グループの名前。 次の文字はすべて使用できません。 / \ [ ] : ; | = , + * ? > < @ "	Expressway で定義されるグループ名は、この Expressway への管理者アクセス権を管理するリモート ディレクトリ サービスでセットアップされているグループ名と一致する必要があります。

フィールド	説明	使用方法のヒント
アクセス レベル（Access level）	管理者グループのメンバーに付与されるアクセス レベル： *[Read-write]*：すべての設定情報の表示と変更を許可します。これにより、デフォルトの **admin** アカウントと同じ権限が与えられます。 *[Read-only]*：ステータスおよび設定情報の表示のみを許可し、変更は許可しません。「**アップグレード（Upgrade）**」ページなどのいくつかのページは、読み取り専用アカウントに対してはブロックされています。 *[オーディタ（Auditor）]*：**[イベントログ（Event Log）]** ページ、[設定ログ（Configuration Log）] ページ、**[ネットワークログ（Network Log）]** ページ、**[アラーム（Alarms）]** ページ、および **[概要（Overview）]** ページのみにアクセスできます。 *[なし（None）]*：すべてのアクセスが拒否されます。 デフォルト：[Read-write]	管理者が複数のグループに属している場合は、管理者が属するすべてのグループ（無効状態のグループは無視）の各アクセス設定で最も高いレベルの権限が割り当てられます。詳細については、下記の複数のグループに属するアカウントのアクセス レベルの決定を参照してください。
Web アクセス（Web Access）	このグループのメンバーが Web インターフェイスを使用してシステムにログインできるかどうかを決定します。 デフォルト：[Yes]	
API アクセス	このグループのメンバーがアプリケーション プログラミング インターフェイス（API）を使用してシステムのステータスおよび設定にアクセスできるかどうかを決定します。 デフォルト：[Yes]	Cisco TMS などのシステムによる XML および REST API へのアクセスを制御します。
状態（State）	グループが有効になっているか、無効になっているかを示します。無効になっているグループのメンバーへのアクセスは拒否されます。	管理者アカウントが有効状態と無効状態の両方が混在する複数の管理者グループに属する場合、アクセスは有効になります。

複数のグループに属するアカウントのアクセス レベルの決定

管理者がさまざまなアクセス レベルの複数のグループに属する場合、最も高いアクセス レベルが付与されます。無効状態のグループは無視されます。

たとえば、以下のグループが設定されているとします。

グループ名	アクセス レベル	Web アクセス	API アクセス
管理者	読み取りと書き込み	-	-
リージョン A	読み取り専用	はい	-
リージョン B	読み取り専用	-	はい
リージョン C	読み取り専用	はい	はい

次の表は、これらのグループの 1 つ以上に属するアカウントに付与されるアクセス権限の例を示しています。

属するグループ	付与されるアクセス権限
管理者とリージョン A	Web インターフェイスへの読み取り/書き込みアクセス、API アクセスなし
管理者とリージョン B	API インターフェイスへの読み取り/書き込みアクセス、Web インターフェイス アクセスなし
管理者とリージョン C	Web インターフェイスと API インターフェイスへの読み取り/書き込みアクセス
リージョン A のみ	Web インターフェイスへの読み取り専用アクセスで、API アクセスなし

忘れた場合のパスワードのリセット

どのアカウント パスワードもリセットすることができます。これを行うには、デフォルトの **admin** アカウントか、または読み取り/書き込みアクセス権があるほかの管理者アカウントとして Expressway にログインします。これができない場合は、コンソールを使用して **admin** パスワードまたは **root** パスワードをリセットします。

（注） パスワードをリセットしても保存済みの設定とデータは影響を受けません。

Web インターフェイスによる管理者アカウントのパスワードの変更

デフォルトの管理者アカウントと追加したローカル管理者アカウントのパスワードは変更できます。

手順

ステップ 1 **[ユーザ（Users）] > [管理者アカウント（Administrator accounts）]**に移動します。

ステップ 2 関連する管理者アカウントの **[アクション（Actions）]** で、**[パスワードの変更（Change password）]** をクリックします。

新しいページが表示され、選択した管理者のパスワードを変更できます。

ステップ 3 新しいパスワードを入力し、確認のために再度入力します。

（注） また、現在ログインしている管理者アカウントのパスワードも入力し、パスワードの変更を許可します。

シリアル接続によるルートまたは管理者パスワードのリセット

ハードウェア Expressway で **admin** パスワード、または **root** パスワードを次のようにリセットします。

手順

ステップ 1 シリアル ケーブルを使用して Expressway に PC を接続します。シリアル ポート/コンソール アクセスは、通常は無効になっていますが、再起動後の 1 分間は常に有効になります。

ステップ 2 Expressway を再起動します。

ステップ 3 ユーザ名 **pwrec** を使用して PC からログインします。パスワードは不要です。

ステップ 4 管理者アカウント認証ソースが [リモート（Remote）] に設定されている場合は、その設定を [両方（Both）] に変更するオプションが表示されます。これにより、ローカル管理者アカウントがシステムにアクセスできるようになります。

ステップ 5 変更するアカウント（**ルート**または**管理者**）を選択します。

ステップ 6 新しいパスワードを入力するように求められます。

次のタスク

pwrec のアカウントは、再起動後に 1 分間だけアクティブになります。その後はパスワードをリセットするためにシステムを再起動する必要があります。

vSphere での root パスワードまたは admin パスワードのリセット

管理者アカウントまたは **root** アカウントのパスワードを忘れた場合、VM（仮想マシン）Expressway を使用している場合は、次の手順を使用してパスワードをリセットできます。

手順

ステップ 1 [vSphere クライアント（vSphere Client）] を開きます。

ステップ 2 リンク [コンソールの起動（Launch Console）] をクリックします。

ステップ 3 Expressway をリブートします。

ステップ 4 vSphere コンソールで、ユーザ名 **pwrec** を使用してログインします。パスワードは必要ありません。

ステップ 5 プロンプトが表示されたら、パスワードを変更するアカウント（*root* または管理者アカウントのユーザ名）を選択します。

ステップ 6 新しいパスワードを入力するように求められます。

次のタスク

pwrec のアカウントは、再起動後に 1 分間だけアクティブになります。その後はパスワードをリセットするためにシステムを再度リブートする必要があります。

root アカウントの使用

Expressway は Expressway オペレーティング システムへのログインに使用できる root アカウントを提供します。このアカウントのユーザ名は **root**（すべて小文字）、デフォルトのパスワードは **TANDBERG**（すべて大文字）です。セキュリティ上の理由から、できるだけ早くパスワードを変更する必要があります。**root** アカウントにデフォルトのパスワードが設定されている場合は、Web インターフェイスと CLI にアラームが表示されます。

（注） **root** アカウントは機密情報にアクセスできる場合があるため、通常運用では使用しないでください。また、このアカウントを使用して特定のシステム設定を実行しないでください。代わりに **admin** アカウントを使用します。

root アカウントのパスワードの変更

手順

ステップ 1 既存のパスワードを使用し、**root** として Expressway にログインします。デフォルトでは、これを実行できるのはシリアル接続または SSH の場合のみです。

ステップ 2 コマンド **passwd** を入力します。

新しいパスワードの入力を求められます。

ステップ 3 新しいパスワードを入力し、プロンプトが表示されたらパスワードを再入力します。

ステップ 4 **exit** と入力して root アカウントからログアウトします。

SSH を使用した root アカウントへのアクセス

（注）
- root アカウントへは、シリアル接続または SSH でのみアクセスできます。
- SSH を使用してログインしているときに SSH アクセスを無効にした場合、現在のセッションはログアウトするまではアクティブですが、その後の SSH アクセスは拒否されます。

SSH を使用して root アカウントへのアクセスを有効または無効にすることができます。

手順

ステップ 1 **root** としてシステムにログインします。

ステップ 2 次のいずれかのコマンドを入力します。
- rootaccess --ssh on**rootaccess --ssh on**：SSH を使用したアクセスを有効にします。
- **rootaccess --ssh off**：SSH を使用したアクセスを無効にします。

ステップ 3 **exit** と入力して root アカウントからログアウトします。

SSO トークンの管理

（注） このページは、**[OAuth トークンによる承認（Authorize by OAuth token）]** で設定された標準 OAuth トークンに適用されます。自己記述 OAuth トークン（[OAuth トークンによる承認（更新あり）（Authorize by OAuth token with refresh）] で設定）には適用されません。

1. **現在 SSO トークンを保持しているユーザのリストを表示**：SSO トークンを保持しているユーザのリストを表示するには、**[ユーザ（Users）]** > **[SSO トークンを保持しているユーザ（SSO token holders）]**のリストを表示します。このページは、特定のユーザのシングルサイオンに関連するトラブルシューティングに役立ちます。
2. **すべての所有者からのトークンの削除**：このページを使用して、**すべての所有者からトークンを削除**することもできます。このオプションはユーザへ中断を余儀なくする可能性があるため、続行する前にその必要性を確認してください。たとえば、セキュリティの侵害を認識している、または内部インフラストラクチャやエッジインフラストラクチャをアップグレードする場合は必要である可能性があります。

特定のユーザのトークン管理

手順

ステップ 1 [任意] 小型のリストを返すようにユーザ名のサブストリングをフィルタリングします。

リスト内に多くのリストがあり、その長いリストが複数ページに及び、それぞれのページに最大 200 のユーザ名がある場合にこれが必要なことがあります。

ステップ 2 ユーザ名をクリックすると、そのユーザが所有するトークンの詳細を表示できます。

[ユーザ **<Username>** の ***SSO* トークン（*SSO tokens for user*）**] ページが表示されます。このページにはそのユーザに発行されたトークンの詳細のリストが表示されます。詳細には、トークンの発行者と有効期限が含まれています。

ステップ 3 （任意）UC サービスへのアクセスを続行する前にユーザの ID を確認する場合は、**[これらのトークンの削除（Delete these tokens）]** をクリックします。

ユーザのクライアントがこの Expressway-C を介して UC サービスに次回アクセスすると、クライアントは新しい署名付き要求を使用して IdP にリダイレクトされます。ユーザは Expressway-C に ID をアサートできるように IdP で再認証する必要があることがあります。ユーザは、承認された新しいトークンを使用して発行することができます。

第 21 章

ステータスとシステム情報

このセクションでは、現在のステータス、登録、現在のコールとコール履歴、Expressway の設定に関する情報を表示できる **[ステータス（Status）]** メニューのオプションについて説明します。

ステータス概要

「概要（Overview）」ページ（**[ステータス（Status）]** > **[概要（Overview）]**）には、Expressway（または、該当する場合はExpressway クラスタ）の現在のステータスの概要が表示されます。このページは、管理者として Expressway にログインした後でデフォルトで表示されます。

次の情報が表示されます。

フィールド	説明
[システム情報（System information）]：このセクションの項目の多くは設定可能です。アイテム名をクリックすると、設定ページに移動します。	
システム名（System name）	Expressway に割り当てられた名前
使用可能時間（Up time）	システムが最後に再起動されてからの経過時間
ソフトウェア バージョン（Software version）	Expressway に現在インストールされているソフトウェアのバージョン
IPv4 アドレス	Expressway の IPv4 アドレス
IPv6 アドレス	Expressway の IPv6 アドレス
オプション	コールと登録の最大制限は、オプション キーの管理によって制御されます。ソフトウェアのバージョンによっては、いくつかの追加機能をオプションキーで制御することもできますが、ここではこの方法を段階的に廃止しています。

リソース使用状況

このセクションには、コールと登録の現在および累積したライセンス使用状況に関する統計情報が表示されます。

現在の使用率とピーク使用率の内訳は次のとおりです。

- リッチ メディア セッション
- 登録（Unified CM のリモート セッションを含む）

  [登録（Registrations）] に示される、Expressway に登録されているデバイスの総数には、TelePresence Room、デスクトップ システム、会議システムが含まれます。

また、リソースとライセンスの使用状況に関する情報も表示されます。

- 監視対象のリソースの使用状況。システム容量のパーセンテージとして表現されます。

- 現在とピーク時の使用状況。各ライセンスタイプに使用可能なライセンスのパーセンテージとして表現されます。それぞれのリッチメディアセッションライセンスで1つのビデオコールまたは2つの音声のみのSIPトラバーサルコールが許可されます。したがって、100のリッチ メディア セッション ライセンスでは、90 のビデオ コールと 20 の SIP 音声専用コールが同時に許可されます。他の音声専用コール（非トラバーサル、H.323 またはインターワーキング）もリッチ メディア セッション ライセンスを使用します。

現在の通話または登録の詳細を表示するには、セクションの該当する項目をクリックします。

（注） すべての統計は、システムが最後に再起動された後のデータに基づいて行われます。値は、再起動後に 0 に設定されます。情報は 5 秒ごとに自動更新されます。

「**リソース使用状況（Resource usage）**」ページに移動すると、総使用率の統計情報を含む多くの詳細を表示できます。

MRA の展開

Expressway を使用して Cisco Unified Communications のモバイルおよびリモートアクセス機能を導入する場合は、Expressway X12.6.1 以降、Expressway-Eには、現在MRAを介して登録されている SIP デバイスに関する使用情報も表示されます。（該当する Expressway に対して MRA サービスを有効にする必要があります）。この情報には、現在アクティブな MRA デバイスの数と、Expressway が最後に再起動してからの MRA 登録のピーク数が表示されます。

クラスタ化システム

Expressway がクラスタの一部である場合は、各ピアの詳細がクラスタ全体の合計とともに表示されます。

システム情報

「システム情報（System information）」ページ（**[ステータス（Status）] > [システム（System）] > [情報（Information）]**）に Expressway のソフトウェア、ハードウェア、および時刻の設定の詳細が表示されます。

[システム情報（System information）] セクションと **[時刻情報（Time information）]** セクションの項目の多くは設定可能です。項目名をクリックするとその項目の設定ページが表示されます。

次の情報が表示されます。

フィールド	説明
[システム情報（System information）] セクション	
システム名	Expressway に割り当てられている名前

フィールド	説明
製品	これは Expressway を特定します。
ソフトウェア バージョン（**Software version**）	Expressway に現在インストールされているソフトウェアのバージョン
ソフトウェアのビルド（**Software build**）	このソフトウェアバージョンのビルド番号
ソフトウェア リリース日（**Software release date**）	このバージョンのソフトウェアがリリースされた日付
ソフトウェア名（**Software name**）	このソフトウェアリリースの内部参照番号
ソフトウェア オプション（**Software options**）	コールの最大数と、追加の Expressway 機能の可用性は、オプション キーの管理を使用 して制御されます。このセクションでは、現在インストールされているオプション機能を示します。
ハードウェア バージョン（**Hardware version**）	Expressway ソフトウェアがインストールされているハードウェアのバージョン番号
シリアル番号（**Serial number**）	Expressway ソフトウェアがインストールされているハードウェアまたは仮想マシンのシリアル番号
VM のサイズ（**VM size**）	（仮想マシンベースのシステムのみ）VM ハードウェアプラットフォームのサイズ（小、中、または大）。
[時刻情報（Time information）] セクション	
使用可能時間（**Up time**）	システムが最後に再起動されてから経過した時間
システム時刻（UTC）（**System time (UTC)**）	NTP サーバによって決定される時間。NTP サーバが設定されていない場合、設定されていない時刻が表示されます。
タイム ゾーン	「**時間（Time）**」ページで設定されているタイムゾーン
ローカル タイム（**Local time**）	NTP サーバが設定されている場合、システム時刻はローカル時刻（ローカルタイムゾーンに従って調整された UTC）で表示されます。NTP サーバが設定されていない場合、Expressway のオペレーティングシステムに従った時刻が表示されます。

フィールド	説明
[アクティブなセッション（Active sessions）] セクション：	
管理者セッション（Administrator sessions）	現在アクティブな管理者セッションの数。リンクをクリックすると、アクティブなセッションのリストが表示されます。
ユーザ セッション（User sessions）	現在のユーザセッションの数。リンクをクリックすると、アクティブなセッションのリストが表示されます。

イーサネットのステータス

「イーサネット（Ethernet）」ページ（**[ステータス（Status）]**>**[システム（System）]**>**[イーサネット（Ethernet）]**）には、Expressway の MAC アドレスとイーサネット速度が表示されます。

このページには、LAN 1 ポートと、高度なネットワーキング オプションがインストールされている場合は、LAN 2 ポートについても次の情報が表示されます。

フィールド	説明
MAC アドレス	その LAN ポートの Expressway のイーサネット デバイスの MAC アドレス。
速度	Expressway の LAN ポートとイーサネット スイッチ間の接続の速度。

イーサネットの速度は、「イーサネット設定」ページで設定できます。

[IPステータス（IP Status）]

「IP のステータス（IP status）」ページ（**[ステータス（Status）]** > **[システム（System）]** > **[IP]**）には、Expressway の現在の IP 設定が表示されます。

次の情報が表示されます。

フィールド	説明
[IP] セクション	

フィールド	説明
プロトコル	Expressway でサポートされる IP プロトコルが示されます。 • *[IPv4 のみ（IPv4 only）]*：IPv4 アドレスを使用したエンドポイントからの登録のみを許可し、IPv4 で通信する 2 つのエンドポイント間のコールのみを受け入れます。IPv4 でのみ他のシステムと通信します。 • *[IPv6 のみ（IPv6 only）]*：IPv6 アドレスを使用したエンドポイントからの登録のみを許可し、IPv6 で通信する 2 つのエンドポイント間のコールのみを受け入れます。IPv6 でのみ他のシステムと通信します。 • *[両方（Both）]*：IPv4 または IPv6 のいずれかのアドレスを使用したエンドポイントからの登録を許可し、どちらのプロトコルを使用したコールでも受け入れます。IPv4 のみのエンドポイントと IPv6 のみのエンドポイント間のコールの場合は、Expressway が IPv4 から IPv6 へのゲートウェイとして機能します。他のシステムとはいずれかのプロトコルで通信します。
IPv4 ゲートウェイ（IPv4 gateway）	Expressway が使用する IPv4 ゲートウェイ。
IPv6 ゲートウェイ（IPv6 gateway）	Expressway が使用する IPv6 ゲートウェイ。
高度なネットワーキング	2 番目の LAN ポートが有効になっているかどうかを示します。これは**高度なネットワーキング**のオプション キーをインストールすることによって有効になります。
LAN 1	LAN 1 ポートの IPv4 アドレスとサブネットマスク、および IPv6 アドレスが表示されます。
LAN 2	**高度なネットワーキング** オプション キーをインストールしている場合、このフィールドには LAN 2 ポートの IPv4 アドレスとサブネットマスク、および IPv6 アドレスが表示されます。
DNS セクション：	

フィールド	説明
サーバ1..5アドレス（Server 1..5 address）	ドメイン名を解決する際に照会する各 DNS サーバの IP アドレス。最大 5 つの DNS サーバを設定できます。
ドメイン	DNS サーバへのクエリを実行する前に、ホスト名に追加する名前を指定します。

IP 設定は「IP の設定」ページで設定できます。

リソース使用状況

「リソース使用状況（Resource Usage）」ページ（**[ステータス（Status）] > [システム（System）] > [リソース使用状況（Resource usage）]**）には、コールと登録の現在および累積的なライセンス使用状況に関する統計情報が表示されます。

現在の使用率とピーク使用率の内訳は次のとおりです。

- リッチ メディア セッション
- 登録（Unified CM のリモート セッションを含む）

  [登録（Registrations）] に示される、Expressway に登録されているデバイスの総数には、TelePresence Room、デスクトップ システム、会議システムが含まれます。

また、リソースとライセンスの使用状況に関する情報も表示されます。

- 監視対象のリソースの使用状況。システム容量のパーセンテージとして表現されます。
- 現在とピーク時の使用状況。各ライセンス タイプに使用可能なライセンスのパーセンテージとして表現されます。それぞれのリッチメディアセッションライセンスで1つのビデオコールまたは2つの音声のみのSIPトラバーサルコールが許可されます。したがって、100 のリッチ メディア セッション ライセンスでは、90 のビデオ コールと 20 の SIP 音声専用コールが同時に許可されます。他の音声専用コール（非トラバーサル、H.323 またはインターワーキング）もリッチ メディア セッション ライセンスを使用します。

現在の通話または登録の詳細を表示するには、セクションの該当する項目をクリックします。

（注） すべての統計は、システムが最後に再起動された後のデータに基づいて行われます。値は、再起動後に 0 に設定されます。情報は 5 秒ごとに自動更新されます。

クラスタ化された Expressway システム

Expressway がクラスタの一部である場合は、各ピアの詳細がクラスタ全体の合計とともに表示されます。詳細については、クラスタについてを参照してください。

登録ステータス（Registration Status）

現在と過去の両方の登録についての登録ステータス情報を表示できます。Expresswayがクラスタの一部である場合は、クラスタ内のピアに適用されるすべての登録が表示されます。

- **「デバイスごとの登録（Registrations by device）」**ページ（**[ステータス（Status）] > [登録（Registrations）] > [デバイスごと（By device）]**）には、Expressway に現在登録されているデバイスのリストが表示されます。このページで、デバイスの登録を削除できます。Expressway がクラスタの一部である場合は、クラスタ全体のすべての登録が表示されます。
- **「エイリアスごとの登録（Registrations by alias）」**ページ（**[ステータス（Status）] > [登録（Registrations）] > [エイリアスごと（By alias）]**）には、すべてのエイリアス、E.164 番号、およびすべてのエンドポイントと現在 Expressway に登録されているシステムで使用されているプレフィックスのリストが表示されます。
- **「登録履歴（Registration history）」**ページ（**[ステータス（Status）] > [登録（Registrations）] > [履歴（History）]**）には、過去のすべての登録のリストが表示されます。このリストには、Expresswayが最後に再起動されてからの過去のすべての登録が含まれています。

次の情報が表示されます。

フィールド	説明
名前（Name）	SIPデバイスでは、SIP AOR です。
番号（Number）	SIP デバイスでは、E.164 番号を登録できないため、常に空白になります。（**エイリアスごとの登録ビューの [エイリアス（Alias）]** 列に表示されます）。
エイリアス（Alias）	デバイスに登録されている SIP AOR （エイリアスごとの登録ビューのみ）。
タイプ（Type）	登録の特性を示します。エンドポイント、MCU、ゲートウェイ、または SIP UA が最も一般的です。
プロトコル（Protocol）	登録がSIPデバイス用かどうかが示されます。
作成時刻（Creation Time）	登録が承認された日時です。NTPサーバーが構成されていない場合は、「時刻が設定されていません」と表示されます。
住所	SIP UA の場合、これはREGISTER要求に示された連絡先アドレスです。

フィールド	説明
デバイス タイプ（Device type）	登録済みデバイスのタイプが示されます。有効なタイプは、[TelePresence Room]、[デスクトップ システム（Desktop System）]、[会議システム（Conference Systems）] です。
終了時刻（End time）	登録が終了された日時（登録履歴ビューのみ）。
デュレーション（Duration）	登録が行われていた時間（登録履歴ビューのみ）。
理由（Reason）	登録が終了された理由。（登録履歴ビューのみ）。
ピア（Peer）	デバイスが登録されているクラスタ ピアを示します。
アクション（Action）	**[表示（View）]** をクリックして「**登録の詳細（Registration details）**」ページに移動し、登録の詳細情報を表示します。

登録の詳細

「**登録の詳細（Registration details）**」ページに表示される情報は、デバイスのプロトコルと登録がまだ最新のものであるかどうかによって異なります。たとえば、SIP 登録にはAOR、連絡先、および該当する場合はパブリック GRUU の詳細が含まれます。また、**[この登録に関与するアクティブなコールを表示（View active calls involving this registration）]** と **[この登録に関与する以前のコールを表示（View previous calls involving this registration）]** を選択する関連タスクも表示されます。これらのオプションを選択すると「**登録ごとのコール（Calls by registration）**」ページに移動し、その特定の登録に関する現在および過去の関連するコール ステータス情報が表示されます。

デバイスの登録解除とブロック

登録ステータスのページには、デバイスを手動で登録解除したり、ブロックしたりするオプションがあります。

- デバイスの登録を解除するには、**[登録解除（Unregister）]** をクリックします。設定によっては、一定の期間が経過すると、デバイスが自動的に再登録されることがあります。これを防ぐには、[許可リスト（Allow List）] や [拒否リスト（Deny List）] などの登録制限ポリシーの設定を使用する必要もあります。
- **[登録解除とブロック（Unregister and block）]** をクリックするとデバイスの登録が解除され、エイリアスが「[登録拒否リスト（Registration Deny List）] の設定」ページに追加されるため、デバイスの自動再登録を防ぐことができます。（このオプションは、**[制限ポリ**

シー（**Restriction policy**）**]** を *[*拒否リスト（*Deny List*）*]* に設定している場合にのみ使用できます）。

（注） Expresswayがクラスタの一部である場合、デバイスを登録解除するには、デバイスが登録されているピアにログインする必要があります。

コール ステータス

コール ステータス情報は現在のコールと完了したコールの両方に対して表示できます。

- **[現在のコール（Current calls）]**：「**コール ステータス（Call status）**」ページ（**[ステータス（Status）] > [コール（Calls）] > [コール（Calls）]**）は、Expressway に登録されたデバイスとの送受信が現在行われているコール、または Expressway を通過しているすべてのコールをリストします。
- **[完了したコール（Completed calls）]**：「**コール履歴（Call history）**」ページ（**[ステータス（Status）] > [コール（Calls）] > [履歴（History）]**）はアクティブでなくなったすべてのコールをリストします。コールが複数のコンポーネントを使用している場合、リストは最新の 500 コールに制限されます（下記参照）。これには、Expressway が最後に再起動して以降に実行されたコールだけが含まれます。

コール ステータス情報の同じセットは、「**登録ごとのコール（Calls by registration）**」ページ（「**登録の詳細（Registration details）**」ページ経由でアクセス可能）でも表示できます。

Expresswayがクラスタに含まれている場合、クラスタ内のピアに適用されるすべてのコールが表示されますが、リストはピア 1 つあたりで最新の 500 コールに限定されます。

コールの概要情報

最初は次の概要情報が表示されます。

フィールド	説明
開始時刻（Start time）	コールが発信された日時。
終了時刻（End time）	コールが終了した日時（完了したコールのみ）。
デュレーション（Duration）	通話時間。
ソース（Source）	コールを発信したデバイスのエイリアス（複数の Expressway を通過するコールであり、[User Policy（ユーザ ポリシー）] が有効になっている場合、発信者の FindMe ID が代わりに表示されます）。

フィールド	説明
宛先（**Destination**）	デバイスからダイヤルされたエイリアス。これは、（検索前トランスフォーメーション、ゾーン トランスフォーメーション、ユーザ ポリシーにより）変換されている場合があるコールの発信先のエイリアスとは異なる場合があります。
タイプ（**Type**）	コールのタイプを示します。
SIP バリアント（**SIP variant**）	標準ベース、*Microsoft AV*、*Microsoft SIP IM&P*、または *Microsoft Share* で、Expressway によってルーティングできる SIP および SDP のさまざまな実装を区別します。H.323 コールについては表示されません。
プロトコル（**Protocol**）	コールが H.323、SIP、または両方のプロトコルを使用したかどうかを示します。B2BUA を通過するコールの場合、「「複数のコンポーネント」」が表示される場合があります。コールコンポーネントのサマリセクションを表示すると、個々のコールコンポーネントのプロトコルを確認できます。
ステータス（**Status**）	コールが終了した理由（完了したコールのみ）。
ピア（**Peer**）	コールの発信に使用されているクラスタ ピアを識別します。
アクション	**[**表示（**View**）**]** をクリックし、そのコールを構成するすべてのコール コンポーネントのリストを含め、そのコールに関する詳細情報を表示します。

コール コンポーネントのサマリ情報

プライマリ リストからコールを選択したら（前述のとおり）、そのコールを構成するすべてのコール コンポーネントを含め、そのコールの詳細が表示されます。

各コール コンポーネントは、次のいずれかのタイプになります。

- *[Expressway]*：標準の Expressway コール
- *[B2BUA]*：メディア暗号化ポリシーまたは ICE メッセージング サポートを適用するため、B2BUA によりルーティングされるコール コンポーネント

- *[Microsoft Lync B2BUA]*：Microsoft Lync B2BUA によりルーティングされるコールコンポーネント

コールコンポーネントの完全な詳細を表示するには、コールコンポーネントに関連付けられている**ローカルコールシリアル番号**をクリックします。これにより、すべてのコールレッグやセッションを含めて、そのコンポーネントに関する詳細情報が表示された「**コールの詳細（Call details）**」ページが開きます。また、トラバーサル コールに最も関係のある個々のメディア チャネル（音声、ビデオ、データなど）をリストする「**コール メディア（Call media）**」ページも表示されます。

Expressway がクラスタの一部であり、コールが 2 つのクラスタ ピアを通過する場合、コールの他方のレッグの詳細を確認するには、**[ほかのクラスタ ピアの関連付け先コールを表示（View associated call on other cluster peer）]** をクリックします。

通話履歴は 500 件未満のコールを反映する場合があります。

コールの中には、複数のコンポーネント、特に B2BUA を介して呼び出されるコールを使用します。このような場合、各個別のコールは、関係する複数のコンポーネントのため、実際には *3* つのコールとしてカウントされます。つまり、通話履歴に実際にリストされているエントリの数は、500 の制限を超える可能性があります。

モバイルおよびリモートアクセス（MRA）コールの識別

コールステータスとコール履歴ページには、すべてのコールタイプが表示されます。Unified CM リモートセッション（MRAが有効になっている場合）と Expressway RMS セッションです。

コールタイプを区別するにはコールコンポーネントをドリルダウンする必要があります。MRA コールには、コールが Expressway-C と Expressway-E のどちらで表示されているかによって、異なるコンポーネント特性があります。

- Expressway-C では、Unified CM のリモート セッションに 3 つのコンポーネントがあります（メディア暗号化の実行に B2BUA を使用するため）。Expressway コンポーネントの 1 つが、Expressway と Unified CM 間に自動的に生成されるネイバー ゾーンの 1 つを経由してコールの経路を指定します（名前の前に **CEtcp** または **CEtls** が付きます）。
- Expressway-E では、1 つのコンポーネントが **CollaborationEdgeZone** を介してコールをルーティングします。

両方のエンドポイントが企業外（つまりオフプレミス）にある場合は、2 つの独立したコールとして扱われます。

リッチメディアセッション（RMA）

システムに RMA キーがインストールされ、Business-to-Business（B2B）コール、サードパーティ製ソリューションへのインターワークコールまたはゲートウェイコールなどをサポートする場合、これらのコールは、コール状態やコール履歴のページに記載されています。

コールの切断

選択したコールを切断するには、**[切断（Disconnect）]** をクリックします。Expressway がクラスタの一部である場合は、コールが関連付けられているピアにログインし、コールを切断できるようにする必要があります。

コールの切断は、プロトコルの動作の違いにより、H.323 コールと SIP コールでは異なる方法で動作します。

- H.323 コールと H.323-SIP インターワーキングが適用されたコール：**Disconnect** コマンドにより、コールが実際に切断されます。
- SIP 間のコール：**Disconnect** コマンドにより、Expressway はコールに使用されていたすべてのリソースを解放し、システムがコールは切断されたと認識します。ただし、SIP コールはピア間のコールであり、SIP のプロキシとして Expressway はエンドポイントに対する権限がありません。リソースの解放には SIP コール切断の副次的な影響はありますが、コール シグナリングまたはメディア、あるいはその両方が（発信されているコールのタイプによっては）アップしたままになる可能性もあります。コールは、関与する SIP エンドポイントがリソースをクリアするまでは実際には切断されません。
- B2BUA 経由の SIP コール：B2BUA はコールの状態を制御できるため、B2BUA を通過するコールのレッグを切断する場合（**[タイプ（Type）]** が *[B2BUA]* の場合）、コールは完全に切断されます。コールが「**コール ステータス（Call status）**」ページに表示されなくなるまで数分かかることがあります。その場合、ブラウザでページを更新する必要があります。

B2BUA コール

「**B2BUA コール（B2BUA calls）**」ページには、B2BUA 経由でルーティングされたコールの概要が表示されます。このページにアクセスするには、**[ステータス（Status）]** > **[コール（Calls）]** > **[コール（Calls）]** に移動するか、**[ステータス（Status）]** > **[コール（Calls）]** > **[履歴（History）]** に移動してから、特定の B2BUA コールの **[表示（View）]** をクリックします。

次の場合は、コールが B2BUA 経由でルーティングされます。

- メディア暗号化ポリシーの設定がコールに適用されている（[自動（Auto）]以外の暗号化設定）。
- Expressway が Cisco Meeting Server に対してコールのロード バランシングを行っている。ロード バランシングが有効にされている場合は、Expressway B2BUA が Meeting Server からの INVITE メッセージを処理します。Meeting Server のロードバランシング サポートは、**プレビュー モードでのみ提供**されることに注意してください。詳細については、現在使用している Expressway バージョンのリリース ノートを参照してください。
- ICE メッセージング サポートの設定のサポートがトリガーされた。
- Microsoft の相互運用性について、コールが **To Microsoft destination via B2BUA** というネイバー ゾーン経由でルーティングされている。

Microsoft 相互運用性コールの場合、**[対応する Expressway コール（Corresponding Expressway call）]** のリンクをクリックすると、Expressway を通過するレッグの詳細を確認できます。

B2BUA コール ヘディアの詳細の表示

「**B2BUA コール メディア（B2BUA call media）**」ページにアクセスするには、「B2BUA コール」ページで **[このコールのメディア統計情報を表示（View media statistics for this call）]** をクリックします。このページには、B2BUA を通過するコールからなる音声およびビデオのメディア チャネルに関する情報が表示されます。Microsoft 相互運用性サービスを使用したコールの場合、これは Expressway、Microsoft サーバ、および該当する場合はトランス コーダの間のレッグを形成します。

（注） B2BUA デバッグ ツールは、ローカルループバック上のポート 13997、13998、および 13999 を使用してメディアプロセスに接続し、メディア統計情報を取得します。これらのポートは接続用に開かれません。厳密には内部で使用する必要があります。これはルートからのみアクセスできます。

検索履歴

「検索履歴（Search history）」ページ（**[ステータス（Status）]>[検索履歴（Search history）]**）には、Expressway が最後に再起動してから実行された最新の 255 件の検索のリストが表示されます。

検索について

コールの発信前にコールするエンドポイントを見つけておく必要があります。Expressway は、コールするエンドポイントを見つける試行の際に一連のメッセージを送受信します。これらのメッセージそれぞれを検索と呼びます。個々のコールは、1 つまたは複数の検索をその検索に関連付けることができ、それらの検索はタイプが異なっていてもかまいません。

送信される検索メッセージのタイプは、コールが SIP 宛かまたは H.323 宛か、およびコール要求をローカルに受信したかまたは外部ゾーンから受信したかによって、次のように異なります。

- ローカルに発信された H.323 コール：2 つのメッセージが送信されます。最初に発信されるメッセージは **ARQ** で、コールするデバイスを見つけます。2 番目に発信されるメッセージはコールの **Setup** で、コールを受け入れるよう求める要求をデバイスに送信します。各メッセージは個別の検索として「**検索履歴（Search history）**」ページに表示されますが、特定のコールに関連付けられるのは **Setup** メッセージのみです。
- 外部ゾーンから発信された H.323 検索：**LRQ** が「**検索履歴（Search history）**」ページに表示されます。

- SIP：コールを送信するために 1 つのメッセージが送信されます（これは **INVITE** または SIP **OPTIONS** のいずれかです）。

（注） 個々のコールは、1 つまたは複数の検索をその検索に関連付けることができ、それらの検索はタイプが異なっていてもかまいません。各検索には個別の検索 ID があります。また、各コールには個別のコールタグ（コールの識別を参照してください）があります。

Expressway は、最大 500 の同時検索をサポートします。

検索履歴リスト

検索履歴のサマリ リストには次の情報が表示されます。

フィールド	説明
開始時刻（**Start time**）	検索を開始した日時。
検索タイプ（**Search type**）	送信するメッセージのタイプ。
ソース（**Source**）	コールを開始したエンドポイントのエイリアス。
宛先（**Destination**）	エンドポイントからダイヤルしたエイリアス。これは、元のエイリアスがローカルに変換されているか、ネイバーが照会される前であるため、コールが実際に発信されるエイリアスと異なっている場合があります。
ステータス（**Status**）	検索が成功したかどうかを示します。
アクション	**[表示（View）]** をクリックすると、「検索の詳細」ページに移動します。このページに、この検索の詳細なリストが表示されます。

リストのフィルタリング

検索のリストを制限するには、1 つ以上の文字を **[フィルタ（Filter）]** フィールドに入力し、**[フィルタ（Filter）]** をクリックします。入力した文字を（表示されたフィールドのいずれかに）含む検索のみが表示されます。

検索の詳細なリストに戻るには、**[リセット（Reset）]** をクリックします。

検索の詳細

「**検索の詳細（Search details）**」ページには、（そのページにどのように到達したかに応じて）個々の検索か、または単一のコールに関連付けられたすべての検索かのいずれかに関する詳細な情報が表示されます。表示される情報は次のとおりです。

- 検索されたサブゾーンとゾーン
- コール パスとホップ
- 検索したエイリアスに適用されたトランスフォーメーション
- コールで使用した SIP バリアント
- 管理ポリシーまたはユーザ ポリシー（FindMe）などのポリシーの使用
- 使用したポリシー サービス

検索に関連付けられたほかの情報と（検索が成功した場合の）結果のコールは、ページの下部にある **[関連タスク（Related tasks）]** セクション内のリンクを使用して表示できます。

- **[このコールタグに関連付けられたすべてのイベントを表示（View all events associated with this call tag）]** をクリックすると、「イベントログ」ページに移動します。このページには、この検索に関連するコールタグに関連付けられたイベントがフィルタリングされて表示されます。
- **[このコール タグに関連付けられた通話情報を表示（View call information associated with this call tag）]** をクリックすると、「**コールの詳細（Call details）**」ページに移動します。このページでは、コールの概要情報を表示できます。
- 個々の検索の詳細を表示しており、同じコールに関連付けられたほかの検索がある場合は、**[このコールタグに関連付けられたすべての検索を表示（View all searches associated with this call tag）]** が表示されます。これをクリックすると、コールのコールタグに関連付けられたすべての検索に関する詳細情報が新しい **[検索の詳細（Search details）]** ページが表示されます。

ローカル ゾーンのステータス

「ローカルゾーンのステータス（Local Zone status）」ページ（**[ステータス（Status）]**>**[ローカルゾーン（Local Zone）]**）には、Expressway のローカルゾーンを構成するサブゾーン（デフォルトサブゾーンとトラバーサルサブゾーン）がリストされます。

次の情報が表示されます。

フィールド	説明
サブゾーン名（**Subzone name**）	この Expressway で現在設定されている各サブゾーンの名前。**サブゾーン名**をクリックすると、そのサブゾーンの設定ページに移動します。
コール（**Calls**）	サブゾーンを現在通過しているコールの数。 （注） 設定によっては、単一のコールが複数のサブゾーンを通過する場合があります。たとえば、ローカルに登録されたエンドポイントからのコールは常にトラバーサルサブゾーンを通過します。そのため、これらのコールは 2 回表示されます（発信元のサブゾーンで 1 回とトラバーサルサブゾーンで 1 回）。
使用済み帯域幅（**Bandwidth used**）	サブゾーンを通過するすべてのコールが使用する帯域幅の総量。

ゾーン ステータス

「ゾーンのステータス（Zone status）」ページ（**[ステータス（Status）]>[ゾーン（Zones）]**）には、Expressway 上のすべての外部ゾーンのリストが表示されます。これには、コールの数と各ゾーンが使用している帯域幅の量が示されます。

ゾーンのリストには、デフォルトゾーンと、作成されているその他のすべてのゾーンが常に含まれます。

次の情報が表示されます。

フィールド	説明
名前（**Name**）	この Expressway 上に現在設定されている各ゾーンの名前。 ゾーンの**名前**をクリックすると、そのゾーンの設定ページが表示されます。
タイプ（**Type**）	ゾーンのタイプ。
コール（**Calls**）	各ゾーンを現在通過している、または各ゾーンで受信したコールの数。

フィールド	説明
使用済み帯域幅（Bandwidth Used）	各ゾーンを通過している、または各ゾーンで受信したすべてのコールが使用する帯域幅の総量。
H.323/SIP のステータス（H.323/SIP status）	ゾーンの H.323 または SIP の接続ステータスを示します。 • *[オフ（Off）]*：ゾーンまたはシステムのどちらかでプロトコルが無効になっています。 • *[アクティブ（Active）]*：そのゾーンに対してプロトコルが有効になっており、1つ以上の接続がアクティブになっています。複数の接続を設定し、それらの接続の一部が失敗した場合は、アクティブな接続数が表示されます。 • *[オン（On）]*：そのゾーンに対してプロトコルが有効になっていることを示します（アクティブな接続がないゾーン タイプ（たとえば、DNS ゾーンや ENUM ゾーンなど）の場合）。 • *[失敗（Failed）]*：そのゾーンに対してプロトコルが有効になっていますが、接続に失敗しました。 • *[チェック中（Checking）]*：そのゾーンに対してプロトコルが有効になっており、現在、システムが接続を確立しようとしています。
検索ルールのステータス（Search rule status）	このエリアを使用して、ゾーンが検索ルールのターゲットになっていないことを示します。

帯域幅

リンクステータス

「リンクステータス（Link status）」ページ（**[ステータス（Status）]**>**[帯域幅（Bandwidth）]**>**[リンク（Links）]**）には、現在、Expressway 上で設定されているすべてのリンクと、コールの数および各リンクで使用されている帯域幅のリストが表示されます。

次の情報が表示されます。

フィールド	説明
名前（**Name**）	各リンクの名前。リンクの**名前**をクリックすると、そのリンクの設定ページが表示されます。
コール（**Calls**）	現在リンクを通過しているコールの総数。 （注） システムがどのように設定されているかによって、単一のコールが複数のリンクを通過する場合があります。
使用済み帯域幅（**Bandwidth Used**）	現在リンクを通過しているコールの総帯域幅。

パイプのステータス

「パイプステータス（**Pipe status**）」ページ（**[ステータス（Status）]**>**[帯域幅（Bandwidth）]**>**[パイプ（Pipes）]**）には、現在、Expressway 上で設定されているすべてのパイプと、コールの数および各パイプで使用されている帯域幅のリストが表示されます。

次の情報が表示されます。

フィールド	説明
名前（**Name**）	各パイプの名前。パイプの**名前**をクリックすると、そのパイプの設定ページが表示されます。
コール（**Calls**）	現在パイプを通過しているコールの総数。 （注） システムがどのように設定されているかによって、単一のコールが複数のパイプを通過する場合があります。
使用済み帯域幅（**Bandwidth Used**）	現在パイプを通過しているコールの総帯域幅。

ポリシー サーバのステータスと復元力

ポリシー サーバへの Expressway の接続を設定する場合、**ステータス パス**を指定する必要があります。ステータス パスはリモート サービスのステータスを取得できる場所からのパスを特定します。デフォルトはステータス（status）です。

最大 3 つの異なるポリシー サーバ アドレスを指定できます。Expressway は 60 秒ごとに、そのアドレスの到達可能性をテストするために指定されたパスの各アドレスをポーリングします。Expressway は、標準 HTTP（S）応答ステータス コードを受け入れます。

（注） ポリシーサービスの開発者は、このコードによってサービスの該当するステータスが確実にわかるようにしなければなりません。

サーバがステータス要求に応答しない場合、Expressway はサーバのステータスが障害状態にあると見なし、ステータスがアクティブ状態に戻るまで、ポリシーサービス要求への問い合わせはされません。サーバのアベイラビリティは 60 秒のポーリング間隔が経過するまで、再度チェックされません。

Expressway がポリシー サービスを要求する必要がある場合、設定したサーバ アドレスの 1 つを使ってサービスに接続しようとします。**[サーバ1アドレス（Server 1 address）]**から始めて、設定されている場合は必要に応じて、**[サーバ2アドレス（Server 2 address）]**、次に **[サーバ3アドレス（Server 3 address）]** という要領で順番に各アドレスを試みます。最新のステータス クエリに基づき、サーバ アドレスがアクティブ状態である場合に限り、Expressway はサーバ アドレスの使用を試みます。

Expressway には、ポリシー サーバへの接続試行ごとに 30 秒の設定不可タイムアウト値があります。ただし、サーバに接続できない場合は、接続障害がすぐに発生します。

（注） TCP 接続のタイムアウトは通常 75 秒です。したがって、実際には、接続がすぐに到達不能になるか、30 秒の要求タイムアウトがまず発生するので、TCP 接続タイムアウトにはならない可能性が高いと言えます。

Expressway は、設定されたアドレスを使用してポリシー サービスへの接続に失敗した場合は、設定された**デフォルト CPL** を使用します。

（注） このメソッドは復元力を提供しますがロードバランシングを提供するわけではないことに注意してください。つまり、サーバアドレスが正しく機能するという前提で、すべての要求が**サーバ 1 アドレス**に送信されます。

Expressway によるポリシー サーバのステータスの表示

各ポリシー サービスへの接続状態の概要ビューは、**「ポリシー サービス ステータス（Policy service status）」**ページ（**[ステータス（Status）]** > **[ポリシーサービス（Policy services）]**）で表示できます。

一連のポリシーサービスには、**「ポリシーサービス（Policy services）」**ページ（**[設定（Configuration）]** > > **[ダイヤルプラン（Dial plan）]** > **[ダイヤルプラン（Dial plan）][ポリ**

シーサービス（**Policy services**）]）で定義されるすべてのサービスとともに、コールポリシーサービスが必要に応じて含まれます。

次の情報が表示されます。

フィールド	説明
名前（**Name**）	ポリシー サービスの名前。 **[名前（Name）]** をクリックすると、設定の変更、または接続の問題の詳細を確認できるそのサービス用の設定ページが表示されます。
URL	サービスのアドレス。 （注） 各サービスは復元力のために複数のサーバ アドレスで設定できることに注意してください。このフィールドは、Expressway が使用する現在選択されているサーバ アドレスを表示します。
ステータス（**Status**）	そのサーバをポーリングした前回の試行に基づく現在のサービス ステータス。
前回の使用（**Last Used**）	サービスが Expressway で最後に要求された時刻を示します。

TURN リレーの使用状況

「**TURN リレーの使用状況（TURN Relay Usage）**」ページ（**[ステータス（Status）] > [TURN リレーの使用状況（TURN relay usage）]**）には、TURN サーバに接続されているすべてのクライアントのサマリ リストが表示されます。

（注） TURN サービスは Expressway-E システムでのみ使用できます。これらのサービスは、**[設定（Configuration）] > [トラバーサル（Traversal）] > [TURN]** で設定できます。

次の情報が表示されます。

フィールド	説明
クライアント（**Client**）	リレーを要求したクライアントの IP アドレス。
メディアの接続先（**Media destinations**）	メディアがリレーされる宛先システムのアドレス。

フィールド	説明
接続プロトコル（Connection Protocol）	クライアントが TCP で接続されているか、または UDP で接続されているかを示します。
リレー（Relays）	クライアントが使用する現在のリレーの数。

クライアント接続の TURN リレーの詳細の表示

特定のクライアントをクリックすると、そのクライアントが使用しているすべてのリレーとポートを表示できます。

関連するリレー ピアのアドレス/ポートがリレーごとに表示されます。また、各リレーの関連付けられたピアのアドレス/ポート（メディアを宛先システムに送信する TURN サーバ リレー ポート）も表示されます。リレーに関する特定の統計情報を表示するには、**[表示（View）]** をクリックし、「TURN リレーのサマリ」ページに移動します。

TURN リレーのサマリ

「TURNリレーのサマリ（TURN relay summary）」ページには、そのリレーに関連付けられた権限、チャネル、および要求のサマリ カウントを含む特定のリレーに関する概要情報が表示されます。

このページにアクセスするには、**[ステータス（Status）]** > **[TURN リレーの使用状況（TURN relay usage）]** に移動し、TURN クライアントの **[表示（View）]** をクリックして、必要なリレーの **[表示（View）]** を再度クリックします。

リレーに関する詳細については、このページの下部にある **[関連タスク（Related tasks）]** セクション内のリンクを使用して表示できます。これらのリンクでは、次を確認できます。

- **[このリレーの権限を表示（View permissions for this relay）]**：このリレーに定義された権限に関する情報。
- **[このリレーのチャネルを表示（View channels for this relay）]**：このリレーに定義されたチャネル バインドに関する情報。
- **[このリレーのカウンタを表示（View counters for this relay）]**：受信した TURN 要求の数と、送信された TURN の成功応答またはエラー応答の数に関する情報。また、このリレーを割り当てたクライアントで送受信されたパケット数のカウントも表示されます。

ユニファイド コミュニケーションのステータス

「ユニファイドコミュニケーションのステータス（Unified Communications status）」ページ（**[ステータス（Status）]** > **[ユニファイドコミュニケーション（Unified Communications）]**）には、モバイルおよびリモート アクセスの概要サービスの現在のステータスが表示されます。

- 設定された Unified CM と IM&P サーバの数（Expressway-C のみ）
- アクティブなプロビジョニング セッションの現在の数（Expressway-C のみ）
- 現在のコールの数
- ユニファイドコミュニケーションサービス用に設定されたすべてのドメインとゾーン
- SSO アクセス要求と応答に関する統計情報

設定上の問題や接続上の問題が検出された場合は、その問題の解決方法に関するリンクまたはガイドラインのいずれかが示されたメッセージが表示されます。

また、次のような詳細なステータス情報も表示されます。

- 現在および最新（赤で表示）のすべてのプロビジョニング セッションのリスト（Expressway-C のみ）
- トラバーサルゾーンを通じて自動的に生成された SSH トンネルのサービス要求のリスト

MRA 認証統計情報のチェック

[ステータス（Status）] > [ユニファイドコミュニケーション（Unified Communications）] > [MRA 認証統計情報の詳細を表示（View detailed MRA authentication statistics）] に移動して、発行された要求と応答の概要と、認証の成功または失敗の詳細な統計情報を表示します。

特定の要求または応答タイプのインスタンスが存在しない場合、そのタイプのカウンタは表示されません。

SSH トンネル ステータス

このページには、この Expressway とその「「トラバーサルパートナー」」との間の SSH トンネルのステータスが表示されます。このステータスは、トンネルのいずれかの側、つまり、Expressway-C または Expressway-E から確認することができます。

次に、SSH トンネルが失敗する理由をいくつか示します。

- Expressway-C が Expressway-E を見つけることができない。
  - それらの間にファイアウォールがありますか。TCP 2222 は Expressway-C から Expressway-E まで開いていますか。
  - Expressway-C および Expressway-E 向けの転送およびリバース DNS エントリがありますか。

  トレースルートと ping を使用して、接続に問題があるかどうかを確認します。
- サーバが互いに信頼していない。
  - パートナーは NTP サーバを使用して同期されていますか。パートナー間の時間差が大きいと、互いの信頼関係が損なわれる可能性があります。

- サーバ証明書は有効で最新のものですか。発行元 CA は相手側から信頼されていますか。
- Expressway-E のローカル データベースに認証アカウントが追加されていますか。
- 同じ認証アカウントが Expressway-C に入力されていますか。

Expressway-C（**[メンテナンス（Maintenance）]** > **[セキュリティ（Security）]** > **[セキュアトラバーサルのテスト（Secure traversal test）]**）からセキュアトラバーサルのテストを行い、Expressway-E の FQDN を入力します。

Microsoft 相互運用性（Microsoft interoperability）

Microsoft に登録済みの FindMe ユーザのステータス

[ステータス（Status）] > **[アプリケーション（Applications）]** > **[Microsoft に登録済みの FindMe ユーザ（Microsoft-registered FindMe users）]** のページには、Microsoft の相互運用性について によって処理されているすべての FindMe ID の現在のステータスがリストされます。

これは、Microsoft クライアントと FindMe の両方が同じ SIP ドメインを使用している場合はその両方が使用する導入環境に適用されます。この機能を有効にするには、「Microsoft 相互運用性の設定」ページで **[FindMe ユーザをクライアントとして Microsoft サーバに登録（Register FindMe users as clients to Microsoft server）]** が *[*はい（*Yes*）*]* に設定されている必要があります。

次の情報が表示されます。

フィールド	説明
URI	FindMe ID。
登録の状態（Registration state）	FindMe ID が Microsoft のフロントエンド サーバに正常に登録されているかどうかを示します。これを行うことによって、Microsoft インフラストラクチャはコールを FindMe ID に転送できます。 （注） FindMe ID が Active Directory で有効なユーザである場合のみ FindMe ユーザを Microsoft インフラストラクチャに登録できます（同様に Microsoft クライアントが登録できるのは、所有している有効なアカウントが AD で有効な場合に限ります）。
ピア（Peer）	URI を登録しているクラスタ ピア。

各 FindMe ID の詳細なステータス情報を表示するには、**[アクション（Action）]** 列の **[編集（Edit）]** をクリックします。これは、登録またはサブスクリプションの失敗の診断に役立ちます。

Microsoft 製品との相互運用性のステータス

Microsoft の相互運用性についてのステータスを確認するには、**[ステータス（Status）] > [アプリケーション（Applications）] > [Microsoft 相互運用性（Microsoft Interoperability）]** に移動します。

このサービスは、Expressway と Microsoft サーバの間の SIP コールをルーティングします。

表示される情報は次のとおりです。

- Microsoft 相互運用性の B2BUA を通過する現在のコールの数
- 許可された Microsoft 相互運用性コールの数のパーセンテージとしてのリソース使用状況

TMS Provisioning Extension サービスのステータス

「TMS Provisioning Extension サービスのステータス（TMS Provisioning Extension service status）」ページ（**[ステータス（Status）] > > [アプリケーション（Applications）] > [TMS Provisioning Extension サービス（TMS Provisioning Extension services）] > [TMS Provisioning Extension サービスのステータス（TMS Provisioning Extension service status）]**）には、Expressway が接続されている（または接続しようとしている）各 Cisco TMSPE サービスのステータスが表示されます。

表示される各サービスのサマリの詳細は次のとおりです。

- 接続の現在のステータス。
- 新しいデータの最新の更新が実行された日時。
- 更新のためにサービスが最後にポーリングされた日時。
- 次回のポーリングの予定時刻。

[表示（View）] をクリックして、次を含むサービスに関する詳細を表示します。

- 接続障害に関するトラブルシューティング情報を含む接続ステータスと設定の追加情報。
- 実際に Cisco TMSPE サービスへの接続があるクラスタ内の Expressway（Expressway がクラスタの一部である場合にのみ表示）。
- 最新の更新の改訂番号を含む、サービスによって提供された各データテーブルの詳細と、それらのテーブル内のレコードを**表示**する機能。

Cisco TMS を使用してサービスの設定を変更することを推奨します。ただし、この Expressway の現在の設定はTMS プロビジョニング拡張サービスの設定ページ（**[システム（System）] > [TMS Provisioning Extension サービス（TMS Provisioning Extension services）]**）から変更できます。

詳細については、Expressway プロビジョニング サーバの項を参照してください。

プロビジョニングサーバのデバイス要求のステータス（CiscoTMSPE）

「デバイス要求のステータス（Device requests status）」ページ（**[ステータス（Status）]** > **[アプリケーション（Applications）]** > **[TMS Provisioning Extension サービス（TMS Provisioning Extension services）]** > **[デバイス要求（Device requests）]**）には、Cisco TMSPE を使用する際の Expressway プロビジョニング サーバのステータスが表示されます。

デバイス プロビジョニングが有効にされている場合、Expressway プロビジョニング サーバは Cisco TMS プロビジョニング（FindMe を含む）メカニズムを通じて Cisco TMS が提供したデータを使用して、プロビジョニング関連のサービスをプロビジョニング済みのデバイスに提供します。

Expressway はプロビジョニング データと FindMe データの Expressway への提供に Cisco TelePresence Management Suite Provisioning Extension（Cisco TMSPE）サービスのみをサポートしています。このモードでは、すべてのプロビジョニング データと FindMe データは、Cisco TMS 内のみで管理、維持されます。

プロビジョニング サーバ

このセクションにはサーバのステータスが表示され、Expressway が最後に再起動されてからサーバが受信したサブスクリプション要求のサマリが示されます。次の数値が表示されます。

- 受信したサブスクリプション要求の総数。
- プロビジョニング応答を正常に送信した要求数
- プロビジョニングを要求しているアカウントが見つからなかったことが原因で失敗した要求数
- プロビジョニングを要求しているアカウントに、そのアカウントに関連付けられたプロビジョニング済みのデバイスがなかったことが原因で失敗した要求数

モデル ライセンス

このセクションには、システム内で使用可能なプロビジョニング ライセンスのステータスが表示されます。表示される情報は次のとおりです。

- 総ライセンス数の上限と現在も使用可能な（制限のない）ライセンスの数
- この Expressway（または Expressway クラスタ）に登録されたデバイスが現在使用しているライセンスの数。この情報は、この Expressway がプロビジョニングしたデバイス タイプごとに分類されます。

ライセンス情報は、Cisco TMSPE デバイス サービスによって、Cisco TMS と Expressway 間で交換されます。デバイス サービスがアクティブになっていない場合は、Expressway のプロビジョニング サーバはデバイスをプロビジョニングできません。

ライセンス制限と制限のないライセンスの数は、Cisco TMS が管理しているすべての Expressway および Expressway クラスタが使用できるライセンスの全体数を示します。そのため、ライセ

ンス制限と制限のないカウント間の違いは、この特定の Expressway または Expressway クラスタに示される使用されたライセンスの数の合計と一致しない場合があります。

電話帳サーバ

電話帳サーバは、電話帳ディレクトリとルックアップ機能をプロビジョニング済みのユーザに提供します。

このセクションにはサーバのステータスが表示され、Expresswayが最後に再起動されてからプロビジョニング済みのユーザからサーバが受信した電話帳検索要求の数のサマリが示されます。

Cisco TMSPE サービスから提供されたユーザ レコード

[ステータス（Status）] > [アプリケーション（Applications）] > [TMSプロビジョニング拡張サービス（TMS Provisioning Extension services）] > [ユーザ（Users）] ...へ移動すると、Cisco TMSPE **ユーザ**サービスによって提供されるデータレコードを表示できます。次に、関連する表を示します。

- **アカウント（Accounts）**
- **グループ（Groups）**
- **テンプレート（Templates）**

選択したテーブルのすべてのレコードが表示されます。

（注） 一部のテーブルには数千個のレコードが含まれており、データが表示されるまでに時間がかかる場合があります。

ビューのフィルタリング

[フィルタ（Filter）] セクションでは、表示された一連のデータをフィルタリングできます。これは、表示する情報が複数ページにわたる場合にのみ表示されます。ステータス ページには、1 ページあたり 200 のレコードが表示されます。

各関連フィールドをフィルタするために使用するテキスト文字列を入力するか、または値を選択し、[フィルタ（Filter）] をクリックします。

選択したフィルタオプションのすべてに一致するレコードのみが表示されます。

（注） テキスト文字列のフィルタリングは、大文字と小文字を区別しません。

より詳細なレコードと関連するレコードの表示

[表示（View）] をクリックすると、選択したレコードに関するより詳細な情報が表示されます。多くのビューでは関連情報をクリックすると、その項目に関連付けられたデータ レコードを表示できます。たとえば、ユーザ グループを表示すると、関連するユーザ テンプレートにもアクセスできます。ユーザ アカウントを表示した場合、[プロビジョニングされたデータの確認] をクリックすると、そのユーザにプロビジョニングされるデータを確認できます。

Cisco TMSPE サービスが提供する FindMe レコード

Cisco TMSPE **FindMe** サービスから提供されたデータ レコードは、**Status** > **Applications** > **TMS Provisioning Extension services** > **FindMe** > **...** にアクセスして表示できます。次に、関連する表を示します。

- **[アカウント（Accounts）]**
- **ロケーション**
- **デバイス**

選択したテーブルのすべてのレコードが表示されます。

（注） 一部のテーブルには数千個のレコードが含まれており、データが表示されるまでに時間がかかる場合があります。

ビューのフィルタリング

[フィルタ（Filter）] セクションでは、表示された一連のデータをフィルタリングできます。これは、表示する情報が複数ページにわたる場合にのみ表示されます。ステータス ページには、1 ページあたり 200 のレコードが表示されます。

各関連フィールドをフィルタするために使用するテキスト文字列を入力するか、または値を選択し、[フィルタ（Filter）] をクリックします。

選択したフィルタオプションのすべてに一致するレコードのみが表示されます。テキスト文字列のフィルタリングでは大文字と小文字が区別されません。

より詳細なレコードと関連するレコードの表示

[表示（View）] をクリックすると、選択したレコードに関するより詳細な情報が表示されます。多くのビューでは関連情報をクリックすると、その項目に関連付けられたデータ レコードを表示できます。たとえば、FindMe ユーザを表示すると、関連する場所のレコードとデバイス レコードにもアクセスできます。

Cisco TMSPE サービスが提供する電話帳レコード

Cisco TMSPE **Phone books** サービスから提供されたデータレコードは、**Status** > **Applications** > **TMS Provisioning Extension services** > **Phone books** > **...** にアクセスして表示できます。次に、関連する表を示します。

- **フォルダ（Folders）**
- **エントリ（Entries）**
- **連絡先メソッド（Contact methods）**
- **ユーザ アクセス（User access）**

選択したテーブルのすべてのレコードが表示されます。

（注） 一部のテーブルには数千個のレコードが含まれており、データが表示されるまでに時間がかかる場合があります。

ビューのフィルタリング

[フィルタ（Filter）] セクションでは、表示された一連のデータをフィルタリングできます。これは、表示する情報が複数ページにわたる場合にのみ表示されます。ステータス ページには、1 ページあたり 200 のレコードが表示されます。

各関連フィールドをフィルタするために使用するテキスト文字列を入力するか、または値を選択し、[フィルタ（Filter）] をクリックします。

選択したフィルタオプションのすべてに一致するレコードのみが表示されます。

（注） テキスト文字列のフィルタリングは、大文字と小文字を区別しません。

より詳細なレコードと関連するレコードの表示

[表示（View）] をクリックすると、選択したレコードに関するより詳細な情報が表示されます。多くのビューでは関連情報をクリックすると、その項目に関連付けられたデータ レコードを表示できます。たとえば、電話帳のエントリを表示すると、関連する連絡先メソッドまたはフォルダにもアクセスできます。

プロビジョニングされたデバイス（Provisioned Devices）

「プロビジョニングされたデバイスのステータス（Provisioned device status）」ページ（**[ステータス（Status）]** > **[アプリケーション（Applications）]** > **[TMS Provisioning Extension サービス（TMS Provisioning Extension services）]** > **[プロビジョニングされたデバイスのステータ**

ス（**Provisioned device status**）]）には、Expresswayのプロビジョニングサーバにプロビジョニング要求を送信したすべてのデバイスのリストが表示されます。

ビューのフィルタリング

[フィルタ（Filter）] セクションでは、表示された一連のデータをフィルタリングできます。これは、表示する情報が複数ページにわたる場合にのみ表示されます。ステータス ページには、1 ページあたり 200 のレコードが表示されます。

各関連フィールドをフィルタするために使用するテキスト文字列を入力するか、または値を選択し、[フィルタ（Filter）] をクリックします。

選択したフィルタオプションのすべてに一致するレコードのみが表示されます。

（注） テキスト文字列のフィルタリングは、大文字と小文字を区別しません。

このリストには、現在および過去にプロビジョニングされたすべてのデバイスが表示されます。最初のプロビジョニング要求が行われた後にデバイスがリストに表示されます。**[アクティブ（Active）]** 列には、デバイスが現在プロビジョニングされているか（そのためにプロビジョニング ライセンスを消費しているか）が表示されます。

プロビジョニングされたデータの確認

「**プロビジョニングされたデータの確認（Check provisioned data）**」ページを使用して、Expressway のExpressway プロビジョニング サーバが特定のユーザとデバイスの組み合わせに提供する設定データを確認できます。

このページには、**[ユーザアカウント（User accounts）]** のステータスページからのみアクセスできます（**[ステータス（Status）]** > **[アプリケーション（Applications）]** > **[TMS Provisioning Extension サービス（TMS Provisioning Extension services）]** > **[ユーザ（Users）]** > **[アカウント（Accounts）]** に移動し、確認するユーザを見つけて **[プロビジョニングされたデータの確認（Check provisioned data）]** をクリックします）。

手順

ステップ 1 **[ユーザ アカウント名（User account name）]** に確認対象のユーザ アカウントの名前が表示されていることを確認します。

ステップ 2 ユーザエンド ポイント デバイスの **[モデル（Model）]** および **[バージョン（Version）]** を選択します。

エンドポイントが実際に使用している **[バージョン（Version）]** が表示されない場合は、最も近い以前のバージョンを選択します。

ステップ 3 [プロビジョニングされたデータの確認（Check provisioned data）] をクリックします。

[結果（Results）]セクションに、そのユーザとデバイスの組み合わせにプロビジョニングされるデータが表示されます。

アラームの管理

アラームは、再起動などの管理者の手動による介入が必要なイベントや設定変更がExpresswayで実行されたときに発生します。アラームは、ディスクやファンの不良、高温など、ハードウェアおよび環境に問題がある場合にも発生します。

「アラーム（Alarms）」ページ（**[ステータス（Status）]** > **[アラーム（Alarms）]**）には、システム上に現在発生しているすべてのアラーム（および、該当する場合は推奨される解決策）のリストが表示されます。Expressway 上で未確認のアラームが発生している場合、アラームアイコン  がすべてのページの右上部に表示されます。「**アラーム（Alarms）**」ページにアクセスするには、アラーム アイコンをクリックします。

各アラームは、アラーム リストの右端の列に表示される 5 桁のアラーム ID によって識別されます。アラームは次のカテゴリに分類されます。

アラーム ID プレフィクス	カテゴリ
10nnn	ハードウェアに関する問題
15nnn	ソフトウェアに関する問題
20nnn	クラスタに関する問題
25nnn	ネットワークおよびネットワーク サービスの設定
30nnn	ライセンス/リソース/オプション キー
35nnn	外部アプリケーションおよびサービス（ポリシーサービスやLDAP/AD設定など）
40nnn	セキュリティの問題（証明書、パスワードまたは安全でない設定など）
45nnn	全般的な Expressway 設定の問題
55nnn	B2BUA の問題
6nnnn	ハイブリッド サービス アラーム
60000 ～ 60099	管理コネクタ アラーム
60100 ～ 60199	カレンダー コネクタ アラーム

アラーム ID プレフィクス	カテゴリ
60300 ～ 60399	コール コネクタ アラーム
9nnnn	重要なイベントアラーム

Expressway で発生したすべてのアラームは、Cisco TMS チケットとしても発生します。アラームのすべての属性（ID、重大度など）が Cisco TMS に送信される情報に含められます。

アラームに対処するには、それぞれの**[アクション（Action）]**ハイパーリンクをクリックし、問題を解決するために必要な設定変更を行います。

アラームを確認すると（アラームを選択し、**[確認（Acknowledge）]** ボタンをクリック）Web UI にアラーム アイコンが表示されなくなりますが、アラームは「**アラーム（Alarms）**」ページに *[承認済み（Acknowledged）]* のステータスで表示されたままになります。新しいアラームが発生した場合は、アラーム アイコンが再び表示されます。

- 「**アラーム（Alarms）**」ページからアラームを削除することはできません。必要なアクションまたは設定変更が行われるまで、Expressway はアラームを削除しません。
- Expressway の再起動後、Expressway にまだ発生している *[確認済み（Acknowledged）]* のアラームが [新規（New）] のステータスで再表示されていたら、これを再確認する必要があります。
- この表示は、Expressway が最後に再起動されてからアラームが最初に発生した時点と最後に発生した時点を示します。
- Expressway がクラスタの一部である場合は、「**アラーム（Alarms）**」ページにそのクラスタ ピアで発生したすべてのアラームが表示されます。ただし、「「現在」」のピア（管理者として現在ログインしているピア）で発生したアラームのみしか確認できません。
- アラーム ID をクリックすると、そのアラームが生成および解除されたときのすべてのオカレンスを示すイベント ログのフィルタリング済みビューが生成されます。

発生する可能性がある特定のアラームに関する詳細については、アラーム参照を参照してください。

ログ

イベントログ

「イベントログ（Event Log）」ページ（**[ステータス（Status）]**> **[ログ（Logs）]**>**[イベントログ（Event Log）]**）では、最後のアップグレード以降にシステム上で発生したイベントのリストであるイベントログを表示し、検索することができます。

イベント ログには最大 2 GB のデータが保持され、このサイズに到達すると、最も古いエントリが上書きされます。ただし、最初の 50 MB のイベント ログ データのみは Web インターフェイスを通じて表示できます。

イベント ログのフィルタリング

[フィルタ（Filter）] セクションでは、イベント ログをフィルタリングできます。これは、表示する情報が複数ページにわたる場合にのみ表示されます。ログ ページには、1 ページあたり 1,000 個のレコードが表示されます。

検索する単語を入力して、[フィルタ（Filter）] をクリックします。入力したすべての単語が含まれているイベントのみが表示されます。

さらに詳細なフィルタリングを行うには、[more options] をクリックします。これにより、次のような追加のフィルタリング方式が提供されます。

- **[次の文字列を含む（Contains the string）]**：ここに入力した正確なフレーズを含むイベントのみが含まれます。
- **[次のいずれかの単語を含む（Contains any of the words）]**：ここに入力した単語のうち少なくとも 1 つを含むイベントが含まれます。
- **[次のいずれかの単語を含めない（Not containing any of the words）]**：ここに入力したいずれかの単語を含むイベントをフィルタで除外します。

（注） フィルタリングに使用する各単語を区切るには、スペースを使用します。

変更したフィルタ条件を再適用するには、**[フィルタ（Filter）]** をクリックします。ログの完全なリストに戻るには、[リセット（Reset）] をクリックします。

ログ文字列の再設定

「**ログ文字列の設定（Configure the log settings）**」ページをクリックすると、「ロギングの設定」ページに移動します。このページから、イベント ログに記録されたイベント レベルを設定でき、イベント ログをコピーできるリモート サーバも設定できます。

ローカル ディスクへの結果の保存

結果セクションの内容をローカル PC またはサーバ上のテキスト ファイルにダウンロードする場合は、[このページを**ダウンロード**（Download this page）] をクリックします。

[結果（Results）] セクション

[結果（Results）] セクションには、現在のフィルタ条件に一致するすべてのイベントが最新のものから順番に表示されます。

ほとんどの **tvcs** イベントでは、1 つ以上のフィールドにハイパーリンクが含まれています（そのようなフィールドは、その上にカーソルを合わせると色が変わります）。ハイパーリンクを

クリックして、同じテキスト文字列を含むイベントのみを表示できます。たとえば、**[Event=]** の後に表示されるテキストをクリックすると、その特定タイプのすべてのイベントが表示されるようにリストがフィルタリングされます。同様に、特定の **[コール ID（Call-Id）]** をクリックすると、その特定のコールへの参照を含んでいるイベントのみが表示されます。

イベント ログのカラー コード

イベントログ内の特定のイベントは色分けされているため、簡単に特定することができます。これらのイベントは次のとおりです。

緑色のイベント：

- System Start
- Admin Session Start/Finish
- Installation of <item> succeeded
- Call Connected
- Request Successful
- Beginning System Restore
- Completed System Restore

オレンジ色のイベント：

- System Shutdown
- Intrusion Protection Unblocking

紫色のイベント：

- Diagnostic Logging

赤色のイベント：

- Registration Rejected
- Registration Refresh Rejected
- Call Rejected
- Security Alert
- License Limit Reached
- Decode Error
- TLS Negotiation Error
- External Server Communications Failure
- Application Failed
- Request Failed
- System Backup Error

- System Restore Error
- Authorization Failure
- Intrusion Protection Blocking

イベントログの形式と内容の詳細については、イベントログ形式とイベントとレベルを参照してください。

設定ログ

「設定ログ（Configuration Log）」ページ（**[ステータス（Status）] > [ログ（Logs）] > [設定ログ（Configuration Log）]**）には、Expressway 設定に対して行われたすべての変更がリストされます。

設定ログは最大で 30 MB のデータを保持し、このサイズに達すると最も古いエントリが上書きされます。Web インターフェイスを使用して設定ログ全体を表示できます。

設定ログのフィルタリング

[フィルタ（Filter）] セクションでは、設定ログをフィルタリングできます。これは、表示する情報が複数ページにわたる場合にのみ表示されます。ログページには、1 ページあたり 1,000 個のレコードが表示されます。

検索する単語を入力して、[フィルタ（Filter）] をクリックします。入力したすべての単語が含まれているイベントのみが表示されます。

さらに詳細なフィルタリングを行うには、[more options] をクリックします。これにより、次のような追加のフィルタリング方式が提供されます。

- **[次の文字列を含む（Contains the string）]**：ここに入力した正確なフレーズを含むイベントのみが含まれます。
- **[次のいずれかの単語を含む（Contains any of the words）]**：ここに入力した単語のうち少なくとも 1 つを含むイベントが含まれます。
- **[次のいずれかの単語を含む（Contains any of the words）]**：ここに入力した単語のうち少なくとも 1 つを含むイベントが含まれます。

（注） フィルタリングに使用する各単語を区切るには、スペースを使用します。

変更したフィルタ条件を再適用するには、**[フィルタ（Filter）]** をクリックします。ログの完全なリストに戻るには、[リセット（Reset）] をクリックします。

[結果（Results）] セクション

[結果（Results）] セクションにはすべての Web ベース イベントが表示されます。最新のイベントが先頭に示されます。

ほとんどのイベントでは、1 つ以上のフィールドにハイパーリンクが含まれています（そのようなフィールドは、その上にカーソルを合わせると色が変わります）。ハイパーリンクをクリックして、同じテキスト文字列を含むイベントのみを表示できます。たとえば、[Event=] の後に表示されるテキストをクリックすると、その特定タイプのすべてのイベントが表示されるようにリストがフィルタリングされます。同様に、特定の**ユーザ**をクリックすると、その特定管理者アカウントに関連するイベントのみが表示されます。

設定ログに表示されるすべてのイベントがレベル 1 のイベントとして記録されます。そのため、ロギングの設定を変更しても設定ログでのそのプレゼンスに影響はありません。

設定ログ イベント

Web インターフェイスを使用して管理者が行った Expressway 設定への変更には *[*システム設定の変更（*System Configuration Changed*）*]* というイベント フィールドがあります。

これらのイベントごとに、**[詳細（Detail）]** フィールドに次の情報が示されます。

- 影響を受けた設定項目
- 変更前と変更後の内容
- 変更を加えた管理者ユーザの名前、および IP アドレス
- 変更が行われた日時

ネットワーク ログ

「ネットワーク ログ（Network Log）」ページ（**[ステータス（Status）] > [ログ（Logs）] > [ネットワークログ（Network Log）]**）には、この Expressway にログオンしたコールシグナリングメッセージのリストが表示されます。

ネットワーク ログには最大 2 GB のデータが保持され、このサイズに到達すると、最も古いエントリが上書きされます。ただし、最初の 50 MB のネットワーク ログ データを Web インターフェイスを通じて表示できます。

ネットワーク ログのフィルタリング

[フィルタ（Filter）] セクションでは、ネットワーク ログをフィルタリングできます。これは、表示する情報が複数ページにわたる場合にのみ表示されます。ログ ページには、1 ページあたり 1,000 個のレコードが表示されます。

検索する単語を入力して、[フィルタ（Filter）] をクリックします。入力したすべての単語が含まれているイベントのみが表示されます。

さらに詳細なフィルタリングを行うには、[more options] をクリックします。これにより、次のような追加のフィルタリング方式が提供されます。

- **[次の文字列を含む（Contains the string）]**：ここに入力した正確なフレーズを含むイベントのみが含まれます。

- **[次のいずれかの単語を含む（Contains any of the words）]**：ここに入力した単語のうち少なくとも 1 つを含むイベントが含まれます。
- **[次のいずれかの単語を含めない（Not containing any of the words）]**：ここに入力したいずれかの単語を含むイベントをフィルタで除外します。

（注） フィルタリングに使用する各単語を区切るには、スペースを使用します。

変更したフィルタ条件を再適用するには、**[フィルタ（Filter）]** をクリックします。ログの完全なリストに戻るには、[リセット（Reset）] をクリックします。

ログ文字列の再設定

「ログ文字列の設定（Configure the log settings）」ページをクリックすると、[ネットワーク ログ レベルの設定]ページに移動します。このページから、ネットワーク ログに記録されたイベント レベルを設定できます。

ローカル ディスクへの結果の保存

結果セクションの内容をローカル PC またはサーバ上のテキスト ファイルにダウンロードする場合は、**[このページをダウンロード（Download this page）]** をクリックします。

[Results] セクション

[結果（Results）] セクションには、ネットワーク ログ モジュールそれぞれがログに記録したイベントが表示されます。

ほとんどのイベントでは、1 つ以上のフィールドにハイパーリンクが含まれています（そのようなフィールドは、その上にカーソルを合わせると色が変わります）。ハイパーリンクをクリックして、同じテキスト文字列を含むイベントのみを表示できます。たとえば、**[Module=]** の後ろに表示されたテキストをクリックすると、リストがフィルタリングされ、その特定のタイプのすべてのイベントが表示されます。

ネットワーク ログに表示されるイベントは、「ネットワーク ログ レベルの設定」ページで設定されたログ レベルによって異なります。

ハードウェア ステータス

「ハードウェア（Hardware）」ページ（**[ステータス（Status）]>[ハードウェア（Hardware）]**）には、Expressway アプライアンスの物理的なステータスに関する情報が表示されます。

表示される情報は次のとおりです。

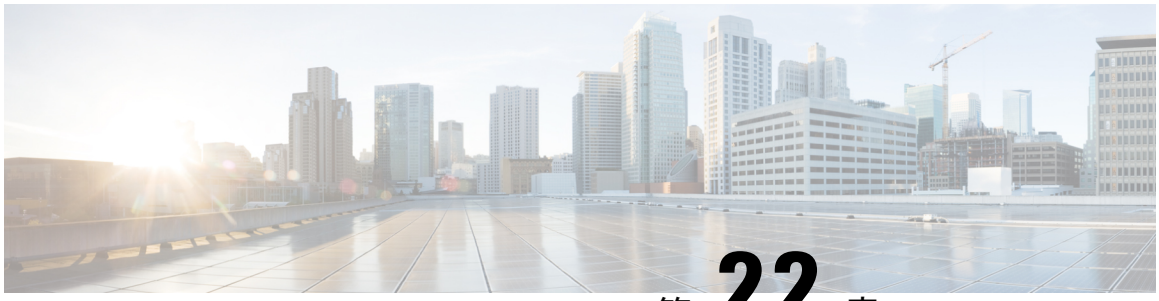
- ファンの回転速度
- コンポーネントの温度

- コンポーネントの電圧

標準的な制限の範囲外で動作しているコンポーネントの特定に役立つように、適正な最小レベルと最大レベルが表示されます。

警告 自分で装置を点検しないでください。カバーを開けたり、取り外したりすると、感電やそのほかの危険があり、保証の適用対象外となります。点検については、資格のある担当者にお問い合わせください。

（注） Expressway が VMware で動作している場合は、ハードウェアのステータス情報は表示されません。



第 22 章

メンテナンス

ここでは、**[設定（Configuration）]>[メンテナンス（Maintenance）]** メニューのオプションについて説明します。

メンテナンスモードを有効にする

メンテナンス モードは通常、アップグレードが必要な場合やクラスタの一部である Expressway ピアの動作を停止する場合に使用します。これにより、他のクラスタピアは通常どおりに動作し続けますが、メンテナンス モードのピアはアップグレードまたは処理が行われます。ピアをメンテナンス モードにすると、それ以降は制御された方法で登録を中止したりコールのそのピアでの管理を中止できます。

ピアがメンテナンス モードになっている間にアラームが発生します。**「リソース使用状況（Resource usage）」** ページ（**[ステータス（Status）]>[システム（System）]>[リソース使用状況（Resource usage）]**）をモニタし、そのピアで現在処理されている登録とコールの数を確認します。

ピアがメンテナンスモードの場合、そのワークロードは他のクラスタノードによって処理されます。したがって、大規模なマルチテナント導入または MRA 導入の場合、他のノードの過負荷を回避するために、一度に 1 つのピアでのみメンテナンスモードを有効にすることをお勧めします。

アクティブコールおよび登録への影響

標準 Expressway セッション（MRA ではない）

- 新しいコールや登録は、クラスタ内の別のピアによって処理されます。
- 既存の登録は期限が切れると別のピアに登録されます（エンドポイントの設定とDNS SRV レコードのセットアップに関する詳細については、『*Expressway* クラスタ作成および保守導入ガイド』を参照してください）。
- 既存のコールはコールが終了するまで継続します。

Unified CM MRA セッション

Expresswayは、新しいコールまたはプロキシ（MRA）トラフィックの受け入れを停止します。既存のコールとチャット セッションは影響を受けません。

ユーザがセッションを正常に終了すると、システムは、特定のタイプのトラフィックを処理していない時点に到達し、そのサービスをシャットダウンします。

Expresswayがメンテナンスモード中、ユーザが新しいコールを発信または新しいチャットセッションを開始しようとすると、クライアントはサービス利用不可応答を受信し、他のピアを使用するように選択できます（可能な場合）。このフェールオーバーの動作はクライアントによって異なりますが、クラスタ内に実行中のピアがある場合、クライアントの再起動により、接続の問題を解決する必要があります。

[ユニファイドコミュニケーションのステータス（Unified Communications status）]ページには、MRA サービスが影響を受けるすべての場所（メンテナンスモード）が示されます。

メンテナンスモードを有効にするプロセス

1. 該当するピアにログインします。
2. 「メンテナンス モード（**Maintenance mode**）」ページ（**[メンテナンス（Maintenance）]**> **[メンテナンス モード（Maintenance mode）]**）に移動します。
3. **[メンテナンス モード（Maintenance mode）]** を *[オン（On）]* に設定します。
4. 確認ダイアログボックスで **[保存（Save）]** をクリックし、**[OK]** をクリックします。

（注） ピアが再起動すると、メンテナンス モードは自動的に無効になります。

手動でコールまたは登録を削除する方法

自動的にクリアしないコールまたは登録を手動で削除するには

- **[ステータス（Status）] > [コール（Calls）]** に移動して、**[すべて選択（Select all）]** をクリックし、**[切断（Disconnect）]** をクリックします（SIP コールがすぐに切断されない場合があります）。
- デバイスによる **[ステータス（Status）] > [登録（Registrations）] > [デバイスで（By device）]** に移動し、**[すべて選択（Select all）]**をクリックしてから **[登録解除（Registration）]** をクリックします。

Conference Factory の登録を終了できます。他のピアには独自の Conference Factory 登録があるため（有効になっている場合）、これはコールのソースにはならず、削除されても別のピアにロールオーバーされません。

Expressway への SSH アクセスの有効化

パスワードベースのログインを必要とすることなく安全にアクセスできるように、Expressway へのアクセスに SSH を有効にすることができます。これは一般に、モニタリングとロギングの効率を高めることを目的としています。この方法でアクセスする Expressway ごとにこの手順を繰り返す必要があります。

⚠

注意 公開キーを許可するには、root アクセスを使用します。セキュリティ上のリスクを増大させたり、サポートされていない設定をしたりしないように注意が必要です。`root` の使用は避けてください。

