Cisco Expressway X8.11.4

リリース ノート

初版：2018 年 7 月

最終更新日：2019 年 12 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 12 月	refresh（表 6）のある OAuth トークンのデフォルト設定を「オン（On）」に修正。	ドキュメントの訂正
2019 年 10 月	「アップグレードの前提条件とソフトウェアの依存関係」について、現在 X8.5.3 以前のシステムに対して 2 段階のソフトウェア アップグレードが必須となるように修正。中間ソフトウェアリリース X X8.8.2 を推奨。	ドキュメントの訂正
2019 年 4 月	Web ユーザ インターフェイスの「概要」ページで、Expressway がレジストラである場合（非トラバーサル コールのカウントおよびステータス表示なし）における予期しない動作の「*注意すべき問題*」セクションに説明を追加。	ドキュメントの追加
2019 年 3 月	クラスタのピアを削除するとデュアル NIC 環境にある LAN2 インターフェイスの「すべての」設定が削除されることを明記（「*クラスタに残っているピアを工場出荷時状態にリセットする*」セクション）。	ドキュメントの追加
2019 年 2 月	11.1.2 以前の Jabber Guest バージョンに関する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。	ドキュメントの訂正
2018 年 11 月	OAuth 更新と IM およびプレゼンス サービスによるプレゼンス冗長グループを使用した MRA 経由のチャット/メッセージング サービスに関する制限を更新。	X8.11.4
2018 年 11 月	メンテナンス リリースの更新。	X8.11.4
2018 年 10 月	メンテナンス リリースの更新。	X8.11.3
2018 年 9 月	「制限」セクションを更新し、中規模システムの逆多重化ポートの動作を明記。	明記

日付	変更内容	理由
2018 年 9 月	メンテナンス リリースの更新。 X8.11 ソフトウェア バージョンが使用できなくなり、使用を止めることを示す情報を追加。	X8.11.2 ソフトウェアの取り消し。
2018 年 9 月	メンテナンス リリースの更新。 また、トークンの更新によるユーザ認証の場合に、すべての事例について、MRA に接続されたチャット/メッセージング サービスがサポートされないことを明記。	X8.11.1
2018 年 7 月	初版。	X8.11

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.n このハードウェアでは X8.10.n 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.n このハードウェアでは X8.10.n より後のバージョンはいずれもサポートされません。

*2016 年 2 月 26 日現在、CE500 アプライアンスと CE1000 アプライアンスはシスコに注文できません。これらのプラットフォームのライフサイクルのその他の重要な日付については、「販売終了のお知らせ」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。

関連ドキュメント

表 3　関連ドキュメントへのリンク

仮想マシンのインストール	Expressway インストール 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：**Expressway インストール ガイド ページの*『Cisco Expressway CE1200 アプライアンス インストレーション ガイド』* **VCS：**VCS インストール ガイド ページの*『Cisco Video Communication Server CE1100 アプライアンス インストレーション ガイド』*
レジストラ / 単一システムの基本設定	**Expressway：**Expressway コンフィギュレーション ガイド ページの*『Cisco Expressway レジストラ導入ガイド』* **VCS：**VCS コンフィギュレーション ガイド ページの*『Cisco Single VCS Control - 基本設定導入ガイド』*
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：**Expressway コンフィギュレーション ガイド ページの*『Cisco Expressway-E および Expressway-C 基本設定導入ガイド』* **VCS：**VCS コンフィギュレーション ガイド ページの*『Cisco TelePresence VCS 基本設定（Control と Expressway）導入ガイド』*
管理およびメンテナンス	**Expressway：** Cisco Expressway シリーズ保守と運用ガイド ページ の*『Cisco Expressway 管理者ガイド』*Cisco Expressway シリーズ保守と運用ガイド ページの*『Cisco Expressway サービスアビリティ ガイド』* **VCS：** Cisco TelePresence VCS 保守と運用ガイド ページ の*『Cisco TelePresence VCS 管理者ガイド』*Cisco TelePresence VCS 保守と運用ガイド ページの*『Cisco TelePresence VCS サービスアビリティ ガイド』*
クラスタ	Cisco Expressway シリーズ 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ス導入ガイド』*
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』*
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 リファレンス 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 and 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 Meeting Server と Cisco Expressway 導入ガイド』* Cisco Meeting Server プログラミング ガイド ページの *『Cisco Meeting Server API リファレンス ガイド』* Cisco Meeting Server のその他のガイドは、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
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 と 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 と Microsoft Skype for Business インフラストラクチャ設定虎の巻』*
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』

