Cisco Expressway X12.5.4

リリースノート

初版: 2019 年 1 月

最終更新日: 2019 年 8 月

プレビュー機能の免責事項

このリリースの一部の機能は、既知の制限や不完全なソフトウェア依存関係があるため、プレビューステータスのみで提供されます。Cisco は、通知なしでいつでもプレビュー機能を無効にする権利を有します。実稼働環境では、プレビュー機能に依存しないでください。Cisco テクニカルサポートでは、プレビュー機能を使用するお客様に、限定的なサポート (重大度 4) を提供します。

目次

はじめに

変更履歴

表 1 リリースノートの変更履歴

日付	変更内容	理由
2019 年 8 月	*クラスタの単一 SAML での表現*セクションを修正し、自己署名証明書を生成するための不適切な要件をクラスタ全体モードで削除します。	ドキュメントの訂正
2019 年 7 月	メンテナンス リリースの更新。	X12.5.4
2019 年 6 月	*廃止または廃止された機能*セクションで表現を調整します。	ドキュメントの説明
2019 年 5 月	メンテナンス リリースの更新。	X12.5.3
2019 年 4 月	メンテナンス リリースの更新。	X12.5.2
2019 年 4 月	X12.5.1 で修正された、未解決の解決済みのバグ CSCvn49463 (ドメイン内 RMS ライセンス) と CSCvp21304 (非トラバーサルコールカウントおよび Expressway がレジストラの場合はステータス表示なし) について言及します。	ドキュメントの追加
2019 年 2 月	メンテナンス リリースの更新。	X12.5.1

表 1 リリースノートの変更履歴 (続き)

日付	変更内容	理由
2019 年 2 月	ハイブリッド サービス アップグレードの説明は、リリースキーを必要としません。既存の OAuth トークンの認証は、*制限の* Jabber 項目で明確にします。11.1 (2) 以前の Jabber Guest バージョンのライセンスの問題を、*未解決および解決済みの問題*に追加します。	ドキュメントの訂正
2019 年 1 月	初版。	X12.5

サポートされるプラットフォーム

表 2: プラットフォームでサポートされる Expressway ソフトウェア バージョン

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 (UCS C220 M5L にプレインストールされた Expressway)	52E######	X8.11.1 以降。
CE1100‡ (UCS C220 M4L にプレインストールされた Expressway)	52D######	X8.6.1 以降。
CE1000 (UCS C220 M3L にプレインストールされた Expressway)	52B######	X8.1.1 ~ X8.10.x このハードウェアでは X8.10.x より後のバージョンはいずれもサポートされません。
CE500 (UCS C220 M3L にプレインストールされた Expressway)	52C######	X8.1.1 ~ X8.10.x このハードウェアでは X8.10.x より後のバージョンはいずれもサポートされません。

‡ 2018 年 11 月 13 日以降、Cisco の CE1100 アプライアンスを注文することはできません。このプラットフォームのライフサイクルにおけるその他の重要な日付については、販売終了の発表を参照してください。

事前通知: 撤回する CE500 および CE1000 アプライアンスのハードウェアサービスサポート

Cisco は、今後のリリースで Cisco Expressway CE500 および CE1000 アプライアンス ハードウェア プラットフォームのサポートサービスを撤回します。詳細については、販売終了のお知らせを参照してください。

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る特定の共通の表現の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にある
仮想マシンのインストール	Expressway 設置ガイドページの Cisco Expresswa 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 インストールガイド
レジストラ / 単一システムの基本設定	Expressway 設定ガイドページの Cisco Expressway レジストラ展開ガイド
ファイアウォール トラバーサル / ペアリング対象システムの基本設定	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	Cisco Expressway シリーズ メンテナンスおよび 運用ガイドの *ページに用意されている* 『Cisco Expressway 管理者ガイド』 のページに用意されている『Cisco Expressway 有用性ガイド』
クラスタ	*Expressway 設定ガイドのページの*『Cisco Expressway クラスタ作成およびメンテナン導入展開ガイド』
証明書	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』
ポート	Expressway 設定ガイドページの『Cisco Expressway IP Port Usage Configuration Guide』
ユニファイド コミュニケーション	Expressway configuration guide ページの『Mobile and Remote Access Through Cisco Expressway』
Cisco Meeting Server	Expressway 設定ガイドのページの『Cisco Meeting Server with Cisco Expressway Deployment Guide』 Cisco Meeting Server プログラミングガイドのページに用意されている『Cisco Meeting Server API Reference Guide』 その他の Cisco Meeting Server のガイドは、Cisco Meeting Server 設定ガイドの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

表 3 関連ドキュメントへのリンク (続き)

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 設定ガイドのページの *『Cisco Expressway with Microsoft Infrastructure Deployment Guide』* *『Cisco Jabber and Microsoft Skype for Business Infrastructure Configuration Cheatsheet』*が Expressway 設定ガイドのページにある
REST API	*『Cisco Expressway REST API Summary Guide』*が Expressway 設定ガイドの ページにある (API が自己文書化されている場合のみ、高レベルの情報ある)
MultiWay 会議	Expressway 設定ガイドページの『Cisco TelePresence Multiway Deployment Guide』

機能の履歴

重要:ソフトウェア バージョン X12.5 以降の新機能は、Cisco TelePresence Video Communication Server 製品 (VCS) ではサポートされません。これらの新機能は Cisco Expressway シリーズ製品 (Expressway) にのみ適用されます。このソフトウェア 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 4 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	X12.5.2	X12.5.3	X12.5.4
仮想化システム - ESXi 6.7 1 認定	サポート対象外	サポート対象外	サポート対象	サポート対象	サポート対象
仮想化システム - ESXi 6.0、6.5、および 6.7 認定	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象
Expressway-E での ACME (Automated Certificate Management Environment) サポート	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象
クラスタ用の単一 SAML	サポート対象	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 (X12.5 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	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: SIP UPDATE 方式サポートされたセッション更新	サポート対象	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: ICE 用メディア パス最適化	サポート対象	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: 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	サポート対象	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: Unified CM SIP 回線での更新 (自己記述) による OAuth	プレビュー	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: 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	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	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	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	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	プレビュー

表 4 リリース番号別の機能履歴 - Cisco Expressway シリーズ (続き)

機能/変更	X12.5	X12.5.1	X12.5.2	X12.5.3	X12.5.4
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	非推奨およびプレビュー

X12.5.4 の変更

注意: X12.5.4 をインストールする前にお読みください。

バージョン X8.5.3 以前を実行している場合は、2 段階のアップグレードが必要です。この場合は、「アップグレードの前提条件と ソフトウェアの依存関係 (25 ページ)」に記載されているように、このリリースにアップグレードする前に、中間の承認済みバージョンにアップグレードする必要があります。

OAuth 更新 (自己記述トークン) を使用した認証で MRA 経由のチャット/メッセージングサービスを必要とし、IM 及びプレゼンスサービスプレゼンス冗長グループを設定する場合は、Cisco Jabber 12.5 以降が必要です。Expressway のこのリリースでは、12.5 より前のバージョンの Jabber が使用されている場合、このシナリオではユーザログインの障害が発生します。

ソフトウェアの変更と拡張

- リリースキーは、X8.6.x 以降のソフトウェアのシステムをこのリリースにアップグレードするために必要ではありません。たとえば、X8.11.4 から X12.5.4 のようになります。
- 一般的なソフトウェアメンテナンスとバグ修正。
- 未解決および解決済みの問題の検索リスト (19 ページ) は、このメンテナンスリリースで更新されています。
- ユーザマニュアルには、特定の共通の設定手順について、Cisco TAC エンジニアによるビデオへのリンクが含まれるようになりました。

以前にプレビューしたサポート対象の機能

次の機能は、以前の機能リリースではプレビューとして導入され、必要なバージョンの Cisco Unified Communications Manager および Jabber を実行するために Cisco Expressway シリーズで完全にサポートされるようになりました。(この機能は、X12.5.3 から Expressway では実際には完全にサポートされていましたが、その時点では外部ソフトウェアの依存関係が未解決であるため、そのバージョンでは発表されていません)。

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

この機能を使用すると、MRA に準拠したデバイスが、アクティベーションコードを使用して MRA 経由で簡単かつ安全に登録できるようになります。これは**設定 >ユニファイドコミュニケーション>設定**ページの**アクティベーションコードのオンボード**設定を許可するを有効にします。

アクティベーションコードを使用したオンボードには、相互 TLS (mTLS) 認証が必要です。アクティベーションコードを持つオンボードが有効か無効かに応じて、TLS は MRA ポート 8443 で自動的に有効または無効になります。

この機能を使用するには、既存の導入で CUCM を更新する必要があります。

X12.5 よりも前のリリースから既存の Expressway をアップグレードした場合は、この機能を使用する前に、Expressway で現在設定されているユニファイド CM を更新してください。これを行うには、**ユニファイドコミュニケーション > 設定**に移動し、設定済みのすべてのユニファイド CM を選択して、**更新**をクリックします。このタスクは、後で追加するユニファイド CM には必要ありません。

MRA: ヘッドセット管理のサポート

MRA 接続を介した Cisco Unified Communications Manager 管理者は、ユーザのヘッドセット管理をサポートしています。これは、MRA に接続されたユーザが独自のヘッドセット設定を行う必要がなくなったことを意味します。

Expressway は、現在、 */headset/metrics* API をサポートしていません。

MRA: サポートされた暗号化された iX (ActiveControl 用)

MRA の ActiveControl は、暗号化された電話プロファイルですでにサポートされています。この機能により、非セキュアな電話セキュリティプロファイルを持つ MRA ビデオエンドポイントと、Jabber クライアントは ActiveControl をネゴシエートできます。これにより、ユーザは、ビデオ会議で名簿リスト、レイアウト、およびその他の iX 依存 ActiveControl 機能を確認できます。