手順

ステップ 1 SSH を使用して `root` としてログインします。

ステップ 2 `.ssh` ディレクトリがまだない場合は、`mkdir /tandberg/.ssh` と入力して、このディレクトリを作成します。

ステップ 3 `/tandberg/.ssh` に公開キーをコピーします。

ステップ 4 `authorized_keys` ファイルに `cat /tandberg/.ssh/id_rsa.pub >> /tandberg/.ssh/authorized_keys` を使用して公開キーを追加します。

id_rsa.pub は、公開キーの名前で置き換えてください。自分のキーをほかの場所に配置しないでください。アップグレード時に失われる可能性があります（`authorized_keys` ファイルが維持されません）。

ステップ 5 ログオフし、自分のキーを使用して SSH アクセスをテストします。

自分のキーで Expressway にアクセスできない場合は、`root` として接続し、`/etc/init.d/sshd restart` を使用して SSH デーモンを再起動します。

Expressway ソフトウェアのアップグレード

ここでは、Expressway ソフトウェアコンポーネントの新しいリリースを既存のシステムにインストールする方法について説明します。コンポーネントのアップグレードは、次の 2 つの方法のいずれかで実行できます。

- **Web インターフェイスの使用 - [メンテナンス（Maintenance ）] > [アップグレード（Upgrade）]** ページを使用した推奨される方法。手順の詳細については、該当するソフトウェアのリリースノートを参照してください。
- **セキュアコピー**（SCP/PSCP）の使用 - 代替方法。この方法は、ネットワーク接続が遅い、または不安定であるなど、特定の場合に役立ちます。

ダウングレードのサポートなし

以前のバージョンへのダウングレードはサポートされていません。

セキュア コピー（SCP/PSCP）を使用したアップグレード

オプションで、このプロセスを使用して、SCP や PSCP（PuTTY無料パッケージの一部）などのセキュアコピープログラムを使用してアップグレードし、ソフトウェアイメージを含むファイルをシステムに転送します。

はじめる前に

このプロセスでは、ソフトウェアイメージファイルを、システムが期待するファイル名に手動で名前を変更する必要があります。デフォルト名（*s42700xXX_XX_XX.tar.gz* と同様）でファイルをアップロードし、アップグレードを開始（インストール）する準備ができている場合にのみ名前を変更することをお勧めします。これにより、プロセスの制御が向上し、続行する前にファイルサイズを確認できます。

ソフトウェアのバージョンによっては、*release-key* ファイルのインストールが必要な場合があります。

手順

ステップ 1 ソフトウェアイメージファイルをアップロードします。

- **システムプラットフォーム**コンポーネント の場合は、システムの /tmp フォルダにアップロードします。例：*scp s42700x12_5_7.tar.gz root@10.0.0.1:/tmp/s42700x12_5_7.tar.gz*
- 他のコンポーネントについては、ファイル名と拡張子を変更しないままシステムの */tmp/pkgs/new/* フォルダにアップロードします。例：*scp root@10.0.0.1:/tmp/pkgs/new/vcs-lang-es-es_8.1_amd64.tlp*

ステップ 2 ファイルのアップロードが完了するまで待ち、ファイルサイズを確認します。デフォルトの */tmp* での */tmp/tandgz-image.tar.gz* ファイルエントリ は 0 バイトです。

ステップ 3 アップグレードを開始する準備ができたら、ファイルの名前を */tmp/tandgz-image.tar.gz* の必要なファイル名に変更（または移動）します（アップグレードプロセスが開始されます）。

例：*mv /tmp/s42700x12_5_7.tar.gz /tmp/tandgz-image.tar.gz*

ステップ 4 プロンプトが表示されたら、root パスワードを入力します。ソフトウェアのインストールが自動的に開始され、SSH/ コンソールで「ソフトウェアアップグレード進行中」と表示されます。

ステップ 5 ソフトウェアが完全にインストールされ、「 のアップグレードが完了するまで待ちます! 新しいソフトウェアは次の再起動時」に使用されます。

ステップ 6 再起動する前に行われた設定変更は、**システムの再起動時に失われるため**、システムをすぐに再起動することをお勧めします 。

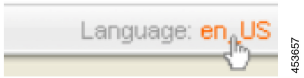
ファームウェアのアップグレード（物理アプライアンスのみ）

このセクションの説明は、Expressway が物理アプライアンス上に導入されていて、何らかの理由でファームウェアをアップグレードする必要がある場合に適用されます。

アップグレードを行うには、Cisco Host Upgrade Utility（HUU）を使用します。これは、UCS C シリーズ サーバ上のファームウェア コンポーネントをアップグレードするためのシスコの専用ツールです。HUU の使用方法について詳しくは、Cisco UCS C シリーズ ラック サーバ ドキュメント ページに用意されている最新の『*Cisco HostUpgrade* ユーティリティ ユーザ ガイド』を参照してください。

言語設定

「言語（Language）」ページ（**[メンテナンス（Maintenance）] > [言語（Language）]**）で、Web ユーザインターフェイスに表示されるテキストに使用する言語を制御します。

	また、「**言語（Language）**」ページには、すべてのページの下部にある**[言語（Language）]** リンクをクリックしても移動することができます。

言語の変更

デフォルトの言語と、個々のブラウザで使用する言語の両方を設定できます。

フィールド	説明	使用方法のヒント
システムのデフォルト言語（**System default language**）	Web インターフェイスで使用されるデフォルト言語。	これは管理者セッションとユーザ（FindMe）セッションに適用されます。インストールされた言語パッケージのセットから選択できます。
このブラウザ（**This browser**）	現在のクライアント マシンの現在のブラウザで使用する言語。これは、システムのデフォルト言語か特定の代替言語のいずれかを使用するように設定できます。	この設定はクライアント コンピュータで現在使用しているブラウザに適用されます。別のブラウザまたは別のコンピュータを使用している Expressway ユーザ インターフェイスにアクセスすると、別の言語が設定されている場合があります。

言語パックのインストール

新しい言語パックをインストールしたり、既存の言語パックの更新バージョンをインストールしたりできます。

言語パックは Expressway ソフトウェア ファイルを取得したときと同じ cisco.com のエリアからダウンロードできます。使用可能なすべての言語が 1 つの言語パックの zip ファイルに含まれています。ソフトウェア リリースと一致する、適切な言語パック バージョンをダウンロードします。

言語パックをダウンロードした後に、ファイルを解凍して一連の .tlp ファイルを抽出します。サポートされている言語ごとに 1 つのファイルがあります。

使用可能な言語のリストについては、使用しているソフトウェア バージョンの関連リリース ノートを参照してください。

（注）

- 英語（en_us）はデフォルトでインストールされ、常に使用できるようになっています。
- 独自の言語パッケージは作成できません。言語パックはシスコからのみ取得できます。
- Expressway ソフトウェアの最新バージョンにアップグレードすると、「「Language pack mismatch」」のアラームが表示されます。関連付けられた言語パックの最新バージョンをインストールし、すべてのテキストが選択した言語で使用できることを確認する必要がある場合があります。

.tlp の言語パッケージ ファイルをインストールするには、次の手順を実行します。

手順

ステップ 1 **[メンテナンス（Maintenance）] > [言語（Language）]** に移動します。

ステップ 2 **[参照（Browse）]** をクリックし、アップロードする **.tlp** 言語パッケージをクリックします。

ステップ 3 [Install] をクリックします。

選択した言語パックが検証され、アップロードされます。これには数秒かかることがあります。

ステップ 4 別の言語をインストールするには、ステップ 2 と 3 を繰り返します。

言語パッケージの削除

言語パッケージを削除するには、次の手順を実行します。

手順

ステップ 1 **「言語（Language）」**ページ（**[メンテナンス（Maintenance）] > [言語（Language）]**）に移動します。

ステップ 2 インストールされた言語パックのリストから、削除する言語パッケージを選択します。

ステップ 3 [Remove] をクリックします。

ステップ 4 確認を求めるメッセージが表示された場合は、**[はい（Yes）]** をクリックします。

選択した言語パックが削除されます。これには数秒かかることがあります。

Expressway データのバックアップと復元

「バックアップと復元（Backup and restore）」ページ（**[メンテナンス（Maintenance）] > [バックアップと復元（Backup and restore）]**）を使用して、Expressway データのバックアップファイルを作成し、Expressway を以前保存した設定に復元します。

バックアップ ファイルを作成するタイミング

バックアップを定期的に作成し、さらに次の状況でも常に作成することをお勧めします。

- アップグレードを実行する前
- システムの復元を実行する前
- デモ環境およびテスト環境（既知の設定に Expressway を復元できるようにする場合）

バックアップ内容

バックアップ ファイルに保存されるデータは次のとおりです。

- ブートス トラップ キー（X8.11 以降）
- システム構成時の設定
- クラスタリング設定
- ローカル認証データ（リモートで管理するアカウントの Active Directory クレデンシャルではありません）。
  - ユーザ アカウントとパスワードの詳細
  - サーバ セキュリティ証明書と秘密キー
- コールの詳細レコード（Expressway の CDR サービスが有効になっている場合）

バックアップ ファイルには、ログ ファイルは含まれません。

バックアップと復元の手順の詳細については、「システム バックアップの作成および以前のバックアップの復元」を参照してください。

クラスタ化システム

クラスタ内のピアのバックアップと復元の詳細については、次を参照してください。

クラスタのアップグレード、バックアップ、および復元

システム バックアップの作成

はじめる前に

- バックアップファイルは常に暗号化されるようになっています（X8.11 以降）。バックアップ ファイルにはブートストラップ キー、認証データ、およびその他の機密情報が含まれるためです。
- バックアップを復元できるシステムは、**そのバックアップを作成したソフトウェアと同じバージョンを実行しているシステム**に限られます。
- ある Expressway でバックアップを作成し、別の Expressway でこのバックアップを復元することができます。たとえば、元のシステムが失敗した場合などです。復元するには、古いシステムで使用していたのと同じオプション キーを新しいシステムにインストールする必要があります。

  別の Expressway で実行したバックアップを復元しようとすると警告メッセージが表示されますが、続行できます。

（FIPS140-2 暗号化モードを使用している場合）FIPS 非準拠システムで作成されたバックアップを FIPS モードで稼動するシステム上で復元することはできません。FIPS 準拠システムのバックアップを FIPS 非準拠システム上で復元することはできます。

- Expressway 間のデータをコピーするためにバックアップを使用しないでください。使用すると、システム固有情報（IP アドレスなど）が重複します。
- バックアップ ファイルには機密情報が含まれるため、テクニカル サポートを受ける場合にこの情報をシスコに送らないでください。代わりにスナップショットと診断ファイルを使用します。

パスワード

- バックアップすべてパスワードで保護されている必要があります。
- 以前のバックアップを復元する際、そのバックアップの作成後に管理者アカウントのパスワードが変更されている場合は、復元後最初にログインするときに、古いパスワードを入力する必要があります。
- Active Directory のクレデンシャルは、システムのバックアップ ファイルに含まれて**いません**。NTLM のデバイス認証を使用する場合は、Active Directory のパスワードを入力して復元後に Active Directory ドメインに再参加する必要があります。
- バックアップと復元するためには、緊急アカウントのパスワードを標準的な管理者アカウント パスワードと同じように処理します。

プロセス

Expressway システム データのバックアップを作成するには、次の手順を実行します。

手順

ステップ 1 **[メンテナンス（Maintenance）] > [バックアップと復元（Backup and Restore）]** に移動します。

ステップ 2 [暗号化パスワード（Encryption password）] に、バックアップ ファイルの暗号化に使用するパスワードを入力します。

注意 バックアップファイルを復元する際は、このパスワードが必要になります。

ステップ 3 [システム バックアップ ファイルの作成（Create system backup file）] をクリックします。

ステップ 4 バックアップ ファイルが作成されるまで待機します。これには数分かかることがあります。ファイルが準備されている間は、このページから移動しないでください。

ステップ 5 バックアップ ファイルが作成されると、ファイルを保存するように求められます。デフォルトのファイル名では次の形式が使用されます：**<software version><hardware serial number><date><time>_backup.tar.enc** Internet Explorer を使用している場合、デフォルトのファ

イル拡張子は **.tar.gz.gz** となります。（ファイル名の拡張子がこのように異なっても運用上の影響はありません。サポート対象のブラウザを使用してバックアップ ファイルを作成し、復元できます。）

ステップ 6 セキュアな場所にバックアップ ファイルを保存します。

以前のバックアップの復元

はじめる前に

⚠

注意 CE1100 またはそれ以前のアプライアンスのバックアップから CE1200 アプライアンスに Expressway-E を復元する場合、CE1200 アプライアンスは Expressway-C として復元される場合があります。この問題が発生するのは、CE1100 または以前のアプライアンスでサービス セットアップ ウィザードを使用してタイプを Expressway-C に変更した後、ウィザードをスキップして設定を完全に完了しなかった場合です。この問題を回避するには、アプライアンスをバックアップする前に、サービス セットアップ ウィザードを実行してタイプを Expressway-E に変更し、ウィザードを完了するようにしてください。

- 復元するバックアップ ファイルのパスワードが必要です。
- 別の Expressway からバックアップファイルを復元する場合は、復元元のシステムに存在しているのと同じライセンスキーを適用する必要があります。
- 復元を実行する前に、Expressway ユニットのサービスを停止の状態にすることを推奨します。
- 復元プロセスには、元のソフトウェアバージョンに戻す**初期設定へのリセット**が含まれます。その後、**バックアップの作成時に実行していたのと同じソフトウェアバージョン**へのアップグレードを行います。
- バックアップが古い場合（希望するバージョンよりも以前のバージョンで作成されていた場合）は、復元後に次の追加手順を実行する必要があります。
  1. ソフトウェア バージョンを必要な最新バージョンにアップグレードします。
  2. バックアップの作成後に加えられたすべての設定変更を手動でやり直します。
- （FIPS140-2 暗号化モードを使用している場合）FIPS 非準拠システムで作成されたバックアップを FIPS モードで稼動するシステム上で復元することはできません。FIPS 準拠システムのバックアップを FIPS 非準拠システム上で復元することはできます。
- システムがクラスタの一部である場合には Expressway にデータを復元できません。クラスタから最初に削除する必要があります。詳細については、クラスタのアップグレード、バックアップ、および復元を参照してください。

パスワード

- バックアップはパスワードで保護されている必要があります。
- 以前のバックアップを復元する際、そのバックアップの作成後に管理者アカウントのパスワードが変更されている場合は、復元後最初にログインするときに、古いパスワードを入力する必要があります。
- Active Directory のクレデンシャルは、システムのバックアップ ファイルに含まれて**いません**。NTLM のデバイス認証を使用する場合は、Active Directory のパスワードを入力して復元後に Active Directory ドメインに再参加する必要があります。
- バックアップと復元するためには、緊急アカウントのパスワードを標準的な管理者アカウント パスワードと同じように処理します。

プロセス

Expressway を以前の設定のシステム データに復元するには、次の手順を実行します。

手順

ステップ 1 最初に、デフォルト設定の復元（初期設定へのリセット）の手順に従って初期設定にリセットします。これにより、設定データが削除され、システムが元の状態に戻ります。システムを最初にセットアップしてからアップグレードしている場合は、リセットしても現在のソフトウェア バージョンが維持されます。

ステップ 2 バックアップの作成時に実行していたのと同じソフトウェアバージョンにシステムをアップグレードします。

- スタンドアロン システムについては、「アップグレード手順」を参照してください。
- クラスタ化システムの場合は、『*Expressway Cluster Creation and Maintenance Deployment Guide*』を参照してください。

ステップ 3 これで次のようにバックアップからシステムを復元することができます。

1. **[メンテナンス（Maintenance）]** > **[バックアップと復元（Backup and Restore）]** に移動します。
2. **[復元（Restore）]** セクションで **[参照（Browse）]** をクリックし、復元するバックアップ ファイルを選択します。
3. **[復号パスワード（Decryption password）]** フィールドに、バックアップ ファイルの作成に使用したパスワードを入力します。
4. [システム バックアップ ファイルのアップロード（Upload system backup file）] をクリックします。

5. Expressway がファイルを確認した後、「**復元の確認（Restore confirmation）**」ページが表示されます。
   - バックアップ ファイルが無効である場合、または誤った復号パスワードが入力された場合は、**[バックアップと復元（Backup and restore）]** の上部にエラー メッセージが表示されます。
   - 現在のソフトウェア バージョンとコール数と登録数が表示されます。
6. 表示される警告メッセージを確認してから続行します。
7. 復元を続行するには、**[システムの復元を続行する（Continue with system restore）]** をクリックします。

   これにより、システムが再起動するため、アクティブ コールがないことを確認します。
8. システムの再起動後、「**ログイン（Login）**」ページが表示されます。

ステップ 4 バックアップ ファイルが古い場合のみ、この手順が適用されます。つまり、バックアップの作成後にソフトウェアバージョンがアップグレードされた場合、システム設定が変更された場合です。この場合、次のように計算します。

1. システムを再びアップグレードします。この場合は、システムに必要なソフトウェア バージョンにアップグレードします。
2. バックアップ後に加えた設定変更をやり直します（復元したシステムでその変更がまだ必要な場合）。

パターンの効果の確認

[パターンの確認（Check pattern）] ツール（**[メンテナンス（Maintenance）]** > **[ツール（Tools）]** > **[パターンの確認（Check pattern）]**）では、Expressway に設定するパターンまたはトランスフォーメーションで期待した結果を得られるかどうかをテストできます。

次の設定時にパターンを使用できます。

- 検索前トランスフォーメーションの設定で何らかの検索を実行する前に変換するエイリアスを指定する
- 検索ルールの設定で検索するエイリアスに基づいて検索をフィルタリングし、検索をゾーンに送信する前にエイリアスを変換する

このツールを使用するには、次の手順を実行します。

手順

ステップ 1 トランスフォーメーションに対してテストする **[エイリアス（Alias）]** を入力します。

ステップ 2 **[パターン（Pattern）]** セクションで、テストする **[パターン文字列（Pattern string）]** の **[パターン タイプ（Pattern type）]** と **[パターン動作（Pattern behavior）]** の組み合わせを入力します。

- **[パターン動作（Pattern behavior）]** に *[置換（Replace）]* を選択した場合は、**[置換文字列（Replace string）]** も入力する必要があります。
- **[パターン動作（Pattern behavior）]** に *[プレフィックスの追加（Add prefix）]* または *[サフィックスの追加（Add suffix）]* を選択した場合は、**[パターン文字列（Pattern string）]** の前または後ろに追加する **[追加テキスト（Additional text）]** 文字列も入力する必要があります。
- Expresswayには、特定の設定要素との照合に使用できる、事前に設定された一連のパターン マッチングの変数が備わっています。

ステップ 3 **[パターンの確認（Check pattern）]** をクリックし、エイリアスがパターンと一致するかどうかをテストします。

[結果（Result）] セクションに、エイリアスがパターンと一致するかどうかが示され、結果のエイリアス（該当する場合はトランスフォーメーションの効果も含む）が表示されます。

エイリアスの検出

[検索（Locate）] ツール（**[メンテナンス（Maintenance）]** > **[ツール（Tools）]** > **[検索（Locate）]**）では、Expressway が指定したエイリアスで識別されたエンドポイントを、指定した「ホップ」回数以内に、そのエンドポイントに実際にコールを発信することなく検出できるかどうかをテストできます。

このツールは、ダイヤル プランやネットワーク導入の問題を診断する際に役立ちます。

手順

ステップ 1 検索する **[エイリアス（Alias）]** を入力します。

ステップ 2 検索の **[ホップ カウント（Hop count）]** を入力します。

ステップ 3 検索を開始するために使用する **[プロトコル（Protocol）]** として *[H.323]* または *[SIP]* のいずれかを選択します。検索プロセス時に検索がインターワーキングされる可能性がありますが、Expressway は常にネイティブ プロトコルを最初に使用して検索ルールと関連付けられた同じプライオリティのターゲット ゾーンとポリシー サービスを検索してから、代替プロトコルを使用して、それらのゾーンを再度検索します。

ステップ 4 検索要求をシミュレーションする **[ソース（Source）]** を選択します。*[デフォルトゾーン（Default Zone）]*（不明なリモートシステム）、*[デフォルトサブゾーン（Default Subzone）]*（ローカルに登録されたエンドポイント）、またはそのほかの設定済みのゾーンまたはサブゾーンから選択します。

ステップ 5 要求を **[認証済み（Authenticated）]** として処理するかどうかを選択します（認証されたメッセージのみに適用するように検索ルールを制限できます）。

ステップ 6 任意で、[送信元エイリアス（Source alias）] を入力することができます。通常、これは、送信元エイリアスに依存するルールがある CPL をルーティング プロセスで使用している場合にのみ関係します（値が指定されていない場合は、デフォルトのエイリアスの `xcom-locate` が使用されます）。

ステップ 7 **[検索（Locate）]** をクリックして検索を開始します。

ステータス バーに **[検索しています...（Searching...）]** と表示され、その後に **[検索が完了しました（Search completed）]** と表示されます。結果には、検索したゾーンのリスト、適用したトランスフォーメーションとコールポリシー、検出された場合はエイリアスが存在するゾーンが含まれます。

検索プロセスは、選択した **[送信元ゾーン（Source zone）]** から Expressway がコール要求を受信したかのように実行されます。詳細については、コール ルーティング プロセスの項を参照してください。

ポートの使用

[メンテナンス（Maintenance）] > **[ツール（Tools）]** > **[ポートの使用状況（Port usage）]** メニューのページは、Expressway で設定されたすべての IP ポートが表形式で表示されます。

これらのページに表示される情報は、その特定の Expressway に固有のもので、Expressway の設定、インストールされたオプション キー、および有効になっている機能によって異なります。

情報はページのどの列ででも並べ替えることができ、IP ポート別や IP アドレス別にリストをソートできます。

各ページには **[CSV にエクスポート（Export to CSV）]** オプションがあります。これによって、スプレッドシート アプリケーションで開くのに適した CSV（カンマ区切り値）形式のファイルに情報を保存できます。

IP ポートは IPv4 アドレスおよび IPv6 アドレス用に個別に設定できません。また、2 つの LAN インターフェイスのそれぞれに設定することもできません。つまり、これは、IP ポートを特定のサービス（SIP、UDP など）用に設定した後は、Expressway 上のそのサービスのすべての IP アドレスに適用されます。これらのページの表にはすべての IP ポートとすべての IP アドレスのリストが表示されるため、Expressway の設定によっては、単一の IP ポートが最大 4 回リストに表示される場合があります。

ポート情報は次のページに分割されています。

- ローカル インバウンド ポート
- ローカル アウトバウンド ポート
- リモート リスニング ポート

また、Expressway-E では、ファイアウォール トラバーサルに使用する特定のリスニング ポートも **[設定（Configuration）] > [トラバーサル（Traversal）] > [ポート（Ports）]** で設定できます。

Cisco Expressway シリーズ設定ガイドのページに用意されている、ご使用のバージョンに対応する『*Cisco Expressway IP Port Usage Configuration Guide*』を参照してください。

ローカル インバウンド ポート

「ローカル インバウンド ポート（Local inbound ports）」ページ（**[メンテナンス（Maintenance）] > [ツール（Tools）] > [ポートの使用状況（Port usage）] > [ローカルインバウンド ポート（Local inbound ports）]**）には、ほかのシステムからインバウンド通信を受信するために使用する Expressway 上のリスニング IP ポートが表示されます。

このページのリストに表示された各ポートについては、Expressway とインバウント通信の送信元の間にファイアウォールがある場合、そのファイアウォールは次を許可する必要があります。

- インバウンド通信の送信元から Expressway 上の IP ポートへの着信トラフィック
- その同じ Expressway IP ポートからインバウンド通信の送信元に返すリターン トラフィック

（注） このファイアウォールの設定は、この Expressway がトラバーサルクライアントまたはトラバーサルサーバの場合、Expressway ファイアウォールトラバーサルが正しく機能するために特に重要です。

Cisco Expressway シリーズ設定ガイドのページに用意されている、ご使用のバージョンに対応する『*Cisco Expressway IP Port Usage Configuration Guide*』を参照してください。

ローカル アウトバウンド ポート

「ローカル アウトバウンド ポート（Local outbound ports）」ページ（**[メンテナンス（Maintenance）] > [ツール（Tools）] > [ポートの使用状況（Port usage）] > [ローカル アウトバウンドポート（Local outbound ports）]**）には、ほかのシステムへのアウトバウンド通信を送信するために使用する Expressway 上の送信元 IP ポートが表示されます。

このページにリストされた各ポートについては、Expressway とアウトバウント通信の宛先の間にファイアウォールがある場合、そのファイアウォールは次を許可する必要があります。

- Expressway の IP ポートからアウトバウンド通信の宛先へのアウトバウンドトラフィック

- その宛先から同じ Expressway IP ポートへのリターントラフィック

（注） このファイアウォールの設定は、この Expressway がトラバーサルクライアントまたはトラバーサルサーバの場合、Expressway ファイアウォールトラバーサルが正しく機能するために特に重要です。

Cisco Expressway シリーズ設定ガイドのページに用意されている、ご使用のバージョンに対応する『*Cisco Expressway IP Port Usage Configuration Guide*』を参照してください。

リモート リスニング ポート

「リモート リスニング ポート（Remote listening ports）」ページ（**[メンテナンス（Maintenance）] > [ツール（Tools）] > [ポートの使用状況（Port usage）] > [リモートリスニングポート（Remote Listening ports）]**）には、Expressway と通信するリモートシステムの宛先 IP アドレスと IP ポートが表示されます。

ファイアウォールは、このページのリストに表示された IP アドレスと IP ポートで識別されたローカル Expressway からリモート デバイスへのトラフィックを許可するように設定する必要があります。

（注） このリストに表示されていない、Expressway がメディアやシグナリングを送信する他のリモートデバイスもありますが、これらのデバイスが Expressway からのトラフィックを受信するポートは宛先デバイスの設定によって決まります。そのため、それらのポートはこのリストに表示できません。[ローカル アウトバウンド ポート] ページにリストされているすべてのポートを開いている場合、Expressway はすべてのリモート ポートと通信できます。こらのリモート システムとポートにファイアウォール上で開く IP ポートを制限する場合は、このページの情報のみが必要です。

Cisco Expressway シリーズ設定ガイドのページに用意されている、ご使用のバージョンに対応する『*Cisco Expressway IP Port Usage Configuration Guide*』を参照してください。

再起動、リブート、およびシャットダウン

「再起動オプション（Restart options）」ページ（**[メンテナンス（Maintenance）]>[再起動オプション（Restart options）]**）を使用すると、ハードウェアに物理的にアクセスすることなく、Expressway を再起動、リブート、またはシャットダウンできます。

注意 ユニットの前面の赤の ALM LED がオンになっている間は Expressway を再起動、リブート、またはシャットダウンしないでください。これは、ハードウェア障害を示しています。シスコのカスタマー サポート担当者に連絡してください。

再起動

再起動機能は Expressway アプリケーション ソフトウェアをシャットダウンして再起動しますが、オペレーティング システムやハードウェアのシャットダウンおよび再起動は行いません。再起動には約 3 分かかります。

通常、何らかの設定変更を有効にしたり、クラスタに対してシステムを追加または削除する場合に再起動が必要です。このような場合はシステム アラームが発生し、システムが再起動されるまではそのままです。

Expressway がクラスタの一部であり、クラスタ内の他のピアも再起動を必要としている場合は、各ピアが再起動するまで次のピアの再起動を待つことを推奨します。

リブート

リブート機能は Expressway アプリケーション ソフトウェア、オペレーティング システム、およびハードウェアをシャットダウンし、再起動します。リブートには約 5 分かかります。

リブートは、通常はソフトウェア アップグレードの後にのみ必要で、アップグレード プロセスの一部として実行されます。予期しないシステム エラーを解決しようとしているときにも、リブートが必要になる場合があります。

シャットダウン

シャットダウンは、通常、メンテナンスまたは再配置の前にユニットのプラグを抜く場合に必要になります。プラグを抜く前にシステムをシャットダウンする必要があります。特に、通常運用時のシステムへの電源を取り外す場合に、制御されていないシャットダウンは避けてください。

アクティブ コールへの影響

これらの再起動オプションのいずれかによって、すべてのアクティブ コールが終了されます。（Expressway がクラスタの一部である場合は、Expressway がシグナリングを取得しているコールのみが終了されます）。

そのため、**[システム ステータス（System status）]** には現在のコールの数が表示されるため、システムを再起動する前にそれらの数を確認できます。システムをすぐに再起動しない場合は、再起動前にこのページを更新し、コールの現在のステータスを確認してください。

[Mobile & Remote Access] が有効になっている場合、現在プロビジョニングされているセッションの数が表示されます（Expressway-C のみ）。

Web インターフェイスを使用した再起動、リブート、およびシャットダウン

Web インターフェイスを使用して Expressway を再起動するには、次の手順を実行します。

1. **[メンテナンス（Maintenance）]** > **[再起動オプション（Restart options）]** に移動します。
2. 現在実行されているコールの数を確認します。
3. 必要に応じて **[再起動（Restart）]**、**[リブート（Reboot）]**、または **[シャットダウン（Shutdown）]** をクリックし、アクションを確認します。

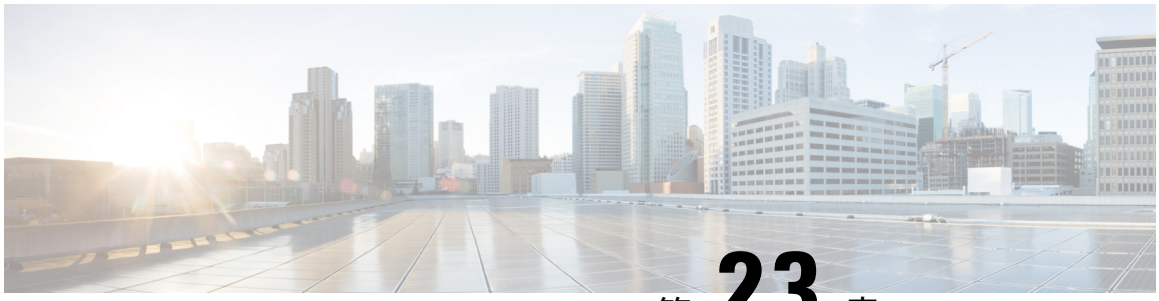
場合によっては、これらのオプションのうち 1 つのみ（たとえば **[再起動（Restart）]** など）を使用できます。これは、通常、アラームまたはバナーメッセージ内のリンクに従った後で「**再起動オプション（Restart options**）」ページにアクセスすると発生します。

- 再起動またはリブート：**[再起動しています（Restarting）] または [リブートしています（Rebooting）]** ページが表示され、オレンジ色のバーで進捗状況が示されます。

  システムが正常に再起動またはリブートされると、「**ログイン（Login**）」ページが表示されます。

- シャットダウン：[シャットダウン中（Shutting down）] ページが表示されます。

  このページは、システムが正常にシャットダウンした後もそのまま表示されますが、このページを更新しようとしたり、Expressway へアクセスしようとしても失敗します。



第 23 章

診断とトラブルシューティング

このセクションでは、システム操作に問題が発生した場合に役立つ情報について説明します。

ネットワーク ユーティリティ

ここでは、ネットワーク ユーティリティ ツールの使用方法について説明します。

- ping：特定のホスト システムが Expressway から接続でき、そのシステムに到達できるようにネットワークが正しく設定されていることを確認できます。
- トレースルート：Expressway から特定の宛先ホスト システムに送信されたネットワーク パケットが取得したルートの詳細を検出することができます。
- Tracepath：Expressway から特定の宛先ホスト システムに送信されたネットワーク パケットが取得したパスを検出することができます。
- DNS ルックアップ：特定のホスト名宛の要求に応答するドメイン名サーバ（DNS サーバ）を確認することができます。
- SRV 接続テスト機能：DNS で特定のサービス レコードをチェックし、返されたレコードへの接続を確認できます。

ping

[Ping] ツール（**[メンテナンス（Maintenance）]** > **[ツール（Tools）]** > **[ネットワーク ユーティリティ（Network utilities）]** > **[Ping]**）を使用して、システムの問題のトラブルシューティングに役立てることができます。

このツールでは、特定のホストシステムに接続できるかと、ネットワークがそのシステムに到達するように正しく設定されているかを確認できます。また、Expressway から宛先ホスト システムへメッセージを送信するためにかかった時間の詳細を報告します。

このツールを使用するには、次の手順を実行します。

1. **[ホスト（Host）]** フィールドに、接続を試みるホスト システムの IP アドレスまたはホスト名を入力します。
2. [Ping] をクリックします。

新しいセクションが表示され、接続試行の結果が示されます。成功すると、次の情報が表示されます。

ホスト	クエリされたホスト システムにより返されたホスト名と IP アドレス。
Response time (ms)	要求を Expressway からホスト システムに送信し、返されるまでにかかった時間（ミリ秒単位）。

トレースルート

[トレースルート（Traceroute）] ツール（**[メンテナンス（Maintenance）]**>**[ツール（Tools）]**>**[ネットワーク ユーティリティ（Network utilities）]**>**[トレースルート（Traceroute）]**）を使用して、システムの問題のトラブルシューティングに役立てることができます。

Expressway から特定の宛先ホスト システムに送信されたネットワーク パケットが取得したルートを検出することができます。パス上の各ノードの詳細、および各ノードが要求に応答するためにかかった時間が報告されます。

このツールを使用するには、次の手順を実行します。

1. **[ホスト（Host）]** フィールドに、パスをトレースするホスト システムの IP アドレスまたはホスト名を入力します。
2. [Traceroute] をクリックします。

トレースの結果を示すバナーがある新しいセクションが表示され、次のようなパス内の各ノードの詳細が示されます。

TTL	（存続時間）。これは、ノードの連番を示す、要求のホップ カウントです。
応答	ノードの IP アドレスと、Expressway から受信した各パケットへの応答にかかった時間（ミリ秒）が表示されます。 *** は、ノードが要求に応答しなかったことを示しています。

Expressway と特定のホスト間で取得するルートは、トレースルート要求ごとに異なる場合があります。

Tracepath

[トレースパス（Tracepath）] ツール（**[メンテナンス（Maintenance）] > [ツール（Tools）] > [ネットワーク ユーティリティ（Network utilities）] > [トレースパス（Tracepath）]**）を使用して、システムの問題のトラブルシューティングに役立てることができます。

Expressway から特定の宛先ホスト システムに送信されたネットワーク パケットが取得したルートを検出することができます。

このツールを使用するには、次の手順を実行します。

1. **[ホスト（Host）]** フィールドに、ルートをトレースするホスト システムの IP アドレスまたはホスト名を入力します。
2. [トレースパス（Tracepath）] をクリックします。

トレースの結果を示したバナーとともに、パスの各ノードの詳細、各ノードが要求に応答するためにかかった時間、および最大伝送ユニット（MTU）を示す新しいセクションが表示されます。

Expressway と特定のホスト間で取得するルートは、トレースパス要求ごとに異なる場合があります。

DNS ルックアップ

[DNS ルックアップ（DNS lookup）] ツール（**[メンテナンス（Maintenance）] > [ツール（Tools）] > [ネットワーク ユーティリティ（Network utilities）] > [DNS ルックアップ（DNS lookup）]**）を使用して、システムの問題のトラブルシューティングに役立てることができます。

指定したホスト名を DNS にクエリし、ルックアップが成功した場合は結果が表示されます。

このツールを使用するには、次の手順を実行します。

1. **[ホスト（Host）]** フィールドに、次のいずれかを入力します。
   - クエリするホストの名前
   - 逆 DNS ルックアップを実行する場合は、IPv4 アドレスまたは IPv6 アドレス
2. **[クエリ タイプ（Query type）]** フィールドで、検索するレコードのタイプを選択します。

   （逆ルックアップの場合は **[クエリ タイプ（Query type）]** は無視され、自動的に PTR レコードが検索されます）。

（注） 適切な逆引きルックアップを容易にするために、152.50.10.in-addr.arpa（アドレスのサブネットは 10.50.152.0/24）とアドレス内のターゲット DNS サーバの形式にします。これにより、サブネット内のすべての要求がデフォルトサーバではなく、ターゲット DNS サーバに送信されます。

オプション	検索対象
すべて	任意のタイプのレコード
A (IPv4 address)	ホスト名をホストの IPv4 アドレスにマッピングするレコード
AAAA (IPv6 address)	ホスト名をホストの IPv6 アドレスにマッピングするレコード
SRV（サービス）（SRV (services)）	SRV レコード（H.323、SIP、ユニファイドコミュニケーション、および TURN サービスに固有のものを含む。下記参照）。
NAPTR（名前の権限ポインタ）（NAPTR (Name authority pointer)）	ドメイン名を（たとえば URI や他のドメイン名に）上書きするレコード

3. デフォルトでは、システムはシステムのデフォルトのすべての DNS サーバ（**[システム（System）] > [DNS]**）にクエリを送信します。特定のサーバのみを照会するには、**[次の DNS サーバに照合して確認する（Check against the following DNS servers）]** を *[カスタム（Custom）]* に設定し、使用する DNS サーバを選択します。
4. [Lookup] をクリックします。

選択した各**クエリ タイプ**に対して個別の DNS クエリが実行されます。DNS に送信されるクエリに含まれるドメインは、指定された**ホスト**が完全修飾名であるかどうかによって異なります（完全修飾ホスト名には少なくとも 1 つの「「ドット」」が含まれています）。

- 指定された**ホスト**が完全修飾名である場合：
  - DNS に対し、最初に**ホスト**のクエリが実行されます。
  - **ホスト**のルックアップが失敗すると、**Host.<system_domain>** に対する追加のクエリが実行されます（**<system_domain>** は **DNS** ページで設定されている**ドメイン名**）。
- 指定された**ホスト**が完全修飾名でない場合：
  - DNS に対し、最初に **Host.<system_domain>** のクエリが実行されます。
  - **ホスト**のルックアップが失敗すると、次は **Host.<system_domain>** のクエリが実行されます

SRV レコード タイプのルックアップの場合、複数の DNS クエリが実行されます。次の _service._protocol の組み合わせごとに SRV クエリが実行されます。

- _h323ls._udp.<domain>
- _h323rs._udp.<domain>
- _h323cs._tcp.<domain>
- _sips._tcp.<domain>
- _sip._tcp.<domain>
- _sip._udp.<domain>
- _collab-edge._tls
- _cisco-uds._tcp
- _turn._udp.<domain>
- _turn._tcp.<domain>

それぞれの場合、その他すべてのクエリ タイプについて、**ホスト**または**Host.<system_domain>** の <domain> に対して 1 つまたは 2 つのクエリが実行されます。

結果

新しいセクションが表示され、すべてのクエリ結果が示されます。成功すると、次の情報が表示されます。

クエリーのタイプ	Expressway によって送信されたクエリのタイプ。
名前	クエリに対する応答に含まれているホスト名。
TTL	このクエリの結果が Expressway にキャッシュされる時間（秒単位）。
クラス	IN（インターネット）は、応答がインターネットホスト名、サーバ、またはIPアドレスを含む DNS レコードであったことを示します。
タイプ	クエリに対する応答に含まれているレコードタイプ。
応答	この**[名前（Name）]**および**[タイプ（Type）]**のクエリに対する応答として受信したレコードの内容。

転送プロトコル

Expressway は UDP と TCP を使用して DNS 解決を行います。DNS サーバからは、通常、UDP とTCP 応答が送られます。UDP 応答が 512 バイトの UDP メッセージ サイズの制限を超えていると、Expressway は UDP 応答を処理できません。一般に、これが問題になることはありません。Expressway は代わりに TCP 応答を処理できるためです。

ただし、ポート 53 での TCP インバウンドをブロックしている場合、UDP 応答のサイズが 512 バイトを超えていると、Expressway は DNS からの応答を処理できません。この場合、DNS ルックアップ ツールを使用しても結果は表示されず、要求したアドレスを必要とするすべての操作は失敗します。

ただし、ポート 53 での TCP インバウンドをブロックしている場合、UDP 応答のサイズが 512 バイトを超えていると、Expressway は DNS からの応答を処理できません。この場合、DNS ルックアップ ツールを使用しても結果は表示されず、要求したアドレスを必要とするすべての操作は失敗します。

SRV 接続テスト機能

SRV 接続テスト機能は、Expressway が所定のドメイン上の特定のサービスに接続できるかどうかをテストするネットワーク ユーティリティです。このツールを使用すると、Cisco Webex ハイブリッド コール サービスやビジネス ツー ビジネス ビデオ コールなどの Expressway ベースのソリューションを設定しながら事前に接続をテストできます。

このツールで接続をテストする際は、クエリする DNS サービス レコード ドメインと、そのドメインでテストするサービス レコード プロトコルを指定します。Expressway は指定されたプロトコルごとに DNS SRV クエリを実行し、DNS から返されたホストへの TCP 接続を試行します。TLS を指定した場合、Expressway は TCP が成功しなければ TLS 接続を試行しません。

Expressway 接続テスト ページに、DNS の応答と接続試行が示されます。接続が失敗した場合は、その理由と併せてその特定の問題を解決するためのアドバイスも表示されます。

接続をトラブルシューティングするには、テストで生成された TCP データを *.pcap* 形式でダウンロードできます。選択的に DNS クエリのダンプ（特定の接続試行）をダウンロードすることも、テスト全体を記録した単一の *.pcap* ファイルを取得することもできます。

このツールを使用するには、次の手順を実行します。

1. **[メンテナンス（Maintenance）]** > **ツール（Tools）]** > **[** > **[ネットワーク ユーティリティ（Network utilities）]** > **[接続テスト（Connectivity Test）]** に移動します。
2. クエリする **[サービス レコード ドメイン（Service Record Domain）]** を入力します（例：`callservice.webex.com`）。
3. テストする **[サービス レコード プロトコル（Service Record Protocols）]** を入力します（例：`_sips._tcp`）。

   複数のプロトコルを指定する場合は、各プロトコルをカンマで区切ります（例：`_sip._tcp,_sips._tcp`）。
4. [実行（Run）] をクリックします。

Expresswayは、サービス、プロトコル、およびドメインの組み合わせで構成されるSRVレコードに対してDNSへクエリを行います。たとえば、`_sip._tcp.callservice.webex.com`と`_sips._tcp.callservice.webex.com`へのクエリなどです。

デフォルトでは、システムはシステムのデフォルトのすべてのDNSサーバ（**[システム（System）] > [DNS]**）にクエリを送信します。

サービス レコードのオプション

導入環境でテストする必要がある、_service._protocolの組み合わせの例を次に示します。

- _h323ls._udp.<domain>
- _h323rs._udp.<domain>
- _h323cs._tcp.<domain>
- _sips._tcp.<domain>
- _sip._tcp.<domain>
- _sip._udp.<domain>
- _collab-edge._tls
- _cisco-uds._tcp
- _turn._udp.<domain>
- _turn._tcp.<domain>
- _cms-web._tls.<domain>
- _sipfederationtls._tcp.<domain>

テスト結果

ページの下部にあるセクションに、クエリ結果と接続テストの結果が示されます。テスト結果には、次の表に記載する情報の一部またはすべてが含まれます。

表 *23 :* 接続テストの結果：*DNS SRV*ルックアップ

結果フィールド	説明
ステージ（Stage）	テストのステージ。クエリに対する応答ごとにステージが1つ、クエリ結果全体に別のステージが1つあります。
サービス レコード（Service Record）	クエリしたレコードセットから検出されたSRVレコード。

結果フィールド	説明
結果（Result）	DNS SRV レコードでマッピングされているホスト（テストが成功した場合）。DNS レコードで定義されている場合、エントリごとのプライオリティ、重み、ポートも示されます。
ヒント（Hint）	このフィールドには、この結果テーブルの値は保持されません。
TCP ダンプ（TCP Dump）	結果全体について、SRV クエリの TCP レコードが含まれる .pcap ファイルをダウンロードすることができます。

表 *24 :* 接続テストの結果：*TCP* 接続

結果	説明
ステージ（Stage）	テストのステージ。サービスに対する TCP プロトコルのクエリによって返されたホストごとにテストが 1 回行われます。すべてのテストを集計した結果もあります。
ターゲット（Target）	DNS SRV クエリによって返されたホスト名。
結果（Result）	テストが正常に完了したことを示します。またはテストが失敗した理由が示されます（既知の場合）。
ヒント（Hint）	失敗したテストのトラブルシューティングに利用できるポインタ。
TCP ダンプ（TCP Dump）	特定の接続試行の TCP レコードが含まれる .pcap ファイルをダウンロードすることができます。

表 *25* : 接続テストの結果 : *TCP* 接続

結果フィールド	説明
ステージ（Stage）	テストの段階。各ホストに、TLS プロトコルでクエリしたサービスに対するテストを 1 つずつ返します。テストは、ホストでサポートされている各 TLS バージョンを使用して次の順序で実行されます。 • TLS 1.2 • TLS 1.1 • TLS 1 たとえば、ホストは 3 つのすべてのバージョンをサポートしており、TLS 1.1 バージョンを使用して接続が成功した場合、チェックは 2 つのテストを返します。 すべてのテストを集計した結果もあります。 （注） Expressway がホストへの TLS 接続を確立できない場合、そのホストに対する TLS 接続試行は行われません。
ターゲット（Target）	DNS SRV クエリによって返されたホスト名。
結果（Result）	テストが正常に完了したことを示します。またはテストが失敗した理由が示されます（既知の場合）。
ヒント（Hint）	失敗したテストのトラブルシューティングに利用できるポインタ。
TCP ダンプ（TCP Dump）	特定の接続試行の TCP レコードが含まれる .pcap ファイルをダウンロードすることができます。

診断ツール

ここでは、Expressway 診断ツールの使用方法について説明します。

- 診断ロギングの設定
- システム スナップショットの作成

- ネットワーク ログ レベルの設定とサポート ログ レベルの設定の高度なロギング設定ツール
- インシデントレポート

Expressway は SIP「セッション識別子」をサポートしています。コールのすべてのデバイスがセッション識別子を使用していると仮定すると、このメカニズムは SIP ヘッダーの *[セッション ID（Session-ID）]* フィールドを使用して、コールのトランジット全体を通して一意のコードを維持します。セッション識別子は、Expressway サーバ上の特定のコールを検索して追跡するために使用できるので、複数のコンポーネントにかかわるコールの問題を調査する場合に便利です。セッション識別子のサポートには、インターワーキングされた SIP/H.323 コールの SIP 側、および Microsoft システムとの間のコールが含まれます。セッション識別子は、RFC 7989 で定義されています。

診断ロギングの設定

診断ログ ツール（**[メンテナンス（Maintenance）]** > **[診断（Diagnostics）]** > **[診断ロギング（Diagnostic logging）]**）は、トラブルシューティングに役立つ場合があります。一定期間のシステムアクティビティの診断ログを生成し、それをダウンロードして、シスコのカスタマーサポート担当者に送信できます。ロギングの進行中に *tcpdump* を取得およびダウンロードすることができます。

はじめに

- 一度に生成できる診断ログは 1 つだけです。新しい診断ログを作成すると、以前に作成されたログが置き換えられます。
- Expressway は、関連するシステムアクティビティを継続的にログに記録します。診断ロギング機能は、診断ロギング時間の開始から診断ロギングが停止するまでのアクティビティを抽出し、便利な Web ベースのダウンロード機能を提供します。
- **[再起動/リブート（Restart/Reboot）]**：診断ログのみが収集されます。他のファイルはバンドルから欠落します。
- 診断ログを起動すると、関連するシステムモジュールのログ レベルが自動的に「「デバッグ」」に設定されます。ログを停止するとログレベルが元の値にリセットされるため、結果の詳細ログレベルで設定されたアラームを無視します。
- 診断ロギングは、Web インターフェイスを介して制御されます。CLI オプションはありません。
- tcpdumpオプションを選択すると、ネットワークインターフェイスごとに最大3つのパケットキャプチャファイルが作成され、それぞれの最大サイズは20MBです（つまり、デュアルネットワークインターフェイスを備えた Expressway で、合計サイズが 80 MB の最大4つのファイルを作成できます）。

（注） X14.0 以降、.pcap ファイルの数はネットワークインターフェイスごとに最大 20 個増加し、tcpdump は Web UI を介して連続的に実行できます。ファイルの最大サイズは 20 MB です。

注意 診断ログを有効にすると、システムのパフォーマンスが影響を受ける可能性があります。診断ログは、シスコのカスタマーサポートのアドバイスに基づいて、またはトラフィックの負荷が軽いときにのみ収集する必要があります。

診断ログを生成するプロセス

1. **[Maintenance]** > **[Diagnostics]** > **[Diagnostic logging]** を選択します。
2. （オプション）*[Take tcpdump while logging]*を選択します。診断ログの進行中に tcpdump を使用するには、このオプションを選択できます。tcpdump は、ロギングの完了時に別のファイルとしてダウンロードできます。

（注） ユーザインターフェイスで tcpdump が有効になっている場合、管理者は **IP アドレス**と**ポート**フィルタを提供できます。

管理者が特定のホスト（IPアドレスまたは完全修飾ドメイン名（FQDN））および/またはポートから送信されるパケットを pcap ファイルで確認する場合、tcpdump フィルタが使用されます。管理者は、フィルタリングされたパケットを取得するために識別されるフィールドに値を指定できます。バージョン X14.0 から、tcpdump は LAN ごとに 20 個の pcap ファイルをキャプチャし、すべての pcap ファイルのサイズは 20 MB です。

この表は、登録数に応じて、1 つの pcap ファイル（最大 20 MB）と 20 の pcap ファイルを生成するのにかかる平均時間（秒単位）を表しています。

Expressway C：

	20 MB	**400 MB**
5 ユーザ	2	40
20 ユーザ	2	40
2500 ユーザ	10	200

Expressway E：

	20 MB	**400 MB**
5 ユーザ	1	20
20 ユーザ	1	20
2500 ユーザ	2	40

これらの数値は、トラブルシューティングに使用される環境に固有のものです。このパフォーマンステストの実行中に、1 ノードとモバイルおよびリモートアクセス（MRA）ビデオを使用しました。

3. **IP アドレス で tcpdump をフィルタリングする（Filter tcpdump by IP address**）を入力します。
4. **ポートで tcpdump をフィルタリングする（Filter tcpdump by port**） を入力します。範囲は 1 ～ 65536 です。
5. [Start new log] をクリックします。
6. （任意）**マーカー** テキストを入力して、**[マーカーの追加（Add Marker）]** をクリックします。
   - 特定のアクティビティが実行される前にマーカー機能を使用して、ログファイルにコメントテキストを追加することができます。これは、診断ログファイル内の特定

のセクションを識別するのに役立ちます。マーカーテキストには、ログファイルに DEBUG_MARKER タグがあります。

- 診断ログの進行中に、必要に応じた数のマーカーを追加できます。

7. 診断ログにトレースするシステムの問題を再現します。
8. [Stop Logging] をクリックします。
9. [ログの収集（Collect Logs）] をクリックします。
10. ログの収集が完了したら、**[ログのダウンロード（Download log）]** をクリックして、ローカル ファイル システムに診断ログ アーカイブを保存します。

    アーカイブを保存するように促されます（実際の表現はブラウザによって異なります）。

診断ログアーカイブに含まれているファイル

- loggingsnapshot_<*system host name*>_<*timestamp*>.txt： ロギング期間中に実行されたアクティビティに応じたログメッセージが記録されています。
- xconf_dump_<*system host name*>_<*timestamp*>.txt：ロギング開始時のシステム設定に関する情報が記録されています。
- xconf_dump_<*system host name*>_<*timestamp*>.xml：XML 形式の xconfig のより完全なバージョン
- xstat_dump_<*system host name*>_<*timestamp*>.txt：ロギング開始時のシステムのステータスに関する情報が記録されています。
- xconf_dump_<*system host name*>_<*timestamp*>.xml：XML 形式の xstatus のより完全なバージョン
- （該当する場合）eth*n*_diagnostic_logging_tcpdump x_<*system host name*>_<*timestamp*> .pcap：ロギング期間中にキャプチャされたパケットが記録されています。
- ca_<*system host name*>_<*timestamp*>.pem
- server_<*system host name*>_<*timestamp*>.pem

要求された場合は、シスコサポートの担当者にこれらのファイルを送信できます。

⚠

注意 *tcpdump* ファイル には、機密情報が含まれている場合があります。*tcpdump* ファイルは、信頼できる受信者にのみ送信してください。送信前にファイルを暗号化し、アウトオブバンドで復号パスワードを送信することを考慮してください。

コラボレーション ソリューション アナライザー ツールへのリンク

必要に応じて、**解析ログ**を使用してコラボレーションソリューションアナライザのトラブルシューティングツールへのリンクを開きます。

ログを再度ダウンロードするには

ログを再度ダウンロードする場合は、**[ログ収集（Log Collection）]**ボタンを使用することで再度収集できます。ボタンがグレー表示されている場合は、ブラウザのページを更新します。

クラスタ化システム

Expresswayがクラスタの一部である場合、一部のアクティビティは「現在」のピア（現在管理者としてログインしているピア）にのみ適用されます。

- ロギングの開始操作と停止操作は、現在のピアには関係なくクラスタ内のすべてのピアに適用されます。
- *tcpdump* 操作は、現在のピアには関係なくクラスタ内のすべてのピアに適用されます。
- 各クラスタ ピアは独自の統合ログを維持し、そのピアでのみ発生するアクティビティを記録します。
- マーカー テキストは、現在のピアにのみ適用されます。
- 現在ピアからの診断ログのみダウンロードできます。
- 他のピアのログへのマーカの追加、または他のピアからの診断ログのダウンロードを行うには、そのピアに管理者としてログインする必要があります。

デバッグを目的として包括的な情報を収集する場合は、クラスタ内のピアごとに診断ログを抽出することを推奨します。

システム スナップショットの作成

「システム スナップショット（System snapshot）」ページ（**[メンテナンス（Maintenance）]** > **[診断（Diagnostics）]** > **[システムスナップショット（System snapshot）]**）では、診断目的で使用できるファイルを作成できます。これらのファイルは、経験している問題のトラブルシューティングに役立てるため、要求されたときにサポート担当者に送信する必要があります。

いくつかのタイプのスナップショット ファイルを作成できます。

- **ステータススナップショット**：システムの現在の設定とステータス設定が含まれています。
- **ログスナップショット**：ログファイル（イベントログ、設定ログ、ネットワークログなど）情報が含まれます。
- **完全なスナップショット**：すべてのシステム情報の完全なダウンロードが含まれています。このスナップショット ファイルの準備の完了には数分かかる場合があり、スナップショットの進行中にシステム パフォーマンスが低下する可能性があります。

システム スナップショットファイルを作成するには、次の手順に従います。

1. スナップショットファイルのダウンロードを開始するには、いずれかのスナップショットボタンをクリックします。通常、サポート担当者が、どのタイプのスナップショットファイルが必要であるかを示します。
   - スナップショット作成プロセスが開始されます。このプロセスはバックグラウンドで動作します。必要に応じてスナップショットページから離れ、後で戻ってきて生成されたスナップショット ファイルをダウンロードすることができます。
   - スナップショット ファイルが作成されると、**[スナップショットのダウンロード（Download snapshot）]** ボタンが表示されます。
2. [スナップショットのダウンロード（Download snapshot）] をクリックします。ポップアップ ウィンドウが表示され、ファイルを保存するよう指示されます（実際の表現は、ブラウザによって異なります）。サポート担当者に簡単にファイルを送信できる場所を選択します。

ネットワーク ログ レベルの設定

「ネットワークログの設定（Network Log configuration）」ページ（**[メンテナンス（Maintenance）] > [診断（Diagnostics）] > [詳細設定（Advanced）] > [ネットワークログの設定（Network Log configuration）]**）を使用して、ネットワークログメッセージモジュールの範囲のログレベルを設定します。

⚠

注意 ログ レベルを変更すると、システムのパフォーマンスに影響を与える可能性があります。シスコ カスタマー サポートのアドバイスがあった場合にのみ、ログ レベルを変更してください。

ログ レベルを変更するには、次の手順を実行します。

1. ログ レベルを変更するモジュールの**名前**をクリックします。
2. ドロップダウン リストから必要な**レベル**を選択します。
   - ログ レベルの *[*致命的（*Fatal*）*]* は冗長性が最も低く、*[*トレース（*Trace*）*]* は冗長性が最も高いレベルです。
   - 各メッセージのカテゴリには、デフォルトで *[*情報（*Info*）*]* のログ レベルが設定されます。
3. [保存（Save）] をクリックします。

サポート ログ レベルの設定

[サポートログの設定（Support Log configuration）] ページ（**[メンテナンス（Maintenance）] > [診断（Diagnostics）] > [詳細設定（Advanced）] > [サポート ログの設定（Support Log**

configuration）]）を使用して、サポートログメッセージモジュールの範囲にログレベルを設定します。

⚠

注意 ログ レベルを変更すると、システムのパフォーマンスに影響を与える可能性があります。シスコ カスタマー サポートのアドバイスがあった場合にのみ、ログ レベルを変更してください。

ログ レベルを変更するには、次の手順を実行します。

1. ログ レベルを変更するモジュールの**名前**をクリックします。
2. ドロップダウン リストから必要な**レベル**を選択します。
   - ログ レベルの *[*致命的（*Fatal*）*]* は冗長性が最も低く、*[*トレース（*Trace*）*]* は冗長性が最も高いレベルです。
   - 各メッセージのカテゴリには、デフォルトで *[*情報（*Info*）*]* のログ レベルが設定されます。
3. [保存（Save）] をクリックします。

インシデントレポート

Expressway のインシデント レポート機能は、アプリケーションの障害などの重要なシステム問題に関する情報を自動的に保存します。ここでは、インシデントレポートを表示する方法について説明します。

また、手動または自動でインシデントレポートをシスコのカスタマーサポートに送信する方法も説明されています。これらのレポートに含まれている情報をシスコのカスタマーサポートによる障害の原因の診断に使用できます。このプロセス中に収集されたすべての情報は社外秘として扱われ、問題を診断して解決する目的のみにシスコの担当者が使用します。

インシデント レポートに関する注意：プライバシー保護された個人データ

シスコに対するレポートにプライバシー保護された個人データが含まれることは決してありません。

プライバシー保護された個人データは、将来、過去、および既存の顧客、従業員、およびその他のすべての個人または団体に関する個人情報が含まれている、顧客が何らかの方法で情報源から受け取るか導出する個人または団体に関するすべての情報を意味します。プライバシー保護された個人データには、名前、住所、電話番号、電子アドレス、社会保障番号、クレジットカード番号、顧客の機密ネットワーク情報（47 U.S.C. § 222 で定義されている内容、およびその施行規則）、IP アドレスまたはその他のハンドセット ID、アカウント情報、信用情報、人

口統計学的情報、および単独または他のデータとの組み合わせで特定の個人に固有の情報を提供できるその他の情報が、制限なく含まれます。

プライバシー保護された個人データは、レポートを自動的に送信するように Expressway が設定されている場合もシスコに送信されないことを確認してください。

このような情報の漏洩を防ぐことができない場合は、自動設定機能は使用しないでください。代わりに、「インシデント レポートの詳細」ページのデータをコピーしてテキスト ファイルに貼り付けます。その後、シスコのカスタマー サポートにファイルを転送する前に、機密情報を削除できます。

インシデント レポートは、常にローカルに保存され、「インシデント レポートの表示」ページで表示できます。

自動インシデント レポートの有効化

自動インシデント レポートを有効にする前に、インシデント レポートに関する注意：プライバシー保護された個人データをお読みください。

インシデント レポートをシスコ カスタマー サポートに自動的に送信するように Expressway を設定するには、次の手順を実行します。

1. **[メンテナンス（Maintenance）]**>**[診断（Diagnostics）]**>**[インシデントレポート（Incident reporting）]**>**[設定（Configuration）]** に移動します。
2. **[インシデント レポート送信モード（Incident reports sending mode）]** を *[オン（On）]* に設定します。
3. エラー レポートの送信先の Web サーバの **[インシデント レポートの URL（Incident reports URL）]** を指定します。デフォルトは `https://cc-reports.cisco.com/submitapplicationerror/` です。
4. オプション。シスコのカスタマー サポートがエラー レポートのフォローアップに使用できる **[連絡先の電子メールアドレス（Contact email address）]** を指定します。
5. オプション。インシデント サーバへの接続に使用する **[プロキシ サーバ（Proxy server）]** を指定します。（http|https）://address:port/ という形式を使用してください（例：`http://www.example.com:3128/`）。
6. **[コアダンプの作成（Create core dumps）]** が *[オン（On）]* に設定されていることを確認します。これは、役立つ診断情報が提供されるため、推奨される設定です。

（注） **[インシデント レポート送信モード（Incident reports sending mode）]** が *[オフ（Off）]* に設定されている場合、インシデントはどの URL にも送信されませんが、ローカルに保存され、**[インシデントの詳細（Incident detail）]** ページからインシデント レポートの表示できます。

インシデント レポートを手動で送信

インシデント レポートをシスコに手動で送信するかどうかを決定する前に、インシデント レポートに関する注意：プライバシー保護された個人データをお読みください。

インシデント レポートをシスコのカスタマー サポートに手動で送信するには、次の手順を実行します。

1. **[メンテナンス（Maintenance）]** > **[診断（Diagnostics）]** > **[インシデント レポート（Incident reporting）]** > **[表示（View）]** に移動します。
2. 送信するインシデントをクリックします。**「インシデントの詳細（Incident detail）」** ページが表示されます。
3. ページの下部にスクロールし、[インシデント レポートのダウンロード（Download incident report）] をクリックします。オプションで、ファイルを保存できます。
4. ファイルをシスコ カスタマー サポートに転送できる場所に保存します。

レポートからの機密情報の削除

ダウンロードしたインシデント レポートは Base64 でエンコードされており、そのファイル内の情報について意味のある表示や編集を行うことはできません。

シスコに送信する前にレポートを編集する必要がある場合は（たとえば、機密情報と考えられるものを削除する必要がある場合）、**「インシデントの詳細（Incident detail）」** ページの情報をコピーしてテキスト ファイルに貼り付け、そのファイル内の情報 を編集してからシスコに送信する必要があります。

インシデント レポートの表示

「インシデント ビュー（Incident view）」 ページ（**[メンテナンス（Maintenance）]** > **[診断（Diagnostics）]** > **[インシデント レポート（Incident reporting）]** > **[表示（View）]**）には、Expressway が最後にアップグレードされてから発生したすべてのインシデント レポートのリストが表示されます。各インシデントに対するレポートが生成され、これらのレポートに含まれている情報をシスコのカスタマー サポートによる障害の原因の診断に使用できます。

各レポートについて、以下の情報が表示されます。

フィールド	説明
時刻	インシデントが発生した日時。
バージョン	インシデントが発生したときに実行していた Expressway ソフトウェアのバージョン。
ビルド	インシデントが発生したときに実行していた Expressway ソフトウェア バージョンの内部ビルド番号。

フィールド	説明
状態（State）	インシデントの現在の状態。 *[保留中（Pending）]*：インシデントがローカルに保存されたが送信されていないことを示します。 *[Sent]*：インシデントの詳細が [インシデント レポート] ページで指定された URL に送信されたことを示します。

特定のインシデント レポートに含まれている情報を表示するには、レポートの [Time] をクリックします。「インシデント レポートの詳細」ページが表示され、画面上にレポートを表示するか、またはシスコのカスタマー サポートに手動で転送するために XML ファイルとしてダウンロードすることができます。

インシデント レポートの詳細

「インシデントの詳細（Incident detail）」ページ（**[メンテナンス（Maintenance）] > [診断（Diagnostics）] > [インシデント レポート（Incident reporting）] > [表示（View）]**、次にレポートの **[時間（Time）]** をクリック）には、特定のインシデント レポートに含まれている情報が表示されます。

[インシデント レポート送信モード（Incident reports sending mode）]（**[メンテナンス（Maintenance）] > [診断（Diagnostics）] > [インシデント レポート（Incident reporting）] > [設定（Configuration）]** を使用）が有効になっている場合、これは外部 Web サービスに送信される情報です。また、これは、[Download incident report] をクリックした場合に Base64 でエンコードされた XML ファイルとしてダウンロードされる情報と同じです。

レポートに含まれている情報は、次のとおりです。

フィールド	説明
時刻	インシデントが発生した日時。
バージョン	インシデントが発生したときに実行していた Expressway ソフトウェアのバージョン。
ビルド	インシデントが発生したときに実行していた Expressway ソフトウェア バージョンの内部ビルド番号。
名前（Name）	ソフトウェアの名前。
System	システム名（設定されている場合）、または IP アドレス。
シリアル番号（Serial number）	ハードウェアのシリアル番号。

フィールド	説明
プロセス ID（Process ID）	インシデントが発生したときに Expressway アプリケーションに設定されていたプロセス ID。
リリース	これが（開発ビルドではなく）リリース ビルドであるかどうかを示す true/false フラグ。
ユーザ名（Username）	このソフトウェアを構築した担当者の名前。リリース ビルドの場合は空白です。
スタック（Stack）	インシデントの原因となった実行スレッドのトレース。
デバッグ情報（Debug information）	すべてのスレッドのアプリケーション コール スタックの完全なトレースおよびレジスタの値。

注意 各コール スタックについて、デバッグ情報には機密情報が含まれている可能性がある変数の内容が含まれています（たとえば、エイリアス値や IP アドレスなど）。ご使用の導入環境で、この情報に特定の個人に固有の情報が含まれている可能性がある場合は、自動インシデント レポートを有効にするかどうかを決定する前に、プライバシー保護された個人データに関するインシデント レポートに関する注意：プライバシー保護された個人データをお読みください。

開発者リソース

Expressway には、シスコのサポート チームと開発チームのみが使用するための機能がいくつか含まれています。シスコのサポート担当者のアドバイスと監視の上で行う場合を除き、これらのページにはアクセスしないでください。

注意 これらのページの機能を誤って使用すると、システムの動作が不安定になったり、パフォーマンス上の問題が発生したり、システム設定が永続的に破損したりする可能性があります。

以下の機能があります。

- デバッグおよびシステム管理ツール
- [Experimental] メニュー

デバッグおよびシステム管理ツール

注意 これらの機能は、シスコのサポート担当者のアドバイスがない限り、お客様は使用できません。これらの機能を誤って使用すると、システムの動作が不安定になったり、パフォーマンス上の問題が発生したり、システム設定が永続的に破損したりする可能性があります。

Expresswayには、デバックとシステム管理用の数多くのツールが搭載されています。管理者はこれらのツールを使用して、設定データへのアクセスや変更、ネットワーク トラフィックへのアクセスなど、ライブ システム上で発生していることを詳細に検査することができます。

これらのツールにアクセスする方法は、次のとおりです。

1. SSH セッションを開始します。
2. 必要に応じて、admin または root としてログインします。
3. シスコのサポート担当者によって指示された手順に従ってください。

[Experimental] メニュー

Expressway Webインターフェイスには、お客様が使用するためのものではないページが数多く含まれています。これらのページは、シスコのサポートおよび開発チームのみが使用するために存在しています。シスコのサポート担当者のアドバイスと監視の上で行う場合を除き、これらのページにはアクセスしないでください。

注意 これらのページの機能を誤って使用すると、システムの動作が不安定になったり、パフォーマンス上の問題が発生したり、システム設定が永続的に破損したりする可能性があります。

これらのページにアクセスする方法は、次のとおりです。

1. `https://<Expressway のホスト名または IP アドレス>/setaccess` に移動します。

   [アクセスの設定（Set access）] ページが表示されます。
2. [アクセスパスワード（Access password）] フィールドに、`qwertsys` と入力します。
3. [アクセスの有効化（Enable access）] をクリックします。

既存のメニュー項目の右側に、新しい**[Experimental]** という最上位メニューが表示されます。

第 24 章

参考資料

ここでは、Expressway の機能および管理に関する補足情報を提供します。

イベント ログ レベルについて

すべてのイベントには、1 ～ 4 の範囲で関連付けられたレベルがあり、レベル 1 のイベントが最も重要と見なされます。次の表に、さまざまなイベントに割り当てられるレベルの概要を示します。

レベル	割り当てられるイベント
1	登録要求やコール試行などの高レベルイベント。人間が簡単に読み取れます。次に例を示します。 • コール試行/接続/切断 • 登録試行/承認/拒否
2	すべてのレベル 1 のイベントに加えて、次のイベントがあります。 送受信されたプロトコル メッセージのログ（SIP、H.323、LDAP など）。H.460.18 キープアライブや H.245 ビデオ高速更新などのノイズの多いメッセージは除きます。
3	すべてのレベル 1 およびレベル 2 のイベントに加えて、次のイベントがあります。 • プロトコルのキープアライブ • コール関連の SIP シグナリング メッセージ
4	最も詳細なレベル：レベル 1、レベル 2、およびレベル 3 のすべてのイベントに加えて、次のイベントがあります。 • ネットワーク レベルの SIP メッセージ

Expressway によってログに記録されるすべてのイベントと、それらがログに記録される詳細レベルの完全なリストについては、イベントとレベルの項を参照してください。

イベント ログ形式

イベント ログは、UNIX syslog 形式の拡張として表示されます。

```
date time process_name: message_details
```

値は次のとおりです。

フィールド	説明
date	メッセージが記録された現地の日付。
time	メッセージが記録された現地の時刻。

フィールド	説明
process_name	ログ メッセージを生成するプログラムの名前。次のようなものが含まれます。 • **tvcs**（Expressway プロセスから発信されるすべてのメッセージの場合） • **web**（すべての Web ログインおよび設定イベントの場合） • **licensemanager**（コール ライセンス マネージャから発信されるメッセージの場合） • **b2bua**（B2BUA イベントの場合） • **portforwarding**（Expressway-C と Expressway-E 間の内部通信の場合） • **ssh**（Expressway-C と Expressway-E 間の ssh トンネルの場合） ただし、Expressway で実行している他のアプリケーションからのメッセージの場合は異なります。
message_details	メッセージの本文（詳細については、メッセージの詳細フィールドの項を参照してください）。

管理者イベント

管理者セッションに関連するイベントは次のとおりです。

- Admin Session Start
- Admin Session Finish
- Admin Session Login Failure

メッセージの詳細フィールドには次が含まれます。

- セッションが関連する管理者の名前および IP アドレス
- ログインが試行、開始、または終了された日時

メッセージの詳細フィールド

tvcs プロセスからログに記録されたすべてのメッセージについては、`message_details` フィールドにメッセージの本文が格納されます。このフィールドは、人間が判読できる、スペースで区切られた複数の `name=value` ペアで構成されています。

`message_details` フィールドの最初の名前要素は常に `Event` であり、最後の名前要素は常に `Level` です。

次の表に、message_details フィールド内の考えられるすべての名前要素を、それぞれの説明とともに通常の表示順で示します。

（注） 次に説明するイベントに加え、非アクティブの状態が1時間経過するごとに、MARK文字列を含む syslog.info イベントがログに記録されます。これは、ロギングがまだアクティブであることを確認するためです。

名前	説明
イベント	ログ メッセージが生成される原因となったイベント。Expressway によってログに記録されるすべてのイベントと、それらがログに記録されるレベルのリストについては、イベントとレベルを参照してください。
ユーザ（User）	ログイン試行が行われたときに入力したユーザ名。
ipaddr	ログインしたユーザの送信元 IP アドレス。
プロトコル（Protocol）	通信に使用されたプロトコルを示します。有効な値は次のとおりです。 • TCP • UDP • TLS
理由（Reason）	イベントに関連する理由に関する情報を含んだテキストの文字列。
サービス	通信に使用されたプロトコルを示します。次のいずれかになります。 • H.323 • SIP • H.225 • H.245 • LDAP • Q.931 • NeighbourGatekeeper • クラスタリング • ConferenceFactory

名前	説明
Message Type	メッセージのタイプを指定します。
Response-code	SIP 応答コードか、または H.323 およびインターワーキング コールの場合は SIP 同等応答コード
Src-ip	送信元 IP アドレス（通信を確立しようとしたデバイスの IP アドレス）。これは、IPv4 アドレスか IPv6 アドレスです。
Dst-ip	宛先 IP アドレス（通信試行の宛先の IP アドレス）。宛先 IP は Src-ip と同じ形式で記録されます。
Src-port	送信元ポート：通信を確立しようとしたデバイスの IP ポート。
Dst-port	宛先ポート：通信試行の宛先の IP ポート。
Src-alias	存在する場合は、メッセージの発信者に関連付けられた最初の H.323 エイリアス。 存在する場合は、メッセージの発信者に関連付けられた最初の H.164 エイリアス。
Dst-alias	存在する場合は、メッセージの受信者に関連付けられた最初の H.323 エイリアス。 存在する場合は、メッセージの受信者に関連付けられた最初の H.164 エイリアス。
詳細（Detail）	イベントの説明的な詳細。
Auth	コール試行が正常に認証されたかどうか。
メソッド	SIP メソッド（INVITE、BYE、UPDATE、REGISTER、SUBSCRIBE など）。
お問い合わせ	連絡先：REGISTER のヘッダー。
AOR	レコードのアドレス。
Call-id	コール ID ヘッダー フィールドは、特定の招待、または特定のクライアントのすべての登録を一意に識別します。
コールシリアル番号	特定のコールのすべてのプロトコル メッセージに共通のローカル コール シリアル番号。

名前	説明
タグ（Tag）	タグは、コールのすべてのフォークについて、Expressway ネットワーク上のすべての検索とプロトコル メッセージに共通です。
ルーティング済みコール	Expressway がコールのシグナリングを取得したことを示します。
移行後	• REGISTER 要求の場合：REGISTER 要求の AOR。 • INVITE の場合：ダイヤルされた元のエイリアス。 • その他のすべての SIP メッセージの場合：宛先の AOR。
Request-URI	この要求の送信先のユーザまたはサービスを示す SIP または SIPS URI。
Num-bytes	メッセージで送受信されたバイト数。
Protocol-buffer	メッセージが復号化できなかったときにバッファに含まれていたデータを表示します。
デュレーション（Duration）	要求/付与された登録満了期間
時刻	YYYY/MM/DD-HH:MM:SS 形式の完全な UTC タイムスタンプ。この形式を使用することによって、シンプルな ASCII テキストの並べ替え/順序付けを時刻で自然に並べ替えることができます。これは、標準的な syslog タイムスタンプの制限により含まれています。
レベル	イベント ログ レベルについての項で定義されているイベント ログのレベル。
UTC 時間	イベントが発生した時刻。UTC 形式で表示されます。

イベントとレベル

次の表に、イベントログに表示される可能性があるイベントのリストを示します。

イベント	説明	レベル
Alarm acknowledged	管理者がアラームを確認しました。**Detail** イベント パラメータによって問題の特性に関する情報が提供されます。	1
Alarm lowered	アラームを発生させる原因となった問題が解決されました。**Detail** イベント パラメータによって問題の特性に関する情報が提供されます。	1
Alarm raised	Expressway が問題を検出し、アラームが発生しました。**Detail** イベント パラメータによって問題の特性に関する情報が提供されます。	1
Admin Session CBA Authorization Failure	Expressway が証明書ベースの認証を使用するように設定されている場合にログイン試行が失敗しました。	1
Admin Session Finish	管理者がシステムからログオフしました。	1
Admin Session Login Failure	管理者としてのログイン試行が失敗しました。これは、誤ったユーザ名またはパスワード（あるいはその両方）が入力されたために発生した可能性があります。	1
Admin Session Start	管理者がシステムにログオンしました。	1
Application Exit	Expressway アプリケーションが終了しました。さらに詳しい情報が、**Detail** イベント パラメータに示される場合があります。	1
Application Failed	Expressway アプリケーションは予期しない障害によりサービスが停止しました。	1

イベント	説明	レベル
Application Start	Expressway が起動しました。より詳しい情報が、**Detail** イベント パラメータに示される場合があります。	1
Application Warning	Expressway アプリケーションはまだ実行していますが、回復可能な問題が発生しています。より詳しい情報が、**Detail** イベント パラメータに示される場合があります。	1
Authorization Failure	ユーザが無効なクレデンシャルを持っている、またはアクセスグループに属していない、あるいはアクセスレベルが「「なし」」のグループに属しています。リモート認証が有効になっている場合に適用されます。	1
Beginning System Backup	システム バックアップが起動しました。	1
Beginning System Restore	システムの復元が開始されました。	1
Call Answer Attempted	コールへの応答を試行しました。	1
Call Attempted	コールを試行しました。	1
Call Bandwidth Changed	コールのエンドポイントがコールの帯域幅を再ネゴシエートしました。	1
Call Connected	コールが接続されました。	1
Call Diverted	コールを転送しました。	1
Call Disconnected	コールが切断されました。	1
Call Inactivity Timer	コールは、非アクティビティにより切断されました。	1

イベント	説明	レベル
Call Rejected	コールが拒否されました。**Reason** イベント パラメータには、H.225 追加原因コードのテキスト表現が含まれています。	1
Call Rerouted	Expressway で **[コールシグナリングの最適化（Call signaling optimization）]** が *[オン（On）]* に設定されており、コール シグナリング パスから Expressway が除外されています。	1
CBA Authorization Failure	証明書ベースの認証を使用したログイン試行が認証の失敗により拒否されました。	1
Certificate Management	セキュリティ証明書がアップロードされたことを示します。詳細については、**Detail** イベント パラメータを参照してください。	1
Completed System Backup	システムのバックアップが完了しました。	1
Completed System restore	システムの復元が完了しました。	1
Configlog Cleared	オペレータがコンフィギュレーション ログをクリアしました。	1
Decode Error	SIP メッセージまたは H.323 メッセージの復号化中に構文エラーが発生しました。	1
Diagnostic Logging	診断のロギングが進行中であることを示します。**Detail** イベント パラメータに追加の詳細情報が示されます。	1

イベント	説明	レベル
Error Response Sent	TURN サーバがクライアントに（STUN プロトコルを使用して）エラー メッセージを送信しました。	3
Eventlog Cleared	オペレータがイベント ログをクリアしました。	
External Server Communication Failure	外部サーバとの通信が予期切失敗しました。**Detail** イベントパラメータで「「応答なし」」と「「応答拒否」」を区別する必要があります。関係するサーバは次のとおりです。 • DNS • LDAP サーバ • ネイバー ベートキーパー • NTP サーバ • ピア	
ハードウェア障害（Hardware failure）	Expressway ハードウェアに問題があります。問題が解決しない場合は、シスコのサポート担当者に連絡してください。	
License Limit Reached	特定の機能のライセンスの制限に到達しました。**Detail** イベント パラメータに関連する機能や制限が示されます。 これが頻繁に発生する場合は、シスコの担当者に連絡し、ライセンスを追加購入してください。	
Message Received	着信 RAS メッセージを受信しました。	2

イベント	説明	レベル
Message Received	着信 RAS NSM キープアライブ、ピア間の H.225、H.254、または RAS メッセージを受信しました。	3
Message Received	（SIP）着信メッセージを受信しました。	4
Message Rejected	次の 2 つの理由のどちらかで発生した可能性があります。 • 認証が有効になっており、エンドポイントがメッセージ（登録要求など）の Expressway への送信試行に失敗した場合。これは、エンドポイントが認証クレデンシャルを提供していないか、またはクレデンシャルが Expressway が予期していたものと一致しないかのいずれかの場合に発生します。 • クラスタリングが有効になっていてもクラスタ上の帯域幅が同一に設定されておらず、さらに、Expressway が不明なピア、リンク、パイプ、サブゾーン、またはゾーンに関連するメッセージを受信した場合。	
Message Sent	送信 RAS メッセージを送信しました。	2
Message Sent	送信 RAS NSM キープアライブ、H.255、H.245、またはピア間の RAS メッセージが送信されました。	3
Message Sent	（SIP）送信メッセージを送信しました。	4

イベント	説明	レベル
Operator Call Disconnect	管理者がコールを切断しました。	1
Outbound TLS Negotiation Error	Expressway は TLS で別のシステムと通信できません。イベント パラメータで詳細情報が提供されます。	1
Package Install	言語パックなどのパッケージがインストールされたか、または削除されました。	2
Policy Change	ポリシー ファイルが更新されました。	1
POST request failed	HTTP POST 要求が未許可セッションから送信されました。	1
プロビジョニング	プロビジョニング サーバからの診断メッセージ。**Detail** イベント パラメータに追加情報が示されます。	1
Reboot Requested	システム リブートが要求されました。**Reason** イベント パラメータに具体的な情報が示されます。	1
Registration Accepted	登録要求が承認されました。	1
Registration Refresh Accepted	登録の更新またはキープ アライブの要求が承認されました。	3
Registration Refresh Rejected	登録更新の要求が拒否されました。	1
Registration Refresh Requested	登録の更新またはキープ アライブの要求を受信しました。	3
Registration Rejected	登録要求が拒否されました。**Reason** イベント パラメータと **Detail** イベント パラメータに、拒否の特性に関する情報が示されます。	1

イベント	説明	レベル
Registration Removed	Expressway によって登録が削除されました。**Reason** イベント パラメータに登録が削除された理由が示されます。理由は次のいずれかです。 • 認証の変更（Authentication change） • ゾーンの競合（Conflicting zones） • オペレータによる強制削除（Operator forced removal） • オペレータによる強制削除（すべての登録を削除）（Operator forced removal (all registrations removed)） • 登録を優先（Registration superseded.）	1
Registration Requested	登録が要求されました。	1
Relay Allocated	TURN サーバ リレーが割り当てられました。	2
Relay Deleted	TURN サーバ リレーが削除されました。	2
Relay Expired	TURN サーバ リレーの期限が切れました。	2
Request Failed	Conference Factory への要求が失敗しました。	1
Request Received	コール関連の SIP 要求を受信しました。	2
Request Received	非コール関連 SIP 要求を受信しました。	3
Request Sent	コール関連の SIP 要求を送信しました。	2

イベント	説明	レベル
Request Sent	非コール関連の SIP 要求を送信しました。	3
Request Successful	成功した要求が Conference Factory に送信されました。	1
Response Received	コール関連の SIP 応答を受信しました。	2
Response Received	非コール関連 SIP 応答を受信しました。	3
Response Sent	コール関連 SIP 応答を送信しました。	2
Response Sent	非コール関連のSIP応答を送信しました。	3
Restart Requested	システムの再起動が要求されました。**Reason** イベント パラメータに具体的な情報が示されます。	1
Search Attempted	検索を試行しました。	1
Search Cancelled	検索がキャンセルされました。	1
Search Completed	検索が完了しました。	1
Search Loop detected	Expressway は **[コールループ検出（Call loop detection）]** モードになっており、ループ化された検索のブランチを特定し、終了させました。	2
Secure mode disabled	Expressway は正常に **[高度なアカウントセキュリティ（Advanced account security）]** モードを終了しました。	1
Secure mode enabled	Expressway は正常に **[高度なアカウント セキュリティ（Advanced account security）]** モードを開始しました。	1

イベント	説明	レベル
Security Alert	Expressway でセキュリティ関連の潜在的な攻撃が検出されました。	1
Success Response Sent	TURN サーバがクライアントに（STUN プロトコルを使用して）成功メッセージを送信しました。	3
System backup completed	システムのバックアップ プロセスが完了しました。	1
System Backup error	システムのバックアップ試行中にエラーが発生しました。	1
System backup started	システムのバックアップ プロセスが開始しました。	1
System Configuration Changed	システムの設定項目が変更されました。**Detail** イベント パラメータに、変更された設定項目の名前と新しい値が格納されます。	1
System restore completed	システムの復元プロセスが完了しました。	1
System restore backing up current config	システムの復元プロセスが現在の設定のバックアップを開始しました。	1
System restore backup of current config completed	システムの復元プロセスが現在の設定のバックアップを完了しました。	1
System restore error	システムの復元を試行中にエラーが発生しました。	1
System restore started	システムの復元プロセスが開始しました。	1
System Shutdown	オペレーティング システムがシャットダウンされました。	1
System snapshot started	システム スナップショットが開始されました。	1