機能の履歴

表 4：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	–	–	–	サポート対象	サポート対象
MRA での Finesse エージェントのサポート	–	–	サポート対象	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	–	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 へのデバイス登録（SIP および H.323）	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
Cisco TMS プロビジョニング アクセスに対する変更	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
Cisco Expressway シリーズでの Multiway 会議	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）	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	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
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	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
大規模 Expressway-E での TURN ポート多重化	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
保存中のデータのセキュリティ強化	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

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
コモン クライテリアの準備	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
バックアップ時の必須パスワード	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
カスタム ドメイン検索	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 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 経由の Mobile and Remote Access*』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）	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	X8.11 関連	X8.11 関連	X8.11 関連	X8.11 関連
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	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
クラスタから離脱したピアの初期設定へのリセット	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

機能の履歴

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
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	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
REST API 拡張	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

注意：X8.11.4 をインストールする前にお読みください。

バージョン X8.9 ～ X8.11.3 はダウンロードできなくなりました

この X8.11.4 メンテナンス リリースは、ダウンロードできなくなった X8.11.x、X8.10.x、および X8.9.x ソフトウェアのすべての以前のバージョンより優先します。**このバージョンにアップグレードすることを強く推奨します。**（これらのリリース ノートの機能リストでは引き続き X8.11 が参照されていますが、ソフトウェアは使用できません）。

現在バージョン X8.5.3 またはそれ以前を実行している Expressway では、2 段階のアップグレードが必要です。

X8.5.3 またはそれ以前のソフトウェアを実行しているシステムでは、「アップグレードの前提条件とソフトウェアの依存関係、31 ページ」で説明しているように、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。

X8.11.4 での変更

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 サービスの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、このシナリオでユーザ ログインの障害が発生します。

セキュリティ アドバイザリのための変更

X8.11.4 は、シスコにより https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20181107-vcsd で公開され CDETS CSCvn17278 により追跡されているセキュリティ アドバイザリに対処するためのメンテナンス リリースです。

その他の未解決の問題に対する変更

このメンテナンス リリースでは他の問題の一部が解決されており、それに伴って「未解決および解決済みの問題、25 ページ」の検索リストが更新されています。

MRA の変更（お客様向けマニュアル）

お客様向けマニュアルが修正され、Mobile and Remote Access（MRA）接続を介した録音（組み込みブリッジ（BiB）の録音を含む）について以前に記載されていなかったこれらの制限が追加されました。

- 録音は、個人どうしの直接コールの場合にのみ機能し、会議では機能しません。
- 現在、サイレント モニタリング機能とウィスパー コーチング機能では、録音はサポートされていません。

Cisco Meeting Server の Web プロキシに関する変更

この項目は、Cisco Meeting WebRTC アプリのサポートを目的として Expressway を Cisco Meeting Server の Web プロキシとして使用する場合に適用されます。以前は、Expressway の WebRTC ソケット タイムアウト値によって WebRTC コールが 1 時間（3600 秒）後にドロップされるようになっていました。このタイムアウトが 12 時間（43200 秒）に延長されました。現在、この設定は設定不可です（CDETS CSCvn28708 参照）。