この機能の設定やインターフェイスの変更はありません。ただし、Expressway をアップグレードした後に、Cisco Unified Communications Manager サーバを再検出する必要がある場合があります。

取り消された機能または廃止された機能

次の機能またはソフトウェアは、**Expressway バージョン x12.5.x** ではサポートされなくなりました。

- Cisco Advanced Media Gateway
- VM 展開の場合、VMware ESXi 仮想ハードウェアバージョン ESXi5.x

次の機能とプレビュー機能は、Expressway バージョン X12.5 以降で廃止され、その**後のリリースではこれらの機能のサポート**が取り消されます。

- サポートされたテレプレゼンス (Movi) の Cisco Jabber Video この項目は、テレプレゼンスの Cisco Jabber Video に関連しており、ユニファイド CM と連携して動作する Cisco Jabber soft クライアントには対応していません (ビデオ通信の Cisco Expressway と連携して動作します)。
- FindMe デバイス/ロケーション プロビジョニングサービス
- Smart Call Home
- Expressway 転送プロキシ

Expressway のソフトウェアバージョン番号

X8.11.4 の後に、他の Cisco 製品のバージョンと適切に適合するように、Expressway のソフトウェアバージョン番号付けが変更されました。Expressway X12.0 のリリースはありません。また、x 8.11.4 と x 12.5. x の 間に他の中間 Expressway リリースはありません。

X12.5.3 の変更

ソフトウェアの変更と拡張

- 一般的なソフトウェアメンテナンスとバグ修正。
- 静的 NAT を TURN にします。以前のリリースでは、Expressway-E の TURN サーバーで静的 NAT が設定された導入環境では、外部ファイアウォールで NAT リフレクションが必要でした。これは、静的 NAT が設定されている場合に、Expressway-E が外部 IP アドレスに着信シグナリングとメディアトラフィックを送信するためです。この状態では、外部ファイアウォール上の NAT リフレクションを「ピン留め」に設定するか、メディアを Expressway に反映する必要があります。一部のファイアウォールでは NAT リフレクションがサポートされていないため、これは推奨される設定ではありません。X12.5.3 から、Expressway TURN サーバーを使用する Expressway 展開で NAT リフレクションの要件を削除することにより、この課題に対処してきました。これで、Expressway は独自のアドレスを検出できるようになりました。

  重要:現在、この変更はスタンドアロンの Expressways にのみ適用され、クラスター化されたシステムには適用されません。
- このメンテナンスリリースでは、19 ページの未解決および解決済みの問題の検索リストが更新されました。

X12.5.2 の変更

その他のソフトウェアの変更と機能拡張

- 一般的なソフトウェアメンテナンスとバグ修正。
- このメンテナンスリリースでは、未解決および解決済みの問題 (19 ページ) の検索リストが更新されました。
- ESXi 6.7 Update 1 バージョンは、ホストの仮想マシンをホストするために正常にテストされました。

- Expressway 小規模仮想マシン (VM) (OVA 仮想アプライアンス)は、Cisco Business Edition (BE) 6000 プラットフォームで動作する小規模な Vm に指定されているのと同じハードウェア要件に従って、VMware ESXi 仮想ハードウェアプラットフォームでサポートされるようになりました。
- X12.5.2 から、バックツーバック ユーザエージェント (B2BUA) は、SIP 応答メッセージの Reason ヘッダーを転送できます。着信 SIP メッセージに複数の Reason ヘッダーが表示される場合、B2BUA は最初の Reason ヘッダーのみを転送することに注意してください。このキャパシティは、ボイスメールに拒否されたコールを転送しない、ユニファイド CM の問題を軽減するために導入されました。Bug 識別子 CSCvk38038 で言及します。

X12.5.1 の変更

ソフトウェアの変更と拡張

- 一般的なソフトウェアメンテナンスとバグ修正。

  注: このメンテナンスリリースで修正されたバグには CSCvp21304 が含まれています。これは、がレジストラーである場合、非トラバーサルコールはカウントされず、コールステータスは web ユーザインターフェイス**概要**ページに表示されません。この問題は、「X8.11.4 リリースノート」の*重要な問題*のリストに含まれており、現在解決されています。
- 以前 (x8.10 から)、Cisco Meeting Server と Microsoft Skype for Business のオンプレミスユーザ間の Expressway を介した企業内/ドメイン内呼び出しは、Expressway-C で RMS ライセンスを消費していました。X12.5.1 以降、これは解決され、これらの呼び出しは MS ライセンスを消費しなくなりました。Bug 識別子 CSCvn49463 で言及します。
- 以前プレビュー状態であったこれらの機能は、Expressway で完全にサポートされるようになりました。
  - Cisco Meeting アプリでは Expressway-E TURN サーバを使用可能
  - Cisco Meeting Server 上のロード バランシング処理のサポート
  - MRA 導入の場合、Cisco Unified Communications Manager SIP 回線での更新 (自己記述) を使用した OAuth。
- このメンテナンスリリースでは、未解決および解決済みの問題 (19 ページ) の検索リストが更新されました。
- これらの変更は、ハイブリッドサービスに対して提供されている型 Sway を使用する導入にのみ影響します。
  - このバージョンの Expressway 管理コネクタソフトウェアの修正は、Expressway 使用してハイブリッドサービスのコネクタをホストする場合に、異なる登録フローに対応します。
  - Cisco Webex ブランドに合わせた表面的なブランディングの修正。

以前にプレビューした X12.5.1 でサポートされている機能

次の機能は、以前の機能リリースではプレビューとして導入されており、Cisco Expressway シリーズの X12.5.1 から完全にサポートされています。

複数の Meeting Server 会議ブリッジに対する SIP プロキシ (Meeting Server ロードバランシングのサポート)

この機能は、Cisco Meeting Server ソフトウェアバージョン 2.3 以前ではサポートされていません。また、 Meeting Server クラスタとのデュアルホーム会議のサポートに関する制限事項が現在存在しています。

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。

Meeting Server ロードバランシングと呼ばれる新しい設定があり、有効にする必要があります (**[構成]> [ゾーン]> [ゾーン]> [ゾーン名]> [詳細]**)。これにより、Cisco Expressway の B2BUA が「2 番目の」Meeting Server からの INVITE を処理して、参加者が接続できるようにします。

エンドポイントが Expressway と Unified CM のどちらに登録されているかに関係なく、Meeting Server のロードバランシングを *オン*に設定することを推奨します。

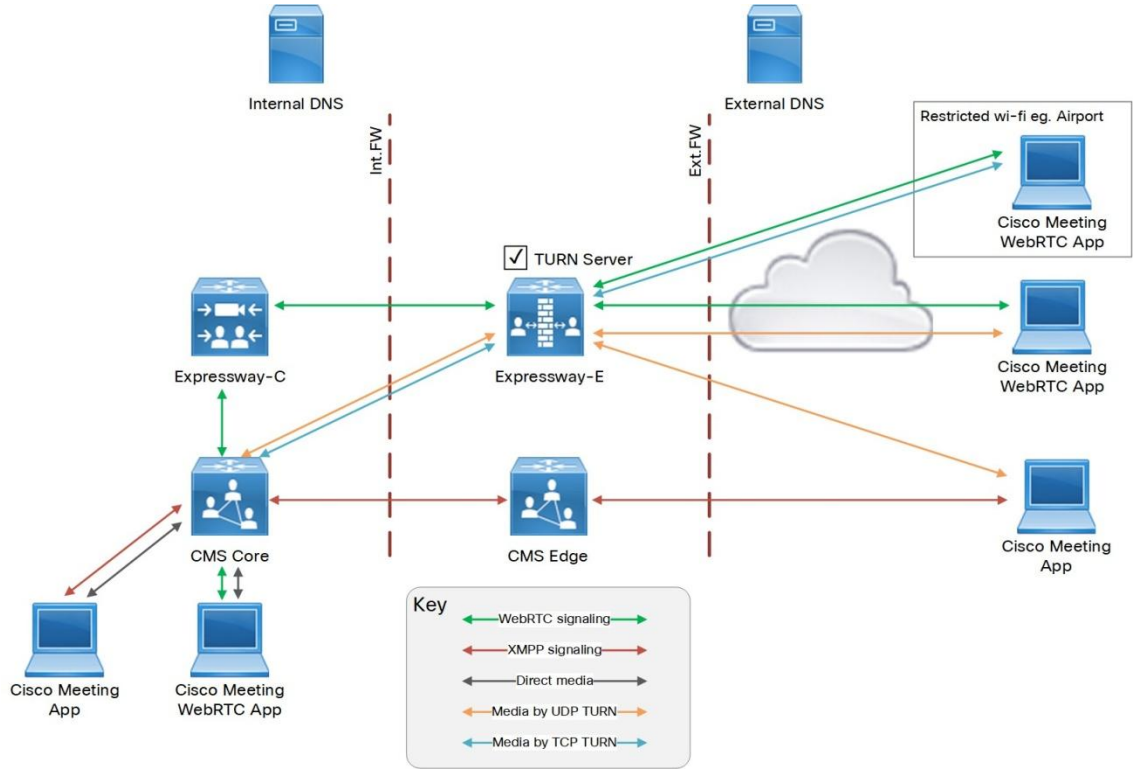
サポート対象およびサポート対象外の機能

- Cisco Expressway は、コール交換を処理するために B2BUA を呼び出します。
- 登録済み H.323 エンドポイントからのコールのロードバランシングもサポートされています。
- さまざまな暗号化モードを、Cisco Expressway との間のコールレッグに適用できます。
- DTLS でセキュアなメディアを使用したコールはサポートされていません。
- Unified CM は、Meeting Server call bridge グループに対して、登録および Cisco Expressway プロキシです。
- Unified CM はレジストラであり、Cisco Expressway は Meeting Server call bridge グループとエンドポイント間の B2BUA です。
- Cisco Expressway はレジストラーであり、B2BUA は関与していません。
- Cisco Expressway はレジストラーであり、B2BUA が関与しています。