イベント	説明	レベル
System snapshot completed	システム スナップショットが完了しました。	1
System Start	オペレーティング システムが起動しました。起動に問題がある場合は、**Detail** イベント パラメータに追加情報が格納されることがあります。	1
TLS Negotiation Error	Transport Layer Security（TLS）接続がネゴシエートに失敗しました。	1
Unregistration Accepted	登録解除要求が承認されました。	1
Unregistration Rejected	登録解除要求が拒否されました。	1
Unregistration Requested	登録解除要求を受信しました。	1
アップグレード	ソフトウェア アップグレード プロセスに関連するメッセージ。**Detail** イベント パラメータに具体的な情報が示されます。	1

CPL リファレンス

コール処理言語（CPL）はコール処理を定義するための XML ベースの言語です。ここでは、Expressway の CPL の実装に関する詳細を示します。CPL 標準規格の RFC 3880.と併せてお読みください。

Expressway には数多くの強力な組み込みトランスフォーメーション機能が備わっています。そのため、高度なコール処理ルールが必要な場合にのみ、CPL が必要になります。

Expressway はほとんどの CPL 標準規格と、一部の TANDBERG 定義の拡張機能をサポートします。トップ レベルのアクションである `<incoming>` と `<outgoing>`（*RFC 3880* で説明）はサポートされません。代わりに、`<taa:routed>` セクション内の CPL の単一のセクションをサポートします。

CPL スクリプトを Expressway にアップロードすることによってコール ポリシーを実装する場合、そのスクリプトは XML スキーマと照合してシンタックスが確認されます。スキーマには、基本の CPL 仕様用のスキーマと TANDBERG 拡張機能用のスキーマの 2 つがあります。どち

らのスキーマも CPL スクリプトを使用したコール ポリシーの設定して、Expressway へのアップロードの前にスクリプトを検証するために使用できます。

次に、シンタックスを許可されるようにする名前空間の正しい使用方法を示します。

```
<?xml version="1.0" encoding="UTF-8" ?>
<cpl xmlns="urn:ietf:params:xml:ns:cpl"
xmlns:taa="http://www.tandberg.net/cpl-extensions"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="urn:ietf:params:xml:ns:cpl cpl.xsd">
 <taa:routed>
  <address-switch field="destination">
   <address is="reception@example.com">
    <proxy/>
   </address>
  </address-switch>
 </taa:routed>
</cpl>
```

送信元アドレスと宛先アドレスの形式

この項の説明でコールの送信元エイリアスまたは宛先エイリアスに言及する場合は、サポートされているすべてのアドレス形式（URI、IP アドレス、E.164 エイリアスなど）を意味します。

CPL アドレス スイッチ ノード

address-switch ノードによって、コールの送信元エイリアスまたは宛先エイリアスに基づき、スクリプトは異なるアクションを実行できます。照合するフィールドを指定してから、アドレス ノードのリストに考えられる一致と関連付けられたアクションを含めます。

address-switch には、field と subfield という 2 つのノード パラメータがあります。

アドレス

address 構造体を address-switch 内に使用して、照合するアドレスを指定します。正規表現の使用をサポートします。

有効な値は次のとおりです。

is=string	選択したフィールドとサブフィールドが指定した文字列と正確に一致しています。
contains=string	選択したフィールドとサブフィールドに指定した文字列が含まれています。CPL 標準規格のみで表示サブフィールドでのこの照合が可能です。ただし、Expressway ではどのタイプのフィールドでもこの照合が可能です。

サブドメイン = 文字列	選択したフィールドが数字（電話のサブフィールドなど）の場合、これはプレフィックスとして一致します。たとえば、address subdomain-of=「555」は 5556734 などと一致します。フィールドが数字でない場合は、通常のドメイン名の照合が適用されます。たとえば、address subdomain-of=「company.com」は nodeA.company.com などと一致します。
regex=「regular expression」	選択したフィールドとサブフィールドは指定した正規表現を照合します。

すべてのアドレスの比較では大文字と小文字の違いが無視されます。たとえば、address is=「Fred」は fred、freD などと一致します。

フィールド

address-switch ノード内では、必須の field パラメータで考慮対象のアドレスを指定します。次に、サポートされる属性とその解釈を示します。

フィールド パラメータの属性	SIP	H.323
認証されていない発信元	着信メッセージの 「From」フィールドと 「ReplyTo」フィールド。	コールを開始した元の LRQ または ARQ の送信元エイリアス。SETUP を RAS の先行メッセージなしに受信した場合は、発信元は SETUP から取得されます。
authenticated-origin および origin	正しく認証されている場合（または関連する **[認証ポリシー（Authentication Policy）]** が *[認証済みとして処理（Treat as authenticated）]* の場合）は、メッセージの 「From」フィールドと 「ReplyTo」フィールド。それ以外の場合は not-present です。	正しく認証されている場合（または関連する **[認証ポリシー（Authentication Policy）]** が *[認証済みとして処理（Treat as authenticated）]* の場合）は、コールを開始した元の LRQ または ARQ の送信元エイリアス。それ以外の場合は not-present。SETUP メッセージは認証されないため、Expressway が SETUP メッセージを先行する RAS メッセージなしに受信した場合、発信元は常に not-present になります。

フィールド パラメータの属性	SIP	H.323
originating-zone	コールの発信元のレッグのゾーンまたはサブゾーンの名前。コールがネイバー ゾーン、トラバーサル サーバ ゾーン、またはトラバーサル クライアント ゾーンから発信された場合、これはゾーン名と等しくなります。コールがローカル サブゾーンのいずれか内のエンドポイントから発信された場合、これはサブゾーンの名前になります。コールがその他のローカルに登録されたエンドポイントから発信された場合、これは 「DefaultSubZone」 になります。それ以外の場合は、「DefaultZone」 になります。	
originating-user	**関連する [認証ポリシー（Authentication Policy）]**が*[クレデンシャルの確認（Check credentials）]* または *[*認証済みとして処理（*Treat as authenticated*）*]* の場合、これは認証に使用されたユーザ名になります。それ以外の場合は not-present になります。	
登録済み-発信元	コールが登録済みのエンドポイントから発信された場合、これは登録したエイリアスのリストになります。それ以外の場合は not-present になります。	
接続先	宛先エイリアス。	
元の宛先	宛先エイリアス。	

適用する認証ポリシー設定は、着信メッセージの送信元に応じて、関連ゾーン用に設定されています。

選択したフィールドに複数のエイリアスが含まれている場合、Expressway は次のアドレス ノードに進む前に各アドレスノードをすべてのエイリアスで照合しようとします。つまり、いずれかのエイリアスに一致する場合はアドレス ノードは一致します。

サブフィールド

address-switch ノードでは、オプションのサブフィールド パラメータで考慮するアドレスに部分を指定します。次の表に、サブフィールドの定義をエイリアス タイプごとに示します。

照合するエイリアス タイプにサブフィールドが指定されていない場合は、not-present アクションが実行されます。

address-type	コールを発信したエンドポイントのタイプに基づいて、h323 または sip のいずれかになります。
user	URI エイリアスの場合は、これによってユーザ名の部分が選択されます。H.323 ID の場合は ID 全体、E.164 番号の場合は番号全体になります。

ホスト	URI エイリアスの場合は、これによってドメイン名の部分が選択されます。エイリアスが IP アドレスの場合は、このサブフィールドはドット付き 10 進法形式の完全なアドレスになります。
tel	E.164 番号の場合は、これによって数字の文字列全体が選択されます。
エイリアスタイプ	エイリアスのタイプの文字列表現を指定します。タイプは、エイリアスの形式から推定されます。可能なタイプは次のとおりです。 • アドレス タイプ • 結果 • URI • url-ID • H.323 ID • h323-ID • ダイヤル番号 • dialedDigits

otherwise

`otherwise` ノードは、`address-switch` で指定されているアドレスが見つかったものの、先行するアドレス ノードが 1 つも一致しなかった場合に実行されます。

Not-Present

`not-present` ノードは、`address-switch` で指定されているアドレスがコール セットアップ メッセージに含まれていなかった場合に実行されます。この形式は、認証を使用するときに最も有効です。認証が有効になっている Expressway は、ポリシーを実行するときに認証されたエイリアスのみを使用します。そのため、認証されていないユーザからコールを受信したときに not-present アクションを使用し、適切なアクションを実行します（「認証されたユーザの発信者名の確認」の例を参照してください）。

参照先

CPL スクリプトは評価されるため、`proxy` ノードが実行される場合はコールの宛先として使用されるアドレス（H.323 ID、URL、および E.164 番号）のリストを保持します。`taa:location`

ノードを使用して場所の設定を変更することで、コールを異なる宛先にリダイレクトできます。

スクリプト実行の開始時に、場所の設定は元の宛先に初期化されます。

次の属性は `taa:location` ノードでサポートされます。正規表現の使用をサポートします。

`Clear = 「yes」	「no」`	新しいロケーションを追加する前に現在の場所の設定をクリアするかどうかを指定します。デフォルトでは、この場所が設定の末尾に追加されます。
`url=string`	場所の設定に追加される新しい場所。所定の文字列でURL（`user@domain.com` など）、H.323 ID または E.164 番号を指定できます。
`priority=<0.0..1.0>	「ランダム」`	0.0 ～ 1.0 の範囲の浮動小数点数か、または、同じ範囲内の乱数を割り当てる `random` のいずれかとして指定されます。1.0 が最も高いプライオリティです。同じプライオリティの場所の検索は並行して実行されます。
`regex=「<regular expression>」 replace=「<string>」`	正規表現に一致する場所を変更する方法を指定します。
`source-url-for-message=「<string>」`	指定された文字列でFromヘッダー（送信元エイリアス）を置換します。
`source-url-for-message-regex=「<regular expression>」` together with `source-url-for-message-replace=「<string>」`	指定した置換文字列で、正規表現に一致するFromヘッダー（送信元エイリアス）を置換します。複数のFromヘッダーがある場合（H.323のみに適用）、一致しないFromヘッダーは変更されずにそのまま残ります。

Fromヘッダーの送信元URLが変更されると、対応する表示名も変更された送信元URLのユーザ名の部分に一致するように変更されます。

Rule-Switch

CPLのこの拡張機能は、コールの送信元と宛先の両方に基づいて決定を下す必要があるコールポリシーのスクリプトを簡単にするために提供されています。`taa:rule-switch` には、順番にテストされる多くのルールを含めることができます。一致が検出されるとすぐにそのルール要素内の CPL が実行されます。

各ルールは次のいずれかの形式である必要があります。

```
<taa:rule-switch>
 <taa:rule origin="<regular expression>" destination="<regular expression>"
message-regex="<regular expression>">
 <taa:rule authenticated-origin="<regular expression>" destination="<regular expression>"
 message-regex="<regular expression>">
```

```
 <taa:rule unauthenticated-origin="<regular expression>" destination="<regular expression>"
 message-regex="<regular expression>">
 <taa:rule registered-origin="<regular expression>" destination="<regular expression>"
message-regex="<regular expression>">
 <taa:rule originating-user="<regular expression>" destination="<regular expression>"
message-regex="<regular expression>">
 <taa:rule originating-zone="<regular expression>" destination="<regular expression>"
message-regex="<regular expression>">
</taa:rule-switch>
```

さまざまな origin セレクタの意味は、CPL アドレス スイッチ ノード の項で説明されているとおりです。

`message-regex` パラメータでは、着信 SIP メッセージ全体に対して正規表現を照合させることができます。

（注） message-regex パラメータを含むルールは H.323 コールを照合しません。

プロキシ

proxy ノードでの実行時に、Expressway はコールを現在のロケーション設定で指定された場所に転送しようとします。ロケーション設定に複数のエントリがある場合は、分岐されたコールになります。現在のロケーション設定が空の場合は、元の宛先にコールが転送されます。

proxy ノードでは、次のオプション パラメータがサポートされます。

`timeout=<1..86400>`	秒単位で指定されたタイムアウト時間
`stop-on-busy = 「yes」 | 「no」`	ビジー応答を受信した場合に検索を停止するかどうか

プロキシ アクションによって、次の表に示す結果となる可能性があります。

`failure`	プロキシがコールのルーティングに失敗しました
busy	宛先を検出したが、ビジー状態になっています
`noanswer`	宛先を検出したが応答がありません
`redirection`	Expressway がコールのリダイレクトを求められています
デフォルト	他の結果が適用されない場合に実行する CPL

CPL はこれらの結果に基づいて、さらにアクションを実行することができます。どの結果ノードも `proxy` ノード内に含まれる必要があります。例：

```
<proxy timeout="10">
 <busy>
```

```
  <!--If busy route to recording service-->
  <location clear="yes" url="recorder">
   <proxy/>
  </location>
 </busy>
</proxy>
```

拒否

`reject` ノードが実行された場合、Expressway はそれ以降のスクリプト処理を中止し、現在のコールを拒否します。

ここでは、カスタムの拒否文字列である `status=string` オプションと `reason=string` オプションがサポートされており、ストリングの一貫性を確保するためにこれらを一緒に使用する必要があります。

サポートされていない CPL 要素

Expressway は現在、CPL RFC で説明されている一部の要素をサポートしていません。次の要素のいずれかを含むスクリプトをアップロードしようとすると、エラー メッセージが生成され、Expressway は既存のポリシーを使用し続けます。

現在、次の要素はサポートされません。

- time-switch
- string-switch
- language-switch
- priority-switch
- redirect
- mail
- log
- subaction
- lookup
- remove-location

CPL の例

ここでは、CPL 選択の例を示します。

- 認証されたユーザの発信者名確認
- ドメインに基づいた発信者名確認
- ローカルに登録されたエンドポイントからのコールのみの許可

- デフォルト ゾーンとデフォルト サブゾーンからのコールのブロック
- ローカル ゲートウェイへのアクセスの制限

CPL の例：認証されたユーザの発信者名確認

（注） この動作はコール ポリシー ルールを使用して設定できるため、CPL スクリプトを使用して行う必要はありません。ただし、UI によって設定されたルールとアップロードされた CPL スクリプトを組み合わせて使用することはできないため、UI ルールを使用して実装できない CPL 要件がある場合は、すべてのルールにスクリプトを使用する必要があります。コール ポリシーについてを参照してください。

この例では、認証された送信元アドレスを持つユーザからのコールのみが許可されます。認証を有効化する方法の詳細については、デバイス認証についてを参照してください。

コールが Expressway-E を通じて着信する場合は、望ましくないコールがネットワーク内に進行しないように Expressway-E での発信者名確認を推奨します。

```
<?xml version="1.0" encoding="UTF-8" ?>
<cpl xmlns="urn:ietf:params:xml:ns:cpl"
 xmlns:taa="http://www.tandberg.net/cpl-extensions"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="urn:ietf:params:xml:ns:cpl cpl.xsd">
 <taa:routed>
  <address-switch field="authenticated-origin">
   <not-present>
    <!-- Reject call with a status code of 403 (Forbidden) -->
    <reject status="403" reason="Denied by policy"/>
   </not-present>
  </address-switch>
 </taa:routed>
</cpl>
```

CPL の例：エイリアスに基づいた発信者名確認

（注） この動作はコール ポリシー ルールを使用して設定できるため、CPL スクリプトを使用して行う必要はありません。ただし、UI によって設定されたルールとアップロードされた CPL スクリプトを組み合わせて使用することはできないため、UI ルールを使用して実装できない CPL 要件がある場合は、すべてのルールにスクリプトを使用する必要があります。コール ポリシーについてを参照してください。

この例では、ユーザ ceo が、ユーザ `vpsales`、`vpmarketing`、または `vpengineering` からのコールのみを受け入れます。

コールが Expressway-E を通じて着信する場合は、望ましくないコールがネットワーク内に進行しないように Expressway-E での発信者名確認を推奨します。

```
<?xml version="1.0" encoding="UTF-8" ?>
<cpl xmlns="urn:ietf:params:xml:ns:cpl"
```

```
xmlns:taa="http://www.tandberg.net/cpl-extensions"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="urn:ietf:params:xml:ns:cpl cpl.xsd">
 <taa:routed>
  <address-switch field="destination">
   <address is="ceo">
    <address-switch field="authenticated-origin">
     <address regex="vpsales|vpmarketing|vpengineering">
      <!-- Allow the call -->
      <proxy/>
     </address>
     <not-present>
      <!-- Unauthenticated user -->
      <!-- Reject call with a status code of 403 (Forbidden) -->
      <reject status="403" reason="Denied by policy"/>
     </not-present>
     <otherwise>
      <!-- Reject call with a status code of 403 (Forbidden) -->
      <reject status="403" reason="Denied by policy"/>
     </otherwise>
    </address-switch>
   </address>
  </address-switch>
 </taa:routed>
</cpl>
```

CPL の例：ドメインに基づいた発信者名確認

（注） この動作はコール ポリシー ルールを使用して設定できるため、CPL スクリプトを使用して行う必要はありません。ただし、UI によって設定されたルールとアップロードされた CPL スクリプトを組み合わせて使用することはできないため、UI ルールを使用して実装できない CPL 要件がある場合は、すべてのルールにスクリプトを使用する必要があります。コールポリシーについてを参照してください。

この例では、ユーザの fred が `annoying.com` のすべてのユーザ、または認証されていないユーザからのコールを受け入れません。その他のすべてのユーザはコールが許可されます。

コールが Expressway-E を通じて着信する場合は、望ましくないコールがネットワーク内に進行しないように Expressway-E での発信者名確認を推奨します。

```
<?xml version="1.0" encoding="UTF-8" ?>
<cpl xmlns="urn:ietf:params:xml:ns:cpl"
xmlns:taa="http://www.tandberg.net/cpl-extensions"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="urn:ietf:params:xml:ns:cpl cpl.xsd">
 <taa:routed>
  <address-switch field="destination">
   <address is="fred">
    <address-switch field="authenticated-origin" subfield="host">
     <address subdomain-of="annoying.com">
      <!-- Don't accept calls from this source -->
      <!-- Reject call with a status code of 403 (Forbidden) -->
      <reject status="403" reason="Denied by policy"/>
     </address>
     <not-present>
      <!-- Don't accept calls from unauthenticated sources -->
      <!-- Reject call with a status code of 403 (Forbidden) -->
```

```
      <reject status="403" reason="Denied by policy"/>
     </not-present>
     <otherwise>
      <!-- All other calls allowed -->
      <proxy/>
     </otherwise>
    </address-switch>
   </address>
  </address-switch>
 </taa:routed>
</cpl>
```

CPL の例：ローカルに登録されたエンドポイントからのコールのみの許可

（注） この例では、管理者がローカルに登録されたエンドポイントから発信されたコールのみを許可しようと考えています。

```
<?xml version="1.0" encoding="UTF-8" ?>
<cpl xmlns="urn:ietf:params:xml:ns:cpl"
 xmlns:taa="http://www.tandberg.net/cpl-extensions"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="urn:ietf:params:xml:ns:cpl cpl.xsd">
 <taa:routed>
  <address-switch field="registered-origin">
   <not-present>
    <reject status="403" reason="Only local endpoints can use this Expressway"/>
   </not-present>
  </address-switch>
 </taa:routed>
</cpl>
```

CPL の例：デフォルト ゾーンとデフォルト サブゾーンからのコールのブロック

（注） この動作はコール ポリシー ルールを使用して設定できるため、CPL スクリプトを使用して行う必要はありません。ただし、UI によって設定されたルールとアップロードされた CPL スクリプトを組み合わせて使用することはできないため、UI ルールを使用して実装できない CPL 要件がある場合は、すべてのルールにスクリプトを使用する必要があります。コール ポリシーについてを参照してください。

ローカルに登録されたエンドポイントからのコールのみを許可するスクリプトは、デフォルト ゾーンまたはデフォルト サブゾーンからでなく、設定されたゾーンからのコールを許可するように拡張できます。

```
<?xml version="1.0" encoding="UTF-8" ?>
<cpl xmlns="urn:ietf:params:xml:ns:cpl"
xmlns:taa="http://www.tandberg.net/cpl-extensions"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="urn:ietf:params:xml:ns:cpl cpl.xsd">
 <taa:routed>
  <address-switch field="registered-origin">
   <not-present>
    <address-switch field="originating-zone">
     <address is="DefaultZone">
```

```
      <!-- Reject call with a status code of 403 (Forbidden) -->
      <reject status="403" reason="Denied by policy"/>
     </address>
     <address is="DefaultSubZone">
      <!-- Reject call with a status code of 403 (Forbidden) -->
      <reject status="403" reason="Denied by policy"/>
     </address>
     <otherwise>
      <proxy/>
     </otherwise>
    </address-switch>
   </not-present>
  </address-switch>
 </taa:routed>
</cpl>
```

CPL の例：ローカル ゲートウェイへのアクセスの制限

（注） この動作はコール ポリシー ルールを使用して設定できるため、CPL スクリプトを使用して行う必要はありません。ただし、UI によって設定されたルールとアップロードされた CPL スクリプトを組み合わせて使用することはできないため、UI ルールを使用して実装できない CPL 要件がある場合は、すべてのルールにスクリプトを使用する必要があります。コール ポリシーについてを参照してください。

次の例では、ゲートウェイが 9 のプレフィックスで Expressway に登録されており、管理者は組織外からのコールをゲートウェイを通じてルーティングしないようにしたいと考えています。

これを行うには、`address-switch` ノードを使用する方法と `taa:rule-switch` ノードを使用する方法の 2 つがあります。次に、それぞれの例を示します。

（注） Cisco Unified Communications Manager でコールルーティングを使用すると、同じ結果を取得できます。この例が示されているのは、これらのタイプのコールがネットワークのさらに深い部分に到達するのを防ぎたいと思う場合があるためです。

address-switch ノードの使用：

```
<?xml version="1.0" encoding="UTF-8" ?>
<cpl xmlns="urn:ietf:params:xml:ns:cpl"
xmlns:taa="http://www.tandberg.net/cpl-extensions"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="urn:ietf:params:xml:ns:cpl cpl.xsd">
 <taa:routed>
  <address-switch field="destination">
   <address regex="9(.*)">
    <address-switch field="originating-zone">
     <!-- Calls coming from the traversal zone are not allowed to use this gateway -->
     <address is="TraversalZone">
      <!-- Reject call with a status code of 403 (Forbidden) -->
      <reject status="403" reason="Denied by policy"/>
     </address>
    </address-switch>
```

```
   </address>
  </address-switch>
 </taa:routed>
</cpl>
```

taa:rule-switch ノードの使用

```
<?xml version="1.0" encoding="UTF-8" ?>
<cpl xmlns="urn:ietf:params:xml:ns:cpl"
 xmlns:taa="http://www.tandberg.net/cpl-extensions"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="urn:ietf:params:xml:ns:cpl cpl.xsd">
 <taa:routed>
  <taa:rule-switch>
   <taa:rule originating-zone="TraversalZone" destination="9(.*)">
    <!-- Calls coming from the traversal zone are not allowed to use this gateway -->
    <!-- Reject call with a status code of 403 (Forbidden) -->
    <reject status="403" reason="Denied by policy"/>
   </taa:rule>
   <taa:rule origin="(.*)" destination="(.*)">
    <!-- All other calls allowed -->
    <proxy/>
   </taa:rule>
  </taa:rule-switch>
 </taa:routed>
</cpl>
```

デバイス認証用の LDAP サーバの設定

LDAP サーバ上の H.350 ディレクトリ サービスに対してデバイスを認証するように Expressway を設定できます。

ここでは、次の方法について説明します。

- LDAP サーバにインストールする必要がある H.350 スキーマのダウンロード
- Expressway で使用するための 2 つの一般的なタイプの LDAP サーバのインストールと設定
  - Microsoft Active Directory用の LDAP サーバの設定
  - OpenLDAP サーバの設定

H.350 スキーマのダウンロード

次の ITU 仕様で、LDAP サーバにインストールする必要があるスキーマについて説明します。

H.350	マルチメディア会議用のディレクトリ サービス アーキテクチャ：ネットワーク上のエンドポイントを表現する LDAP スキーマ
H.350.1	H.323 用のディレクトリ サービス アーキテクチャ：H.323 のエンドポイントを表現する LDAP スキーマ

H.350.2	H.235 用のディレクトリ サービス アーキテクチャ：H.235 の要素を表現する LDAP スキーマ
H.350.4	SIP 用のディレクトリ サービス アーキテクチャ：SIP のエンドポイントを表現する LDAP スキーマ

スキーマは Expressway の Web インターフェイスからダウンロードできます。次の手順を実行します。

1. **[設定（Configuration）] > [認証（Authentication）] > [デバイス（Devices）] > [H.350 ディレクトリ スキーマ（H.350 directory schemas）]** に移動します。ダウンロード可能なスキーマのリストが表示されます。
2. 各ファイルの横にある **[ダウンロード（Download）]** ボタンをクリックし、ファイルを開きます。
3. ブラウザの **[名前を付けて保存（Save As）]** コマンドを使用してファイルをファイル システムに保存します。

Microsoft Active Directory用の LDAP サーバの設定

前提条件

次の手順は、Active Directory がすでにインストールされていると想定しています。Active Directory のインストールの詳細については、Windows のドキュメントを参照してください。

次の手順は、Windows Server 2003 Enterprise Edition 用です。このバージョンの Windows を使用していない場合は、手順が異なります。

H.350 スキーマのインストール

H.350 スキーマのダウンロード、次のようにインストールします。

コマンド プロンプトを右クリックし、[管理者として実行（Run as administrator）] を選択して管理者特権でのコマンドプロンプトを開きます。ファイルごとに次のコマンドを実行します。

```
ldifde -i -c DC=X <ldap_base> -f filename.ldf
```

値は次のとおりです。

`<ldap_base>` は Active Directory サーバのベース DN です。

H.350 オブジェクトの追加

組織階層を作成します。

1. Active Directory の **[ユーザとコンピュータ（Users and Computers）]** MMC スナップインを開きます。

2. ベース DN で、[新しい組織ユニット（New Organizational Unit）] を右クリックします。
3. *h350* という組織ユニットを作成します。

独自の組織ユニット内に H.350 ディレクトリを保持して H.350 オブジェクトを他のタイプのオブジェクトと区別することをお勧めします。これによって、BaseDN への Expressway 読み取りアクセスのみを許可するアクセス制御を設定してディレクトリの他のセクションへのアクセスを制限できます。

H.350 オブジェクトを追加するには、次の手順を実行します。

1. 次の内容の ldif ファイルを作成します。

```
# MeetingRoom1 endpoint
dn: commUniqueId=comm1,ou=h350,DC=X
objectClass: commObject
objectClass: h323Identity
objectClass: h235Identity
objectClass: SIPIdentity
commUniqueId: comm1
h323Identityh323-ID: MeetingRoom1
h323IdentitydialedDigits: 626262
h235IdentityEndpointID: meetingroom1
h235IdentityPassword: mypassword
SIPIdentityUserName: meetingroom1
SIPIdentityPassword: mypassword
SIPIdentitySIPURI: sip:MeetingRoom@X
```

2. 次のコマンドを使用して ldif ファイルをサーバに追加します。

```
ldifde -i -c DC=X <ldap_base> -f filename.ldf
```

値は次のとおりです。

`<ldap_base>` は Active Directory サーバのベース DN です。

上記の例では、`MeetingRoom1` の H.323 ID エイリアス、`626262` の E.164 エイリアス、および `MeetingRoom@X` の SIP URI を持つ単一のエンドポイントを追加します。また、エントリには認証時に使用された、ID が `meetingroom1`、パスワードが `mypassword` の H.235 および SIP クレデンシャルも存在します。

H.323 の登録では、H.323 と H.235 の属性を検索し、SIP は SIP の属性を検索します。したがって、エンドポイントを 1 つのプロトコルだけで登録する場合は、もう一方のプロトコルに関連するエレメントを組み込む必要はありません。

（注） `ldif` ファイル内の SIP URI には、プレフィックスとして `sip:` が付けられている必要があります。

エイリアスが LDAP データベース内にない場合の動作の詳細については、「LDAP を使用したデバイスの認証」の項の登録用エイリアスのソースを参照してください。

TLS での保護

TLS を使用するように Active Directory を有効にするには、証明書を要求し、Active Directory サーバにインストールする必要があります。証明書は次の要件を満たす必要があります。

- ローカル コンピュータの個人証明書ストアにあること。これは、[証明書（Certificates）] MMC スナップインを使用して確認できます。
- 証明書に関連付けられている秘密キーの取得方法に関する機密情報がローカルに保存されていること。証明書を表示すると、「「この証明書に対応する秘密キーを所有しています（You have a private key that corresponds to this certificate）」」というメッセージが表示されます。
- 強力な秘密キー保護が有効になっていない秘密キーを所有していること。これはキー要求に追加できる属性です。
- Enhanced Key Usage の拡張にサーバ認証オブジェクトの識別子が含まれており、これもキー要求の一部になっていること。
- ドメイン コントローラとクライアントの両方が信頼する CA から発行されていること。
- ドメイン コントローラの Active Directory 完全修飾ドメイン名が件名フィールドの共通名、またはサブジェクト代替名拡張子の DNS エントリに含まれていること。

LDAP サーバへの接続上で TLS を使用するように Expressway を設定するには、CA の証明書を信頼できる CA 証明書としてアップロードする必要があります。これを行うには、Expressway で **[メンテナンス（Maintenance）] > [セキュリティ（Security）] > [信頼できる CA 証明書（Trusted CA certificate）]**に移動します。

OpenLDAP サーバの設定

前提条件

次の手順では、OpenLDAP サーバがすでにインストールされていることを前提としています。OpenLDAP のインストールの詳細については、http://www.openldap.org にあるマニュアルを参照してください。

次に、Linux プラットフォームで OpenLDAP の標準インストールを使用する例を示します。他のプラットフォームのインストールについては、OpenLDAP のコンフィギュレーション ファイルの場所が異なる場合があります。詳細については、OpenLDAP のインストール マニュアルを参照してください。

H.350 スキーマのインストール

1. Expressway からすべてのスキーマ ファイルをダウンロードします（**[設定（Configuration）] > [認証（Authentication）] > [デバイス（Devices）] > [LDAP スキーマ（LDAP schemas）]**）。ファイル名のすべての文字が小文字であり、各ファイル名には .schema 拡張子が付けられていることを確認します。したがって

   commobject.schema

h323identity.schema

h235identity.schema

sipidentity.schema

2. 各スキーマ ファイルのインデックスは slapcat を使用して特定します。たとえば、**commobject.schema** の場合は次のようになります。

   ```
   スド スラップキャット -f schema_convert.conf -F ldif_output -n 0 |grep コミュニケートオブジェクト、cn=スキーマ
   ```

   この場合は、次のような情報が返されます。`dn:cn={14}commobject、cn=schema、cn=config`

   波カッコ {} 内のインデックス値は異なります。

3. `slapcat` を使用して、各スキーマ ファイルを ldif 形式に変換します。前のコマンドによって返されたインデックス値を使用します。たとえば、**commobject.schema** の場合は次のようになります。

   ```
   slapcat -f schema_convert.conf -F ldif_output -n0 -H
   ldap:///cn={14}commobject,cn=schema,cn=config -l cn=commobject.ldif
   ```

4. テキスト エディタを使用して、新たに作成したファイル（commobject ファイルの場合は **cn=commobject.ldif**）を編集し、次の行を削除します。

   ```
   structuralObjectClass:
   entryUUID:
   creatorsName:
   createTimestamp:
   entryCSN:
   modifiersName:
   modifyTimestamp:
   ```

5. `ldapadd` を使用して、各スキーマを ldap データベースに追加します。たとえば、**cn=commobject.ldif** の場合は次のようになります。

   ```
   sudo ldapadd -Q -Y EXTERNAL -H ldapi:/// -f cn\=commobject.ldif
   ```

   （`cn` の後ろのバックスラッシュはエスケープ文字です）。

6. 各スキーマ ファイルに上記のステップを繰り返します。

詳細については、https://help.ubuntu.com/13.04/serverguide/openldap-server.html を参照してください。

H.350 オブジェクトの追加

組織階層を作成します。

1. 次の内容の `ldif` ファイルを作成します。

   ```
   # This example creates a single organizational unit to contain the H.350 objects
   dn: ou=h350,dc=my-domain,dc=com
   objectClass: organizationalUnit
   ou: h350
   ```

2. 次の形式の `slapadd` を使用して、この ldif ファイルをサーバに追加します。

```
slapadd -l <ldif_file>
```

この組織ユニットは、Expressway が検索を実行する BaseDN を形成します。この例では、BaseDN は `ou=h350,dc=my-domain,dc=com` となります。

独自の組織ユニット内に H.350 ディレクトリを保持して H.350 オブジェクトを他のタイプのオブジェクトと区別することをお勧めします。これによって、BaseDN への Expressway 読み取りアクセスのみを許可するアクセス制御を設定してディレクトリの他のセクションへのアクセスを制限できます。

（注） `ldif` ファイル内の SIP URI には、プレフィックスとして `sip:` が付けられている必要があります。

H.350 オブジェクトを追加するには、次の手順を実行します。

1. 次の内容の ldif ファイルを作成します。

```
# MeetingRoom1 endpoint
dn: commUniqueId=comm1,ou=h350,dc=mydomain,dc=com
objectClass: commObject
objectClass: h323Identity
objectClass: h235Identity
objectClass: SIPIdentity
commUniqueId: comm1
h323Identityh323-ID: MeetingRoom1
h323IdentitydialedDigits: 626262
h235IdentityEndpointID: meetingroom1
h235IdentityPassword: mypassword
SIPIdentityUserName: meetingroom1
SIPIdentityPassword: mypassword
SIPIdentitySIPURI: sip:MeetingRoom@domain.com
```

2. 次の形式の `slapadd` を使用して、この ldif ファイルをサーバに追加します。

```
slapadd -l <ldif_file>
```

上記の例では、`MeetingRoom1` の H.323 ID エイリアス、`626262` の E.164 エイリアス、および `MeetingRoom@domain.com` の SIP URI を持つ単一のエンドポイントを追加します。また、エントリには認証時に使用された、ID が `meetingroom1`、パスワードが `mypassword` の H.235 および SIP クレデンシャルも存在します。

H.323 の登録では、H.323 と H.235 の属性を検索し、SIP は SIP の属性を検索します。したがって、エンドポイントを 1 つのプロトコルだけで登録する場合は、もう一方のプロトコルに関連するエレメントを組み込む必要はありません。

エイリアスが LDAP データベース内にない場合の動作の詳細については、「LDAP を使用したデバイスの認証」の項の登録用エイリアスのソースを参照してください。

TLS での保護

LDAP サーバへの接続は、Transport Level Security（TLS）を接続上で有効にすることによって暗号化できます。これを行うには、Expressway がサーバの ID を検証できるように LDAP サー

バのX.509証明書を作成する必要があります。証明書を作成した後は、証明書に関連付けられた次の3つのファイルをLDAPサーバにインストールする必要があります。

- LDAPサーバの証明書
- LDAPサーバの秘密キー
- LDAPサーバの証明書の署名に使用された認証局（CA）の証明書

3つのファイルはすべてPEMファイル形式である必要があります。

LDAPサーバは、証明書を使用するように設定する必要があります。次の手順を実行します。

- /etc/openldap/slapd.confを編集し、次の3つの行を追加します。

```
TLSCACertificateFile <path to CA certificate>
TLSCertificateFile <path to LDAP server certificate>
TLSCertificateKeyFile <path to LDAP private key>
```

TLS設定を有効にするには、OpenLDAPデーモン（`slapd`）を再起動する必要があります。

LDAPサーバへの接続上でTLSを使用するようにExpresswayを設定するには、CAの証明書を信頼できるCA証明書としてアップロードする必要があります。これを行うには、Expresswayで**[メンテナンス（Maintenance）]** > **[セキュリティ（Security）]** > **[信頼できるCA証明書（Trusted CA certificate）]**に移動します。

コラボレーションソリューションアナライザツールの使用

コラボレーション ソリューション アナライザは、Cisco Technical Assistance Center（TAC）が導入の検証（およびログファイル解析）を支援するために作成したものです。たとえば、ビジネス ツー ビジネス コール テスターを使用して、コールの検証とテストを行うことができます。これには、Microsoft インターワーキングコールが含まれます。

コラボレーション ソリューション アナライザを使用するには、カスタマー アカウントまたはパートナー アカウントが必要です。

スタート ガイド

1. ログ分析ツールを使用する予定の場合は、最初に、お使いのExpresswayのログを収集します。
2. https://cway.cisco.com/tools/CollaborationSolutionsAnalyzer/にログインします

   X12.6からは、**[診断ロギング（Diagnostic logging）]**ページの**[ログの分析（Analyze log）]**ボタン（**[メンテナンス（Maintenance）]** > **[診断（Diagnostics）]**）を使用し、コラボレーションソリューションアナライザのトラブルシューティングツールへのリンクを開けます。
3. 使用するツールをクリックします。たとえば、ログを使用するには、次のようにします。

1. [ログ分析（Log analysis）] をクリックします。
2. ログファイルをアップロードします。
3. 分析するファイルを選択します。
4. **[分析の実行（Run Analysis）]** をクリックします。

   ツールはログファイルを分析し、生のログよりも理解しやすい形式で情報を表示します。たとえば、ラダー図を生成して SIP コールを表示することができます。

デフォルトの SSH キーの変更

デフォルトキーを使用すると、Expressway に対して確立された SSH セッションが「「中間者」」攻撃に対して脆弱になる可能性があります。そのため、Expressway に一意の新しい SSH キーを生成することを推奨します。

Expressway が工場出荷時のデフォルトの SSH キーで設定されているままである場合は、「「セキュリティアラート：SSH サービスはデフォルトキーを使用しています（Security alert: the SSH service is using the default key）」」というアラームメッセージが表示されます。

Expressway に新しい SSH キーを生成するには、次の手順を実行します。

1. CLI に *root* としてログインします。
2. `regeneratesshkey` と入力します。
3. `exit` と入力して root アカウントからログアウトします。
4. Web インターフェイスにログインします。
5. **[メンテナンス（Maintenance）]** > **[再起動（Restart）]** に移動します。「**再起動（Restart）**」ページが表示されます。
6. 現在実行されているコールと登録の数を確認します。
7. **[システムの再起動（Restart system）]** をクリックし、求められたら再起動を確認します。

クラスタ化された Expressway システムがある場合は、クラスタ ピアそれぞれに新しい SSH キーを生成する必要があります。各ピアに順番にログインし、上記の手順に従います。クラスタ化を解除したり、複製を無効にしたりする必要はありません。

SSH を使用して Expressway へ次回ログインする際に、Expressway のキー ID が変更されたという警告を受け取る場合があります。この警告を抑制するには、SSH クライアントに適したプロセスに従ってください。

その後で Expressway が以前のバージョンの Expressway ファームウェアにダウングレードされた場合は、デフォルトの SSH キーが復元されます。

デフォルト設定の復元（初期設定へのリセット）

まれに、システムで「「factory-reset」」スクリプトを実行する必要が生じる場合があります。これは、ソフトウェアイメージを再インストールし、設定をデフォルトの最小機能にリセットするものです。

はじめる前に

システムの最初のセットアップ以降に、アップグレードした場合、リセットにより、最新のソフトウェア バージョンが再インストールされます。

工場出荷時のリセット手順は、重大な障害が発生した後のシステム リカバリを目的としています。**物理ストレージから情報を消去するためのセキュリティ メカニズムとしては設計されていません。**リセットを使用して、システムを「「クリーン」」または「「空白」」の安全な状態に戻すことはしないようにしてください。リセットは、システムを最小の設定状態に戻すことだけを目的としています。

システムは、リセットによってインストールされたソフトウェア バージョンに現在適用されるデフォルト設定値を使用します。これは特にシステムが古いバージョンからアップグレードされている場合など、以前に設定された値と異なる可能性があります。特に、これは多重化されたメディア ポートなどのポート設定に影響する場合があります。デフォルトの設定を復元した後は、必要に応じて、これらのポート設定を、ファイアウォールが想定しているものと一致するポート設定にリセットしてください（次に、必要に応じてオプション キー、SSHキーとFIPS140モードのようないくつかの設定値を保持することは可能ですが、これらの値をすべてリセットすることをお勧めします）。

前提条件

- このプロセスを完了するには仮想マシン コンソールが必要になるため、**VM コンソールを開くための適切な VMware アクセスが必要**です。
- 以下で説明する手順は、正常にインストールされた最新のソフトウェア イメージに基づいてシステムを再構築します。再インストールには、**/mnt/harddisk/factory-reset/** システム フォルダに格納されている次の 2 つのファイルが使用されます。これらのファイルがシステムに存在しない場合があります（最も一般的にはアップグレードされていない新規 VM のインストールの場合）。その場合、ルートとして SCP を使用して、ファイルを配置する必要があります。
  - 16 文字のリリース キーが含まれた、*rk* という名前のテキスト ファイル
  - .tar および .gz 形式のソフトウェア イメージが含まれた、*tandberg-image.tar.gz* という名前のファイル。ダウンロードしたバージョン固有の tar ファイルの名前を *tandgz-image.tar.gz* に手動で変更する必要があります。

デフォルト設定へのリセット プロセス

この手順はコンソールから実行する必要があります（または、ハードウェアベースの CE アプライアンスの場合は、オプションでキーボードとモニターを使用してアプライアンスへの直接接続を使用できます）。ネットワーク設定が書き換えられるため、すべてのコールとリセットを開始するために使用した SSH セッションが切断され、手順によって生成される出力を確認できなくなります。

このプロセスには約 20 分かかります。

1. **root** としてシステムにログインします。
2. `factory-reset` と入力します。
3. 必要に応じて質問に回答します。以下の推奨される応答を入力すると、システムが完全にリセットされ、工場出荷時のデフォルト状態に戻ります。

プロンプト	推奨される応答
オプション キーを保持しますか [はい/いいえ] ?（Keep option keys [YES/NO]?）	NO
FIPS140 設定を保持しますか [はい/いいえ] ?（Keep FIPS140 configuration [YES/NO]?）	NO
IP 構成を保持しますか [はい/いいえ] ?（Keep IP configuration [YES/NO]?）	NO
ssh キーを保持しますか [はい/いいえ] ?（Keep ssh keys [YES/NO]?）	NO
サーバ証明書、関連するキー、および CA 信頼ストアを保持しますか [はい/いいえ]（Keep server certificate, associated key and CA trust store [YES/NO]?） このオプションでは SNI/ドメイン証明書は保持されません。どのように応答するかにかかわらず、これらの証明書は常に削除されます。（[はい（Yes）] と応答した場合）サーバ証明書とそれに関連付けられているキーと CA 信頼ストアのみが保存されます。	NO
root パスワードおよび管理者パスワードを保持しますか [はい/いいえ] ?（Keep root and admin passwords [YES/NO]?）	NO
ログ ファイルを保存しますか [はい/いいえ] ?（Save log files [YES/NO]?）	NO

4. 操作を続行することを確定します。
5. VM 起動後に、インストール ウィザードが表示されます。VM コンソールを使用してウィザードを完了する必要があります。ステップ 3 での応答に応じてウィザードの質問の一部はスキップされますが、IP 設定とパスワードを維持しているとしても、VM コンソールを使用してインストール ウィザードを完了する必要があります。

（注） 使用していた FIPS140 を再び有効にする場合は、FIPS140-2 暗号化モードの設定このガイドの項を参照してください。

USB スティクによるリセット - CE ハードウェアアプライアンス

このセクションは、VM ベースの仮想化 Expressway には適用されません。

Cisco TAC は、代替リセット方法を提案して、ソフトウェアイメージを USB スタックにダウンロードしてから、USB 接続された状態でシステムを再起動します。

この方式を使用した場合は、USB スティックの使用後の消去と再構築が必要です。あるシステムをリセットしてから USB スティックを抜き取り、それを別のシステムに再使用しないでください。

（注） リセット機能は、内部リカバリパーティション（IRP）を通じて CE ハードウェアアプライアンスに組み込まれています。詳細については、インストールおよびアップグレードガイドページの『*CEnnnn* アプライアンス のインストールおよびアップグレード ガイド』を参照してください。

パターン マッチングの変数

Expressway では、許可リストと拒否リストについて、検索ルールやゾーン変換を構成する際に、多数の機能でパターンマッチングが利用されます。

これらのパターン マッチのそれぞれで、Expressway ではパターンをチェックする前に現在の設定値で置換する変数を使用できます。

これらの変数は、次のいずれかまたは両方として使用できます。

- 検索するパターンのすべてまたは一部
- 検出されたパターンを置換する文字列のすべてまたは一部

変数は、すべてのタイプのパターン（プレフィックス、サフィックス、正規表現、および完全一致）で使用できます。

次の表に、変数として有効な文字列と、それらが表現する値を示します。

文字列	返される値の表現	パターンフィールドでの使用時	置換フィールドでの使用時
%ip%	xConfiguration Ethernet 1 IP V4 Address xConfiguration Ethernet 1 IP V6 Address xConfiguration Ethernet 2 IP V4 Address xConfiguration Ethernet 2 IP V6 Address	すべての IPv4 アドレスと IPv6 アドレスに一致しています。 Expressway がクラスタの一部である場合にすべてのピアアドレスに適用されます。	該当なし
%ipv4%	xConfiguration Ethernet 1 IP V4 Address xConfiguration Ethernet 2 IP V4 Address	LAN 1 および LAN 2 に現在設定されている IPv4 アドレスに一致しています。 Expressway がクラスタの一部である場合にすべてのピアアドレスに適用されます。	該当なし
%ipv4_1%	xConfiguration Ethernet 1 IP V4 Address	LAN 1 に現在設定されている IPv4 アドレスに一致しています。 Expressway がクラスタの一部である場合にすべてのピアアドレスに適用されます。	LAN 1 IPv4 アドレスで文字列を置き換えます。 Expressway がクラスタの一部である場合は、ローカル ピアのアドレスが常に使用されます。
%ipv4_2%	xConfiguration Ethernet 2 IP V4 Address	LAN 2 に現在設定されている IPv4 アドレスに一致しています。 Expressway がクラスタの一部である場合にすべてのピアアドレスに適用されます。	LAN 2 IPv4 アドレスで文字列を置き換えます。 Expressway がクラスタの一部である場合は、ローカル ピアのアドレスが常に使用されます。

文字列	返される値の表現	パターンフィールドでの使用時	置換フィールドでの使用時
%ipv6%	xConfiguration Ethernet 1 IP V6 Address xConfiguration Ethernet 2 IP V6 Address	LAN 1 および LAN 2 に現在設定されている IPv6 アドレスに一致しています。 Expressway がクラスタの一部である場合にすべてのピアアドレスに適用されます。	該当なし
%ipv6_1%	xConfiguration Ethernet 1 IP V6 Address	LAN 1 に現在設定されている IPv6 アドレスに一致しています。 Expressway がクラスタの一部である場合にすべてのピアアドレスに適用されます。	LAN 1 IPv6 アドレスで文字列を置き換えます。 Expressway がクラスタの一部である場合は、ローカルピアのアドレスが常に使用されます。
%ipv6_2%	xConfiguration Ethernet 2 IP V6 Address	LAN 2 に現在設定されている IPv6 アドレスに一致しています。 Expressway がクラスタの一部である場合にすべてのピアアドレスに適用されます。	LAN 2 IPv6 アドレスで文字列を置き換えます。 Expressway がクラスタの一部である場合は、ローカルピアのアドレスが常に使用されます。
%systemname%	xConfiguration SystemUnit Name	Expressway のシステム名に一致しています。	Expressway のシステム名で文字列を置き換えます。

パターンが特定の名前に一致するかどうか、および予想どおりに変換されているかどうかは、パターンの効果の確認 ツール（**[メンテナンス（Maintenance）] > [ツール（Tools）] > [パターンの確認（Check pattern）]**）を使用してテストできます。

ポート リファレンス

Cisco Expressway シリーズ設定ガイドのページに用意されている、ご使用のバージョンに対応する『*Cisco Expressway IP Port Usage Configuration Guide*』を参照してください。

正規表現

正規表現は、エイリアストランスフォーメーション、ゾーントランスフォーメーション、CPL ポリシー、ENUM など、数多くの Expressway 機能と組み合わせて使用できます。Expressway は POSIX 形式の正規表現構文を使用します。次の表に、正規表現構文で一般的に使用される特殊文字を示します。これは、使用可能なすべての表現のサブセットでしかありません。正規表現構文の詳細については、『*Regular Expression Pocket Reference*』という資料を参照してください。

文字	説明	例
.	任意の単一文字と一致します。	
\d	任意の 10 進数（0 ～ 9）と一致します。	
*	直前の文字または式の 0 回以上の繰り返しと一致します。	.* は、文字のシーケンスと一致します。
+	直前の文字または式の 1 回以上の繰り返しと一致します。	
?	直前の文字または式の 0 回または 1 回以上の繰り返しと一致します。	`9?123` は、9123 および 123 と一致します。
{n}	直前の文字または式の n 回の繰り返しと一致します。	`\d{3}` は 3 桁の数字と一致します。
{n,m}	直前の文字または式の n ～ m 回の繰り返しと一致します。	`\d{3,5}` は、3 桁、4 桁、5 桁の数字と一致します。
[...]	一連の指定した文字と一致します。セット内の各文字を個別に指定するか、または、範囲内の最初の文字、その後に - 文字、その後に範囲内の最後の文字を入力して、範囲を指定することができます。 [] 内では特殊文字を使用できません。特殊文字はそのままの文字として扱われます。	`[a-z]` は英字と一致します。 `[0-9#*]` は単一の E.164 文字と一致します。E.164 文字のセットは、0 ～ 9 の数字とハッシュキー（#）およびアスタリスクキー（*）から構成されます。

文字	説明	例
[^...]	指定した文字のセットを除くすべてと一致します。セット内の各文字を個別に指定するか、または、範囲内の最初の文字、その後に - 文字、その後に範囲内の最後の文字を入力して、範囲を指定することができます。 [] 内では特殊文字を使用できません。特殊文字はそのままの文字として扱われます。	`[^a-z]` は英字以外の文字と一致します。 `[^0-9#*]` は 0 ～ 9 の数字、ハッシュ キー（#）、およびアスタリスク キー（*）以外と一致します。
(...)	一連の一致文字をまとめてグループ化します。グループは、置換文字列の一部として、文字列 \1、\2 などを使用して順番に参照できます。	ユーザのフルネームが含まれている URI をイニシャルに基づいた URI に変換するように正規表現を組み立てることができます。正規表現 `(.).*_(.).*(@example.com)` はユーザの `john_smith@example.com` と照合し、置換文字列 `\1\2\3` を使用して `js@example.com` に変換します。
|	1つの表現または代替表現に一致します。	`.*@example.(net|com)` はドメイン `example.com` またはドメイン `example.net` の URI と一致します。
\	正規表現の特殊文字をエスケープします。	
^	行の先頭を示します。 開き大カッコの直後に使用されると、大カッコ内の文字セットは否定されます。	`[^abc]` は、a、b、c、のいずれでもない任意の単一文字と一致します。
$	行の末尾を意味します。	`^\d\d\d$` は正確に 3 桁の文字列と一致します。

文字	説明	例
(?!...)	否定先読み。存在すべきでない副次式を定義します。	`(?!.*@example.com$).*` は `@example.com` で終了しない文字列と一致します。 `(?!alice).*` は `alice` で開始されない文字列と一致します。
(?<!...)	否定後読み。存在すべきでない副次式を定義します。	`.*(?<!net)` は `net` で終了しない文字列と一致します。

正規表現の比較は大文字と小文字を区別しません。

正規表現の使用例については、CPL の例の項を参照してください。

サポートされる文字

Expressway は CLI や Web インターフェイスにテキストが入力されると、次の文字をサポートします。

- A ～ Z および a ～ z の文字
- 10 進数（0 ～ 9）
- アンダースコア (_)
- マイナス記号/ハイフン（-）
- 等号（=）
- プラス記号 (+)
- アットマーク（@）
- カンマ（,）
- ピリオド/終止符（. ）
- 感嘆符（! ）
- スペース

次の文字は特に許可されていません。

- タブ
- 山カッコ（< と >）
- アンパサンド（&）
- キャレット (^)

特定のテキストフィールド（管理者グループの設定グループを含む）には異なる制限事項があります。これらについては、本ガイドの関連する項に示します。

大文字と小文字の区別

CLIやWebインターフェイスを使用して入力するテキスト項目は大文字と小文字が区別されません。例外として、パスワードとローカル管理者名は大文字と小文字が区別されます。

製品 ID と対応するキー

Cisco PID（製品識別子）は、製品名、モデル名、または製品番号とも呼ばれる場合があります。次に、ソフトウェアバージョンに応じて Expressway に適用できる PID の例を示します。多くは、後のソフトウェアバージョンで段階的に廃止されています。たとえば、リリースキーは Cisco Expressway 製品の X12.5.4 から使用されなくなりました。

機能、ライセンスオプション	製品ID（PID）	キー パターン	適用対象	目的
リリース キー	LIC-SW-VMVCS-K9	16 桁の数	VCS 制御 VCS Expressway	システムを有効にする。キーはソフトウェアのシリアル番号と特定の基本バージョンに固有です。ほとんどの機能は、このキーなしでは無期限には機能しません。
リリース キー	LIC-SW-EXP-K9	16 桁の数	Expressway-C Expressway-E	システムを有効にする。キーはソフトウェアのシリアル番号と特定の基本バージョンに固有です。ほとんどの機能は、このキーなしでは無期限には機能しません。
Expressway シリーズ	LIC-EXP-SERIES	116341E00-m-########	Expressway-C Expressway-E	Expressway シリーズのシステムを有効にします（Cisco Webex ハイブリッドサービスを除く）

機能、ライセンス オプション	製品ID（PID）	キー パターン	適用対象	目的
リッチ メディア セッション ライセンス	LIC-EXP-RMS	116341Yn-m-########	Expressway-C Expressway-E	

機能、ライセンス オプション	製品ID（PID）	キー パターン	適用対象	目的
				Expressway がメディア ストリームを処理する（メディアを「トラバース」または「ハンドル」するとも言われる）必要がある場合に Expressway により有効にされたコール。 RMS ライセンスは次の機能が必要なコールで使用されます。 • IPv4-IPv6 インターワーキング • H.323-SIP インターワーキング • 別のエンティティに代わるメディアの暗号化 • Microsoft SIP から標準ベースの SIP へのインターワーキング （注） 両方のエンドポイントがシスコインフラストラクチャの実効

機能、ライセンスオプション	製品ID（PID）	キー パターン	適用対象	目的
				的なライセンスに登録されている場合は、必須ではありません。 RMS ライセンスは CMR クラウドのコールでは使用されません

機能、ライセンス オプション	製品ID（PID）	キー パターン	適用対象	目的
トラバーサル コール ライセンス	シラミ-VCSE-n	116341Wn-m########	VCS 制御 VCS Expressway	VCS がメディア ストリームを処理する（メディアを「トラバース」または「ハンドル」するとも言われる）必要がある場合に VCS により有効にされたコール。 トラバーサル コール ライセンスは次の機能が必要なコールで使用されます。 • IPv4-IPv6 インターワーキング • H.323-SIP インターワーキング • 別のエンティティに代わるメディアの暗号化 • Microsoft SIP から標準ベースの SIP へのインターワーキング トラバーサル コール ライセンスは CMR クラウドのコールでは使用されません

機能、ライセンス オプション	製品ID（PID）	キー パターン	適用対象	目的
非トラバーサル コール ライセンス	シラミ-VCS-n	116341Vn-m-########	VCS 制御 VCS Expressway	メディア トラバーサルを必要としない（シグナリングのみ）VCS により有効にされたコール
登録ライセンス	ライセンス・アンド・ス・アンド・グ	116341Rn-m-########	VCS 制御 VCS Expressway	VCS への発信者の登録
ルーム システムの登録ライセンス	LIC-EXP-ルーム	116341An-m-########	Expressway-C Expressway-E	Expressway-C への TelePresence ルーム登録
デスクトップ システム ライセンス登録	リック・エップ・ド・スク	116341Bn-m-########	Expressway-C Expressway-E	Expressway-C へのデスクトップ エンドポイント登録
TURN リレー ライセンスが必要です（TURN relay licenses）	LIC-EXP-TURN	116341In-m-########	VCS Expressway Expressway-E	Jabber Guest、Microsoft 相互運用性（オフサイト MS クライアント）
トラバーサル サーバ機能 （X12.6 以降では使用されません）	LIC-EXP-E	116341T00-m-########	VCS Expressway Expressway-E	ファイアウォール トラバーサル：MRA、B2B、CMR クラウド、CMR Hybrid、プロキシ登録、Jabber Guest、MS 相互運用性（オフサイト MS クライアント）
FindMe 機能	LIC-VCS-FINDME	116341U00-m-########	VCS 制御 Expressway-C	Cisco TMS で管理する複数のエイリアス。 このキーは明示的に必須ではありませんが、ロードされても動作に影響しません。

機能、ライセンスオプション	製品ID（PID）	キー パターン	適用対象	目的
SIP 機能のインターワーキング H.323	LIC-EXP-GW	116341G00-m-########	VCS 制御 VCS Expressway Expressway-C Expressway-E	このキーは明示的に必須ではありませんが、ロードされても動作に影響しません。
デバイスのプロビジョニング機能	リック・VCS-デヴプロヴ	116341P00-m-########	VCS 制御 Expressway-C	Cisco TMS の設定および電話帳を使用したエンドポイントのプロビジョニング。 このキーは明示的に必須ではありませんが、ロードされても動作に影響しません。
高度なネットワーク機能	LIC-EXP-AN	116341L00-m-########	VCS Expressway Expressway-E	2 つ目の NIC とスタティック NAT の有効化。 このキーは明示的に必須ではありませんが、ロードされても動作に影響しません。
高度なアカウントのセキュリティ機能	LIC-VCS-JITC	116341J00-m-########	VCS 制御 VCS Expressway	FIPS140-2 暗号化モードの有効化（高度にセキュアな環境） 高度なアカウントセキュリティモードの有効化
高度なアカウントのセキュリティ機能	LIC-EXP-JITC=	116341J00-m-########	Expressway-C Expressway-E	FIPS140-2 暗号化モードの有効化（高度にセキュアな環境） 高度なアカウントセキュリティモードの有効化

機能、ライセンス オプション	製品ID（PID）	キー パターン	適用対象	目的
Microsoft 相互運用性（Microsoft interoperability）	LIC-EXP-MSFT	116341C00-m########	VCS 制御 Expressway-C	次を含む Expressway と Microsoft インフラストラクチャ間のすべての統合：A/V コールのインターワーキング、Microsoft クライアントからのデスクトップ共有、チャットおよびプレゼンス フェデレーションと IM&P。

n - このキーで提供されるライセンス数。この位置に 00 が含まれる場合、キーは複数のライセンス用ではなく 1 つの機能用であることを意味します。

m - キー、通常1.のインデックス。

~ #十六進数。

許可リストは、ファイルの参照を決定します

CSVファイルを使用してルールを定義できます。この項では、各ルールの引数に許容されるデータへの参照を提供し、CSV 形式のルールを示します。

表 *26 :* リストルールの引数を許可する

引数インデックス	パラメータ名	必須/任意	サンプル値
0	Url	必須	protocol://host[:port][/path] それぞれの説明は次のとおりです。 • protocol は http または https です。 • host には DNS 名または IP アドレスを指定できます。 • :port はオプションです。：の後に 0 ～ 65535 の範囲の 1 つの数値のみが続きます（例：:8443 ポートが指定されて、Expresswayはプロビジョニングされたプロトコルのデフォルトポートを使用します（80または443） • /path はオプションです。HTTP 仕様に準拠する必要があります。
1	導入	任意	このルールを使用する導入の名前。複数の導入がある場合は必須です。それ以外の場合は空白の引数を入力します。

引数インデックス	パラメータ名	必須/任意	サンプル値
2	HttpMethods	任意	HTTP メソッドのカンマ区切りリスト。必要に応じて二重引用符で囲います。 例：`"GET,PUT"`
3	MatchType	任意	`exact` または `prefix`。 デフォルト：`prefix`
4	説明	任意	ルールの説明。スペースを含む場合は二重引用符で囲みます。

CSV ファイルの例

```
Url,Deployment,HttpMethods,MatchType,Description
https://myServer1:8443/myPath1,myDomain1,GET,,"First Rule"
http://myServer2:8000/myPath2,myDomain200,"GET,PUT",exact,
https://myServer3:8080/myPath3,myDomain1,,prefix,"Third Rule"
https://myServer4/myPath4,myDomain1,,prefix,"Fourth Rule"
http://myServer5/myPath5,myDomain1,,prefix,"Fifth Rule"
```

- ファイルの最初の行にパラメータ名（記載のとおり）をリストします
- 1 行ごとに 1 つのルール、ルールごとに 1 行
- カンマで引数を区切ります
- 上記の表に示すように、ルール値は正しい順序にします
- スペースを含む値は二重引用符で囲みます

許可リスト テスト ファイル リファレンス

CSV ファイルを使用してテストを定義できます。この項では、各テストの引数に許容されるデータへの参照を提供し、CSV 形式のテストを示します。

表 *27:* リストテスト引数の許可

引数インデックス	パラメータ名	必須/任意	サンプル値
0	Url	必須	`protocol://host[:port][/path]` それぞれの説明は次のとおりです。 • protocol は `http` または `https` です。 • host には DNS 名または IP アドレスを指定できます。 • :port はオプションです。：の後に 0 ～ 65535 の範囲の 1 つの数値のみが続きます。 • /path はオプションです。HTTP 仕様に準拠する必要があります。
1	ExpectedResult	必須	`allow` または `block`。テストで、指定した URL をルールによって許可またはブロックする必要があると前提するかどうかを指定します。
2	導入	任意	この URL を使用してテストする導入の名前。この引数を省略すると、テストはデフォルトの導入を使用します。
3	説明	任意	ルールの説明。スペースを含む場合は二重引用符で囲みます。

引数インデックス	パラメータ名	必須/任意	サンプル値
4	HttpMethod	任意	テストする HTTP メソッドを 1 つ指定します。例：PUT 指定しない場合、デフォルトで GET に設定されます。

CSV ファイルの例

```
Url,ExpectedResult,Deployment,Description,HttpMethod
https://myServer1:8443/myPath1,block,"my deployment","a block test",GET
http://myServer2:8000/myPath2,allow,"my deployment","an allow test",PUT
https://myServer4/myPath4,allow,,,GET
http://myServer4/myPath4,block,,,POST
```

- 最初の行にパラメータ名（記載のとおり）をリストします
- 1 行ごとに 1 つのテスト、テストごとに 1 行
- カンマで引数を区切ります
- 上記の表に示すように、テスト値は正しい順序にします
- スペースを含む値は二重引用符で囲みます

Expressway マルチテナンシーの概要

Expressway の製品ラインは、Cisco Hosted Collaboration Solution で次のようなさまざまなエッジアクセス機能を提供するために使用されます。

- Mobile & Remote Access（MRA）を使用すると、Cisco Jabber などのエンドポイントは、エンタープライズ ネットワーク外のエンドポイントに対して Cisco Unified Communications Manager によって提供される登録、コール制御、プロビジョニング、メッセージング、プレゼンス サービスを設定することができます。Expressway は、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。
- ビジネス ツー ビジネス（B2B）によって、インターネット経由で到達可能な Cisco Hosted Collaboration Solution を利用しない企業との間でダイヤルできるセキュアな接続オプションが可能になります。
- Cisco Webex ハイブリッド サービスは、オンプレミスの機器と Cisco Collaboration Cloud を関連付けて統合された Cisco Webex エクスペリエンスを実現します。

これらのサービスを導入するには、Cisco Expressway-E クラスタと Expressway-C クラスタを顧客ごとに設定および管理する必要があります。小規模のお客様の場合は、これが非効率的なリソースの使用や管理上の負担の増大の原因になる可能性があります。

このオーバーヘッドを軽減するために、マルチテナント構成を導入することができます。これにより、パートナーは最大 50 の顧客間で Expressway-E クラスタを共有しながら、専用の Expressway-C クラスタを顧客ごとに展開できます。

この専用 Expressway-C クラスタは、MRA、B2B、およびハイブリッドの 3 つのサービスすべてに使用できます。この設定は、顧客あたり最大約 500 のユーザがいる小規模な顧客をサポートすることを目的としています。

大規模なお客様の場合は、シングルテナント（専用の）Expressway-E クラスタを使用して、顧客の規模とパフォーマンスの要件を満たすことを推奨します。

マルチテナント Expressway の制限

マルチテナント Expressway には、標準の Expressway 製品に関連していくつかの制限があります。次の機能は、マルチテナント モードでサポートされません。

- Jabber Guest
- 以下を含むさまざまなモードにおける H323
  - H323/SIP インターワーキング
  - ビジネス ツー ビジネス H323
  - H323 ゲートキーパー
- Lync の相互運用
- Skype for Business の相互運用
- IPv6
- Cisco Meeting Server（CMS）

詳細情報

マルチテナント機能の詳細については、「Cisco Hosted Collaboration Solution ドキュメント」ページに用意されている次のドキュメントを参照してください。

- Cisco Hosted Collaboration Solution Reference Network Design Guide
- Cisco Hosted Collaboration Customer Onboarding Guide
- Cisco Hosted Collaboration Solution Capacity Planning Guide
- Cisco Hosted Collaboration Solution Troubleshooting Guide

マルチテナント Expressway のサイジング

以前の Expressway リリースでは、Expressway-E および Expressway-C クラスタ展開は、一致するクラスタと OVA のサイズに制限されていました。Expressway-E クラスタ内のノード数は、Expressway-C クラスタ内のノード数と一致する必要があります。各ノードは、両方のクラスタで同じ OVA サイズでなければなりません。

マルチテナント展開オプションを使用すると、その制限が緩和されます。推奨される展開は、共有の 6 ノード大規模 OVA Expressway-E クラスタと、顧客ごとに専用の 2 ノード中規模 OVA Expressway-C クラスタです。

2 ノード中規模 OVA クラスタが提供する容量を超える容量が必要な顧客の場合は、要件を満たす専用の Expressway-E クラスタを導入することをお勧めします。

全体的なサイジングの推奨事項については、『*Cisco Hosted Collaboration Solution* 参照 ネットワーク 設計ガイド』の「コラボレーション ソリューション サイジング ガイダンス」の章を参照してください。特に、この章の「Expressway」の項では、Expressway クラスタのサイジングと容量について説明しています。

マルチテナント展開では、Expressway-E の容量はすべての顧客で共有されますが、Expressway-C クラスタの容量はその顧客専用です。次の表に、顧客ごとの推奨容量を示します。ビデオおよびオーディオのみのコールの数値は、いずれかのコールタイプのものであることに注意してください。両方ではありません。

共有 Expressway-E クラスタのサイジング

クラスタ サイズ	プロキシ実施済みMRA登録	ビデオ コール	音声専用コール
6 ノード、大規模 OVA N+2 の配置であるため、容量は 4 ノード用であり、2 ノードで障害が発生しても容量の損失はありません。	10,000	2,000	4,000
顧客ごとの最大（50 の顧客に対し）	200	40	80

専用の Expressway-C クラスタのサイジング

クラスタ サイズ	プロキシ実施済みMRA登録	ビデオ コール	音声専用コール
2 ノード、中規模 OVA N+1 の配置であるため、容量は単一ノードであり、1 ノードで障害が発生しても容量の損失はありません。	2,500	100	200

上記の表では、ビデオ通話と音声のみの通話は、MRA コール、B2B コール、およびハイブリッド コールの合計を占めています。共有の Expressway-E クラスタごとに推奨される最大顧客数 50 において、顧客あたりの平均同時 MRA 登録の最大数は 200 であり、Expressway-C クラスタの容量をはるかに下回ります。

同様に、顧客あたりの平均同時ビデオ通話の最大数は 40 であり、これもまた Expressway-C クラスタの容量を下回ります。Expressway-C クラスタのこの空き容量は、プロキシされた登録またはコール キャパシティに影響を与えることなく、共存するハイブリッド コネクタによって使用されます。

Expressway-E を共有している顧客の規模を計画する際に考慮すべき 2 つの使用例があります。これらの両方の使用例では、Expressway-E クラスタが制限要因です。Expressway-C には多くの容量があります。

使用例 1

ほとんどの顧客は、社内接続に MPLS を使用しており、自宅やモバイルでは MRA のみを使用しています。この場合、常にごく一部のユーザ（10-20%）しか MRA に登録されていません。1 顧客あたりの最大ユーザ数は約 500 です。

使用例 2

ほとんどの顧客は MPLS を使用しておらず、すべての接続に MRA を使用しています。この場合、100% のユーザが MRA に登録されています。1 顧客あたりの最大ユーザ数は 200 を超えてはいけません。

次の表に、これらの展開オプションを要約します。

表 *28 :* 導入シナリオ

使用例	顧客あたりの平均最大ユーザ数	一度に MRA 経由で登録できるユーザのパーセンテージ	注記
1	500	40%	ほとんどの顧客が社内接続に MPLS を使用している場合に、これを使用します。

使用例	顧客あたりの平均最大ユーザ数	一度に MRA 経由で登録できるユーザのパーセンテージ	注記
2	200	100 %	ほとんどの顧客が社内接続に MRA を使用している場合に、これを使用します。

Cisco Hosted Collaboration Solution ページの『マルチテナントおよび *Cisco Expressway*』を参照してください。

アラーム参照

以下の表に、Expressway で発生する可能性のあるアラームのリストを示します。

- 表 29 : ハードウェア アラーム
- 表 30 : ソフトウェアアラーム
- 表 31 : クラスタアラーム
- 表 32 : ネットワークアラーム
- 表 33 : ライセンスアラーム
- 表 34 : 外部アプリケーション/サービスアラーム
- 表 35 : セキュリティアラーム
- 表 36 : 設定ミスアラーム
- 表 37 : バックツーバックユーザエージェントアラーム
- 表 38 : 管理コネクタアラーム
- 表 39 : カレンダーコネクタ アラーム
- 表 40 : コールコネクタアラーム
- 表 41 : 重要なイベントアラーム
- 表 42 : テレメトリーアラーム

表 *29 :* ハードウェア アラーム

ID	タイトル	説明	ソリューション	重大度
10001	ハードウェア障害（Hardware failure）	ハードウェアで次の問題が発生したときに生成されます。 • しきい値を下回るファン速度。 • しきい値を上回るシステム温度。 • しきい値を下回るシステム入力電圧。 • しきい値を上回るシステム入力電圧。	Cisco RMA プロセスに従って交換部品を入手します。サーバ コンポーネントを交換する方法については、「Cisco UCS C220 M4 ラック サーバ」ページの『*Cisco UCS C220 M4* サーバーのインストール および サービス ガイド』を参照してください。	クリティカル
10002	RAID の劣化（RAID degraded）	<problem description>	Cisco RMA プロセスに従って交換部品を入手します。サーバ コンポーネントを交換する方法については、「Cisco UCS C220 M4 ラック サーバ」ページの『*Cisco UCS C220 M4* サーバーのインストール および サービス ガイド』を参照してください。	クリティカル

ID	タイトル	説明	ソリューション	重大度
10003	PSUの冗長性の損失（PSU redundancy lost）	<problem description>	Cisco RMAプロセスに従って交換部品を入手します。サーバ コンポーネントを交換する方法については、「Cisco UCS C220 M4 ラック サーバ」ページの『*Cisco UCS C220 M4* サーバーのインストール および サービス ガイド』を参照してください。	クリティカル
10004	RAIDの再構築（RAID rebuilding）	<problem description>	再構築が完了するまで待ちます。正常に完了すると、すべてのRAID関連のアラームが自動的に引き下げられます。	クリティカル
10005	不適切なハードウェアの警告	現在のハードウェアが、このバージョンのExpressway でサポートされているVMの設定要件を満たしていません。	サポートされるハードウェアバージョンへのアップグレードについては、シスコの担当者にお問い合わせください。サポートされるバージョンについては、「Expressway インストール ガイド」ページの「*Cisco Expressway on Virtual Machine Installation Guide*」を参照 してください。	警告

表 *30 :* ソフトウェアアラーム

ID	タイトル	説明	ソリューション	重大度
15004	アプリケーションに障害が発生しました（Application failed）	予期しないソフトウェア エラーが <module> で検出されました（An unexpected software error was detected in <module>）	インシデント レポートの表示 ページを表示します。	エラー
15005	データベースの障害（Database Failure）	データベースを削除し、バックアップから復元した後でシステムをリブートしてください（Please remove database and restore from backup, then reboot the system）	システムを再起動します	警告
15006	再起動が必要です（Restart required）	言語パックがインストールされましたが、これを有効にするにはリスタートが必要です	システムを再起動します。	警告
15007	システムがビジー（The system is busy）	システムがシャットダウンするか、起動します（The system is shutting down, or starting）		アラート
15008	データ ベースをロードできませんでした（Failed to restore database）	データ ベースをロードできませんでした。一部の設定データが失われました（The database failed to load; some configuration data has been lost）	システム データをバックアップから復旧します。	警告

ID	タイトル	説明	ソリューション	重大度
15009	初期設定へのリセットが開始されました（Factory reset started）	初期設定へのリセットが開始されました（Factory reset started）		アラート
15010	アプリケーションに障害が発生しました（Application failed）	予期しないソフトウェア エラーが <module> で検出されました（An unexpected software error was detected in <module>）	インシデント レポート ページを表示します。	エラー
15011	アプリケーションに障害が発生しました（Application failed）	予期しないソフトウェア エラーが <module> で検出されました（An unexpected software error was detected in <module>）	インシデント レポート ページを表示します。	エラー
15012	言語パッケージの不一致（Language pack mismatch）	一部のテキスト ラベルが変換できない可能性があります（Some text labels may not be translated）	シスコの担当者に連絡し、最新の言語パックが使用可能かどうかを確認します	警告
15013	初期設定へのリセットに失敗しました（Factory reset failed）	初期設定へのリセットに失敗しました（Factory reset failed）		アラート
15014	再起動が必要です（Restart required）	コアダンプモードが変更されましたが、この変更を有効にするにはリスタートが必要です	システムを再起動します。	警告

ID	タイトル	説明	ソリューション	重大度
15015	メンテナンスモード	Expressway がメンテナンスモードになっており、コールや登録を受け入れなくなりました（The Expressway is in Maintenance mode and will no longer accept calls and registrations）		警告
15016	ディレクトリサービスのデータベース障害（Directory service database failure）	ディレクトリサービスのデータベースが実行していません（The directory service database is not running）	システムを再起動します。	警告
15017	アプリケーションに障害が発生しました（Application failed）	OpenDS サービスが突然停止し、再起動しました（The OpenDS service has stopped unexpectedly and has been restarted）	問題が解決しない場合は、シスコの担当者に連絡してください	警告

ID	タイトル	説明	ソリューション	重大度
15018	ブートの選択の不一致（Boot selection mismatch）	ブートしたシステムが予期していた設定と一致しません。これは、ブート中のシリアルコンソールでのユーザ入力か、誤った文字によって発生した可能性があります（Booted system does not match expected configuration; this may be caused by user input or spurious characters on the serial console during the boot）	システムを再起動します	クリティカル
15019	アプリケーションに障害が発生しました（Application failed）	予期しないソフトウェア エラーが検出されました（An unexpected software error was detected） <details>	システムを再起動します。問題が解決しない場合はシスコのサポート担当者に連絡してください。	クリティカル
15021	Cisco XCP ルータの遅延再起動	Cisco XCP ルータの遅延再起動機能が有効になっているため、Cisco XCP ルータ サービスは現在最新の設定では動作していません。	[Cisco XCP ルータの遅延再起動ページ（Delayed Cisco XCP Router restart）] でルータを再起動するか、またはスケジュールされた時間に再起動するように設定します。	警告
15022	再起動が必要です（Restart required）	ドメイン証明書設定が変更されました。これを有効にするには再起動が必要です。	システムを再起動します。	警告

ID	タイトル	説明	ソリューション	重大度
15023	復元に失敗（Restore failed）	バックアップが復元されませんでした。システムは、以前の設定に復元されます。	エラー ログで詳細を確認して操作を再試行します。問題が解決しない場合は、シスコのサポート担当者に連絡してください。	エラー
15024	暗号化デバイスの障害（Crypto device failure）	設定された暗号デバイスで暗号化/解読化サイクルをテスト中にエラーが検出されました。	HSM 設定 ページで詳細をご確認ください	クリティカル
15025	HSM 登録解除の障害（HSM disenrollment failure）	HSM へのピアの登録解除に失敗しました。	HSM 設定 ページで詳細をご確認ください	エラー
15026	HSM 登録の障害（HSM enrollment failure）	HSM へのピアの登録に失敗しました。	HSM 設定 ページで詳細をご確認ください	エラー（Error）
15027	HSMの障害	HSM の障害には管理者の注意が必要です。	HSM 設定 ページで詳細をご確認ください	クリティカル
15028	再起動が必要です（Restart required）	サーバ証明書と秘密キーが変更されましたが、この変更を適用するには再起動が必要です（Server certificate and private key have been changed, however a restart is required for this to take effect.）	変更を有効にするためにExpresswayを再起動します。	警告

ID	タイトル	説明	ソリューション	重大度
15029	クラッシュレポートの送信に失敗しました	クラッシュレポートをサーバに送信できませんでした。	Expressway とクラッシュレポートサーバ間のネットワーク接続を確認します。クラッシュレポートサーバ証明書の有効期限が切れていないか、無効にされ、CA チェーン内の証明書が信頼ストアで更新されたのを確認します。	
15030	Unified CM データのクロスチェックの失敗（Unified CM data crosscheck failure）	Expressway の Unified CM 構成データは一貫していません。	すべての Unified CM サーバを削除してから、再度追加してください。詳細については、『Cisco Expressway 導入ガイドによるモバイルおよび Remote Access』の「Unified CM サーバの検出」セクションをご覧ください。	エラー（Error）
15031	HSM TLPがインストールされていません	HSM の障害には管理者の注意が必要です。	詳細についてはアップグレードページを参照してください。	エラー（Error）

ID	タイトル	説明	ソリューション	重大度
15022	Unified CMサーバを使用できません	発行者のUnified CM設定に使用できないサーバが含まれています。	詳細については、イベントログを参照してください。問題を解決して更新します。詳細については、『Cisco Expressway 導入ガイドによるモバイルおよび Remote Access』の「Unified CM サーバの検出」セクションをご覧ください。	警告

表 *31* : クラスタアラーム

ID	タイトル	説明	ソリューション	重大度
20020	再起動が必要です（Restart required）	TLS 検証設定がアクティブなステータスと一致しません。	システムを再起動します。	警告
20021	クラスタ通信障害（Cluster communication failure）	<peers> との TCP 接続をポート <ports> で確立できません	ポート リファレンス ガイドを確認します。	警告
20003	無効なクラスタ設定（Invalid cluster configuration）	クラスタ設定が無効です（The cluster configuration is invalid）	「クラスタリング（Clustering）」ページをチェックして、このシステムの IP アドレスが含まれていること、および重複する IP がないことを確認します。	警告

ID	タイトル	説明	ソリューション	重大度
20004	クラスタ通信障害（Cluster communication failure）	システムがクラスタ内のピアの 1 つまたは複数と通信できません（The system is unable to communicate with one or more of the cluster peers）	クラスタリング設定を確認します。	警告
20005	無効なピア アドレス（Invalid peer address）	無効なピア アドレスが 1 つ以上あります（One or more peer addresses are invalid）	「クラスタリング（Clustering）」ページをチェックし、すべての [ピア（Peer）] フィールドに有効な IP アドレスが使用されていることを確認します。	警告
20006	クラスタ データベース通信障害（Cluster database communication failure）	1 つ以上のクラスタ ピアでデータベースを複製できません（The database is unable to replicate with one or more of the cluster peers）	クラスタリング設定を確認し、再起動します。	警告
20007	再起動が必要です（Restart required）	クラスタ設定が変更されました。これを有効にするには再起動が必要です（Cluster configuration has been changed, however a restart is required for this to take effect）	システムを再起動します。	警告

ID	タイトル	説明	ソリューション	重大度
20008	クラスタ複製エラー（Cluster replication error）	アップグレードが進行中のため、設定の自動レプリケーションが一時的に無効にされました（Automatic replication of configuration has been temporarily disabled because an upgrade is in progress）	アップグレードが完了するまで待ちます。	警告
20009	クラスタ複製エラー（Cluster replication error）	設定の自動レプリケーション中にエラーが発生しました（There was an error during automatic replication of configuration）	クラスタ レプリケーションの手順を表示します。	警告
20011	クラスタ複製エラー（Cluster replication error）	このピアの設定がプライマリの設定と競合しています。設定を手動で同期化する必要があります（This peer's configuration conflicts with the primary's configuration, manual synchronization of configuration is required）	クラスタ レプリケーションの手順を表示します。	警告

ID	タイトル	説明	ソリューション	重大度
20012	クラスタ複製エラー（Cluster replication error）	このピアのクラスタ設定がプライマリ設定ピアの設定と一致しません（This peer's cluster configuration settings do not match the configuration primary peer's settings）	このピアのクラスタを設定します	警告
20014	クラスタ複製エラー（Cluster replication error）	プライマリまたはこのピアの設定ファイルが見つかりません。設定を手動で同期化する必要があります（Cannot find primary or this peer's configuration file, manual synchronization of configuration is required）	クラスタ レプリケーションの手順を表示します。	警告
20015	クラスタ複製エラー（Cluster replication error）	ピアのリストにローカル Expressway が表示されません（The local Expressway does not appear in the list of peers）	このクラスタのピアのリストを確認します。	警告
20016	クラスタ複製エラー（Cluster replication error）	プライマリ ピアに到達できません（The primary peer is unreachable）	このクラスタのピアのリストを確認します。	警告

ID	タイトル	説明	ソリューション	重大度
20017	クラスタ複製エラー（Cluster replication error）	プライマリ設定 ID に一貫性がありません。設定を手動で同期する必要があります（Configuration primary ID is inconsistent, manual synchronization of configuration is required）	クラスタ レプリケーションの手順を表示します。	警告
20018	無効なクラスタリング設定（Invalid clustering configuration）	H.323 モードを有効にする必要があります。クラスタリングではピア間に H.323 通信を使用します（H.323 mode must be turned On - clustering uses H.323 communications between peers）	H.323 モードを設定します。	警告
20019	クラスタ名が設定されていません（Cluster name not configured）	FindMe またはクラスタリングを使用している場合は、クラスタ名を定義する必要があります（If FindMe or clustering are in use a cluster name must be defined.）	クラスタ名を設定します。	警告

表 *32 :* ネットワークアラーム

ID	タイトル	説明	ソリューション	重大度
25001	再起動が必要です（Restart required）	ネットワーク設定が変更されました。これを有効にするには再起動が必要です（Network configuration has been changed, however a restart is required for this to take effect）	システムを再起動します。	警告
25002	日時を確認できません（Date and time not validated）	システムは NTP サーバから正確な日時を取得できません（The system is unable to obtain the correct time and date from an NTP server）	時刻設定を確認します。	警告
25003	IP 設定の不一致（IP configuration mismatch）	IP プロトコルは IPv4 と IPv6 の両方に設定されていますが、システムには定義されている IPv4 アドレスがありません（IP protocol is set to both IPv4 and IPv6, but the system does not have any IPv4 addresses defined）	IP 設定を構成します。	警告