X8.11.3 での変更

未解決の問題と制限に対する変更

X8.11.3 はメンテナンス リリースです。「未解決および解決済みの問題、25 ページ」の検索リストが更新されています。

このリリースでは、いくつかの制限が修正または軽減されています。

- 以前は、Meeting Server Call Bridge クラスタを使用していて、Expressway を Meeting Server のエッジとしている Microsoft ベースのユーザについて、デュアルホーム会議がサポートされていませんでしたが、このシナリオがサポートされるようになりました。
- 1 Gbps NIC を備えた Medium 規模のアプライアンスベース システムは、アップグレード時に自動的に Large システムに変換されます。この結果、Large システムのデフォルトの逆多重化ポートがファイアウォール上で開いていない限り、Expressway による逆多重化ポートの動作が原因でコールがドロップされます。このリリースでは、新しいシステム サイズの選択の設定を使用して、デフォルト サイズを Medium に手動でリセットできます（次のポイントを参照）。
- Cisco Expressway CE1200 アプライアンスを Expressway-E システムとして設定している場合、以前は、特に Expressway-E に適用される REST API コマンドが使用できませんでしたが、それらのコマンドがサポートされるようになりました。

アプライアンスのシステム サイズの選択

CE1100 または CE1200 アプライアンスで、システム サイズを手動で Medium または Large に変更できるようになりました。それには、[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。

X8.11.2 での変更

未解決の問題に対する変更

X8.11.2 はメンテナンス リリースです。「未解決および解決済みの問題、25 ページ」の検索リストが更新されています。

MRA の変更

次の変更は、Cisco Unified Communications Manager の Mobile and Remote Access（MRA）機能を使用している環境に適用されます。

- サポート対象のデバイスで、Cisco Finesse エージェントとコンタクト センターのシンクライアント デスクトップが MRA 接続経由でサポートされるようになりました。

X8.11.1 での変更

新しい CE1200 アプライアンス

このソフトウェア メンテナンス リリースに合わせて、新しい CE1200 アプライアンスが導入されました。

すでに CE500、CE1000、または CE1100 アプライアンスを展開しているユーザに向けて、このセクションでは、CE1200 での違いについていくつか説明します。

- CE1200 は Cisco Expressway シリーズ製品の範囲で使用することを念頭に設計されており、Cisco VCS 製品をサポートしていません。リリース キーがプレインストールされた状態で出荷されています。
- 以前のアプライアンスとは異なり、CE1200 は、Cisco Expressway-C または Cisco Expressway-E として動作できる単一の多目的サーバです。デフォルトでは、常に Expressway-C がプレインストールされた状態で出荷されています。サーバを Expressway-E として展開するには、サービス セットアップ ウィザード**で [タイプ（Type）]** オプションを [Expressway-E] として設定します（ウィザードは、初めて Expressway Web ユーザ インターフェイスを起動したときに実行されます）。または、**[ステータス（Status）] > [概要（Overview）]** ページからいつでも実行できます。トラバーサル サーバのオプション キーは、Cisco Expressway-E への変更の目的で使用されなくなりました。
- CE1200 は、最大 5000 の Mobile and Remote Access の登録をサポートでき、他の物理アプライアンスや VM ベース システムでサポートされている 2500 の MRA 登録数よりも増やされています。

CE1100 モデルが含まれている既存のクラスタに CE1200 アプライアンスを追加するには、クラスタに CE1200 を追加する「前」に、[ステータス（Status）] > [概要（Overview）] ページのサービス セットアップ ウィザードを使用して、他のピアに合わせて [タイプ（Type）] オプションを設定します（Expressway-E または Expressway-C）。

シングル NIC 展開での Jabber Guest ライセンスの問題の解決

Jabber Guest 11.1.2 バージョン以降を実行している場合、このメンテナンス リリースによって、Expressway-E でではなく Expressway-C で消費されている Jabber Guest コールについて、RMS ライセンスに関する以前の問題が解決します。（CDETS CSCvf34525）。