Expressway-E TURN サーバを使用した Cisco Meeting App

X8.11 での TURN サーバーの機能強化により、Expressway-E TURN サーバを使用すれば、Expressway-E を使用して WebRTC を Meeting Server ーにプロキシする場合で Cisco Meeting App と Cisco Meeting Server の間のメディアパスの検出およびメディアリレーを行うことができます。

図 1 TURN サーバを共有する Cisco Meeting WebRTC アプリと Cisco Meeting アプリ



この図では、TURN 要求と WebRTC 要求に対して TCP 443 でリッスンするように設定されています。TURN クライアント (Meeting Server Core、Meeting App、および Cisco Meeting WebRTC App) はすべて、TURN 要求に対して UDP 3478 を使用しようとします。

WebRTC App が UDP 3478 へのアウトバウンド接続を確立できない場合は、デフォルトで 443 である TCP オーバーライドポートを使用してメディアリレーを要求します。

Meeting Server の Edge は、Cisco ミーティングアプリケーションの XMPP シグナリングを通過するために引き続き必要です。ただし、Meeting Server Edge サーバの TURN サービスを使用する必要はありません。

MRA: Unified CM SIP 回線での更新 (自己記述) による OAuth

Expressway X12.5 以降のバージョンでは Jabber クライアントに対してのみ、サポートされたユニファイド CM および Jabber のバージョンに従うことによって、Cisco Unified Communications Manager SIP 回線インターフェイスでの更新を伴う OAuth がサポートされます。このオプションが Cisco Unified Communications Manager SIP 回線および Jabber クライアントで有効になっている場合、オンプレミスのクライアントはクライアント証明書ではなく自己記述トークンによって承認されます。

この機能を使用することによって、Certificate Authority Proxy Function (CAPF) を使用せずにセキュアな SIP および SRTP が許可され、MRA を介した ICE および ICE パススルーコールによるエンドツーエンドの暗号化が有効になります。

Cisco Unified Communications Manager SIP 回線インターフェイスで更新して OAuth を有効にする方法

1. Cisco Unified Communications Manager ノードの要件は、次のとおりです。
   a. CLI コマンド**ユーティリティの sip-oauth enable を使用して、**Sip oauth モードを有効にします。
   b. SIP OAuth がデフォルトのポートでリッスンするように設定されているかどうかを確認します (**システム > Cisco のユニファイド CM**)。

      デフォルトのポートは、オンプレミスの場合は 5090、MRA の場合は 5091 です。ポートの競合を回避するには、これらのポートが Cisco Unified Communications Manager 内の既存の **SIP トランク**をリッスンするように設定されていないことを確認します。

SIP 回線で SIP OAuth を有効にするための設定は、便宜上、ここで要約しています。詳細については、Cisco Unified Communications Manager のマニュアルを参照してください。

2. SIP OAuth の Cisco Unified Communications Manager を有効にした後、Cisco Unified Communications Manager ノードを検出するか、または更新します。

   新しい CEOAuth (TLS) ゾーンは、Expressway-C に自動で作成されます。たとえば、 *Ceoauth < Unified CM 名 >*です。オンプレミスエンドポイントから発信された要求を Cisco Unified Communications Manager ノードにプロキシする検索ルールが作成されます。このゾーンは、Cisco Unified Communications Manager が混合モードで設定されているかどうかに関係なく、TLS 接続を使用します。Expressway-C は、信頼を確立するために、ホスト名とサブジェクトの別名 (SAN) の詳細も Cisco Unified Communications Manager クラスタに送信します
3. Jabber クライアントを Cisco Jabber 12.5 以降にアップグレードします。これは、MRA またはオンプレミスクライアントが更新で OAuth を使用して接続するために必要です。
4. 電話セキュリティプロファイル (**システム>セキュリティ>電話セキュリティプロファイル**) で OAuth 認証を有効にし、 Jabber クライアントに電話セキュリティプロファイルを適用します。

X12.5 の新機能

仮想化システム - ESXi 6.0、6.5、および 6.7 認定

この項目は、仮想化システムに適用されます。このリリースでは、ESXi の仮想ハードウェアバージョンをホストするために必要なバージョンの仮想ハードウェアバージョンが変更され、**必要な最小バージョンが ESXi 6.0** (ESXi 5.0 および ESXi 5.5 は、VMware でサポートされなくなりました)。 VMware 次の ESXi バージョンが Expressway X12.5 に対して正常にテストされました:

- ESXi 6.0
- ESXi 6.5 (アップデート 2)
- ESXi 6.7 (ESXi 側チャネル対応スケジューラは、X12.5 ではサポートされていません)

ACME 自動証明書署名

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 Cisco 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。この機能の主な利点は、Expressway-E を識別するサーバ証明書を低コストで生成できることです。したがって、MRA (モバイルおよび Remote Access) などの Expressway-E ベースの導入環境のコストを削減できます。

基礎となる検証メカニズムにより、この機能は MRA 導入環境に最も役立つ可能性があります。ビジネス ツー ビジネス (B2B) アプリケーションでは、ACME 証明書にプライマリ ドメインを含めるのが常に実用的であるとは限りません。

設定プロセスはシンプルです。Cisco Expressway-E で、証明書署名要求 (CSR) を作成するための情報を入力します。これにより、Expressway の ACME クライアントが認証局とやり取りして証明書を要求します。Expressway によってダウンロードされた証明書は、クリックするだけで導入できます。ACME 証明書の有効期間は意図的に短くされているため、この手動による手順を行った後、証明書が期限切れにならないように更新をスケジュールできます。

ACME プロトコルに伴う潜在的なセキュリティ侵害の 1 つとして、Cisco Expressway-E 上のポート 80 でのインバウンド HTTP 接続が必要になることです。このリスクを管理するには Expressway のセキュリティ機能を使用できますが、極めてセキュアな環境では、ACME を無効にして、任意の認証局で従来の CSR 手順を使用することもできます。

Jabber Guest での ACME サポートの制限

現在、Expressway では Jabber Guest 導入環境で ACME をサポートしていません。

クラスタ用の単一 SAML

X12.5 から Cisco Expressway は、IdP との SAML 契約に対して単一のクラスタ全体のメタデータファイルを使用することをサポートしています。以前は、Expressway-C クラスタで 1 つのピアごとにメタデータファイルを生成する必要がありました (たとえば、6 つのメタデータファイルなど)。

6 つのピアがあるクラスタの場合)。これで、クラスタ全体とピア単位の両方のモードがサポートされるようになりました。設定は [オン (on)] です。**設定 > ユニファイドコミュニケーション > 設定 > SAML メタデータ。**

クラスタ全体のモードでは、SAML アグリーメントのプライマリピアからメタデータファイルをエクスポートします。他のピアからエクスポートすることはできません。何らかの理由でプライマリピアを変更した場合は、新しいプライマリピアからメタデータファイルを再度エクスポートしてから、メタデータファイルを IdP に再インポートする必要があります。

MRA: ICE 用メディア パス最適化

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。

Web ユーザインターフェイスの新しい**ステータス > ICE パススルーメトリック**ページには、完了した ICE パススルーコールに関するメトリックデータが表示されます。

詳細情報

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、設定ガイドのページに用意されている『Cisco Expressway を介した *モバイルおよび Remote Access* 導入ガイドページ』を参照してください。

Ice に関する背景情報については、 *『Expressway Maintain and Operate Guides』の『*CISCO EXPRESSWAY Administrator GUIDE 』の *ICE および TURN サービス*について説明しています。

この ICE プロトコルは RFC 5245 で定義されています。

MRA: 改善されたデュアル ネットワーク ドメイン処理

この機能の主要なアプリケーションは、独立した内部および外部ネットワークドメインを使用した MRA 展開用です。*_CISCO UDS* SRV レコードを内部 DNS に追加することは必須ではなくなりました。

X12.5 から、Cisco Expressway シリーズでは、MRA クライアントが外部ドメインを使用して *_collab- Edge* SRV レコード、およびその同じ外部ドメインの*_cisco uds* SRV レコードは、Expressway-C で解決できません。これは通常、外部ドメインでスプリット DNS が利用できないケースです。X12.5 よりも前は、*_cisco* 解決するためのクライアント要件を満たすために、代替サブドメインまたはその他の DNS 回避策を使用する必要があります。

この機能は、MRA に接続されたデバイス用であることに注意してください。*_Cisco uds* レコードは、ローカル/内部 Jabber クライアントには依然として必要です。

制限:このケースは、FQDNs に対してのみ IP アドレスで識別される CUCM ノードではサポートされず、FQDN のみでサポートされます。

また、この機能は、ユーザがオンプレミスで作業している場合でも、MRA 経由の Jabber アクセス*のみ*を許可する MRA 展開のセカンダリケースもサポートします。この場合、必要なドメインは 1 つだけです。通常は、DNS レコードはパブリックに解決できます (ただし、オフプレミス時に MRA アクセスがユーザに許可されていない場合は必須ではありません)。<IM&P ノードアドレス>X12.5 の変更は、 *Cisco Expressway-C または Jabber クライアント*に対して使用可能な_cisco-uds._tcp.<external-domain>の DNS SRV レコードが必要ないことを意味します。

この機能の設定やインターフェイスの変更はありません。Expressway for MRA でネットワークドメインと DNS レコードを設定する方法の詳細については、 *『Expressway Mobile and Remote Access Deployment Guide』を参照してください*。

MRA: セッション更新時の SIP UPDATE メソッドのサポート

Cisco Expressway シリーズでは、X12.5 から、セッションの更新だけを目的とした MRA 接続上の SIP 更新方式がサポートされています。つまり、定期的なセッション更新 (RFC 4028) のセッションタイマーを送受信します。セッションリフレッシュの SIP UPDATE は、企業間展開ではサポートされていません。

注意: 絶対に必要でない限り、この方法を有効にしないでください。Expressway-C と Unified CM の間で re-INVITE (最招待) メソッド ベースのセッション更新に問題がある場合にのみ、セッション更新の SIP UPDATE を有効にします