ID	タイトル	説明	ソリューション	重大度
25004	IP 設定の不一致（IP configuration mismatch）	IP プロトコルは IPv4 と IPv6 の両方に設定されていますが、システムには定義されている IPv4 ゲートウェイがありません（IP protocol is set to both IPv4 and IPv6, but the system does not have an IPv4 gateway defined）	IP 設定を構成します。	警告
25006	再起動が必要です（Restart required）	高度なネットワークのオプションキーが変更されました。これを有効にするには再起動が必要です（Advanced Networking option key has been changed, however a restart is required for this to take effect）	必要な LAN 設定とスタティック NAT 設定を「IP」ページで構成してから、システムを再起動します。	警告
25007	再起動が必要です（Restart required）	QoS 設定が変更されました。これを有効にするには再起動が必要です（QoS settings have been changed, however a restart is required for this to take effect）	システムを再起動します。	警告

ID	タイトル	説明	ソリューション	重大度
25008	再起動が必要です（Restart required）	ポート設定が変更されました。これを有効にするには再起動が必要です（Port configuration has been changed, however a restart is required for this to take effect）	システムを再起動します。	警告
25009	再起動が必要です（Restart required）	イーサネット設定が変更されました。これを有効にするには再起動が必要です（Ethernet configuration has been changed, however a restart is required for this to take effect）	システムを再起動します。	警告
25010	再起動が必要です（Restart required）	IP 設定が変更されました。これを有効にするには再起動が必要です（IP configuration has been changed, however a restart is required for this to take effect）	システムを再起動します。	警告
25011	再起動が必要です（Restart required）	HTTPS サービスが変更されました。これを有効にするには再起動が必要です（HTTPS service has been changed, however a restart is required for this to take effect）	システムを再起動します。	警告

ID	タイトル	説明	ソリューション	重大度
25013	IP 設定の不一致（IP configuration mismatch）	IP プロトコルは IPv4 と IPv6 の両方に設定されていますが、システムには定義されている IPv6 ゲートウェイがありません（IP protocol is set to both IPv4 and IPv6, but the system does not have an IPv6 gateway defined）	IP 設定を構成します。	警告
25014	設定の警告（Configuration warning）	IP プロトコルは IPv4 と IPv6 の両方に設定されていますが、Expressway には定義されている IPv6 アドレスがありません（IP protocol is set to both IPv4 and IPv6, but the Expressway does not have any IPv6 addresses defined）	IP 設定を構成します。	警告
25015	再起動が必要です（Restart required）	SSH サービスが変更されました。これを有効にするには再起動が必要です（SSH service has been changed, however a restart is required for this to take effect）	システムを再起動します。	警告

ID	タイトル	説明	ソリューション	重大度
25016	非推奨のイーサネット速度（Ethernet speed not recommended）	イーサネット インターフェイスの速度設定が 1000Mb/s 全二重または 100Mb/s 全二重以外の値にネゴシエートされています。これによりネットワーク上でパケット損失が発生する可能性があります（An Ethernet interface speed setting has been negotiated to a value other than 1000Mb/s full duplex or 100Mb/s full duplex; this may result in packet loss over your network）	イーサネット パラメータを設定します。	警告
25017	再起動が必要です（Restart required）	HTTP サービスが変更されました。これを有効にするには再起動が必要です（HTTP service has been changed, however a restart is required for this to take effect）	システムを再起動します。	警告
25018	ポート競合（Port conflict）	<function> <port> と <function> <port> 間にポートの競合が発生しています（There is a port conflict between <function> <port> and <function> <port>）	ポート設定を「ローカル インバウンド ポート（Local inbound ports）」ページと「ローカル アウトバウンド ポート（Local outbound ports）」ページで確認します。	警告

ID	タイトル	説明	ソリューション	重大度
25019	詳細なログ レベルを設定しました（Verbose log levels configured）	ネットワーク ログまたはサポート ログの 1 つ以上のモジュールが [デバッグ（Debug）] レベルまたは [トレース（Trace）] レベルに設定されています（One or more modules of the Network Log or Support Log are set to a level of Debug or Trace）	ネットワーク ログ モジュールとサポート ログ モジュールは、シスコのサポート担当者による別途のアドバイスがない限り、[情報（Info）] レベルに設定する必要があります。診断ロギングが進行中の場合は、診断ロギングが停止した時点で自動的にリセットされます。	警告
25020	NTP クライアント障害（NTP client failure）	システムが NTP クライアントを実行できません（The system is unable to run the NTP client）	キー設定や有効期限を含め、NTP のステータス情報を確認します。	警告
25021	NTP サーバが使用できません（NTP server not available）	システムは NTP サーバに接続できません（The system is unable to contact an NTP server）	時刻設定とステータスを確認します。また、DNS 設定を確認します。	警告
25022	トラバーサル ゾーンの時刻が同期されていません（Time not synchronized over traversal zone）	このサーバのシステム時刻が、SIP トラバーサル ゾーンのもう一方のサーバのシステム時刻と異なっています（The system time of this server is different from that on a server on the other side of a SIP traversal zone）	システムの時刻設定が一貫していることを確認します。変更を行った場合は、それが有効になるまで時間がかかることがあります。	警告

ID	タイトル	説明	ソリューション	重大度
25023	XMPP のフェデレーション設定警告	フェデレーション用の Expressway アドレスを使用した Unified CM IM and Presence サービス サーバの設定に失敗しました（Failed to configure Unified CM IM and Presence Service servers with Expressway address for XMPP federation）	IM and Presence サービス サーバが稼働していることを確認し、AXL サービスがそこで実行されていることを確認してから、サーバを更新します。	警告
25024	XMPP 設定エラー	XMPP ネットワーク アドレスの設定が無効です（Invalid configuration of XMPP network address）	IPv4 アドレスが正しいことを確認します。127.0.0.1（ループバック アドレス）を使用することができます	エラー
25026	再起動が必要です（Restart required）	Web 管理ポート設定が変更されました。これを有効にするには再起動が必要です（Web administration port has been changed, however a restart is required for this to take effect）	システムを再起動します。	警告

ID	タイトル	説明	ソリューション	重大度
25027	SSLH 障害（SSLH failure）	設定ファイルが書き込まれていないため、プロトコル多重化サービスを開始できません。Expressway-E が TCP 443 で TURN 要求と WebRTC 要求をリッスンできません（The protocol multiplexing service cannot start because the configuration file was not written. The Expressway-E is not able to listen on TCP 443 for TURN and WebRTC requests.）	TURN サービスを再設定します。	クリティカル
25028	HSM ボックスの接続の問題	一部の HSM モジュールに問題があります	HSM 設定 ページで詳細をご確認ください	アラート
25029	再起動が必要です（Restart required）	TURN プロトコルモードを UDP に変更されました。このため、TCP 443 TURN サービスはオフになっていますが、これを有効にする場合は再起動が必要です。	システムを再起動します。	

ID	タイトル	説明	ソリューション	重大度
25030	DNS 逆引き検索に失敗	アドレス <サーバの *IP* アドレス> の DNS 逆引き参照を実行できませんでした。これにより、MRA ログインが失敗する可能性があります。	DNS サーバが、そのアドレス <サーバの*IP*アドレス*&gt* に対して有効な PTR レコードで設定されていることを確認してください。	エラー（Error）
25031	証明書検証が失敗しました（Certificate verification failed）	アドレス <*IP Address of E server*> の PTR レコードの FQDN が、IP <*IP Address of E server*> を持つそのサーバの証明書に提示された SAN エントリと一致しません。	Expressway-E のサーバ証明書に SAN エントリとして存在する FQDN を持つアドレス <*IP Address of E server*> に対して、有効な PTR レコード (1 つだけ) が作成されていることを確認してください。	エラー（Error）

表 *33* : ライセンスアラーム

ID	タイトル	説明	ソリューション	重大度
30001	キャパシティ警告（Capacity warning）	同時発生トラバーサル コールの数がライセンス供与されている上限に近づいています（The number of concurrent traversal calls has approached the licensed limit）	シスコの担当者にお問い合わせください。	警告

ID	タイトル	説明	ソリューション	重大度
30002	キャパシティ警告（Capacity warning）	同時発生トラバーサル コールの数がユニットの物理的な上限に近づいています（The number of concurrent traversal calls has approached the unit's physical limit）	シスコの担当者にお問い合わせください。	警告
30003	キャパシティ警告（Capacity warning）	同時発生非トラバーサル コールの数がユニットの物理的な上限に近づいています（The number of concurrent non-traversal calls has approached the unit's physical limit）	シスコの担当者にお問い合わせください。	警告
30004	キャパシティ警告（Capacity warning）	非トラバーサルの同時コールの数がライセンス制限に近づきました	シスコの担当者にお問い合わせください。	警告
30005	キャパシティ警告（Capacity warning）	TURN リレーの使用率がユニットの物理的な上限に近づいています（TURN relays usage has approached the unit's physical limit）	シスコの担当者にお問い合わせください。	警告

ID	タイトル	説明	ソリューション	重大度
30007	キャパシティ警告（Capacity warning）	TURN リレーの使用率がライセンス供与されている上限に近づいています（TURN relays usage has approached the licensed limit）	シスコの担当者にお問い合わせください。	警告
30009	TURN リレーをインストールしました（TURN relays installed）	TURN サービスは Expressway-E のみで使用できます。TURN のオプション キーは無視されました（TURN services are only available on Expressway-E; TURN option key ignored）	オプション キーの管理を追加/削除します。	警告
30010	キャパシティ警告（Capacity warning）	同時登録の数がライセンス制限に近づきました	シスコの担当者にお問い合わせください。	警告
30011	TURN リレー ライセンスが必要です（TURN relay licenses required）	TURN サービスは有効になっていますが、TURN リレー ライセンスのオプション キーがインストールされていません（TURN services are enabled but no TURN relay license option keys are installed）	オプション キーの管理を追加するか、TURN サービスの設定を無効にします。	警告

ID	タイトル	説明	ソリューション	重大度
30012	損失したクラスタピアのライセンス使用状況（License usage of lost cluster peer）	クラスタ ピア <n> は <n> 時間以上、使用できない状態になっています。クラスタ全体で使用可能な合計から <date> にライセンスが削除されます（Cluster peer <n> has been unavailable for more than <n> days. Its licenses will be removed from the total available for use across the cluster on <date>.）。	このピアの問題を解決するか、このピアをクラスタ設定から削除します。	警告
30013	損失したクラスタピアのライセンス使用状況（License usage of lost cluster peer）	複数のクラスタピアが <n> 時間以上、使用できない状態になっています。クラスタ全体で使用可能な合計からライセンスが次のように削除されます（Several cluster peers have been unavailable for more than <n> days. Their licenses will be removed from the total available for use across the cluster as follows:） <details>.	このピアの問題を解決するか、このピアをクラスタ設定から削除します。	警告

ID	タイトル	説明	ソリューション	重大度
30014	損失したクラスタピアのライセンス使用状況（License usage of lost cluster peer）	クラスタ ピア <n> は <n> 日以上、使用できない状態になっています。クラスタ全体で使用可能な合計から <date> にライセンスが削除されます（Cluster peer <n> has been unavailable for more than <n> days. Its licenses will be removed from the total available for use across the cluster on <date>.）。	このピアの問題を解決するか、このピアをクラスタ設定から削除します。	警告
30015	損失したクラスタピアのライセンス使用状況（License usage of lost cluster peer）	複数のクラスタピアが <n> 日以上、使用できない状態になっています。クラスタ全体で使用可能な合計からライセンスが次のように削除されます（Several cluster peers have been unavailable for more than <n> days. Their licenses will be removed from the total available for use across the cluster as follows:）<details>.	このピアの問題を解決するか、このピアをクラスタ設定から削除します。	警告

ID	タイトル	説明	ソリューション	重大度
30016	損失したクラスタピアのライセンスがライセンスプールから除去されました（Licenses of lost cluster peer have been taken off the license pool）	クラスタ ピア <n> は <n> 日以上、使用できない状態になっています。クラスタ全体で使用可能な合計から <date> にライセンスが削除されました（Cluster peer <n> has been unavailable for more than <n> days. Its licenses have been removed from the total available for use across the cluster on <date>.）。	このピアの問題を解決するか、このピアをクラスタ設定から削除します。	警告
30017	損失したクラスタピアのライセンスがライセンスプールから除去されました（Licenses of lost cluster peer have been taken off the license pool）	複数のクラスタピアが <n> 日以上、使用できない状態になっています。クラスタ全体で使用可能な合計からライセンスが次のように削除されました（Several cluster peers have been unavailable for more than <n> days. Their licenses have been removed from the total available for use across the cluster as follows:）<details>.	このピアの問題を解決するか、このピアをクラスタ設定から削除します。	警告

ID	タイトル	説明	ソリューション	重大度
30018	プロビジョニング ライセンスの上限に到達しました（Provisioning licenses limit reached）	同時にプロビジョニングされたデバイスの数がライセンス供与された上限に到達しました（The number of concurrently provisioned devices has reached the licensed limit）	プロビジョニングの制限は Cisco TMS によって設定されます。追加ライセンスが必要な場合は、シスコの担当者にお問い合わせください。	警告
30019	コール ライセンスの上限に到達しました（Call license limit reached）	同時発生非トラバーサルコール イセンスのライセンス上限の <n> に到達しました（You have reached your license limit of <n> concurrent traversal call licenses）	問題が解決しない場合は、シスコの担当者に連絡し、コール ライセンスを追加購入してください。	警告
30020	コール ライセンスの上限に到達しました（Call license limit reached）	同時発生トラバーサル コール ライセンスのライセンス上限の <n> に到達しました（You have reached your license limit of <n> concurrent traversal call licenses）	問題が解決しない場合は、シスコの担当者に連絡し、コール ライセンスを追加購入してください。	警告
30021	TURN リレー ライセンスの上限に到達しました（TURN relay license limit reached）	同時発生 TURN リレー ライセンスのライセンス上限の <n> に到達しました（You have reached your license limit of <n> concurrent TURN relay licenses）	問題が解決しない場合は、シスコの担当者に連絡し、TURN リレー ライセンスを追加購入してください。	警告

ID	タイトル	説明	ソリューション	重大度
30022	コール キャパシティの上限に到達しました（Call capacity limit reached）	同時非トラバーサル コール数がユニットの物理的上限に達しました（The number of concurrent non-traversal calls has reached the unit's physical limit）	システムに容量を追加します。シスコの担当者にお問い合わせください。	警告
30023	コール キャパシティの上限に到達しました（Call capacity limit reached）	同時発生トラバーサル コールの数がユニットの物理的な上限に到達しました（The number of concurrent traversal calls has reached the unit's physical limit）	システムに容量を追加します。シスコの担当者にお問い合わせください。	警告
30024	TURN リレー キャパシティの上限に到達しました（TURN relay capacity limit reached）	同時発生 TURN リレー コールの数がユニットの物理的な上限に到達しました（The number of concurrent TURN relay calls has reached the unit's physical limit）	システムに容量を追加します。シスコの担当者にお問い合わせください。	警告
30025	再起動が必要です（Restart required）	オプション キーまたはタイプが変更されました。これを有効にするには再起動が必要です（An option key or the type has been changed, however a restart is required for this to take effect）	再起動、リブート、およびシャットダウン	警告

ID	タイトル	説明	ソリューション	重大度
30026	ルーム システムのライセンスの上限に近づいています（Approaching room system license limit）	TelePresence Room システムの同時登録数がライセンスの上限に近づいています（The number of concurrent registered TelePresence room systems is approaching the license limit）	追加ライセンスが必要な場合は、シスコの担当者にお問い合わせください。	警告
30027	キャパシティ警告（Capacity warning）	TelePresence Room システムとデスクトップ システムの同時登録数が、1 つ以上のピアで物理的な上限に達しました（The number of concurrent registered TelePresence room systems and registered desktop systems has reached the physical limit in one or more peer(s)）	すべてのピアに登録が均等に配分されていることを確認します。システムに容量を追加します。シスコの担当者にお問い合わせください。	警告
30028	ルーム システムの登録の上限に到達しました（Room system registrations limit reached）	TelePresence Room システムの登録数がライセンスの上限に到達しました（The number of registered TelePresence room systems has reached the license limit）	追加のルーム システム ライセンスを購入するには、シスコの担当者にお問い合わせください。	警告

ID	タイトル	説明	ソリューション	重大度
30029	デスクトップ システムのライセンスの上限に近づいています（Approaching desktop system license limit）	デスクトップ システムの同時登録数がライセンスの上限に近づいています（The number of concurrent registered desktop systems is approaching the license limit）	追加ライセンスが必要な場合は、シスコの担当者にお問い合わせください。	警告
30030	キャパシティ警告（Capacity warning）	TelePresence Room システムとデスクトップ システムの登録数がユニットの物理的な上限に到達しました（The number of registered TelePresence room systems and registered desktop systems has reached the unit's physical limit）	システムに容量を追加します。シスコの担当者にお問い合わせください。	警告
30031	デスクトップ システムのライセンスの上限に到達しました（Desktop system license limit reached）	デスクトップ システムの登録数がライセンスの上限に到達しました（The number of registered desktop systems has reached the license limit）	デスクトップ システムのライセンスを購入するには、シスコの担当者にお問い合わせください。	警告
30035	Eval の Smart ライセンス	システムは 1 日、2 日、3 日、7 日、30 日後に期限切れになる評価モードで動作しています	Cisco Smart Software Manager または衛星にシステムを登録します	警告
30036	Smart ライセンスが過負荷状態でコンプライアンスに適合していません	ライセンス数が不足しているため、システムが動作しています	Cisco Smart Software Manager で追加のライセンスを設定します	アラート

ID	タイトル	説明	ソリューション	重大度
30037	Smart ライセンス準拠外のプロビジョニングはありません	ライセンス数が不足しているため、システムが動作しています	ユーザおよびデバイスのプロビジョニング機能を復元するには、Cisco Smart Software Manager で追加ライセンスを取得してください	クリティカル
30038	Smart ライセンスプロビジョニングなしEvalの有効期限が切れました	ライセンス評価期間が期限切れで、製品が適用モードになっています	ユーザおよびデバイスのプロビジョニング機能を回復するには、ネットワーク接続を確認して、ライセンス認証を更新してください。	クリティカル
30039	期限切れ承認の Smart ライセンスの有効期限が切れました	ライセンス認証の期限が切れました	ユーザとデバイスのプロビジョニングする機能が失われないよう、ネットワーク接続とライセンス認証の更新を確認してください	アラート
30040	Smart ライセンスプロビジョニング認証が期限切れです	ライセンス認証が期限切れで、製品が強制モードになっています	ユーザおよびデバイスのプロビジョニング機能を回復するには、ネットワーク接続を確認して、ライセンス認証を更新してください。	クリティカル

ID	タイトル	説明	ソリューション	重大度
30041	Smart ライセンスの登録が期限切れです	ライセンス登録の有効期限が切れ、システムが Cisco Smart Software Manager または衛星の登録を解除されています	Cisco Smart Software Manager または衛星へのネットワーク接続を確認してください。また、システムクロックが正しいことを確認してから、システムを Cisco Smart Software Manager またはサテライトに登録します。問題が解決しない場合は、TAC ケースを上げてください。	エラー（Error）
30042	Smart ライセンス通信エラー	システムが Cisco Smart Software Manager または衛星との通信に失敗しました	Cisco Smart Software Manager または衛星へのネットワーク接続を確認してください	エラー（Error）
30043	Smart ライセンス認証の有効期限が間もなく切れます	ライセンス認可期間が間もなく終了します	承認の更新を開始してください	警告
30044	Smart ライセンスの更新認証に失敗しました	ライセンス認証の更新に失敗しました	承認の更新を再試行してください。問題が解決しない場合は、TAC ケースを上げてください	エラー（Error）
30045	Smart ライセンスの更新登録に失敗しました	ライセンス登録の更新に失敗しました	登録の更新を再試行してください。問題が解決しない場合は、TAC ケースを上げてください	エラー（Error）

ID	タイトル	説明	ソリューション	重大度
30046	Smart ライセンス登録の有効期限が間もなく切れます	Cisco Smart Software Manager または衛星への登録はすぐに期限切れになります	ユーザまたはデバイスをプロビジョニングする機能が失われないように登録更新を開始してください	警告

表 *34* : 外部アプリケーション/サービスアラーム

ID	タイトル	説明	ソリューション	重大度
35001	設定の警告（Configuration warning）	Active Directory モードは有効になっていますが、NDS ホスト名が設定されていません（Active Directory mode has been enabled but the DNS hostname has not been configured）	DNS の設定を設定します。	警告
35002	設定の警告（Configuration warning）	Active Directory モードは有効になっていますが、NTP サーバが設定されていません（Active Directory mode has been enabled but the NTP server has not been configured）	時刻の設定 サーバを設定します。	警告
35003	設定の警告（Configuration warning）	Active Directory モードは有効になっていますが、DNS サーバが設定されていません（Active Directory mode has been enabled but no DNS servers have been configured）	DNS の設定 サーバを設定します。	警告

ID	タイトル	説明	ソリューション	重大度
35004	LDAP 設定が必要です（LDAP configuration required）	管理者アカウントまたは FindMe アカウントにリモート ログイン認証を使用していますが、有効な LDAP サーバ アドレス、ポート、Bind_DN、および Base_DN が設定されていません（Remote login authentication is in use for administrator accounts but a valid LDAP Server address, Port, Bind_DN and Base_DN have not been configured）	LDAP を使用したリモート アカウント認証の設定を設定します	警告
35005	設定の警告（Configuration warning）	Active Directory モードは有効になっていますが、ドメインが設定されていません（Active Directory mode has been enabled but a domain has not been configured）	[Active Directory サービス（Active Directory Service）] ページでドメインを設定します	警告
35007	設定の警告（Configuration warning）	Active Directory SPNEGO が無効になっています。SPNEGO 設定を有効にすることを推奨します（Active Directory SPNEGO disabled; you are recommended to enable the SPNEGO setting）	SPNEGO を有効にします。	警告

ID	タイトル	説明	ソリューション	重大度
35008	設定の警告（Configuration warning）	Active Directory モードは有効になっていますが、ワークグループが設定されていません（Active Directory mode has been enabled but a workgroup has not been configured）	[Active Directory サービス（Active Directory Service）] ページでワークグループを設定します。	警告
35009	TMS プロビジョニング拡張サービスの通信障害（TMS Provisioning Extension services communication failure）	Expressway は TMS Provisioning Extension サービスと通信できません。TMS がこのクラスタに対してユーザのプロビジョニングを行っていない場合は、電話帳サービスの障害も発生している可能性があります（The VCS is unable to communicate with the TMS Provisioning Extension services. Phone book service failures can also occur if TMS does not have any users provisioned against this cluster.）	「TMS Provisioning Extension サービスのステータス」ページに移動し、障害が発生したサービスを選択して問題に関する詳細を表示します	警告

ID	タイトル	説明	ソリューション	重大度
35010	TMS プロビジョニング拡張サービス データのインポート障害（TMS Provisioning Extension services data import failure）	Expressway の内部テーブルの制限超過が発生するため、TMS Provisioning Extension サービスからのインポートがキャンセルされました（An import from the TMS Provisioning Extension services has been canceled as it would cause the Expressway to exceed internal table limits）	Expressway イベント ログで詳細を確認した後、TMS 内の対応するデータを確認します。TMS 内のデータを修正した後、TMS Provisioning Extension サービスのステータスを実行する必要があります。	警告
35011	TMS プロビジョニング拡張サービス データのインポート障害（TMS Provisioning Extension services data import failure）	TMS プロビジョニング拡張サービスからインポートしたレコードのうち 1 つ以上が認識できないデータ形式であったためドロップされました（One or more records imported from the TMS Provisioning Extension services have been dropped due to unrecognized data format）	Expressway イベント ログで詳細を確認した後、TMS 内の対応するデータを確認します。TMS 内のデータを修正した後、TMS Provisioning Extension サービスのステータスを実行する必要があります。	警告
35012	LDAP サーバへの接続に失敗しました（Failed to connect to LDAP server）	H.350 デバイス認証用の LDAP サーバに接続できません（Failed to connect to the LDAP server for H.350 device authentication）	H.350 ディレクトリ サービスが正しく設定されていることを確認します。	警告

ID	タイトル	説明	ソリューション	重大度
35013	ユニファイド コミュニケーション SSH トンネルの障害（Unified Communications SSH tunnel failure）	[このシステムは 1 つ以上のリモート ホストと通信できません（This system cannot communicate with one or more remote hosts）]：<*Host 1, Host 2, ...*> ホストのリストは 200 文字に切り詰められます。	イベント ログを確認し、Expressway-C と Expressway-E 間のトラバーサル ゾーンがアクティブであることを確認します。	警告
35014	ユニファイド コミュニケーション SSH トンネル通知の障害（Unified Communications SSH tunnel notification failure）	このシステムは、1 つ以上のリモート ホストと通信できません（This system cannot communicate with one or more remote hosts）	ファイアウォールが Expressway-C のエフェメラル ポートから Expressway-E の 2222 TCP へのトラフィックを許可することを確認します。	警告
35015	Unified CM のポート競合（Unified CM port conflict）	Unified CM <name> とユニファイド コミュニケーション間で Unified CM <name> にポート競合が発生しています（両方ともポート <number> を使用しています）	回線側（ユニファイド コミュニケーション）と SIP トランク トラフィックに Unified CM 上の同じポートを使用できません。Unified CM 上のポート設定を確認し、必要に応じて <zone> を再設定します。	警告

ID	タイトル	説明	ソリューション	重大度
35016	SAML メタデータが変更されました（SAML metadata has been modified）	設定変更によってローカル SAML メタデータが変更されました。ID プロバイダーのどのコピーとも異なっています。このメタデータはサーバ証明書または SSO 対応ドメインの変更によって、あるいはトラバーサル サーバ ピアの番号またはそれらのアドレスの変更によって変更された可能性があります（Configuration changes have modified the local SAML metadata, which is now different to any copies on Identity Provider(s). This metadata may have been modified by changing the server certificate or the SSO-enabled domains, or by changing the number of traversal server peers or their addresses）	アイデンティティ プロバイダーにインポートできるよう、SAML メタデータをエクスポートします。	警告

表 *35* : セキュリティアラーム

ID	タイトル	説明	ソリューション	重大度
40001	セキュリティ アラート（Security alert）	CRL 配布ポイントが自動更新用に定義されていません（No CRL distribution points have been defined for automatic updates）	証明書失効リスト（CRL）の管理を確認します。	警告
40002	セキュリティ アラート（Security alert）	CRL ファイルの自動更新に失敗しました（Automatic updating of CRL files has failed）	問題が解決しない場合は、シスコの担当者に連絡してください	警告
40003	安全でないパスワードが使用されています（Insecure password in use）	root ユーザにデフォルトのパスワードが設定されています（The root user has the default password set）	root アカウントの使用手順を表示します。	警告

ID	タイトル	説明	ソリューション	重大度
40004	証明書ベースの認証が必要です（Certificate-based authentication required）	高度なアカウントセキュリティモードでは、システムのクライアント証明書ベースのセキュリティを[証明書ベースの認証（Certificate-based authentication）]に設定することを推奨します（Your system is recommended to have client certificate-based security set to Certificate-based authentication when in advanced account security mode）	ネットワークサービスを設定します	警告
40005	安全でないパスワードが使用されています（Insecure password in use）	admin ユーザにデフォルトのパスワードが設定されています（The admin user has the default password set）	管理者アカウントの設定を変更します。	エラー
40006	セキュリティ アラート（Security alert）	CRL の更新をダウンロードできません（Unable to download CRL update）	証明書失効リスト（CRL）の管理とログを確認します。	警告
40007	セキュリティ アラート（Security alert）	CRL 自動更新用の設定ファイルが見つかりませんでした（Failed to find configuration file for CRL automatic updates）	問題が解決しない場合は、シスコの担当者に連絡してください	警告

ID	タイトル	説明	ソリューション	重大度
40008	セキュリティ アラート（Security alert）	SSHサービスがデフォルトのキーを使用しています（The SSH service is using the default key）	デフォルトのSSHキーの変更手順を表示します	警告
40009	再起動が必要です（Restart required）	HTTPS クライアント証明書の検証モードが変更されました。これを有効にするには再起動が必要です（HTTPS client certificates validation mode has changed, however a restart is required for this to take effect）	再起動、リブート、およびシャットダウン	警告
40011	アカウント単位のセッションの制限が必要です（Per-account session limit required）	高度なアカウントセキュリティモードでは、ゼロ以外のアカウント単位のセッションの制限が必要（A non-zero per-account session limit is required when in advanced account security mode）	ネットワークサービスを設定します。	警告

ID	タイトル	説明	ソリューション	重大度
40012	外部マネージャの接続に HTTP を使用しています（External manager connection is using HTTP）	高度なアカウントセキュリティモードでは、外部マネージャへの接続に HTTPS を使用することを推奨します（You are recommended to use HTTPS connections to the external manger when in advanced account security mode）	外部マネージャ設定値の設定を設定します。	警告
40013	HTTPS クライアント証明書の検証が無効になっています（HTTPS client certificate validation disabled）	高度なアカウントセキュリティモードでは、HTTPS 接続に対してクライアント側の証明書の検証を有効にすることを推奨します（You are recommended to enable client side certificate validation for HTTPS connections when in advanced account security mode）	ネットワークサービスを設定します	警告
40014	タイムアウト時間が必要です（Time out period required）	高度なアカウントセキュリティモードでは、ゼロ以外のシステムセッション タイムアウト時間が必要です（A non-zero system session time out period is required when in advanced account security mode）	ネットワークサービスを設定します。	警告

ID	タイトル	説明	ソリューション	重大度
40015	システム セッションの制限が必要です（System session limit required）	高度なアカウント セキュリティ モードでは、ゼロ以外のシステム セッションの制限が必要です（A non-zero system session limit is required when in advanced account security mode）	ネットワーク サービスを設定します。	警告
40016	暗号化が必要です（Encryption required）	高度なアカウント セキュリティ モードでは、ログイン アカウントのLDAPサーバ設定で暗号化を[TLS] に設定することを推奨します（Your login account LDAP server configuration is recommended to have encryption set to TLS when in advanced account security mode）	LDAP を使用したリモート アカウント認証の設定を設定します。	警告
40017	インシデント レポートが有効になっています（Incident reporting enabled）	高度なアカウント セキュリティ モードでは、インシデント レポートを無効にすることを推奨します（You are recommended to disable incident reporting when in advanced account security mode）	インシデントレポートを設定します。	警告

ID	タイトル	説明	ソリューション	重大度
40018	安全でないパスワードが使用されています（Insecure password in use）	1 人以上のユーザが厳密でないパスワードを使用しています（One or more users has a non-strict password）		警告
40019	外部マネージャの証明書チェックを無効にしました（External manager has certificate checking disabled）	高度なアカウントセキュリティモードでは、外部マネージャの証明書チェックを有効にすることを推奨します（You are recommended to enable external manager certificate checking when in advanced account security mode）	外部マネージャ設定値の設定を設定します。	警告
40020	セキュリティ アラート（Security alert）	Active Directory サービスへの接続に TLS 暗号化を使用していません（The connection to the Active Directory Service is not using TLS encryption）	Active Directory サービスの接続設定を行います	警告
40021	リモート ロギングが有効になっています（Remote logging enabled）	高度なアカウントセキュリティモードでは、リモート syslog サーバを無効にすることを推奨します（You are recommended to disable the remote syslog server when in advanced account security mode）	ロギングの設定を設定します。	警告

ID	タイトル	説明	ソリューション	重大度
40022	セキュリティ アラート（Security alert）	Active Directory セキュア チャネルが無効になっています。セキュア チャネル設定を有効にすることを推奨します（Active Directory secure channel disabled; you are recommended to enable the secure channel setting）	セキュア チャネルを有効にします。	警告
40024	CRL チェックが必要です（CRL checking required）	高度なアカウント セキュリティ モードでは、ログイン アカウントの LDAP サーバ設定で証明書失効リスト（CRL）のチェックを [すべて（All）] に設定することを推奨します（Your login account LDAP server configuration is recommended to have certificate revocation list (CRL) checking set to All when in advanced account security mode）	LDAP を使用したリモート アカウント認証の設定を設定します。	警告
40025	SNMP が有効になっています（SNMP enabled）	高度なアカウント セキュリティ モードでは、SNMP を無効にすることを推奨します（You are recommended to disable SNMP when in advanced account security mode）	SNMP 設定値の設定を設定します。	警告

ID	タイトル	説明	ソリューション	重大度
40026	リブートが必要です（Reboot required）	高度なアカウントセキュリティモードを変更しました。これを有効にするにはリブートが必要です（The advanced account security mode has changed, however a reboot is required for this to take effect）	再起動、リブート、およびシャットダウン	警告
40027	セキュリティ アラート（Security alert）	TMS プロビジョニング拡張サービスへの接続に TLS 暗号化を使用していません（The connection to the TMS Provisioning Extension services is not using TLS encryption）	TMS プロビジョニング拡張サービスの接続を設定します。	警告
40028	安全でないパスワードが使用されています（Insecure password in use）	root ユーザのパスワードは MD5 を使用してハッシュされますが、これでは十分に安全といえません（The root user's password is hashed using MD5, which is not secure enough）	root アカウントの使用手順を表示します。	警告

ID	タイトル	説明	ソリューション	重大度
40029	LDAP サーバの CA 証明書がありません（LDAP server CA certificate is missing）	LDAP データベースの有効な CA 証明書がアップロードされていません。これは TLS を介した接続に必要です（A valid CA certificate for the LDAP database has not been uploaded; this is required for connections via TLS）	有効な CA 証明書をアップロードします。	警告
40030	セキュリティ アラート（Security alert）	ファイアウォール ルールのアクティブ化に失敗しました。ファイア ウォール設定に少なくとも 1 つの拒否されたルールが含まれています（Firewall rules activation failed; the firewall configuration contains at least one rejected rule）	侵入からの保護を確認して拒否されたルールを修正し、再有効化を試みます。	警告
40031	セキュリティ アラート（Security alert）	以前のファイア ウォール設定を復元できません（Unable to restore previous firewall configuration）	侵入からの保護を確認後、拒否されたルールを修正してルールをアクティブ化して、承認します。問題が解決しない場合は、シスコの担当者にお問い合わせください。	警告

ID	タイトル	説明	ソリューション	重大度
40032	セキュリティ アラート（Security alert）	ファイアウォールを初期化できません（Unable to initialize firewall）	再起動、リブート、およびシャットダウン問題が解決しない場合は、シスコの担当者にお問い合わせください	警告
40033	設定の警告（Configuration warning）	デフォルトのゾーン アクセス ルールは有効になっていますが、SIP over UDP または SIP over TCP を有効のままにしておくと、このセキュリティ機能を回避する手段を提供することになります（The Default Zone access rules are enabled, but leaving SIP over UDP or SIP over TCP enabled offers a way to circumvent this security feature）	SIP の設定で UDP と TCP を無効にして TLS を使用した証明書アイデンティティ チェックを適用するか、またはデフォルト ゾーンの設定に対するアクセス ルールを無効にします。	警告
40034	セキュリティ アラート（Security alert）	ファイアウォールのアクティブ化に失敗しました。ファイアウォール設定にプライオリティの重複があります（Firewall rules activation failed; the firewall configuration contains rules with duplicated priorities）	侵入からの保護をチェックしてすべてのルールに一意のプライオリティがあることを確認してからアクティブ化を再試行します。	警告

ID	タイトル	説明	ソリューション	重大度
40036	委任クレデンシャルチェックエラー	SIPドメイン <domain> に関連付けられたトラバーサルサーバゾーンは、トラバーサルクライアントシステムに接続できません	ドメインとそれに関連付けられたトラバーサルサーバゾーンが正しく設定されていることを確認します。また、リモートトラバーサルクライアントシステムを確認する必要もあります	警告
40037	委任クレデンシャルチェックエラー	委任クレデンシャルチェック要求の受信に使用するトラバーサルクライアントゾーン <zone> に通信の問題があります	そのトラバーサルクライアントゾーンが正しく設定されていることを確認します。また、リモートトラバーサルサーバ システムを確認する必要があります	警告
40038	委任クレデンシャルチェック設定エラー	SIPドメイン <domain>に関連付けられているトラバーサルサーバゾーンでTLS検証モードが有効になっていません	ドメインをチェックし、TLS 検証モードが関連付けられているトラバーサルサーバゾーンで有効になっていることを確認します	警告
40039	委任クレデンシャルチェック設定エラー	委任認証要求を受け入れるように設定されたトラバーサルクライアントゾーン (<zone>) でTLS検証モードが有効になっていません	TLS確認モードがトラバーサルクライアントゾーンで有効になっていることを確認します	警告

ID	タイトル	説明	ソリューション	重大度
40040	ユニファイド コミュニケーションの設定エラー（Unified Communications configuration error）	TLS検証モードがユニファイド コミュニケーション サービス用に設定されたトラバーサル ゾーンで有効になっていません（TLS verify mode is not enabled on a traversal zone configured for Unified Communications services）	TLS検証モードがトラバーサル ゾーンで有効になっていることを確認します。また、リモート トラバーサル システムを確認する必要もあります。	警告
40041	セキュリティ アラート（Security alert）	自動化された侵入からの保護のルールが使用できません（Automated intrusion protection rules are not available）	失敗したサービスを無効にしてから、もう一度有効にします。	警告
40042	FIPS1 40-2 コンプライアンスの規制（FIPS140-2 compliance restriction）	一部のSIP設定がTLSトランスポートを使用していません。FIPS140-2に準拠するにはTLS が必要です（Some SIP configuration is not using TLS transport; FIPS140-2 compliance requires TLS）	[SIP] ページでTLSがシステム全体で対応する唯一のトランスポートであり、すべてのゾーンが TLS を使用していることを確認します。または、FIPS140-2に移行する場合は、FIPS 対応のデータのバックアップを復元できます。	警告

ID	タイトル	説明	ソリューション	重大度
40043	ユニファイド コミュニケーションの設定エラー（Unified Communications configuration error）	メディア暗号化がユニファイド コミュニケーション サービス用に設定されたトラバーサル ゾーンに適用されません（Media encryption is not enforced on a traversal zone configured for Unified Communications services）	メディア暗号化がトラバーサル ゾーンに対して [強制暗号化（Force encrypted）] に設定されていることを確認します。	警告
40044	システムのリセットが必要です（System reset required）	FIPS140-2 モードが有効化されています。システム リセットを実行するには、このプロセスを完了させる必要があります（FIPS140-2 mode has been enabled; a system reset is required to complete this process）	すべてのアラームがクリアされていることを確認してから、システムのリセットを実行する前にシステムのバックアップを実行します。	警告
40045	再起動が必要です（Restart required）	FIPS140-2 モードが無効化されています。システム リセットを実行するには、このプロセスを完了させる必要があります（FIPS140-2 mode has been disabled; a system restart is required to complete this process）	再起動、リブート、およびシャットダウン	警告

ID	タイトル	説明	ソリューション	重大度
40046	FIPS1 40-2 コンプライアンスの規制（FIPS140-2 compliance restriction）	クラスタ化されたシステムが FIPS140-2 に準拠していません（Clustered systems are not FIPS140-2 compliant）	クラスタを解除します。	警告
40048	ユニファイド コミュニケーションの設定エラー（Unified Communications configuration error）	ユニファイド コミュニケーション サービスは有効になっていますが、SIP TLS が無効になっています（Unified Communications services are enabled but SIP TLS is disabled）	SIP TLS モードが [SIP の設定（SIP configuration）] ページで [オン（On）] に設定されていることを確認します。	警告
40049	クラスタ TLS の許容（Cluster TLS permissive）	クラスタ TLS 検証モードで無効な証明書が許容されています（Cluster TLS verification mode permits invalid certificates）	クラスタの TLS 検証モードを Enforcing に変更します	通知
40050	セキュリティ アラート（Security alert）	新しいファイアウォール設定をインストールできません（Unable to install new firewall configuration）	侵入からの保護とレート制限設定を確認し、拒否されたルールを修正します。システムを再起動しないでください。問題が解決しない場合は、シスコの担当者にお問い合わせください。	

ID	タイトル	説明	ソリューション	重大度
40051	サーバ証明書によって CMS が特定されません（CMS not Identified by Server Certificate）	CMS アドレス <*address*>は Expressway-C で入力されましたが、Expressway-E サーバ証明書で特定されません（CMS address <address> has been entered on the Expressway-C but is not identified by the Expressway-E server certificate）	Expressway-C の CMS アドレスが Expressway-E サーバの SAN エントリに一致することを確認します。CMS を SAN として含む新しいサーバ証明書の Expressway のサーバ証明書の管理するか、Expressway-C 上の CMS を編集（または削除）します。	
40052	証明書エラー（Certificate error）	サーバ証明書には共通名（CN）属性がありません。一部のサービスは CN なしでは動作しません（Server certificate does not have a Common Name (CN) attribute. Some services do not work without the CN）	証明書を更新します。	
40053	無効な暗号化設定（Invalid Cipher config）	次のエントリには、FIPS140-2 モードで無効な暗号値 <*List*> があります（The following entries have cipher values that are invalid in FIPS140-2 mode: <List>）	最小限 TLS バージョンと暗号スイートの設定で影響を受ける暗号化エントリを再設定してください。	

ID	タイトル	説明	ソリューション	重大度
40054	トークンの復号の失敗（Token decryption failure）	Expressway-C は、Unified CM によって発行された OAuth トークンの復号化に失敗しました。これは、発行者の変更が原因である可能性があります（The Expressway-C failed to decrypt or decode an OAuth token issued by Unified CM. This could be caused by changes to the issuer.）。	Cisco Unified Communications Manager の設定を更新します。	警告
40055	キー ファイルの更新に失敗しました（Failed to update key file））	一貫性のない状態のためにシステム キー ファイルの更新に失敗しました（Failed to update system key file due to inconsistent state）	システムを再起動します。それでも問題が解決しない場合は、シスコの担当者にお問い合わせください。	警告
40061	ACME 自動署名の障害（ACME auto-sign failure）	サーバ証明書の自動署名コマンドを実行中に障害が検出されました（A failure was detected while running the auto-sign command for the server certificate）	詳細については、サーバ証明書のページを参照してください。	警告

ID	タイトル	説明	ソリューション	重大度
40062	ACME 自動署名の障害（ACME auto-sign failure）	SNI ドメイン [<*domain*>] の自動署名コマンドを実行中に障害が検出されました（A failure was detected while running the auto-sign command for SNI domains [<domain>]）	詳細については、ドメイン証明書のページを参照してください。	警告
40063	ACME 自動展開の障害（ACME auto-deploy failure）	サーバ証明書の自動展開コマンドを実行中に障害が検出されました（A failure was detected while running the auto-deploy command for the server certificate）	詳細については、サーバ証明書のページを参照してください。	警告
40064	ACME 自動展開の障害（ACME auto-deploy failure）	SNI ドメイン [<domain>] の自動展開コマンドを実行中に障害が検出されました（A failure was detected while running the auto-deploy command for SNI domains [<domain>]）	詳細については、ドメイン証明書のページを参照してください。	警告
40066	HSM 証明書が使用されていません	HSM 証明書がインストールされていますが、使用されていません	HSM 設定 ページで詳細をご確認ください	アラート
40068	サーバ証明書の有効性	サーバ証明書の有効期限が切れた、またはサーバ証明書が本日期限切れです	新しいサーバ証明書を作成してアップロードします	クリティカル

ID	タイトル	説明	ソリューション	重大度
40069	サーバ証明書の有効性	<*n*>日でサーバ証明書の有効期限が切れます	新しいサーバ証明書を作成してアップロードすることをお勧めします	アラート
40100	セキュリティ アラート（Security alert）	ファイアウォール ルールがネットワーク インターフェイスと同期されていません（Firewall rules are not synchronized with network interfaces）	システムを再起動します。それでも問題が解決しない場合は、シスコの担当者にお問い合わせください。	警告

表 *36*：設定ミスアラーム

ID	タイトル	説明	ソリューション	重大度
45001	コール ポリシー ファイルのロードに失敗しました（Failed to load Call Policy file）	<failure details>	コール ポリシーの設定を設定します。	警告
45002	設定の警告（Configuration warning）	デフォルト サブゾーンとデフォルト ゾーン間に予期していたデフォルト リンクがありません（Expected default link between the Default Subzone and the Default Zone is missing）	デフォルト リンクを設定します。	警告

ID	タイトル	説明	ソリューション	重大度
45003	設定の警告（Configuration warning）	H.323 モードと SIP モードがオフに設定されています。それらの一方または両方を有効にしてください（H.323 and SIP modes are set to Off; one or both of them should be enabled）	H.323 の設定 モードまたは SIP の設定 モードあるいはその両方を設定します。	警告
45006	設定の警告（Configuration warning）	デフォルト サブゾーンとクラスタ サブゾーン間に予期していたデフォルト リンクがありません（Expected default link between the Default Subzone and the Cluster Subzone is missing）	デフォルト リンクを設定します。	警告
45007	設定の警告（Configuration warning）	デフォルト サブゾーンとトラバーサル サブゾーン間に予期していたデフォルト リンクがありません（Expected default link between the Default Subzone and the Traversal Subzone is missing）	デフォルト リンクを設定します。	警告

ID	タイトル	説明	ソリューション	重大度
45008	設定の警告（Configuration warning）	トラバーサル サブゾーンとデフォルト ゾーン間に予期していたデフォルト リンクがありません（Expected default link between the Traversal Subzone and the Default Zone is missing）	デフォルト リンクを設定します。	警告
45009	設定の警告（Configuration warning）	プロビジョニングを正しく動作させるには、デフォルト ゾーンと、プロビジョニング要求を受信する関連ゾーンで認証ポリシーを有効にする必要があります（For provisioning to work correctly, authentication policy must be enabled on the Default Zone and any other relevant zone that receives provisioning requests）	各関連ゾーンの認証ポリシーを「[クレデンシャルの確認（Check credentials）]」または「[認証済みとして処理（Treat as authenticated）]」に設定します。	警告

ID	タイトル	説明	ソリューション	重大度
45012	設定の警告（Configuration warning）	プレゼンス サービスが正しく動作するためには、デフォルト サブゾーンとそれに関連するすべてのサブゾーンが有効化されている必要があります。エンドポイントが登録されていない場合も、デフォルト ゾーンでの認証が有効化されていなければなりません。	デフォルトサブゾーンと各関連サブゾーンおよびゾーンの認証ポリシーを 「[クレデンシャルの確認（Check credentials）]」 または 「[認証済みとして処理（Treat as authenticated）]」 に設定します。	警告
45013	設定の警告（Configuration warning）	電話帳を正しく動作させるには、デフォルト サブゾーンとその他の関連サブゾーンで認証ポリシーを有効にする必要があります。また、エンドポイントが登録されていない場合は、デフォルト ゾーンで認証を有効にする必要もあります（For phone book requests to work correctly, authentication policy must be enabled on the Default Subzone and any other relevant subzone; authentication must also be enabled on the Default Zone if the endpoints are not registered）	デフォルトサブゾーンと各関連サブゾーンおよびゾーンの認証ポリシーを 「[クレデンシャルの確認（Check credentials）]」 または 「[認証済みとして処理（Treat as authenticated）]」 に設定します。	警告

ID	タイトル	説明	ソリューション	重大度
45014	設定の警告（Configuration warning）	SIP メディア暗号化モードが「Force encrypted」または「Force unencrypted」の状態で、ゾーン内で H.323 が有効になっています。	関連するゾーンで H.323 を無効にするか、別の SIP メディア暗号化モードを選択します	警告
45016	設定の警告（Configuration warning）	ゾーンの SIP メディア暗号化モードは「[ベストエフォート（Best effort）]」または「[強制暗号化（Force encrypted）]」に設定されていますが、トランスポートが TLS ではありません。TLS は暗号化に必要です。（A zone has a SIP media encryption mode of "Best effort" or "Force encrypted" but the transport is not TLS. TLS is required for encryption.）	関連するゾーンで SIP トランスポートを TLS に設定するか、または別の SIP メディア暗号化モードを選択します。	警告

ID	タイトル	説明	ソリューション	重大度
45017	設定の警告（Configuration warning）	サブゾーンの SIP メディア暗号化モードは「[ベスト エフォート（Best effort）]」または「[強制暗号化（Force encrypted）]」に設定されていますが、TLS が有効になっていません。TLS は暗号化に必要です。（A zone has a SIP media encryption mode of "Best effort" or "Force encrypted" but the transport is not TLS. TLS is required for encryption.）	[SIP の設定（SIP configuration）] ページで TLS を有効にするか、または関連するサブゾーンまたはデフォルト サブゾーンに別の SIP メディア暗号化モードを選択します	警告
45018	設定の警告（Configuration warning）	DNS ゾーン（<zone_name>）など）の SIP のデフォルト トランスポート プロトコルが <protocol>）に設定されていますが、そのプロトコルはシステム全体にわたって無効になっています（DNS zones (including <zone_name>) have their SIP default transport protocol set to <protocol>), but that protocol is disabled system-wide.）。	DNS ゾーンの SIP のデフォルトのトランスポート プロトコルとシステム全体の SIP トランスポートの設定が一貫していることを確認します。	警告

ID	タイトル	説明	ソリューション	重大度
45019	メディア ポートの不足（Insufficient media ports）	ライセンス供与されたコールの数をサポートするにはメディア ポートの数が足りません（There is an insufficient number of media ports to support the number of licensed calls）	メディア ポート範囲を拡大します。	警告
45021	HSMサーバ設定の問題	HSM サーバ構成に問題があります	HSM 設定 ページで詳細をご確認ください	アラート
45022	再起動が必要です（Restart required）	DMI 管理構成が変更されましたが、これを有効にするには再起動が必要です。	再起動、リブート、およびシャットダウン	警告
45023	設定エラー	複数の接続間でホスト/ポートタプルを共有しようと試みます。	ゾーンを確認して、ホスト名またはポートの競合を修正します	エラー（Error）

ID	タイトル	説明	ソリューション	重大度
45024	SSLH 障害（SSLH failure）	管理 *DMI* のみモードが設定され、Web Administration がポート 443 を使用している場合、プロトコル多重サービスは開始できません。Expressway が TCP 443 で TURN 要求と WebRTC 要求をリッスンできません（The protocol multiplexing service cannot start because the configuration file was not written. The Expressway-E is not able to listen on TCP 443 for TURN and WebRTC requests.）		クリティカル

表 *37* : バックツーバックユーザエージェントアラーム

ID	タイトル	説明	ソリューション	重大度
55001	B2BUA サービス再起動が必要です（B2BUA service restart required）	一部の B2BUA サービス固有の設定が変更されました。これを有効にするには再起動が必要です（Some B2BUA service specific configuration has changed, however a restart is required for this to take effect）	B2BUAサービスをリスタートする	警告

ID	タイトル	説明	ソリューション	重大度
55002	B2BUA の誤設定（B2BUA misconfiguration）	Expressway 通信用の B2BUA ポートの設定が誤っています（The port on B2BUA for Expressway communications is misconfigured）	[B2BUA の設定（B2BUA configuration）]（詳細設定）を確認します。	警告
55003	B2BUA の誤設定（B2BUA misconfiguration）	Microsoft デバイスの信頼できるホストの IP アドレスが無効です（Invalid trusted host IP address of Microsoft device）	設定されている信頼できるホストのアドレスを確認します	警告
55004	B2BUA の誤設定（B2BUA misconfiguration）	Microsoft コール通信用の B2BUA ポートの設定が誤っています（The port on B2BUA for Microsoft call communications is misconfigured）	[B2BUA の設定（B2BUA configuration）]（詳細設定）を確認します。	警告
55005	B2BUA の誤設定（B2BUA misconfiguration）	Microsoftの宛先アドレスが誤って設定されています（The Microsoft destination address is misconfigured）	B2BUA の設定を確認します。	警告
55006	B2BUA の誤設定（B2BUA misconfiguration）	Microsoftの宛先ポートが誤って設定されています（The Microsoft destination port is misconfigured）	B2BUA の設定を確認します。	警告

ID	タイトル	説明	ソリューション	重大度
55007	B2BUA の誤設定（B2BUA misconfiguration）	Microsoft トランス ポート タイプの設定が誤っています（The Microsoft transport type is misconfigured）	B2BUA の設定を確認します。	警告
55008	B2BUA の誤設定（B2BUA misconfiguration）	サービスの FQDN がないか、または無効です（Missing or invalid FQDN of service）	Expressway のシステム ホスト名とドメイン名を確認します	警告
55009	B2BUA の誤設定（B2BUA misconfiguration）	サービスの IP アドレスが無効です（Invalid IP address of service）	Expressway の LAN 1 IPv4 アドレスを確認します	警告
55010	B2BUA の誤設定（B2BUA misconfiguration）	B2BUA メディア ポート範囲の終了値の設定が誤っています（The B2BUA media port range end value is misconfigured）	[B2BUA の設定（B2BUA configuration）]（詳細設定）を確認します。	警告
55011	B2BUA の誤設定（B2BUA misconfiguration）	B2BUA メディア ポート範囲の開始値の設定が誤っています（The B2BUA media port range start value is misconfigured）	[B2BUA の設定（B2BUA configuration）]（詳細設定）を確認します。	警告
55012	B2BUA の誤設定（B2BUA misconfiguration）	無効なMicrosoftの相互運用性モード（Invalid Microsoft interoperability mode）	B2BUA の設定を確認します。	警告

ID	タイトル	説明	ソリューション	重大度
55013	B2BUA の誤設定（B2BUA misconfiguration）	オプション キーが無効です（Invalid option key）	オプション キーを確認します	警告
55014	B2BUA の誤設定（B2BUA misconfiguration）	ホップ カウントが無効です（Invalid hop count）	[B2BUA の設定（B2BUA configuration）]（詳細設定）を確認します。	警告
55015	B2BUA の誤設定（B2BUA misconfiguration）	トランスコーダの信頼できるホストの IP アドレスが無効です（Invalid trusted host IP address of transcoder）	設定されている信頼できるホストのアドレスを確認します	警告
55016	B2BUA の誤設定（B2BUA misconfiguration）	この B2BUA 用のトランスコーダを有効にする設定が誤っています（The setting to enable transcoders for this B2BUA is misconfigured）	B2BUA の設定（トランスコーダの設定）を確認します。	警告
55017	B2BUA の誤設定（B2BUA misconfiguration）	トランスコーダ通信用の B2BUA ポートの設定が誤っています（The port on B2BUA for transcoder communications is misconfigured）	B2BUA の設定（トランスコーダの設定）を確認します。	警告

ID	タイトル	説明	ソリューション	重大度
55018	B2BUA の誤設定（B2BUA misconfiguration）	トランスコーダ アドレスまたはポートの詳細、あるいはその両方の設定が誤っています（Transcoder address and/or port details are misconfigured）	B2BUA 設定（トランスコーダの設定）と設定されている信頼できるホストのアドレスを確認します	警告
55019	B2BUA の誤設定（B2BUA misconfiguration）	TURN サーバのアドレスが無効です（Invalid TURN server address）	B2BUA の設定（TURN の設定）を確認します。	警告
55021	B2BUA の誤設定（B2BUA misconfiguration）	この B2BUA に TURN サービスを提供するための設定が誤っています（The setting to offer TURN services for this B2BUA is misconfigured）	B2BUA の設定（TURN の設定）を確認します。	警告
55026	B2BUA の誤設定（B2BUA misconfiguration）	TURN サービスは有効になっていますが、有効な TURN サーバが設定されていません（The B2BUA has been enabled to use transcoders, but there are no transcoders configured）	TURN サーバのアドレスを設定します	警告
55028	B2BUA の誤設定（B2BUA misconfiguration）	メディア ポート範囲の最初と最後の設定が誤っています（The start and end media port ranges are misconfigured）	B2BUA のメディア ポート範囲の設定を確認します。	警告

ID	タイトル	説明	ソリューション	重大度
55029	B2BUA の誤設定（B2BUA misconfiguration）	B2BUA が使用するメディア ポート範囲が <module> で使用するメディア ポート範囲と重複しています	両方のサービスのポート設定を確認します。	警告
55030	B2BUA の誤設定（B2BUA misconfiguration）	Expressway の通信に B2BUA が使用するポートは <module> も使用します（The port used by the B2BUA for Expressway communications is also used by <module>）	両方のサービスのポート設定を確認します。	警告
55031	B2BUA の誤設定（B2BUA misconfiguration）	Microsoft コールの通信に B2BUA が使用するポートは <module> も使用します（The port used by the B2BUA for Microsoft call communications is also used by <module>）	両方のサービスのポート設定を確認します。	警告
55032	B2BUA の誤設定（B2BUA misconfiguration）	トランスコーダの通信に B2BUA が使用するポートは <module> も使用します（The port used by the B2BUA for transcoder communications is also used by <module>）	両方のサービスのポート設定を確認します。	警告

ID	タイトル	説明	ソリューション	重大度
55033	B2BUA の誤設定（B2BUA misconfiguration）	Microsoft の有効な信頼できるホストが設定されていません（No valid Microsoft trusted hosts have been configured）	少なくとも 1 つの信頼できるホストデバイスを設定します	警告
55034	B2BUA の誤設定（B2BUA misconfiguration）	トランスコーダの有効な信頼できるホストが設定されていません（No valid transcoder trusted hosts have been configured）	少なくとも 1 つのトランスコーダの信頼できるホストを設定します。	警告
55035	B2BUA 接続の問題（B2BUA connectivity problem）	B2BUA がトランスコーダに接続できません（The B2BUA cannot connect to the transcoders）	B2BUAサービスをリスタートする	警告
55036	B2BUA 接続の問題（B2BUA connectivity problem）	B2BUA が Expressway に接続できません（The B2BUA cannot connect to the Expressway）	B2BUAサービスをリスタートする	警告
55037	B2BUA 接続の問題（B2BUA connectivity problem）	B2BUA が Microsoft 環境に接続できません（The B2BUA cannot connect to the Microsoft environment）	「Microsoft 相互運用性のステータス（Microsoft interoperability status）」ページで問題の詳細を確認します。設定変更を行った後に B2BUA サービスの再起動が必要になる場合があります	警告

ID	タイトル	説明	ソリューション	重大度
55101	B2BUA の誤設定（B2BUA misconfiguration）	Expressway の許可済みホスト IP アドレスが無効です（Invalid Expressway authorized host IP address）	サービスを再起動します。問題が解決しない場合は、シスコの担当者に連絡してください。	警告
55102	B2BUA の誤設定（B2BUA misconfiguration）	Expressway の連絡先アドレスの URI 形式が無効です（Invalid URI format of Expressway contact address）	サービスを再起動します。問題が解決しない場合は、シスコの担当者に連絡してください。	警告
55103	B2BUA の誤設定（B2BUA misconfiguration）	Expressway の暗号化モードが無効です（Invalid Expressway encryption mode）	サービスを再起動します。問題が解決しない場合は、シスコの担当者に連絡してください。	警告
55104	B2BUA の誤設定（B2BUA misconfiguration）	Expressway ICE モードが無効です（Invalid Expressway ICE mode）	サービスを再起動します。問題が解決しない場合は、シスコの担当者に連絡してください。	警告
55105	B2BUA の誤設定（B2BUA misconfiguration）	Expressway のネクスト ホップのホスト設定が無効です（Invalid Expressway next hop host configuration）	サービスを再起動します。問題が解決しない場合は、シスコの担当者に連絡してください。	警告
55106	B2BUA の誤設定（B2BUA misconfiguration）	Expressway のネクスト ホップの活性モードが無効です（Invalid Expressway next hop liveness mode）	サービスを再起動します。問題が解決しない場合は、シスコの担当者に連絡してください。	警告

ID	タイトル	説明	ソリューション	重大度
55107	B2BUA の誤設定（B2BUA misconfiguration）	Expressway のネクスト ホップ モードが無効です（Invalid Expressway next hop mode）	サービスを再起動します。問題が解決しない場合は、シスコの担当者に連絡してください。	警告
55108	B2BUA の誤設定（B2BUA misconfiguration）	Expressway のネクスト ホップ ポートが無効です（Invalid Expressway next hop port）	サービスを再起動します。問題が解決しない場合は、シスコの担当者に連絡してください。	警告
55109	B2BUA の誤設定（B2BUA misconfiguration）	Expressway のトランスポート タイプが無効です（Invalid Expressway transport type）	サービスを再起動します。問題が解決しない場合は、シスコの担当者に連絡してください。	警告
55110	B2BUA の誤設定（B2BUA misconfiguration）	B 側の連絡先アドレスの URI 形式が無効です（Invalid URI format of B side contact address）	サービスを再起動します。問題が解決しない場合は、シスコの担当者に連絡してください。	警告
55111	B2BUA の誤設定（B2BUA misconfiguration）	B 側の暗号化モードが無効です（Invalid B side encryption mode）	サービスを再起動します。問題が解決しない場合は、シスコの担当者に連絡してください。	警告
55112	B2BUA の誤設定（B2BUA misconfiguration）	B 側の ICE モードが無効です（Invalid B side ICE mode）	サービスを再起動します。問題が解決しない場合は、シスコの担当者に連絡してください。	警告

ID	タイトル	説明	ソリューション	重大度
55113	B2BUA の誤設定（B2BUA misconfiguration）	B 側のネクストホップの活性モードが無効です（Invalid B side next hop liveness mode）	サービスを再起動します。問題が解決しない場合は、シスコの担当者に連絡してください。	警告
55114	B2BUA の誤設定（B2BUA misconfiguration）	B 側のネクストホップ モードが無効です（Invalid B side next hop mode）	サービスを再起動します。問題が解決しない場合は、シスコの担当者に連絡してください。	警告
55115	B2BUA の誤設定（B2BUA misconfiguration）	コマンド リスニング ポートが無効です（Invalid command listening port）	サービスを再起動します。問題が解決しない場合は、シスコの担当者に連絡してください。	警告
55116	B2BUA の誤設定（B2BUA misconfiguration）	デバッグ ステータス パスが無効です（Invalid debug status path）	サービスを再起動します。問題が解決しない場合は、シスコの担当者に連絡してください。	警告
55117	B2BUA の誤設定（B2BUA misconfiguration）	サービスが無効です（Invalid service）	サービスを再起動します。問題が解決しない場合は、シスコの担当者に連絡してください。	警告
55118	B2BUA の誤設定（B2BUA misconfiguration）	ソフトウェア文字列が無効です（Invalid software string）	サービスを再起動します。問題が解決しない場合は、シスコの担当者に連絡してください。	警告

ID	タイトル	説明	ソリューション	重大度
55119	B2BUA の誤設定（B2BUA misconfiguration）	トランスコーディング サービスの連絡先アドレスのURI形式が無効です（Invalid URI format of transcoding service contact address）	サービスを再起動します。問題が解決しない場合は、シスコの担当者に連絡してください。	警告
55120	B2BUA の誤設定（B2BUA misconfiguration）	トランスコーディング サービスの暗号化モードが無効です（Invalid transcoding service encryption mode）	サービスを再起動します。問題が解決しない場合は、シスコの担当者に連絡してください。	警告
55121	B2BUA の誤設定（B2BUA misconfiguration）	トランスコーディング サービスのICE モードが無効です（Invalid transcoding service ICE mode）	サービスを再起動します。問題が解決しない場合は、シスコの担当者に連絡してください。	警告
55122	B2BUA の誤設定（B2BUA misconfiguration）	トランスコーディング サービスのネクスト ホップの活性モードが無効です（Invalid transcoding service next hop liveness mode）	サービスを再起動します。問題が解決しない場合は、シスコの担当者に連絡してください。	警告
55123	B2BUA の誤設定（B2BUA misconfiguration）	トランスコーディング サービスのトランス ポート タイプの設定が誤っています（The transcoding service transport type is misconfigured）	サービスを再起動します。問題が解決しない場合は、シスコの担当者に連絡してください。	警告

ID	タイトル	説明	ソリューション	重大度
55124	B2BUA の誤設定（B2BUA misconfiguration）	必須 TURN サービスの設定が誤っています（The mandatory TURN server setting is misconfigured）	サービスを再起動します。問題が解決しない場合は、シスコの担当者に連絡してください。	警告
55125	B2BUA の誤設定（B2BUA misconfiguration）	Expressway のネクスト ホップのホスト設定が無効です（Invalid Expressway next hop host configuration）	サービスを再起動します。問題が解決しない場合は、シスコの担当者に連絡してください。	警告
55126	B2BUA の誤設定（B2BUA misconfiguration）	Expressway の許可済みホスト IP アドレスが無効です（Invalid Expressway authorized host IP address）	サービスを再起動します。問題が解決しない場合は、シスコの担当者に連絡してください。	警告
55127	B2BUA の誤設定（B2BUA misconfiguration）	FQDN 設定がないため、B2BUA アプリケーションを起動できません（Cannot start B2BUA application because FQDN configuration is missing）	**システムホスト名**と**ドメイン名**を [DNS] ページで設定してから B2BUA サービスを再起動します。	警告
55128	B2BUA の誤設定（B2BUA misconfiguration）	IPv4 インターフェイスのアドレス設定がないため、B2BUA アプリケーションを起動できません（Cannot start B2BUA application because IPv4 interface address configuration is missing）	LAN 1 IPv4 アドレスを「IP」ページで設定してから B2BUA サービスを再起動します	警告

ID	タイトル	説明	ソリューション	重大度
55129	B2BUA の誤設定（B2BUA misconfiguration）	クラスタ名の設定がないため、B2BUA アプリケーションを起動できません（Cannot start B2BUA application because cluster name configuration is missing）	クラスタ名を [クラスタリング（Clustering）] ページで設定します。	警告
55130	B2BUA の誤設定（B2BUA misconfiguration）	クラスタ名が無効です（Invalid cluster name）	クラスタ名を確認してから B2BUA サービスを再起動します	警告
55131	B2BUA の誤設定（B2BUA misconfiguration）	セッション更新間隔が無効です（Invalid session refresh interval）	B2BUA の設定（詳細設定）を確認してから B2BUA サービスを再起動します。	警告
55132	B2BUA の誤設定（B2BUA misconfiguration）	コール リソース制限が無効です（Invalid call resource limit）	サービスを再起動します。問題が解決しない場合は、シスコの担当者に連絡してください。	警告
55133	B2BUA の誤設定（B2BUA misconfiguration）	B2BUA セッションの更新間隔が最小セッション更新間隔より小さくなっています（The B2BUA session refresh interval is smaller than the minimum session refresh interval）	両方の設定を [B2BUA の設定（B2BUA configuration）]（詳細設定）で確認してから B2BUA サービスを再起動します。	警告

ID	タイトル	説明	ソリューション	重大度
55134	B2BUA の誤設定（B2BUA misconfiguration）	最小セッション更新間隔が無効です（Invalid minimum session refresh interval）	B2BUA の設定（詳細設定）を確認してから B2BUA サービスを再起動します。	警告
55135	B2BUA 設定の警告（B2BUA configuration warning）	Microsoft の信頼できるホスト デバイスが多数設定されています。そのため、パフォーマンスに影響を与える可能性があります。極端な場合は、コールが接続に十分なネットワーク リソースにアクセスできなくなる可能性があります（A large number of Microsoft trusted host devices have been configured; this may impact performance, or extreme cases it may prevent calls from accessing enough network resources to connect）	「B2BUA の信頼できるホスト（B2BUA trusted hosts）」ページでトポロジを確認し、信頼できるホスト デバイスの数を減らすようにします。	警告
55137	B2BUA の誤設定（B2BUA misconfiguration）	VCS マルチストリーム モードが無効です（Invalid VCS multistream mode）	B2BUA の設定（詳細設定）を確認してから B2BUA サービスを再起動します。	警告
55139	B2BUA の誤設定（B2BUA misconfiguration）	VCS マルチストリーム モードが無効です（Invalid VCS multistream mode）	B2BUA の設定（詳細設定）を確認してから B2BUA サービスを再起動します。	警告

ID	タイトル	説明	ソリューション	重大度
55142	RDP TCP/UDP ポートが不足しています（Insufficient RDP TCP/UDP ports）	RDP コールの最大数をサポートするには TCP/UDP ポートの数が足りません（There is an insufficient number of TCP/UDP ports to support the maximum number of RDP calls）	B2BUA 設定の RDP TCP/UDP ポート範囲を拡大します	警告

表 *38* : 管理コネクタアラーム

ID	タイトル	説明	ソリューション	重大度
60050	（ハイブリッドサービス）接続エラー（[Hybrid services] Connectivity error）	Cisco Collaboration Cloud のアドレス：<*string*> に到達できませんでした	<*string*> または <*string*> を確認するか、またはネットワーク ユーティリティ <*string*> を使用して、このアドレスを確認します。	エラー
60051	（ハイブリッドサービス）通信エラー（[Hybrid services] Communication error）	Cisco Collaboration Cloud からの HTTP エラー コード <*string*>（アドレス：<*string*>）	ハイブリッドサービスのステータスを確認します。問題が続くようであれば、Cisco Collaboration Cloud の管理者へお問い合わせください。	エラー

ID	タイトル	説明	ソリューション	重大度
60052	（ハイブリッド サービス）通信エラー（[Hybrid services] Communication error）	<*string*>	<*string*>、<*string*>、<*string*> のアドレスを確認してください。アドレスが問題の原因でない場合は、Cisco Collaboration Cloud 管理者にお問い合わせください。	エラー
60053	（ハイブリッド サービス）アクセス エラー（[Hybrid services] Access error）	<*string*>	Cisco Collaboration Cloud 管理者にお問い合わせください。	エラー
60054	（ハイブリッド サービス）コネクタ インストール エラー（[Hybrid services] Connector install error）	<*string*>	Cisco Collaboration Cloud 管理者にお問い合わせください。	エラー
60055	（ハイブリッド サービス）証明書が無効なためダウンロードに失敗しました（[Hybrid services] Download failed because the certificate was not valid）	<*string*>	Expressway の信頼できる CA リストで、受信した証明書に署名した CA を確認します。	エラー
60056	（ハイブリッド サービス）証明書が無効なためアップグレードに失敗しました（[Hybrid services] Upgrade failed because certificate was not valid）	<*string*>	Expressway の信頼できる CA リストで、受信した証明書に署名した CA を確認します。	エラー

ID	タイトル	説明	ソリューション	重大度
60057	（ハイブリッドサービス）証明書名が一致しなかったためアップグレードに失敗しました（[Hybrid services] Upgrade failed because certificate name did not match）	<*string*>	<*string*>からの証明書の CN または SAN がホスト名と一致していることを確認します。	エラー
60058	（ハイブリッドサービス）CA 証明書が見つからなかったため接続に失敗しました（[Hybrid services] Connection failed because the CA certificate was not found）	<*string*> から証明書に署名したルート CA が Expressway の信頼できる CA リストにないため、Cisco Collaboration Cloud に安全に接続できません。	Expressway の信頼できる CA リストを更新し、受信した証明書に署名した CA を含めます。	エラー
60059	（ハイブリッドサービス）証明書名が一致しなかったため接続に失敗しました（[Hybrid services] Connection failed because the certificate name did not match）	<*string*> からの証明書に、ホスト名と一致する CN または SAN 属性がありませんでした。	リモート サーバからの証明書の CN または SAN がホスト名と一致していることを確認します。	エラー

ID	タイトル	説明	ソリューション	重大度
60060	（ハイブリッドサービス）証明書が検証されなかったため接続に失敗しました（[Hybrid services] Connection failed because the certificate was not validated）	Expressway が <*string*> からの証明書を検証できませんでした。これは、Expressway が CA を信頼していないか、または証明書が現在有効でないために発生する可能性があります。	Expressway <*string*> リストに、受信した証明書に署名した CA のルート証明書が含まれていることを確認します。CA 証明書が最新であり、失効していないことを確認します。<*string*> が設定されており、Expressway が同期していることを確認します。これらの潜在的原因を排除できる場合は、シスコにご連絡ください。送信したサーバ証明書が無効である可能性があります。	エラー
60061	（ハイブリッドサービス）ユーザの選択によりアップグレードが阻止されました（[Hybrid services] Upgrade prevented by user choice）	以前に、Cisco Collaboration Cloud によって現在アドバタイズされているコネクタのアップグレードが拒否されました。次のバージョンが利用可能になると、自動アップグレードが継続されます。アドバタイズされるバージョン：<*string*>	コネクタのバージョンを確認します。	アラート
60062	（ハイブリッドサービス）コネクタ ディセーブル エラー（[Hybrid services] Connector disable error）	<*string*>	Cisco Collaboration Cloud 管理者にお問い合わせください。	エラー

ID	タイトル	説明	ソリューション	重大度
60063	（ハイブリッドサービス）コネクタ イネーブル エラー（[Hybrid services] Connector enable error）	<*string*>	Cisco Collaboration Cloud 管理者にお問い合わせください。	エラー
60064	（ハイブリッドサービス）コネクタが予期せず実行していません（[Hybrid services] Connector unexpectedly not running）	<*string*>	停止したコネクタを再起動します。そのコネクタが最近アップグレードされた場合は、以前のバージョンにロールバックしてください。エラーが解消されない場合は、Cisco Collaboration Cloud 管理者に連絡してください。	エラー
60065	（ハイブリッドサービス）コネクタのバージョンの不一致（[Hybrid services] Connector version mismatch）	<*string*>	Cisco Collaboration Cloud 管理者にお問い合わせください。	エラー
60066	（ハイブリッドサービス）定期的な認証の更新に失敗しました（[Hybrid services] Routine authentication refresh failed）	Expressway は定期的に <*string*> を通じて認証を更新しますが、今回は成功しませんでした。Expressway は <*string*> 分以内に再試行します。	この問題が解消されない場合は、Cisco Collaboration Cloud 管理者に連絡してください。	エラー
60067	（ハイブリッドサービス）接続エラー（[Hybrid services] Connectivity Error）	<*string*> にアクセスしようとしてエラーが発生しました。Expressway は約 <*string*> 秒後に再試行します。	<*string*> をチェックし、エラーが続く場合はネットワークの問題を確認してください。	エラー

ID	タイトル	説明	ソリューション	重大度
60068	（ハイブリッド サービス）Cisco Collaboration Cloud からの無効な応答（[Hybrid services] Invalid responses from Cisco Collaboration Cloud）	<*string*> から無効なデータが受信されました。	Cisco Collaboration Cloud の予定されたアドレスがあるか確認します。	エラー
60069	（ハイブリッド サービス）サービス コネクタなし（[Hybrid services] No service connectors）	ハイブリッド サービスに登録されていますが、サービス コネクタがインストールされていません。管理コネクタがアクティブで、Cisco Collaboration Cloud への不要な接続を確立しています。	シスコ クラウド コラボレーション管理に移動し、組織が 1 つ以上のハイブリッド サービスを使用する権利があることを確認します。ハイブリッド サービスを使用していない場合は、この Expressway を <*string*> することを強く推奨します。	アラート
60070	（ハイブリッド サービス）HTTP 例外（[Hybrid services] HTTP exception）	<*string*> からの HTTP 応答を処理中に受信された例外：<*string*>	問題が解消されない場合は、Cisco Collaboration Cloud 管理者に連絡してください。	エラー
60071	（ハイブリッド サービス）キー エラー（[Hybrid services] Key error）	このシステムは、コネクタ ファイルのデータ エラーのために正しく登録できませんでした。関連するサービスは、正常に登録されているように見えても、期待どおりに機能しません。	再度登録を試みてください（最初に登録を解除する必要がある場合があります）。問題が解消されない場合は、Cisco Collaboration Cloud 管理者に連絡してください。	エラー

ID	タイトル	説明	ソリューション	重大度
60072	（ハイブリッドサービス）サポートされていない Expressway バージョン（[Hybrid services] Unsupported Expressway version）	ご使用の Expressway のバージョンは、ハイブリッド サービスではサポートされなくなりました。ハイブリッド サービスを引き続き使用するには、新しいバージョンにアップグレードする必要があります。	cisco.com にある最新の Expressway バージョンにアップグレードしてください。	アラート
60073	（ハイブリッドサービス）サポートされていない Expressway バージョン（[Hybrid services] Unsupported Expressway version）	Cisco Expressway の新バージョンがリリースされました。最新の機能を使用し、次の Expressway バージョンがリリースされたときにサポートされていないハイブリッド サービスの展開を避けるため、できるだけ早くこのバージョンにアップグレードすることをお勧めします。現在のバージョンは次の Expressway リリースまでサポートされます。	cisco.com にある最新の Expressway バージョンにアップグレードしてください。	アラート
60074	（ハイブリッドサービス）接続エラー（[Hybrid services] Connectivity error）	Cisco Collaboration Cloud に到達できません。	Teams Service のネットワーク要件を確認し、強調表示されているプロキシガイドラインに従います。	error

表 *39 :* カレンダーコネクタ アラーム

ID	タイトル	説明	ソリューション	重大度
60100	Microsoft Exchange サーバが到達不能（Microsoft Exchange Server unreachable）	Microsoft Exchange Server へのアクセス エラーが発生しました。これが解決されるまで、カレンダー サービス要求および通知は処理されません。詳細情報：これには <*string*> が含まれます。最後の既知のエラー：<*string*>	Microsoft Exchange Server とカレンダー コネクタ間のネットワークの接続性を確認します。Microsoft Exchange Server 上の負荷を確認します。	クリティカル
60101	Microsoft Exchange Server アクセスが拒否されました（Microsoft Exchange Server access denied）	Microsoft Exchange Server へのアクセスが拒否されました。これが解決されるまで、カレンダー サービス要求および通知は処理されません。詳細情報：これには <*string*> が含まれます。最後の既知のエラー：<*string*>	サービス アカウントに有効なクレデンシャルと正しいアクセス許可があり、ロックされていないことを確認します。	クリティカル

ID	タイトル	説明	ソリューション	重大度
60102	Microsoft Exchange Server 証明書を検証できません（Microsoft Exchange Server certificate not validated）	Microsoft Exchange Server の証明書を検証できませんでした。これが解決されるまで、カレンダーサービス要求および通知は処理されません。詳細情報：これには *<string>* が含まれます。最後の既知のエラー：*<string>*	Microsoft Exchange Server 証明書が有効なことを確認します。	クリティカル
60103	Microsoft Exchange Server のバージョンがサポートされていません（Microsoft Exchange Server version unsupported）	設定された Microsoft Exchange Server のバージョンがサポートされていません。詳細情報：*<string>*	Microsoft Exchange Server をサポートされているバージョンにアップグレードする必要があります。	クリティカル
60104	Microsoft Exchange Server が設定されていません（No Microsoft Exchange Server configured）	Microsoft Exchange Server の設定が構成されていないため、カレンダー コネクタが停止しました。	カレンダー コネクタに少なくとも 1 つの Microsoft Exchange Server を設定し、それを再度有効にします。	クリティカル

ID	タイトル	説明	ソリューション	重大度
60110	Microsoft Exchange Autodiscover が到達不能（Microsoft Exchange Autodiscover unreachable）	ユーザの自動検出中に Microsoft Exchange Server へのアクセスでタイムアウトが発生しました。これが解決されるまで、カレンダー サービス要求および通知は処理されません。詳細情報：これには <*string*> が含まれます。最後の既知のエラー：<*string*>	Microsoft Exchange Autodiscover Server とカレンダー コネクタ間のネットワークの接続性を確認します。	クリティカル
60111	Microsoft Exchange Autodiscover のアクセスが拒否されました（Microsoft Exchange Autodiscover access denied）	ユーザの自動検出中に Microsoft Exchange Server へのアクセスが拒否されました。これが解決されるまで、カレンダー サービス要求および通知は処理されません。詳細情報：これには <*string*> が含まれます。最後の既知のエラー：<*string*>	サービス アカウントに有効なクレデンシャルと正しいアクセス許可があり、ロックされていないことを確認します。	クリティカル

ID	タイトル	説明	ソリューション	重大度
60112	Microsoft Exchange Autodiscover 証明書を検証できません（Microsoft Exchange Autodiscover certificate not validated）	自動検出中に、Microsoft Exchange Server の証明書を検証できませんでした。これが解決されるまで、カレンダーサービス要求および通知は処理されません。詳細情報：これには <*string*> が含まれます。最後の既知のエラー：<*string*>	サーバ証明書が有効なことを確認します。	クリティカル
60113	リダイレクトされた Microsoft Exchange Autodiscovery URL が信頼されていません（Redirected Microsoft Exchange Autodiscovery URL not trusted）	リダイレクトされた Microsoft Exchange Autodiscovery URL が変更され、信頼されていません。詳細情報：<*string*>	Exchange サービス レコードを開き、再度レコードを保存します。新しいリダイレクション URL が信頼されることを確認します。	クリティカル
60120	Microsoft Exchange Autodiscover LDAP が到達不能（Microsoft Exchange Autodiscover LDAP unreachable）	自動検出中に Microsoft LDAP サーバへのアクセスでタイムアウトが発生しました。これが解決されるまで、カレンダーサービス要求および通知は処理されません。詳細情報：これには <*string*> が含まれます。最後の既知のエラー：<*string*>	Microsoft Exchange Autodiscover LDAP Server とカレンダー コネクタ間のネットワークの接続性を確認します。	クリティカル

ID	タイトル	説明	ソリューション	重大度
60121	Microsoft Exchange Autodiscover LDAP のアクセスが拒否されました（Microsoft Exchange Autodiscover LDAP access denied）	自動検出中に Microsoft LDAP Server へのアクセスが拒否されました。これが解決されるまで、カレンダー サービス要求および通知は処理されません。詳細情報：これには <*string*> が含まれます。最後の既知のエラー：<*string*>	サービス アカウントに有効なクレデンシャルと正しいアクセス許可があり、ロックされていないことを確認します。	クリティカル
60130	Microsoft Exchange Server のユーザ サブスクリプションの失敗（Microsoft Exchange Server user subscription failure）	;<*string*> ユーザが Microsoft Exchange Server に登録できませんでした（<string> users failed to subscribe to Microsoft Exchange Server(s).）詳細情報：ユーザには <*string*> が含まれています。	Microsoft Exchange Server がビジー状態でないこと、および Microsoft Exchange Server とカレンダー コネクタとの間のネットワークの接続性を確認します。	エラー
60131	SMTP アドレスにメールボックスがありません（SMTP address has no mailbox）	メールボックスが関連付けられていない複数の（<*string*>）SMTP アドレスが検出されました（Multiple (<string>) SMTP address(es) have been detected with no associated mailbox(es).）詳細情報：<*string*>	ターゲット メールボックスが完全に有効で、ターゲット サーバが正しいことを確認します。	エラー

ID	タイトル	説明	ソリューション	重大度
60132	サブスクリプションが動作していません（Subscription not operational）	カレンダー サービスが Microsoft Exchange Server から 1 人以上のユーザの通知を受信していません。これが対処されるまで、これらのユーザのカレンダー サービス要求および通知は処理されません。	Microsoft Exchange Server が正しく機能していることと、ネットワークに接続していることを確認します。この状態が続く場合は、カレンダー サービスの再起動を検討してください。	エラー
60140	会議通知の着信率が高すぎます（Meeting notification incoming rate too high）	<*string*> カレンダー サービス ユーザの着信会議通知率が高すぎます（The incoming meeting notification rate is too high for <string> Calendar Serviceuser(s).）詳細情報：ユーザには <*string*> が含まれています。	Microsoft Exchange Server でユーザのメールボックスを確認します。	エラー
60142	会議の処理時間が長すぎます（Meeting processing time too long）	カレンダー サービスの会議の処理時間が、少なくとも 1 人のユーザに対して 5 分のしきい値を超えています。	Microsoft Exchange Server とカレンダー サービスでユーザの通知率を確認します。	エラー
60150	Cisco Collaboration Cloud のモニタ サービスが到達不能（Cisco Collaboration Cloud Monitor Service unreachable）	現在必要なクラウド サービスに到達できません。これが解決されるまで、カレンダー サービス要求および通知は処理されません。詳細情報：<*string*>	インターネットへの接続を確認します。	クリティカル