注：これとは別に、シングル NIC 展開での Jabber Guest の問題は依然として残っており、Expressway-E では、Jabber Guest コールごとの RMS ライセンスのカウントが失敗します（CDETS CSCva36208）。

MRA の変更

下記の変更は、Cisco Unified Communications Manager の Mobile and Remote Access（MRA）機能を使用している環境に適用されます。

- Cisco Unified Communications Manager version 11.5（1）SU5 以降のバージョンを実行していて、関連する変更を加えている場合、ハント グループ（ハント パイロットやハント リストを含む）は MRA 経由でサポートされます。
- Expressway CE1200 アプライアンスは、最大 5000 の Mobile and Remote Access の登録をサポートできることが検証されています。これは、以前のアプライアンスで検証された 2500 から増えています。（MRA の登録数が 2500 のままとなっている 以前の物理アプライアンス モデルや VM システムについては、この変更は適用されません。）

X8.11 の機能（現在は X8.11.4）

デバイス登録の拡張

Expressway-E への登録

X8.11 以降、Cisco Expressway-E で SIP レジストラと H.323 ゲートキーパー機能がサポートされます。これにより、SIP および H.323 エンドポイントを直接 Expressway-E に登録できるようになりました。

ライセンス

すでに Expressway-C にライセンスが存在する場合、ライセンスが適用されている既存のエンドポイントの一部または全部を Expressway-E に登録するには、関連するオプション キーを Expressway-C から手動で削除した後、Expressway-E にリロードする必要があります。

H.323 デバイスに関する情報

- Expressway-C への H.323 の登録と同様に、Expressway-E に登録された H.323 デバイスはそれぞれ、TelePresence Room System ライセンスを消費します。
- 現時点では、リモートの H.323 デバイスによる Expressway-C または Expressway-E へのプロキシの登録はサポートされていません。

Cisco TMS Provisioning Access（ユーザ、FindMe、電話帳、およびデバイス プロビジョニング）の変更

Expressway はオプションで、Cisco TMS によって（Cisco TMSPE を介して）ホストされている FindMe やその他のプロビジョニング サービスにアクセスすることもできます。以前は、必要なオプション キーを持っている場合に、この機能はデフォルトで有効になっていました。

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。

X8.11 以降、以前の Cisco Expressway-C での場合と同様に、Cisco Expressway-E でのデバイス プロビジョニングがサポートされます。デバイス プロビジョニングが両方のコンポーネントでサポートされるようになりましたが、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。

Expressway での Multiway

Cisco Expressway シリーズでは、以前 Cisco VCS 製品でのみサポートされていた Multiway 会議がサポートされるようになりました。Multiway 会準拠のエンドポイント、および Cisco TelePresence Server または Cisco TelePresence MCU シリーズの会議ブリッジの場合、ポイントツーポイント コールのビデオ発信者は、手動で第三者をコールに追加し、インスタント会議を作成することができます。

注：Multiway 会議は「Conference Factory」と呼ばれる Cisco Expressway の基本機能に依存しています。このため、Multiway 会議に関連するドキュメント、ライセンス、およびユーザ インターフェイスの設定の一部で、Conference Factory という用語が使用されています。

ライセンス

Multiway 会議機能では、Cisco Expressway-C で「Conference System」ライセンスが必要です。このライセンスは無料ですが、Conference Factory（つまり、Multiway 会議）を有効にすると登録リソースが 1 つ占有されます。

Cisco Meeting Server との統合の改善

（プレビュー）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）

この機能は現在プレビュー ステータスにあります。Cisco Meeting Server ソフトウェア バージョン 2.3 およびそれ以前ではサポートされていません。また、Meeting Server クラスタを使用したデュアルホーム会議のサポートについて、現在制限事項があります。