Expressway は、デフォルトでセッションの更新に re-INVITE メソッドを使用します。SIP UPDATE 方式を使用するには、SIP **シグナリングを通過するゾーン (**設定 > ゾーン > ゾーン) で、**セッション更新の SIP UPDATE** 設定を有効にする必要があります。自動生成されたゾーンの優先方式として SIP アップデートを設定するには、**SIP** を有効にします。

各 Unified CM ノードを検出したときのセッションリフレッシュ設定の更新 (**設定> ユニファイドコミュニケーション > Unified CM サーバ (Unified CM servers)**) 。

MRA を介したセッション更新サポートの SIP UPDATE にはいくつかの制限があります。たとえば、SIP UPDATE メソッド (RFC 3311) に依存する次の機能ではエラーが生じます。

- エンドツーエンドのセキュアコールのために、MRA エンドポイントのセキュリティアイコンを表示するように要求します。
- MRA エンドポイントの名前または番号を表示するための発信者 ID を変更するように要求します。

Expressway X12.5 を使用する Cisco Webex Hybrid Services

- USome Expressway ベースのハイブリッドサービスでは、クラスター内にピアが 1 つしかない場合 (「1 つのクラスター」) でも、コネクターホストをクラスターとして構成する必要があります。Cisco Expressway を工場出荷時の状態にリセットする場合を除き、クラスタリング設定を変更するときは、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ないように注意してください。登録、すべてのコネクタ、および関連するすべての設定が失われます。以前のプレビューの、X12.5.1 でサポートされている 13 ページの機能を参照してください。
- 管理コネクタは、Expressway をアップグレードする前に最新のものにする必要があります。Expressway をアップグレードする前に、Cisco Webex クラウドによってアドバタイズされた管理コネクタのアップグレードを承認して受け入れます。そうでない場合、アップグレード後にコネクタで問題が発生する場合があります。
- Cisco Webex Hybrid Services のコネクタをホストするために使用される Expressway は、Cisco Webex に登録する前に、サポートされている Expressway ソフトウェアバージョンを実行する必要があります。(Expressway 全体をアップグレードする必要なしに、Expressway の管理コネクタコンポーネントのみをアップグレードできます。)

  ハイブリッド コネクタ ホスティングでサポートされる Expressway のバージョンの詳細については、「コネクタ ホストにおける Cisco Webex ハイブリッドサービスのサポート」を参照してください。
- コネクタホスト Expressway を X8.11 から X12.5.x にアップグレードする場合、次の両方の条件が Expressway に適用される場合、リリースキーは*必要ありません*。
  - リリースキー要件を無効にするサービス選択ウィザードを使用して、ハイブリッドサービス用に構成されました。
  - リリースキーはまだありません。つまり、Expressway はコネクタホスト以外として使用されていません。

  これらの条件は、ほとんどのハイブリッドサービス展開で満たされています。ただし、展開で Expressway コネクタホストにリリースキーが必要な場合、このリリースにアップグレードするには新しいリリースキーが必要です。

REST API 拡張

リモート構成を簡素化するために、REST API を引き続き拡張します。新しい機能を追加するときに、構成、コマンド、およびステータス情報への REST API アクセスを追加しますが、REST API を以前のバージョンで導入された機能に選択的に改造しています。

たとえば、Cisco Prime Collaboration Provisioning などのサードパーティシステムは、API を使用して Expressway の次の機能/サービスを制御できます。

構成 API	API がバージョンで導入されました
クラスタ	X8.11
Smart Call Home	X8.11
Microsoft 製品との相互運用性	X8.11
B2BUA TURN サーバ	X8.10
admin アカウント	X8.10

構成 API	API がバージョンで導入されました
ファイアウォールルール	X8.10
SIP 設定	X8.10
サーバ名の識別用のドメイン証明書	X8.10
MRA 拡張機能	X8.9
ビジネスツービジネス コール	X8.9
MRA	X8.8

API は、RESTful API モデリング言語 (RAML) を使用して自己文書化されています。システムの RAML 定義にアクセスするには、 **https://<*ip address*>/api/provisioning/raml** を使用します。Api へのアクセス方法と使用方法の高度な概要については、『Expressway 設置ガイド』 ページの 『Cisco Expressway REST API 要約ガイド』で利用できます。

以前のリリースを含むすべてのプレビュー機能

次の機能はプレビューステータスのみです。これらの一部は、当初は X8.11 以前のバージョンのプレビュー機能として導入されました。

- MRA を介した複数のプレゼンスドメイン/複数の IM アドレスドメイン
- (現在廃止) Smart Call Home

(プレビュー - 現在廃止) Smart Call Home

この機能は Expressway X12.5 から廃止され、**サポートは今後のリリースで廃止されます。**

Smart Call Home は、Expressway の組み込みサポート機能です。プロアクティブな診断とリアルタイムのアラートを提供し、高いネットワーク可用性と運用効率の向上を実現します。Smart Call Home は、スケジュールベースの通知とイベントベースの通知をユーザに送信します。

- スケジュールベースの通知: インベントリ、テレメトリー、および設定に関するメッセージです。これらのメッセージを使用してデバイス レポートを生成し、障害の傾向を特定することでハードウェアとソフトウェアの品質を向上させます。これらの通知は、毎月 1 日に送信されます。
- イベントベースの通知: Expressway ですでにサポートされているアドホック イベントです (アラームや ACR など) 。これらの通知は、イベントが発生すると Smart Call Home サーバにポストされます。

注: web ユーザインターフェイスには、Smart Call Home を使用した SMTP のオプションが含まれていますが、現時点では、この機能は、通常はこのように実装されていません。

(プレビュー) 複数のプレゼンスドメイン/ MRA 上の複数の IM アドレスドメイン

この機能はプレビューステータスにあります。

Jabber 10.6 以降は、ユーザーが複数のドメインに編成されているインフラストラクチャ、またはサブドメインを持つドメイン (IM および Presence サービス 10.0.x 以降の対象) に展開できます。

未解決および解決済みの問題

バグ検索ツール

以下のリンクに従って、このリリースで未解決および解決済みの問題に関する最新情報をお読みください。

- 変更された日付順に並べられたすべての未解決の問題 (最新のものが最初)
- X12.5.4 によって解決された問題
- X12.5.3 によって解決された問題
- X12.5.2 によって解決された問題
- X12.5.1 によって解決された問題
- X12.5 によって解決された問題

このバージョンの注目すべき問題

シングル NIC 展開での Jabber Guest コールのライセンスの問題

現在、ソフトウェアには、単一の NIC 導入での Jabber Guest コールに対する予期しないリッチメディアセッション (RMS) ライセンスの動作が存在します。

- Expressway-E は、Jabber ゲスト呼び出しごとに 1 つの RMS ライセンスをカウントする必要がありますが、カウントされません。この問題により、サーバが複数のコールを処理している場合でも使用率が低くなるため、サーバの負荷について混乱が生じる可能性があります。Bug ID CSCva36208 はで特定されています。
- **この問題は、リリース 11.1 (2)**よりも前の Jabber Guest バージョンを持つユーザにのみ適用されます。 11.1 (2) 以降のユーザは影響を受けません。影響を受けるケースでは、Jabber Guest コールごとに、Cisco Expressway-E で RMS ライセンスを消費することがありますが、実際には RMS ライセンスが Cisco Expressway-**で消費されます。**C. この問題は、X8.10 および Bug ID CSCvf34525 で特定されています。影響を受けた場合は、Cisco の担当者にお問い合わせください。

デュアル NIC Jabber Guest の導入を推奨します。

制限事項

一部の表現機能はプレビューであるか、外部の依存関係があります。

重要:新しい表現機能を可能な限り迅速に提供することを目的としています。まだ利用できない他の Cisco 製品の更新が必要な場合や、既知の問題や制限が一部の機能の展開に影響するため、新機能が公式にサポートされない場合があります。ユーザがこの機能を使用してなおメリットを享受できる場合は、リリースノートで「プレビュー」としてマークしています。プレビュー機能は使用できます**が、実稼働環境では使用しないようにする必要があります (**「機能の免責事項 (1 ページ) 」を参照してください)。場合によっては、この機能を使用しないことを推奨します。これは、それ以降の更新が、その他の製品に対して行われるまでです。

このリリースのプレビューステータスでのみ提供される機能は、これらのノートの「 機能の履歴 (表) 」に記載されています。

サポートされていない機能

- DTLS は Expressway によって終了されません。メディアを保護するための DTLS はサポートされていません。SRTP は、コールを保護するために使用されます。DTLS コールを発信しようとする試みは失敗します。DTLS プロトコルは SDP に挿入されますが、暗号化された iX プロトコルを通過する場合に限ります。
- X12.5 から、Expressway は、RFC 4028 で指定されているように、セッションの更新のみを目的として、MRA 接続を介した SIP UPDATE のサポートを限定的に提供します。ただし、この機能を使用するための特別な要件がない場合は、この設定をオンにしないでください。SIP UPDATE のその他の使用はサポートされておらず、このメソッドに依存する機能は期待どおりに機能しません。
- 音声コールは、状況によってはビデオコールとしてライセンスされる場合があります。厳密な音声のみのコールは、ビデオ通話よりも少ないライセンスを消費します。ただし、音声通話には、ActiveControl を有効にする iX チャネルなどの非オーディオチャネルが含まれている場合、ライセンスのためにビデオ通話として扱われます。

モバイルおよび Remote Access に関する制限事項

重要: Mobile & Remote Access (mra) に対して使用する場合は、サポートされていないさまざまな機能と制限が現在存在します。MRA と連動しないことがわかっている主要なサポートされていない機能のリストは、『 *Cisco Expressway* guide 』に記載されている、「サポートされている*主要な機能およびサポートされていないモバイルおよび Remote Access*」のキーで詳しく説明します。