ID	タイトル	説明	ソリューション	重大度
60151	Cisco Collaboration Cloud のモニタサービスへのアクセスが拒否されました（Cisco Collaboration Cloud Monitor Service access denied）	Cisco Collaboration Cloud サービスへのアクセスが拒否されました。これが解決されるまで、カレンダーサービス要求および通知は処理されません。詳細情報：<*string*>	テクニカル サポートにお問い合わせください。	クリティカル
60152	Cisco Collaboration Cloud API サービスが到達不能（Cisco Collaboration Cloud API Service unreachable）	現在必要なクラウド サービスに到達できません。これが解決されるまで、カレンダーサービス要求および通知は処理されません。詳細情報：<*string*>	インターネットへの接続を確認します。	クリティカル
60153	Cisco Collaboration Cloud API サービスへのアクセスが拒否されました（Cisco Collaboration Cloud API Service access denied）	Cisco Collaboration Cloud サービスへのアクセスが拒否されました。これが解決されるまで、カレンダーサービス要求および通知は処理されません。詳細情報：<*string*>	テクニカル サポートにお問い合わせください。	クリティカル
60154	暗号化サービスからのキーの取得が失敗しました（Retrieving key from encryption service failed）	カレンダー コネクタが既存のキーを取得できなかったか、または暗号化サービスから新しいキーを生成する要求を失敗しました。詳細情報：暗号化サービスは <*string*> です。	暗号化サービスがオンになっていることを確認します。	エラー

ID	タイトル	説明	ソリューション	重大度
60155	Cisco Collaboration Cloud のモニタ メッセージ サービスが接続されていません（Cisco Collaboration Cloud Monitor message service not connected）	カレンダー コネクタが Cisco Collaboration Cloud のモニタ メッセージ サービスに接続できませんでした。詳細情報：クラウド サービス ルートは <*string*> です。	Cisco Collaboration Cloud のモニタ メッセージ サービスへのネットワーク接続を確認します。	クリティカル
60156	Cisco Collaboration Cloud API メッセージ サービスが接続されていません（Cisco Collaboration Cloud API message service not connected）	カレンダー コネクタが Cisco Collaboration Cloud API メッセージ サービスに接続できませんでした。詳細情報：クラウド サービス ルートは <*string*> です。	Cisco Collaboration Cloud API メッセージ サービスへのネットワーク接続を確認します。	クリティカル
60160	Cisco Collaboration Meeting Rooms（CMR）サービスに到達不能またはアクセスが拒否されました（Cisco Collaboration Meeting Rooms (CMR) service unreachable or access denied）	Cisco Collaboration Meeting Rooms（CMR）サービスに現在到達できないか、またはアクセスが拒否されました。これが解決されるまで、@webex 会議は処理されません。詳細情報：CMR サービスのサイト名には <*string*> が含まれています。	ネットワーク接続と CMR サービスに設定されているアカウント クレデンシャルを確認します。	エラー

ID	タイトル	説明	ソリューション	重大度
60161	WebEx ユーザ アカウントが使用できません（WebEx user account not available）	<*string*> Webex ユーザアカウントは利用できません。アカウントの問題が解決されるまで、これらのユーザの @webex 会議は処理されません。詳細情報：影響を受けるユーザには <*string*> が含まれています。	WebEx サービス アカウントとユーザ アカウントを確認します。ユーザに WebEx アカウントがあるか、アカウントがロックアウトされていないか、非アクティブ化されていないか、または Personal Room が無効になっているか確認します。	警告
60162	Cisco WebEx 管理者パスワードの有効期限が切れている、または無効です（Cisco WebEx administrator password has expired or invalid）	期限切れまたは無効な管理者パスワードが原因で Cisco WebEx サービスにアクセスできません。これが解決されるまで、影響を受けるサイトでの @webex 会議は処理されません。詳細情報：Webex サービス サイト名には <*string*> が含まれています。	影響を受ける WebEx サーバで、期限切れまたは無効な管理者パスワードを変更します。	エラー
60163	Cisco WebEx 管理者パスワードの有効期限が切れます（Cisco WebEx administrator password expiring）	<*string*> サイトの Cisco Webex 管理者パスワードの有効期限が間もなく切れます。詳細情報：管理者パスワードの期限が切れる Webex サービス サイトには <*string*> が含まれています。	影響を受ける WebEx サーバで、期限が切れる管理者パスワードを変更します。	警告

ID	タイトル	説明	ソリューション	重大度
60164	Cisco WebEx 管理者アカウントがロックアウトされました（Cisco WebEx administrator account locked out）	管理者アカウントがロックアウトされているため、Cisco WebEx サービスにアクセスできません。これが解決されるまで、影響を受けるサイトでの @webex 会議は処理されません。詳細情報：Webex サービスサイト名には <*string*> が含まれています。	影響を受ける WebEx サーバで管理者アカウントをロック解除します。	エラー
60170	管理コネクタが実行されていません（Management Connector not running）	管理コネクタが実行されていないため、カレンダーコネクタが動作していません。	**[アプリケーション（Applications）]** > **[クラウド拡張（Cloud Extensions）]** > **[コネクタ管理（Connector Management）]** に移動して、管理コネクタを開始します。	エラー
60171	管理コネクタが動作していません（Management Connector not operational）	管理コネクタが動作していないため、カレンダーコネクタが動作していません。	管理コネクタのステータスを確認し、必要に応じて再起動します。	エラー
60190	カレンダー コネクタが動作していません（Calendar Connector not operational）	1 つ以上のクラウド サービスおよび/またはオンプレミス サービスが動作していないため、カレンダーコネクタが動作していません。	詳細については、カレンダー コネクタのステータスを確認してください。	クリティカル

表 *40 :* コールコネクタアラーム

ID	タイトル	説明	ソリューション	重大度
60300	ユーザにはディレクトリ番号が設定されていません。（The user is not configured with any directory numbers.）	ユーザにディレクトリ番号が設定されていません（The user is not configured with a primary directory number）：user[<*string*>]:<*string*>	Unified CM でユーザに関連付けられているデバイスに少なくとも 1 つの回線を追加します。	警告
60301	ユーザのコントロール リストに有効なデバイスがありません。（The user has no valid devices in the control list.）	ユーザのコントロール リストに有効なデバイスがありません（The user has no valid devices in the control list）：user[<*string*>]:<*string*>	回線が少なくとも 1 つある有効なデバイスを少なくとも 1 つ Unified CM のユーザに関連付けます。	警告
60302	ユーザにディレクトリ URI が設定されていません。（The user is not configured with a directory URI.）	ユーザにディレクトリ URI が設定されていません（The user is not configured with a primary directory number）：user[<*string*>]:<*string*>	Unified CM のユーザのアカウント設定で、ディレクトリ URI の値を入力します。	警告
60303	この電子メールアドレスを持つユーザが見つかりませんでした（Could not find a user with this email address.）	この電子メールアドレスを持つユーザを見つけることができませんでした（Could not find a user with this email address）：user[<*string*>]:<*string*>	Unified CM でユーザの電子メールアドレスを入力します。	警告

ID	タイトル	説明	ソリューション	重大度
60304	電子メールとディレクトリ URI の不一致（Email mismatch with directory URI）	ユーザの電子メールがディレクトリ URI と一致しません（The user's email does not match the directory URI ）：user[<*string*>]: <*string*>	ユーザの電子メールとディレクトリ URI が Unified CM で同じであることを確認します。	警告
60305	ユーザのプライマリ ディレクトリ URI が、プライマリ回線用に設定されたディレクトリ URI と一致しません（The user's primary directory URI does not match the directory URI configured for the primary line.）	ユーザのプライマリ ディレクトリ URI が、プライマリ回線用に設定されたディレクトリ URI と一致しません（The user's primary directory URI does not match the directory URI configured for the primary line）：user[<*string*>]: <*string*>	Unified CM で、関連するデバイス上のユーザのディレクトリ URI と回線 URI が同一であることを確認します。	警告
60306	ユーザが有効な CTI リモートデバイスで構成されていません（The user is not configured with a valid CTI remote device.）	ユーザが有効な CTI リモートデバイスで構成されていません（The user is not configured with a valid CTI remote device）：user[<*string*>]: <*string*>	Unified CM で CTI リモート デバイスを設定し、ユーザのコントロール リストに追加します。	警告

ID	タイトル	説明	ソリューション	重大度
60307	Webex SIP アドレスを Webex クラウドにルーティングできません（Webex SIP address cannot be routed to the Webex cloud.）	ユーザの Webex SIP アドレスを Webex クラウドにルーティングできません（The user's Webex SIP address cannot be routed to the Webex cloud）） : user[<*string*>]: <*string*>	Unified CM で再ルーティング コーリング サーチ スペースと、Webex SIP アドレス パターン用に設定されたパーティションを確認します。	エラー
60308	すでに使用中の Webex SIP アドレスです（Webex SIP address is already in use.）	ユーザの Webex SIP アドレスは別のユーザに割り当てられています（The User's Webex SIP address is assigned to another user） : user[<*string*>]: <*string*>	Cisco Unified CM Administration で、ユーザのリモート接続先がデバイスですでに使用されているかどうかを確認してください。	エラー
60309	ユーザのリモート接続先が削除されませんでした（The user's remote destination was not removed.）	ユーザがコール サービス接続で非アクティブ化されたときに、リモート接続先が削除されませんでした（When the user is deactivated for Call Service Connect, the remote destination was not removed. ） : user[<*string*>]: <*string*>	Cisco Unified CM Administration で、ユーザのリモート接続先がデバイスですでに使用されているかどうかを確認してください。Unified CM ユーザの CTI リモート デバイスからリモート接続先を削除します。	警告

ID	タイトル	説明	ソリューション	重大度
60310	Unified CM でユーザの Webex SIP アドレスを追加できません（Unable to add the user's Webex Teams SIP address in Unified CM.）	Unified CM でユーザの Webex SIP アドレスを追加できません（Unable to add the user's Webex SIP address in Unified CM）：user[<*string*>]:<*string*>	Cisco Unified CM Administration で、手動で作成済みのリモート接続先が存在する場合はそれを削除します。これにより、コール コネクタによって自動的にリモート接続先が再作成されます。	エラー
60311	ユーザにプライマリ ディレクトリ番号が設定されていません。（The user is not configured with a primary directory number.）	ユーザにプライマリ ディレクトリ番号が設定されていません（The user is not configured with a primary directory number）：user[<*string*>]:<*string*>	Unified CM でユーザのプライマリ ディレクトリ番号を設定します。	警告
60315	自動 Spark リモート デバイスが省略された名前で作成されました（Automatic Spark Remote Device created with truncated name）	コールサービス接続のアクティベーション中に、自動 Spark リモート デバイス名が短縮されました。- ユーザ [<*string*>]<*string*> に nam <*string*>のデバイスがあります。	この問題を避けるには、ユーザ ID を 15 文字以下にする必要があります。	警告

ID	タイトル	説明	ソリューション	重大度
60316	Spark リモート デバイスを削除できません（Unable to delete Spark Remote Device）	コール コネクタは、コール サービス接続が非アクティブ化された後、Spark リモート デバイスを削除できません（Call connector cannot delete the Spark remote device after Call Service Connect was deactivated）：user[<*string*>]: <*string*>	Unified CM でエラー メッセージを確認します。	警告
60317	コール コネクタは、Unified CM に CTI リモート デバイスを作成できません（Call connector is unable to create a CTI Remote Device in Unified CM.）	コール コネクタは、Unified CM に CTI リモート デバイスを作成できません（Call connector is unable to create a CTI Remote Device in Unified CM）：user[<*string*>]: <*string*>	競合する可能性のあるデバイス名を確認します。	警告
60318	コール コネクタが CTI リモート デバイスを作成するには、ユーザはモビリティを有効にする必要があります（Users must have mobility enabled for call connector to create a CTI remote device.）	ユーザがモビリティを有効にしなければ、コールコネクタは Webex のリモート デバイスを作成できません（Users must have mobility enabled for call connector to create a Remote Device for Webex Teams）：user[<*string*>]: <*string*>	Unified CM ユーザがモビリティに対し有効になっているかどうか確認します。	警告

ID	タイトル	説明	ソリューション	重大度
60319	Unified CM AXL への接続が失われました（Connectivity to Unified CM AXL Service lost）	Unified CM AXL サービスへの接続が失われました（Connectivity to Unified CM AXL Service lost）：Unified CM [<*string*>]	AXL サービスが Unified CM 上で動作しているかどうかを確認し、ネットワークの問題を解決します。	error
60320	Unified CM CTIManager サービスに接続できません（Cannot connect to Unified CM CTIManager Service.）	Unified CM CTIManager サービスに接続できません（Cannot connect to Unified CM CTIManager Service）：Unified CM [<*string*>]	CTIManager サービスが Unified CM 上で動作しているかどうかを確認し、ネットワークの問題を解決します。	エラー
60321	証明書検証が失敗しました（Certificate verification failed）	Webex クラウドから提供された証明書を検証できなかったため、コール コネクタが停止しました（Call Connector stopped as it could not verify the certificate provided by the Webex cloud.）	Expressway 登録プロセスの一環として証明書をダウンロードし、Expressway-C を登録します。それでもエラーが続く場合は、Expressway-C 信頼ストア内の Webex 証明書を更新します。	エラー
60322	完全修飾ドメイン名が無効です（Fully Qualified Domain Name is not valid）	完全修飾ドメイン名が空です（Fully Qualified Domain Name is Empty）：user[<*string*>]: <*string*>	Unified CM エンタープライズ パラメータに完全修飾ドメイン名を追加します。手順については、マニュアルを参照してください。	警告

ID	タイトル	説明	ソリューション	重大度
60323	完全修飾ドメイン名が無効です（Fully Qualified Domain Name is not valid）	完全修飾ドメイン名にワイルドカードが含まれています（Fully Qualified Domain Name contains wild card）：user[<*string*>]: <*string*>	Unified CM エンタープライズ パラメータにワイルドカードを含まない新しい完全修飾ドメイン名を追加します。	警告
60324	Unified CM AXL サーバに到達できません（Unable to reach the Unified CM AXL server.）	Unified CM AXL サーバに到達できません（Unable to reach the Unified CM AXL server）：server[<*string*>]	コール コネクタと Unified CM 間のネットワーク接続を確認します。	エラー
60325	Unified CM AXL サーバで認証できません（Unable to authenticate with Unified CM AXL server）	Unified CM AXL サーバで認証できません：[<*string*>]	コール コネクタの設定時に指定した Unified CM ユーザ クレデンシャルを確認します。	エラー
60326	Unified CM AXL 通信用に設定されたユーザが承認されていません（User configured for Unified CM AXL communication is not authorized）	Unified CM AXL 通信用に設定されたユーザが承認されていません（User configured for Unified CM AXL communication is not authorized）：server [<*string*>]	コール コネクタの UCM 設定で設定されているユーザのアクセス ロールを確認します。	エラー
60327	Unified CM が設定されていません（No Unified CM Configured）	Unified CM がコール コネクタに設定されていません。	コール コネクタに Unified CM を設定します。	警告

ID	タイトル	説明	ソリューション	重大度
60328	ユーザが複数の Unified CM クラスタに対して設定されています。（The user is configured for more than one Unified CM cluster.）	ユーザが複数の Unified CM クラスタに対して設定されています：user[<*string*>]: <*string*>	このコール コネクタに設定されているすべての Unified CM でユーザのホーム クラスタ設定を確認します。	警告
60329	コール コネクタが無効な Webex SIP アドレスを受信しました。（Call connector received an invalid Webex SIP Address.）	無効な Spark SIP アドレス：user[<*string*>]: <*string*> の場合	ユーザおよびデバイス設定を確認します。マニュアルに従って再設定を行い、必要に応じて有効な Webex SIP アドレスを再設定します。	エラー
60330	ユーザが複数の CTI リモートデバイスで設定されています（The user is configured with more than one CTI remote device.）	ユーザが複数の CTI リモートデバイスで設定されています（The user is configured with more than one CTI remote device）：user[<*string*>]: <*string*>	Unified CM でユーザのコントロールリストから余分なデバイスを削除します。	警告
60331	CTI リモートデバイスには設定されたディレクトリ番号はありません。（The CTI remote device has no configured directory numbers.）	CTI リモートデバイスにディレクトリ番号が設定されていません（The CTI remote device has no configured directory numbers）：user[<*string*>]: <*string*>	Unified CM で、ユーザに関連付けられた CTI リモート デバイスに少なくとも 1 つの回線を追加します。	警告

ID	タイトル	説明	ソリューション	重大度
60332	Unified CM CTIManager で、リモート接続先を更新する要求がタイムアウトしました。（In Unified CM CTIManager, a request timed out to update the remote destination.）	Unified CM CTIManager で、リモート接続先の更新要求がタイムアウトしました（In Unified CM CTIManager, a request timed out to update the remote destination）：user[<*string*>]: <*string*>	Unified CM CTIManager サービスが起動して実行していることを確認します。	警告
60333	Unified CM CTIManager に接続できません（Unable to connect to Unified CM CTIManager）	Unified CM CTIManager に接続できません。	コール コネクタと Unified CM 間のネットワーク接続を確認します。	エラー
60334	Unified CM CTIManager に設定されたユーザを認証できません（Unable to authenticate user configured for Unified CM CTIManager）	Unified CM CTIManager に設定されたユーザを認証できません。	コール コネクタの Unified CM 設定でユーザ クレデンシャルを確認します。	エラー
60335	Unified CM のデバイス所有権の競合（Conflict in Device Ownership on Unified CM.）	Unified CM がデバイスの所有者との競合を示しています（Unified CM shows a conflict with the owner of the device）：user[<*string*>]: <*string*>	Unified CM で設定を確認します。	警告

ID	タイトル	説明	ソリューション	重大度
60336	ユーザ用に作成しようとしたCTIリモート デバイスと同じ名前のデバイスが存在します（A device exists with the same name as the CTI remote device tried to create for the user.）	作成しようとしたCTIリモートデバイスと同じ名前のデバイスが存在します（A device exists with the same name as the CTI remote device tried to create）：user[<*string*>]: <*string*>	Unified CMでデバイス名と設定を確認します。	警告
60337	CTIリモートデバイスがユーザ用に正常に作成されましたが、コールイベントを受信するデバイス サブスクリプションが失敗しました。（CTI remote device successfully created for the user, but the device subscription to receive call events failed.）	CTIリモートデバイスがユーザ用に正常に作成されましたが、コールイベントを受信するデバイス サブスクリプションが失敗しました（CTI remote device successfully created for the user, but the device subscription to receive call events failed）：user[<*string*>]: <*string*> の場合	Unified CMで設定を確認し、再試行します。	警告
60338	Unified CMの無効なリモート接続先（Invalid remote destination on Unified CM.）	Unified CMの無効なリモート接続先（Invalid remote destination on Unified CM）：user[<*string*>]: <*string*> の場合	マニュアルのユーザおよびリモートデバイスの設定手順に従って、有効なWebex SIPアドレスを作成します。	警告

ID	タイトル	説明	ソリューション	重大度
60339	このユーザのリモート接続先の制限を超えています（The user exceeds the remote destination limit.）	Webex SIP アドレスを作成できません。Cisco Unified CM でのこのユーザのリモート接続先の制限を超えています（Unable to create a Webex SIP address. The user exceeds the remote destination limit in Cisco Unified CM.）	未使用のリモート接続先を削除するか、制限を増やします。	エラー
60340	ユーザにホームクラスタが設定されていません。（The user is not configured with a home cluster.）	このユーザのホーム クラスタは設定されていません（The user is not configured with a home cluster）：user[<*string*>]: <*string*>	Unified CM でこのユーザのホームクラスタを設定します。	警告
60341	コール コネクタの構成が無効です（Call connector invalid configuration）	無効な構成の理由（Invalid Configuration reason）=[<*string*>]	設定エラーを修正してから、コール コネクタを再起動します。	エラー
60342	コール コネクタのバージョンがWebex クラウドと一致しません（Call connector version mismatch with the Webex cloud）	[<*string*>] 状態の無効なメッセージを受信しました。Webex クラウドとバージョンが一致していない可能性があります（Invalid message received in state [<string>], potential version mismatch with the Webex cloud）	admin.webex.com にアクセスし、[サービス（Services）]>[ハイブリッド コール（Hybrid Call）]>[すべて表示（View all）] に移動してリソースを開き、最新のコール コネクタ ソフトウェアにアップグレードします。	エラー

ID	タイトル	説明	ソリューション	重大度
60343	Webex SIP アドレスが 48 文字の制限を超えています（Webex SIP Address exceeds the 48 character limit.）	ユーザの Webex SIP アドレスを追加できません（Unable to add Webex SIP address for a user.）Unified CM は、48 文字を超えるリモート接続先をサポートしていません（Unable to add Webex SIP for a user. Unified CM does not support remote destinations that are longer than 48 characters.）	Webex SIP アドレスが 48 文字の制限を超えないようにデバイス名を変更します。	エラー
60344	ユーザのディレクトリ URI が組織の検証済みドメイン リストにありません（User's directory URI is not in the organization's verified domain list）	ユーザのディレクトリ URI が組織の検証済みドメイン リストにありません（User's directory URI is not in the organization's verified domain list）：user[<*string*>]: <*string*> にドメイン リスト = <*string*> があります。	ユーザのディレクトリ URI と、このユーザの検証済みドメインのリストを確認します。	警告
60345	Unified CM クラスタのデータキャッシュの構築に失敗しました（Failed to Build Unified CM Cluster Data-Cache）	Unified CM クラスタのデータキャッシュの構築に失敗しました（Failed to Build Unified CM Cluster Data-Cache）：server[<*string*>]	AXL サービスが Unified CM クラスタ ノード上で動作しているかどうかを確認し、ネットワークの問題を解決します。	エラー

ID	タイトル	説明	ソリューション	重大度
60346	Cisco Collaboration Cloud サービスとの認証の失敗（Authentication Failure with Cisco Collaboration Cloud Services.）	Expressway で利用できる認証クレデンシャルが無効です。	Expressway に移動し、**[アプリケーション（Applications）]** > **[ハイブリッドサービス（Hybrid Services）]** > **[コネクタ管理（Connector Management）]** でクラウドに再登録します。	エラー
60347	Cisco Collaboration Cloud サービスとの承認の失敗（Authorization Failure with Cisco Collaboration Cloud Services.）	この Expressway が Cisco Collaboration Cloud サービスにアクセスするためのロールまたはアクセス範囲が無効です。	Expressway に移動し、**[アプリケーション（Applications）]** > **[ハイブリッドサービス（Hybrid Services）]** > **[コネクタ管理（Connector Management）]** でクラウドに再登録します。	エラー
60348	Cisco Collaboration Cloud からの接続がダウンしています（Connection from the Cisco Collaboration Cloud is down.）	Cisco Collaboration Cloud からの接続がダウンしています。	ネットワーク DNS またはプロキシ設定を確認してから、再度試してください。	エラー
60349	Cisco Collaboration Cloud への接続がダウンしています（Connection to the Cisco Collaboration Cloud is down.）	Cisco Collaboration Cloud への接続がダウンしています。	ネットワーク DNS またはプロキシ設定を確認してから、再度試してください。	エラー

ID	タイトル	説明	ソリューション	重大度
60350	組織のハイブリッド ボイスメールを有効にできません（Cannot enable hybrid voicemail for your organization.）	組織のハイブリッド ボイスメールを有効にできません。	このエラーが解消されない場合は、試用チームに連絡するか、または Cisco Spark アプリを通じてフィードバックを送信してサポートにお問い合わせください。	警告
60351	コール コネクタが無効なハイブリッド ボイスメール設定を検出しました（Call connector detected an invalid hybrid voicemail configuration.）	コール コネクタが無効なハイブリッド ボイスメール設定を検出しました。	ハイブリッド ボイスメールの展開手順を確認します。このエラーが解消されない場合は、試用チームに連絡するか、または Cisco Spark アプリを通じてフィードバックを送信してサポートにお問い合わせください。	エラー
60352	UCM にこのディレクトリ URI を持つディレクトリ番号が存在しません（No Directory Number exists in UCM with this directory URI）	UCM にこのディレクトリ URI を持つディレクトリ番号が存在しません。	このディレクトリ URI を使用して UCM にディレクトリ番号を設定します。	エラー
60353	Unified CM で AXL 変更通知が開始されません（AXL Change Notification is not started at Unified CM.）	Unified CM で AXL 変更通知が開始されません（AXL Change Notification is not started at Unified CM）：server[<*string*>]	Unified CM のエンタープライズ パラメータで AXL 変更通知を有効にします。	エラー

表 *41 :* 重要なイベントアラーム

ID	タイトル	説明	ソリューション	重大度
90001	緊急コール	緊急コールは、ゾーン（ゾーン名）、送信元 IP（*IP* アドレス）から（*[user@example.com]*）によって実行されています。	NA	emergency

表 *42 :* テレメトリーアラーム

ID	タイトル	説明	ソリューション	重大度
60800	CollectD サービスダウン	Core Telemetry Service が動作しない	テレメトリ—コネクタを無効にして有効にし、ネットワークの問題を確認します。問題が解決しない場合は、シスコのサポート担当者に連絡してください。	クリティカル
60801	クラウドに接続された UC 接続のダウン	クラウドに接続されている UC への接続が切断されている	テレメトリ—コネクタを無効にして有効にし、ネットワークの問題を確認します。問題が解決しない場合は、シスコのサポート担当者に連絡してください。	クリティカル

ID	タイトル	説明	ソリューション	重大度
60802	設定エラー	設定の更新または設定の取得の失敗	テレメトリ—コネクタを無効にして有効にし、ネットワークの問題を確認します。また、クラスタまたはノードが認証され、適切にオンボードされているかも確認します。それでも問題が解決しない場合は、シスコのサポート担当者に連絡してください。	エラー（Error）
60803	認証エラー	1 つ以上のリモートコネクタ接続またはトランザクション処理で認証に失敗しました	テレメトリ—コネクタを無効にして有効にし、ネットワークの問題を確認します。また、クラスタまたはノードが承認され、適切にオンボードされ、必要な証明書がインストールされているかも確認します。それでも問題が解決しない場合は、シスコのサポート担当者に連絡してください。	エラー（Error）

ID	タイトル	説明	ソリューション	重大度
60804	CA 証明書の読み取りエラー	CA 証明書の読み取りまたは組み込みに失敗しました	• また、クラスタまたはノードが承認され、適切にオンボードされ、必要な証明書がインストールされていることを確認します。 • 必要な証明書を再インストールします。 • テレメトリ—コネクタを無効にして有効にし、ネットワークの問題を確認します。 問題が解決しない場合は、シスコのサポート担当者に連絡してください。	エラー（Error）

ID	タイトル	説明	ソリューション	重大度
60805	無効な証明書エラー	無効な証明書がロードされている	• また、クラスタまたはノードが承認され、適切にオンボードされ、有効な証明書がインストールされていることを確認します。 • 正しい証明書および有効な証明書を再インストールします。 • テレメトリ—コネクタを無効にして有効にし、ネットワークの問題を確認します。 問題が解決しない場合は、シスコのサポート担当者に連絡してください。	エラー（Error）

コマンド リファレンス — xConfiguration

設定の個々の項目を設定および変更するには、`xConfiguration` グループのコマンドを使用します。各コマンドは、メインの要素と、その後に続く 1 つ以上のサブ要素から構成されます。

既存の設定に関する情報を取得するには、次のように入力します。

- `xConfiguration`：現在のすべての設定を返す場合。
- `xConfiguration <element>`：指定した要素とそのすべてのサブ要素を返す場合。
- そのサブ要素の設定を返す `xConfiguration <element> <subelement>`

各 `xConfiguration` コマンドの使用に関する情報を取得するには、次のように入力します。

- `xConfiguration ? xConfiguration`：コマンドで使用可能なすべての要素のリストを返す場合。
- `xConfiguration ??xConfiguration` ：コマンドで使用可能なすべての要素のリストと、各要素の値空間、説明、およびデフォルト値を返す場合。
- `xConfiguration <element> ?`：使用可能なすべてのサブ要素とそれらの値空間、説明、およびデフォルト値を返す場合。
- `xConfiguration <element> <sub-element> ?`：使用可能なすべてのサブ要素とそれらの値空間、説明、およびデフォルト値を返す場合

設定項目を設定するには、コマンドを次のように入力します。次の表記法を使用して、各コマンドに有効な値を山カッコ内に示し、その後に各コマンドを示します。

表 *43 : CLI* リファレンスで使用されるデータ表記規則

書式	意味
<0..63>	整数値が必要であることを示します。数値は最小値と最大値を示しています。この例では、0 ～ 63 の範囲内の値にする必要があります。
<S: 7,15>	**S** は引用符で囲まれた文字列値が必要であることを示します。数値は文字列の最小文字数と最大文字数を示します。この例では、文字列の長さを 7 ～ 15 文字にする必要があります。
<Off/Direct/Indirect>	コマンドの有効な一連の値を示します。値は引用符で囲まないでください。
[1..50]	角カッコはこの特定の項目を複数設定できることを示します。各項目には示された範囲内のインデックスが割り当てられます。 たとえば、`IP Route [1..50] Address <S: 0,39>` は最大 50 の IP ルートを指定でき、各ルートには最大 39 文字の長さのアドレスが必要であることを意味します。

xConfiguration コマンド

次の表に、使用可能なすべての **xConfiguration** コマンドを示します。

表 *44 : xConfiguration CLI* リファレンス

xConfiguration Administration DeviceProvisioning: <On/Off> Expressway Web ユーザインターフェイスで **[システム（System）]** > **[TMS プロビジョニング拡張サービス（TMS Provisioning Extension services）]** ページにアクセスさせるかどうかを指定します。アクセス可能な場合、このページから、Cisco TelePresence Management Suite Provisioning Extension（Cisco TMSPE）とユーザ、デバイス、FindMe、電話帳のプロビジョニング サービスに接続できます。デフォルト：Off *On*：**[システム（System）]** > **[TMS プロビジョニング拡張サービス（TMS Provisioning Extension services）]** ページにアクセス可能になり、この Expressway のプロビジョニングサービスを設定できます。 *Off*：**[システム（System）]** > **[TMS プロビジョニング拡張サービス（TMS Provisioning Extension services）]** ページにはアクセスできません。 例：`xConfiguration Administration DeviceProvisioning: On`
xConfiguration Administration HTTP Mode: <On/Off> HTTP コールを HTTPS ポートにリダイレクトするかどうかを決定します。変更を有効にするには、システムを再起動する必要があります。デフォルトは On です。 *On*：コールは HTTPS にリダイレクトされます。 *Off*：HTTP アクセスは使用できません。 例：`xConfiguration Administration HTTP Mode: On`
xConfiguration Administration HTTPS Mode: <On/Off> Web インターフェイス経由で Expressway にアクセスできるかどうかを決定します。Web インターフェイスと TMS アクセスの両方を有効にするには、これを On にする必要があります。変更を有効にするには、システムを再起動する必要があります。デフォルトは On です。 例：`xConfiguration Administration HTTPS Mode: On`
xConfiguration Administration LCDPanel Mode: <On/Off> Expressway の前面の LCD パネルでシステムを識別するかどうかを制御します。デフォルトは On です。 *On*：システム名とアクティブな IP アドレスのうち最初のアドレスが表示されます。 *Off*：LCD パネルにはシステムに関する識別情報は表示されません。 例：`xConfiguration Administration LCDPanel Mode: On`
xConfiguration Administration SSH Mode: <On/Off> SSH と SCP を使用して Expressway にアクセスできるかどうかを決定します。変更を有効にするには、システムを再起動する必要があります。デフォルトは On です。 例：`xConfiguration Administration SSH Mode: On`

xConfiguration Alarm Notification Email Custom Alarm ID: <String>

1 つ以上のカスタマイズされたアラーム通知が設定されている場合。カスタマイズまたは無効化された通知のアラーム ID。

xConfiguration Alarm Notification Email Custom Disable Notify: <Off>

1 つ以上のカスタマイズされたアラーム通知が設定されている場合。

xConfiguration Alarm Notification Email Custom Email: <String>

1 つ以上のカスタマイズされたアラーム通知が設定されている場合。選択したアラーム通知の送信に使用される電子メール ID（最大長 254）。

xConfiguration Alarm Notification Email Destination Alert: <S: 0, 254>

厳しい属性 「Alert」 を使用するアラームの電子メール通知先。

例：`xConfiguration Alarm Notification Email Destination Alert: 「ucadmin@example.com」`

xConfiguration Alarm Notification Email Destination Critical: <S: 0, 254>

厳しい属性 「Critical」 を使用するアラームの電子メール通知先。

例：`xConfiguration Alarm Notification Email Destination Alert: 「ucadmin@example.com」`

xConfiguration Alarm Notification Email Destination Debug: <S: 0, 254>

厳しい属性 「Debug」 を使用するアラームの電子メール通知先。

例：`Configuration Alarm Notification Email Destination Debug: 「uctech@example.com」`

xConfiguration Alarm Notification Email Destination Emergency: <S: 0, 254>

厳しい属性 「Emergency」 を使用するアラームの電子メール通知先。

例：`xConfiguration Alarm Notification Email Destination Emergency: 「ert@example.com」`

xConfiguration Alarm Notification Email Destination Error: <S: 0, 254>

厳しい属性 「Error」 を使用するアラームの電子メール通知先。

例：`xConfiguration Alarm Notification Email Destination Error: 「ucadmin@example.com」`

xConfiguration Alarm Notification Email Destination Info: <S: 0, 254>

厳しい属性 「Info」 を使用するアラームの電子メール通知先。

例：`xConfiguration Alarm Notification Email Destination Info: 「ucadmin@example.com」`

xConfiguration Alarm Notification Email Destination Notice: <S: 0, 254>

厳しい属性 「Notice」 を使用するアラームの電子メール通知先。

例：`xConfiguration Alarm Notification Email Destination Notice: 「ucadmin@example.com」`

xConfiguration Alarm Notification Email Destination Warning: <S: 0, 254>

厳しい属性 「Warning」 を使用するアラームの電子メール通知先。

例：`xConfiguration Alarm Notification Email Destination Warning: 「ucadmin@example.com」`

xConfiguration Alarm Notification SMTP Mode: <On/Off>

アラームベースの電子メール通知を使用するかどうかを決定します。デフォルトはオフです。

例：`xConfiguration Alarm Notification SMTP Mode: On`

xConfiguration Alarm Notification SMTP Server Email: <S: 0, 254>

アラームベースの電子メール通知が設定されている通知先アドレスに送信される送信元電子メール。

例：`Alarm Notification SMTP Server Email: 「ucadmin@example.com」`

xConfiguration Alarm Notification SMTP Server Host: <S: 0, 128>

アラームベースの電子メール通知の送信に使用するSMTPサーバのIPアドレスまたはFQDN。

例：`xConfiguration Alarm Notification SMTP Server Host: 「email.example.com」`

xConfiguration Alarm Notification SMTP Server Password: <Password>

アラームベースの電子メール通知の送信に使用される SMTP サーバのパスワード。

例：`xConfiguration Alarm Notification SMTP Server Password: 「{cipher}$NNxx1xxx-xxxx-xxxx-xxxn-fnxnxNNNxxxN$1$xX+xnXnnXxnnxxnnnXXXnxnXXxnxXxxx/XXxnxnxxxx=」`

xConfiguration アラーム通知 SMTP サーバポート：

アラームベースの電子メール通知の送信に使用する SMTP サーバのポート番号。デフォルトは 587 です。

例：`xConfiguration Alarm Notification SMTP Server Port: 587`

xConfiguration Alternates Cluster Name: <S: 0,128>

この Expressway クラスタ宛の SRV レコードに使用する完全修飾ドメイン名。たとえば、「「cluster1.example.com」」など。名前には、文字、数字、ハイフン、および下線のみ使用できます。

警告：このExpresswayでユーザアカウントを設定した後にクラスタ名を変更した場合は、その新しいクラスタ名を使用してユーザアカウントを再設定する必要がある場合があります。

例：`Configuration Alternates Cluster Name: 「Regional」`

xConfiguration Alternates ConfigurationPrimary: <1..6>

他のすべてのピアに設定を複製するプライマリがこのクラスタ内のどのピアかを指定します。クラスタは、ローカル Expressway を含む最大 6 つのピアで構成されます。

例：`xConfiguration Alternates ConfigurationPrimary: 1`

xConfiguration Alternates Peer [1..6] Address: <S: 0, 128>

この Expressway が所属するクラスタ内の 1 つのピアのアドレスを指定します。クラスタは、ローカル Expressway を含む最大 6 つのピアで構成されます。シスコはされたFQDNを使用することをお勧めします。これは、IPアドレスにすることができます。

例：`xConfigurationの 1つのピアアドレス:「「cluster1peer3.example.com」」`

xConfiguration ApacheModReqTimeOut

1 つの短縮コマンドを使用して、要求のタイムアウトに使用可能なすべてのプロパティを設定できます。

例：`xConfiguration ApacheModReqTimeout Apachehead:20 Apachebody:20 Status:On`

xConfiguration ApacheModReqTimeOut Apachebody: <0..120>

Apache Web サーバが要求の本文を待機する秒数を変更します。タイムアウトの期限が切れる前に要求の本文全体を受信しなかった場合、Apache はタイムアウト エラーを返します。デフォルト：20。

例：`xConfiguration ApacheModReqTimeout Apachebody:20`

xConfiguration ApacheModReqTimeOut Apacheheader: <0..120>

Apache Web サーバが要求のヘッダーを待機する秒数を変更します。タイムアウトの期限が切れる前に要求のヘッダー全体を受信しなかった場合、Apacheはタイムアウトエラーを返します。デフォルト：20。

例：`xConfiguration ApacheModReqTimeout Apacheheader:20`

xConfiguration ApacheModReqTimeOut Status: <On/Off>

カスタムの Apache 要求のタイムアウトを切り替えます。切り替えを省略した場合は、タイムアウトのステータスが表示されます。

On：デフォルトの Apache 要求タイムアウトよりも `Apachebody` と `Apacheheader` の設定（またはデフォルト）が優先されます。

Off：`Apachebody` と `Apacheheader` は影響を与えません。Apache 要求のタイムアウトはデフォルトで 300 秒に設定されています。

例：`xConfiguration ApacheModReqTimeout Status:On`

xConfiguration Applications ConferenceFactory Alias: <S:0,60>

Multiway 機能がアクティブになったときにエンドポイントがダイヤルするエイリアス。これは、Multiway 機能の開始に使用できるすべてのエンドポイントに事前に設定する必要があります。

例：`xConfiguration Applications ConferenceFactory Alias: 「multiway@example.com」`

xConfiguration Applications ConferenceFactory Mode: <On/Off>

Mode オプションを使用して Conference Factory アプリケーションを有効または無効にできます。デフォルト：Off

例：`xConfiguration Applications ConferenceFactory Mode: Off`

xConfiguration Applications ConferenceFactory Range End: <1..65535>

会議エイリアスの生成に使用するテンプレート内の %% を置き換える範囲の最後の数値。デフォルト：65535。

例：`xConfiguration Applications ConferenceFactory Range End: 30000`

xConfiguration Applications ConferenceFactory Range Start: <1..65535>

会議エイリアスの生成に使用するテンプレート内の %% を置き換える範囲の最初の数値。デフォルト：65535。

例：`xConfiguration Applications ConferenceFactory Range Start: 10000`

xConfiguration Applications ConferenceFactory Template: <S:0,60>

Multiway 会議を MCU に作成するためにダイヤルするよう Expressway がエンドポイントに通知するエイリアス。このエイリアスは、完全修飾 SIP エイリアスとして MCU にルーティングする必要があります。

例：`xConfiguration Applications ConferenceFactory Template: 「563%%@example.com」`

xConfiguration Applications External Status [1..10] Filename: <S:0,255>

外部アプリケーション用にアタッチするステータスが含まれている XML ファイル。

例：`xConfiguration Applications External Status 1 Filename: 「foo.xml」`

xConfiguration Applications External Status [1..10] Name: <S:0,64>

ステータスが参照される外部アプリケーションの記述名。

例：`xConfiguration Applications External Status 1 Name: 「foo」`

xConfiguration Authentication ADS ADDomain: <S: 0,255>

Expressway が AD ドメインに参加するときに使用する Kerberos レルム。注：このフィールドは大文字と小文字を区別します。

例：`xConfiguration Authentication ADS ADDomain: 「CORPORATION.INT」`

xConfiguration Authentication ADS Clockskew: <1..65535>

Kerberos メッセージが無効だと見なされる前に、Expressway と KDC 間で許可される最大クロック スキュー（秒単位）。デフォルトは 300 です。

例：`xConfiguration Authentication ADS Clockskew: 300`

xConfiguration Authentication ADS CipherSuite: <S:1,2048>

Expressway が AD ドメインに参加するために TLS 暗号化 LDAP 接続を実行するときに使用する暗号スイートを指定します。このコマンドは「OpenSSL 暗号」形式の文字列を受け入れます（https://www.openssl.org/docs/man1.0.2/apps/ciphers.html#CIPHER-LIST-FORMAT を参照してください）。

例：`xConfiguration Authentication ADS CipherSuite: 「HIGH:MEDIUM:!ADH:!aNULL:!eNULL:-AES128-SHA256:@STRENGTH」`

xConfiguration Authentication ADS DC [1..5] Address: <S: 0,39>

Expressway が AD ドメインに参加するときに使用できるドメイン コントローラのアドレス。特定の AD を指定しなかった場合は、AD の検出に DNS SRV クエリが使用されます。

例：`xConfiguration Authentication ADS DC 1 Address: 「192.168.0.0」`

xConfiguration Authentication ADS Encryption: <Off/TLS>

ADS サーバへの LDAP 接続に使用する暗号化を設定します。

（注） 無効な暗号を削除しましたが、保持された 1 つの暗号（eTYPE-アーク FOUR-HMAC-MD5）を削除して、後方互換性を確保しました。

デフォルトは TLS です。

[Off]：暗号化は使用されません。

TLS：TLS 暗号化を使用します。

例：`xConfiguration Authentication ADS Encryption: TLS`

xConfiguration Authentication ADS KDC [1..5] Address: <S: 0,39>

AD ドメインへ接続するときに使用する Kerberos 配布センター（KDC）のアドレス。特定の KDC を指定しなかった場合は、KDC の検出に DNS SRV クエリが使用されます。

例：`xConfiguration Authentication ADS KDC 1 Address: 「192.168.0.0」`

xConfiguration Authentication ADS KDC [1..5] Port: <1..65534>

Expressway が AD ドメインに参加するときに使用できる KDC のポートを指定します。デフォルト：88。

例：`xConfiguration Authentication ADS KDC 1 Port: 88`

xConfiguration Authentication ADS MachineName: <S: 0..15>

Expressway が AD ドメインに参加するときに使用するデフォルトの NETBIOS マシン名を上書きします。

例：`xConfiguration Authentication ADS MachineName: 「short_name」`

xConfiguration Authentication ADS MachinePassword Refresh: <On/Off>

AD ドメインに参加するときに、この Samba クライアントがマシンのパスワードを 7 日おきに更新する必要があるかどうかを決定します。デフォルトは On です。

例：`xConfiguration Authentication ADS MachinePassword Refresh: On`

xConfiguration Authentication ADS Mode: <On/Off>

Expressway が AD との関係の形成を試行するかどうかを示します。デフォルト：Off

例：`xConfiguration Authentication ADS Mode: On`

xConfiguration Authentication ADS SPNEGO: <Enabled/Disabled>

クライアント（Expressway）がサーバ（AD ドメイン コントローラ）で認証するときに SPNEGO（Simple and Protected GSSAPI Negotiation Mechanism）を使用するかどうかを示します。デフォルト：有効.

例：`xConfiguration Authentication ADS SPNEGO: Enabled`

xConfiguration Authentication ADS SecureChannel: <Auto/Enabled/Disabled>

Expressway から AD ドメイン コントローラに送信されたデータをセキュア チャネル経由で送信するかどうかを示します。デフォルト：[Auto]

例：`xConfiguration Authentication ADS SecureChannel: Auto`

xConfiguration Authentication ADS Workgroup: <S: 0,15>

Expressway が AD ドメインに参加するときに使用するワークグループ。

例：`xConfiguration Authentication ADS Workgroup: 「corporation」`

xConfiguration Authentication Account Admin Account [1..n] AccessAPI: <On/Off>

このアカウントがアプリケーション プログラミング インターフェイス（API）を使用してシステムのステータスと設定にアクセスできるかどうかを決定します。デフォルトは On です。

例：`xConfiguration Authentication Account Admin Account 1 AccessAPI: On`

xConfiguration Authentication Account Admin Account [1..n] AccessWeb: <On/Off>

このアカウントが Web インターフェイスを使用してシステムにログインできるかどうかを決定します。デフォルトは On です。

例：`xConfiguration Authentication Account Admin Account 1 AccessWeb: On`

xConfiguration Authentication Account Admin Account [1..n] Enabled: <On/Off>

アカウントが有効になっているか、無効になっているかを示します。無効なアカウントへのアクセスは拒否されます。デフォルトは On です。

例：`xConfiguration Authentication Account Admin Account 1 Enabled: On`

xConfiguration Authentication Account Admin Account [1..n] Name: <S: 0, 128>

管理者アカウントのユーザ名。

例：`xConfiguration Authentication Account Admin Account 1 Name: 「bob_smith」`

xConfiguration Authentication Account Admin Account [1..n] Password: <Password>

この管理者が Expressway へのログインに使用するパスワード。

例：`xConfiguration Authentication Account Admin Account 1 Password: 「abcXYZ_123」`

xConfiguration Authentication Account Admin Group [1..n] AccessAPI: <On/Off>

このグループのメンバーがアプリケーション プログラミング インターフェイス（API）を使用してシステムのステータスおよび設定にアクセスできるかどうかを決定します。デフォルトは On です。

例：`xConfiguration Authentication Account Admin Group 1 AccessAPI: On`

xConfiguration Authentication Account Admin Group [1..n] AccessWeb: <On/Off>

このグループのメンバーが Web インターフェイスを使用してシステムにログインできるかどうかを決定します。デフォルトは On です。

例：`xConfiguration Authentication Account Admin Group 1 AccessWeb: On`

xConfiguration Authentication Account Admin Group [1..n] Enabled: <On/Off>

グループが有効になっているか、無効になっているかを示します。無効になっているグループのメンバーへのアクセスは拒否されます。デフォルトは On です。

例：`xConfiguration Authentication Account Admin Group 1 Enabled: On`

xConfiguration Authentication Account Admin Group [1..n] Name: <S: 0, 128>

管理者グループの名前。

例：`xConfiguration Authentication Account Admin Group 1 Name: 「administrators」`

xConfiguration Authentication Certificate Crlcheck: <None/Peer/All>

HTTPS クライアント証明書を証明書失効リスト（CRL）と照合して確認するかどうかを指定します。CRL データは CRL の管理ページを使用して Expressway にアップロードされます。デフォルトは All です。

[なし（None）]：CRL チェックは実行されません。

[ピア（Peer）]：クライアントの証明書を発行した CA に関連付けられた CRL のみを確認します。

[すべて（All）]：クライアントの証明書を発行した CA の信頼できる証明書チェーン内のすべての CRL を確認します。

例：`xConfiguration Authentication Certificate Crlcheck: All`

xConfiguration Authentication Certificate Crlinaccessible: <Ignore/Fail>

たとえば、失効の送信元に通信できない、または適切な失効リストが提示されないなど、失効ステータスを確立できない場合の失効リストの確認の動作を制御します。デフォルトは Ignore です。

Ignore：失効していないものとして証明書を処理します。

Fail：失効しているものとして証明書を処理します（したがって、TLS 接続は許可しません）。

例：`xConfiguration Authentication Certificate Crlinaccessible: Ignore`

xConfiguration Authentication Certificate Mode: <NotRequired/Validation/Authentication>

クライアント システム（通常は Web ブラウザ）が HTTPS を使用して Expressway と通信するために必要なセキュリティ レベルを制御します。デフォルトは NotRequired です。

NotRequired：クライアントシステムはどのような形式の証明書も提示する必要はありません。

Validation：クライアントシステムは、信頼できる認証局（CA）が署名した有効な証明書を提示する必要があります。Not required から Certificate validation に変更した場合は、再起動が必要です。

Authentication：クライアントシステムは、信頼できる CA が署名した有効な証明書を提示する必要があり、その証明書にはクライアントの認証クレデンシャルを含める必要があります。このモードを有効にすると、標準のログイン メカニズムは使用できなくなります。

例：`xConfiguration Authentication Certificate Mode: NotRequired`

xConfiguration Authentication Certificate UsernameRegex: <String>

Expressway に提示するクライアント証明書に適用する正規表現。(? regex) を使用してキャプチャ グループの名前を指定することで、照合するサブパターンを関連付けられたテンプレートで置き換えることができます。デフォルトは /Subject:.*CN= (? ([^,\]|(\,))*)/m

例：`xConfiguration Authentication Certificate UsernameRegex: 「/Subject:.*CN= (? ([^,\]|(\,))*)/m」`

xConfiguration Authentication Certificate UsernameTemplate: <String>

正規表現に使用する固定テキストとキャプチャしたグループ名の組み合わせを含んだテンプレート。各キャプチャ グループ名は # を使用して、たとえば prefix#Group1#suffix のように区切ります。各キャプチャ グループ名は正規表現の処理から取得されたテキストに置き換えられます。置換された文字列は、ユーザの認証クレデンシャル（ユーザ名）として使用されます。デフォルトは #captureCommonName# です。

例：`xConfiguration Authentication Certificate UsernameTemplate: 「#captureCommonName#」`

xConfiguration Authentication H350 BindPassword: <S: 0, 60>

LDAP サーバにバインドするときに使用するパスワードを設定します。

例：`xConfiguration Authentication H350 BindPassword: 「abcXYZ_123」`

xConfiguration Authentication H350 BindSaslMode: <None/DIGEST-MD5>

LDAP サーバにバインドするときに使用する SASL（Simple Authentication and Security Layer）のメカニズム。デフォルトは DIGEST-MD5 です。

None：メカニズムを使用しません。

[DIGEST-MD5]：DIGEST-MD5 メカニズムを使用します。

例：`xConfiguration Authentication H350 BindSaslMode: DIGEST-MD5`

xConfiguration Authentication H350 BindUserDn: <S: 0, 500>

LDA Pサーバにバインドするときに使用するユーザの識別名を設定します。

例：`xConfiguration Authentication H350 BindUserDn: 「manager」`

xConfiguration Authentication H350 BindUserName: <S: 0, 500>

LDAP サーバにバインドするときに使用するユーザ名を設定します。SASL を使用する場合にのみ適用されます。

例：`xConfiguration Authentication H350 BindUserName: 「manager」`

xConfiguration Authentication H350 DirectoryBaseDn: <S: 0, 500>

LDAP サーバに接続するときに使用するユーザの識別名を設定します。

例：`xConfiguration Authentication H350 DirectoryBaseDn: 「dc=example,dc=company,dc=com」`

xConfiguration Authentication H350 LdapEncryption: <Off/TLS>

LDAP サーバへの接続に使用する暗号化を設定します。デフォルト：TLS。

[Off]：暗号化は使用されません。

TLS：TLS 暗号化を使用します。

例：`xConfiguration Authentication H350 LdapEncryption: TLS`

xConfiguration Authentication H350 LdapServerAddress: <S: 0, 256>

デバイス認証のための LDAP クエリを実行するときに使用する LDAP サーバの IP アドレスまたは完全修飾ドメイン名

例：`xConfiguration Authentication H350 LdapServerAddress: 「ldap_server.example.com」`

xConfiguration Authentication H350 LdapServerAddressResolution: <AddressRecord/ServiceRecord>

LDAP サーバアドレスが FQDN として指定されている場合の解決方法を定義します。デフォルトは AddressRecord です。

[アドレス レコード（Address record）]：DNS A レコードまたは AAAA レコード ルックアップ。

[SRV レコード（SRV record）]：DNS SRV レコード ルックアップ。

例：`xConfiguration Authentication H350 LdapServerAddressResolution: AddressRecord`

xConfiguration Authentication H350 LdapServerPort: <1..65535>

デバイス認証のための LDAP クエリを実行するときに使用する LDAP サーバの IP ポートを設定します。通常、セキュリティで保護されていない接続は 389 を使用します。デフォルト：389

例：`xConfiguration Authentication H350 LdapServerPort: 389`

xConfiguration Authentication H350 Mode: <On/Off>

デバイス認証への H.350 ディレクトリの使用を有効または無効にします。デフォルト：Off

例：`xConfiguration Authentication H350 Mode: Off`

xConfiguration Authentication LDAP AliasOrigin: <LDAP/Endpoint/Combined>

エイリアスの確認および登録方法を決定します。デフォルトは LDAP です。

LDAP：エンドポイントによって提示されたエイリアスを LDAP データベースのリストにあるエイリアスと照合して確認します。

Endpoint：エンドポイントによって提示されたエイリアスを使用します。LDAP データベースにあるエイリアスはすべて無視されます。

Combined：エンドポイントが提示したエイリアスのほかに LDAP データベースのリストにあるエイリアスも使用します。

例：`xConfiguration Authentication LDAP AliasOrigin: LDAP`

xConfiguration Authentication Password: <S: 0, 215>

別のシステムでの認証時に Expressway が使用するパスワード。プレーンテキストの最大長は 128 文字で、暗号化されます。注：トラバーサル クライアント ゾーンには適用されません。

例：`xConfiguration Authentication Password: 「password123」`

xConfiguration Authentication Remote Digest Cache ExpireCheckInterval: <0..65535>

ダイジェスト認証のキャッシュ有効期限の秒単位の確認間隔。デフォルトは 600 です。

例：`xConfiguration Authentication Remote Digest Cache ExpireCheckInterval: 600`

xConfiguration Authentication Remote Digest Cache Lifetime: <0..43200>

秒単位のダイジェスト認証暫定ハッシュのライフタイム。デフォルトは 600 です。

例：`xConfiguration Authentication Remote Digest Cache Lifetime: 600`

xConfiguration Authentication Remote Digest Cache Limit: <0..65535>

ダイジェスト認証のキャッシュ有効期限の秒単位の確認間隔。デフォルトは 10000 です。

例：`xConfiguration Authentication Remote Digest Cache Limit: 10000`

xConfiguration Authentication Remote Digest Cache Mode: <On/Off>

ダイジェスト認証キャッシュを有効にするかどうかを制御します。デフォルト：[オン（On）]

例：`xConfiguration Authentication Remote Digest Cache Mode: On`

xConfiguration Authentication StrictPassword Enabled: <On/Off>

ローカル管理者アカウントのパスワードは、それらが受け入れられる前に最小レベルの複雑性を満たしているかどうかを決定します。さらに、パスワードは「「abc」」や「「123」」などの連続する文字を多く含んでいたり、違う文字がほとんど含まれていないディクショナリの単語に基づいたものや、あるいは回文にはしないでください。デフォルトは Off です。

On：ローカル管理者パスワードは複雑度の要件を満たす必要があります。

Off：パスワードの複雑度は確認されません。

例：`xConfiguration Authentication StrictPassword Enabled: Off`

xConfiguration Authentication StrictPassword MaximumConsecutiveRepeated: <0..255>

同じ文字を連続して繰り返すことができる最大回数。値を 0 にするとこの確認が無効になります。デフォルト：0

例：`xConfiguration Authentication StrictPassword MaximumConsecutiveRepeated: 0`

xConfiguration Authentication StrictPassword MinimumClasses: <0..4>

使用する必要がある文字クラスの最小数。文字クラスには、数字、大文字、小文字、特殊文字の 4 種類があります。これらすべての使用を求めずに 2 ～ 3 の異なる文字クラスを必須とする場合に、この設定を使用します。値を 0 にするとこの確認が無効になります。デフォルト：[0]。

例：`xConfiguration Authentication StrictPassword MinimumClasses: 0`

xConfiguration Authentication StrictPassword MinimumDigits: <0..255>

使用する必要がある数字の最小数。値を0にするとこの確認が無効になります。デフォルト：2。

例：`xConfiguration Authentication StrictPassword MinimumDigits: 2`

xConfiguration Authentication StrictPassword MinimumLength: <6..255>

パスワードの最小の長さ。デフォルトは 15 です。

例：`xConfiguration Authentication StrictPassword MinimumLength: 15`

xConfiguration Authentication StrictPassword MinimumLowerCase: <0..255>

使用する必要がある小文字の最小数。値を 0 にするとこの確認が無効になります。デフォルト：2。

例：`xConfiguration Authentication StrictPassword MinimumLowerCase: 2`

xConfiguration Authentication StrictPassword MinimumOther: <0..255>

使用する必要がある特殊文字の最小数。特殊文字は英字や数字ではない文字のことです。値を 0 にするとこの確認が無効になります。デフォルト：2

例：`xConfiguration Authentication StrictPassword MinimumOther: 2`

xConfiguration Authentication StrictPassword MinimumUpperCase: <0..255>

使用する必要がある大文字の最小数。値を 0 にするとこの確認が無効になります。デフォルト：2

例：`xConfiguration Authentication StrictPassword MinimumUpperCase: 2`

xConfiguration Authentication UserName: <S: 0, 128>

別のシステムでの認証時にExpresswayで使用するユーザ名。注：トラバーサルクライアントゾーンには適用されません。

例：`xConfiguration Authentication UserName: 「user123」`

xConfiguration Bandwidth Default: <64..65535>

エンドポイントで帯域幅が指定されていないExpresswayが管理するコールに使用する帯域幅（kbps 単位）。デフォルト：384。

例：`xConfiguration Bandwidth Default: 384`

xConfiguration Bandwidth Downspeed PerCall Mode: <On/Off>

要求を満たすために使用できるコール単位の帯域幅が不足している場合にExpresswayがコールのダウンスピードを試行するかどうかを決定します。デフォルトは On です。

On：Expressway はより低い帯域幅でのコールの発信を試行します。

Off：コールは拒否されます。

例：`xConfiguration Bandwidth Downspeed PerCall Mode: On`

xConfiguration Bandwidth Downspeed Total Mode: <On/Off>

要求を満たすために使用できる総帯域幅が不足している場合にExpresswayがコールのダウンスピードを試行するかどうかを決定します。デフォルトは On です。

On：Expressway はより低い帯域幅でのコールの発信を試行します。

Off：コールは拒否されます。

例：`xConfiguration Bandwidth Downspeed Total Mode: On`

xConfiguration Bandwidth Link [1..3000] Name: <S: 1, 50>

このリンクに名前を割り当てます。

例：`xConfiguration Bandwidth Link 1 Name: 「HQ to BranchOffice」`

xConfiguration Bandwidth Link [1..3000] Node1 Name: <S: 0, 50>

このリンクを適用する最初のゾーンまたはサブゾーンを指定します。

例：`xConfiguration Bandwidth Link 1 Node1 Name: 「HQ」`

xConfiguration Bandwidth Link [1..3000] Node2 Name: <S: 0, 50>

このリンクを適用する 2 番目のゾーンまたはサブゾーンを指定します。

例：`xConfiguration Bandwidth Link 1 Node2 Name: 「BranchOffice」`

xConfiguration Bandwidth Link [1..3000] Pipe1 Name: <S: 0, 50>

このリンクと関連付ける最初のパイプを指定します。

例：`xConfiguration Bandwidth Link 1 Pipe1 Name: 「512Kb ASDL」`

xConfiguration Bandwidth Link [1..3000] Pipe2 Name: <S: 0, 50>

このリンクと関連付ける 2 番目のパイプを指定します。

例：`xConfiguration Bandwidth Link 1 Pipe2 Name: 「2Gb Broadband」`

xConfiguration Bandwidth Pipe [1..1000] Bandwidth PerCall Limit: <1..100000000>

このパイプのコール単位の帯域幅の制限がある場合、どのコールにも使用可能な帯域幅の最大量（kbps 単位）を設定します。デフォルト：1920。

例：`xConfiguration Bandwidth Pipe 1 Bandwidth PerCall Limit: 256`

xConfiguration Bandwidth Pipe [1..1000] Bandwidth PerCall Mode: <Limited/Unlimited/NoBandwidth>

このパイプで個々のコールの帯域幅を制限するかどうかを決定します。デフォルトはUnlimitedです。

NoBandwidth：使用可能な帯域幅はありません。コールは、このパイプで発信できません。

例：`xConfiguration Bandwidth Pipe 1 Bandwidth PerCall Mode: Limited`

xConfiguration Bandwidth Pipe [1..1000] Bandwidth Total Limit: <1..100000000>

このパイプの帯域幅が制限されている場合にパイプで常に使用可能な最大帯域幅（kbps単位）を設定します。デフォルトは 500000 です。

例：`xConfiguration Bandwidth Pipe 1 Bandwidth Total Limit: 1024`

xConfiguration Bandwidth Pipe [1..1000] Bandwidth Total Mode: <Limited/Unlimited/NoBandwidth>

このパイプで総帯域幅制限を適用するかどうかを決定します。デフォルトはUnlimitedです。

NoBandwidth：使用可能な帯域幅はありません。コールは、このパイプで発信できません。

例：`xConfiguration Bandwidth Pipe 1 Bandwidth Total Mode: Limited`

xConfiguration Bandwidth Pipe [1..1000] Name: <S: 1, 50>

このパイプに名前を割り当てます。

例：`xConfiguration Bandwidth Pipe 1 Name: 「512Kb ASDL」`

xConfiguration Call Loop Detection Mode: <On/Off>

Expressway がコール ループを確認するかどうかを指定します。デフォルトは On です。

例：`xConfiguration Call Loop Detection Mode: On`

xConfiguration Call Routed Mode: <Always/Optimal>

Expressway がコールにシグナリングをルーティングするかどうかを指定します。デフォルトは [常に緊急にする（Always）] です。

Always：Expressway は常にコール シグナリングをルーティングします。

Optimal：可能な場合、Expressway はコール シグナリング パスからその Expressway 自体を削除します。つまり、コールはコール ライセンスを消費しない場合があります。

例：`xConfiguration Call Routed Mode: Always`

xConfiguration Call Services CallsToUnknownIPAddresses: <Off/Direct/Indirect>

Expressway またはそのネイバーの 1 つの登録されていないシステムに Expressway がコールを試行する方法。デフォルトは Indirect です。

*[*直接（*Direct*）*]*：Expressway がネイバーを照会することなく、エンドポイントが不明な IP アドレスにコールできます。端部がローカルシステムに直接登録されていたかのように、コール セットアップが実行されます。

*[*間接（*Indirect*）*]*：不明な IP アドレスへのコールを受信すると、Expressway はネイバーにそのリモートアドレスを照会し、許可されれば、ネイバーを通じてコールをルーティングします。

*[*オフ（*Off*）*]*：Expressway に直接登録されたエンドポイントが Expressway に直接登録されたシステムの IP アドレスのみをコールする可能性があります。

例：`xConfiguration Call Services CallsToUnknownIPAddresses: Indirect`

xConfiguration Call Services Fallback Alias: <S: 0, 60>

Expressway の IP アドレスまたはドメイン名が指定されていても、コール エイリアスが指定されていないコールの場合に、着信メッセージを発信するエイリアスを指定します。

例：`xConfiguration Call Services Fallback Alias: 「reception@example.com」`

xConfiguration CollaborationEdge AllowEmbeddedSafari: <Yes/No>

これは、iOS 9 以降を使用している iPad または iPhone が OAuth トークンを使用して認可する場合に、それらの iPad または iPhone 上の Cisco Jabber 11.8 以降にのみ適用されます。

Yes を選択すると、iOS デバイス上の Jabber がネイティブ Safari ブラウザに認証ページを表示できるようになります。

No を選択すると、iOS デバイス上の Jabber は、Safari ブラウザではなく WebView ブラウザに認証ページを表示します。

（注） このオプションを切り替える場合は、Cisco Unified Communications Manager の **[iOS の SSO ログイン動作（SSO Login Behavior for iOS）]** についても対応する選択を行ってください。

例：`xConfiguration CollaborationEdge AllowEmbeddedSafari: No`

xConfiguration CollaborationEdge AllowList DefaultMethods: <String>

HTTP 許可リストに 1 つ以上のデフォルト HTTP メソッドを設定します。

設定パラメータ：

メソッド：<OPTIONS/GET/HEAD/POST/PUT/DELETE>：コンマ区切りの 1 つ以上の http メソッドのセット

例：`xConfiguration CollaborationEdge AllowList DefaultMethods: PUT,GET,POST`

xConfiguration CollaborationEdge AllowOnboardingOverMra: <On/Off>

MRA デバイスのアクティベーション コードによるオンボーディングを有効または無効にします。有効/無効にすると、その設定に応じて自動的に mTLS が MRA ポート上で有効または無効にされます。mTLS に必要な CA 証明書は自動生成されます。

例`xCo : nfiguration CollaborationEdge AllowOnboardingOverMra: On`

xConfiguration CollaborationEdge AllowRedirectUri: <On/Off>

リダイレクトURIを有効または無効にします。クライアントがOAuthフロー（およびMRA）に埋め込みブラウザを使用できるようにします。デフォルト値は*no*です。このオプションを有効にするには値を *[*はい（*Yes*）*]* に設定します。

例：`xConfiguration CollaborationEdge AllowRedirectUri: Off`

xConfiguration CollaborationEdge Enabled: <On/Off>

この Expressway の Mobile & Remote Access を有効または無効にします。

例：`xConfiguration CollaborationEdge Enabled: On`

xConfiguration CollaborationEdge InternalCheck: <No/Yes>

このスイッチは、使用可能な認証モードに関して Expressway-C がユーザのホーム ノードを確認するかどうかを決定します。*No* を選択すると、Expressway は、実際にホームノードを確認することなく、Expressway-C で有効になっている認証モードが使用可能であることをクライアントに通知します。その結果、通常、内部ネットワークのトラフィックが減少します。ただし、このオプションは、すべてのノードで同じ認証モードが使用可能であることが分かっている場合にのみ選択してください。

Expressway-E がクライアントに応答する前に Expressway-C がユーザのホームノードについて確認できるようにするには、*Yes* を選択します。

例：`xConfiguration CollaborationEdge InternalCheck: No`

xConfiguration CollaborationEdge JabbercEnabled: <On/Off>

この Expressway の Jabber Guest サービスを有効または無効にします。

例：`xConfiguration JabbercEnabled: Off`

xConfiguration CollaborationEdge JabbercProxyProtocol: <http/https>

Expressway を通じて Jabber Guest サービスをプロキシ送信するために使用するプロトコルを選択します。

例：`xConfiguration JabbercProxyProtocol: https`

xConfiguration CollaborationEdge LegacyCred: <On/Off>

MRA クライアントが Expressway に提供するユーザ名とパスワードに基づいて Unified Communications サービスが MRA クライアントを認可する場合は、On を選択します。

例：`xConfiguration CollaborationEdge LegacyCred: Off`

xConfiguration CollaborationEdge LegacySso: <On/Off/Exclusive>

MRA クライアントが Expressway に提供する OAuth トークンに基づいて Unified Communications サービスが MRA クライアントを認可する場合は、On を選択します。これは自己記述 OAuth トークン タイプではありません。

例：`xConfiguration CollaborationEdge LegacySso: Off`

xConfiguration CollaborationEdge OauthLocal: <On/Off>

Unified Communications サービスへの Mobile & Remote Access の OAuth ローカル認証を有効または無効にします。

例：`xConfiguration CollaborationEdge OauthLocal: Off`

xConfiguration CollaborationEdge OauthSso: <On/Off>

Unified Communications サービスへの Mobile & Remote Access の OAuth シングル サインオンを有効または無効にします。

例：`xConfiguration CollaborationEdge OauthSso: Off`

xConfiguration CollaborationEdge RFC3327Enabled: <On/Off>

自動的に生成されたネイバー ゾーンを経由するレジスタの変更のパス ヘッダー サポート Unified CMノードを参照してください。

On：Expressway-Cは自身のアドレスをREGISTERメッセージのPathヘッダーおよびREGISTERメッセージへの応答に挿入します。

Off：Expressway-Cは、REGISTERメッセージのContactヘッダーのアドレスを上書きします。

例：`xConfiguration CollaborationEdge rfc3327Enabled: On`

xConfiguration CollaborationEdge SSO Scope: <PEER/CLUSTER>

Expressway ピアごとに、選択した IdP で SAML 合意を使用する場合は、PEER を指定します。クラスタに 1 つの SAML 合意を使用する場合は、CLUSTER を指定します。

例：`xConfiguration CollaborationEdge SSO Scope: CLUSTER`

xConfiguration CollaborationEdge SSO IdP <index> Digest: <sha1/sha256>

クライアントに渡す SAML 認証要求に署名するときに Expressway が使用するハッシュ アルゴリズムを変更します。

<*index*>は、Expressway に設定されているリストから特定の IdP を識別する整数です。

例：`xConfiguration CollaborationEdge SSO IdP 1 Digest: sha256`

xConfiguration CollaborationEdge SsoAlwaysAvailable: <On/Off>

Expressway-C がユーザのホーム ノードに使用可能な SSO があることを確認するかどうかを決定します。

On：Expressway-Eは、ホームノードを実際に確認せずに、SSOが使用可能であるとクライアントに常に通知します。

Off：Expressway-Eがクライアントに応答する前に、Expressway-Cが常にユーザのホームノードで SSO が使用できることを確認できるようにします。

例：`xConfiguration CollaborationEdge SsoAlwaysAvailable: Off`

（注） デフォルト値の *Off* は、Web UI で [内部 SSO のアベイラビリティの確認（**Check for internal SSO availability**）] をデフォルトの *[*はい（*Yes*）*]* に設定することと同じです。

xConfiguration CollaborationEdge SsoEnabled: <On/Off>

UC サービスへの Mobile & Remote Access のシングル サインオンを切り替えます。

例：`xConfiguration CollaborationEdge SsoEnabled: Off`

xConfiguration CollaborationEdge SsoSipTokenExtraTtl: <0..172800>

指定した秒数で SIP 認証のライフタイムを延長します。

重要　存続可能時間の拡張は、オンプレミスの UC クレデンシャルが期限切れになった後も、外部ユーザがエッジ経由で SIP を使用できることを意味します。これにより、（再認証が必要であることに気付かなかった場合でも）通話を受け入れることができる短いウィンドウがユーザに提供されますが、この利便性とセキュリティリスクの増大のバランスをとる必要があります。

例：`xConfiguration CollaborationEdge SsoSipTokenExtraTtl: 0`

xConfiguration CollaborationEdgeDeployments <index> DeploymentId: <1..65535>

特定の導入の導入 ID を変更します。

<*index*>は、Expressway に設定されているリストから特定の IdP を識別する整数です。

例：`xConfiguration CollaborationEdgeDeployments 1 DeploymentId: 5`

xConfiguration CollaborationEdgeDeployments <index> UserReadableName: <String>

この導入の名前を入力します。この Expressway を使用して提供するユニファイド コミュニケーション サービスを複数の導入を使用してパーティション化することができます。ユニファイドコミュニケーション サービスをパーティション化するための導入の使用を参照してください。

<*index*>は、Expressway に設定されているリストから特定の IdP を識別する整数です。

例：`xConfiguration CollaborationEdgeDeployments 1 UserReadableName: StagingDeployment`

xConfiguration Ciphers SIPTLSCiphers Value: <S:0,2048>

SIP TLS 暗号スイートを「OpenSSL 暗号方式」の形式で使用するように指定します（https://www.openssl.org/docs/manmaster/man1/ciphers.html#CIPHER-LIST-FORMAT を参照してください）。この機能を有効にするには、再起動が必要です。また、aNULL 暗号方式はインバウンド接続ではサポートされません。

デフォルト：`EECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:+ADH`

例：`xConfiguration Ciphers SIPTLSCiphers Value: 「EECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:+ADH」`

SIP TLS プロトコル値を変更するには、*SIP Advanced SipTlsVersions* を参照してください。

xConfiguration Ciphers HTTPSCiphers Value: <S:0,2048>

HTTPS 暗号スイートを「OpenSSL 暗号方式」の形式で使用するように指定します（https://www.openssl.org/docs/manmaster/man1/ciphers.html#CIPHER-LIST-FORMAT を参照してください）。

デフォルト：`EECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL`

例：`xConfiguration Ciphers HTTPSCiphers Value: 「EECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL」`

xConfiguration Ciphers HTTPSProtocol Value: <S:minTLSv1.0, minTLSv1.1, minTLSv1.2>

HTTPS TLS プロトコルの最小バージョンを指定します。

デフォルト：`minTLSv1.2`

例：`xConfiguration Ciphers HTTPSProtocol Value: 「minTLSv1.2」`

xConfiguration Ciphers SMTPTLSCiphers Value: <S:0,2048>

「OpenSSL 暗号」形式で使用する SMTP TLS 暗号スイートを指定します（以下参照、https://www.openssl.org/docs/manmaster/man1/ciphers.html#CIPHER-LIST-FORMAT

デフォルト：`EECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL`

例：`xConfiguration Ciphers SMTPTLSCiphers Value: "EECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL"`

xConfiguration Ciphers SMTPTLSProtocol Value: <S:minTLSv1.0, minTLSv1.1, minTLSv1.2>

SMTP TLS プロトコルの最小バージョンを指定します。

デフォルト：`minTLSv1.2`

例：`xConfiguration Ciphers SMTPTLSProtocol Value: "minTLSv1.2"`

xConfiguration Ciphers ReverseProxyTLSCiphers Value: <S:0,2048>

リバース プロキシ TLS 暗号スイートを「OpenSSL 暗号方式」の形式で使用するように指定します（https://www.openssl.org/docs/manmaster/man1/ciphers.html#CIPHER-LIST-FORMAT を参照してください）。

デフォルト：`EECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL`

例：`xConfiguration Ciphers ReverseProxyTLSCiphers Value: 「EECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL」`

xConfiguration Ciphers ReverseProxyTLSProtocol Value: <S:minTLSv1.0, minTLSv1.1, minTLSv1.2>

リバース プロキシ TLS プロトコルの最小バージョンを指定します。

デフォルト：`minTLSv1.2`

例：`xConfiguration Ciphers ReverseProxyTLSProtocol Value: 「minTLSv1.2」`

xConfiguration Ciphers UcClientTLSCiphers Value: <S:0,2048>

UC クライアント TLS 暗号スイートを「OpenSSL 暗号方式」の形式で使用するように指定します（https://www.openssl.org/docs/manmaster/man1/ciphers.html#CIPHER-LIST-FORMAT を参照してください）。

デフォルト：`EECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL`

例：`xConfiguration CiphersUcClientTLSCiphers Value: 「EECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL」`

xConfiguration Ciphers UcClientTLSProtocol Value: <S:minTLSv1.0, minTLSv1.1, minTLSv1.2>

UC クライアント TLS プロトコルの最小バージョンを指定します。

デフォルト：`minTLSv1.2`

例：`xConfiguration Ciphers UcClientTLSProtocol Value: 「minTLSv1.2」`

xConfiguration Ciphers XCPTLSCiphers Value: <S:0,2048>

XCP TLS 暗号スイートを「OpenSSL 暗号方式」の形式で使用するように指定します（https://www.openssl.org/docs/manmaster/man1/ciphers.html#CIPHER-LIST-FORMAT を参照してください）。この機能を有効にするには、再起動が必要です。

デフォルト：`EECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL`

例：`xConfiguration Ciphers XCPTLSCiphers Value: 「EECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL」`

xConfiguration Ciphers XCPTLSProtocol Value: <S:minTLSv1.0, minTLSv1.1, minTLSv1.2>

XCP TLS プロトコルの最小バージョンを指定します。

デフォルト：`minTLSv1.2`

例：`xConfiguration Ciphers XCPTLSProtocol Value: minTLSv1.2`

xConfiguration Ciphers sshd_ciphers Value: <S:0,2048>

「openssh」 形式の管理/ルート SSH 接続（TCP/22）に利用可能な暗号方式を設定します。

デフォルト：
`aes256-gcm@openssh.com,aes128-gcm@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr`

例：`xConfiguration Ciphers sshd_ciphers Value: 「aes256-gcm@openssh.com,aes128-gcm@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr」`

xConfiguration Ciphers sshd_kex Value: <S:0,2048>

「openssh」 形式の管理/ルート SSH 接続（TCP/22）のキー交換アルゴリズムを設定します。

デフォルト：
`ecdh-sha2-nistp521,ecdh-sha2-nistp384,ecdh-sha2-nistp256,diffie-hellman-group-exchange-sha256,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1`

例：`xConfiguration Ciphers sshd_kex Value: 「ecdh-sha2-nistp521,ecdh-sha2-nistp384,ecdh-sha2-nistp256,diffie-hellman-group-exchange-sha256,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1」`

xConfiguration Ciphers sshd_macs Value: <S:0,2048>

「openssh」 形式の管理/ルート SSH 接続（TCP/22）のメッセージ認証コードダイジェストを設定します。

デフォルト：`hmac-sha2-512,hmac-sha2-256,hmac-sha1`

例：`xConfiguration Ciphers sshd_macs Value: 「hmac-sha2-512,hmac-sha2-256,hmac-sha1」`

xConfiguration Ciphers sshd_pfwd_ciphers Value: <S:0,2048>

順方向および逆方向の HTTP プロキシ（つまり、APNS および MRA HTTP トラフィック）に使用される SSH トンネルで使用できる暗号方式。

デフォルト：`aes256-ctr`

例：`xConfiguration Ciphers sshd_pfwd_ciphers Value: 「aes256-ctr」`

xConfiguration DNS PerDomainServer [1..5] Address: <S: 0, 39>

関連付けられたドメイン名のホスト名を解決するときのみに使用する DNS サーバの IP アドレス。

例：`xConfiguration DNS PerDomainServer 1 Address: 「192.168.12.1」`

xConfiguration DNS PerDomainServer [1..5] Domain1: <S: 0, 39>

この特定の DNS サーバで解決する最初のドメイン名。

例：`xConfiguration DNS PerDomainServer 1 Domain1: 「dept.example.com」`

xConfiguration DNS PerDomainServer [1..5] Domain2: <S: 0, 39>

この特定の DNS サーバで解決する 2 番目のドメイン名。

例：`xConfiguration DNS PerDomainServer 1 Domain2: 「other.example.com」`

xConfiguration DNS Server [1..5] Address: <S: 0, 39>

ドメイン名を解決するときに使用するデフォルトの DNS サーバの IP アドレス。最大で 5 のサーバを指定できます。デフォルトの DNS サーバは、ルックアップするドメインに定義されたドメイン単位の DNS サーバがない場合に使用します。

例：`xConfiguration DNS Server 1 Address: 「192.168.12.0」`

xConfiguration EdgeConfigServer CredentialTtl: <0..604800>

SSO 認証には適用されません。

Expressway がクライアントの認証に成功するために送信する認証トークンのライフタイムを指定します。正常に認証されたクライアントは、このトークンが期限切れになる前に更新を要求する必要があります。更新しないと、再認証が必要になります。

例：`xConfiguration EdgeConfigServer CredentialTtl: 28800`

xConfiguration EdgeConfigServer PurgeInterval: <0..604800>

SSO 認証には適用されません。

Expressway がキャッシュ クリアの動作の間に待機する時間を指定します。キャッシュがクリアされると、期限切れのトークンのみが削除されるため、この設定は期限切れトークンをキャッシュに保持できる最長時間となります。

例：`xConfiguration EdgeConfigServer PurgeInterval: 43200`

xConfiguration EdgeConfigServer RateLimitLogins: <0..100>

VCS を使用してユーザのクレデンシャルをレートコントロール期間ごとに許可する回数を制限します。同じユーザ クレデンシャルを使用しているデバイスは、この回数に対して考慮されます。

上限に到達すると、これらのクレデンシャルを使用するためのそれ以降の試行が現在のレート コントロールの期限が切れるまで拒否されます。

レート コントロール機能を無効にするには 0 を入力します。

例：`xConfiguration EdgeConfigServer RateLimitLogins: 3`

xConfiguration EdgeConfigServer RateLimitPeriod: <0..86400>

許可がカウントされる期間（秒単位）を定義します。レート コントロールが有効になっている場合は、ユーザの最初の許可でカウンタとタイマーが起動します。レート コントロールの期限が切れるとカウンターがリセットされ、ユーザの次の許可によって新しい期間が開始されます。

レート コントロール機能を無効にするには 0 を入力します。

例：`xConfiguration EdgeConfigServer RateLimitPeriod: 300`

xConfiguration ErrorReport Contact: <S: 0, 128>

必要に応じて、インシデント レポートでフォローアップするオプションの連絡先電子メール アドレス。

例：`xConfiguration ErrorReport Contact: 「bob smith」`

xConfiguration ErrorReport CoreDump: <On/Off>

診断コアダンプ ファイルを作成するかどうかを決定します。デフォルトは On です。

例：`xConfiguration ErrorReport CoreDump: On`

xConfiguration ErrorReport Mode: <On/Off>

アプリケーション機能の詳細情報を Web サービスに自動的に送信するかどうかを決定します。デフォルト：Off

例：`xConfiguration ErrorReport Mode: Off`

xConfiguration ErrorReport Proxy: <S: 0, 128>

インシデント レポート サーバへの HTTP/HTTPS 接続に使用するオプションのプロキシ サーバ。

例：`xConfiguration ErrorReport Proxy: https://proxy_address/submiterror/`

xConfiguration ErrorReport Url: <S: 0, 128>

アプリケーション障害の詳細情報を送信する Web サービスの URL。デフォルト：https://cc-reports.cisco.com/submitapplicationerror/

例：`xConfiguration ErrorReport Url: https://cc-reports.cisco.com/submitapplicationerror/`

xConfiguration Ethernet [1..2] IP V4 Address: <S: 7,15>

指定した LAN ポートの IPv4 アドレスを指定します。注：変更を有効にするには、システムを再起動する必要があります。

例：`xConfiguration Ethernet 1 IP V4 Address: 「192.168.10.10」`

xConfiguration Ethernet [1..2] IP V4 StaticNAT Address: <S:7,15>

Expressway がスタティック NAT モードで動作している場合、これによりそのスタティック NAT の外部パブリック IPv4 アドレスを指定します。変更を有効にするには、システムを再起動する必要があります。

例：`xConfiguration Ethernet 1 IP V4 StaticNAT Address: 「64.22.64.85」`

xConfiguration Ethernet [1..2] IP V4 StaticNAT Mode: <On/Off>

Expressway をスタティック NAT の背後に配置するかどうかを指定します。変更を有効にするには、システムを再起動する必要があります。デフォルト：Off

例：`xConfiguration Ethernet 1 IP V4 StaticNAT Mode: On`

xConfiguration Ethernet [1..2] IP V4 SubnetMask: <S: 7,15>

指定した LAN ポートの IPv4 サブネット マスクを指定します。変更を有効にするには、システムを再起動する必要があります。

例：`xConfiguration Ethernet 1 IP V4 SubnetMask: 「255.255.255.0」`

xConfiguration Ethernet [1..2] IP V6 Address: <S: 0, 39>

指定した LAN ポートの IPv6 アドレスを指定します。変更を有効にするには、システムを再起動する必要があります。

例：`xConfiguration Ethernet 1 IP V6 Address: 「2001:db8::1428:57ab」`

xConfiguration Ethernet [1..2] Speed: <Auto/10half/10full/100half/100full/1000full

指定した LAN ポートからのイーサネット リンクの速度を設定します。速度を自動的に設定するには Auto を使用します。変更を有効にするには、システムを再起動する必要があります。デフォルト：[Auto]