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、そのサーバは応答コード「488 Not Acceptable Here」でコールを拒否します。拒否されたコールは、コール制御層で別のサーバ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]**）。この設定により、Cisco Expressway の B2BUA が「2 番目の」Meeting Server からの INVITE を処理して、参加者の接続を可能にします。

エンドポイントが Expressway に登録されているか Unified CM 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（On）」に設定することを推奨します。

既知のサポート対象機能と制限事項

- 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。
- DTLS 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。
- Cisco Expressway との間のコール レッグにはさまざまな暗号化モードを適用できます。

複数の Meeting Server Web ブリッジに対する Web プロキシ

Cisco Expressway は、Cisco Meeting WebRTC アプリのプロキシとして動作している場合に、Meeting Server Web ブリッジのロード バランシングと冗長性をサポートするようになりました。

以前のバージョンでは、Cisco Expressway は複数の Web ブリッジを限定的な方法でサポートしていました。これは、DNS SRV クエリから返されるすべての Web ブリッジ アドレスにわたって接続を均等に分散させようとするものです。しかし、これらのアドレスが到達不可能だった場合、Cisco Expressway は正常に適応できず、接続が失敗していました。

この機能の設定については変更はありません。単一のアドレス（Expressway UI で「ゲスト アカウント クライアント URI（Guest account client URI）」と呼ばれています）を入力します。Web ブリッジが複数ある場合、Expressway-C は、DNS を使用してそれらの IP アドレスを検出した後、ラウンドロビンを使用してそれらの Web ブリッジ間で WebRTC 接続を均等に分散します。

X8.11 の機能拡張として、Expressway は、Web ブリッジであると認識した IP アドレスの動的なリストを維持するようになりました。具体的には、Meeting Server の Web プロキシ機能について次のような改善が施されています。

- Expressway-C は定期的に DNS をクエリして、展開環境に対する意図的な変更をすべて検出します。 たとえば、SRV レコードに対して追加または削除されたホスト アドレスなどです。
- Expressway-C は、DNS から返されたホスト アドレスをプローブして、それらが到達可能かどうか、また Web ブリッジかどうかを（API コールを使用して）確認します。
- アドレスが到達可能でない場合、またはホストが Web ブリッジでない場合、Expressway-C はそのアドレスへの webRTC 接続の送信を停止します。
- DNS SRV クエリが成功すると、UI ページのステータス領域に、重みや優先順位などの結果が表示されます。
- UI には、アドレスごとに「失敗（failed）」または「アクティブ（active）」のステータスも表示されます。

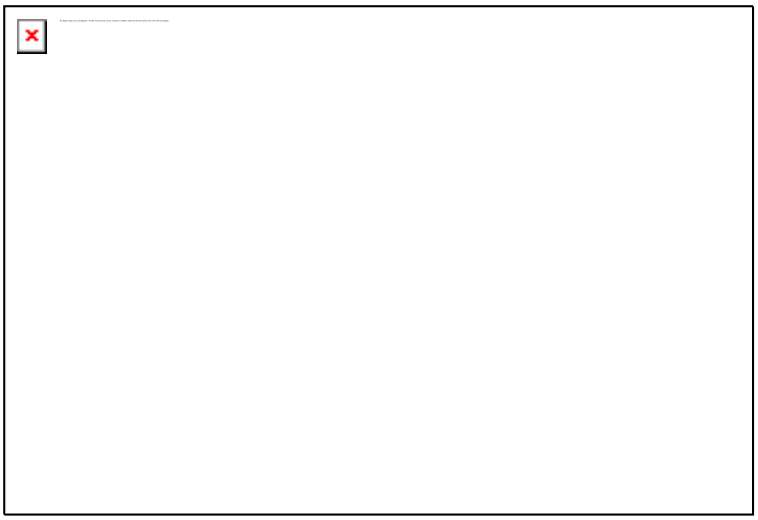
注：Expressway-C は、Cisco Meeting WebRTC アプリから Meeting Server Web ブリッジへのステートフル接続を維持しません。たとえば Web ブリッジ ホストがダウンした場合など、接続に障害が発生した場合は、そのホストに対する既存のコールが失われ、クライアントは Web ブリッジへのコールの再確立を試行する必要があります。その場合、Expressway は、障害が発生したホストへの新しい WebRTC 接続をプロキシしません。