8800 シリーズと 7800 シリーズの最近の一部の Cisco IP 電話では、現在 MRA がサポートされていません。MRA をサポートしている 7800/8800 シリーズの電話機の詳細については、『Cisco Expressway による*モバイルおよび Remote Access* ガイド』の*前提条件の*項を参照するか、Cisco の担当者にお問い合わせください。

MRA を介したセッション更新サポートの SIP UPDATE にはいくつかの制限があります。たとえば、SIP UPDATE メソッド (RFC 3311) に依存する次の機能ではエラーが生じます。

- エンドツーエンドのセキュアコールのために、MRA エンドポイントのセキュリティアイコンを表示するように要求します。
- MRA エンドポイントの名前または番号を表示するための発信者 ID を変更するように要求します。

クラスタ内のピアを追加または削除するときのスプリアスアラーム

新しいピアがクラスタに追加されると、システムは、クラスタが実際に正しく形成されている場合でも、複数の 20021 アラーム (*クラスタ通信の失敗:... を確立できません) を発生させる可能性があります。*アラームは、クラスタ内の既存のピアに表示されます。通常、不要なアラームは、新しいピアが正常に追加された時点から 5 分以上経過した後に低下します。

これらのアラームは、ピアがクラスタから削除された場合にも発生します。これは一般に、ピアを削除する場合に有効なアラーム動作です。ただし、ピアを追加する場合と同様に、アラームが 5 分以上低下することはありません。

CE1200 アプライアンス

- 特定のシナリオでは、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 アプライアンスへのフルアプライアンスへの復元で問題が発生します。詳細については、これらのリリースノートの後半のアップグレード手順に記載されています。これには、各問題の解決方法が含まれます。
  - 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。
  - 誤ったバナーが Web ユーザインターフェイスに表示されることがあります。
- CE1200 アプライアンスには、最小ソフトウェアバージョン X8.11.1 以降が必要です。システムは以前のバージョンのソフトウェアのダウングレードを防ぐことはできませんが、Cisco では以前のバージョンのアプライアンスをサポートしていません。
- Expressway を使用すると、CLI を使用して Traversal Server または CE1200 Sway シリーズキーを追加または削除できますが、実際には、これらのキーはアプライアンスの場合には効果がありません。サービスセットアップウィザード (タイプ設定) は、アプライアンスが Expressway-C または Expressway-E のどちらであるかを管理し、以前のアプライアンスの場合の Traversal Server キーの管理ではありません。

仮想システム

物理的な Expressway アプライアンスの場合、Advanced Networking オプションを使用すると、設定された各イーサネットポートで速度と Duplex mode を設定できます。ただし、仮想マシンベースの Expressway システムに対して、イーサネット ポートごとに速度を設定することはできません。

また、仮想マシンベースのシステムでは、実際の物理的 NIC 速度に関係なく、Expressway とイーサネットネットワーク間の接続速度が常に 10000 Mb/s と表示されます。これは、物理 NIC から実際の速度を取得できないという仮想マシンの制限が原因です。

Gbps の NIC 逆多重化ポートを搭載した中規模アプライアンス

1 Gbps の NIC を使用する中規模システムを X8.10 以降に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 36000 ~ 36011 はファイアウォールで開かれないため、Expressway-E はコールをドロップします。X8.11.3 から、[システム]> [管理設定]**ページ (展開構成**リストから *中*を選択) を使用して、システムサイズを手動で中に戻すことができます。この問題が X8.11.3 よりも前のリリースで発生した場合、回避策はファイアウォール上の大規模システムのデフォルトの逆多重化ポートを開くことです。

言語パック

Expressway web ユーザインターフェイスを変換すると、新しい表現言語パックを X8.10.3 から入手できます。古い言語パックは、x8.10 では動作しません。ソフトウェア (または x8.9.)。パックをインストールまたは更新する手順については、*Cisco Expressway 管理者ガイド*を参照してください。

オプションキーは 65 キー以下のみに対して有効

65 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、それらは Expressway Web インターフェイスに通常どおり表示されます (**メンテナンス > オプションキー)**。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。Bug ID CSCvf78728 はで特定されています。

Xmpp フェデレーション-IM & P ノード障害の動作

XMPP 外部フェデレーションを使用する場合、停止後に IM および Presence サービスノードが別のノードにフェールオーバーしても、影響を受けるユーザーは他のノードに動的に移動されないことに注意してください。Expressway はこの機能をサポートしておらず、テストされていません。

Cisco Webex Calling が Dual-NIC Expressway で失敗する場合

この問題は、Dual-NIC Expressway-E を使用して、Expressway を展開する場合に適用されます。同じ (重複する) スタティックルートが外部インターフェイスと Expressway-C を持つインターフェイスの両方に適用される場合、Cisco Webex Calling 要求は失敗する可能性があります。 これは、Webex INVITES を非 NAT として扱い、SIP Via ヘッダーからソースアドレスを直接抽出する現在の Expressway-E ルーティング動作によるものです。

ルートが重複するリスクとこの問題が発生するリスクを最小限に抑えるため、スタティックルートをできるだけ具体的にすることをお勧めします。

デュアルホーム会議-SIP メッセージサイズ

Microsoft 側で起動された AVMCU で Expressway および Meeting Server を介して を使用してデュアルホーム会議を使用する場合は、最大 SIP メッセージサイズを 32768 バイト (デフォルト) 以上に設定する必要があります。大規模な会議 (つまり、約 9 人以上の参加者から) に対して、より大きな値が必要になる可能性があります。**設定 > プロトコル >[SIP] で SIP 最大サイズを介して定義されます。**

Expressway および Cisco Meeting Server を使用したドメイン内 Microsoft Interop

Microsoft の相互運用性のために Meeting Server を使用する場合、現時点では次のイントラドメイン/expressway シナリオに制限が適用されます。

***単一のドメイン**と、**Microsoft フロントエンドサーバに直接接続された Expressway-E** がある設定で、個別の Microsoft および標準ベースの SIP ネットワークを展開します。(サブネットワーク間で内部ファイアウォールを使用するため、またはその他の理由で使用します) 。たとえば、1 つの (サブ) ネットワーク内の Cisco Unified Call Manager と、同じドメイン内の 2 番目 (サブ) ネットワーク内の Microsoft。*

この場合、通常、2 つのネットワーク間の Microsoft の相互運用性はサポートされていません。また、Meeting Server と Microsoft 間のコールは拒否されます。

回避策

Expressway-E を介在させずにドメイン内ネットワークを展開できない場合 (Meeting Server <> Expressway-C <> Microsoft を構成することはできません) 、回避策は Expressway-E を使用して各サブネットに Expressway-C を展開し、Expressway-E がそれらの間を移動することです。具体的な場所は次のとおりです。

Meeting Server <> Expressway-C <> ファイアウォール <> Expressway-E <> ファイアウォール <> Expressway-C <> Microsoft

チェーン化される Expressway-Es によるライセンスの動作

Expressway-E をチェーンファイアウォールを通過する場合 (X8.10 以降) 、このライセンスの動作に注意してください。

- ファイアウォールを介して Cisco Webex cloud に接続すると、トラバーサルクライアントロールでトラバーサルゾーンを設定する*追加の* Expressway-E の各ユーザが、(通話ごとに) リッチメディアセッションライセンスを消費します。以前と同様に、元の Expressway-C と Expressway-E のペアはライセンスを消費しません。
- ファイアウォールを介してサードパーティの組織 (ビジネスツービジネスコール) に接続すると、チェーン内の*すべて*のライン sway (トラバーサルペアの元のものを含む) は、リッチメディアセッションライセンス (コールごと) を消費します。以前と同様に、元の Expressway-C はライセンスを消費しません。

Jabber を使用した OAuth トークン認証

Cisco Unified Communications Manager に設定されている MRA アクセスポリシー設定に関係なく、Jabber ユーザが 11.9 (トークン認証サポートなし) より前のバージョンを実行しており、Expressway がトークン以外の認証方法を許可するように構成されている場合、非トークン認証方式を許可するように設定されています。これらのユーザは、ユーザ名とパスワード、または従来のシングルサインオンによって認証できます。

注:展開で MRA ポリシーを厳密に適用することが選択されている場合、自己記述トークン(「OAuth with Refresh」)をサポートしていないエンドポイントで MRA を使用することはできません。これには、Cisco TelePresence TC と CE エンドポイント、およびアクティベーションコード機能をオンボーディングしていない Cisco IP 電話 7800 または 8800 シリーズのエンドポイントが含まれます。

Expressway 転送プロキシ

注意: 組み込み型 Expressway 転送プロキシは使用しないでください。この機能は後続の Expressway リリースから廃止され、サポートは今後のリリースで廃止されます。転送プロキシを導入する必要がある場合は、代わりに適切なサードパーティの HTTPS プロキシを使用する必要があります。

TURN サーバ

現在、TCP 443 TURN サービスと TURN ポートの多重化は、CLI ではサポートされていません。これらの機能を有効にするには、Expressway web インターフェイスを使用します (**設定 > トラバーサル > TURN**)。

相互運用性

テスト結果

この製品の相互運用性テストの結果は、http://www.cisco.com/go/tp-interop に投稿され、にその他の Cisco テレプレゼンス製品の相互運用性テストの結果もここで確認できます。

注目すべき相互運用性の考慮事項

X8.7.x (以前のバージョン) は、Cisco Unified Communications Manager IM and Presence Service 11.5 (1) 以降と相互運用できません。これは、IM および Presence サービスのそのバージョンでの意図的な変更に起因し、Expressway X8.8 以降で対応する変更があります。

継続的な相互運用性を確保するには、IM および Presence サービスシステムをアップグレードする*前に*、このシステムをアップグレードする必要があります。この問題の症状としては、次のような Expressway のエラーが挙げられます。