例：`xConfiguration Ethernet 1 Speed: Auto`

xConfiguration ExternalManager Address: <S: 0, 128>

外部マネージャの IP アドレスまたは完全修飾ドメイン名（FQDN）を設定します。

例：`xConfiguration ExternalManager Address: 「192.168.0.0」`

xConfiguration ExternalManager Path: <S: 0, 255>

外部マネージャの URL を設定します。デフォルトは tms/public/external/management/SystemManagementService.asmx です。

例：`xConfiguration ExternalManager Path: 「tms/public/external/management/SystemManagementService.asmx」`

xConfiguration ExternalManager Protocol: <HTTP/HTTPS>

外部マネージャに接続するために使用するプロトコル。デフォルトは HTTPS です。

例：`xConfiguration ExternalManager Protocol: HTTPS`

xConfiguration ExternalManager Server Certificate Verification Mode: <On/Off>

外部マネージャによって提供される証明書を確認するかどうかを制御します。デフォルトは On です。

例：`xConfiguration ExternalManager Server Certificate Verification Mode: On`

xConfiguration H323 Gatekeeper AutoDiscovery Mode: <On/Off>

Expressway がエンドポイントからのゲートキーパー検出要求に応答するかどうかを決定します。デフォルトは On です。

例：`xConfiguration H323 Gatekeeper AutoDiscovery Mode: On`

xConfiguration H323 Gatekeeper CallSignaling PortRange End: <1024..65534>

コールの確立後に使用する範囲の上位ポートを指定します。デフォルト：19999。

例：`xConfiguration H323 Gatekeeper CallSignaling PortRange End: 19999`

xConfiguration H323 Gatekeeper CallSignaling PortRange Start: <1024..65534>

コールの確立後に使用する範囲の下位ポートを指定します。デフォルト：15000。

例：`xConfiguration H323 Gatekeeper CallSignaling PortRange Start: 15000`

xConfiguration H323 Gatekeeper CallSignaling TCP Port: <1024..65534>

H.323 コール シグナリングをリッスンするポートを指定します。デフォルト：1720。

例：`xConfiguration H323 Gatekeeper CallSignaling TCP Port: 1720`

xConfiguration H323 Gatekeeper CallTimeToLive: <60..65534>

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。

例：`xConfiguration H323 Gatekeeper CallTimeToLive: 120`

xConfiguration H323 Gatekeeper Registration RIPAllRequests: <On/Off>

Expresswayがリクエストを処理中グリーティングとH.323の登録要求に応答するかどうかを決定します。

リモートLDAPディレクトリ サービスの登録要求を認証するときに登録タイムアウトが発生したらこの設定を有効にします。デフォルト：Off

例:`xConfiguration H323のゲートキーパー登録RIPAllRequests:オフ`

xConfiguration H323 Gatekeeper Registration ConflictMode: <Reject/Overwrite>

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する場合のシステムの動作。デフォルトは Reject です。

Reject：登録を拒否します。

*[*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。

例：`xConfiguration H323 Gatekeeper Registration ConflictMode: Reject`

xConfiguration H323 Gatekeeper Registration UDP Port: <1024..65534>

H.323 UDP 登録に使用するポートを指定します。デフォルト：1719。

例：`xConfiguration H323 Gatekeeper Registration UDP Port: 1719`

xConfiguration H323 Gatekeeper TimeToLive: <60..65534>

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：1800。

例：`xConfiguration H323 Gatekeeper TimeToLive: 1800`

xConfiguration H323 Gateway CallerId: <IncludePrefix/ExcludePrefix>

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。デフォルトは ExcludePrefix です。

IncludePrefix：ISDN ゲートウェイのプレフィックスを送信元の E.164 番号に挿入します。

ExcludePrefix：送信元の E.164 number のみを表示します。

例：`xConfiguration H323 Gateway CallerId: ExcludePrefix`

xConfiguration H323 Mode: <On/Off>

Expressway が H.323 ゲートキーパー機能を提供するかどうかを決定します。デフォルト：Off

例：`xConfiguration H323 Mode: On`

xConfiguration Interworking BFCP Compatibility Mode: <Auto/TAA/Draft>

H.323 インターワーキング BFCP コントロールに対する SIP の互換性設定を制御します。デフォルト：[Auto]

例：`xConfiguration Interworking BFCP Compatibility Mode: Auto`

xConfiguration Interworking Encryption KeySize2048: <On/Off>

H.323-SIP インターワーキングの暗号化に使用する 2048 ビットの Diffie-Hellman キーが Expressway に含まれるかどうかを決定します。デフォルトは On です。

*[*オン（*On*）*]:*Expressway は、1024 ビットと 2048 ビットの両方の暗号キー長を提供します。

*[*オフ（*Off*）*]*：Expressway は 2048 ビットの暗号化キー長を提供しません。

例：`xConfiguration Interworking Encryption KeySize2048: On`

xConfiguration Interworking Encryption Mode: <Auto/Off>

Expressway が SIP エンドポイントと H.323 エンドポイント間の暗号化されたコールを許可するかどうかを決定します。デフォルト：[Auto]

Off：インターワーキングコールは暗号化されません。

Auto：エンドポイントが要求した場合はインターワーキング コールが暗号化されます。

例：`xConfiguration Interworking Encryption Mode: Auto`

xConfiguration Interworking Encryption Replay Protection Mode: <On/Off>

コールをインターワーキングするときに、着信 SRTP の再生保護を Expressway が実行するかどうかを制御します。デフォルト：Off

On：再生された SRTP パケットは Expressway でドロップされます。

Off：Expressway は再生された SRTP パケットを確認しません。

例：`xConfiguration Interworking Encryption Replay Protection Mode: Off`

xConfiguration Interworking Mode: <On/Off/RegisteredOnly>

Expressway を SIP コールと H.323 コール間のゲートウェイとして機能させるかどうかを決定します。デフォルトは RegisteredOnly です。

Off：Expressway は SIP-H.323 ゲートウェイとして機能しません。

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-H.323 ゲートウェイとして機能します。

RegisteredOnly：Expressway は、少なくとも 1 つのエンドポイントがローカルに登録されている場合にのみ、SIP-H.323 ゲートウェイとして機能します。

例：`xConfiguration Interworking Mode: On`

xConfiguration Interworking Require Invite Header Mode: <On/Off>

SIP と H.323 インターワーキング機能がダイアログを構成する INVITE の必須ヘッダーで com.tandberg.sdp.duo.enable と com.tandberg.sdp.bfcp.udp を送信するかどうかを制御します。デフォルト：Off

例：`xConfiguration Interworking Require Invite Header Mode: Off`

xConfiguration IP DNS Domain Name: <S: 0, 128>

DNS サーバに照会する前に、非修飾ホスト名に追加する名前。NTP サーバ、LDAP サーバ、外部マネージャ サーバ、およびリモート ログ サーバの非修飾ドメイン名の解決を試行するときに使用します。また、**システム ホスト名**とともに使用して、SIP メッセージングでのこの Expressway への参照を識別します。

例：`xConfiguration IP DNS Domain Name: 「example.com」`

xConfiguration IP DNS Hostname : <S: 0, 63>

このシステムが認識しているDNSホスト名。これは完全修飾ドメイン名ではなく、ホストのラベル部分です。名前には、英字、数字、ハイフン、および下線のみを使用できます。最初の文字は英字、最後の文字は英字または数字にする必要があります。

例：`xConfiguration IP DNS Hostname: 「localsystem」`

xConfiguration IP DNS MaxPort: <1024..65535>

DNS クエリの送信に使用する範囲の上位送信元ポート。要求は、この範囲からランダムにポートを選択します。警告：設定したソースポート範囲が狭いと、DNSスプーフィング攻撃に対する脆弱性が高まります。デフォルト：65535。

例：`xConfiguration IP DNS MaxPort: 65535`

xConfiguration IP DNS MinPort: <1024..65535>

DNS クエリの送信に使用する範囲の下位送信元ポート。要求は、この範囲からランダムにポートを選択します。警告：設定したソースポート範囲が狭いと、DNSスプーフィング攻撃に対する脆弱性が高まります。デフォルト：1024。

例：`xConfiguration IP DNS MinPort: 1024`

xConfiguration IP DNS SearchDomains: <S: 0, 1024>

DNSサーバを照会するときに追加で検索するドメイン名のスペース区切りリスト。NTPサーバ、LDAPサーバ、外部マネージャサーバ、およびリモートログサーバの非修飾ドメイン名の解決を試行するときに使用します。ローカル システム ホスト名とともに使用して、SIPメッセージングでこのシステムへの参照を識別することもできます。（ピア固有）

例：`xConfiguration IP DNS SearchDomains: 「example1.int」「" "example2.int」「example3.int」`

xConfiguration IP DNS UseEphemeralPortRange: <On/Off>

発信 DNS クエリがシステムの通常のエフェメラル ポート範囲を使用するか、設定可能なカスタム ポート範囲を使用するかを決定します。デフォルトは On です。

例：`xConfiguration IP DNS UseEphemeralPortRange: On`

xConfiguration IP Ephemeral PortRange End: <1024..65534>

Expressway コール処理によって禁止されていない限り、エフェメラルアウトバウンド接続に使用する範囲内の最上位のポート。デフォルト：35999。

例：`xConfiguration IP Ephemeral PortRange End: 35999`

xConfiguration IP Ephemeral PortRange Start: <1024..65534>

Expressway コール処理によって禁止されていない限り、エフェメラルアウトバウンド接続に使用する範囲内の最下位のポート。デフォルトは 30000 です。

例：`xConfiguration IP Ephemeral PortRange Start: 30000`

xConfiguration IP External Interface: <LAN1/LAN2>

外部に面している LAN インターフェイスを定義します。デフォルトは LAN1 です。

例：`xConfiguration IP External Interface: LAN1`

xConfiguration IP Gateway: <S: 7,15>

Expressway の IPv4 ゲートウェイを指定します。注：変更を有効にするには、システムを再起動する必要があります。デフォルトは 127.0.0.1 です。

例：`xConfiguration IP Gateway: "192.168.127.0"`

xConfiguration IP QoS Mode: <None/DiffServ>

すべてのシグナリングとメディア パケットに適用する QoS （Quality of Service）タグのタイプ。変更を有効にするには、システムを再起動する必要があります。デフォルト：[None]。

None：特定の QoS タグは適用されません。

DiffServ：指定したタグ値を IPv4 ヘッダーの TOS（サービスのタイプ）フィールドまたは IPv6 ヘッダーの TC（トラフィッククラス）フィールドに挿入します。

例：`xConfiguration IP QoS Mode: DiffServ`

重要 重要:このコマンドは、バージョン X8.9 から廃止されており、コマンド `QoS Audio`、`QoS Video`、`QoS XMPP`、および `QoS Signaling` に置き換わります。

xConfiguration IP QoS Value: <0..63>

システムを介してルーティングされるすべてのシグナリング トラフィックとメディア トラフィックにスタンプする値。変更を有効にするには、システムを再起動する必要があります。デフォルト：[0]。

例：`xConfiguration IP QoS Value: 16`

重要 重要:このコマンドは、バージョン X8.9 から廃止されており、コマンド `QoS Audio`、`QoS Video`、`QoS XMPP`、および `QoS Signaling` に置き換わります。

xConfiguration IP RFC4821 Mode: <Auto/Enabled/Disabled>

Expressway ネットワーク インターフェイスが RFC4821 Packetization Layer Path MTU Discovery をいつ使用するかを決定します。変更を有効にするには、システムを再起動する必要があります。デフォルトで、ディセーブルになっています。

Enabled：常にパケット化レイヤの MTU プロービングが実行されます。

Auto：デフォルトで無効になっていますが、ICMP ブラックホールが検出された場合に有効になります。

Disabled：パケット化レイヤの MTU プロービングは実行されません。

例：`xConfiguration IP RFC4821 Mode: Disabled`

xConfiguration IP Route [1..50] Address: <S: 0, 39>

このルートを適用するネットワークを決定するためにプレフィックス長とともに使用する IP アドレスを指定します。

例：`xConfiguration IP Route 1 Address: 「128.168.0.0」`

xConfiguration IP Route [1..50] Gateway: <S: 0, 39>

このルートのゲートウェイの IP アドレスを指定します。

例：`xConfiguration IP Route 1 Gateway: 「192.168.0.0」`

xConfiguration IP Route [1..50] Interface: <Auto/LAN1/LAN2>

このルーティングに使用する LAN インターフェイスを指定します。Auto：使用に最適なインターフェイスを Expressway が選択します。デフォルト：[Auto]

例：`xConfiguration IP Route 1 Interface: Auto`

xConfiguration IP Route [1..50] PrefixLength: <0..128>

このルートを適用するネットワークを決定するときに一致する必要がある IP アドレスのビット数。デフォルト：32。

例：`xConfiguration IP Route 1 PrefixLength: 16`

xConfiguration IP V6 Gateway: <S: 0, 39>

Expressway の IPv6 ゲートウェイを指定します。変更を有効にするには、システムを再起動する必要があります。

例：`xConfiguration IP V6 Gateway: 「3dda:80bb:6::9:144」`

xConfiguration IPProtocol: <Both/IPv4/IPv6>

Expressway が IPv4、IPv6、またはデュアル スタックのいずれのモードで実行するかを選択します。変更を有効にするには、システムを再起動する必要があります。デフォルトは IPv4 です。

例：`xConfiguration IPProtocol: IPv4`

xConfiguration Language Default: <S: 0, 128>

Web インターフェイスで使用されるデフォルト言語。デフォルトは "en_US" です。

例：`xConfiguration Language Default: 「en_US」`

xConfiguration Log CDR Service: <off/serviceonly/serviceandlogging>

この Expressway によって生成されるコール詳細レコードを記録する方法を選択します。

Off：コール詳細レコードは記録されません。

serviceonly：コール詳細レコードは7日間ローカルに保存された後に削除されます。記録されたレコードにはユーザ インターフェイスからアクセスできません。

serviceandlogging：serviceonly と同様ですが、CDR にはローカルイベントログからアクセスできます。syslog サーバのアドレスを追加した場合、それらのアドレスにレコードが情報メッセージとして送信されます。

デフォルト：*Off*

例：`xConfiguration Log CDR Service: serviceonly`

xConfiguration Log Level: <1..4>

イベントロギングの粒度を制御します。1は最も詳細度が低く、4が最も高くなります。注：この設定は過去に遡ることはできません。現時点以降のイベントログに書き込むイベントを決定します。デフォルトは 1 です。

例：`xConfiguration Log Level: 1`

xConfiguration Log MediaStats Logging: <On/Off>

メディア統計情報のロギングを切り替えます。デフォルト：Off

例：`xConfiguration Log MediaStats Logging: On`

xConfiguration Log SystemMetrics Interval: <30..600>

メトリック収集イベント間で待機する秒数を設定します。

重要 間隔が短いほどシステムのパフォーマンスに大きな影響を与え、長いほどメトリックが大まかになります。非常に高精度なメトリックが必要な場合以外は、最も長い間隔を使用することをお勧めします。

デフォルト：60

例：`xConfiguration Log SystemMetrics Interval: 60`

xConfiguration Log SystemMetrics Mode: <On/Off>

システム メトリック収集サービスを切り替えます。このシステムのメトリックの収集を開始するには、On と入力します。

デフォルトは *Off* です。

例：`xConfiguration Log SystemMetrics Mode: On`

xConfiguration Log SystemMetrics Network Address: <S: 0,1024>

リスニング サーバのアドレスを入力します。IP アドレス、ホスト名、または FQDN を使用できます。

デフォルト：空

例：`xConfiguration log SystemMetrics Network Address: 「192.168.0.5」`

LxConfiguration Log SystemMetrics Network Port: <1..65535>

システム メトリック トラフィックを予期するリスニング サーバのポートを入力します。

デフォルトは *25826* です。

例：`xConfiguration log SystemMetrics Network Port: 25826`

Configuration Logger Network [1..n] Level: <FATAL/ERROR/WARN/INFO/DEBUG/TRACE>

指定したモジュールのロギング レベル。デフォルト：INFO

例：`xConfiguration Logger Developer 1 Level: INFO`

xConfiguration Login Remote LDAP BaseDN Accounts: <S: 0,255>

管理者アカウントやユーザ アカウントの検索時にベースとして使用する識別名を設定します。

例：`xConfiguration Login Remote LDAP BaseDN Accounts: 「ou=useraccounts,dc=corporation,dc=int」`

xConfiguration Login Remote LDAP BaseDN Groups: <S: 0,255>

管理者グループやユーザ グループの検索時にベースとして使用する識別名を設定します。

例：`xConfiguration Login Remote LDAP BaseDN Groups: 「ou=groups,dc=corporation,dc=int」`

xConfiguration Login Remote LDAP CRLCheck: <None/Peer/All>

LDAP サーバとの TLS 接続を確立するときに証明書失効リスト（CRL）を確認するかどうかを指定します。CRL データは、信頼できる CA 証明書 PEM ファイルを使用して Expressway にアップロードされます。デフォルト：[None]。

*[*なし（*None*）*]*：CRL チェックは実行されません。

*[*ピア（*Peer*）*]*：LDAP サーバの証明書を発行した CA に関連付けられた CRL のみを確認します。

*[*すべて（*All*）*]*：LDAP サーバ証明書を発行した CA の信頼できる証明書チェーン内のすべての CRL を確認します。

例：`xConfiguration Login Remote LDAP CRLCheck: Peer`

xConfiguration Login Remote LDAP DirectoryType: <ActiveDirectory>

アクセスするLDAPディレクトリのタイプを定義します。デフォルトはActiveDirectoryです。

ActiveDirectory：ディレクトリは Windows Active Directory です。

例：`xConfiguration Login Remote LDAP DirectoryType: ActiveDirectory`

xConfiguration Login Remote LDAP Encryption: <Off/TLS>

LDAP サーバへの接続に使用する暗号化を設定します。デフォルトは TLS です。

[Off]：暗号化は使用されません。

TLS：TLS 暗号化を使用します。

例：`xConfiguration Login Remote LDAP Encryption: Off`

xConfiguration Login Remote LDAP SASL: <None/DIGEST-MD5>

LDAP サーバにバインドするときに使用する SASL（Simple Authentication and Security Layer）のメカニズム。デフォルトは DIGEST-MD5 です。

None：メカニズムを使用しません。

[DIGEST-MD5]：DIGEST-MD5 メカニズムを使用します。

例：`xConfiguration Login Remote LDAP SASL: DIGEST-MD5`

xConfiguration Login Remote LDAP SearchOptimize NestedDepth: <1..16>

LDAP 認証のサブグループ検索深度レベルを設定します。デフォルト：16

例：`xConfiguration Login Remote LDAP SearchOptimize NestedDepth: "1"`

xConfiguration Login Remote LDAP SearchOptimize SkipMembers: <Yes/No>

LDAP 認証用のグループを検索するときに、グループメンバールックアップをスキップするかどうかを定義します。デフォルト：[はい（Yes）]

例：`xConfiguration Login Remote LDAP SearchOptimize SkipMembers: "No"`

xConfiguration Login Remote LDAP Server Address: <S: 0,128>

LDAP クエリを実行するときに使用する LDAP サーバの IP アドレスまたは完全修飾ドメイン名を設定します。

例：`xConfiguration Login Remote LDAP Server Address: 「server.example.com」`

xConfiguration Login Remote LDAP Server FQDNResolution: <AddressRecord/SRVRecord>

LDAP サーバ アドレスが FQDN として指定されている場合の解決方法を定義します。デフォルトは AddressRecord です。

AddressRecord：DNS A レコードまたは AAAA レコード ルックアップ。

SRVRecord：DNS SRV レコード ルックアップ。SRV record：DNS SRV レコード ルックアップ。

例：`xConfiguration Login Remote LDAP Server FQDNResolution: AddressRecord`

xConfiguration Login Remote LDAP Server Port: <1..65534>

LDAP クエリを実行するときに使用する LDAP サーバの IP ポートを設定します。非セキュア接続は 389、セキュア接続は 636 を使用します。他のポートはサポートされていません。デフォルト：389。

例：`xConfiguration Login Remote LDAP Server Port: 389`

xConfiguration Login Remote LDAP VCS BindDN: <S: 0,255>

LDA Pサーバにバインドするときに使用するユーザの識別名を設定します。

例：`xConfiguration Login Remote LDAP VCS BindDN: 「systemmanager」`

xConfiguration Login Remote LDAP VCS BindPassword: <S: 0,122>

LDAP サーバにバインドするときに使用するパスワードを設定します。プレーン テキストの最大長は 60 文字で、暗号化されます。

例：`xConfiguration Login Remote LDAP VCS BindPassword: 「password123」`

xConfiguration Login Remote LDAP VCS BindUsername: <S: 0,255>

LDAP サーバにバインドするときに使用するユーザ名を設定します。SASL を使用する場合にのみ適用されます。

例：`xConfiguration Login Remote LDAP VCS BindUsername: 「systemmanager」`

Configuration Login Remote Protocol: <LDAP>

外部プロトコルに接続するために使用するプロトコル。デフォルトは LDAP です。

例：`xConfiguration Login Remote Protocol: LDAP`

xConfiguration Login Source Admin: <LocalOnly/RemoteOnly/Both>

アクセスが許可される前に管理者のログイン クレデンシャルを認証する場所を定義します。デフォルトは LocalOnly です。

LocalOnly：Expressway に保存されているローカルデータベースと照合してクレデンシャルを確認します。

RemoteOnly：Windows Active Directory などの外部クレデンシャルディレクトリと照合してクレデンシャルを確認します。これによって、デフォルトの admin アカウントを使用したログイン アクセスが無効になります。

Both：最初に Expressway に保存されているローカル データベースと照合して確認し、一致するアカウントが見つからなかった場合は外部クレデンシャル ディレクトリが代わりに使用されます。

例：`xConfiguration Login Source Admin: LocalOnly`

xConfiguration Login User [1..n] Name: <S: 0,60>

ローカル認証データベースにこのエントリの名前を定義します。

例：`xConfiguration Login User 1 Name: 「alice」`

xConfiguration Login User [1..n] Password: <S: 0,128>

ローカル認証データベースにこのエントリのパスワードを定義します。

例：`xConfiguration Login User 1 Password: 「abcXYZ_123」`

xConfiguration Management Interface HstsMode: <On/Off>

Web ブラウザがこのサーバへのアクセスにセキュアな接続のみを使用するように指示するかどうかを決定します。この機能を有効にすると、中間者（MITM）攻撃に対する保護が強化されます。デフォルトは On です。

[オン（On）]：Web サーバからのすべての応答は、有効期限が 1 年の Strict Transport Security ヘッダーが追加されて送信されます。

[オフ（Off）]：Strict Transport Security ヘッダーは送信されず、ブラウザは通常どおりに動作します。注：変更を有効にするには、システムを再起動する必要があります。

例：`xConfiguration Management Interface HstsMode: On`

xConfiguration Management Interface Port: <1..65535>

管理者が Expressway Web インターフェイスにアクセスするための https リスニング ポートを設定します。デフォルト：443。

例:`xConfiguration IPアドレス ポート:7443`

xConfiguration Management Session InactivityTimeout: <0..65535>

管理セッション（シリアルポート、HTTPS、またはSSH）がタイムアウトになる前に、管理セッションが非アクティブになる期間（分）を設定します。セッションタイムアウトをオフにするには値を 0 に設定します。デフォルトは 30 です。

例：`xConfiguration Management Session InactivityTimeout: 30`

xConfiguration Management Session MaxConcurrentSessionsTotal: <0..65535>

システムで許可される同時管理者セッションの最大数。これには、Web セッション、SSH セッション、およびシリアル セッションが含まれます。値を 0 にすると、セッション制限はオフになります。デフォルト：[0]。

例：`xConfiguration Management Session MaxConcurrentSessionsTotal: 0`

xConfiguration Management Session MaxConcurrentSessionsUser: <0..65535>

個々の管理者アカウントがシステムで許可される同時セッションの数。これには、Web セッション、SSH セッション、およびシリアル セッションが含まれます。値を 0 にすると、セッション制限はオフになります。デフォルト：[0]。

例：`xConfiguration Management Session MaxConcurrentSessionsUser: 0`

xConfiguration NetworkLimits

機能を制限するまでレートを設定します。`xconfig networklimits ?` と入力して、ヘルプを確認する。

例：`xConfiguration NetworkLimits Configuration GarbageCollectSecs: 5`

xConfiguration NTP Server [1..5] Address: <S: 0, 128>

システム時刻を同期するときに使用する最大 5 つの NTP サーバの IP アドレスまたは完全修飾ドメイン名（FQDN）を設定します。

例：`xConfiguration NTP Server 1 Address: 「ntp.server.example.com」`

xConfiguration Option [1..64] Key: <S: 0, 90>

ソフトウェア オプションのオプション キーを指定します。これらのキーは、システムのキャパシティを引き上げるなど、特別な機能を追加するためにシステムに追加されます。詳細については、シスコのサポート担当者にお問い合わせください。

例：`xConfiguration Option 1 Key: 「1X4757T5-1-60BAD5CD」`

xConfiguration Policy AdministratorPolicy Mode: <Off/LocalCPL/LocalService/PolicyService>

コール ポリシーの使用を有効または無効にします。デフォルト：Off

Off：コールポリシーを無効にします。

LocalCPL：アップロードした CPL ファイルのポリシーを使用します。

LocalService：グループポリシーの情報とローカルファイルを使用します。

PolicyService：外部ポリシーサービスを使用します。

例：`xConfiguration Policy AdministratorPolicy Mode: Off`

xConfiguration Policy AdministratorPolicy Service DefaultCPL: <S: 0,255>

リモート サービスが使用できない場合に Expressway が使用する CPL。デフォルトは <reject status='403' reason='Service Unavailable'/> です。

例：`xConfiguration Policy AdministratorPolicy Service DefaultCPL: 「<reject status='403' reason='Service Unavailable'/>」`

xConfiguration Policy AdministratorPolicy Service Password: <S: 0,82>

リモートサービスにログインして照会するためにExpresswayが使用するパスワードを指定します。プレーン テキストの最大長は 30 文字で、これらの文字は暗号化されます。

例：`xConfiguration Policy AdministratorPolicy Service Password: 「password123」`

xConfiguration Policy AdministratorPolicy Service Path: <S: 0,255>

リモート サービスの URL を指定します。

例：`xConfiguration Policy AdministratorPolicy Service Path: 「service」`

xConfiguration Policy AdministratorPolicy Service Protocol: <HTTP/HTTPS>

リモートサービスに接続するために使用するプロトコルを指定します。デフォルトはHTTPSです。

例：`xConfiguration Policy AdministratorPolicy Service Protocol: HTTPS`

xConfiguration Policy AdministratorPolicy Service Server [1..3] Address: <S: 0,128>

リモート サービスの IP アドレスまたは完全修飾ドメイン名（FQDN）を指定します。

例：`xConfiguration Policy AdministratorPolicy Service Server 1 Address: 「service.server.example.com」`

xConfiguration Policy AdministratorPolicy Service Status Path: <S: 0..255>

リモート サービス ステータスを取得するためのパスを指定します。デフォルトは status です。

例：`xConfiguration Policy AdministratorPolicy Service Status Path: status`

xConfiguration Policy AdministratorPolicy Service TLS CRLCheck Mode: <On/Off>

ポリシー サービスによって提供された証明書の証明書失効リストのチェックを制御します。有効になっている場合は、サーバの X.509 証明書が、その証明書の証明書発行機関の失効リストと照合して確認されます。デフォルトは Off です。

例：`xConfiguration Policy AdministratorPolicy Service TLS CRLCheck Mode: Off`

xConfiguration Policy AdministratorPolicy Service TLS Verify Mode: <On/Off>

X.509 証明書のチェック、およびこの Expressway とポリシー サービス間の相互認証を制御します。有効になっている場合は、アドレス フィールドで指定したサーバの FQDN または IP アドレスがサーバの X.509 証明書内（サブジェクト共通名またはサブジェクト代替名のどちらかの属性）に含まれている必要があります。デフォルトは On です。

例：`xConfiguration Policy AdministratorPolicy Service TLS Verify Mode: On`

xConfiguration Policy AdministratorPolicy Service UserName: <S: 0,30>

リモート ポリシー サービスにログインして照会するために Expressway が使用するユーザ名を指定します。

例：`xConfiguration Policy AdministratorPolicy Service UserName: 「user123」`

xConfiguration Policy FindMe CallerID: <FindMeID/IncomingID>

着信コールの発信元が呼び出し先にどのように表示されるかを決定します。デフォルトは IncomingID です。

IncomingID：コールが発信されたエンドポイントのアドレスを表示します。

FindMeID：発信エンドポイントのアドレスに関連付けられた FindMe ID を表示します。

例：`xConfiguration Policy FindMe CallerId: FindMeID`

xConfiguration Policy FindMe Mode: <Off/On/ThirdPartyManager>

FindMe アプリケーションの動作方法を設定します。デフォルトは Off です。

Off：FindMe を無効にします。

On：FindMe を有効にします。

ThirdPartyManager：オフボックスのサードパーティ製 FindMe マネージャを使用します。

例：`xConfiguration Policy FindMe Mode: On`

xConfiguration Policy FindMe Server Address: <S: 0, 128>

リモート FindMe マネージャの IP アドレスまたは完全修飾ドメイン名（FQDN）を指定します。

例：`xConfiguration Policy FindMe Server Address: 「userpolicy.server.example.com」`

xConfiguration Policy FindMe Server Password: <S: 0, 82>

リモート FindMe マネージャにログインして照会するために Expressway が使用するパスワードを指定します。プレーンテキストの最大長は30文字で、これらの文字は暗号化されます。

例：`xConfiguration Policy FindMe Server Password: 「password123」`

xConfiguration Policy FindMe Server Path: <S: 0, 255>

リモート FindMe マネージャの URL を指定します。

例：`xConfiguration Policy FindMe Server Path: 「service」`

xConfiguration Policy Services Service [1..20] DefaultCPL: <S: 0,255>

リモート サービスが使用できない場合に Expressway が使用する CPL。デフォルトは <reject status='504' reason='Policy Service Unavailable'/> です。

例：`xConfiguration Policy Services Service 1 DefaultCPL: 「<reject status='403' reason='Service Unavailable'/>」`

xConfiguration Policy Services Service [1..20] Description: <S: 0,64>

自由形式のポリシー サービスの説明。

例：`xConfiguration Policy Services Service 1 Description: 「Conference management service」`

xConfiguration Policy Services Service [1..20] HTTPMethod: <POST/GET>

リモート サービスに使用する HTTP 方式のタイプを指定します。デフォルトは POST です。

例：`xConfiguration Policy Services Service 1 HTTPMethod: POST`

xConfiguration Policy Services Service [1..20] Name: <S: 0,50>

このサービス ポリシーに名前を割り当てます。

例：`xConfiguration Policy Services Service 1 Name: 「Conference handler」`

xConfiguration Policy Services Service [1..20] Password: <S: 0,82>

リモートサービスにログインして照会するためにExpresswayが使用するパスワードを指定します。プレーン テキストの最大長は 30 文字で、これらの文字は暗号化されます。

例：`xConfiguration Policy Services Service 1 Password: 「password123」`

xConfiguration Policy Services Service [1..20] Path: <S: 0,255>

リモート サービスの URL を指定します。

例：`xConfiguration Policy Services Service 1 Path: 「service」`

xConfiguration Policy Services Service [1..20] Protocol: <HTTP/HTTPS>

リモートサービスに接続するために使用するプロトコルを指定します。デフォルトはHTTPSです。

例：`xConfiguration Policy Services Service 1 Protocol: HTTPS`

xConfiguration Policy Services Service [1..20] Server [1..3] Address: <S: 0,128>

リモート サービスの IP アドレスまたは完全修飾ドメイン名（FQDN）を指定します。

例：`xConfiguration Policy Services Service 1 Server 1 Address: 「192.168.0.0」`

xConfiguration Policy Services Service [1..20] Status Path: <S: 0..255>

リモート サービス ステータスを取得するためのパスを指定します。デフォルトは status です。

例：`xConfiguration Policy Services Service 1 Status Path: status`

xConfiguration Policy Services Service [1..20] TLS CRLCheck Mode: <On/Off>

ポリシー サービスによって提供された証明書の証明書失効リストのチェックを制御します。有効になっている場合は、サーバの X.509 証明書が、その証明書の証明書発行機関の失効リストと照合して確認されます。デフォルトは Off です。

例：`xConfiguration Policy Services Service 1 TLS CRLCheck Mode: Off`

xConfiguration Policy Services Service [1..20] TLS Verify Mode: <On/Off>

X.509 証明書のチェック、およびこの Expressway とポリシー サービス間の相互認証を制御します。有効になっている場合は、アドレス フィールドで指定したサーバの FQDN または IP アドレスがサーバの X.509 証明書内（サブジェクト共通名またはサブジェクト代替名のどちらかの属性）に含まれている必要があります。デフォルトは On です。

例：`xConfiguration Policy Services Service 1 TLS Verify Mode: On`

xConfiguration Policy Services Service [1..20] UserName: <S: 0,30>

リモートサービスにログインして照会するためにExpresswayが使用するユーザ名を指定します。

例：`xConfiguration Policy Services Service 1 UserName: 「user123」`

xConfiguration QoS Audio <0..63>

音声トラフィックの QoS マーキング用の DSCP（Differentiated Service Code Point）の値を定義します。DSCP 値は、Expressway を介してルーティングされる SIP と H.323 のオーディオ メディア トラフィックに、IP パケット ヘッダーにそれを記述することによってスタンプ（マーク）されます。IPv4 の場合は ToS フィールド、IPv6 の場合は TC フィールドに書き込まれます。値「「0」」は、標準のベストエフォートサービスを指定します。デフォルト：46。

変更を有効にするには、システムを再起動する必要があります。

例：`xConfiguration QoS Audio: 30`

xConfiguration QoS Video <0..63>

ビデオ トラフィックの QoS マーキング用の DSCP の値を定義します。DSCP 値は、Expressway を介してルーティングされる SIP と H.323 のビデオ メディア トラフィックに、IP パケット ヘッダーにそれを記述することによって スタンプ（マーク）されます。IPv4 の場合は ToS フィールド、IPv6 の場合は TC フィールドに書き込まれます。値「「0」」は、標準のベストエフォートサービスを指定します。デフォルト：34。

変更を有効にするには、システムを再起動する必要があります。

例:`xConfigurationのQoSのビデオ:43`

xConfiguration QoS XMPP <0..63>

IM & Presence トラフィックの QoS マーキング用の DSCP の値を定義します。DSCP 値は、Expressway を介してルーティングされる XMPP トラフィックに、IP パケット ヘッダーにそれを記述することによって スタンプ（マーク）されます。IPv4 の場合は ToS フィールド、IPv6 の場合は TC フィールドに書き込まれます。値「「0」」は、標準のベストエフォートサービスを指定します。デフォルト：24。

変更を有効にするには、システムを再起動する必要があります。

例:`xConfiguration QoS XMPP:34`

xConfiguration QoS Signaling <0..63>

シグナリング トラフィックの QoS マーキング用の DSCP の値を定義します。DSCP 値は、Expressway を介してルーティングされる SIP と H.323 のシグナリング トラフィックに、IP パケットヘッダーにそれを記述することによってスタンプ（マーク）されます。IPv4 の場合は ToS フィールド、IPv6 の場合は TC フィールドに書き込まれます。値「「0」」は、標準のベストエフォートサービスを指定します。デフォルト：24。

変更を有効にするには、システムを再起動する必要があります。

例：`xConfiguration QoS Signaling: 34`

xConfiguration Registration AllowList [1..2500] Description: <S: 0,64>

自由形式の許可リスト ルールの説明。

例：`xConfiguration Registration AllowList 1 Description: "Everybody at @example.com"`

xConfiguration Registration AllowList [1..2500] Pattern String: <S: 0, 60>

許可リストに追加するエントリを指定します。エンドポイントのエイリアスの 1 つが許可リストのパターンの 1 つと一致した場合に登録が許可されます。

例：`xConfiguration Registration AllowList 1 Pattern String: 「john.smith@example.com」`

xConfiguration Registration AllowList [1..2500] Pattern Type: <Exact/Prefix/Suffix/Regex>

許可リスト内のエントリがプレフィックスか、サフィックスか、正規表現か、または完全一致かを指定します。デフォルトは Exact です。

Exact：文字列は 1 文字も違うことなくエイリアスと一致する必要があります。

[プレフィックス（Prefix）]：文字列がエイリアスの先頭に表示される必要があります。

Suffix：文字列がエイリアスの末尾に表示される必要があります。

Regex：文字列は正規表現として処理されます。

例：`xConfiguration Registration AllowList 1 Pattern Type: Exact`

xConfiguration Registration AllowList [1..2500] Pattern Type: <Exact/Prefix/Suffix/Regex>

許可リスト内のエントリがプレフィックスか、サフィックスか、正規表現か、または完全一致かを指定します。デフォルトは Exact です。

Exact：文字列は 1 文字も違うことなくエイリアスと一致する必要があります。

[プレフィックス（Prefix）]：文字列がエイリアスの先頭に表示される必要があります。

Suffix：文字列がエイリアスの末尾に表示される必要があります。

Regex：文字列は正規表現として処理されます。

例：`xConfiguration Registration AllowList 1 Pattern Type: Exact`

xConfiguration Registration DenyList [1..2500] Description: <S: 0,64>

自由形式の拒否リスト ルールの説明。

例：`xConfiguration Registration DenyList 1 Description: 「Anybody at @nuisance.com」`

xConfiguration Registration DenyList [1..2500] Pattern String: <S: 0, 60>

拒否リストに追加するエントリを指定します。エンドポイントのエイリアスの 1 つが拒否リストのパターンの 1 つと一致した場合は登録が許可されません。

例：`xConfiguration Registration DenyList 1 Pattern String: 「john.jones@example.com」`

xConfiguration Registration DenyList [1..2500] Pattern Type: <Exact/Prefix/Suffix/Regex>

拒否リスト内のエントリがプレフィックスか、サフィックスか、正規表現か、または完全一致かを指定します。デフォルトは Exact です。

Exact：文字列は 1 文字も違うことなくエイリアスと一致する必要があります。

[プレフィックス（Prefix）]：文字列がエイリアスの先頭に表示される必要があります。

Suffix：文字列がエイリアスの末尾に表示される必要があります。

Regex：文字列は正規表現として処理されます。

例：`xConfiguration Registration DenyList 1 Pattern Type: Exact`

xConfiguration Registration RestrictionPolicy Mode: <None/AllowList/DenyList/Directory/PolicyService>

システムに登録できるエンドポイントを決定するときに使用するポリシーを指定します。デフォルト：[None]。

None：制限はありません。

AllowList：許可リストに設定されたエイリアスに登録しようとしているエンドポイントのみが登録できます。

DenyList：拒否リストに設定されたエイリアスに登録しようとしているエンドポイントを除くすべてのエンドポイントが登録できます。

Directory：ローカルディレクトリ内にあるエイリアスを登録するエンドポイントのみが登録できます。

PolicyService：ポリシーサービスで許可されている詳細で登録するエンドポイントのみが登録できます。

例：`xConfiguration Registration RestrictionPolicy Mode: None`

xConfiguration Registration RestrictionPolicy Service DefaultCPL: <S: 0,255>

リモート サービスが使用できない場合に Expressway が使用する CPL。デフォルトは <reject status='504' reason='Policy Service Unavailable'/> です。

例：`xConfiguration Registration RestrictionPolicy Service DefaultCPL: 「<reject status='403' reason='Service Unavailable'/>」`

xConfiguration Registration RestrictionPolicy Service Password: <S: 0,82>

リモートサービスにログインして照会するためにExpresswayが使用するパスワードを指定します。プレーン テキストの最大長は 30 文字で、これらの文字は暗号化されます。

例：`xConfiguration Registration RestrictionPolicy Service Password: 「password123」`

Configuration Registration RestrictionPolicy Service Path: <S: 0,255>

リモート サービスの URL を指定します。

例：`xConfiguration Registration RestrictionPolicy Service Path: 「service」`

xConfiguration Registration RestrictionPolicy Service Protocol: <HTTP/HTTPS>

リモートサービスに接続するために使用するプロトコルを指定します。デフォルトはHTTPSです。

例：`xConfiguration Registration RestrictionPolicy Service Protocol: HTTPS`

xConfiguration Registration RestrictionPolicy Service Server [1..3] Address: <S: 0,128>

リモート サービスの IP アドレスまたは完全修飾ドメイン名（FQDN）を指定します。

例：`xConfiguration Registration RestrictionPolicy Service Server 1 Address: 「192.168.0.0」`

xConfiguration Registration RestrictionPolicy Service Status Path: <S: 0..255>

リモート サービス ステータスを取得するためのパスを指定します。デフォルトは status です。

例：`xConfiguration Registration RestrictionPolicy Service Status Path: status`

xConfiguration Registration RestrictionPolicy Service TLS CRLCheck Mode: <On/Off>

ポリシー サービスによって提供された証明書の証明書失効リストのチェックを制御します。有効になっている場合は、サーバの X.509 証明書が、その証明書の証明書発行機関の失効リストと照合して確認されます。デフォルトは Off です。

例：`xConfiguration Registration RestrictionPolicy Service TLS CRLCheck Mode: Off`

xConfiguration Registration RestrictionPolicy Service TLS Verify Mode: <On/Off>

X.509 証明書のチェック、およびこの Expressway とポリシー サービス間の相互認証を制御します。有効になっている場合は、アドレス フィールドで指定したサーバの FQDN または IP アドレスがサーバの X.509 証明書内（サブジェクト共通名またはサブジェクト代替名のどちらかの属性）に含まれている必要があります。デフォルトは On です。

例：`xConfiguration Registration RestrictionPolicy Service TLS Verify Mode: On`

xConfiguration Registration RestrictionPolicy Service UserName: <S: 0,30>

リモートサービスにログインして照会するためにExpresswayが使用するユーザ名を指定します。

例：`xConfiguration Registration RestrictionPolicy Service UserName: 「user123」`

xConfiguration Remote Syslog [1..4] Address: <S: 0..128>

ログを書き込む最大 4 つのリモート syslog サーバの IP アドレスまたは完全修飾ドメイン名（FQDN）。これらのサーバは、BSD または IETF syslog プロトコルをサポートしている必要があります。

例：`xConfiguration Remote Syslog 1 Address: 「remote_server.example.com」`

xConfiguration Remote Syslog [1..4] Crlcheck: <On/Off>

syslog サーバが提供する証明書を証明書失効リスト（CRL）と照合して確認するかどうかを制御します。デフォルトは Off です。

例：`xConfiguration Remote Syslog 1 Crlcheck: Off`

xConfiguration Remote Syslog [1..4] Format: <bsd/ietf>

リモート syslog メッセージが作成される形式。デフォルトは bsd です。

例：`xConfiguration Remote Syslog 1 Format: bsd`

xConfiguration Remote Syslog [1..4] Loglevel: <emergency/alert/critical/error/warning/notice/informational/debug>

この syslog サーバに送信するログ メッセージの最小重大度を選択します。デフォルトは informational です。

例：`xConfiguration Remote Syslog 1 Loglevel: informational`

xConfiguration Remote Syslog [1..4] Mode: <bsd/ietf/ietf_secure/user_defined>

syslog サーバにメッセージを送信するときに使用する syslog プロトコルを選択します。または、user_defined を選択してトランスポート タイプ、ポート、および形式を個々に設定します。デフォルトは bsd です。

例：`xConfiguration Remote Syslog 1 Mode: bsd`

xConfiguration Remote Syslog [1..4] Port: <1..65535>

使用する UDP/TCP 宛先ポート。推奨されるポート：UDP=514 TCP/TLS=6514 デフォルト：514。

例：`xConfiguration Remote Syslog 1 Port: 514`

xConfiguration Remote Syslog [1..4] Transport: <udp/tcp/tls>

syslog サーバと通信するときに使用するトランスポート プロトコル。TLS 暗号化を使用する場合、適切な CA 証明書ファイルをアップロードする必要があります。デフォルトは UDP です。

例：`xConfiguration Remote Syslog 1 Transport: udp`

xConfiguration ResourceUsage Warning Activation Level: <0..100>

コール数または登録数がライセンス供与された最大キャパシティに到達していることを Expressway がいつどのような場合に警告するかを制御します。この数は、到達したときに警告をトリガーする最大数のパーセンテージを表します。0：警告は表示されません。デフォルト：90。

例：`xConfiguration ResourceUsage Warning Activation Level: 90`

xConfiguration SIP Advanced SipMaxSize: <1..1048576>

サーバで処理できる 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 `32768` です。

例：`xConfiguration SIP Advanced SipMaxSize: 32768`

xConfiguration SIP Advanced SipTcpConnectTimeout: <1..150>

発信 SIP TCP 接続が確立されるまで待機する最大秒数を入力します。デフォルトは 10 です。

例：`xConfiguration SIP Advanced SipTcpConnectTimeout: 10`

xConfiguration SIP Advanced SipTlsDhKeySize: <1024/2048/3072>

Diffie-Hellmanキー交換を使用する着信接続にデフォルト キーのサイズを指定します（ビット）。

デフォルト：1024。

（注） 変更を有効にするには、システムを再起動する必要があります。

例：`xConfiguration SIP Advanced SipTlsDhKeySize: 1024`

xConfiguration SIP Advanced SipTlsVersions: <TLSv1/TLSv1.1/TLSv1.2/TLSv1:TLSv1.1/TLSv1:TLSv1.2/TLSv1.1:TLSv1.2/TLSv1:TLSv1.1:TLSv1.2>

サポートされる SIP TLS プロトコル バージョンを指定します。デフォルト:TLSv1:TLSv1.1:TLSv1.2

例：`xConfiguration SIP Advanced SipTlsVersions: TLSv1.1:TLSv1.2`

xConfiguration SIP Authentication Digest Nonce ExpireDelta: <30..3600>

nonce を再利用できる最大時間（秒単位）を指定します。デフォルトは 300 です。

例：`xConfiguration SIP Authentication Digest Nonce ExpireDelta: 300`

xConfiguration SIP Authentication Digest Nonce Length: <32..512>

SIP ダイジェスト認証で使用するために生成する nonce または cnonce の長さ。デフォルトは 60 です。

例：`xConfiguration SIP Authentication Digest Nonce Length: 60`

xConfiguration SIP Authentication Digest Nonce Limit: <1..65535>

保存する nonce の数の最大限度。デフォルト：10000。

例：`xConfiguration SIP Authentication Digest Nonce Limit: 10000`

xConfiguration SIP Authentication Digest Nonce Maximum Use Count: <1..1024>

Expressway が生成する nonce をクライアントが使用できる最大回数。デフォルト：128。

例：`xConfiguration SIP Authentication Digest Nonce Maximum Use Count: 128`

xConfiguration SIP Authentication NTLM Mode: <On/Off/Auto>

NTLM プロトコルを使用して Expressway がエンドポイントにいつチャレンジするかを制御します。デフォルトは Auto です。

Off：Expressway は NTLM プロトコルを含むチャレンジを送信しません。

On：Expressway は常に NTLM をチャレンジに組み込みます。

Auto：Expressway はエンドポイントのタイプに基づいて NTLM でチャレンジするかどうかを決定します。

例：`xConfiguration SIP Authentication NTLM Mode: Auto`

xConfiguration SIP Authentication NTLM SA Lifetime: <30..43200>

NTLM セキュリティ アソシエーションのライフタイムを秒単位で指定します。デフォルト：28800。

例：`xConfiguration SIP Authentication NTLM SA Lifetime: 28800`

xConfiguration SIP Authentication NTLM SA Limit: <1..65535>

保存する NTLM セキュリティ アソシエーションの最大数。デフォルトは 10000 です。

例：`xConfiguration SIP Authentication NTLM SA Limit: 10000`

xConfiguration SIP Authentication Retry Limit: <1..16>

403 Forbidden 応答を受信する前に、認証の失敗によって SIP UA がチャレンジする回数。これが SIP ダイジェストのチャレンジ（NTLM 以外のチャレンジ）のみにみ適用されます。デフォルトは 3 です。

例：`xConfiguration SIP Authentication Retry Limit: 3`

xConfiguration SIP Domain [1..200] Authzone: <S: 0,128>

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。

例：`xConfiguration SIP Domain 1 Authzone: 「traversalzone」`

xConfiguration SIP Domain [1..200] Edge: <On/Off>

リモートおよびモバイルのコラボレーション機能が有効かどうか。デフォルトは Off です。

例：`xConfiguration SIP Domain 1 Edge: On`

xConfiguration SIP Domain [1..200] Name: <S: 0,128>

この Expressway が権限を持つドメインを指定します。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。

例：`xConfiguration SIP Domain 1 Name: 「100.example-name.com」`

xConfiguration SIP Domain [1..200] Sip: <On/Off>

Expressway はこのドメインの SIP レジストラとして機能し、このドメインを含むエイリアスで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るかどうかを指定します。デフォルトは On です。

例：`xConfiguration SIP Domain 1 Sip: On`

xConfiguration SIP GRUU Mode: <On/Off>

GRUU（RFC5627）サポートがアクティブかどうかを制御します。デフォルトは On です。

例：`xConfiguration SIP GRUU Mode: On`

xConfiguration SIP MediaRouting ICE Mode: <On/Off>

ICE 参加者が NAT デバイスの背後まで通過する場合に ICE から ICE 以外のコールのメディアを Expressway が取得するかどうかを制御します。デフォルトは Off です。

例：`xConfiguration SIP MediaRouting ICE Mode: Off`

xConfiguration SIP Mode: <On/Off>

Expressway が SIP レジストラと SIP プロキシの機能を提供するかどうかを決定します。デフォルトは Off です。

例：`xConfiguration SIP Mode: On`

xConfiguration SIP PreRoutedRouteHeader: <S:0,128>

事前にルーティングした新しいルートヘッダーパスの通過を許可する要求メッセージを制御します。

X12.5 と同様に、このフラグは SIP REGISTER メッセージに対してのみ使用できます。

例：`xConfiguration SIP PreRoutedRouteHeader: 「REGISTER」`

xConfiguration SIP Registration Call Remove: <Yes/No>

SIP 登録の期限が切れか、または削除されたときに、関連付けられたコールをドロップするかどうかを指定します。デフォルトは No です。

例：`xConfiguration SIP Registration Call Remove: No`

xConfiguration SIP Registration Mode: <Off/On>

Expressway が SIP 登録を提供するかどうかを決定します。デフォルトは On です。

例：`xConfiguration SIP Registration Proxy Mode: Off`

xConfiguration SIP Registration Outbound Flow Timer: <0..600>

アウトバウンド登録応答内の Flow-Timer ヘッダーの値を指定します。ユーザエージェントがキープアライブを送信していない場合に、サーバが登録フローが終了したと見なした後の秒数を定義します。デフォルトは 0 です（ヘッダーは追加されません）。

例：`xConfiguration SIP Registration Outbound Flow Timer: 0`

xConfiguration SIP Registration Outbound Refresh Maximum: <30..7200>

アウトバウンド登録の 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には、小さな値（[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）が返されることになります。デフォルトは 3600 秒です。

例：`xConfiguration SIP Registration Outbound Refresh Maximum: 3600`

xConfiguration SIP Registration Outbound Refresh Minimum: <30..7200>

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。この値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。

例：`xConfiguration SIP Registration Outbound Refresh Minimum: 300`

onfiguration SIP Registration Outbound Refresh Strategy: <Maximum/Variable>

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。デフォルトはVariableです。

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。

例：`xConfiguration SIP Registration Outbound Refresh Strategy: Variable`

xConfiguration SIP Registration Proxy Mode: <Off/ProxyToKnownOnly/ProxyToAny>

プロキシ登録をどのように処理するかを指定します。デフォルトは Off です。

Off：登録要求はプロキシ経由で送信されません。

ProxyToKnownOnly：登録要求はプロキシ経由でネイバーのみに送信されます。

ProxyToAny：登録要求は、Expressway の既存のコール処理ルールに従ってプロキシ経由で送信されます。

例：`xConfiguration SIP Registration Proxy Mode: Off`

xConfiguration SIP Registration Standard Refresh Maximum: <30..7200>

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。その値は、標準的な登録更新戦略に従って計算されます。デフォルトは 60 秒です。

例：`xConfiguration SIP Registration Standard Refresh Maximum: 60`

xConfiguration SIP Registration Standard Refresh Minimum: <30..3600>

標準的な登録についての SIP 登録更新期間の最小許容値。この値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。

例：`xConfiguration SIP Registration Standard Refresh Minimum: 45`

xConfiguration SIP Registration Standard Refresh Strategy: <Maximum/Variable>

標準的な登録についてのSIP登録有効期限の生成に使用する方法。デフォルトはMaximumです。

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。

例：`xConfiguration SIP Registration Standard Refresh Strategy: Maximum`

xConfiguration SIP Require Duo Video Mode: <On/Off>

Expressway でサポートするエンドポイントに com.tandberg.sdp.duo.enable 拡張子を使用する必要があるかどうかを制御します。デフォルトは On です。

例：`xConfiguration SIP Require Duo Video Mode: On`

xConfiguration SIP Require UDP BFCP Mode: <On/Off>

Expressway でサポートするエンドポイントに com.tandberg.udp.bfcp 拡張子を使用する必要があるかどうかを制御します。デフォルトは On です。

例：`xConfiguration SIP Require UDP BFCP Mode: On`

xConfiguration SIP Routes Route [1..20] Address: <S:0,39>

一致している SIP 要求が転送されるこのルートのネクスト ホップの IP アドレスを指定します。注：このコマンドは、開発者のみが使用できます。

例：`xConfiguration SIP Routes Route 1 Address: "127.0.0.1"`

xConfiguration SIP Routes Route [1..20] Authenticated: <On/Off>

認証した要求を転送するかどうか。デフォルトは Off です。注：このコマンドは、開発者のみが使用できます。

On：着信メッセージが認証されている場合にのみ、要求をルートに転送します。

Off：このルートに一致するメッセージを常に転送します。

例：`xConfiguration SIP Routes Route 1 Authenticated: On`

xConfiguration SIP Routes Route [1..20] Header Name: <S:0,64>

照合する SIP ヘッダー フィールドの名前（Event など）。注：このコマンドは、開発者のみが使用できます。

例：`xConfiguration SIP Routes Route 1 Header Name: "Event"`

xConfiguration SIP Routes Route [1..20] Header Pattern: <S:0,128>

指定した SIP ヘッダー フィールドと照合する正規表現。注：このコマンドは、開発者のみが使用できます。

例：`xConfiguration SIP Routes Route 1 Header Pattern: 「(my-event-package)(.*)」`

xConfiguration SIP Routes Route [1..20] Method: <S:0,64>

このルートを選択するために照会する SIP メソッド（INVITE、SUBSCRIBE など）。注：このコマンドは、開発者のみが使用できます。

例：`xConfiguration SIP Routes Route 1 Method: 「SUBSCRIBE」`

xConfiguration SIP Routes Route [1..20] Port: <1..65534>

一致している SIP 要求がルーティングされるこのルートのネクスト ホップ上のポートを指定します。デフォルトは 5060 です。注：このコマンドは、開発者のみが使用できます。

例：`xConfiguration SIP Routes Route 1 Port: 22400`

xConfiguration SIP Routes Route [1..20] Request Line Pattern: <S:0,128>

SIP 要求の行と照合する正規表現。注：このコマンドは、開発者のみが使用できます。

例：`xConfiguration SIP Routes Route 1 Request Line Pattern: 「.*@(%localdomains%|%ip%)」`

xConfiguration SIP Routes Route [1..20] Tag: <S:0,64>

作成するルートを識別するために外部アプリケーションが指定したタグ値。注：このコマンドは、開発者のみが使用できます。

例：`xConfiguration SIP Routes Route 1 Tag: 「Tag1」`

xConfiguration SIP Routes Route [1..20] Transport: <UDP/TCP/TLS>

このルートに転送された SIP メッセージに使用するトランスポート タイプを決定します。デフォルトは TCP です。注：このコマンドは、開発者のみが使用できます。

例：`xConfiguration SIP Routes Route 1 Transport: TCP`

xConfiguration SIP Session Refresh Minimum: <90..7200>

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。詳細については、RFC 4028 の Min-SE ヘッダーの定義を参照してください。デフォルトは 500 です。

例：`xConfiguration SIP Session Refresh Minimum: 500`

xConfiguration SIP Session Refresh Value: <90..86400>

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。詳細については、RFC 4028 の Session-Expires の定義を参照してください。デフォルトは 1800 です。

例：`xConfiguration SIP Session Refresh Value: 1800`

xConfiguration SIP TCP Mode: <On/Off>

TCP プロトコルを使用した着信 SIP コールと発信 SIP コールを許可するかどうかを決定します。デフォルトは Off です。

例：`xConfiguration SIP TCP Mode: On`

xConfiguration SIP TCP Outbound Port End: <1024..65534>

アウトバウンド TCP/TLS SIP 接続で使用する範囲内の上位ポートを指定します。デフォルトは 29999 です。

例：`xConfiguration SIP TCP Outbound Port End: 29999`

xConfiguration SIP TCP Outbound Port Start: <1024..65534>

アウトバウンド TCP/TLS SIP 接続で使用する範囲内の下位ポートを指定します。デフォルトは 25000 です。

例：`xConfiguration SIP TCP Outbound Port Start: 25000`

xConfiguration SIP TCP Port: <1024..65534>

着信 SIP TCP コールのリスニング ポートを指定します。デフォルトは 5060 です。

例：`xConfiguration SIP TCP Port: 5060`

xConfiguration SIP TLS Certificate Revocation Checking CRL Mode: <On/Off>

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 Expressway に手動でダウンロードするか、または事前に設定された URI から自動的にダウンロードするか、あるいは X.509 証明書に含まれた CRL 配布ポイント（CDP）URI から自動的にダウンロードすることができます。デフォルトは On です。

例：`xConfiguration SIP TLS Certificate Revocation Checking CRL Mode: On`

xConfiguration SIP TLS Certificate Revocation Checking CRL Network Fetch Mode: <On/Off>

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。デフォルトは On です。

例：`xConfiguration SIP TLS Certificate Revocation Checking CRL Network Fetch Mode: On`

xConfiguration SIP TLS Certificate Revocation Checking Mode: <On/Off>

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。デフォルトは Off です。

例：`xConfiguration SIP TLS Certificate Revocation Checking Mode: Off`

xConfiguration SIP TLS Certificate Revocation Checking OCSP Mode: <On/Off>

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、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。デフォルトは On です。

例：`xConfiguration SIP TLS Certificate Revocation Checking OCSP Mode: On`

xConfiguration SIP TLS Certificate Revocation Checking Source Inaccessibility Behavior: <Ignore/Fail>

失効の送信元に接続できない場合の失効確認動作を制御します。デフォルトは Fail です。

Fail：失効しているものとして証明書を処理します（したがって、TLS 接続は許可しません）。

Ignore：失効していないものとして証明書を処理します。

例：`xConfiguration SIP TLS Certificate Revocation Checking Source Inaccessibility Behavior: Fail`

xConfiguration SIP TLS Mode: <On/Off>

TLS プロトコルを使用した着信 SIP コールと発信 SIP コールを許可するかどうかを決定します。デフォルトは On です。

例：`xConfiguration SIP TLS Mode: On`

xConfiguration SIP TLS Port: <1024..65534>

着信 SIP TLS コールのリスニング ポートを指定します。デフォルトは 5061 です。

例：`xConfiguration SIP TLS Port: 5061`

xConfiguration SIP UDP Mode: <On/Off>

UDP プロトコルを使用した着信 SIP コールと発信 SIP コールを許可するかどうかを決定します。デフォルトは Off です。

例：`xConfiguration SIP UDP Mode: On`

xConfiguration SIP UDP Port: <1024..65534>

着信 SIP UDP コールのリスニング ポートを指定します。デフォルト：5060。

例：`xConfiguration SIP UDP Port: 5060`

xConfiguration SNMP CommunityName: <S: 0, 16>

Expressway の SNMP コミュニティ名。デフォルト：public

例：`xConfiguration SNMP CommunityName: 「public」`

xConfiguration SNMP SystemContact: <S: 0, 70>

Expressway の問題についての問い合わせが可能な担当者の名前。デフォルトは Administrator です。

例：`xConfiguration SNMP SystemContact: Administrator`

xConfiguration SNMP SystemLocation: <S: 0, 70>

The physical location of the system.

例：`xConfiguration SNMP SystemLocation: 「Server Room 128」`

xConfiguration SNMP V1Mode: <On/Off>

SNMP バージョン 1 のサポートを有効または無効にします。デフォルトは Off です。

例：`xConfiguration SNMP V1Mode: Off`

xConfiguration SNMP V2cMode: <On/Off>

SNMP バージョン 2c のサポートを有効または無効にします。デフォルトは On です。

例：`xConfiguration SNMP V2cMode: On`

xConfiguration SNMP V3AuthenticationMode: <On/Off>

SNMP バージョン 3 の認証を有効または無効にします。デフォルトは On です。

例：`xConfiguration SNMP V3AuthenticationMode: On`

xConfiguration SNMP V3AuthenticationPassword: <S: 0,215>

SNMP バージョン 3 の認証パスワードを設定します。パスワードは 8 文字以上にする必要があります。

例：`xConfiguration SNMP V3AuthenticationPassword: 「password123」`

xConfiguration SNMP V3AuthenticationType: <MD5/SHA>

SNMP バージョン 3 の認証タイプを設定します。デフォルトは SHA です。

例：`xConfiguration SNMP V3AuthenticationType: SHA`

xConfiguration SNMP V3Mode: <On/Off>

SNMP バージョン 3 のサポートを有効または無効にします。デフォルトは On です。

例：`xConfiguration SNMPV3 Mode: On`

xConfiguration SNMP V3PrivacyMode: <On/Off>

SNMP バージョン 3 のプライバシーを有効または無効にします。デフォルトは On です。

例：`xConfiguration SNMP V3PrivacyMode: On`

xConfiguration SNMP V3PrivacyPassword: <S: 0,215>

SNMP バージョン 3 のプライバシー パスワードを設定します。パスワードは 8 文字以上にする必要があります。

例：`xConfiguration SNMP V3PrivacyPassword: 「password123」`

xConfiguration SNMP V3PrivacyType: <AES>

SNMP バージョン 3 のプライバシー タイプを設定します。デフォルトは AES です。

例：`xConfiguration SNMP V3PrivacyType: AES`

xConfiguration SNMP V3UserName: <S: 0,70>

SNMP V3 を使用するときに使用するユーザ名を設定します。

例：`xConfiguration SNMP V3UserName: 「user123」`

xConfiguration SystemUnit Maintenance Mode: <On/Off>

メンテナンスモードにExpresswayを設定します。新しいコールと登録は拒否され、既存のコールと登録は期限切れにできます。デフォルトは Off です。

例：`xConfiguration SystemUnit Maintenance Mode: Off`

xConfiguration SystemUnit Name: <S:, 0, 50>

Expresswayの名前を定義します。システム名は Web インターフェイスのさまざまな場所やユニットの前面パネルに表示されます。システムを一意に識別する名前を選択します。

例：`xConfiguration SystemUnit Name: 「MainHQ」`

xConfiguration TimeZone Name: <S: 0, 64>

Expressway のローカル タイム ゾーンを設定します。タイム ゾーンの名前は、POSIX 命名規則（Europe/London や America/New_York など）に従います。デフォルトは GMT です。

例：`xConfiguration TimeZone Name: 「GMT」`

xConfiguration Transform [1..100] Description: <S: 0,64>

自由形式のトランスフォーメーションの説明。

例：`xConfiguration Transform [1..100] Description: 「Change example.net to example.com」`

xConfiguration Transform [1..100] Pattern Behavior: <Strip/Replace>

エイリアスをどのように変更するかを示します。デフォルトは Strip です。

Strip：一致しているプレフィックスまたはサフィックスをエイリアスから削除します。

Replace：置換文字列内のテキストでエイリアスの一致している部分を置換します。

AddPrefix：エイリアスの前に置換文字列を追加します。

AddSuffix：エイリアスの後ろに置換文字列を追加します。

例：`xConfiguration Transform 1 Pattern Behavior: Replace`

xConfiguration Transform [1..100] Pattern Replace: <S: 0, 60>

選択したパターン動作とともに使用するテキスト文字列。

例：`xConfiguration Transform 1 Pattern Replace: 「example.com」`

xConfiguration Transform [1..100] Pattern String: <S: 0, 60>

エイリアスと比較するパターン。

例：`xConfiguration Transform 1 Pattern String: 「example.net」`

Configuration Transform [1..100] Pattern Type: <Exact/Prefix/Suffix/Regex>

適用するトランスフォーメーションで、パターン文字列をエイリアスとどのように照合するか。デフォルトは Prefix です。

*[*完全一致（*Exact*）*]*：文字列全体がエイリアスと 1 文字も違うことなく完全に一致する必要があります。

*[*プレフィックス（*Prefix*）*]*：文字列がエイリアスの先頭に表示される必要があります。

Suffix：文字列がエイリアスの末尾に表示される必要があります。

Regex：文字列は正規表現として処理されます。

例：`xConfiguration Transform 1 Pattern Type: Suffix`

xConfiguration Transform [1..100] Priority: <1..65534>

指定したトランスフォーメーションにプライオリティを割り当てます。トランスフォーメーションはプライオリティ順に着信メッセージと比較されます。また、プライオリティはトランスフォーメーションごとに一意である必要があります。デフォルトは 1 です。

例：`xConfiguration Transform 1 Priority: 10`

xConfiguration Transform [1..100] State: <Enabled/Disabled>

トランスフォーメーションが有効になっているか、無効になっているかを示します。無効になっているトランスフォーメーションは無視されます。

例：`xConfiguration Transform 1 State: Enabled`

xConfiguration Traversal Media Port End: <1025..65533>

トラバーサル コールでは（Expressway がシグナリングとともにメディアも取得する）、メディアに使用する範囲の上位ポートを指定します。ポートはこの範囲からペアで割り当てられ、各ペアの最初は偶数になります。したがって、この範囲は奇数で終了する必要があります。デフォルトは 59999 です。

例：`xConfiguration Traversal Media Port End: 59999`

xConfiguration Traversal Media Port Start: <1024..65532>

トラバーサル コールでは（Expressway がシグナリングとともにメディアも取得する）、メディアに使用する範囲の下位ポートを指定します。ポートはこの範囲からペアで割り当てられ、各ペアの最初は偶数になります。したがって、この範囲は偶数で始まる必要があります。デフォルトは 36000 です。

例：`xConfiguration Traversal Media Port Start: 36000`

xConfiguration Traversal Server H323 Assent CallSignaling Port: <1024..65534>

Assent シグナリングに使用する Expressway 上のポート。デフォルトは 2776 です。

例：`xConfiguration Traversal Server H323 Assent CallSignaling Port: 2777`

xConfiguration Traversal Server H323 H46018 CallSignaling Port: <1024..65534>

H460.18 シグナリングに使用する Expressway 上のポート。デフォルトは 2777 です。

例：`xConfiguration Traversal Server H323 H46018 CallSignaling Port: 2777`

xConfiguration Traversal Server TURN Authentication Realm: <S: 1,128>

認証チャレンジでサーバが送信するレルム。デフォルトは TANDBERG です。

例：`xConfiguration Traversal Server TURN Authentication Realm: 「TANDBERG」`

xConfiguration Traversal Server TURN Authentication Remote Mode: <On/Off>

サーバが要求を認証する必要があるかどうかを決定します。有効にすると、サーバはその応答も認証します。デフォルトは On です。

例：`xConfiguration Traversal Server TURN Authentication Remote Mode: On`

xConfiguration Traversal Server TURN Media Port End: <1024..65534>

TURN リレーに使用する範囲の上位ポート。デフォルトは 61799 です。

例：`xConfiguration Traversal Server TURN Media Port End: 61799`

xConfiguration Traversal Server TURN Media Port Start: <1024..65534>

TURN リレーに使用する範囲の下位ポート。デフォルトは 60000 です。

例：`xConfiguration Traversal Server TURN Media Port Start: 60000`

xConfiguration Traversal Server TURN Mode: <On/Off>

Expressway が TURN サービスをトラバーサル クライアントに提供するかどうかを決定します。デフォルトは Off です。

例：`xConfiguration Traversal Server TURN Mode: Off`

xConfiguration Traversal Server TURN Port: <1024..65534>

TURN 要求のリスニング ポート。デフォルトは 3478 です。

例：`xConfiguration Traversal Server TURN Port: 3478`

xConfiguration Traversal Server TURN PortRangeEnd: <1024..65534>

TURN 要求に使用する範囲の上位ポート。デフォルトは 3483 です。

例：`xConfiguration Traversal Server TURN PortRangeEnd: 3483`

xConfiguration Traversal Server TURN PortRangeStart: <1024..65534>

TURN 要求に使用する範囲の下位ポート。デフォルトは 3478 です。

例：`xConfiguration Traversal Server TURN PortRangeStart: 3478`

Configuration Traversal Server TURN ProtocolMode: <TCP/UDP/Both>

TURN 要求に許可されたプロトコル。デフォルトは [両方（Both）] です。

例：`xConfiguration Traversal Server TURN ProtocolMode: Both`

xConfiguration xConfiguration Traversal Server TURN Authentication Mode: <On/Off>>

サーバで要求の認証を必要とするかどうかを指定します。有効にすると、サーバはその応答も認証します。デフォルトは On です。

例：`xConfiguration Traversal Server TURN Authentication Mode: On`

xConfiguration XCP Config FcmService: <On/Off>

MRA を使用した Jabber Android デバイスの FCM プッシュ通知を有効にするかどうかを制御します。デフォルトは Off です。

例：`xConfiguration XCP Config FcmService: On`

xConfiguration XCP DelayedRestart EnableDelayedRestart: <On/Off>

Cisco XCP ルータの遅延再起動機能が有効かどうかを制御します。デフォルトは Off です。

例：`xConfiguration DelayedRestart EnableDelayedRestart: On`

xConfiguration XCP DelayedRestart EnableScheduledRestart: <On/Off>

Cisco XCP ルータのスケジュール設定された再起動が有効かどうかを制御します。デフォルトは Off です。

例：`xConfiguration XCP DelayedRestart EnableScheduledRestart: On`

xConfiguration XCP DelayedRestart MultitenancyEnabled: <On/Off>

マルチテナンシーをオンにして、Cisco XCP ルータの遅延再起動を設定します。デフォルトは Off です。

例：`xConfiguration XCP DelayedRestart MultitenancyEnabled: On`

xConfiguration XCP DelayedRestart ScheduledTime:

スケジュール設定された再起動が実行される毎日の時刻。

例：`xConfiguration XCP DelayedRestart ScheduledTime: 01.00`

xConfiguration XCP DelayedRestartNotify RestartTime:

再起動時間の通知を設定します。

例：`xConfiguration DelayedRestartNotify RestartTime: 01.00`

xConfiguration XCP TLS Certificate CVS CertificateRevocationCheck: <On/Off>

証明書失効リスト（CRL）を XCP TLS 接続の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 の使用に加えて、CRL は Expressway に手動でダウンロードするか、または事前に設定された URI から自動的にダウンロードするか、あるいは X.509 証明書に含まれた CRL 配布ポイント（CDP）URI から自動的にダウンロードすることができます。デフォルトは Off です。

例：`xConfiguration XCP TLS Certificate CVS CertificateRevocationCheck: Off`

xConfiguration XCP TLS Certificate CVS ConvertIpToHostname: <On/Off>

Expressway が証明書の確認のために自動的に XCP ピアの IP アドレスを FQDN に変換するかどうかを制御します。デフォルトは On です。

例：`xConfiguration XCP TLS Certificate CVS ConvertIpToHostname: On`

xConfiguration XCP TLS Certificate CVS CrlNetworkFetchEnabled: <On/Off>

Expressway にその 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。デフォルトは On です。

例：`xConfiguration XCP TLS Certificate CVS CrlNetworkFetchEnabled: On`

xConfiguration XCP TLS Certificate CVS EnableCvs: <On/Off>

XCP TLS 接続時に XCP ピアの証明書を確認するかどうかを制御します。*Off* にすると、そのほかすべての XCP TLS 証明書 CVS の設定オプションが無効になります。デフォルトは On です。

例：`xConfiguration XCP TLS Certificate CVS EnableCvs: On`

xConfiguration XCP TLS Certificate CVS FailOnInaccessibleSource: <On/Off>

失効の送信元に接続できない場合の証明書の確認動作を制御します。

On：失効しているものとして証明書を処理します（したがって、TLS接続は許可しません）。

Off：失効していないものとして証明書を処理します。

デフォルトは On です。

例：`xConfiguration XCP TLS Certificate CVS FailOnInaccessibleSource: On`

xConfiguration XCP TLS Certificate CVS UseCrl: <On/Off>

XCP TLS 接続の確立時に交換される証明書の失効について、Expressway が自身の CRL を確認するかどうかを制御します。デフォルトは On です。

例：`xConfiguration XCP TLS Certificate CVS UseCrl: On`

xConfiguration XCP TLS Certificate CVS UseOcsp: <On/Off>

証明書が失効しているかどうかを確認するために、Expressway が OCSP を使用して証明書失効チェックを実行できるかどうかを制御します。OCSP を使用するには、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。デフォルトは On です。

例：`xConfiguration XCP TLS Certificate CVS UseOcsp: On`

xConfiguration XCP TLS Certificate CVS VerifyHostname: <On/Off>

Expressway が自身のピアの設定に対し、XCP ホストの証明書を確認するかどうかを制御します。デフォルトは On です。

例：`xConfiguration XCP TLS Certificate CVS VerifyHostname: On`

xConfiguration Zones DefaultZone Authentication Mode: <DoNotCheckCredentials/TreatAsAuthenticated/CheckCredentials>

Expressway がこのゾーンからの着信メッセージをどのように認証するかを制御し、それらのメッセージを認証または未認証として処理するか、あるいは拒否するかを制御します。H.323 メッセージ、ローカル ドメインから発信される SIP メッセージか非ローカル ドメインから発信される SIP メッセージかによって動作が異なります。デフォルトは DoNotCheckCredentials です。

例：`xConfiguration Zones DefaultZone Authentication Mode: DoNotCheckCredentials`

xConfiguration Zones DefaultZone SIP Media Encryption Mode: <Off/On/BestEffort/Auto>

このゾーンで送受信される SIP コール（インターワーキング コールを含む）に Expressway によって適用されるメディア暗号化ポリシー。デフォルトは Auto です。

On：すべてのメディアを暗号化する必要があります。

Off：すべてのメディアの暗号化を解除する必要があります。

BestEffort：使用可能な場合は暗号化を使用します。使用できない場合は暗号化されていないメディアにフォールバックします。

Auto：メディア暗号化ポリシーは適用されません。

例：`xConfiguration Zones DefaultZone SIP Media Encryption Mode: Auto`

xConfiguration Zones DefaultZone SIP Media ICE Support: <On/Off>

このゾーン内のデバイスで ICE をサポートするかどうかを制御します。デフォルトは Off です。

On：このゾーンでは ICE をサポートします。

Off：このゾーンでは ICE をサポートしません。

例：`xConfiguration Zones DefaultZone SIP Media ICE Support: On`

xConfiguration Zones DefaultZone SIP Multistream Mode: <Off/On>

Expresswayがこのゾーンのデバイス間のマルチストリームを許可するかどうかを制御します。デフォルトは On です。

On：マルチストリームを許可します。

Off：マルチストリームを拒否します。

例：`xConfiguration Zones DefaultZone SIP Multistream Mode: Off`

xConfiguration Zones DefaultZone SIP Record Route Address Type: <IP/Hostname>

Expressway がその IP アドレスを使用するか、このゾーンへの発信 SIP 要求の Record-Route または Path ヘッダーのホスト名を使用するかを制御します。注：ホスト名にこの値を設定すると、有効な DNS システム ホスト名も Expressway で設定する必要があります。デフォルトは IP です。

例：`xConfiguration Zones DefaultZone SIP Record Route Address Type: IP`

xConfiguration Zones DefaultZone SIP SipUpdateRefresh Support: <On/Off>

このゾーンで SIP UPDATE メッセージによるセッション更新をサポートするかどうかを指定します。

On：*SIP* セッションを更新するために、このゾーンから *SIP UPDATE* メッセージを送信します。

Off：このゾーンでは *SIP* セッション更新用の *SIP UPDATE* メッセージを送信しません。

デフォルトは Off です。

例：`xConfiguration Zones DefaultZone SIP SipUpdateRefresh Support: Off`

xConfiguration Zones DefaultZone SIP TLS Verify Mode: <On/Off>

外部サービスによって提供される証明書に記載されているホスト名を Expressway で検証するかどうかを制御します。有効にすると、証明書のホスト名（共通名とも呼ぶ）は、デフォルト ゾーンのアクセス ルールで指定されたパターンと照合されます。デフォルトは Off です。

例：`xConfiguration Zones DefaultZone SIP TLS Verify Mode: Off`

xConfiguration Zones LocalZone DefaultSubZone Authentication Mode: <DoNotCheckCredentials/TreatAsAuthenticated/CheckCredentials>

Expressway がこのサブゾーンからの着信メッセージをどのように認証するかを制御し、それらのメッセージを認証または未認証として処理するか、あるいは拒否するかを制御します。H.323 メッセージ、ローカル ドメインから発信される SIP メッセージか非ローカル ドメインから発信される SIP メッセージかによって動作が異なります。デフォルトは DoNotCheckCredentials です。

例：`xConfiguration Zones LocalZone DefaultSubZone Authentication Mode: DoNotCheckCredentials`

xConfiguration Zones LocalZone DefaultSubZone Bandwidth PerCall Inter Limit: <1..100000000>

デフォルト サブゾーン内のエンドポイントで送受信するすべてのコールの帯域幅制限（モードが Limited に設定されている場合にのみ適用）。デフォルトは 1920 です。

例：`xConfiguration Zones LocalZone DefaultSubZone Bandwidth PerCall Inter Limit: 1920`

Configuration Zones LocalZone DefaultSubZone Bandwidth PerCall Inter Mode: <Limited/Unlimited/NoBandwidth>

デフォルト サブゾーン内のエンドポイントで送受信するすべてのコールの帯域幅に制限を設けるかどうかを制御します。

NoBandwidth：使用可能な帯域幅はありません。デフォルト サブゾーンとの間でコールを行うことはできません。

デフォルトは Unlimited です。

例：`xConfiguration Zones LocalZone DefaultSubZone Bandwidth PerCall Inter Mode: Limited`

xConfiguration Zones LocalZone DefaultSubZone Bandwidth PerCall Intra Limit: <1..100000000>

デフォルト サブゾーン内の 2 つのエンドポイント間のすべてのコールの帯域幅制限（モードが Limited に設定されている場合にのみ適用）。デフォルトは 1920 です。

例：`xConfiguration Zones LocalZone DefaultSubZone Bandwidth PerCall Intra Limit: 1920`

xConfiguration Zones LocalZone DefaultSubZone Bandwidth PerCall Intra Mode: <Limited/Unlimited/NoBandwidth>

デフォルト サブゾーン内の 2 つのエンドポイント間のいずれかのコールの帯域幅に制限を設けるかどうかを制御します。

NoBandwidth：使用可能な帯域幅はありません。デフォルト サブゾーン内ではコールを発信できません。

デフォルトは Unlimited です。

例：`xConfiguration Zones LocalZone DefaultSubZone Bandwidth PerCall Intra Mode: Limited`

xConfiguration Zones LocalZone DefaultSubZone Bandwidth Total Limit: <1..100000000>

デフォルト サブゾーンの総帯域幅制限を設定します（モードが Limited に設定されている場合にのみ適用）。デフォルトは 500000 です。

例：`xConfiguration Zones LocalZone DefaultSubZone Bandwidth Total Limit: 500000`

xConfiguration Zones LocalZone DefaultSubZone Bandwidth Total Mode: <Limited/Unlimited/NoBandwidth>

デフォルト サブゾーンにエンドポイントが常に使用する総帯域幅の制限を設けるかどうかを決定します。

NoBandwidth：使用可能な帯域幅はありません。デフォルト サブゾーン内ではコールを送受信できません。

デフォルトは Unlimited です。

例：`xConfiguration Zones LocalZone DefaultSubZone Bandwidth Total Mode: Limited`

xConfiguration Zones LocalZone DefaultSubZone Registrations: <Allow/Deny>

デフォルト サブゾーンに割り当てられている登録を受け入れるかどうかを制御します。デフォルトは Allow です。

例：`xConfiguration Zones LocalZone DefaultSubZone Registrations: Allow`

xConfiguration Zones LocalZone DefaultSubZone SIP Media Encryption Mode: <Off/On/BestEffort/Auto>

このサブゾーンで送受信される SIP コール（インターワーキング コールを含む）に Expressway によって適用されるメディア暗号化ポリシー。デフォルト： [Auto]

On：すべてのメディアを暗号化する必要があります。

Off：すべてのメディアの暗号化を解除する必要があります。

BestEffort：使用可能な場合は暗号化を使用します。使用できない場合は暗号化されていないメディアにフォールバックします。

Auto：メディア暗号化ポリシーは適用されません。

例：`xConfiguration Zones LocalZone DefaultSubZone SIP Media Encryption Mode: Auto`

xConfiguration Zones LocalZone DefaultSubZone SIP Media ICE Support: <On/Off>

このゾーン内のデバイスで ICE をサポートするかどうかを制御します。デフォルトは Off です。

On：このゾーンでは ICE をサポートします。

Off：このゾーンでは ICE をサポートしません。

例：`xConfiguration Zones LocalZone DefaultSubZone SIP Media ICE Support: On`

xConfiguration Zones LocalZone DefaultSubZone SIP Multistream Mode: <Off/On>

Expressway がこのゾーンのデバイス間のマルチストリームを許可するかどうかを制御します。デフォルトは On です。

On：マルチストリームを許可します。

Off：マルチストリームを拒否します。

例：`xConfiguration Zones LocalZone DefaultSubZone SIP Multistream Mode: Off`

xConfiguration Zones LocalZone DefaultSubZone SIP SipUpdateRefresh Support: <On/Off>

このゾーンで SIP UPDATE メッセージによるセッション更新をサポートするかどうかを指定します。

On：*SIP* セッションを更新するために、このゾーンから *SIP UPDATE* メッセージを送信します。

Off：このゾーンでは *SIP* セッション更新用の *SIP UPDATE* メッセージを送信しません。

デフォルトは Off です。

例：`xConfiguration Zones LocalZone DefaultSubZone SIP SipUpdateRefresh Support: On`

xConfiguration Zones LocalZone SIP Record Route Address Type: <IP/Hostname>

Expressway がその IP アドレスを使用するか、このゾーンへの発信 SIP 要求の Record-Route または Path ヘッダーのホスト名を使用するかを制御します。注：ホスト名にこの値を設定すると、有効な DNS システム ホスト名も Expressway で設定する必要があります。デフォルトは IP です。

例：`xConfiguration Zones LocalZone SIP Record Route Address Type: IP`

xConfiguration Zones LocalZone SubZones MembershipRules Rule [1..3000] Description: <S: 0,64>

自由形式のメンバーシップ ルールの説明。

例：`xConfiguration Zones LocalZone SubZones MembershipRules Rule 1 Description: 「Office-based staff」`

xConfiguration Zones LocalZone SubZones MembershipRules Rule [1..3000] Name: <S: 0,50>

このメンバーシップ ルールに名前を割り当てます。

例：`xConfiguration Zones LocalZone SubZones MembershipRules Rule 1 Name: 「Office Workers」`

xConfiguration Zones LocalZone SubZones MembershipRules Rule [1..3000] Pattern String: <S: 0,60>

エイリアスを比較するパターンを指定します。

例：`xConfiguration Zones LocalZone SubZones MembershipRules Rule 1 Pattern String: 「@example.com」`

nfiguration Zones LocalZone SubZones MembershipRules Rule [1..3000] Pattern Type: <Exact/Prefix/Suffix/Regex>