（プレビュー）Cisco Meeting App アプリでは Expressway-E TURN サーバを使用可能

この機能は現在プレビュー ステータスにあります。

X8.11 での TURN サーバの機能強化により、Expressway-E を使用して WebRTC を Meeting Server に対してプロキシしている場合でも、Expressway-E TURN サーバを使用して Cisco Meeting App と Cisco Meeting Server 間でメディア パスの検出とメディア 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 App と Cisco Meeting App



この図では、TURN 要求と WebRTC 要求について TCP 443 でリッスンするように Expressway-E が設定されています。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 の使用を試みます。

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、TCP オーバーライド ポート（デフォルトでは 443 ）を使用してメディア リレーを要求します。

Meeting Server Edge は、Cisco Meeting App 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。

TURN サーバの機能拡張

TCP 443 での TURN

TCP ポート 443 で TURN 要求と Cisco Meeting Server 要求の両方をリッスンするように Expressway-E を設定できます。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。これにより、外部ユーザは TURN サービスを使用して、ファイアウォール ポリシーが制限された環境からでも Meeting Server のスペースに参加できます。

現在、ポート 443 で HTTPS 要求をリッスンするように Web 管理者ポートを設定している場合は、HTTP 要求をリッスンするために別のポートに変更する必要があります（**[システム（System）] > [管理設定（Administration settings）]** の [**Web 管理者ポート（Web administrator port）**] 設定）。Expressway-E は、TCP ポート 443 で Web 管理と TURN 要求の両方をリッスンすることはできません。

Large Expressway での TURN ポート多重化

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ように Large Expressway-E 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、内部的にそれらの要求をポート範囲に逆多重化します。TURN クライアントではポートの 1 つを認識するだけで済みますが、Large Expressway-E TURN サーバの全機能を使用できます。

ただし、TCP 443 TURN サービスが有効にされている場合は、技術的な制約により外部ポートで TCP TURN 要求が多重化されません。この場合、サポートされる TCP TURN リレーの数は 1000 に制限されます。

セキュリティの強化

保存中のデータのセキュリティ強化

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。各 Expressway システム（ハードウェア バージョンと VM バージョンの両方）では、そのシステムに local なデータを暗号化するための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 にアップグレードすると新しいキーが作成され、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。
- キーが UI で公開されることはありません。ローカルでもリモートでもキーがログに記録されることはありません。

コモン クライテリアの準備

X8.11 では、情報技術セキュリティ評価のための共通基準（コモン クライテリア）を満たすように Expressway を設定できます。X8.11 の新しいセキュリティ設定は次のとおりです。

- Expressway-C と Expressway-E 間の SSH トンネルは、設定可能な暗号とキー交換アルゴリズムを備えています。
- [メンテナンス（Maintenance）] > [セキュリティ（Security）] > [SSH の設定（SSH configuration）] Web UI ページで、「暗号方式」と「公開キー アルゴリズム」の設定を変更できます。
- ロギングを、証明書に準拠したモードに設定できます（[メンテナンス（Maintenance）] > [ロギング（Logging）] で、[証明書ロギング（Certification logging）] モードを変更します）。
- 新しい管理者にパスワードのリセットを強制するオプション。このオプションは、新しいユーザを追加するときに [ユーザ（Users）] > [管理者アカウント（Administrator accounts）] に表示されます。

注：また、Expressway のコモン クライテリア作業の一部として、CA 証明書のチェックで *BasicConstraints* 拡張の存在が必須となりました。