***<IM&P node address>*と通信できませんでした。AXL クエリ HTTP エラー "'HTTPError:500'"**

ともに実行できるのはどのような Expressway Services ですか。

*Cisco Expressway シリーズの保守および操作ガイド*ページの Cisco Expressway 管理者ガイドでは、同じ Expressway システムまたはクラスタ上で共存することができます。表「*同時にホストできるサービス*」を「概要」セクションに表示する。たとえば、MRA が CMR Cloud と共存できるかどうかを知る必要がある場合 (これは可能)、表によってわかります。

X12.5.4 へのアップグレード

前提条件とソフトウェアの依存関係

注意: このセクションには、アップグレード後にシステムが正常に動作しなくなる可能性のある問題に関する重要な情報が含まれています。アップグレードする前に、このセクションを確認し、導入に適用されるタスクを完了してください。

X8.5.3 以前のデュアル Expressway システムには 2 段階のアップグレードが必要

バージョン X8.6 **よりも前のソフトウェアを実行しているシステムをアップグレードする場合は、まず中間リリースにアップグレードしてから、X12.5.4 ソフトウェア**をインストールする必要があります (この要件は、X8.11.x 以降のバージョンへのすべてのアップグレードに適用されます)。既存のシステムバージョンによっては、ファイルサイズの問題**が原因でアップグレードが失敗し、後のバージョンでデータベース形式が変更されたために**データが破損するリスクがあります。中間リリースとして X8.8.2 にアップグレードすることをお勧めします。ただし、別のバージョンを使用する特定の理由がある場合は、この X12.5.4 ソフトウェアをインストールする前に、X8.6 と X8.8.2 を含む任意のバージョンにアップグレードできます。

- バージョン X8.8.2 のリリースノートは、次のから入手できます。
  https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-release-notes-list.html

すべての導入の手順:

ダウングレードはサポートされません。新しいバージョンを実行しているシステムに以前のバージョンの Expressway バージョンをインストールしないでください。これを行うと、システム設定は保持されません。

X8.11 から、アップグレード後にシステムが再起動すると、新しい暗号化メカニズムが使用されます。これは、そのリリースで導入された、ソフトウェアインストールごとの一意の信頼のあるルートに起因します。

X8.8 から、ソフトウェアは以前のバージョンよりも安全性が高くなります。アップグレードにより、導入が期待どおりに機能しなくなる可能性があります。また、X8.8 以降にアップグレードする前に、次の環境上の問題を確認する必要があります。

- 証明書: 証明書の検証が X8.8 で強化されました。
  - TLS 接続を検証するために、アップグレードの前後に(**メンテナンス > セキュリティ > セキュアトラバーサルテスト**)のセキュアなトラバーサルテストを試行てください。
  - ユニファイドコミュニケーションノードは、Expressway-C の信頼リストにある CA によって発行された有効な証明書を使用していますか。
  - 自己署名証明書を使用する場合、それらは一意ですか。Expressway の信頼できる CA リストには、展開内のすべてのノードの自己署名証明書が含まれていますか。
  - Expressway の信頼できる CA リスト内のすべてのエントリは一意ですか。重複をなくす必要があります。
  - 他のインフラストラクチャへの接続で TLS 検証が有効になっている場合 (常にユニファイド コミュニケーション トラバーサルゾーンの場合は常にデフォルトで、ユニファイド コミュニケーション ノードへのゾーンの場合はオプション)、ホストの証明書の CN または SAN フィールドにホスト名が存在することを確認する必要があります。失敗した展開を解決するための簡単な方法であっても、TLS 検証モードを無効にすることは推奨されません。
- DNS エントリ: Expressway がやり取りするすべてのインフラストラクチャ システムに対して、DNS の前方および後方ルックアップがありますか？バージョン X8.8 以降では、Expressway-E システムに対して順方向および逆方向の DNS エントリを作成する必要があります。これにより、システムに TLS 接続を行うシステムが FQDN を解決し、証明書を検証できます。

  Expressway がシステムのホスト名と IP アドレスを解決できない場合は、複雑な展開 (例、MRA) は、アップグレード後に期待どおりに動作を停止する可能性があります。
- クラスタピア: 有効な証明書があるかどうかを確認します。デフォルトの証明書を使用している場合は、(少なくとも) 内部生成された証明書に置き換えるか、またはピアの信頼リストを発行 CA で更新する必要があります。X8.8 から、クラスタリング通信は、IPSec の代わりにピア間の TLS 接続を使用します。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。

CE1200 アプライアンスを使用する導入

CE1100 以前のアプライアンスバックアップから Expressway-E を CE1200 アプライアンスに復元する場合、CE1200 アプライアンスは Expressway-C として復元する場合があります。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次の手順を実行します。

1. サービスセットアップウィザードを実行し、タイプを Expressway-E に変更します。
2. ウィザードを完了します。

また、CE1100 バックアップから Expressway-E 構成を CE1200 アプライアンスに復元すると、CE1200 アプライアンスは、Expressway-E として復元します (予想どおり) 。ただし、CE1100 タイプがどのように設定されているかによっては、web インターフェイスバナーが [入力 Sway-C] として表示されることがあります。この問題が発生した場合は、サービスセットアップウィザード (**ステータス > の概要**ページ)に移動し、**タイプ**を *Expressway-E* に変更してから、システムを再起動します。この問題が発生するのは、タイプを Expressway-E に変更するために CE1100 でトラバーサルサーバのオプションキーが使用されている場合だけです。これは、サービスセットアップウィザードを使用した場合には発生しません。

MRA を使用する導入

このセクションは、Expressway for MRA (Cisco Unified Communications 製品を使用したモバイルおよびリモートアクセス) を使用する場合にのみ適用されます。

- ユニファイド コミュニケーション インフラストラクチャ ソフトウェアの最小バージョンの適用: 一部のバージョンのユニファイド CM IM および Presence サービスと Cisco Unity Connection には、CiscoSSL アップデートにパッチが適用されています。Expressway をアップグレードする前に、Expressway MRA　導入ガイドに記載されている最小バージョンを実行していることを確認します (Expressway　設定ガイドページの「Cisco Expressway を介した *モバイルおよび Remote Access*」を参照してください) 。

  IM および Presence サービス 11.5 は例外です。*IM および Presence サービスを 11.5 にアップグレード*する前に、Expressway を x8.8 以降にアップグレードする必要があります。
- Expressway-C と Cisco Expressway-E **は一緒にアップグレードする必要があります**。Expressway-C と Expressway-E を異なるバージョンで長期間使用することはお勧めしません。
- この項目は、TC または Collaboration Endpoint (CE) ソフトウェアを実行しているクラスター化された Unified CM とエンドポイントで、MRA に使用される Expressway をアップグレードする場合に適用されます。この場合、Expressway をアップグレードする*前に*、以下に (または後続で) リストされている関連する TC または CE メンテナンスリリースをインストールする必要があります。これは、フェールオーバーに関する既知の問題を回避するために必要です。推奨される TC / CE メンテナンスリリースがない場合、エンドポイントが登録された元の Unified CM が何らかの理由で失敗した場合、エンドポイントは別の Unified CM へのフェールオーバーを試行しません。Bug ID CSCvh97495 を特定します。

  - TC7.3.11
  - CE8.3.3
  - CE9.1.2
- X8.10.x のバージョンは、MRA 認証 (アクセス制御) 設定を Expressway-E から Expressway-C に移動し、既存の設定を保持できないデフォルト値を適用します。アップグレード後、**これらのアップグレード手順で後述**するように、Expressway のアクセス制御設定を再構成する必要があります。

Cisco Unified Communications Manager IM and Presence Service 11.5(1) を記載した X8.7.x 以前のバージョンを使用した導入

Expressway の X8.7.x 以前のバージョンでは、Cisco Unified Communications Manager IM and Presence Service 11.5 (1) 以降と相互運用できません。IM and プレゼンスサービスソフトウェアの前に、このソフトウェアをアップグレードする必要があります。詳細については、「相互運用性」 (24 ページ)を参照してください。

Cisco Webex Hybrid Services を使用する導入

管理コネクタは、Expressway をアップグレードする前に最新のものにする必要があります。Expressway をアップグレードする前に、Cisco Webex クラウドによってアドバタイズされた管理コネクタのアップグレードを承認して受け入れます。そうでない場合、アップグレード後にコネクタで問題が発生する場合があります。

ハイブリッドコネクタ ホスティングでサポートされる Expressway のバージョンの詳細については、『Connector Host Support for Cisco Webex Hybrid Services』を参照してください。

アップグレード手順

はじめる前に

- システムのアクティビティレベルが低い場合は、アップグレードを実行します。
- 『アップグレードの前提条件とソフトウェアの依存関係 (25 ページ)』にあるすべての関連タスクが完了していることを確認してください。
- アップグレードする前に、MRA 認証の設定に注意してください。この項目は、MRA の Expressway を使用し、X8.9.x 以前から X8.10 以降にアップグレードする場合にのみ適用されます。バージョン X8.10 以降では、MRA 認証 (アクセスコントロール) 設定を、Expressway-E から Expressway-C に移動しました。アップグレードでは、既存の Cisco Expressway-E 設定は保持されないため、アップグレード後は、その MRA のアクセス制御設定を確認し、必要に応じて展開に合わせて調整する必要があります。既存の MRA 認証設定にアクセスするには、次のようにします。
  a. Expressway で、**設定 > Unified Communications > 設定**に移動し、**シングルサインオン サポート**を見つけます。既存の値 ([On]、[Exclusive]、または [Off]) に注意してください。
  b. **シングルサインオンのサポート**が[on]または[Exclusive]に設定されている場合は、次の関連フィールドの現在の値にも注意してください。
     - **内部認証の可用性の確認 (Check for internal authentication availability)**
     - **Jabber iOS クライアントによる、組み込みの**

Safari のクラスタ化されたシステムの使用の許可

クラスタ化されたシステムをアップグレードするには、『Cisco Expressway シリーズ設定ガイド』のページに用意されている『*Expressway Cluster Creation and Maintenance Deployment Guide*』クラスタのアップグレードに関する次の重要な要件については、このガイドで説明していますが、便宜上、ここでも繰り返します。