パターンとエイリアスを照合する方法。

例：`xConfiguration Zones LocalZone SubZones MembershipRules Rule 1 Pattern Type: Suffix`

xConfiguration Zones LocalZone SubZones MembershipRules Rule [1..3000] Priority: <1..65534>

エンドポイントのアドレスが複数のルールを満たす場合に、ルールを適用する順序（および、そのために、エンドポイントを割り当てるサブゾーン）を決定します。最もプライオリティの高いルール（1、次が 2、その次が 3 など）が最初に適用されます。複数のサブネット ルールが同じプライオリティの場合、最も大きなプレフィックス長を持つルールが最初に適用されます。エイリアス パターン マッチ ルールで同じプライオリティのものは、設定順に検索されます。デフォルトは 100 です。

例：`xConfiguration Zones LocalZone SubZones MembershipRules Rule 1 Priority: 100`

xConfiguration Zones LocalZone SubZones MembershipRules Rule [1..3000] State: <Enabled/Disabled>

メンバーシップ ルールが有効になっているか、無効になっているかを示します。無効になっているメンバーシップ ルールは無視されます。デフォルトは Enabled です。

例：`xConfiguration Zones LocalZone SubZones MembershipRules Rule 1 State: Enabled`

xConfiguration Zones LocalZone SubZones MembershipRules Rule [1..3000] SubZoneName: <S: 0,50>

アドレスがこのルールを満たす場合にエンドポイントを割り当てるサブゾーン。

例：`xConfiguration Zones LocalZone SubZones MembershipRules Rule 1 SubZoneName: 「Branch Office」`

xConfiguration Zones LocalZone SubZones MembershipRules Rule [1..3000] Subnet Address: <S: 0,39>

このサブネットを識別するために（プレフィクス長とともに）使用する IP アドレス指定します。

例：`xConfiguration Zones LocalZone SubZones MembershipRules Rule 1 Subnet Address: 「192.168.0.0」`

xConfiguration Zones LocalZone SubZones MembershipRules Rule [1..3000] Subnet PrefixLength: <1..128>

このサブネットに所属するために IP アドレスと一致する必要があるサブネット アドレスのビット数。デフォルトは 32 です。

例：`xConfiguration Zones LocalZone SubZones MembershipRules Rule 1 Subnet PrefixLength: 32`

xConfiguration Zones LocalZone SubZones MembershipRules Rule [1..3000] Type: <Subnet/AliasPatternMatch>

このルールに適用するアドレスのタイプ。

*[*サブネット（*Subnet*）*]*：IP アドレスが設定した IP アドレス サブネットに含まれる場合は、デバイスを割り当てます。

AliasPatternMatch：エイリアスが設定したパターンと一致する場合は、デバイスを割り当てます。

例：`xConfiguration Zones LocalZone SubZones MembershipRules Rule 1 Type: Subnet`

xConfiguration Zones LocalZone SubZones SubZone [1..1000] Authentication Mode: <DoNotCheckCredentials/TreatAsAuthenticated/CheckCredentials>

Expressway がこのサブゾーンからの着信メッセージをどのように認証するかを制御し、それらのメッセージを認証または未認証として処理するか、あるいは拒否するかを制御します。H.323 メッセージ、ローカル ドメインから発信される SIP メッセージか非ローカル ドメインから発信される SIP メッセージかによって動作が異なります。詳細については、『Administrator Guide』を参照してください。デフォルトは DoNotCheckCredentials です。

例：`xConfiguration Zones LocalZone SubZones SubZone 1 Authentication Mode: DoNotCheckCredentials`

xConfiguration Zones LocalZone SubZones SubZone [1..1000] Bandwidth PerCall Inter Limit: <1..100000000>

このサブゾーン内のエンドポイントで送受信するいずれかのコールに帯域幅制限（kbps 単位）（モードが Limited に設定されている場合にのみ適用）。デフォルトは 1920 です。

例：`xConfiguration Zones LocalZone SubZones SubZone 1 Bandwidth PerCall Inter Limit: 1920`

xConfiguration Zones LocalZone SubZones SubZone [1..1000] Bandwidth PerCall Inter Mode: <Limited/Unlimited/NoBandwidth>

サブ ゾーン内のエンドポイントで送受信するいずれかのコールの帯域幅に制限を設けるかどうかを決定します。デフォルトは Unlimited です。

NoBandwidth：使用可能な帯域幅はありません。このサブゾーンではコールを送受信できません。

例：`xConfiguration Zones LocalZone SubZones SubZone 1 Bandwidth PerCall Inter Mode: Limited`

xConfiguration Zones LocalZone SubZones SubZone [1..1000] Bandwidth PerCall Intra Limit: <1..100000000>

このサブゾーン内の 2 つのエンドポイントのいずれかのコールに帯域幅制限（モードが Limited に設定されている場合にのみ適用）。デフォルトは 1920 です。

例：`xConfiguration Zones LocalZone SubZones SubZone 1 Bandwidth PerCall Intra Limit: 1920`

xConfiguration Zones LocalZone SubZones SubZone [1..1000] Bandwidth PerCall Intra Mode: <Limited/Unlimited/NoBandwidth>

このサブゾーン内の 2 つのエンドポイントで送受信するいずれかのコールの帯域幅に制限を設けるかどうかを決定します。デフォルトは Unlimited です。

NoBandwidth：使用可能な帯域幅はありません。このサブゾーンではコールを発信できません。

例：`xConfiguration Zones LocalZone SubZones SubZone 1 Bandwidth PerCall Intra Mode: Limited`

xConfiguration Zones LocalZone SubZones SubZone [1..1000] Bandwidth Total Limit: <1..100000000>

このサブゾーンの総帯域幅制限を設定します（モードが Limited に設定されている場合にのみ適用）。デフォルトは 500000 です。

例：`xConfiguration Zones LocalZone SubZones SubZone 1 Bandwidth Total Limit: 500000`

xConfiguration Zones LocalZone SubZones SubZone [1..1000] Bandwidth Total Mode: <Limited/Unlimited/NoBandwidth>

このサブゾーンにエンドポイントが常に使用するコールの総帯域幅の制限を設けるかどうかを制御します。デフォルトは Unlimited です。

NoBandwidth：使用可能な帯域幅はありません。このサブゾーンから、またはこのサブゾーン内でコールを発信できません。

例：`xConfiguration Zones LocalZone SubZones SubZone 1 Bandwidth Total Mode: Limited`

xConfiguration Zones LocalZone SubZones SubZone [1..1000] Name: <S: 0, 50>

このサブゾーンに名前を割り当てます。

例：`xConfiguration Zones LocalZone SubZones SubZone 1 Name: 「BranchOffice」`

xConfiguration Zones LocalZone SubZones SubZone [1..1000] Registrations: <Allow/Deny>

このサブゾーンに割り当てられている登録を受け入れるかどうかを制御します。デフォルトは Allow です。

例：`xConfiguration Zones LocalZone SubZones SubZone 1 Registrations: Allow`

xConfiguration Zones LocalZone SubZones SubZone [1..1000] SIP Media Encryption Mode: <Off/On/BestEffort/Auto>

このサブゾーンで送受信される SIP コール（インターワーキング コールを含む）に Expressway によって適用されるメディア暗号化ポリシー。デフォルト： [Auto]

On：すべてのメディアを暗号化する必要があります。

Off：すべてのメディアの暗号化を解除する必要があります。

BestEffort：使用可能な場合は暗号化を使用します。使用できない場合は暗号化されていないメディアにフォールバックします。

Auto：メディア暗号化ポリシーは適用されません。

例：`xConfiguration Zones LocalZone SubZones SubZone 1 SIP Media Encryption Mode: Auto`

xConfiguration Zones LocalZone SubZones SubZone [1..1000] SIP Media ICE Support: <On/Off>

このゾーン内のデバイスで ICE をサポートするかどうかを制御します。デフォルトは Off です。

On：このゾーンでは ICE をサポートします。

Off：このゾーンでは ICE をサポートしません。

例：`xConfiguration Zones LocalZone SubZones Subzone 1 SIP Media ICE Support: On`

xConfiguration Zones LocalZone SubZones SubZone [1..1000] SIP Multistream Mode: <Off/On>

Expressway がこのゾーンのデバイス間のマルチストリームを許可するかどうかを制御します。デフォルトは On です。

On：マルチストリームを許可します。

Off：マルチストリームを拒否します。

例：`xConfiguration Zones LocalZone SubZones Subzone 1 SIP Multistream Mode: Off`

xConfiguration Zones LocalZone Traversal H323 Assent Mode: <On/Off>

ファイアウォール トラバーサルに Assent モードを使用する H.323 コールを許可するかどうかを決定します。Expressway に直接登録されているトラバーサル対応エンドポイントに適用します。デフォルトは On です。

例：`xConfiguration Zones LocalZone Traversal H323 Assent Mode: On`

xConfiguration Zones LocalZone Traversal H323 H46018 Mode: <On/Off>

ファイアウォール トラバーサルに H460.18 モードを使用する H.323 コールを許可するかどうかを決定します。Expressway に直接登録されているトラバーサル対応エンドポイントに適用します。デフォルトは On です。

例：`xConfiguration Zones LocalZone Traversal H323 H46018 Mode: On`

xConfiguration Zones LocalZone Traversal H323 H46019 Demultiplexing Mode: <On/Off>

Expresswayに直接登録されているトラバーサル対応のエンドポイントからのコールにExpresswayが逆多重化モードで動作するかどうかを制御します。デフォルトはOffです。

On：すべてのコールに同じ2つのポートを使用できるようにします。

Off：各コールが個別のポートペアをメディアに使用します。

例：`xConfiguration Zones LocalZone Traversal H323 H46019 Demultiplexing Mode: Off`

xConfiguration Zones LocalZone Traversal H323 Preference: <Assent/H46018>

Expressway に直接登録されているエンドポイントが Assent プロトコルと H460.18 プロトコルの両方をサポートしている場合は、この設定で使用する Expressway を決定します。デフォルトは Assent です。

例：`xConfiguration Zones LocalZone Traversal H323 Preference: Assent`

xConfiguration Zones LocalZone Traversal H323 TCPProbe KeepAliveInterval: <1..65534>

ファイアウォールの NAT バインドを有効に保つため、コールが確立した後に Expressway に直接登録されているトラバーサル対応エンドポイントが TCP プローブを送信する間隔（秒単位）を設定します。デフォルトは 20 です。

例：`xConfiguration Zones LocalZone Traversal H323 TCPProbe KeepAliveInterval: 20`

xConfiguration Zones LocalZone Traversal H323 TCPProbe RetryCount: <1..65534>

Expresswayに直接登録されているトラバーサル対応エンドポイントがTCPプローブの送信を試行する回数を設定します。デフォルトは5です。

例：`xConfiguration Zones LocalZone Traversal H323 TCPProbe RetryCount: 5`

xConfiguration Zones LocalZone Traversal H323 TCPProbe RetryInterval: <1..65534>

Expresswayに直接登録されているトラバーサル対応エンドポイントがTCPプローブを送信する頻度（秒単位）を設定します。デフォルトは2です。

例：`xConfiguration Zones LocalZone Traversal H323 TCPProbe RetryInterval: 2`

xConfiguration Zones LocalZone Traversal H323 UDPProbe KeepAliveInterval: <1..65534>

ファイアウォールの NAT バインドを有効に保つため、コールが確立した後に Expressway に直接登録されているトラバーサル対応エンドポイントがUDPプローブを送信する間隔（秒単位）を設定します。デフォルトは 20 です。

例：`xConfiguration Zones LocalZone Traversal H323 UDPProbe KeepAliveInterval: 20`

xConfiguration Zones LocalZone Traversal H323 UDPProbe RetryCount: <1..65534>

Expresswayに直接登録されているトラバーサル対応エンドポイントがUDPプローブの送信を試行する回数を設定します。デフォルトは5です。

例：`xConfiguration Zones LocalZone Traversal H323 UDPProbe RetryCount: 5`

xConfiguration Zones LocalZone Traversal H323 UDPProbe RetryInterval: <1..65534>

Expressway に直接登録されているトラバーサル対応エンドポイントが UDP プローブを送信する頻度（秒単位）を設定します。デフォルトは 2 です。

例：`xConfiguration Zones LocalZone Traversal H323 UDPProbe RetryInterval: 2`

xConfiguration Zones LocalZone TraversalSubZone Bandwidth PerCall Limit: <1..100000000>

Expressway が処理するトラバーサル コールのいずれかに適用する帯域幅制限（kbps 単位）（モードが Limited に設定されている場合のみ）。デフォルトは 1920 です。

例：`xConfiguration Zones LocalZone TraversalSubZone Bandwidth PerCall Limit: 1920`

xConfiguration Zones LocalZone TraversalSubZone Bandwidth PerCall Mode: <Limited/Unlimited/NoBandwidth>

Expressway が処理するいずれかのトラバーサル コールの帯域幅に制限を設けるかどうかを決定します。デフォルトは Unlimited です。

NoBandwidth：使用可能な帯域幅はありません。トラバーサル コールは発信できません。

例：`xConfiguration Zones LocalZone TraversalSubZone Bandwidth PerCall Mode: Limited`

xConfiguration Zones LocalZone TraversalSubZone Bandwidth Total Limit: <1..100000000>

Expressway が処理するすべてのトラバーサル コールに許可する総帯域幅制限（kbps 単位）（モードが Limited に設定されている場合のみ）。デフォルトは 500000 です。

例：`xConfiguration Zones LocalZone TraversalSubZone Bandwidth Total Limit: 500000`

xConfiguration Zones LocalZone TraversalSubZone Bandwidth Total Mode: <Limited/Unlimited/NoBandwidth>

Expressway が処理するすべてのトラバーサル コールの総帯域幅に制限を設けるかどうかを決定します。デフォルトは Unlimited です。

NoBandwidth：使用可能な帯域幅はありません。トラバーサル コールは発信できません。

例：`xConfiguration Zones LocalZone TraversalSubZone Bandwidth Total Mode: Limited`

xConfiguration Zones Policy Mode: <SearchRules/Directory>

宛先の検索を試行するときに使用するモード。デフォルトは SearchRules です。

SearchRules：クエリするゾーンとその順序を決定する設定済みの検索ルールを使用します。

Directory：要求を正しいゾーンに送信するためにディレクトリ サービスの機能を使用します。

例：`xConfiguration Zones Policy Mode: SearchRules`

xConfiguration Zones Policy SearchRules Rule [1..2000] Authentication: <Yes/No>

この検索ルールを認証された検索要求にのみ適用するかどうかを指定します。デフォルトは No です。

例：`xConfiguration Zones Policy SearchRules Rule 1 Authentication: No`

ration Zones Policy SearchRules Rule [1..2000] Description: <S: 0,64>

自由形式の検索ルールの説明。

例：`xConfiguration Zones Policy SearchRules Rule 1 Description: 「Send query to the DNS zone」`

xConfiguration Zones Policy SearchRules Rule [1..2000] Mode: <AliasPatternMatch/AnyAlias/AnyIPAddress>

クエリをターゲットゾーンに送信するかどうかを決定します。デフォルトはAnyAliasです。

AliasPatternMatch：エイリアスが対応するパターン タイプと文字列とが一致する場合にのみ照会します。

AnyAlias：いずれかのエイリアス（IP アドレスではない）のゾーンを照会します。

AnyIPAddress：指定した IP アドレス（エイリアスではない）のゾーンを照会します。

例：`xConfiguration Zones Policy SearchRules Rule 1 Mode: AnyAlias`

xConfiguration Zones Policy SearchRules Rule [1..2000] Name: <S: 0,50>

検索ルールの記述名。

例：`xConfiguration Zones Policy SearchRules Rule 1 Name: 「DNS lookup」`

xConfiguration Zones Policy SearchRules Rule [1..2000] Pattern Behavior: <Strip/Leave/Replace>

ターゲットゾーンに送信する前に、エイリアスの一致した部分を変更するかどうかを決定します（エイリアス パターン マッチ モードにのみ適用します）。デフォルトは Strip です。

[変更しない（Leave）]：エイリアスは変更されません。

[除去（Strip）]：一致するプレフィックスまたはサフィックスをエイリアスから削除します。

[置換（Replace）]：エイリアスの一致部分が [置換文字列（Replace string）] のテキストで置き換えられます。

例：`xConfiguration Zones Policy SearchRules Rule 1 Pattern Behavior: Strip`

xConfiguration Zones Policy SearchRules Rule [1..2000] Pattern Replace: <S: 0,60>

パターンに一致するエイリアスの部分を置き換える文字列（置換パターン動作にのみ適用します）。

例：`xConfiguration Zones Policy SearchRules Rule 1 Pattern Replace: 「@example.net」`

xConfiguration Zones Policy SearchRules Rule [1..2000] Pattern String: <S: 0,60>

エイリアスと比較するパターン（エイリアス パターン マッチ モードにのみ適用します）。

例：`xConfiguration Zones Policy SearchRules Rule 1 Pattern String: 「@example.com」`

xConfiguration Zones Policy SearchRules Rule [1..2000] Pattern Type: <Exact/Prefix/Suffix/Regex>

適用するルールで、パターン文字列をどのようにエイリアスと照合するか（エイリアス パターン マッチ モードにのみ適用します）。デフォルトは Prefix です。

*[*完全一致（*Exact*）*]*：文字列全体がエイリアスと 1 文字も違うことなく完全に一致する必要があります。

*[*プレフィックス（*Prefix*）*]*：文字列がエイリアスの先頭に表示される必要があります。

Suffix：文字列がエイリアスの末尾に表示される必要があります。

Regex：文字列は正規表現として処理されます。

例：`xConfiguration Zones Policy SearchRules Rule 1 Pattern Type: Suffix`

xConfiguration Zones Policy SearchRules Rule [1..2000] Priority: <1..65534>

他の検索ルールのプライオリティと比較したときに、このルールを適用する検索プロセスの順序。プライオリティ 1 のすべてのルールが最初に適用され、次にプライオリティ 2 のすべてのルールが適用されます。デフォルトは 100 です。

例：`xConfiguration Zones Policy SearchRules Rule 1 Priority: 100`

xConfiguration Zones Policy SearchRules Rule [1..2000] Progress: <Continue/Stop>

エイリアスがこの検索ルールと一致する場合の進行中の検索動作を指定します。「Stop」を選択した場合、このルールと同じプライオリティのルールは適用されます。デフォルトは Continue です。

*[*続行（*Continue*）*]*：エイリアスが特定したエンドポイントが検出されるまで、残りの検索ルールを（プライオリティ順に）適用します。

*[*停止（*Stop*）*]*：エイリアスで特定されたエンドポイントがターゲット ゾーンで検出されない場合でも、これ以上は検索ルールを適用しません。

例：`xConfiguration Zones Policy SearchRules Rule 1 Progress: Continue`

xConfiguration Zones Policy SearchRules Rule [1..2000] Protocol: <Any/H323/SIP>

照会するルールに必要な送信元のプロトコル。

例：`xConfiguration Zones Policy SearchRules Rule 1 Protocol: Any`

xConfiguration Zones Policy SearchRules Rule [1..2000] Source Mode: <Any/AllZones/LocalZone/Named>

このルールを適用する要求のソース。デフォルトは Any です。

*[*いずれか（*Any*）*]*：ローカル登録されたデバイス、ネイバーまたはトラバーサルゾーン、および登録されていないデバイス。

[All Zones]：ローカルに登録されたデバイスとネイバーまたはトラバーサルゾーン。

*[*ローカル ゾーン（*Local Zone*）*]*：ローカル登録されたデバイスのみ。

Named：特定のゾーンまたはサブゾーン。

例：`xConfiguration Zones Policy SearchRules Rule 1 Source Mode: Any`

xConfiguration Zones Policy SearchRules Rule [1..2000] Source Name: <S: 0..50>

このルールを適用する送信元（サブ）ゾーンの名前。

例：`xConfiguration Zones Policy SearchRules Rule 1 Source Name: 「Local Office」`

xConfiguration Zones Policy SearchRules Rule [1..2000] State: <Enabled/Disabled>

検索ルールが有効になっているか、無効になっているかを示します。無効になっている検索ルールは無視されます。デフォルトは Enabled です。

例：`xConfiguration Zones Policy SearchRules Rule 1 State: Enabled`

xConfiguration Zones Policy SearchRules Rule [1..2000] Target Name: <S: 0,50>

エイリアスが検索ルールと一致するかどうかを照会するゾーンまたはポリシー サービス。

例：`xConfiguration Zones Policy SearchRules Rule 1 Target Name: 「Sales Office」`

xConfiguration Zones Policy SearchRules Rule [1..2000] Target Type: <Zone/PolicyService>

この検索ルールを適用するターゲットのタイプ。

例：`xConfiguration Zones Policy SearchRules Rule 1 Target Type: Zone`

xConfiguration Zones Zone [1..1000] DNS IncludeAddressRecord: <On/Off>

NAPTR（SIP）レコードまたは SRV（SIP と H.323）レコードがこのゾーンを介してダイヤルされたエイリアスで検出されなかった場合は、Expressway が A および AAAA DNS レコードを照会するかどうかを決定します。デフォルトは Off です。

例：`xConfiguration Zones Zone 1 DNS IncludeAddressRecord: Off`

xConfiguration Zones Zone [1..1000] DNS Interworking SIP Audio DefaultCodec: <G711u/G711a/G722_48/G722_56/G722_64/G722_1_16/G722_1_24/G722_1_32/G722_1_48/G723_1/G728/G729/AACLD_48/AACLD_56/AACLD_64/AMR>

空の INVITE を許可しない場合に使用する音声コーデックを指定します。デフォルトは G711u です。

例：`xConfiguration Zones Zone 1 DNS Interworking SIP Audio DefaultCodec: G711u`

xConfiguration Zones Zone [1..1000] DNS Interworking SIP EmptyInviteAllowed: <On/Off>

Expressway がこのゾーンに送信する SIP INVITE メッセージを SDP を使用せずに生成するかどうかを制御します。SDP を使用していない INVITE は、宛先デバイスがコーデックの選択を開始するよう求められることを意味し、コールが H.323 からローカルにインターワーキングされていた場合に使用されます。デフォルトは On です。

On：SDP を使用していない SIP INVITE が生成され、このネイバーに送信されます。

Off：SIP INVITE が生成され、事前設定された SDP が挿入されてから INVITE が送信されます。

例：`xConfiguration Zones Zone 1 DNS Interworking SIP EmptyInviteAllowed: On`

xConfiguration Zones Zone [1..1000] DNS Interworking SIP Video DefaultBitrate: <64..65535>

空の INVITE を許可しない場合に使用するビデオ ビット レートを指定します。デフォルトは 384 です。

例：`xConfiguration Zones Zone 1 DNS Interworking SIP Video DefaultBitrate: 384`

xConfiguration Zones Zone [1..1000] DNS Interworking SIP Video DefaultCodec: <None/H261/H263/H263p/H263pp/H264>

空の INVITE を許可しない場合に使用するビデオ コーデックを指定します。デフォルトは H263 です。

例：`xConfiguration Zones Zone 1 DNS Interworking SIP Video DefaultCodec: H263`

xConfiguration Zones Zone [1..1000] DNS Interworking SIP Video DefaultResolution: <None/QCIF/CIF/4CIF/SIF/4SIF/VGA/SVGA/XGA>

空の INVITE を許可しない場合に使用すビデオ解像度を指定します。デフォルトは CIF です。

例：`xConfiguration Zones Zone 1 DNS Interworking SIP Video DefaultResolution: CIF`

xConfiguration Zones Zone [1..1000] DNS SIP Default Transport: <UDP/TCP/TLS>

DNS NAPTR レコードと SIP URI パラメータによって必要なトランスポート情報が得られないときに DNS ゾーンからの SIP コールに使用するトランスポート タイプを決定します。RFC 3263 では、UDP を使用する必要があると提案しています。デフォルトは UDP です。

例：`xConfiguration Zones Zone [1..1000] DNS SIP Default Transport: UDP`

xConfiguration Zones Zone [1..1000] DNS SIP Media AesGcm Support: <Off/On>

このゾーンを通過するメディアの AES GCM アルゴリズムによる暗号化/復号化を有効にします。デフォルトは Off です。

例：`xConfiguration Zones Zone 1 DNS SIP Media AesGcm Support: On`

xConfiguration Zones Zone [1..1000] DNS SIP SipUpdateRefresh Support: <Off/On>

このゾーンで SIP UPDATE メッセージによるセッション更新をサポートするかどうかを指定します。

On：*SIP* セッションを更新するために、このゾーンから *SIP UPDATE* メッセージを送信します。

Off：このゾーンでは *SIP* セッション更新用の *SIP UPDATE* メッセージを送信しません。

デフォルトは Off です。

例：`xConfiguration Zones Zone 1 DNS SIP SipUpdateRefresh Support: On`

xConfiguration Zones Zone [1..1000] DNS SIP Media Encryption Mode: <Off/On/BestEffort/Auto>

このゾーンで送受信される SIP コール（インターワーキング コールを含む）に Expressway によって適用されるメディア暗号化ポリシー。デフォルトは Auto です。

On：すべてのメディアを暗号化する必要があります。

Off：すべてのメディアの暗号化を解除する必要があります。

BestEffort：使用可能な場合は暗号化を使用します。使用できない場合は暗号化されていないメディアにフォールバックします。

Auto：メディア暗号化ポリシーは適用されません。

例：`xConfiguration Zones Zone 1 DNS SIP Media Encryption Mode: Auto`

xConfiguration Zones Zone [1..1000] DNS SIP Media ICE Support: <On/Off>

このゾーン内のデバイスで ICE をサポートするかどうかを制御します。デフォルトは Off です。

On：このゾーンでは ICE をサポートします。

Off：このゾーンでは ICE をサポートしません。

例：`xConfiguration Zones Zone 1 DNS SIP Media ICE Support: Off`

xConfiguration Zones Zone [1..1000] DNS SIP Media ICEPassThrough Support: <On/Off>

このゾーン内のデバイスで ICE パススルーをサポートするかどうかを制御します。デフォルト：Off

On：このゾーンでは ICE パススルーをサポートします。

Off：このゾーンでは ICE パススルーをサポートしません。

例：`xConfiguration Zones Zone 1 DNS SIP Media ICEPassThrough Support: On`

xConfiguration Zones Zone [1..1000] DNS SIP Poison Mode: <On/Off>

ローカル Expressway が再度受信した場合は拒否するように、このゾーンに送信された SIP 要求を「ポイゾニング」するかどうかを決定します。デフォルトは Off です。

[オン（On）]：このゾーンを介して送信され、このExpressway が再度受信する SIP 要求は拒否されます。

Off：このゾーンを介して送信され、この Expressway が再度受信する SIP 要求は通常どおりに処理されます。

例：`xConfiguration Zones Zone 1 DNS SIP Poison Mode: Off`

xConfiguration Zones Zone [1..1000] DNS SIP PreloadedSipRoutes Accept: <Off/On>

[プリロードされた SIP ルートのサポート（Preloaded SIP routes support）] を [オン（On）] に切り替えて、Route ヘッダーを含んだ SIP INVITE 要求をこのゾーンで処理できるようにします。このヘッダーを含んでいる SIP INVITE 要求をゾーンで拒否するには、[プリロードされた SIP ルートのサポート（Preloaded SIP routes support）] を [オフ（Off）] に切り替えます。

例：`xConfiguration Zones Zone 3 Neighbor SIP PreloadedSipRoutes Accept: On`

xConfiguration Zones Zone [1..1000] DNS SIP Record Route Address Type: <IP/Hostname>

Expressway がその IP アドレスを使用するか、このゾーンへの発信 SIP 要求の Record-Route または Path ヘッダーのホスト名を使用するかを制御します。注：ホスト名にこの値を設定すると、有効な DNS システム ホスト名も Expressway で設定する必要があります。デフォルトは IP です。

例：`xConfiguration Zones Zone 1 DNS SIP Record Route Address Type: IP`

xConfiguration Zones Zone [1..1000] DNS SIP SearchAutoResponse: <On/Off>

H.323 検索としてこのゾーン宛に発信された SIP 検索を Expressway が受信したときの動作を制御します。デフォルトは Off です。

Off：SIP OPTION メッセージはこのゾーンに送信されます。

On：検索に自動的に応答します。検索が転送されることはありません。

例：`xConfiguration Zones Zone 1 DNS SIP SearchAutoResponse: Off`

xConfiguration Zones Zone [1..1000] DNS SIP TLS Verify Mode: <On/Off>

DNS ルックアップにより返されたこの Expressway と宛先システム サーバ間の X.509 証明書チェックを制御します。有効になっている場合は、DNS ルックアップに送信されたドメイン名（サブジェクト共通名の属性かサブジェクト代替名の属性）がサーバの X.509 証明書に含まれている必要があります。

デフォルトは Off です。

例：`xConfiguration Zones Zone 1 DNS SIP TLS Verify Mode: On`

xConfiguration Zones Zone [1..1000] DNS SIP TLS Verify Subject Name: <S: 0..128>

トラバーサル クライアントの X.509 証明書で検索する証明書の所有者の名前（サブジェクト共通名の属性またはサブジェクト代替名の属性のいずれかに含まれている必要があります）。空の場合は、解決された URI のドメインの部分が使用されます。

例：`xConfiguration Zones Zone 1 DNS SIP TLS Verify Subject Name: 「example.com」`

xConfiguration Zones Zone [1..1000] DNS SIP UDP BFCP Filter Mode: <On/Off>

このゾーンに送信された INVITE 要求から UDP/BFCP をフィルタリングにより除去するかどうかを決定します。UDP/BFCP プロトコルをサポートしない SIP デバイスとの相互運用性を有効にするためにこのオプションが必要な場合があります。デフォルトは Off です。

[オン（On）]：UDP/BFCP プロトコルを参照しているメディア回線が TCP/BFCP で置き換えられ、無効になります。

[オフ（Off）]：INVITE 要求は変更されません。

例：`xConfiguration Zones Zone 1 DNS SIP UDP BFCP Filter Mode: Off`

xConfiguration Zones Zone [1..1000] DNS ZoneProfile: <Default/Custom/CiscoUnifiedCommunicationsManager/CiscoUnifiedCommunicationsManagerBFCP/NortelCS1000/NonRegisteringDeviceLocalB2BUAService>

ゾーンの詳細な設定方法を決定します。

Default：工場出荷時の初期設定を使用します。

[カスタム（Custom）]：各設定を個別に行うことができます。

Preconfigured profiles：事前設定されたプロファイルのいずれかを選択して、そのタイプのシステムへの接続に必要な適切な設定を自動的に使用します。

例：`xConfiguration Zones Zone 1 DNS ZoneProfile: Default`

xConfiguration Zones Zone [1..1000] ENUM DNSSuffix: <S: 0, 128>

変換された E.164 番号に追加する DNS ゾーン。これにより、このゾーンで照会する ENUM ホスト名が作成されます。

例：`xConfiguration Zones Zone 2 ENUM DNSSuffix: 「e164.arpa」`

xConfiguration Zones Zone [1..1000] H323 Mode: <On/Off>

このゾーンでの H.323 コールの送受信を許可するかどうかを決定します。デフォルトは On です。

例：`xConfiguration Zones Zone 2 H323 Mode: On`

xConfiguration Zones Zone [1..1000] HopCount: <1..255>

エイリアス検索要求をこのゾーンに送信するときに使用するホップ カウントを指定します。注：別のゾーンから受信した検索要求にすでにホップ カウントが割り当てられている場合は、2 つの値のうちの小さいほうが使用されます。デフォルトは 15 です。

例：`xConfiguration Zones Zone 2 HopCount: 15`

xConfiguration Zones Zone [1..1000] Name: <S: 1, 50>

このゾーンに名前を割り当てます。

例：`xConfiguration Zones Zone 3 Name: 「UK Sales Office」`

xConfiguration Zones Zone [1..1000] Neighbor Authentication Mode: <DoNotCheckCredentials/TreatAsAuthenticated/CheckCredentials>

Expressway がこのゾーンからの着信メッセージをどのように認証するかを制御し、それらのメッセージを認証または未認証として処理するか、あるいは拒否するかを制御します。H.323 メッセージ、ローカル ドメインから発信される SIP メッセージか非ローカル ドメインから発信される SIP メッセージかによって動作が異なります。デフォルトは DoNotCheckCredentials です。

例：`xConfiguration Zones Zone 3 Neighbor Authentication Mode: DoNotCheckCredentials`

xConfiguration Zones Zone [1..1000] Neighbor H323 CallSignaling Port: <1024..65534>

この Expressway で送受信する H.323 コールに使用するネイバーのポート。デフォルトは 1720 です。

例：`xConfiguration Zones Zone 3 Neighbor H323 CallSignaling Port: 1720`

xConfiguration Zones Zone [1..1000] Neighbor H323 Port: <1024..65534>

この Expressway で送受信する H.323 検索に使用するネイバーのポート。デフォルトは 1719 です。

例：`xConfiguration Zones Zone 3 Neighbor H323 Port: 1719`

xConfiguration Zones Zone [1..1000] Neighbor H323 SearchAutoResponse: <On/Off>

Expressway がこのゾーン宛の H323 検索を受信したときの動作を決定します。デフォルトは Off です。

Off：LRQ メッセージがゾーンに送信されます。

On：検索に自動的に応答します。検索が転送されることはありません。

例：`xConfiguration Zones Zone 3 Neighbor H323 SearchAutoResponse: Off`

xConfiguration Zones Zone [1..1000] Neighbor Interworking SIP Audio DefaultCodec: <G711uG711aG722_48G722_56G722_64G722_1_16G722_1_24G722_1_32G722_1_48G723_1G728G729AACLD_48AACLD_56AACLD_64AMR>

空の INVITE を許可しない場合に使用する音声コーデックを指定します。デフォルトは G711u です。

例：`xConfiguration Zones Zone 3 Neighbor Interworking SIP Audio DefaultCodec: G711u`

xConfiguration Zones Zone [1..1000] Neighbor Interworking SIP EmptyInviteAllowed: <On/Off>

Expressway がこのゾーンに送信する SIP INVITE メッセージを SDP を使用せずに生成するかどうかを決定します。SDP を使用していない INVITE は、宛先デバイスがコーデックの選択を開始するよう求められることを意味し、コールが H.323 からローカルにインターワーキングされていた場合に使用されます。デフォルトは On です。

On：SDP を使用していない SIP INVITE が生成され、このネイバーに送信されます。

Off：SIP INVITE が生成され、事前設定された SDP が挿入されてから INVITE が送信されます。

例：`xConfiguration Zones Zone 3 Neighbor Interworking SIP EmptyInviteAllowed: On`

xConfiguration Zones Zone [1..1000] Neighbor Interworking SIP Encryption EncryptSRTCP: <Yes/No>

Expressway はこのゾーンへのコールで暗号化された SRTCP を提供するかどうかを制御します。Expressway は INFO 要求を送信します。デフォルトは No です。

例：`xConfiguration Zones Zone 3 Neighbor Interworking SIP Encryption EncryptSRTCP: No`

xConfiguration Zones Zone [1..1000] Neighbor Interworking SIP Search Strategy: <Options/Info>

H.323 コールとインターワーキングするときに Expressway が SIP エンドポイントをどのように検索するかを決定します。デフォルトは Options です。

Options：Expressway は OPTIONS 要求を送信します。

Info：Expressway は INFO 要求を送信します。

例：`xConfiguration Zones Zone 3 Neighbor Interworking SIP Search Strategy: Options`

xConfiguration Zones Zone [1..1000] Neighbor Interworking SIP Video DefaultBitrate: <64..65535>

空の INVITE を許可しない場合に使用するビデオ ビット レートを指定します。デフォルトは 384 です。

例：`xConfiguration Zones Zone 3 Neighbor Interworking SIP Video DefaultBitrate: 384`

xConfiguration Zones Zone [1..1000] Neighbor Interworking SIP Video DefaultCodec: <None/H261/H263/H263p/H263pp/H264>

空の INVITE を許可しない場合に使用するビデオ コーデックを指定します。デフォルトは H263 です。

例：`xConfiguration Zones Zone 3 Neighbor Interworking SIP Video DefaultCodec: H263`

xConfiguration Zones Zone [1..1000] Neighbor Interworking SIP Video DefaultResolution: <None/QCIF/CIF/4CIF/SIF/4SIF/VGA/SVGA/XGA>

空の INVITE を許可しない場合に使用すビデオ解像度を指定します。デフォルトは CIF です。

例：`xConfiguration Zones Zone 3 Neighbor Interworking SIP Video DefaultResolution: CIF`

xConfiguration Zones Zone [1..1000] Neighbor Monitor: <Yes/No>

ゾーンがそのネイバー ピアをモニタするかどうかを指定します。LQR H323、または SIP OPTIONS、あるいはその両方がピアに定期的に送信されます。いずれかのピアが応答に失敗すると、そのピアは非アクティブとマークされます。どのピアも応答を管理していない場合、そのゾーンは非アクティブとマークされます。デフォルトは Yes です。

例：`xConfiguration Zones Zone 3 Neighbor Monitor: Yes`

xConfiguration Zones Zone [1..1000] Neighbor Peer [1..6] Address: <S:0,128>

ネイバーの IP アドレスまたは完全修飾ドメイン名（FQDN）を指定します。ネイバー ゾーンが Expressway クラスタの場合、これはそのクラスタ ピアの 1 つになります。

例：`xConfiguration Zones Zone 3 Neighbor Peer 1 Address: 「192.44.0.18」`

xConfiguration Zones Zone [1..1000] Neighbor Registrations: <Allow/Deny>

このゾーンを通じてルーティングされたプロキシ経由で送信される SIP 登録を受け入れるかどうかを制御します。デフォルトは Allow です。

例：`xConfiguration Zones Zone 3 Neighbor Registrations: Allow`

xConfiguration Zones Zone [1..1000] Neighbor RetainConnectionOnParseErrorMode: <mode>

形式が不正な、または破損した SIP メッセージに対するシステムの許容度を制御します。

Drop All：システムは、形式が不正な、または破損した SIP メッセージを受信した時点で SIP 接続を閉じます。

RetainSome：システムは、形式が不正でも必須ではないヘッダーが設定された SIP メッセージを受信した場合、SIP 接続を維持します。必須のヘッダーの形式が不正な場合は、接続を閉じます。

Retain All: システムは、(必須ヘッダーを含む) 形式が不正なヘッダーを持つ SIP メッセージを受信しても SIP 接続を維持します。

デフォルトは DropAll です。

（注）
- *Content-Length* ヘッダーは例外です。設定されているモードにかかわらず、このヘッダーが存在しないか形式が不正な場合、接続は常に閉じられます。
- Expressway が不正な形式のメッセージを 11 個以上続けて受信した場合も、モードにかかわらず接続が閉じられます。
- CMR Cloud 導入環境では、RetainAll モードを設定することをお勧めします。

例：`xConfiguration Zones Zone 3 RetainConnectionOnParseErrorMode: RetainSome`

xConfiguration Zones Zone [1..1000] Neighbor SIP Authentication Trust Mode: <On/Off>

このゾーンからの認証された SIP メッセージ（P-Asserted-Identity ヘッダーを含んでいるもの）を信頼できるかどうかを制御します。デフォルトは Off です。

On：それ以上のチャレンジを行うことなく、メッセージが信頼されます。

Off：認証のため、メッセージにチャレンジが実行されます。

例：`xConfiguration Zones Zone 3 Neighbor SIP Authentication Trust Mode: On`

xConfiguration Zones Zone [1..1000] Neighbor SIP B2BUA Refer Mode: <Forward/Terminate>

SIP REFER 要求の処理方法を決定します。

*[*転送（*Forward*）*]*：SIP REFER 要求がターゲットに転送されます。

*[*終了（*Terminate*）*]*：SIP REFER 要求は Expressway によって終了されます。

デフォルトは Forward です。

例：`xConfiguration Zones Zone 3 Neighbor SIP B2BUA Refer Mode: Terminate`

xConfiguration Zones Zone [1..1000] Neighbor SIP B2BUA Replaces Mode: <Forward/Terminate>

Meeting Server コール ブリッジ グループからの INVITE メッセージに対して、Expressway でロード バランシングを処理できるようにします。デフォルトは Forward です。

Terminate：Expressway B2BUA が Meeting Server からの INVITE を処理します。この Expressway に登録されているエンドポイント、あるいは隣接する VCS または Expressway に登録されているエンドポイントに対してロード バランシングを有効にする必要があります。

Forward：Expressway は Meeting Server からの INVITE をプロキシします。エンドポイントが Unified CM に登録されている場合、Unified CM で代わりにこれらの INVITE を処理できるため、このオプションを使用できます。

例：`xConfiguration Zones Zone 3 Neighbor SIP B2BUA Replaces Mode: Terminate`

xConfiguration Zones Zone [1..1000] Neighbor SIP B2BUA Service Identifier: <0..64>

ローカル SIP Back-to-Back User Agent サービスのインスタンスを表す識別子。

例：`xConfiguration Zones Zone 3 Neighbor SIP B2BUA Service Identifier: 1`

xConfiguration Zones Zone [1..1000] Neighbor SIP ClassFiveResponseLiveness: <Yes/No>

ネイバー ピアからのクラス 5 の SIP 応答により、ゾーンが使用についてアライブであると見なされるようになるかどうかを指定します。デフォルトは Yes です。

例：`xConfiguration Zones Zone 3 Neighbor SIP ClassFiveResponseLiveness: Yes`

xConfiguration Zones Zone [1..1000] Neighbor SIP Encryption Mode: <Auto/Microsoft/Off>

Expressway によるこのゾーンで暗号化された SIP コールの処理方法を決定します。デフォルトは Auto です。

Auto：セキュア SIP トランスポート（TLS）が使用されている場合、SIP コールが暗号化されます。

[Microsoft]：SIP コールは MS-SRTP を使用して暗号化されます。

[オフ（Off）]：SIP コールは暗号化されません。

例：`xConfiguration Zones Zone 3 Neighbor SIP Encryption Mode: Auto`

xConfiguration Zones Zone [1..1000] Neighbor SIP MIME Strip Mode: <On/Off>

複数の MIME ストリッピングをこのゾーンからの要求上で実行するかどうかを制御します。Microsoft Office Communications Server 2007 に接続する場合は、On に設定する必要があります。デフォルトは Off です。

例：`xConfiguration Zones Zone 3 Neighbor SIP MIME Strip Mode: Off`

xConfiguration Zones Zone [1..1000] Neighbor SIP Media AesGcm Support: <Off/On>

このゾーンを通過するメディアの AES GCM アルゴリズムによる暗号化/復号化を有効にします。デフォルトは Off です。

例：`xConfiguration Zones Zone 1 Neighbor SIP Media AesGcm Support: On`

xConfiguration Zones Zone [1..1000] Neighbor SIP Media Encryption Mode: <Off/On/BestEffort/Auto>

このゾーンで送受信される SIP コール（インターワーキング コールを含む）に Expressway によって適用されるメディア暗号化ポリシー。デフォルト： [Auto]

On：すべてのメディアを暗号化する必要があります。

Off：すべてのメディアの暗号化を解除する必要があります。

BestEffort：使用可能な場合は暗号化を使用します。使用できない場合は暗号化されていないメディアにフォールバックします。

Auto：メディア暗号化ポリシーは適用されません。

例：`xConfiguration Zones Zone 3 Neighbor SIP Media Encryption Mode: Auto`

xConfiguration Zones Zone [1..1000] Neighbor SIP Media ICE Support: <On/Off>

このゾーン内のデバイスで ICE をサポートするかどうかを制御します。デフォルトは Off です。

On：このゾーンでは ICE をサポートします。

Off：このゾーンでは ICE をサポートしません。

例：`xConfiguration Zones Zone 3 Neighbor SIP Media ICE Support: On`

xConfiguration Zones Zone [1..1000] Neighbor SIP Media ICEPassThrough Support: <On/Off>

このゾーン内のデバイスで ICE パススルーをサポートするかどうかを制御します。デフォルト：Off

On：このゾーンでは ICE パススルーをサポートします。

Off：このゾーンでは ICE パススルーをサポートしません。

例：`xConfiguration Zones Zone 3 Neighbor SIP Media ICEPassThrough Support: On`

xConfiguration Zones Zone [1..1000] Neighbor SIP MediaRouting Mode: <Auto/Signaled/Latching>

このネイバーで送受信するコールのメディアの Expressway による処理方法と、このネイバー宛のメディアを転送する場所。デフォルトは Auto です。.

Signaled：このネイバーで送受信されるコールのメディアは常に取得されます。このネイバーから受信した SDP でシグナリングされたとおりに転送されます。

Latching：このネイバーで送受信されるコールのメディアは常に取得されます。メディアは、このネイバーからのメディアを受信する IP アドレスとポートに転送されます。

Auto：コールがトラバーサルコールの場合にのみ、メディアが取得されます。このネイバーが NAT の背後にある場合、Expressway はこのゾーンからのメディアを受信するメディアを IP アドレスとポートに転送されます（ラッチング）。または、SDP でシグナリングされた IP アドレスとポートにメディアが転送されます（シグナリング）。

例：`xConfiguration Zones Zone 3 Neighbor SIP MediaRouting Mode: Auto`

xConfiguration Zones Zone [1..1000] Neighbor SIP Multistream Mode: <Off/On>

Expressway がこのゾーンのデバイス間のマルチストリームを許可するかどうかを制御します。デフォルトは On です。

On：マルチストリームを許可します。

Off：マルチストリームを拒否します。

例：`xConfiguration Zones Zone 1 Neighbor SIP Multistream Mode: Off`

xConfiguration Zones Zone [1..1000] Neighbor SIP Poison Mode: <On/Off>

ローカル Expressway が再度受信した場合は拒否するように、このゾーンに送信された SIP 要求を「ポイゾニング」するかどうかを制御します。デフォルトは Off です。

[オン（On）]：このゾーンを介して送信され、このExpressway が再度受信する SIP 要求は拒否されます。

Off：このゾーンを介して送信され、この Expressway が再度受信する SIP 要求は通常どおりに処理されます。

例：`xConfiguration Zones Zone 3 Neighbor SIP Poison Mode: Off`

xConfiguration Zones Zone [1..1000] Neighbor SIP Port: <1024..65534>

この Expressway で送受信する SIP コールに使用するネイバーのポートを指定します。デフォルトは 5061 です。

例：`xConfiguration Zones Zone 3 Neighbor SIP Port: 5061`

xConfiguration Zones Zone [1..1000] Neighbor SIP PreloadedSipRoutes Accept: <Off/On>

[プリロードされた SIP ルートのサポート（Preloaded SIP routes support）] を [オン（On）] に切り替えて、Route ヘッダーを含んだ SIP INVITE 要求をこのゾーンで処理できるようにします。このヘッダーを含んでいる SIP INVITE 要求をゾーンで拒否するには、[プリロードされた SIP ルートのサポート（Preloaded SIP routes support）] を [オフ（Off）] に切り替えます。

例：`xConfiguration Zones Zone 3 Neighbor SIP PreloadedSipRoutes Accept: On`

xConfiguration Zones Zone [1..1000] Neighbor SIP ProxyRequire Strip List: <S: 0,255>

このゾーンから受信した SIP 要求の Proxy-Require ヘッダーを検索し、そのヘッダーから削除するオプション タグのカンマ区切りのリスト。デフォルトでは、オプションタグは指定されません。

例：`xConfiguration Zones Zone 3 Neighbor SIP ProxyRequire Strip List: 「com.example.something,com.example.somethingelse」`

xConfiguration Zones Zone [1..1000] Neighbor SIP RFC3327 Enabled: <Yes/No>

このゾーンに REGISTER メッセージがプロキシ転送されるときに Expressway が RFC3327 Path ヘッダーを挿入するかどうかを制御します。無効にすると、Expressway が代わりに連絡先ヘッダーを書き換えて、RFC3327 をサポートしない SIP レジストラとのインターワーキングを許可します。デフォルトは Yes です。

例：`xConfiguration Zones Zone [1..1000] Neighbor SIP RFC3327 Enabled: Yes`

（注） バージョン X8.9 で、MRA に使用するネイバー ゾーンの自動作成機能を制御するトグルを導入しました。このバージョンのこれらのゾーンでは、デフォルトは No です。`xConfiguration CollaborationEdge RFC3327Enabled` を参照してください。

xConfiguration Zones Zone [1..1000] Neighbor SIP Record Route Address Type: <IP/Hostname>

Expressway がその IP アドレスを使用するか、このゾーンへの発信 SIP 要求の Record-Route または Path ヘッダーのホスト名を使用するかを制御します。注：ホスト名にこの値を設定すると、有効な DNS システム ホスト名も Expressway で設定する必要があります。デフォルトは IP です。

例：`xConfiguration Zones Zone 3 Neighbor SIP Record Route Address Type: IP`

xConfiguration Zones Zone [1..1000] Neighbor SIP SearchAutoResponse: <On/Off>

H.323 検索としてこのゾーン宛に発信された SIP 検索を Expressway が受信したときの動作を制御します。デフォルトは Off です。

Off：SIP OPTION メッセージはこのゾーンに送信されます。

On：検索に自動的に応答します。検索が転送されることはありません。

例：`xConfiguration Zones Zone 3 Neighbor SIP SearchAutoResponse: Off`

xConfiguration Zones Zone [1..1000] Neighbor SIP SipUpdateRefresh Support: <On/Off>

このゾーンで SIP UPDATE メッセージによるセッション更新をサポートするかどうかを指定します。

On：*SIP* セッションを更新するために、このゾーンから *SIP UPDATE* メッセージを送信します。

Off：このゾーンでは *SIP* セッション更新用の *SIP UPDATE* メッセージを送信しません。

デフォルトは Off です。

例：`xConfiguration Zones Zone 3 Neighbor SIP SipUpdateRefresh Support: Off`

xConfiguration Zones Zone [1..1000] Neighbor SIP TLS Verify Mode: <On/Off>

この Expressway とネイバー システム間のインバウンド接続とアウトバンド接続の X.509 証明書チェックと相互認証を制御します。有効になっている場合は、ピア アドレス フィールドで指定したネイバー システムの FQDN または IP アドレスがネイバーの X.509 証明書内（サブジェクト共通名またはサブジェクト代替名のどちらかの属性）に含まれている必要があります。デフォルトは Off です。

例：`xConfiguration Zones Zone 3 Neighbor SIP TLS Verify Mode: On`

xConfiguration Zones Zone [1..1000] Neighbor SIP Transport: <UDP/TCP/TLS>

このネイバーで送受信する SIP コールに使用するトランスポート タイプを決定します。デフォルトは TLS です。

例：`xConfiguration Zones Zone 3 Neighbor SIP Transport: TLS`

xConfiguration Zones Zone [1..1000] Neighbor SIP UDP BFCP Filter Mode: <On/Off>

このゾーンに送信された INVITE 要求から UDP/BFCP をフィルタリングにより除去するかどうかを決定します。UDP/BFCP プロトコルをサポートしない SIP デバイスとの相互運用性を有効にするためにこのオプションが必要な場合があります。デフォルトは Off です。

[オン（On）]：UDP/BFCP プロトコルを参照しているメディア回線が TCP/BFCP で置き換えられ、無効になります。

[オフ（Off）]：INVITE 要求は変更されません。

例：`xConfiguration Zones Zone 3 Neighbor SIP UDP BFCP Filter Mode: Off`

xConfiguration Zones Zone 1 Neighbor SIP UDP IX Filter Mode: <On/Off> このゾーンに送信された INVITE 要求から UDP/UDT/IX または UDP/DTLS/UDT/IX をフィルタリングにより除去するかどうかを決定します。 UDP/UDT/IX プロトコルまたは UDP/DTLS/UDT/IX プロトコルをサポートしない SIP デバイスとの相互運用性を有効にするためにこのオプションが必要な場合があります。デフォルトは Off です。 *[オン（On）]*：UDP/UDT/IX プロトコルまたは UDP/DTLS/UDT/IX プロトコルを参照するメディア回線を RTP/AVP に置き換えて無効にします。 *[オフ（Off）]*：INVITE 要求は変更されません。 例：`xConfiguration Zones Zone 1 neighbor SIP UDP IX Filter Mode: On`
xConfiguration Zones Zone [1..1000] Neighbor SIP UPDATE Strip Mode: <On/Off> このゾーンで送受信するすべての要求と応答の Allow ヘッダーから Expressway が UPDATE メソッドを削除するかどうかを制御します。デフォルトは Off です。 例：`xConfiguration Zones Zone 3 Neighbor SIP UPDATE Strip Mode: Off`
xConfiguration Zones Zone [1..1000] Neighbor SignalingRouting Mode: <Auto/Always> このネイバーで送受信するコールのシグナリングを Expressway がどのように処理するかを指定します。デフォルトは Auto です。 *Auto*：コールルーテッドモードの設定に従ってシグナリングを取得します。 *Always*：コールルーテッド モードの設定に関係なく、ネイバーで送受信するコールのシグナリングを常に取得します。 例：`xConfiguration Zones Zone 3 Neighbor SignalingRouting Mode: Auto`
xConfiguration Zones Zone [1..1000] Neighbor ZoneProfile: <Default/Custom/CiscoUnifiedCommunicationsManager/CiscoUnifiedCommunicationsManagerBFCP/NortelCS1000/NonRegisteringDevice/LocalB2BUAService> ゾーンの詳細な設定方法を決定します。 *Default*：工場出荷時の初期設定を使用します。 *[カスタム（Custom）]*：各設定を個別に行うことができます。 *Preconfigured profiles*：事前設定されたプロファイルのいずれかを選択して、そのタイプのシステムへの接続に必要な適切な設定を自動的に使用します。 例：`xConfiguration Zones Zone 3 Neighbor ZoneProfile: Default`
xConfiguration Zones Zone [1..1000] SIP Mode: <On/Off> このゾーンでの SIP コールの送受信を許可するかどうかを決定します。デフォルトは On です。 例：`xConfiguration Zones Zone 3 SIP Mode: On`

xConfiguration Zones Zone [1..1000] TraversalClient Authentication Mode: <DoNotCheckCredentials/TreatAsAuthenticated/CheckCredentials>

Expressway がこのゾーンからの着信メッセージをどのように認証するかを制御し、それらのメッセージを認証または未認証として処理するか、あるいは拒否するかを制御します。H.323 メッセージ、ローカル ドメインから発信される SIP メッセージか非ローカル ドメインから発信される SIP メッセージかによって動作が異なります。デフォルトは DoNotCheckCredentials です。

例：`xConfiguration Zones Zone 4 TraversalClient Authentication Mode: DoNotCheckCredentials`

xConfiguration Zones Zone [1..1000] TraversalClient Authentication Password: <S: 0,215>

トラバーサル サーバに接続するときに Expressway で使用するパスワード。プレーン テキストの最大長は 128 文字で、暗号化されます。

例：`xConfiguration Zones Zone 4 TraversalClient Authentication Password: 「password123」`

xConfiguration Zones Zone [1..1000] TraversalClient Authentication UserName: <S: 0,128>

トラバーサル サーバに接続するときに Expressway で使用するユーザ名。

例：`xConfiguration Zones Zone 4 TraversalClient Authentication UserName: 「clientname」`

xConfiguration Zones Zone [1..1000] TraversalClient H323 Port: <1024..65534>

この Expressway からの H.323 ファイアウォール トラバーサル コールに使用するトラバーサル サーバのポート。トラバーサル サーバが Expressway-E の場合、この Expressway に関連付けられた Expressway-E のトラバーサル ゾーンで設定されているポート番号にする必要があります。

例：`xConfiguration Zones Zone 4 TraversalClient H323 Port: 2777`

xConfiguration Zones Zone [1..1000] TraversalClient H323 Protocol: <Assent/H46018>

2 つのファイアウォール トラバーサル プロトコルのうちのどちらをトラバーサル サーバで送受信するコールに使用するかを決定します。注：このトラバーサル クライアントで送受信するコールのサーバに同じプロトコルを設定する必要があります。デフォルトは Assent です。

例：`xConfiguration Zones Zone 4 TraversalClient H323 Protocol: Assent`

xConfiguration Zones Zone [1..1000] TraversalClient Peer [1..6] Address: <S:0,128>

トラバーサル サーバの IP アドレスまたは完全修飾ドメイン名（FQDN）を指定します。トラバーサル サーバが Expressway-E クラスタの場合、これはそのクラスタ ピアの 1 つになります。

例：`xConfiguration Zones Zone 4 TraversalClient Peer 1 Address: 「10.192.168.1」`

xConfiguration Zones Zone [1..1000] TraversalClient Registrations: <Allow/Deny>

このゾーンを通じてルーティングされたプロキシ経由で送信される SIP 登録を受け入れるかどうかを制御します。デフォルトは Allow です。

例：`xConfiguration Zones Zone 4 TraversalClient Registrations: Allow`

xConfiguration Zones Zone [1..1000] TraversalClient RetryInterval: <1..65534>

トラバーサル サーバへの接続の確立に失敗した試行を再度試す間隔（秒単位）。デフォルトは 120 です。

例：`xConfiguration Zones Zone 4 TraversalClient RetryInterval: 120`

xConfiguration Zones Zone [1..1000] TraversalClient SIP SipUpdateRefresh Support: <Off/On>

このゾーンで SIP UPDATE メッセージによるセッション更新をサポートするかどうかを指定します。

On：*SIP* セッションを更新するために、このゾーンから *SIP UPDATE* メッセージを送信します。

Off：このゾーンでは *SIP* セッション更新用の *SIP UPDATE* メッセージを送信しません。

デフォルトは Off です。

例：`xConfiguration Zones Zone 1 TraversalClient SIP SipUpdateRefresh Support: On`

xConfiguration Zones Zone [1..1000] TraversalClient SIP Media AesGcm Support: <Off/On>

このゾーンを通過するメディアの AES GCM アルゴリズムによる暗号化/復号化を有効にします。デフォルトは Off です。

例：`xConfiguration Zones Zone 1 TraversalClient SIP Media AesGcm Support: On`

xConfiguration Zones Zone [1..1000] TraversalClient SIP Media Encryption Mode: <Off/On/BestEffort/Auto>

このゾーンで送受信される SIP コール（インターワーキング コールを含む）に Expressway によって適用されるメディア暗号化ポリシー。デフォルトは Auto です。

On：すべてのメディアを暗号化する必要があります。

Off：すべてのメディアの暗号化を解除する必要があります。

BestEffort：使用可能な場合は暗号化を使用します。使用できない場合は暗号化されていないメディアにフォールバックします。

Auto：メディア暗号化ポリシーは適用されません。

例：`xConfiguration Zones Zone 4 TraversalClient SIP Media Encryption Mode: Auto`

xConfiguration Zones Zone [1..1000] TraversalClient SIP Media ICE Support: <On/Off>

このゾーン内のデバイスで ICE をサポートするかどうかを制御します。デフォルトは Off です。

On：このゾーンでは ICE をサポートします。

Off：このゾーンでは ICE をサポートしません。

例：`xConfiguration Zones Zone 4 TraversalClient SIP Media ICE Support: On`

xConfiguration Zones Zone [1..1000] TraversalClient SIP Media ICEPassThrough Support: <On/Off>

このゾーン内のデバイスで ICE パススルーをサポートするかどうかを制御します。デフォルト：Off

On：このゾーンでは ICE パススルーをサポートします。

Off：このゾーンでは ICE パススルーをサポートしません。

例：`xConfiguration Zones Zone 4 TraversalClient SIP Media ICEPassThrough Support: On`

xConfiguration Zones Zone [1..1000] TraversalClient SIP Multistream Mode: <Off/On>

Expressway がこのゾーンのデバイス間のマルチストリームを許可するかどうかを制御します。デフォルトは On です。

On：マルチストリームを許可します。

Off：マルチストリームを拒否します。

例：`xConfiguration Zones Zone 1 TraversalClient SIP Multistream Mode: Off`

xConfiguration Zones Zone [1..1000] TraversalClient SIP Poison Mode: <On/Off>

ローカル Expressway が再度受信した場合は拒否するように、このゾーンに送信された SIP 要求を「ポイゾニング」するかどうかを制御します。デフォルトは Off です。

[オン（On）]：このゾーンを介して送信され、この Expressway が再度受信する SIP 要求は拒否されます。

Off：このゾーンを介して送信され、この Expressway が再度受信する SIP 要求は通常どおりに処理されます。

例：`xConfiguration Zones Zone 4 TraversalClient SIP Poison Mode: Off`

xConfiguration Zones Zone [1..1000] TraversalClient SIP Port: <1024..65534>

この Expressway からの SIP コールに使用するトラバーサル サーバのポートを指定します。トラバーサル サーバが Expressway-E の場合、この Expressway のトラバーサル ゾーンで設定されているポート番号にする必要があります。

例：`xConfiguration Zones Zone 4 TraversalClient SIP Port: 5061`

xConfiguration Zones Zone [1..1000] TraversalClient SIP PreloadedSipRoutes Accept: <Off/On>

[プリロードされた SIP ルートのサポート（Preloaded SIP routes support）] を [オン（On）] に切り替えて、Route ヘッダーを含んだ SIP INVITE 要求をこのゾーンで処理できるようにします。このヘッダーを含んでいる SIP INVITE 要求をゾーンで拒否するには、[プリロードされた SIP ルートのサポート（Preloaded SIP routes support）] を [オフ（Off）] に切り替えます。

例：`xConfiguration Zones Zone 3 Neighbor SIP PreloadedSipRoutes Accept: On`

xConfiguration Zones Zone [1..1000] TraversalClient SIP Protocol: <Assent/TURN/ICE>

どのファイアウォール トラバーサル プロトコルをトラバーサル サーバで送受信する SIP コールに使用するかを決定します。注：このトラバーサル クライアントで送受信するコールのサーバに同じプロトコルを設定する必要があります。デフォルトは Assent です。

例：`xConfiguration Zones Zone 4 TraversalClient SIP Protocol: Assent`

xConfiguration Zones Zone [1..1000] TraversalClient SIP TLS Verify Mode: <On/Off>

この Expressway とトラバーサル サーバ間での X.509 証明書チェックと相互認証を制御します。有効になっている場合は、ピア アドレス フィールドで指定したサーバの FQDN または IP アドレスがサーバの X.509 証明書内（サブジェクト共通名またはサブジェクト代替名のどちらかの属性）に含まれている必要があります。デフォルトは Off です。

例：`xConfiguration Zones Zone 4 TraversalClient SIP TLS Verify Mode: On`

xConfiguration Zones Zone [1..1000] TraversalClient SIP Transport: <TCP/TLS>

トラバーサル サーバで送受信する SIP コールに使用するトランスポート タイプを決定します。デフォルトは TLS です。

例：`xConfiguration Zones Zone 4 TraversalClient SIP Transport: TLS`

xConfiguration Zones Zone [1..1000] TraversalServer Authentication Mode: <DoNotCheckCredentials/TreatAsAuthenticated/CheckCredentials>

Expressway がこのゾーンからの着信メッセージをどのように認証するかを制御し、それらのメッセージを認証または未認証として処理するか、あるいは拒否するかを制御します。H.323 メッセージ、ローカル ドメインから発信される SIP メッセージか非ローカル ドメインから発信される SIP メッセージかによって動作が異なります。デフォルトは DoNotCheckCredentials です。

例：`xConfiguration Zones Zone 5 TraversalServer Authentication Mode: DoNotCheckCredentials`

xConfiguration Zones Zone [1..1000] TraversalServer Authentication UserName: <S: 0,128>

トラバーサル サーバで認証するときに、トラバーサル クライアントが使用する名前。トラバーサル クライアントが Expressway の場合は、その Expressway の認証ユーザ名にする必要があります。トラバーサル クライアントがゲートキーパーの場合は、そのゲートキーパーのシステム名にする必要があります。

例：`xConfiguration Zones Zone 5 TraversalServer Authentication UserName: 「User123」`

xConfiguration Zones Zone [1..1000] TraversalServer H323 H46019 Demultiplexing Mode: <On/Off>

トラバーサル クライアントからのコールに対して、Expressway が逆多重化モードで動作するかどうかを決定します。デフォルトは Off です。

On：すべてのコールに同じ 2 つのポートを使用できるようにします。

Off：各コールが個別のポートペアをメディアに使用します。

例：`xConfiguration Zones Zone 5 TraversalServer H323 H46019 Demultiplexing Mode: Off`

xConfiguration Zones Zone [1..1000] TraversalServer H323 Port: <1024..65534>

このトラバーサル クライアントからの H.323 ファイアウォール トラバーサルに使用する Expressway のポートを指定します。デフォルトは 6001 です（新しいゾーンごとに 1 ずつ増加）。

例：`xConfiguration Zones Zone 5 TraversalServer H323 Port: 2777`

xConfiguration Zones Zone [1..1000] TraversalServer H323 Protocol: <Assent/H46018>

2 つのファイアウォール トラバーサル プロトコルのうちのどちらをトラバーサル クライアントで送受信するコールに使用するかを決定します。注：このトラバーサル サーバで送受信するコールのクライアントに同じプロトコルを設定する必要があります。デフォルトは Assent です。

例：`xConfiguration Zones Zone 5 TraversalServer H323 Protocol: Assent`

xConfiguration Zones Zone [1..1000] TraversalServer Registrations: <Allow/Deny>

このゾーンを通じてルーティングされたプロキシ経由で送信される SIP 登録を受け入れるかどうかを制御します。デフォルトは Allow です。

例：`xConfiguration Zones Zone 5 TraversalServer Registrations: Allow`

xConfiguration Zones Zone [1..1000] TraversalServer SIP SipUpdateRefresh Support: <Off/On>

このゾーンで SIP UPDATE メッセージによるセッション更新をサポートするかどうかを指定します。

On：*SIP* セッションを更新するために、このゾーンから *SIP UPDATE* メッセージを送信します。

Off：このゾーンでは *SIP* セッション更新用の *SIP UPDATE* メッセージを送信しません。

デフォルトは Off です。

例：`xConfiguration Zones Zone 1 TraversalServer SIP SipUpdateRefresh Support: On`

xConfiguration Zones Zone [1..1000] TraversalServer SIP Media AesGcm Support: <Off/On>

このゾーンを通過するメディアの AES GCM アルゴリズムによる暗号化/復号化を有効にします。デフォルトは Off です。

例：`xConfiguration Zones Zone 1 TraversalServer SIP Media AesGcm Support: On`

xConfiguration Zones Zone [1..1000] TraversalServer SIP Media Encryption Mode: <Off/On/BestEffort/Auto>

このゾーンで送受信される SIP コール（インターワーキング コールを含む）に Expressway によって適用されるメディア暗号化ポリシー。デフォルト： [Auto]

On：すべてのメディアを暗号化する必要があります。

Off：すべてのメディアの暗号化を解除する必要があります。

BestEffort：使用可能な場合は暗号化を使用します。使用できない場合は暗号化されていないメディアにフォールバックします。

Auto：メディア暗号化ポリシーは適用されません。

例：`xConfiguration Zones Zone 5 TraversalServer SIP Media Encryption Mode: Auto`

xConfiguration Zones Zone [1..1000] TraversalServer SIP Media ICE Support: <On/Off>

このゾーン内のデバイスで ICE をサポートするかどうかを制御します。デフォルトは Off です。

On：このゾーンでは ICE をサポートします。

Off：このゾーンでは ICE をサポートしません。

例：`xConfiguration Zones Zone 5 TraversalServer SIP Media ICE Support: On`

xConfiguration Zones Zone [1..1000] TraversalServer SIP Media ICEPassThrough Support: <On/Off>

このゾーン内のデバイスで ICE パススルーをサポートするかどうかを制御します。デフォルト：Off

On：このゾーンでは ICE パススルーをサポートします。

Off：このゾーンでは ICE パススルーをサポートしません。

例：`xConfiguration Zones Zone 5 TraversalServer SIP Media ICEPassThrough Support: On`

xConfiguration Zones Zone [1..1000] TraversalServer SIP Multistream Mode: <Off/On>

Expresswayがこのゾーンのデバイス間のマルチストリームを許可するかどうかを制御します。デフォルトは On です。

On：マルチストリームを許可します。

Off：マルチストリームを拒否します。

例：`xConfiguration Zones Zone 1 TraversalServer SIP Multistream Mode: Off`

xConfiguration Zones Zone [1..1000] TraversalServer SIP Poison Mode: <On/Off>

ローカル Expressway が再度受信した場合は拒否するように、このゾーンに送信された SIP 要求を「ポイゾニング」するかどうかを制御します。デフォルトは Off です。

[オン（On）]：このゾーンを介して送信され、このExpressway が再度受信する SIP 要求は拒否されます。

Off：このゾーンを介して送信され、この Expressway が再度受信する SIP 要求は通常どおりに処理されます。

例：`xConfiguration Zones Zone 5 TraversalServer SIP Poison Mode: Off`

xConfiguration Zones Zone [1..1000] TraversalServer SIP Port: <1024..65534>

このトラバーサル クライアントからの SIP ファイアウォール トラバーサルに使用する Expressway のポート。デフォルトは 7001 です（新しいゾーンごとに 1 ずつ増加）。

例：`xConfiguration Zones Zone 5 TraversalServer SIP Port: 5061`

xConfiguration Zones Zone [1..1000] TraversalServer SIP PreloadedSipRoutes Accept: <Off/On>

[プリロードされた SIP ルートのサポート（Preloaded SIP routes support）] を [オン（On）] に切り替えて、Route ヘッダーを含んだ SIP INVITE 要求をこのゾーンで処理できるようにします。このヘッダーを含んでいる SIP INVITE 要求をゾーンで拒否するには、[プリロードされた SIP ルートのサポート（Preloaded SIP routes support）] を [オフ（Off）] に切り替えます。

例：`xConfiguration Zones Zone 3 Neighbor SIP PreloadedSipRoutes Accept: On`

xConfiguration Zones Zone [1..1000] TraversalServer SIP Protocol: <Assent/TURN/ICE>

どのファイアウォール トラバーサル プロトコルをトラバーサル クライアントで送受信する SIP コールに使用するかを決定します。注：このトラバーサル サーバで送受信するコールのクライアントに同じプロトコルを設定する必要があります。デフォルトは Assent です。

例：`xConfiguration Zones Zone 5 TraversalServer SIP Protocol: Assent`

xConfiguration Zones Zone [1..1000] TraversalServer SIP TLS Verify Mode: <On/Off>

この Expressway とトラバーサル クライアント間での X.509 証明書チェックと相互認証を制御します。有効にした場合は、TLS 検証サブジェクト名を指定する必要があります。デフォルトは Off です。

例：`xConfiguration Zones Zone 5 TraversalServer SIP TLS Verify Mode: On`

xConfiguration Zones Zone [1..1000] TraversalServer SIP TLS Verify Subject Name: <S: 0,128>

トラバーサル クライアントの X.509 証明書で検索する証明書の所有者の名前（サブジェクト共通名の属性またはサブジェクト代替名の属性のいずれかに含まれている必要があります）。

例：`xConfiguration Zones Zone 5 TraversalServer SIP TLS Verify Subject Name: 「myclientname」`

xConfiguration Zones Zone [1..1000] TraversalServer SIP Transport: <TCP/TLS>

トラバーサル クライアントと Expressway 間の SIP コールに 2 つのトランスポート タイプのどちらを使用するかを決定します。デフォルトは TLS です。

例：`xConfiguration Zones Zone 5 TraversalServer SIP Transport: TLS`

xConfiguration Zones Zone [1..1000] TraversalServer TCPProbe KeepAliveInterval: <1..65534>

コールが確立した後、ファイアウォールのNATバインドを有効にしておくために、トラバーサル クライアントが TCP プローブを Expressway に送信する間隔（秒単位）を設定します。デフォルト：20。

例：`xConfiguration Zones Zone 5 TraversalServer TCPProbe KeepAliveInterval: 20`

xConfiguration Zones Zone [1..1000] TraversalServer TCPProbe RetryCount: <1..65534>

トラバーサル クライアントが Expressway への TCP プローブの送信を試行する回数を設定します。デフォルトは 5 です。

例：`xConfiguration Zones Zone 5 TraversalServer TCPProbe RetryCount: 5`

xConfiguration Zones Zone [1..1000] TraversalServer TCPProbe RetryInterval: <1..65534>

トラバーサル クライアントが Expressway に TCP プローブを送信する頻度（秒単位）を設定します。デフォルトは 2 です。

例：`xConfiguration Zones Zone 5 TraversalServer TCPProbe RetryInterval: 2`

xConfiguration Zones Zone [1..1000] TraversalServer UDPProbe KeepAliveInterval: <1..65534>

コールが確立した後、ファイアウォールのNATバインドを有効にしておくために、トラバーサル クライアントが UDP プローブを Expressway に送信する間隔（秒単位）を設定します。デフォルトは 20 です。

例：`xConfiguration Zones Zone 5 TraversalServer UDPProbe KeepAliveInterval: 20`

xConfiguration Zones Zone [1..1000] TraversalServer UDPProbe RetryCount: <1..65534>

トラバーサル クライアントが Expressway への UDP プローブの送信を試行する回数を設定します。デフォルトは 5 です。

例：`xConfiguration Zones Zone 5 TraversalServer UDPProbe RetryCount: 5`

xConfiguration Zones Zone [1..1000] TraversalServer UDPProbe RetryInterval: <1..65534>

トラバーサル クライアントが Expressway に UDP プローブを送信する頻度（秒単位）を設定します。デフォルトは 2 です。

例：`xConfiguration Zones Zone 5 TraversalServer UDPProbe RetryInterval: 2`

xConfiguration Zones Zone [1..1000] Type: <Neighbor/TraversalClient/TraversalServer/ENUM/DNS>

ローカル Expressway に関連して、指定したゾーンの特性を決定します。

Neighbor：新しいゾーンはローカル Expressway のネイバーになります。

TraversalClient：ゾーン間にファイアウォールがあり、ローカル Expressway が新しいゾーンのトラバーサルクライアントになります。

TraversalServer：ゾーン間にファイアウォールがあり、ローカル Expressway が新しいゾーンのトラバーサルサーバになります。

ENUM：ゾーンに ENUM ルックアップで検出されたエンドポイントが含まれます。

DNS：ゾーンに DNS ルックアップで検出されたエンドポイントが含まれます。

例：`xConfiguration Zones Zone 3 Type: Neighbor`

xConfiguration license smart debug: <error/trace/debug/all>

スマートライセンシングのデバッグを有効します。デフォルト：エラー

Error：スマートライセンシングで発生したエラーをログに記録します。

Trace：通常のスマートライセンシング操作中にトレースメッセージをログに記録します。

Debug：デバッグメッセージをログに記録します。

All：3 つのレベルをすべて有効します。（ピア固有）

例：`xConfiguration license smart debug: all`

xConfiguration license smart deregister: <On/Off>

評価期間が満了していなければ、製品は評価モードに戻ります。製品で使用されるすべてのライセンス付与がバーチャルアカウントにすぐに戻されて、他の製品インスタンスで使用できるようになります。（ピア固有）

例：`xConfiguration license smart deregister: On`

xConfiguration license smart enable mode: <On/Off>

この製品インスタンスでスマートライセンシングを有効にします。デフォルトは Off です。

On：スマートライセンシングを使用してライセンスを管理します。

Off：従来の PAK ベースのライセンスを使用して、ライセンスを管理します。スマートライセンシングが [オン（On）] に設定されている場合、Web インターフェイスを使用して [オフ（Off）] に設定することはできません)。スマートライセンシングを無効にして従来のライセンスを使用するには、システムリセットを実行します。デフォルトはOffです。（ピア固有）

例：`xConfiguration license smart enable: On`

xConfiguration license smart privacy: <none/all/hostname/version>

この製品インスタンスのホスト名と IP アドレスを Cisco Smart Software Manager または Cisco Smart Software Manager Satellite と交換する必要がない場合に使用します。（ピア固有）

例：`xConfiguration license smart privacy: all`

xConfiguration license smart register idtoken: <String>

Smart Software Manager または Smart Software Manager サテライトから生成した製品インスタンス登録トークンを使用して製品を登録します。（ピア固有）

例：`xConfiguration license smart register idtoken: <Token>`

xConfiguration license smart renew ID: <On/Off>

Cisco Smart Software Manager のネットワーク接続の問題が原因で自動登録の更新に失敗した場合は、この操作を実行します。（ピア固有）

例：`xConfiguration license smart renew ID: On`

xConfiguration license smart renew auth: <On/Off>

Cisco Smart Software Manager によるネットワーク接続の問題が原因で、自動認証ステータスの更新に失敗した場合は、この操作を実行します。（ピア固有）

例：`xConfiguration license smart renew auth: On`

xConfiguration license smart transport: <direct/satellite>

この製品インスタンスが Cisco Smart Software Manager と通信して使用情報を送受信する方法を決定します。

Direct：Cisco Smart Software Manager とインターネットを介して直接通信します。

Satellite：オンプレミスに導入された Smart Software Manager のサテライトを介して通信します。

例：`xConfiguration license smart transport: direct`

xConfiguration license smart reregister: <String>

次の場合に、この操作を実行して製品インスタンスを再登録します（この製品インスタンスの以前の登録の試行が、ネットワーク接続の問題によって失敗し、この問題を解決した後に再登録する必要があります）。仮想アカウントにすでに登録されている製品インスタンスを別の仮想アカウントに再登録するには。（ピア固有）

例：`xConfiguration license smart reregister: <Token>`

xConfiguration license smart url: <String>

Cisco Smart Software Manager のサテライトサーバの URL を入力します。（ピア固有）

例：`xConfiguration license smart url: http://www.alpha.crate.cisco.com/Transport gateway`

コマンド リファレンス — xCommand

項目を追加または削除し、システム コマンドを発行するには、**xCommand** グループのコマンドを使用します。

ここでは、現在利用可能なすべての **xCommand** コマンドを記載します。

コマンドを発行するには、示されているとおりにコマンドを入力した後、1 つまたは複数の所定のパラメータと値を入力します。次の表記法を使用して、各パラメータの有効な値を山かっこ内に示し、その後に各パラメータを示します。

書式	意味
<0..63>	整数値が必要であることを示します。数値は最小値と最大値を示しています。 この例では、0 ～ 63 の範囲内の値にする必要があります。
<S: 7,15>	**S** は引用符で囲まれた文字列値が必要であることを示します。数値は文字列の最小文字数と最大文字数を示します。 この例では、文字列の長さを 7 ～ 15 文字にする必要があります。
<Off/Direct/Indirect>	コマンドの有効な一連の値を示します。値は引用符で囲まないでください。
(r)	これが必須パラメータであることを示します。(r) はコマンド自体の一部ではないことに注意してください。

各 **xCommand** コマンドの使用に関する情報を CLI 内から取得するには、次のように入力します。

- **xCommand**または **xCommand ?** ：使用可能なすべての **xCommand** コマンドを取得する場合。
- **xCommand ??** ：現在のすべての **xCommand** コマンドと、各コマンドの説明、パラメータのリスト、各パラメータの値空間と説明を取得する場合。
- **xCommand <command> ?**：特定のコマンドとそのパラメータ、各パラメータの値空間と説明を返す場合。

set-access コマンド（試験版）について

set-access コマンドを使用すると、Expressway の内部システム コマンドにアクセスできます。**これらのコマンドは、シスコのサポートおよび開発チームのみが使用するために存在するもの**

です。シスコのサポート担当者のアドバイスや指示がない限り、これらのコマンドにはアクセスしないでください。

⚠

注意 これらのコマンドを誤って使用すると、システムの動作が不安定になったり、パフォーマンス上の問題が発生したり、システム設定が永続的に破損したりする可能性があります。

set-access を使用するには、次の手順に従います。

1. CLI に管理者としてログインします。
2. `set-access qwertsys` と入力します。

   これにより、set-access に関連付けられているシステム コマンド（名前が「「sys-」」で始まるコマンド）が有効になります。
3. 使用可能なコマンドをリストするには、? と入力します。

xCommand コマンド

次の表に、使用可能なすべての **xCommand** コマンドを記載します。

表 *45 : xCommand CLI reference*

xCommand ACME Delete Pending Cert
保留中の証明書を削除します。 *Domain*：<文字列> 保留中の証明書とは、ACME プロバイダーにより署名された後、Expressway にまだ導入されていないか、導入されていない可能性がある証明書を意味します。 引数を渡さずに、または空の文字列を渡してこのコマンドを実行すると、保留中のサーバ証明書が削除されます。引数を渡して実行すると、指定したドメインに対して保留中になっている証明書が削除されます。 例：`xCommand ACME Delete Pending Cert` `xCommand ACME Delete Pending Cert Domain:「example.com」`

xCommand ACME Deploy

保留中の証明書を導入します。

Domain：<文字列>

ReloadCerts：<*On/Off*>

引数を渡さずにこのコマンドを実行すると、保留中のサーバ証明書が導入され、必要なプロセスに対して証明書がリロードされます。

引数を渡すと、指定したドメインの証明書が導入されます。また、ReloadCerts パラメータで指定されている場合は証明書のリロードも行われます。

例：`xCommand ACME Deploy`

`xCommand ACME Deploy Domain:「example.com」 ReloadCerts:「On」`

xCommand ACME Get Pending Cert

保留中の証明書を取得します。

Domain：<文字列>

保留中の証明書とは、ACME プロバイダーにより署名された後、Expressway にまだ導入されていないか、導入されていない可能性がある証明書を意味します。

引数を渡さずにこのコマンドを実行すると、保留中のサーバ証明書が取得されます。引数を渡して実行すると、指定したドメインの保留中の証明書が返されます。

例：`xCommand ACME Get Pending Cert`

`xCommand ACME Get Pending Cert Domain:「example.com」`

xCommand ACME Providers Read

ACME プロバイダーに関する情報を読み取ります。

ProviderUuid: <「*Default*」*/String*>

引数を渡さずにこのコマンドを実行すると、データベース内のすべてのプロバイダーに関する情報が返されます。文字列「Default」を渡すと、デフォルトのプロバイダーに関する情報が返されます。特定のプロバイダーに関する情報を返すには、そのプロバイダーの UUID を指定します。

例：`xCommand ACME Providers Read`

`xCommand ACME Providers Read ProviderUuid: 「Default」`

`xCommand ACME Providers Read ProviderUuid: 「Provider-UUID」`

xCommand ACME Providers Write

プロバイダーに関する情報を更新します。

Default：<*On/Off*>

Email(r)：<文字列>

Name：<文字列>

ProviderUuid(r): <「*Default*」*/String*>

TermsOfService(r): <Accepted>

Url：<*String*>

ProviderUuid、Email、TermsOfService の各引数を指定する必要があります。このコマンドでは、特定のプロバイダーの電子メールアドレスとサービス利用規約のみを更新できます。ほかの引数を指定しても、すべて無視されます。

例：`xCommand ACME Providers Write ProviderUuid: 「Default」 Email: new-email@example.com 「 TermsOfService: 」「Accepted」`

xCommand ACME Reset

Expressway-E 上の ACME サービスをリセットし、CLI、REST API、または Web インターフェイスを使用して実行されたすべての設定を削除します。

Action：<*execute*>

このコマンドは Expressway-E 上でのみ呼び出すことができます。SIGN、DISCARD、または DEPLOY コマンドの実行中は、このコマンドを実行できません。Acmereset を実行できるのは、すべてのドメイン証明書とサーバ証明書に対して ACME サービスが無効にされている場合のみです。