バックアップ時の必須パスワード

バックアップ ファイルがすべてのケースで暗号化されるようになりました。また、すべてのバックアップおよび復元の操作でパスワードを指定する必要があります。

注意：バックアップから復元する場合、関連するバックアップ ファイルのパスワードが必要になります。

Mobile and Remote Access の導入

これらの機能および機能拡張は、Expressway が MRA 用に設定されている場合（つまり、Cisco Unified Communications インフラストラクチャに登録されたモバイル デバイスまたはリモート デバイスを使用した展開の場合）に関連します。

カスタム ドメイン検索

X8.11 は以前の MRA の制限事項に対応しています。この制限事項は、Unified Communications インフラストラクチャの DNS ドメインが、AXL を使用してそのインフラストラクチャに接続する Expressway-C の DNS ドメインと異なる場合に適用されていました。

以前のリリースでは、MRA の接続を設定するときに、UC ホストの FQDN を入力する必要がありました。X8.11 以降では、カスタム ドメインを入力し、ホスト名のみを使用して UC ノードを検出できます。入力したアドレスが FQDN または IP アドレス（たとえば、`yourhostname`）ではない場合、Expressway-C は DNS で `yourhostname.Expressway-C-domain` を検索します。この検索でホスト アドレスが返されない場合、Expressway-C は DNS をクエリして `yourhostname.custom-domain` を探します。

その後、Expressway-C は、DNS から返されたホストへの AXL 接続を通常どおり試行します。

この動作は、Expressway-C から別のサブドメインにある外部ノードに接続し、完全修飾でないホスト名を使用する場合に関連します。現在、Expressway はホスト名を FQDN に解決できるようになり、ノード間で接続を設定するときにホストの FQDN を入力する必要がなくなりました。

注：この変更は Expressway の全体的なシステム機能拡張であり、MRA の使用に限定されるものではありません。

インターコムにおける MRA 経由の IP フォンのサポート

この機能をサポートする IP フォンの場合、インターコムのサポートが MRA 経由で使用可能になりました。

MRA 経由での組み込みブリッジの録音

組み込みブリッジの録音がサポートされるようになりました。以前はプレビュー ステータスとなっていました。

Expressway は、MRA 経由の組み込みブリッジ（BiB）録音をサポートしています。この機能は、欧州連合の *Markets in Financial Instruments Directive*（MiFID II）における電話録音の要件を遵守するのに役立ちます。

仕組み

BiB を使用して、オフプレミスで作業しているユーザが発信または受信したコールの音声部分を録音できます。

- BiB は Expressway で常に有効になっています。
- BiB は Cisco Unified Communications Manager で設定できます。BiB が有効になっている場合、Unified CM は、エンドポイント間での発着コールをメディア録音サーバにフォークします。

前提条件

MRA 経由の BiB には下記またはそれ以降のコンポーネントが必要です。

- 互換性のあるクライアント：
  - Windows 版 Cisco Jabber 11.9
  - Mac 版 Cisco Jabber 11.9
  - iPhone および iPad 版 Cisco Jabber 11.9
  - Android 版 Cisco Jabber 11.9
  - **MRA をサポートする** Cisco IP 電話 7800 シリーズまたは 8800 シリーズ デバイス（これらすべての電話機が MRA 互換であるとは限りません）

    現在 MRA をサポートしている 7800/8800 シリーズ電話機の詳細については、Expressway コンフィギュレーション ガイド ページにある最新の『*Cisco Expressway 経由の Mobile and Remote Access*』ガイドの「前提条件」セクションを参照するか、シスコの担当者にお問い合わせください。
- レジストラ/コール制御エージェント：**Cisco Unified Communications Manager 11.5（1）SU3**

  BiB は、Expressway に登録されたエンドポイントではサポートされていません。
- エッジ トラバーサル：**Expressway X8.11.1**
- レコーディング サーバ：このドキュメントの範囲外です。（Cisco Unified Communications Manager における録音の設定方法の詳細については、『Cisco Unified Communications Manager 機能設定ガイド』を参照してください。）