注意:クラスタ化されたシステムでは、設定データが失われるリスクを回避し、サービスの継続性を維持するために、まずプライマリピアをアップグレードしてから、下位ピアを一度に 1 つずつアップグレードすることが不可欠です。

トラバーサルゾーンを介して接続された、Expressway-C および Expressway-E システムのアップグレード

トラバーサルゾーンを介して接続されている Expressway-C (トラバーサルクライアント) および Expressway-E (トラバーサルサーバ) システムでは、両方とも同じソフトウェアバージョンを実行することをお勧めします。

ただし、ある Expressway システムから、Expressway の以前の機能リリースを実行している別のシステムへのトラバーサルゾーンリンクをサポートしています (たとえば、X8.11 システムから X8.10 システムへ) 。つまり、Expressway-C システムと Expressway-E システムを同時にアップグレードする必要はありません。

モバイルおよび Remote Access などの一部のサービスでは、Expressway-C システムと Expressway-E システムの両方で同じソフトウェアバージョンを実行する必要があります。

プロセス

このプロセスは、クラスタ化されたシステム、またはデバイスプロビジョニング (Cisco TMSPE) を使用する、または FindMe (Expressway を管理する Cisco TMS を使用) をアップグレードする場合には適用されません。そのような場合は、*代わりに Expressway クラスター作成およびメンテナンス展開ガイド*の指示に従ってください。

1. アップグレードする前に Expressway システムをバックアップします (**メンテナンス > バックアップと復元**) 。
2. メンテナンス モードを有効にします。
   a. **[メンテナンス (Maintenance)] > [メンテナンスモード (Maintenance mode)] に移動します。**
   b. **[メンテナンスモード (Maintenance mode)]** を *[オン (On)]* に設定します。
   c. **[保存(Save)]** をクリックし、確認ダイアログで**[確認(OK)]**をクリックします

3. コールがクリアされ、登録がタイムアウトになるまで待機します。
   - 必要に応じて、自動的にクリアされないコールを手動で削除します (**ステータス > コール**、[**すべて選択 (Select all)**]、**[切断 (Disconnect)] をクリックし**ます)。
   - 必要な場合、自動的にクリアされない登録を手動で削除します (Web ブラウザを使用し、**[ステータス (Status)] 、 [登録 (Registrations)] 、[デバイスごと (By device)]**、[すべて選択 (Select all)]を**クリックしてから**[登録解除 (Unregister)]をクリックします) 。 に移動して、削除するデバイスの横のチェックボックスをオンにして、[登録解除 (Unregister)] をクリックします) 。
4. Expressway をアップグレードして再起動します (**[メンテナンス]> [アップグレード]**) 。

   X12.5.4 リリース (たとえば、X8.x から X12.5.4) にアップグレードする場合は、リリースキーは必要ありません。

   経過表示バーが終了を示した後に、Web ブラウザインターフェイスが再起動プロセス中にタイムアウトする場合があることに注意してください。これは、Expressway がディスクファイル システムチェックを実行する場合に発生する可能性があります。これは、約 30 回の再起動ごとに実行されます。
5. この手順は、MRA に対して、Expressway を使用するかどうかによって異なります。
   - MRA を使用しない場合は、アップグレードが完了し、すべての Expressway の設定が期待どおりになります。
   - MRA を使用していて、X8.9.x 以前のバージョンからアップグレードする場合は、 「付録 1: MRA 導入のアップグレード後のタスク (31 ページ) 」の説明に従って、MRA アクセスコントロールの設定を再設定する必要があります。

コラボレーション ソリューション アナライザの使用

*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。

注: 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。

使用する前に

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 からログを収集します。
2. https://cway.cisco.com/tools/CollaborationSolutionsAnalyzer/にログインします
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。
   a. **[ログ分析 (Log analysis)]**をクリックします。
   b. ログファイルをアップロードします。
   c. 分析するファイルを選択します。
   d. **[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。

Bug Search Tool の使用

バグ検索ツールには、問題の説明と利用可能な解決策など、このリリースおよび以前のリリースの未解決の問題と解決済みの問題に関する情報があります。これらのリリースノートに示されている ID によって、それぞれの問題の説明に直接移動できます。

このマニュアルに記載された問題に関する情報を検索するには、次の手順を実行します。

1. ウェブ ブラウザを使用して、バグ検索ツール に移動します。
2. cisco.com のユーザ名とパスワードでログインします。
3. **検索**フィールドにバグ ID を入力し、**[検索]**をクリックします。

ID がわからない場合に情報を検索するには、次の手順を実行します。

1. **検索**フィールドに製品名を入力して**[検索]**をクリックします。
2. 表示されるバグのリストで**フィルタ**ドロップダウン リストを使用し、*キーワード*、*変更日 (Modified Date)* 、*重大度 (Severity)* 、*ステータス (Status)* 、または *テクノロジー (Technology)* のいずれかでフィルタリングを行います。

バグ検索ツールのホームページで**詳細検索**を使用して、特定のソフトウェアバージョンを検索します。

Bug Search Tool のヘルプ ページには、Bug Search Tool の使用に関する詳細情報があります。

マニュアルの入手方法およびテクニカル サポート

電子メールまたは RSS フィードを介して送信される柔軟な通知アラートをカスタマイズするには、Cisco 通知サービスをご利用ください。

ドキュメントの入手、Cisco Bug Search Tool (BST) の使用、サービス要求の送信、追加情報の収集の詳細については、『*What's New in Cisco Product Documentation*』を参照してください。

新しく作成された、または改訂された Cisco のテクニカル コンテンツをお手元で直接受け取るには、『What's New in Cisco Product Documentation』RSS フィードをご購読ください。RSS フィードは無料のサービスです。

付録 1: MRA 導入のアップグレード後のタスク

このセクションは、Expressway 経由でのモバイルおよび Remote Access を使用しており、X8.9.x またはそれ以前から X8.10 以降にアップグレードする場合にのみ適用されます。システムを再起動した後、MRA アクセスコントロールの設定を再設定する必要があります。

1. Expressway-C で、**[設定] > [ユニファイド コミュニケーション] > [設定]**を選択します。
2. 次のいずれかを実行します。
   - 新しい MRA アクセスコントロール方式を X8.10 から利用するには、このページで選択した方法で適切な値を設定します。どの値を適用するかについては、次の最初の表を参照してください。
   - または、アップグレード前の認証アプローチを保持するには、このページで適切な値を設定して、Expressway-E の以前のバージョンの設定に一致させます。古い Expressway-E 設定を Expressway-C の 新しい同等の設定にマッピングする方法については、下の 2 番目の表を参照してください。
3. 自己記述トークン (**OAuth トークンによる承認 (更新あり) (Authorize by OAuth token with refresh)** ユニファイド CM ノードを更新します。**設定 > ユニファイドコミュニケーション > *< UC サーバタイプ >***に移動し、**[サーバの更新 (refresh servers)]** をクリックします。

重要:

- アップグレード後は、**[内部認証の可用性の確認 (Check for internal authentication availability)]** 設定がオフになります。ユニファイド CM の認証設定によっては、一部の Cisco Jabber ユーザによるリモートログインが妨げられる場合があります。
- X8.9 の*[エクスクルーシブ (Exclusive)]*オプションは、*SAML SSO 認証*への**認証パス**を設定することによって設定されるようになりました。これには、ユーザ名とパスワードによる認証禁止が適用されます。

Web UI で実際に表示されるフィールドは、MRA が有効かどうか (**[ユニファイド コミュニケーション モード (Unified Communications mode)]** が *[モバイルおよび Remote Access]* に設定されている) 、および選択された認証パスによって異なります。テーブル内のすべてのフィールドが必ずしも表示されるわけではありません。

表 5: MRA アクセス制御の設定

フィールド	説明	デフォルト
認証パス (Authentication path)	MRA が有効になるまで非表示のフィールド。MRA 認証の制御方法を定義します。 *[SAML SSO 認証 (SAML SSO*authentication)]: クライアントは外部 IdP によって認証されます。 *[UCM/LDAP 基本認証 (UCM/LDAP basic authentication)]: クライアントは、LDAP クレデンシャルに対して Unified CM によってローカルに認証されます。* *[SAML SSO および UCM/LDAP*: どちらの方法も許可します。 *[なし (None)]*:認証は適用されません。これは、MRA が最初に有効になるまでのデフォルトです。一部の展開では実際には MRA ではない機能を許可するために MRA をオンにする必要があるため、 (MRA をただオフにするのではなく) [なし (None)] オプションが必要です。(Meeting Server の Web プロキシ、XMPP フェデレーションなど) 。これらの顧客のみが [なし (None)] を使用する必要があ	MRA の前になし オンにする UCM/LDAP MRA をオンにした後
OAuth トークンによる承認 (更 新 あ り) (Authorize by OAuth token with refresh)	このオプションでは、承認のための自己記述トークンが必要です。サポート用のインフラストラクチャを持つすべての展開で推奨される承認オプションです。 現在、この承認方法を使用できるのは Jabber クライアントだけです。他の MRA エンドポイントは現在サポートしていません。また、クライアントは、更新を伴う OAuth トークン承認モードにある必要があります。 (欠落または誤って切り取り)	点灯

表 5: MRA アクセス制御の設定 (続き)