例：`xCommand ACME Reset execute`

```
xCommand ACME Reset Action: 「execute」
```

xCommand ACME Revoke

ACME 証明書を取り消します。

CertPath：<文字列>

Provider：<文字列>

ACME 証明書を取り消すには、その前に、取り消す証明書内のドメイン名/SAN エントリの管理権限を持っていることをプロバイダーに証明する必要があります。

これを証明するには、通常の送信および署名プロセスに従って、元の証明書と同じドメイン名/SAN エントリが含まれる新しい証明書を生成する必要があります。

この新しい証明書を受け取った後、古い証明書のパスを指定した `acmerevoke` を使用して古い証明書を取り消します。

デフォルトの ACME プロバイダーを使用した例：`xCommand ACME Revoke 「/path_to_cert_to_be_revoked」`

特定の ACME プロバイダーを使用した例：`xCommand ACME Revoke CertPath: 「/path_to_cert_to_be_revoked」 Provider:「ACME_Provider_Name」`

xCommand ACME Settings Read

ACME の設定を読み取ります。

Domain：<文字列>

サーバ証明書の ACME 設定を読み取るに、パラメータを指定せずにこのコマンドを入力します。特定のドメインの ACME 設定を読み取る場合は、そのドメインを指定します。

例：`xCommand ACME Settings Read`

`xCommand ACME Settings Read 「example.com」`

xCommand ACME Settings Write

ACME の設定を書き込みます。

AcmeManaged(r): < 無効化/手動または自動 >

Domain：<文字列>

ProviderUuid：<文字列>

RenewKey：<*Retain/Rotate*>

RenewalSchedule：<文字列>

ドメインを指定しない場合、このコマンドにより、サーバ証明書を管理しているACMEサービスの設定が書き込まれます。ドメインを指定すると、そのドメインの設定が書き込まれます。

指定したドメインにまだACMEが設定されていない場合、このコマンドはデフォルトプロバイダーの UUID を使用してそのドメインの ACME 設定を書き込みます。

指定したドメインにすでにACMEが設定されている場合、このコマンドは指定された設定だけを更新し、指定されていない設定は変更しません。

AcmeManaged パラメータを指定する必要があります。AcmeManaged を Automated に設定する場合は、RenewalSchedule と RenewKey も指定する必要があります。

例：`xCommand ACME Settings Write AcmeManaged: 「Manual」`

```
xCommand ACME Settings Write AcmeManaged: 「Automated」 Domain: 「example.com」
RenewalSchedule: 「{ 「DaysOfWeek」:[ 「Mon」 ],「TimeOfDay」:「04:00」 }」 RenewKey: 「Rotate」
```

xCommand ACME Sign

CSR に署名します。

Domain：<文字列>

NumSanEntries：<*-2147483648..2147483647*>

サーバ証明書の CSR を該当する ACME プロバイダーに送信する場合は、パラメータを指定せずにコマンドを入力します。ドメイン証明書の CSR を該当する ACME プロバイダーに送信する場合は、ドメインを指定します。

`NumSanEntries`パラメータは指定しないでください。これはユーザが変更するためのものではありません。

例：`xCommand Acme Sign`

```
xCommand ACME Sign Domain: 「example.com」
```

xCommand Admin Account Add

ローカル管理者アカウントを追加します。

Name(r): <S: 0, 128>

このアカウントのユーザ名。

Password(r)：<パスワード>

この アカウントのパスワード。

AccessAPI：*<On/Off>*

このアカウントが API を使用してシステムのステータスと設定にアクセスできるかどうか。デフォルトは On です。

AccessWeb：*<On/Off>*

このアカウントが Web インターフェイスを使用してシステムにログインできるかどうか。デフォルトは On です。

Enabled：*<On/Off>*

アカウントが有効になっているか、無効になっているかを示します。無効なアカウントへのアクセスは拒否されます。デフォルトは On です。

例：`xCommand Admin Account Add Name: 「bob_smith」Password: 「abcXYZ_123」 AccessAPI: On AccessWeb: On Enabled: On`

xCommand Admin Account Delete

ローカル管理者アカウントを削除します。

Name(r): <S: 0, 128>

削除するアカウントのユーザ名。

例：`xCommand Admin Account Delete: 「bob_smith」`

xCommand Admin Group Add

Name(r): <S: 0, 128>

管理者グループの名前。

AccessAPI：*<On/Off>*

このグループのメンバーが API を使用してシステムのステータスと設定にアクセスできるかどうか。デフォルトは On です。

AccessWeb：*<On/Off>*

このグループのメンバーが Web インターフェイスを使用してシステムにログインできるかどうか。デフォルトは On です。

Enabled：*<On/Off>*

グループが有効であるか無効であるかを示します。無効なグループのメンバーへのアクセスは拒否されます。デフォルトは On です。

例：`xCommand Admin Group Add Name: 「administrators」AccessAPI: On AccessWeb: On Enabled: On`

xCommand Admin Group Delete

管理者グループを削除します。

Name(r): <S: 0, 128>

削除するグループの名前。

例：`xCommand Admin Group Delete: 「administrators」`

xCommand Allow List Add

許可リストにエントリを追加します。

PatternString(r)：*<S: 1, 60>*

許可リストに追加するエントリを指定します。エンドポイントのエイリアスの 1 つが許可リストのパターンの 1 つと一致した場合に登録が許可されます。

PatternType：*<Exact/Prefix/Suffix/Regex>*

許可リスト内のエントリがプレフィックスか、サフィックスか、正規表現か、または完全一致かを指定します。

Exact：文字列は 1 文字も違うことなくエイリアスと一致する必要があります。

[プレフィックス（Prefix）]：文字列がエイリアスの先頭に表示される必要があります。

Suffix：文字列がエイリアスの末尾に表示される必要があります。

Regex：文字列は正規表現として処理されます。

デフォルトは Exact です。

Description: <S: 0,64>

自由形式の許可リスト ルールの説明。

例：`xCommand Allow List Add PatternString: 「John.Smith@example.com」 PatternType: Exact Description: 「Allow John Smith」`

xCommand Allow List Delete

許可リストからエントリを削除します。

AllowListId(r)：*<1..2500>*

削除するエントリのインデックス。

例：`xCommand Allow List Delete AllowListId: 2`

xCommand Boot

Expresswayをリブートします。

このコマンドにはパラメータがありません。

例：`xCommand Boot`

xCommand Check Bandwidth

指定したタイプと帯域幅のコールが 2 つのノード間で取得するステータスとルート（ノードとリンクのリスト）を返す診断ツール。このコマンドは、既存のシステム設定を変更しません。

Node1(r)：*<S: 1, 50>*

コールを発信するサブゾーンまたはゾーン。

Node2(r)：*<S: 1, 50>*

コールが終端されるサブゾーンまたはサブゾーン。

Bandwidth(r)：*<1..100000000>*

コールの要求された帯域幅（kbps 単位）。

CallType(r)：*<Traversal/NonTraversal>*

コール タイプがトラバーサルか非トラバーサルか。

例：`xCommand Check Bandwidth Node1: 「DefaultSubzone」 Node2: 「UK Sales Office」 Bandwidth: 512 CallType: nontraversa`

xCommand Check Pattern

システムにエイリアス トランスフォーメーションを設定する前にそのトランスフォーメーション（ローカルまたはゾーン）の結果を確認できる診断ツール。

Target(r)：*<S: 1, 60>*

パターン マッチまたはトランスフォーメーションのテストに使用するエイリアス。

Pattern(r)：*<S: 1, 60>*

エイリアスと比較するパターン。

Type(r)：*<Exact/Prefix/Suffix/Regex>*

適用するパターン動作のエイリアスとパターン文字列をどのように照合するか。

Behavior(r)：*<Strip/Leave/Replace/AddPrefix/AddSuffix>*

エイリアスをどのように変更するかを示します。

Replace：*<S: 0, 60>*

選択したパターン動作とともに使用するテキスト文字列。

例：`xCommand Check Pattern Target: 「bob@a.net」 Pattern:「@a.net」 Type: 「suffix」 Behavior: replace Replace: 「@a.com」`

xCommand Clear All Status

システムのすべてのステータスと履歴をクリアします。

例：`xCommand Clear All Status`

xCommand Cluster Address Mapping Add

Fqdn(r)：<値>

IpAddress(r)：<値>

FQDN/IP マッピング エントリをクラスタ アドレス マッピング テーブルに追加します。

xCommand Cluster Address Mapping Delete

Fqdn(r)：<値>

IpAddress(r)：<値>

FQDN/IP マッピング エントリをクラスタ アドレス マッピング テーブルから削除します。

xCommand CMS Add

Cisco Meeting Server Web ブリッジを管理します。ゲスト アカウント クライアント URI を追加します。

Name: <値>

例：`xCommand CMS Add name: 「join.example.com」`

xCommand CMS Delete

Cisco Meeting Server Web ブリッジを管理します。ゲスト アカウント クライアント URI を削除します。

Name: <値>

例：`xCommand CMS Delete name: 「join.example.com」`

xCommand Credential Add

ローカル認証データベースにエントリを追加します。

Name(r)：<文字列>

ローカル認証データベースにこのエントリの名前を定義します。

Password(r)：<パスワード>

ローカル認証データベースにこのエントリのパスワードを定義します。

プレーン テキストの最大長は 128 文字で、これらの文字は暗号化されます。

例：`xCommand Credential Add Name: 「alice」 Password: 「abcXYZ_123」`

xCommand Credential Delete

ローカル認証データベースからエントリを削除します。

Name(r)：<文字列>

削除するエントリの名前。

例：`xCommand Credential Delete Name: 「alice」`

xCommand CUCM Config Add

Unified CM パブリッシャでルックアップを実行します。

Address(r)：<値>

Unified CM パブリッシャの FQDN または IP アドレス。

Axlpassword(r)：<値>

Unified CM パブリッシャにアクセスするために Expressway が使用するパスワード。

Axlusername(r)：<値>

Unified CM パブリッシャにアクセスするために Expressway が使用するユーザ名。

CertValidationDisabled：<*On/Off*>

Unified CM パブリッシャが提示した証明書と照合する X.509 証明書の確認を制御します。デフォルトは On です。

例：`xCommand CUCM Config Add Address: 「cucm.example.com」 Axlpassword: 「xyz」 Axlusername: 「abc」`

xCommand CUCM Config Delete

Unified CM パブリッシャの詳細情報を削除します。

Address(r)：<値>

Unified CM パブリッシャの FQDN または IP アドレス。

例：`xCommand CUCM Config delete Address: 「cucm.example.com」`

xCommand CUCM Mixed Mode Check

Address(r)：<値>

Unified CM パブリッシャの FQDN または IP アドレス。

Axlpassword(r)：<値>

Unified CM パブリッシャにアクセスするために Expressway が使用するパスワード。

Axlusername(r)：<値>

Unified CM パブリッシャにアクセスするために Expressway が使用するユーザ名。

Command Custom Notification Add

アラームベースの電子メール通知用にカスタマイズされたエントリを追加します。アラーム ID ごとに、アラーム ID の通知を無効にするか、指定された電子メールアドレスに送信します。

alarm_id：<String> 通知をカスタマイズまたは無効化するアラーム ID を入力します。

custom_email：<S:0,254> 通知が「カスタム」の場合は、選択したアラーム通知の送信に使用する電子メール ID を入力します。

disable_notify：<on/off> 選択したアラームに対するアクションを選択します。

- [オン（On）]：選択したアラームに関する通知は送信されません。
- [オフ（Off）]：選択したアラームに関する通知が電子メールフィールドに入力された電子メール ID に送信されます。

デフォルトは On です。

カスタム通知を追加するには、disable_notify を 「[オフ（Off）]」 に指定します。

カスタム通知が追加された後は、xconfiguration コマンドの 「[アラーム通知電子メール（Alarm Notification Email）]」にリストされます。

xCommand Custom Notification Delete

アラームベースの電子メール通知用にカスタマイズされたエントリを削除します。

alarm_id(r): <*String*>：通知をカスタマイズまたは無効化するアラーム ID を入力します。

xCommand Default Links Add

デフォルトのサブゾーン、トラバーサル サブゾーン、およびデフォルト ゾーン間のリンクを復元します。

このコマンドにはパラメータがありません。

例：`xCommand Default Links Add`

xCommand Default Values Set

システム パラメータをデフォルト値にリセットします。レベル 1 は、レベル 2 とレベル 3 の項目を除き、ほとんどの設定項目をデフォルト値にリセットします。レベル 2 は、リモート認証関連の設定項目とレベル 1 の項目をデフォルト値にリセットします。レベル 3 は、重大なすべての設定項目と、レベル 1 および レベル 2 の項目をデフォルト値にリセットします。

Level(r)：*<1..3>*

リセットするシステム パラメータのレベル。

例：`xCommand Default Values Set Level: 1`

xCommand Deny List Add

拒否リストにエントリを追加します。

PatternString(r)：*<S: 1, 60>*

拒否リストに追加するエントリを指定します。エンドポイントのエイリアスの 1 つが拒否リストのパターンの 1 つと一致した場合は登録が許可されません。

PatternType：*<Exact/Prefix/Suffix/Regex>*

拒否リスト内のエントリがプレフィックスか、サフィックスか、正規表現か、または完全一致かを指定します。

Exact：文字列は 1 文字も違うことなくエイリアスと一致する必要があります。

[プレフィックス（Prefix）]：文字列がエイリアスの先頭に表示される必要があります。

Suffix：文字列がエイリアスの末尾に表示される必要があります。

Regex：文字列は正規表現として処理されます。

デフォルトは Exact です。

Description: <S: 0, 64>

自由形式の拒否リスト ルールの説明。

例：`xCommand Deny List Add PatternString: 「sally.jones@example.com」 PatternType: exact Description: 「Deny Sally Jones」`

xCommand Deny List Delete

拒否リストからエントリを削除します。

DenyListId(r)：*<1..2500>*

削除するエントリのインデックス。

例：`xCommand Deny List Delete DenyListId: 2`

xCommand Disconnect Call

コールを切断します。

Call：*<1..1000>*

切断するコールのインデックス。

CallSerialNumber：*<S: 1, 255>*

切断するコールのシリアル番号。コール インデックスかコール シリアル番号かのいずれかを指定する必要があります。

例：`xCommand Disconnect Call CallSerialNumber: 「6d843434-211c-11b2-b35d-0010f30f521c」`

xCommand DNS Lookup

指定したホスト名について DNS を照会します。

Hostname：<値>

照会するホストの名前。

RecordType：<*all/a/aaaa/srv/naptr*>

検索するレコードのタイプ。指定しない場合は、すべてのレコード タイプが返されます。

例：`xCommand DNS Lookup Hostname: 「example.com」 RecordType: all`

xCommand DNS Per Domain Server Add

特定のドメインのホスト名を解決するためのみに使用する DNS サーバを追加します。

Address(r)：<値>

関連付けられたドメイン名のホスト名を解決するときに使用する DNS サーバの IP アドレス。

Domain1(r)：<値>

特定の DNS サーバに関連付けるドメイン。

Domain2(r)：<値>

特定の DNS サーバに関連付けるオプションの 2 番目のドメイン。

Index：<*0..5*>

追加するサーバのインデックス。

例：`xCommand DNS Server Add Address: 「192.168.12.0」 Index: 1`

xCommand DNS Per Domain Server Delete

特定のドメインのホスト名を解決するために使用する DNS サーバを削除します。

Address：<値>

削除する DNS サーバの IP アドレス。

例：`xCommand DNS Per Domain Server Delete Address: 「192.168.12.0」`

xCommand DNS Server Add

デフォルトの DNS サーバを追加します。デフォルトのサーバは、ルックアップするドメインに定義されたドメイン単位の DNS サーバがない場合に使用します。

Address(r)：<値>

ドメイン名を解決するときに使用するデフォルトの DNS サーバの IP アドレス。

Index：<*0..5*>

追加するサーバのインデックス。

例：`xCommand DNS Server Add Address: 「192.168.12.0」 Index: 1`

xCommand DNS Server Delete

DNS サーバを削除します。

Address：<値>

削除する DNS サーバの IP アドレス。

例：`xCommand DNS Server Delete Address: 「192.168.12.0」`

xCommand Domain Add

この Expressway が権限を持つドメインを追加します。

Name(r): <S: 1, 128>

ドメイン名。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。

Edgesip：*<On/Off>*

Unified CM が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を提供します。デフォルトは Off です。

Edgexmpp：*<On/Off>*

Unified CM IM&P サービスがこの SIP ドメインのインスタント メッセージングとプレゼンスのサービスを提供します。デフォルトは Off です。

Sip：*<On/Off>*

Expressway がこのドメインに権限を持つかどうかを制御します。Expressway は、ドメインの SIP レジストラおよびプレゼンスサーバーとして機能し、このドメインを含むエイリアスで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。

Xmppfederation：*<On/Off>*

XMPP フェデレーションにドメインを使用できるかどうかを制御します。デフォルトは Off です。

例：`xCommand Domain Add Name: 「100.example-name.com」 Authzone: 「Traversal zone」 Edge: Off Sip: On`

xCommand Domain Delete

ドメインを削除します。

ドメイン *Id(r): <1..200>*

削除するドメインのインデックス。

例：`xCommand Domain Delete DomainId: 2`

xCommand Domain Certs

サーバ名指定（SNI）のマルチドメイン証明書を管理します。

各ドメイン証明書 xCommand には、実行する操作を指定する「command」パラメータと、その後に特定のコマンドに必要な追加パラメータが必要です。

ドメイン証明書コマンドと関連するパラメータ：

domain_list：SNI の証明書を管理するドメインを一覧表示します。

パラメータ：（なし）

例：`xCommand Domain Certs command: domain_list`

domain_create：SNI の証明書を管理するための新しいドメインを作成します。

パラメータ：domain

例：`xCommand Domain Certs command: domain_create domain: a.com`

domain_delete：指定した証明書ドメインを削除します。

パラメータ：domain

例：`xCommand Domain Certs command: domain_delete domain: a.com`

is_csr_pending：ドメインの証明書署名要求が保留中の場合は true を返します。

パラメータ：domain

例：`xCommand Domain Certs command: is_csr_pending domain: a.com`

csr_create：ドメインの証明書署名要求を作成します。

パラメータ：domain、subjectfields、sans、digestalgorithm、keysize

例：`xCommand Domain Certs command: csr_create domain: a.com keysize: 4096 digestalgorithm: sha256 sans: 'DNS:host1.a.com, DNS:host2.a.com' subjectfields: '{ 「CN」 「www.a.com」, 「C」: 「US」, 「ST」: 「North Carolina」, 「L」:「RTP」, 「O」: 「a」, 「OU」: 「example org unit」, 「emailAddress」: 「admin@a.com」 }'`

（注）
- xCommand パラメーター値は、スペースを含めることができるように、単一引用符で囲むことができます。
- sans はオプションのカンマで区切られたホスト名のリストです。各ホスト名の先頭には「DNS:」が追加されています（RFC5280 参照）。
- subjectfields は、各 [サブジェクト名（Subject Name）] フィールドの名前と値のペアのリストを含む JSON オブジェクトです（RFC5280 参照）。
- JSON の名前と値は、次のように二重引用符で囲む必要があります。
- keysize は、CSR 用に生成された秘密キーのビットの長さです。
- digestalgorithm は、CSR に署名するために使用されるメッセージ ダイジェスト アルゴリズムの名前です（「openssl dgst」を参照）。

csr_get：保留中の証明書署名要求を PEM 形式で返します。

パラメータ：domain

例：`xCommand Domain Certs command: csr_get domain: a.com`

csr_delete：保留中の証明書署名要求を削除します。

パラメータ：domain

例：`xCommand Domain Certs command: csr_delete domain: a.com`

is_cert_set：ドメインに対して証明書が設定されている場合は true を返します。

パラメータ：domain

例：`xCommand Domain Certs command: is_cert_set domain: a.com`

cert_put：証明書と秘密キーをアップロードします。

パラメータ：domain、certpath、keypath

例：`xCommand Domain Certs command: cert_put domain: a.com certpath: /tmp/cert.pem keypath: /tmp/key.pem`

（注）
- 証明書とキーがまだアップロードされていない場合は、両方を指定する必要があります。
- 証明書署名要求が進行中の場合は、証明書のみをアップロードできます。

cert_get：ドメインの証明書を PEM 形式で返します。

パラメータ：domain

例：`xCommand Domain Certs command: cert_get domain: a.com`

cert_delete：ドメインの証明書と秘密キーを削除します。

パラメータ：domain

例：`xCommand Domain Certs command: cert_delete domain: a.com`

default command help："

Certpath：<文字列>

Command：
<domain_list/domain_create/domain_delete/csr_create/csr_get/csr_delete/cert_put/cert_get/cert_delete/is_csr_pending/is_cert_set>

Digestalgorithm：*</sha256/sha384/sha512>*

Domain：<文字列>

Keypath：<文字列>

Keysize：<値>

San：<文字列>

Subjectfields：<文字列>

xCommand Edge SSO Delete Tokens

特定のユーザに対して発行されたすべてのトークンを削除します。

Username(r)：<文字列>

削除するユーザのトークンを指定します。

例：`xCommand Edge SSO Delete Tokens Username: 「APerson」`

xCommand Edge SSO Purge Tokens

すべてのユーザに発行したすべてのトークンを削除します。

例：`xCommand Edge SSO Purge Tokens`

xCommand Edge SSO Status Clear

SSO 要求/応答カウンタを 0 にリセットします。

例：`xCommand Edge SSO Status Clear`

xCommand Feedback Deregister

特定のフィードバック要求を非アクティブ化します。

ID：*<1..3>*

非アクティブ化するフィードバック要求のインデックス。

例：`xCommand Feedback Deregister ID: 1`

xCommand Feedback Register

式で記述されたイベントまたはステータス変更に関する通知をアクティブ化します。通知は、指定された URL に XML 形式で送信されます。最大 15 の式を 3 のフィードバック ID に登録できます。

ID：*<1..3>*

この特定のフィードバック要求の ID。

URL(r): <S: 1, 256>

通知が送信される URL。

Expression.1..15：*<S: 1, 256>*

通知するイベントまたはステータス変更。有効な式は次のとおりです。

```
Status/Ethernet   Event/RegistrationFailure  Event/AuthenticationFailure
Event/    Status/Calls    Event/CallDisconnected
Event/CallFailure   Status/NTP    Status/LDAP
Status/Zones   Event/Bandwidth    Event/Locate
Status/Feedback   Event/CallAttempt   Event/CallConnected
Event/ResourceUsage   Status/ExternalManager
```

例：`xCommand Feedback Register ID: 1 URL: 「http://192.168.0.1/feedback/」 Expression.1: 「Status/Calls」 Expression.2: 「Event/CallAttempt」`

xCommand Find Registration

指定したエイリアスに関連付けられた登録に関する情報を返します。エイリアスはコマンドが発行された Expressway に登録されている必要があります。

Alias(r)：*<S: 1, 60>*

検出する必要があるエイリアス。

例：`xCommand Find Registration Alias: 「john.smith@example.com」`

xCommand Fips

FIPS140-2暗号化モードを設定します。

Command：*<leave/enter/status>*

システムの FIPS140-2 暗号化モードの現在のステータスを入力、維持、または提供します。

例：`xCommand Fips Command: enter`

xCommand Force Config Update

このピアの関連設定を強制的に更新し、クラスタ プライマリの設定と一致するようにします。

このコマンドにはパラメータがありません。

例：`xCommand Force Config Update`

重要 HSM 機能は、Expressway ソフトウェアバージョンに応じて、プレビュー機能のみ使用できます。たとえば、バージョン X12.6 のプレビュー機能です。

Expressway バージョンのリリースノートを確認してから使用する前、またそのステータスがソフトウェアバージョンのプレビューである場合は、**プレビュー機能として実装する場合、およびExpresswayリリースノートに含まれるプレビューの免責事項に従って、そのステータスがソフトウェアバージョンのプレビューである場合に限り 、この 2 つのコマンドを使用してください。**

xCommand HSM Mode Read

Expressway に設定されている現在の HSM モードに戻します。

例：`xCommand HSM Mode Read`

xCommand HSM Mode Write

Expressway の HSM モードを変更します。Expressway で HSM 設定と少なくとも 1 つの HSM モジュールがすでに構成されている場合にのみ使用できます。

Mode：<enabled, disabled>

例：`xCommand HSM Mode Write Mode: enabled`

xCommand HSM Module Add

Expressway 構成に新しい HSM モジュールを追加します。このコマンドを使用する前に、HSM プロバイダーの設定を構成する必要があります。

Ip(r): <S: 0, 1024>

追加する HSM デバイスの IP アドレス。

Port：<1..65535>

nShield HSM との通信に使用されているポート。オプション。デフォルトは 9004 です。

Esn: <S: 0, 1024>

nShield HSM のシリアル番号。必須。

Kneti: <S: 0, 1024>

nShield HSM の検証に使用されるセキュリティハッシュ。必須。

例：`xCommand HSM Module Add Ip: 1.1.1.1 Port: 9004 Esn: abcd-abcd-abcd Kneti: abcd1234abcd1234a`

xCommand HSM Module Remove

Expressway で使用されるモジュールのリストから HSM モジュールを削除します。

Ip(r): <S: 0, 1024>

このコマンドには、すでに設定されている HSM モジュールの IP アドレスが必要です。

例：`xCommand HSM Module Remove Ip: 1.1.1.1`

xCommand HSM Modules

Expressway により使用されるすべての HSM モジュールの一覧を返します。

例：`xCommand HSM Modules`

xCommand HSM Settings Read

現在設定されている HSM 設定を返します。

例：`xCommand HSM settings Read`

xCommand HSM Settings Write

使用する HSM プロバイダーを設定します（サポートされているプロバイダーの詳細については、*Expressway* リリースノートを参照してください。サポートはプレビューベースのみである可能性があります）。

Provider(r): <nShield>

設定する HSM プロバイダー。

Rfsip: <S: 0, 1024>

Thales RFS（リモートファイルシステム）の IP アドレス。HSM を使用する場合は必須です。

Rfsport: <1..65535>

RFS との通信に使用されるポート。HSM を使用する場合は必須です。デフォルト 9004

例：`xCommand HSM Settings Write Provider: 「nShield」 Rfsip: 「1.1.1.1」 Rfsport: 「9004」`

xCommand HTTP Allow List Export

HTTP 許可リストのルールをデータベースから CSV 形式でエクスポートします。

File: <S>

ルールが CSV 形式でエクスポートされるファイルへのパスを指定します。

Deployment： *<S>*

URL と共に使用し、どの導入でこのルールを使用するかを指定します。複数の導入がない場合は必要ありません。複数の導入がある場合、導入を指定しなければ、ルールではデフォルトの導入が使用されます。

xCommand HTTP Allow List Export Test

HTTP 許可リストのテストをデータベースから CSV 形式でエクスポートします。

File: <S>

テストが CSV 形式でエクスポートされるファイルへのパスを指定します。

Deployment： *<S>*

URL と共に使用し、どの導入でこのテストを使用するかを指定します。複数の導入がない場合は必要ありません。複数の導入がある場合、導入を指定しなければ、ルールではデフォルトの導入が使用されます。

xCommand HTTP Allow List Rule Add

HTTP の許可リストに 1 つまたは複数のルールを追加します。少なくとも URL または URLFile を指定する必要があります。

URL(r)： *<S>*

HTTP クライアントにアクセスを許可するリソースの URL を指定します。IPv6 アドレスには RFC 2732 形式を使用する必要があります。

例：`https://[2001:DB8::1]:8443/path` または `https://www.example.com:8443/resource`

URLFile を指定する場合は URL を指定しないでください。

URL にはプロトコル（`http://` または `https://`）とホスト名を含める必要があります。また、URL をより限定的なものにするには、ドメイン、ポート、パスも含めます。URL の一部を省略すると、Expressway はデフォルトを指定します。たとえば `http://hostname` とするとクライアントは `http://hostname.SystemDNSDomain:80` に含まれるすべてにアクセスできます。http のデフォルト ポートは 80、https のデフォルト ポートは 443 です。

URLFile(r)： *<S>*

複数のルールを含むCSV ファイルへのパスを指定します。許可リストは、ファイルの参照を決定しますを参照してください。

URL を指定する場合は URLFile を指定しないでください。

MatchType:<exact/starts-with/startswith/prefix>

URL と共に使用し、ルールが URL に含まれるものに正確に一致するか、またはプレフィックス一致の基本としてそれを使用するかを指定します。指定しない場合、デフォルトで `exact` に設定されます。そのほかの選択肢はすべて同等です。

Deployment：*<S:*「*Your Deployment 1*」/「*Your Deployment 2*」*>*

URL と共に使用し、どの導入でこのルールを使用するかを指定します。複数の導入がない場合は必要ありません。複数の導入がある場合、導入を指定しなければ、ルールではデフォルトの導入が使用されます。

Description: <S: 128>

ルールを説明するテキスト。

HttpMethods:<OPTIONS/GET/HEAD/POST/PUT/DELETE>

このルールで許可する一連のメソッドをカンマで区切って指定します。メソッドを指定しない場合、ルールでは **[設定（Configuration）] > [ユニファイド コミュニケーション（Unified Communications）] > [HTTP 許可リスト（HTTP allow list）] > [編集可能なインバウンド ルール（Editable inbound rules）]** に設定されたデフォルトのメソッドが使用されます。

例：`xCommand HTTP Allow List Rule Add URLfile: 「tmp/rules.csv」`

例 2：`xCommand HTTP Allow List Rule Add URL: 「https://cucm2.example.com:8443/partial/path」 MatchType: starts-with Description: 「https access to read everything below partial/path/ on cucm2.example.com」 HttpMethods: 「OPTIONS,GET」`

xCommand HTTP Allow List Rule Delete

HTTP の許可リストから 1 つまたは複数のルールを削除します。少なくとも URL または URLFile を指定する必要があります。シングル ホストの複数のルールがあればそのほかのパラメータを指定する必要があります。

URL(r)： *<S>*

削除するルールのURLを指定します。

URLFile を指定する場合は URL を指定しないでください。

URL にはプロトコル（`http://` または `https://`）とホスト名を含める必要があります。また、URL をより限定的なものにするには、ドメイン、ポート、パスも含めます。URL の一部を省略すると、Expressway はデフォルトを指定します。たとえば `http://hostname` とすると `http://hostname.SystemDNSDomain:80` のルールを削除します。http のデフォルト ポートは 80、https のデフォルト ポートは 443 です。

URLFile(r)： *<S>*

削除する複数のルールを含む CSV ファイルへのパスを指定します。

URL を指定する場合は URLFile を指定しないでください。

MatchType:<exact/starts-with/startswith/prefix>

URL と共に使用し、ルールが URL に含まれるものに正確に一致するか、またはプレフィックス一致の基本としてそれを使用するかを指定します。指定しない場合、デフォルトで `exact` に設定されます。そのほかの選択肢はすべて同等です。

Deployment： *<S>*

URL と共に使用し、どの導入でこのルールを使用するかを指定します。複数の導入がない場合は必要ありません。複数の導入がある場合、導入を指定しなければ、ルールではデフォルトの導入が使用されます。

Description: <S: 128>

ルールを説明するテキスト。

HttpMethods:<OPTIONS/GET/HEAD/POST/PUT/DELETE>

このルールで許可する一連のメソッドをカンマで区切って指定します。メソッドを指定しない場合、ルールでは **[設定（Configuration）] > [ユニファイドコミュニケーション（Unified Communications）] > [HTTP 許可リスト（HTTP allow list）] > [編集可能なインバウンドルール（Editable inbound rules）]** に設定されたデフォルトのメソッドが使用されます。

例 1：`xCommand HTTP Allow List Rule Delete URLfile: 「tmp/rules.csv」`

例 2：`xCommand HTTP Allow List Rule Delete URL: 「https://cucm2.example.com:8443/partial/path」 MatchType: starts-with Description: 「https access to read everything below partial/path/ on cucm2.example.com」 HttpMethods: 「OPTIONS,GET」`

xCommand HTTP Allow List Rules Test

(Experimental)

（CSV ファイルに定義されている）ルールのリストに対して（CSV ファイルに定義されている）URL のコレクションをテストします。このコマンドを使用して、ルールを適用する前にテストしたり、既存のルールが正常に機能しているかどうかテストしたりできます。

テスト、またはルール、あるいはその両方をCSVファイルとして指定できます。両方を指定すると、Tests CSV ファイル内のテストが、Rules CSV ファイル内にルールに対して実行されます。1 つまたは両方のパラメータを除外する場合、このコマンドは、Expressway に既にあるルールまたはテスト（あるいはその両方）を使用します。（Workflow ルールを確認するには、`xstatus collaborationedge httpallowlist` を使用してください）。

Tests： <*S*>

複数のテストを含むCSVファイルへのパス（たとえば`/tmp/tests.csv`）を指定します。許可リスト テスト ファイル リファレンスを参照してください。

Rules： <*S*>

ユーザがテストする複数のルールを含むCSVファイルへのパスを指定します。たとえば`/tmp/rules.csv`許可リストは、ファイルの参照を決定しますを参照してください。

例：`xCommand HTTP Allow List Rules Test Tests: 「/tmp/tests.csv」 Rules: 「/tmp/rules.csv」`

xCommand HTTP Allow List Test Add

(試験版)

HTTP 許可リストに対してテストする 1 つ以上の URL を追加します。少なくとも URL または URLFile を指定する必要があります。URL を指定する場合は、ExpectedResult を指定する必要があります。

URL(r)： *<S>*

テスト URL を指定します。IPv6 アドレスには RFC 2732 形式を使用する必要があります。

例：`https://[2001:DB8::1]:8443/path` または `https://www.example.com:8443/resource`

URLFile を指定する場合は URL を指定しないでください。

URL にはプロトコル（`http://` または `https://`）とホスト名を含める必要があります。また、URL をより限定的なものにするには、ドメイン、ポート、パスも含めます。URL の一部を省略すると、Expressway はデフォルトを指定します。たとえば `http://hostname` とすると `http://hostname.SystemDNSDomain:80` の URL をテストします。http のデフォルト ポートは 80、https のデフォルト ポートは 443 です。

URLFile(r)： *<S>*

複数のテストを含む CSV ファイルへのパスを指定します。許可リスト テスト ファイル リファレンスを参照してください。

URL を指定する場合は URLFile を指定しないでください。

ExpectedResult （R）:<allow/block>

許可リストに従って URL を許可またはブロックするかどうかを指定するには、URL と共に指定する必要があります。

Deployment： *<S>*

URL と共に使用し、どの導入でこのテストを使用するかを指定します。複数の導入がない場合は必要ありません。複数の導入がある場合は、導入を指定しなければテストはデフォルトの導入を使用します。

Description: <S: 128>

テストを説明するテキスト。

HttpMethod:<OPTIONS/GET/HEAD/POST/PUT/DELETE>

テストする 1 つのメソッドを指定します。メソッドを指定しないと、テストでは GET が使用されます。

例 1：`xCommand HTTP Allow List Test Add URLfile: 「/tmp/tests.csv」`

例 2：`xCommand MRA Allow List Test Add URL:「https://cucm2.example.com:8443/partial/path」 ExpectedResult: block Description: 「https access to write to partial/path/ on cucm2.example.com」 HttpMethod: 「POST」`

xCommand HTTP Allow List Test Delete

(試験版)

HTTP の許可リストから 1 つまたは複数のテスト URL を削除します。少なくとも URL または URLFile を指定する必要があります。URL を指定する場合は、ExpectedResult を指定する必要があります。

URL(r)： *<S>*

削除するテスト URL を指定します。

URLFile を指定する場合は URL を指定しないでください。

URLFile(r)： *<S>*

削除する複数のテストを含む CSV ファイルへのパスを指定します。

URL を指定する場合は URLFile を指定しないでください。

ExpectedResult （R）:<allow/block>

削除するテストで期待される成果を指定します。テストを削除するには、必要。

Deployment： *<S>*

削除するテストを使用している導入を指定します。複数の導入がない場合は必要ありません。

Description: <S: 128>

テストを説明するテキスト。相互に区別できない複数のテストがある場合以外、テストを削除する必要はありません。

HttpMethod:<OPTIONS/GET/HEAD/POST/PUT/DELETE>

削除するテストで使用されているメソッドを指定します。メソッドを省略すると、Expressway はこのコマンドで現在のデフォルトのメソッドを使用します。これは、テストが対応するメソッドで作成されていないと削除が失敗する可能性があることを意味します。

例 1：`xCommand HTTP Allow List Test Delete URLfile: 「/tmp/tests.csv」`

例 2：`xCommand HTTP Allow List Test Delete URL: 「https://cucm2.example.com:8443/partial/path」 ExpectedResult: allow HttpMethod: 「get」`

xCommand HTTP Proxy Jabber CTargets Add

Jabber Guest サーバを設定して Jabber Guest ドメインと関連付けます。

DomainIndex(r)：*<0..200>*

この Jabber Guest サーバが関連付けられたドメインのインデックス。

Host(r)：*<S:1,1024>*

選択したドメインに使用する Jabber Guest サーバの FQDN。これは、非修飾ホスト名または IP アドレスではなく、FQDN である必要があります。

同じドメインに別のプライオリティで代替アドレスを指定できます。

Priority：*<0..9>*

このドメインに対してこのホスト名への接続を試行する順序。ドメインのプライオリティ 1 のすべてのホスト名が最初に試行され、次にプライオリティ 2 のすべてのホスト名という順で実行されます。

例：`xCommand HTTP Proxy Jabber CTargets Add DomainIndex: 2 Host: jabberguest.example.com`

Command HTTP Proxy Jabber CTargets Delete

設定された Jabber Guest サーバを Expressway から削除します。

*Host(r): <S:1,1024>*削除する Jabber Guest サーバの FQDN。

xCommand IMP Server Add

Microsoft SIP Simple メッセージをルーティングする外部のメッセージング サーバを追加します。

IMP(r): <値> *configuration/b2bua/imp/imp*

xCommand IMP Server Delete

外部メッセージング サーバを削除します。

IMP(r): <値> *configuration/b2bua/imp/imp*

xCommand License Smart Deregister

評価期間が満了していなければ、製品は評価モードに戻ります。製品で使用されるライセンス付与がバーチャルアカウントにすぐに戻されて、他の製品インスタンスで使用できるようになります。

xCommand License Smart Register Idtoken: <String>

Smart Software Manager または Smart Software Manager サテライトから生成した製品インスタンス登録トークンを使用して製品を登録します。

xCommand License Smart Renew Auth

Cisco Smart Software Manager によるネットワーク接続の問題が原因で、自動認証ステータスの更新に失敗した場合は、この操作を実行します。

xCommand License Smart Renew ID

Cisco Smart Software Manager のネットワーク接続の問題が原因で自動登録の更新に失敗した場合は、この操作を実行します。

xCommand License Smart Reregister: <String>

次の場合、この操作を実行して製品インスタンスを再登録します。

- この製品インスタンスの以前の登録の試行は、ネットワーク接続の問題のために失敗しました。この問題を解決した後に再登録する必要があります。
- 仮想アカウントにすでに登録されている製品インスタンスを別の仮想アカウントに再登録するには。

xCommand Link Add

新しいリンクを追加して設定します。

LinkName(r)：*<S: 1, 50>*

このリンクに名前を割り当てます。

Node1：*<S: 1, 50>*

このリンクを適用する最初のゾーンまたはサブゾーンを指定します。

Node2：*<S: 1, 50>*

このリンクを適用する 2 番目のゾーンまたはサブゾーンを指定します。

Pipe1：*<S: 1, 50>*

このリンクと関連付ける最初のパイプを指定します。

Pipe2：*<S: 1, 50>*

このリンクと関連付ける 2 番目のパイプを指定します。

例：`xCommand Link Add LinkName: 「Subzone1 to UK」 Node1: 「Subzone1」 Node2: 「UK Sales Office」 Pipe1: 「512Kb ASDL」`

xCommand Link Delete

リンクを削除します。

LinkId(r)：*<1..3000>*

削除するリンクのインデックス。

例：`xCommand Link Delete LinkId: 2`

xCommand Locate

Expressway のロケーション アルゴリズムを実行し、指定したエイリアスによって識別されたエンドポイントをローカルに検索し、指定した「ホップ」の回数内にネイバー上やDNS システムを通じて検出されたシステム上で見つけます。結果はxFeedback を通じて報告されます。そのため、このコマンド（xFeedback register event/locate）を発行する前にこのメカニズムをアクティブにする必要があります。

Alias(r)：*<S: 1, 60>*

見つけるエンドポイントに関連付けられたエイリアス。

HopCount(r)：*<0..255>*

検索で使用するホップ カウント。

Protocol(r)：*<H323/SIP>*

検索を開始するために使用するプロトコル。

SourceZone：*<S: 1, 50>*

検索要求をシミュレートするためのゾーン。デフォルトゾーン（不明なリモートシステム）、ローカル ゾーン（ローカルに登録されたエンドポイント）、またはその他の設定済みのネイバー、トラバーサル クライアントまたはトラバーサル サーバ ゾーンから選択します。

Authenticated：*<Yes/No>*

検索要求を認証済みとして処理するかどうか。

SourceAlias：*<S: 0, 60>*

検索要求に使用する送信元エイリアス。デフォルトは xcom-locate です。

例：`xCommand Locate Alias: 「john.smith@example.com」 HopCount: 15 Protocol: SIP SourceZone: LocalZone Authenticated: Yes SourceAlias: alice@example.com`

xCommand Network Interface

LAN 2 ポートが管理およびコール シグナリングに有効になっているかどうかを制御します。

DualInterfaces(r)：*<enable/disable/status>*

LAN 2 ポートの現在のステータスの設定またはレポート。

例：`xCommand Networkinterface DualInterfaces: enable`

DedicatedManagementInterface: <enable/disable/status>

有効にすると、専用管理インターフェイス（DMI）が管理トラフィックに LAN3 ポートを使用します。（DMI を無効にしようとして、管理サービスがインターフェイスとしてのみ使用している場合、コマンドは失敗します。）

例：`xCommand Network Interface DedicatedManagementInterface: enable`

xCommand Network Limits

機能を制限するまでレートを制御します。

ヘルプを読むには、`xCommand Network Limits ?`を入力します。

xCommand NTP Server Add

システム時刻を同期するときに使用する NTP サーバを追加します。

Address(r)：<値>

追加する NTP サーバの IP アドレスまたは完全修飾ドメイン名（FQDN）。

例：`xCommand NTP Server Add Address: ntp.server.example.com`

xCommand NTP Server Delete

Address(r)：<値>

削除する NTP サーバの IP アドレスまたは完全修飾ドメイン名（FQDN）。

例：`xCommand NTP Server Delete Address: 「ntp.server.example.com」`

xCommand Option Key Add

Expressway に新しいオプション キーを追加します。これらのキーは、Expressway のキャパシティを引き上げるなど、特別な機能を追加するために Expressway に追加されます。詳細については、シスコの担当者にお問い合わせください。

Key(r): <S: 0, 90>

ソフトウェア オプションのオプション キーを指定します。

例：`xCommand Option Key Add Key: 「1X4757T5-1-60BAD5CD」`

xCommand Option Key Delete

Expressway からソフトウェア オプション キーを削除します。

OptionKeyId(r)：*<1..64>*

削除するソフトウェア オプションの ID を指定します。

例：`xCommand Option Key Delete OptionKeyId: 2`

xCommand Ping

特定のホスト システムが接続可能であることを確認します。

Hostname：<値>

接続を試みるホスト システムの IP アドレスまたはホスト名。

例：`xCommand Ping Hostname: 「example.com」`

xCommand Pipe Add

新しいパイプを追加して設定します。

PipeName(r)：*<S: 1, 50>*

このパイプに名前を割り当てます。

TotalMode：*<Unlimited/Limited/NoBandwidth>*

パイプの総帯域幅の制限を制御します。

NoBandwidth：このパイプを使用してコールを発信できません。デフォルトはUnlimitedです。

Total：*<1..100000000>*

このパイプの帯域幅が制限されている場合にパイプで常に使用可能な最大帯域幅（kbps単位）を設定します。デフォルトは500000です。

PerCallMode：*<Unlimited/Limited/NoBandwidth>*

個々のコールの帯域幅制限を制御します。

NoBandwidth：このパイプを使用してコールを発信できません。デフォルトはUnlimitedです。

PerCall：<1..100000000> 制限付きのコール単位モードでは、コールごとに使用可能な最大帯域幅（kbps単位）を設定します。デフォルトは1920です。

例：`xCommand Pipe Add PipeName: 「512k ADSL」 TotalMode: Limited Total: 512 PerCallMode: Limited PerCall: 128`

xCommand Pipe Delete

パイプを削除します。

PipeId(r)：*<1..1000>*

削除するパイプのインデックス。

例：`xCommand Pipe Delete PipeId: 2`

xCommand Policy Service Add

ポリシー サービスを追加します。

Name(r): <S: 0, 50>

このサービス ポリシーに名前を割り当てます。

Description: <S: 0, 64>

自由形式のポリシー サービスの説明。

Protocol：*<HTTP/HTTPS>*

リモートサービスに接続するために使用するプロトコルを指定します。デフォルトはHTTPSです。

Verify：*<On/Off>*

X.509 証明書のチェック、およびこの Expressway とポリシー サービス間の相互認証を制御します。有効になっている場合は、アドレス フィールドで指定したサーバの FQDN または IP アドレスがサーバの X.509 証明書内（サブジェクト共通名またはサブジェクト代替名のどちらかの属性）に含まれている必要があります。デフォルトは On です。

CRLCheck：*<On/Off>*

ポリシー サービスによって提供された証明書の証明書失効リストのチェックを制御します。有効になっている場合は、サーバの X.509 証明書が、その証明書の証明書発行機関の失効リストと照合して確認されます。デフォルトは Off です。

Address：*<S: 0, 128>*

リモート サービスの IP アドレスまたは完全修飾ドメイン名（FQDN）を指定します。

Path：*<S: 0, 255>*

リモート サービスの URL を指定します。

StatusPath：*<S: 0..255>*

リモート サービス ステータスを取得するためのパスを指定します。デフォルトは status です。

UserName: <S: 0, 30>

リモートサービスにログインして照会するためにExpresswayが使用するユーザ名を指定します。

Password: <S: 0, 82>

リモートサービスにログインして照会するためにExpresswayが使用するパスワード。プレーンテキストの最大長は 30 文字です。

DefaultCPL：*<S: 0, 255>*

リモート サービスが使用できない場合に使用する CPL。デフォルトは <reject status='403' reason='Service Unavailable'/> です。

例：`xCommand PolicyServiceAdd Name: 「Conference」 Description: 「Conference service」`

```
Protocol: HTTPS Verify: On CRLCheck: On Address: 「service.example.com」 Path: 「service」
StatusPath: 「status」 UserName: 「user123」 Password: 「password12」3 DefaultCPL: 「<reject
status='403' reason='Service Unavailable'/>」
```

xCommand Policy Service Delete

ポリシー サービスを削除します。

PolicyServiceId(r)：*<1..20>*

削除するポリシー サービスのインデックス。

例：`xCommand Policy Service Delete PolicyServiceId: 1`

xCommand Remote Syslog Add

リモート syslog サーバのアドレスを追加します。

Address(r)：<値>

リモート syslog サーバの IP アドレスまたは FQDN。

Crlcheck：*<On/Off>*

syslog サーバが提供する証明書を証明書失効リスト（CRL）と照合して確認するかどうかを制御します。デフォルト：Off

Format：*<bsd/ietf>*

リモート syslog メッセージが作成される形式。デフォルト：bsd

Loglevel：*<emergency/alert/critical/error/warning/notice/informational/debug>*

この syslog サーバに送信するログ メッセージの最小重大度。デフォルトは informational です。

Mode：*<bsd/ietf/ietf_secure/user_defined>*

syslog サーバにメッセージを送信するときに使用する syslog プロトコル。デフォルトは bsd です。

Port：*<1..65535>*

使用する UDP/TCP 宛先ポート。推奨されるポート：UDP=514 TCP/TLS=6514 デフォルト：514

Transport：*<udp/tcp/tls>*

syslog サーバと通信するときに使用するトランスポートプロトコル。デフォルトは udp です。

例：`xCommand RemoteSyslogAdd Address: 「remote_server.example.com」 Crlcheck: Off Format: bsd Loglevel: warning Mode: bsd Port: 514 Transport: udp`

xCommand Remote Syslog Delete

Address(r)：<値>

削除するリモート syslog サーバの IP アドレスまたは完全修飾ドメイン名（FQDN）。

Port(r)：*<1..65535>*

削除するリモート syslog サーバが使用するポート。

Transport(r)：*<udp/tcp/tls>*

削除するリモート syslog サーバが使用するトランスポート プロトコル。

例：`xCommand RemoteSyslogDelete Address: 「remote_server.example.com」 Port: 514 Transport: udp`

xCommand Remove Registration

Expressway から登録を削除します。

Registration：*<1..3750>*

削除する登録のインデックス。

RegistrationSerialNumber：*<S: 1, 255>*

削除する登録のシリアル番号。

例：`xCommand RemoveRegistration RegistrationSerialNumber: 「a761c4bc-25c9-11b2-a37f-0010f30f521c」`

xCommand Restart

完全なシステム リブートを実行せずに Expressway を再起動します。

このコマンドにはパラメータがありません。

例：`xCommand Restart`

xCommand Route Add

新しい IP ルーティング（スタティック ルートとも呼ぶ）を追加して設定します。

Address(r)：*<S: 1, 39>*

このルートを適用するネットワークを決定するためにプレフィックス長とともに使用する IP アドレスを指定します。デフォルトは 32 です。

PrefixLength(r)：*<1..128>*

このルートを適用するネットワークの決定時に一致する必要がある IP アドレスのビット数を指定します。

Gateway(r)：*<S: 1, 39>*

このルートのゲートウェイの IP アドレスを指定します。

Interface：*<Auto/LAN1/LAN2>*

このルーティングに使用する LAN インターフェイス。*Auto*：使用に最適なインターフェイスを Expressway が選択します。デフォルトは Auto です。

例：`xCommand RouteAdd Address: 「10.13.8.0」 PrefixLength: 32 Gateway: 「192.44.0.1」`

xCommand Route Delete

ルートを削除します。

RouteId(r)：*<1..50>*

削除するルートのインデックス。

例：`xCommand Route Delete RouteId: 1`

xCommand Secure Mode

高度なアカウント セキュリティのオプションを制御します。

Command(r)：*<on/off/status>*

削除するルートのインデックス。

例：`xCommand Secure Mode Command: off`

xCommand Search Rule Add

ゾーンまたはポリシー サービスに検索やコールをルーティングする新しい検索ルールを追加します。

Name(r): <S: 0, 50>

検索ルールの記述名。

ZoneName: <S: 0, 50>

エイリアスが検索ルールと一致するかどうかを照会するゾーンまたはポリシー サービス。

Description: <S: 0, 64>

自由形式の検索ルールの説明。

例：`xCommand SearchRuleAdd Name: 「"DNS lookup」 ZoneName: 「Sales Office" Description」: 「Send query to the DNS zone」`

xCommand Search Rule Delete

検索ルールを削除します。

SearchRuleId(r)：*<1..2000>*

削除する検索ルールのインデックス。

例：`xCommand Search Rule Delete SearchRuleId: 1`

xCommand Trace Path

特定の宛先ホスト システムに送信されたネットワーク パケットが取得したパスを検出します。

Hostname：<値>

パスをトレースするホスト システムの IP アドレスまたはホスト名。

例：`xCommand Tracepath Hostname: 「example.com」`

xCommand Trace Route

特定の宛先ホストシステムに送信されたネットワーク パケットが取得したルートを検出します。また、パスの各ルータの詳細と、各ルータが要求への応答にかかった時間を報告します。

Hostname：<値>

ルートをトレースするホスト システムの IP アドレスまたはホスト名。

例：`xCommand Traceroute Hostname: 「example.com」`

xCommand Transform Add

新しいトランスフォーメーションを追加して設定します。

Pattern(r)：*<S: 1, 60>*

エイリアスを比較するパターンを指定します。

Type：*<Exact/Prefix/Suffix/Regex>*

適用するトランスフォーメーションで、パターン文字列をエイリアスとどのように照合するか。

*[*完全一致（*Exact*）*]*：文字列全体がエイリアスと 1 文字も違うことなく完全に一致する必要があります。

*[*プレフィックス（*Prefix*）*]*：文字列がエイリアスの先頭に表示される必要があります。

Suffix：文字列がエイリアスの末尾に表示される必要があります。

Regex：文字列は正規表現として処理されます。デフォルトは Prefix です。

Behavior：*<Strip/Replace/AddPrefix/AddSuffix>*

エイリアスをどのように変更するかを示します。

Strip：一致しているプレフィックスまたはサフィックスをエイリアスから削除します。

Replace：置換文字列内のテキストでエイリアスの一致している部分を置換します。

AddPrefix：エイリアスの前に置換文字列を追加します。

AddSuffix：エイリアスの後ろに置換文字列を追加します。デフォルトは Strip です。

Replace：*<S: 0, 60>*

選択したパターン動作とともに使用するテキスト文字列。

Priority：*<1..65534>*

指定したトランスフォーメーションにプライオリティを割り当てます。トランスフォーメーションはプライオリティ順に着信メッセージと比較されます。また、プライオリティはトランスフォーメーションごとに一意である必要があります。デフォルトは 1 です。

Description: <S: 0, 64>

自由形式のトランスフォーメーションの説明。

State：*<Enabled/Disabled>*

トランスフォーメーションが有効になっているか、無効になっているかを示します。無効になっているトランスフォーメーションは無視されます。デフォルトは Enabled です。

例：`xCommand TransformAdd Pattern: 「example.net」 Type: suffix Behavior: replace Replace: 「example.com」 Priority: 3 Description: 「Change example.net to example.com」 State: Enabled`

xCommand Transform Delete

トランスフォーメーションを削除します。

TransformId(r)：*<1..100>*

削除されるトランスフォーメーションのインデックス。

例：`xCommand Transform Delete TransformId: 2`

xCommand Ucxn Config Add

Mobile & Remote Access で使用できるように Cisco Unity Connection サーバへのリンクを設定します。

Address(r)：*<S:0,1024>*

Unity Connection パブリッシャの FQDN または IP アドレス。

CertValidationDisabled：*<On/Off>*

CertValidationDisabled がオフ になっている場合、Cisco Unity Connection システムの FQDN または IP アドレスはそのシステムが提示する X.509 証明書内（証明書のサブジェクト共通名またはサブジェクト代替名のいずれか）に含まれている必要があります。証明書自体も有効であり、信頼された認証局によって署名されている必要があります。

DeploymentId：*<1..65535>*

この Unity Connection パブリッシャは、選択した導入環境に関連付けられ、選択した導入環境の他のメンバーのみと通信できます。そのほかの導入環境のメンバーとは通信できません。

Password(r): <S: 1,1024>

Expressway-C が Cisco Unity Connection パブリッシャにアクセスするために使用するパスワード。

Username(r)：*<S:1,1024>*

Unified Connection パブリッシャにアクセスするために Expressway で使用されるユーザ名。たとえば、UC パブリッシャにおけるシステム管理者のロール。

xCommand Ucxn Config Delete

VCS から Cisco Unity Connection サーバへのリンクを削除します。

Address(r)：*<S:0,1024>*

Unity Connection パブリッシャの FQDN または IP アドレス。

xCommand XMPP Delete

IM and Presence サーバの詳細情報を削除します。

Address(r)：<値>

削除するリモート IM and Presence サーバの IP アドレスまたは完全修飾ドメイン名（FQDN）。

例：`xCommand XMPP Delete Address: 「imp_server.example.com」`

xCommand XMPP Discovery

IM and Presence サーバの詳細情報を検出します。

Address(r)：<値>

検出するリモート IM and Presence サーバの IP アドレスまたは完全修飾ドメイン名（FQDN）。

Axlpassword(r)：<パスワード>

IM and Presence パブリッシャへのアクセスに使用するパスワード。

Axlusername(r)：<文字列>

IM and Presenceパブリッシャにアクセスするためのユーザ名。

CertValidationDisabled：*<On/Off>*

IM and Presence パブリッシャが提示した証明書と照合した X.509 証明書の確認を制御します。デフォルトは On です。

例：`xCommand Xmppdiscovery Address: 「imp.example.com」 Axlpassword: 「xyz」 Axlpassword: 「abc」`

xCommand Zone Add

新しいゾーンを追加して設定します。

ZoneName(r)：*<S: 1, 50>*

このゾーンに名前を割り当てます。

Type(r)：*<Neighbor/TraversalClient/TraversalServer/ENUM/DNS>*

ローカル Expressway に関連して、指定したゾーンの特性を決定します。

Neighbor：新しいゾーンはローカル Expressway のネイバーになります。

TraversalClient：ゾーン間にファイアウォールがあり、ローカル Expressway が新しいゾーンのトラバーサル クライアントです。

TraversalServer：ゾーン間にファイアウォールがあり、ローカル Expressway が新しいゾーンのトラバーサル サーバです。

ENUM：ゾーンに ENUM ルックアップで検出されたエンドポイントが含まれます。

DNS：ゾーンに DNS ルックアップで検出されたエンドポイントが含まれます。

例：`xCommand ZoneAdd ZoneName: 「UK Sales Office」 Type: Neighbor`

xCommand Zone Delete

ゾーンを削除します。

ZoneId(r)：*<1..1000>*

削除するゾーンのインデックス。

例：`xCommand Zone Delete ZoneId: 2`

xCommand Zone List

指定したエイリアスの検索で、照会されるゾーンと適用されるトランスフォーメーションのリスト（プライオリティ別にグループ化）を返します。

このコマンドは、既存のシステム設定を変更しません。

Alias(r)：*<S: 1, 60>*

検索するエイリアス。

例：`xCommand ZoneList Alias: 「john.smith@example.com」`

コマンド リファレンス - xStatus

システムの現在のステータスに関する情報を返すには、**xStatus** グループのコマンドを使用します。各 **xStatus** の要素は 1 つ以上のサブ要素に関する情報を返します。

ここでは、現在使用可能な **xStatus** コマンドと、各コマンドによって返される情報を記載します。

既存のステータスに関する情報を取得するには、次のように入力します。

- **xStatus**：すべてのステータス要素の現在のステータスを返す場合。
- **xStatus <element>**：特定の要素とそのすべてのサブ要素の現在のステータスを返す場合
- **xStatus <element> <sub-element>**そのグループのサブ要素の現在のステータスを返す場合。

xStatus コマンドに関する情報を取得するには、次のように入力します。

- **xStatus ?**：**xStatus**コマンドで使用可能なすべての要素のリストを返す場合。

xStatus の要素

現在の xStatus の要素は次のとおりです。

- Alarm
- Alternates
- アプリケーション
- Authentication
- Authzkeys
- B2BUACalls
- B2buapresencerelayservice
- B2buapresencerelayuser
- CDR

- Cafe
- Calls
- Cloud
- Cluster
- CollaborationEdge
- Edgeauth
- Edgecmsserver
- EdgeConfigProvisioning
- Edgeconfigprovisioning
- Edgedomain
- Edgeexternalfqdn
- Edgeauthcodecache
- Edgesso
- ExternalManager
- Fail2ban
- Feedback
- Fips
- Firewall
- Gwtunnels
- H323
- HTTPProxy
- Hardware
- IntrusionProtection
- Iptablesacceptedrule
- Iptablesrule
- License
- Links
- Mediastatistics
- MicrosoftContent
- MicrosoftIMP
- NetworkInterface
- NetworkLimits（試験版）

- Ntpcertificates
- Options
- PhonebookServer
- Pipes
- Policy
- PortUsage
- Registrations
- ResourceUsage
- Resourceusage
- SIP
- SipServiceDomains
- SipServiceZones
- SystemMetrics
- SystemUnit
- TURN
- Teststatus
- Time
- Traversalserverresourceusage
- Tunnels
- Warnings
- XMPP
- Xcps2s
- ゾーン

外部ポリシーの概要

Cisco Expressway（Expressway）には、登録ポリシーとコール ポリシー設定のサポートが組み込まれています。また、より複雑なポリシー決定を実行するためのCPL（コール処理言語）もサポートします。CPLはマシン生成言語として設計されていて、特に直感的ではありません。Expressway は高度なコール ポリシー決定を行うために CPL をロードできますが、複雑な CPL は作成とメンテナンスが困難です。

Expressway外部ポリシー機能では、ポリシー決定を外部システムで行うことができ、実行するアクションの過程で Expressway に指示できます（たとえば、登録を承認するか、コールを分岐するかなど）。コール ポリシーは Expressway とは別に管理でき、Expressway では使用でき

ない機能を実行できます。外部ポリシー サーバは、ポリシー サーバがアクセスできる任意のソースからのデータに基づいてルーティングを決定できます。したがって、企業は特定の要件に基づいてルーティングを決定できます。

外部ポリシー サーバを使用するよう Expressway を設定すると、Expressway は外部ポリシー サーバにサービス要求を送信します（HTTP または HTTPS 経由で）。サービスは Expressway が次に実行する CPL スニペットを含む応答を返信します。

外部ポリシー サーバの使用

外部ポリシー サーバを使用するよう Expressway を設定できる主なエリアは次のとおりです。

- 登録ポリシー：登録を許可または拒否します。
- コール ポリシー（別名、管理ポリシー）：許可、拒否、ルーティング（コールに失敗した場合は、フォールバックで）およびコールの分岐をコントロールします。
- 検索ルール（ポリシーは、特定のダイヤル プランの検索ルールに適用にできます）。

これらのエリアごとに、ポリシー サービスを使用するかしないかを独自に設定できます。ポリシー サービスを使用する場合は、ポリシー サービスによる決定によって、Expressway による決定が置き換えられます（補完ではない）。

ポリシー サービスを設定するときは、次の点を考慮します。

- 最大 3 つの外部ポリシー サーバを指定して、復元力を提供できます（ロード バランシングではない）。
- サービスが使用できない場合に、デフォルト CPL をフォールバックとして Expressway で処理するように設定できます。
- サービスのステータスおよび到達可能性をステータス パスを使用して問い合わせることができます。

ポリシー サービスの詳細（CPL の例を含む）については、『*Expressway* 外部ポリシーの導入ガイド.』を参照してください。

外部ポリシー要求のパラメータ

Expressway は、ポリシー サービスを使用するときに、コール要求または登録要求に関する情報を POST メッセージでそのサービスに送信します。その際、名前と値のペアで構成される一連のパラメータを使用します。サービスは、これらのパラメータと、それ自体のポリシー決定のロジックおよび裏付けとなるデータに基づいて決定を行うことができます（たとえば、LDAP データベースや他の情報源などの外部データ ルックアップを介した登録やコールの発着信を許可するエイリアスのリストなど）。

サービス応答は、CPL が本文に含まれている 200 OK メッセージである必要があります。

次の表に、要求に含まれている可能性があるパラメータのリストを示し、そのパラメータが含まれている要求タイプを √ で示します。また、状況に応じて、許容される値の範囲を示します。

パラメータ名	値	登録ポリシー（**Registration policy**）	検索ルール	コールポリシー
ALIAS		√		
ALLOW_INTERWORKING	TRUE / FALSE		√	√
AUTHENTICATED	TRUE / FALSE		√	√
AUTHENTICATED_SOURCE_ALIAS			√	√
AUTHENTICATION_USERNAME			√	√
CLUSTER_NAME		√	√	√
DESTINATION_ALIAS			√	√
DESTINATION_ALIAS_PARAMS			√	√
GLOBAL_CALLSERIAL_NUMBER	GUID		√	√
LOCAL_CALLSERIAL_NUMBER	GUID		√	√
METHOD	INVITE / ARQ / LRQ / OPTIONS / SETUP / REGISTER	√	√	√
NETWORK_TYPE	IPV4 / IPV6		√	√
POLICY_TYPE	REGISTRATION / SEARCH / ADMIN	√	√	√
PROTOCOL	SIP/H323	√	√	√
REGISTERED_ALIAS			√	√
SOURCE_ADDRESS		√	√	√
SOURCE_IP		√	√	√
SOURCE_PORT		√	√	√

パラメータ名	値	登録ポリシー（Registration policy）	検索ルール	コールポリシー
TRAVERSAL_TYPE	TYPE_[UNDEF / ASSENTSERVER / ASSENTCLIENT / H460SERVER / H460CLIENT / TURNSERVER / TURNCLIENT / ICE]		√	√
UNAUTHENTICATED_ORIGIN			√	√
UTCTIME		√	√	√
ZONE_NAME			√	√

暗号化のサポート

外部ポリシー サーバは TLS および AES-256/AES-128/3DES-168 をサポートする必要があります。

SHA-1 は MAC および Diffie-Hellman/Elliptic Curve Diffie-Hellman キー交換に必要です。Expressway は MD5 をサポートしません。

ポリシー サービスのデフォルト CPL

ポリシー サービスを設定するときは、サービスが使用できない場合に、Expressway が使用するデフォルト **CPL** を指定できます。

登録とコール ポリシーのデフォルト **CPL** は次のとおりです。

<reject status='403' reason='Service Unavailable'/>

これは、要求を拒否します。

検索ルールが使用するポリシー サービスのデフォルト **CPL** は次のとおりです。

<reject status='504' reason='Policy Service Unavailable'/>

これは、その特定の検索ルールによって検索を停止します。

このデフォルト CPL は、ポリシー サーバとの接続が切断された場合に、すべてのコール要求と登録要求が拒否されることを意味します。この動作が不要な場合は、代替のデフォルト CPL を指定することを推奨します。

コールまたは登録が拒否される場合に、どのサービスがなぜ要求を拒否するのかが明確になるように、サービスの各タイプにそれぞれ一意の理由値を使用することを推奨します。

フラッシュ ステータス ワード参照テーブル

フラッシュ ステータス ワードは、NTP サーバの同期の問題を診断するために使用されます。

これは、*ntpq* プログラムの *rv* コマンドで表示されます。これは、以下のように、16進数でコーディングされた多数のビットで構成されています。

コード	タグ	メッセージ	説明
0001	TEST1	pkt_dup	重複パケット
0002	TEST2	pkt_bogus	偽造パケット
0004	TEST3	pkt_unsync	サーバが同期していない
0008	TEST4	pkt_denied	アクセス拒否
0010	TEST5	pkt_auth	認証エラー
0020	TEST6	pkt_stratum	無効な飛びまたはストラタム
0040	TEST7	pkt_header	ヘッダー距離超過
0080	TEST8	pkt_autokey	Autokey シーケンスのエラー
0100	TEST9	pkt_crypto	Autokey プロトコルのエラー
0200	TEST10	peer_stratum	無効なヘッダーまたはストラタム
0400	TEST11	peer_dist	距離のしきい値超過
0800	TEST12	peer_loop	同期ループ
1000	TEST13	peer_unreach	到達不能または選択なし

サポートされている RFC

Expressway は次の RFC をサポートしています。

表 *46 :* サポートされている *RFC*

RFC	説明
791	Internet Protocol（インターネットプロトコル）
1213	『Management Information Base for Network Management of TCP/IP-based internets』
1305	『Network Time Protocol (Version 3) Specification, Implementation and Analysis』
2327	SDP: Session Description Protocol
2460	Internet Protocol, Version 6 (IPv6) Specification (partial, static global addresses only)
2464	『Transmission of IPv6 Packets over Ethernet Networks』
2560	『X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP』
2782	「A DNS RR for specifying the location of services (DNS SRV)」
2833	「RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals」
2915	The Naming Authority Pointer (NAPTR) DNS Resource Record
2976	SIP INFO 方式
3164	『The BSD syslog Protocol』
3261	Session Initiation Protocol
3263	Locating SIP Servers
3264	An Offer/Answer Model with the Session Description Protocol (SDP)
3325	「Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks」
3326	The Reason Header Field for the Session initiation Protocol (SIP)
3265	Session Initiation Protocol (SIP) – Specific Event Notification

RFC	説明
3327	Session Initiation Protocol (SIP) Extension Header Field for Registering Non-Adjacent Contacts
3489	STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)
3515	「The Session Initiation Protocol (SIP) Refer Method」
3550	『RTP: A Transport Protocol for Real-Time Applications』
3581	An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing
3596	『DNS Extensions to Support IP Version 6』
3761	The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)
3880	Call Processing Language (CPL): A Language for User Control of Internet Telephony Services
3891	Replaces header
3892	Referred-by header
3903	Session Initiation Protocol (SIP) Extension for Event State Publication
3944	H.350 Directory Services
3986	Uniform Resource Identifier (URI): Generic Syntax
4028	Session Timers in the Session Initiation Protocol
4213	Basic Transition Mechanisms for IPv6 Hosts and Routers
4291	『IP Version 6 Addressing Architecture』
4443	『Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification』
4480	RPID: Rich Presence Extensions to the Presence Information Data Format (PIDF)

RFC	説明
4787	『Network Address Translation (NAT) Behavioral Requirements for Unicast UDP』
4861	『Neighbor Discovery for IP version 6 (IPv6)』
5095	『Deprecation of Type 0 Routing Headers in IPv6』
5104	Codec Control Messages in the RTP Audio-Visual Profile with Feedback (AVPF): Temporary Maximum Media Stream Bit Rate Request (TMMBR)
5245	Interactive Connectivity Establishment (ICE)
5389	Session Traversal Utilities for NAT (STUN)
5424	The Syslog Protocol
5626	Managing Client-Initiated Connections in the Session Initiation Protocol (SIP)
5627	Obtaining and Using Globally Routable User Agent URIs (GRUUs) in the Session Initiation Protocol (SIP)。この RFC については一部のみをサポートしています。パブリック GRUU はサポートしていますが、一時 GRUU はサポートしていません。
5766	『Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN)』
5806	Diversion Indication in SIP
6156	Traversal Using Relays around NAT (TURN) Extension for IPv6

ソフトウェア バージョン履歴

ここでは、バージョン X8.7 以降のソフトウェア リリースで行われた機能の更新の概要を示します。特定の機能については、該当するソフトウェア バージョンのリリース ノートを参照してください。

ソフトウェア バージョン X 12.5 以降の新機能は、Cisco VCS ではサポートされておらず、Cisco Expressway 製品のみに適用されます。VCS システムの場合、このバージョンはメンテナンスおよびバグ修正のみを目的として VCS に用意されています。

X12.6 機能

表 *47 :* リリース番号別の機能履歴 - *Cisco Expressway* シリーズ

機能/変更	ステータス（Status）
MRA を介したウィスパーコーチング/ウィスパーアナウンスメント	X12.6.2 以降でサポート
カスタマイズ可能なアラームベースの電子メール通知	X12.6.2 以降でサポート
MRA を介したエージェント グリーティング	X12.6.2 以降でサポート
アクティブな MRA 登録数の表示	X12.6.1 以降でサポート
MRA を介したサイレント モニタリング	X12.6.1 以降でサポート
セキュリティ機能の拡張	X12.6 以降でサポート
スマートライセンシング	X12.6 以降でサポート
オプション キーではなく UI 設定による、タイプおよびシリーズの設定	X12.6 以降でサポート
アラームベースの電子メール通知	X12.6 以降でサポート
ハードウェア セキュリティ モジュール（HSM）のサポート	プレビュー
IM&P 用の Android プッシュ通知パブリッシャー	プレビュー（X12.6.2 からはデフォルトで無効）
Cisco Contact Center のヘッドセット機能	プレビュー
MRA での複数のプレゼンスドメイン	プレビュー
Expressway 転送プロキシ	X12.6.2 から削除
Smart Call Home	X12.6.2 から削除
Advanced Media Gateway	X12.6 から削除

X12.5 機能

表 *48 :* リリース番号別の機能履歴 - *Cisco Expressway* シリーズ

機能/変更	X12.5	X12.5.1	X 12.5.2、X 12.5.3	X12.5.4、 X12.5.5、 X12.5.6、 X12.5.9 （X12.5.7 & X12.5.8 の再設定）
「Kariの法律」の直通911番（該当するB2B導入の場合）	該当なし	該当なし	該当なし	X12.5.7以降でサポートされています。
仮想化システム - ESXi認定およびバージョンのサポート	詳細については、仮想マシン設置ガイドの *Cisco Expressway* を参照してください。			
Expressway-EでのACME (Automated Certificate Management Environment) サポート	対応	サポート対象	サポート対象	サポート対象
クラスタ用の単一SAML	対応	サポート対象	サポート対象	サポート対象
複数のMeeting Server会議ブリッジに対するSIPプロキシ - Cisco Meeting Serverロードバランシングのサポート（X12.5では最新になっていません）以前はプレビュー ステータスであったため参照用に含めました)	プレビュー	対応	サポート対象	サポート対象

機能/変更	X12.5	X12.5.1	X 12.5.2、X 12.5.3	X12.5.4、 X12.5.5、 X12.5.6、 X12.5.9 （X12.5.7 & X12.5.8 の再設定）
MRA: ICE 用メディア パス最適化	対応	サポート対象	サポート対象	サポート対象
MRA: スプリット DNS のない改善されたデュアル ネットワーク ドメイン処理	対応	サポート対象	サポート対象	サポート対象
MRA：Unified CM SIP 回線での更新（自己記述）による OAuth	プレビュー	対応	サポート対象	サポート対象
MRA: アクティベーション コードを使用したデバイス オンボーディング	プレビュー	プレビュー	プレビュー	サポート対象
MRA: 暗号化 iX のサポート	プレビュー	プレビュー	プレビュー	サポート対象
MRA: ヘッドセット管理のサポート	プレビュー	プレビュー	プレビュー	サポート対象
X12.5 の新機能ではなく、以前のプレビューステータスによる情報が含まれている機能は次のとおりです。				
Cisco Meeting App アプリでは Expressway-E TURN サーバを使用可能	プレビュー	対応	サポート対象	サポート対象
MRA での複数のプレゼンスドメイン	プレビュー	プレビュー	プレビュー	プレビュー

機能/変更	X12.5	X12.5.1	X 12.5.2、X 12.5.3	X12.5.4、 X12.5.5、 X12.5.6、 X12.5.9 （X12.5.7 & X12.5.8 の再設定）
Smart Call Home	非推奨およびプレビュー	非推奨およびプレビュー	非推奨およびプレビュー	非推奨およびプレビュー

X8.11 の機能

表 *49 :* リリース番号別の機能履歴

機能/変更	X8.11（破棄）	X8.11.1（破棄）	X8.11.2（破棄）	X8.11.3（破棄）	X 8.11.4
アプライアンスのシステムサイズの選択	—	—	—	対応	サポート対象
MRA での Finesse エージェントのサポート	—	—	対応	サポート対象	サポート対象
CE1200 アプライアンス用ソフトウェアの最初のリリース	—	対応	サポート対象	サポート対象	サポート対象
Expressway E へのデバイス登録（SIP および H.323）	対応	サポート対象	サポート対象	サポート対象	サポート対象
Cisco TMS プロビジョニング アクセスに対する変更	対応	サポート対象	サポート対象	サポート対象	サポート対象

機能/変更	X8.11（破棄）	X8.11.1（破棄）	X8.11.2（破棄）	X8.11.3（破棄）	X 8.11.4
Cisco Expressway シリーズでの Multiway 会議	対応	サポート対象	サポート対象	サポート対象	サポート対象
複数の Meeting Server 会議ブリッジに対する SIP プロキシ（Cisco Meeting Server ロード バランシングのサポート）	プレビュー	プレビュー	プレビュー	プレビュー	プレビュー
複数の Meeting Server Web ブリッジに対する Web プロキシ	対応	サポート対象	サポート対象	サポート対象	サポート対象
Cisco Meeting App アプリでは Expressway-E TURN サーバを使用可能	プレビュー	プレビュー	プレビュー	プレビュー	プレビュー
TCP 443 での TURN	対応	サポート対象	サポート対象	サポート対象	サポート対象
大規模 Expressway-E での TURN ポート多重化	対応	サポート対象	サポート対象	サポート対象	サポート対象
保存中のデータのセキュリティ強化	対応	サポート対象	サポート対象	サポート対象	サポート対象
コモン クライテリアの準備	対応	サポート対象	サポート対象	サポート対象	サポート対象

機能/変更	X8.11（破棄）	X8.11.1（破棄）	X8.11.2（破棄）	X8.11.3（破棄）	X 8.11.4
バックアップ時の必須パスワード	対応	サポート対象	サポート対象	サポート対象	サポート対象
カスタム ドメイン検索	対応	サポート対象	サポート対象	サポート対象	サポート対象
MRA での組み込みブリッジの録音（X8.11 での新機能ではありません。以前はプレビュー ステータスであったため参照用に含めました） MRA を介した BiB に関する情報が、*Cisco Expressway* を使用したモバイルおよびリモート アクセス ガイドに記載されました	サポート対象（以前はプレビュー版）	対応	サポート対象	サポート対象	サポート対象
MRA でのアクセス ポリシーのサポート（X8.11 での新機能ではありません。以前はプレビュー ステータスであったため参照用に含めました）	サポート対象（以前はプレビュー版） Cisco Jabber 12.0 が必要です	X8.11 関連	X8.11 関連	X8.11 関連	X8.11 関連

機能/変更	X8.11（破棄）	X8.11.1（破棄）	X8.11.2（破棄）	X8.11.3（破棄）	X 8.11.4
MRA での複数のプレゼンスドメイン（X8.11 での新機能ではありません。以前はプレビュー ステータスであったため参照用に含めました)	プレビュー	プレビュー	プレビュー	プレビュー	プレビュー
ライセンス キーの統合	対応	サポート対象	サポート対象	サポート対象	サポート対象
クラスタから離脱したピアの初期設定へのリセット	対応	サポート対象	サポート対象	サポート対象	サポート対象
Smart Call Home（X8.11 での新機能ではありません。以前はプレビュー ステータスであったため参照用に含めました)	プレビュー	プレビュー	プレビュー	プレビュー	プレビュー
SRV 接続テスト ツール	対応	サポート対象	サポート対象	サポート対象	サポート対象
REST API 拡張	対応	サポート対象	サポート対象	サポート対象	サポート対象

X8.10 の機能

表 *50 :* リリース番号別の機能履歴

機能/変更	X8.10	X 8.10.1	X 8.10.2	X8.10.3（変更なし）	X8.10.4（変更なし）
MRA での組み込みブリッジの録音	サポート対象外	サポート対象外	プレビュー	プレビュー	プレビュー
MRA のプッシュ通知のサポートの強化	プレビュー	対応	サポート対象	サポート対象	サポート対象
MRA の自己記述トークンのサポート（更新を伴う OAuth トークン）	プレビュー	対応	サポート対象	サポート対象	サポート対象
MRA のアクセス制御設定の変更	対応	サポート対象	サポート対象	サポート対象	サポート対象
MRA のアクセス ポリシーのサポート	プレビュー	プレビュー	プレビュー	プレビュー	プレビュー
TLS および暗号スイートのデフォルトへの変更	対応	サポート対象	サポート対象	サポート対象	サポート対象
メディア暗号化の AES-GCM 暗号モード	対応	サポート対象	サポート対象	サポート対象	サポート対象
マルチテナンシーの Cisco XCP ルータの遅延再起動	対応	サポート対象	サポート対象	サポート対象	サポート対象
マルチテナンシーのサーバ名指定	対応	サポート対象	サポート対象	サポート対象	サポート対象

機能/変更	X8.10	X 8.10.1	X 8.10.2	X8.10.3（変更なし）	X8.10.4（変更なし）
セッション識別子のサポート	対応	サポート対象	サポート対象	サポート対象	サポート対象
REST API 拡張	対応	サポート対象	サポート対象	サポート対象	サポート対象
Smart Call Home（X8.10 の新機能ではありません。以前はプレビュー ステータスであったため参照用に含めました)	プレビュー	プレビュー	プレビュー	プレビュー	プレビュー

X8.9 の機能

表 *51* : リリース番号別の機能履歴

機能/変更	X8.9	X8.9.1	X8.9.2
Apple Push Notification サービスの Cisco Jabber for iPhone and iPad へのパススルー	サポート対象外	対応	サポート対象
Cisco Meeting Server 用の Microsoft SIP トラフィックのエッジトラバーサル	対応	サポート対象	サポート対象
Meeting Server の Web プロキシ	サポート対象外	サポート対象外	サポートあり
Skype for Business または Office 365 組織との IM and Presence サービス フェデレーション	プレビュー	対応	サポート対象
H.323 ゲートキーパーとしての Cisco Expressway	対応	サポート対象	サポート対象

機能/変更	X8.9	X8.9.1	X8.9.2
REST API 拡張	対応	サポート対象	サポート対象
MRA での SSO のために Jabber for iPhone and iPad に Safari の使用を許可	対応	サポート対象	サポート対象
MRA エンドポイントの共有回線および複数回線のサポート	プレビュー	対応	サポート対象
Smart Call Home	プレビュー	プレビュー	プレビュー
セキュアなインストール ウィザード	対応	サポート対象	サポート対象
DiffServ コードポイント マーキング	対応	サポート対象	サポート対象
MRA のメンテナンス モード	対応	サポート対象	サポート対象

X8.8 機能

表 *52 :* リリース番号別の機能履歴

機能/変更	X8.8
Expresswayの登録	サポートあり
ビジネス2016年のSkype for BusinessとビジネスモバイルサポートにSkype for Business	サポートあり
Microsoft SIPトラフィック用に仲介国	サポートあり
マルチストリーム サポート	サポートあり
セットアップ ウィザードを選択できます	サポートあり
MRA 許可リストの改善	サポートあり
MRAのリモート設定のAPI	サポートあり
減少VM、CPU予約	サポートあり
最高レベルの環境	サポートあり

機能/変更	X8.8
ソフトウェア パッケージのサインイン	サポートあり
制限されたSSL/TLSサポート	サポートあり

X8.7 機能

表 *53*：リリース番号別の機能履歴

機能/変更	X8.7
Office-Reverse（DVO-R）によるダイヤル	サポートあり
ゲートウェイ クラスタによる Lync 画面の共有	サポートあり
サポートされている Cisco IP Phone を使用したモバイルおよびリモート アクセス	サポートあり
ハイブリッド サービスと Expressway/VCS のブランド変更	サポートあり
VMWare vSphere® 6.0 でのホスティング	サポートあり
syslog 出力のキーワード フィルタ	サポートあり

法的通知

知的財産権

この管理者ガイドおよび関連する製品には、TANDBERG およびそのライセンサーの専有情報が含まれています。製品に関する情報は、下記の**著作権情報**および**特許情報**の項に記載されています。

TANDBERG® は Tandberg ASA に帰属する登録商標です。本書で使用されているその他の商標は、それぞれの所有者に帰属します。本書は、著作権と知的財産権の情報を含めて、すべて複製することができますが、この製品の使用に関連付けられている数量に制限されます。前の文に記載されている制限付き例外を除いて、本書のいかなる部分も、電子的、機械的、複写などの形式や手段を問わず、事前に書面で TANDBERG の許可を得ることなく、複製、検索システムへの保管、または伝送することはできません。

著作権情報

AVC Video のライセンス

各 AVC/H.264 製品に関し、シスコには次の通知を提供する義務があります。

この製品は、AVC 特許ポートフォリオ ライセンスに基づいて消費者の個人的な使用、または報酬を受けないその他の利用方法が認められています。報酬を受けないその他の利用方法とは、（i）AVC標準に従ったビデオのエンコード、（ii）個人的な活動に従事する消費者がエンコードした AVC ビデオ、または AVC ビデオの供給が許されたビデオ プロバイダーから入手した AVC ビデオの復号化、あるいはその両方のことをいいます。その他のいかなる使用に対してもライセンスは供与されず、それが示唆されることもありません。追加情報は MPEG LA, L.L.C.でご確認いただけます。

参照先。http://www.mpegla.com

そのため、サービスプロバイダー、コンテンツプロバイダー、および放送事業者は、AVC/H.264 のエンコーダまたはデコーダ、あるいはその両方の使用については、使用する前に MPEG LA から別途ライセンスを取得する必要があります。

特許情報

この製品は、次の特許の 1 つ以上の対象になっています。

- US7,512,708
- EP1305927
- EP1338127