フィールド	説明	デフォルト
OAuth トークンによる承認 (Authorize by OAuth token) (以前は SSO モード)	**[認証パス (Authentication path)]** が *[SAML SSO]* または *[SAML SSO および UCM/LDAP (SAML SSO and UCM/LDAP)]* の場合に利用可能。 このオプションには、IdP を使用した認証が必要です。現在、Jabber クライアントのみがこの承認方法を使用できますが、他の MRA エンドポイントではサポートされていません。	オフ
ユーザクレデンシャルによる承認 (Authorize by user credentials)	**[認証パス (Authentication path)]**が *[UCM/LDAP]* または *[SAML SSO および UCM/LDAP (SAML SSO and UCM/LDAP)]* の場合に利用可能。 ユーザクレデンシャルによる認証を実行しようとするクライアントは、MRA によって許可されます。これには、Jabber、およびサポートされている IP フォンと TelePresence デバイスが含まれます。	オフ
内部認証の可用性の確認 (Check for internal authentication availability)	**[OAuth トークンによる承認 (更新あり) (Authorize by OAuth token with refresh)]** または **[OAuth トークンによる承認 (Authorize by OAuth token)]**が有効になっている場合に利用可能。 最適なセキュリティとネットワーク トラフィックの削減のため、デフォルトは [いいえ (No)] です。 Expressway-C がホーム ノードをチェックするかどうかを選択することにより、Expressway-E がリモート クライアント認証要求にどのように反応するかを制御します。 要求は、クライアントが OAuth トークンによってユーザを認証しようとする可能性があるかどうかを尋ね、その要求には Expressway-C がユーザのホーム クラスタを見つけるためのユーザ ID が含まれています。 *[はい (Yes)]:* get_ Edge _sso 要求は、OAuth トークンがサポートされているかどうかをユーザのホーム Unified CM に尋ねます。ホーム Unified CM は、Jabber クライアントの *get_ Edge _sso* 要求によって送信された ID から決定されます。 *[いいえ (No)]*: Expressway が内部的に見えないように設定されている場合、 Edge の認証設定に応じて、すべてのクライアントに同じ応答が送信されます。 選択するオプションは、実装およびセキュリティ ポリシーによって異なります。すべての Unified CM ノードで OAuth トークンがサポートされている場合は、*[いいえ (No)]*を選択して応答時間とネットワーク全体のトラフィックを減らすことができます。または、ロールアウト中にクライアントが Edge 構成を取得するモードを使用するようにする場合や、すべてのノードで OAuth を保証できない場合は、*[はい (Yes)]* を選択します。 **注意: これを *[はい (Yes)]* に設定すると、認証されていないリモート クライアントからの不正な着信要求を許可する可能性があります。** この設定に [いいえ (No)] を指定すると、Expressway は不正な要求を回避します。	いいえ (No)

表 5: MRA アクセス制御の設定 (続き)

フィールド	説明	デフォルト
ID プロバイダー: IdP の作成または変更 (Identity providers: Create or modify IdPs)	**[認証パス (Authentication path)]** が *[SAML SSO]* または *[SAML SSO および UCM/LDAP (SAML SSO and UCM/LDAP)] の場合に利用可能。* **ID プロバイダーの選択** Cisco コラボレーション ソリューションは、SAML 2.0 (セキュリティ アサーション マークアップ言語) を使用して、ユニファイド コミュニケーション サービスを利用するクライアント用の SSO (シングル サインオン) を有効にします。 使用する環境に SAML ベース SSO を選択した場合は、次の点に注意してください。 ■ SAML 2.0 は、SAML 1.1 との互換性がないため、SAML 2.0 標準を使用する IdP を選択する必要があります。 ■ SAML ベースのアイデンティティ管理は、コンピューティングとネットワーキング業界のベンダーによって異なる方法で実装されています。したがって、SAML 標準に準拠するための幅広く受け入れられている規制はありません。 ■ 選択した IdP の設定や管理ポリシーは、Cisco TAC (テクニカル アシスタンス センター) のサポート対象外です。IdP ベンダーとの関係とサポート契約を利用して、IdP を正しく設定する上での支援を得られるようにしてください。Cisco は IdP に関するエラー、制限、または特定の設定に関する責任を負いません。 Cisco コラボレーション インフラストラクチャは、SAML 2.0 への準拠を主張する他の IdP と互換性がある可能性もありますが、Cisco コラボレーション ソリューションでテストされているのは次の IdP だけです。 ■ OpenAM 10.0.1 ■ Active Directory Federation Services 2.0 (AD FS 2.0) ■ PingFederate® 6.10.0.4	–
ID プロバイダー: SAML データのエクスポート (Identity providers: Export SAML data)	**[認証パス (Authentication path)]** が *[SAML SSO]* または *[SAML SSO および UCM/LDAP (SAML SSO and UCM/LDAP)] の場合に利用可能。* SAML データの操作の詳細については、「Edge 経由の SAML SSO 認証 (1 ページ)」を参照してください。	–

表 5: MRA アクセス制御の設定 (続き)

フィールド	説明	デフォルト
Jabber iOS クライアントによる組み込みの Safari の使用の許可 (Allow Jabber iOS clients to use embedded Safari)	デフォルトでは、IdP または Unified CM の認証ページは、iOS デバイスの組み込み Web ブラウザ (Safari ブラウザではない) に表示されます。このデフォルトのブラウザは iOS の信頼ストアにアクセスできないので、デバイスに導入された証明書を使用することはできません。 この設定では、オプションで、iOS デバイス上の Jabber がネイティブの Safari ブラウザを使用することができます。Safari ブラウザ *では、デバイスの信頼ストアにアクセスできる*ため、OAuth 導入時にパスワードレス認証または二要素認証を有効化できるようになりました。 このオプションには潜在的なセキュリティの問題が存在します。認証が完了した後で、Safari から Jabber にブラウザ制御を返す機能は、カスタム プロトコル ハンドラを呼び出すカスタム URL 方式を使用します。Jabber 以外の別のアプリケーションがこの方式を妨害し、iOS から制御を取得できます。その中で、 この場合、アプリケーションは URL の OAuth トークンにアクセスできます。 すべてのモバイル デバイスが管理されているなどの理由で、iOS デバイスに Jabber のカスタム URL 形式を登録する他のアプリケーションがないと確信する場合、オプションを有効にしても安全です。別のアプリケーションがカスタム Jabber URL を妨害する可能性が心配な場合、組み込み Safari ブラウザを**有効に**しません。	いいえ (No)
SIP トークンの余分なパケット存続時間 (SIP token extra time to live)	**[OAuth トークンによる承認 (Authorize by OAuth token)]** が *[オン (On)]* の場合に利用可能。 必要に応じて、簡単な OAuth トークンの存続可能時間 (秒) を延長します。クレデンシャルの有効期限が切れた後、コールを受け入れるための短い時間枠をユーザに提供します。ただし、潜在的なセキュリティ リスクが増加します。	0 秒

表 6 アップグレードによって適用される MRA アクセス制御値

オプション	アップグレード後の値	...の前	...の現在
認証パス (Authentication path)	アップグレード前の設定が適用されます **注:** **[SSO モード]**: x8.9 の*[オフ (Off)]*は、x8.10 の 2 つの設定になります。 ▪ **認証パス**=*UCM/LDAP* ▪ **ユーザクレデンシャルによる承認 (Authorize by user credentials)** =*オン* **[SSO モード]**: x8.9 の*[エクスクルーシブ (Exclusive)]*は、x8.10 の 2 つの設定です。 ▪ **認証パス**=*SAML SSO* ▪ **OAuth トークンによる承認**=*オン* **[SSO モード]**: x8.9 の*[オフ (Off)]*は、x8.10 の 3 つの設定になります。 ▪ **認証パス**=*SAML SSO/および UCM/LDAP* ▪ **OAuth トークンによる承認**=*オン* ▪ **ユーザクレデンシャルによる承認 (Authorize by user credentials)** =*オン*	両方（Both）	Expressway-C
OAuth トークンによる承認 (更新あり) (Authorize by OAuth token with refresh)	オフ	–	Expressway-C
OAuth トークンによる承認 (Authorize by OAuth token) (以前は SSO モード)	アップグレード前の設定が適用されます	両方（Both）	Expressway-C
ユーザクレデンシャルによる承認 (Authorize by user credentials)	アップグレード前の設定が適用されます	両方（Both）	Expressway-C
内部認証の可用性の確認 (Check for internal authentication availability)	いいえ (No)	Expressway-E	Expressway-C
ID プロバイダー: IdP の作成または変更 (Identity providers: Create or modify IdPs)	アップグレード前の設定が適用されます	Expressway-C	Expressway-C (変更なし)
ID プロバイダー: SAML データのエクスポート (Identity providers: Export SAML data)	アップグレード前の設定が適用されます	Expressway-C	Expressway-C (変更なし)
Jabber iOS クライアントによる組み込みの Safari の使用の許可 (Allow Jabber iOS clients to use embedded Safari)	いいえ (No)	Expressway-E	Expressway-C
SIP トークンの余分なパケット存続時間 (SIP token extra time to live)	アップグレード前の設定が適用されます	Expressway-C	Expressway-C (変更なし)

Cisco の法的情報

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェアライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

Cisco が導入する TCP ヘッダー圧縮は、カリフォルニア大学バークレー校 (UCB) により、UNIX オペレーティング システムの UCB パブリック ドメイン バージョンの一部として開発されたプログラムに適応したものです。全著作権所有。著作権©1981、カリフォルニア大学理事。(Copyright © 1981, Regents of the University of California.)

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。Cisco およびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、Cisco およびその供給者は、このマニュアルに適用できるまたは適用できないことによって、発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性が Cisco またはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワークトポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

印刷版と複製ソフトは公式版とみなされません。最新版はオンライン版を参照してください。

Cisco は世界各国 200 箇所にオフィスを開設しています。各オフィスの住所、電話番号、FAX 番号については、Cisco のウェブサイト www.cisco.com/go/offices をご覧ください 。

Cisco の商標

Cisco および Cisco ロゴは、Cisco またはその関連会社の米国およびその他の国における商標または登録商標です。Cisco の商標の一覧については、www.cisco.com/go/trademarks をご覧ください。掲載されている第三者の商標はそれぞれの権利者の財産です。「パートナー」または「partner」という用語は、Cisco と他社との間のパートナーシップ関係を意味するものではありません。(1110R)