Cisco Jabber エンドポイントのコールの録音には、次のような制限があります。（これらは MRA 経由だけでなくオンプレミスでも適用されます。）

- Cisco Unified Communications Manager では、Jabber モバイル デバイスを CTI モニタリングすることはできません。
- Jabber は、メディア ストリームへの録音トーンの挿入をサポートしていません。

MRA 経由のアクセス ポリシーのサポート

MRA 経由のアクセス ポリシーがサポートされるようになりました。以前はプレビュー ステータスとなっていました。

X8.10 以降、Expressway では、Unified CM で指定する MRA アクセス ポリシー設定が適用されます。これらは Unified CM のユーザ プロファイルでオプションとして設定し、個別のユーザがアクセスできるサービス（[なし（None）]、[IM & P]、[音声とビデオ（Voice & Video）]、または [すべて（All）]）を定義します。次の条件が適用される場合は、Expressway で MRA アクセス ポリシーだけが適用されます。

- Expressway は、MRA 認証の自己記述トークンを処理するように設定されています（[リフレッシュを伴う OAuth トークンによる認証（Authorize by OAuth token with refresh）] を [オン（On）] に設定）。
- コール パス内の他の製品も、トークンのアクセス ポリシー要素を含む自己記述トークンをサポートしています。

注： MRA アクセス ポリシーは、クライアントが自己記述トークンを使用している場合にのみ適用できます。そのため、自己記述トークン認証が MRA に許可されている「唯一の」認証方法である場合に最も効果的です。

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

この機能は現在プレビュー 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 以降が対象）に展開できます。

サービスアビリティの改善

ライセンス キーの統合

Expressway のライセンスに次の項目が標準機能として追加されました。これらは以前は別個のオプション キーとして適用されていました。

- *LIC-EXP-AN*：高度なネットワーキングを有効にします（Expressway-E のみ）
- *IC-EXP-TURN*：TURN リレーを有効にします（Expressway-E のみ）
- *LIC-VCS-DEVPROV*：デバイスのプロビジョニングを有効にします
- *LIC-VCS-FINDME*：FindMe サービスを有効にします

注： これらのキーが適用されている既存のシステムをアップグレードする場合、管理者の便宜を図るため、アップグレード後はたとえ不要となった場合でもキーが Web ユーザ インターフェイスに表示されたままになります。

クラスタから離脱したピアの初期設定へのリセット

X8.11 以降では、クラスタ ピアがクラスタから削除されたとき、またはクラスタが解消されたときのクラスタ ピアの動作が変更されました。この変更は、X8.11 において一意の信頼のルートを改善する一環として行われています。クラスタからピアを削除するには、そのピアにあるすべてのピア アドレス フィールドをクリアします。X8.11 以降でこれを実行すると、**次回の再起動時に初期設定へのリセットの準備**が行われます（また、この状態になっていることを通知するバナーが表示されます）。

初期設定へのリセットを避ける必要がある場合は、クラスタリング ピアのアドレス フィールドを以前と同じ状態に復元してください。元のピア アドレスを同じ順序で置き換えてから、設定を保存してバナーをクリアしてください。

ピアが再起動すると、初期設定へのリセットが自動的にトリガーされ、機密データとクラスタリング設定が削除されます。リセットによって、次に示す基本的なネットワーク情報を除くすべての設定がクリアされます。これらは、引き続き Expressway にアクセスできるようにするために LAN1 インターフェイスに対して保存されます。**デュアル NIC オプションを使用する場合は、すべての LAN2 設定がリセットによって完全に削除される**ことに注意してください。

- IP アドレスを保存
- サーバ証明書、関連付けられた秘密キー、および CA 信頼ストアを保存
- 管理者アカウント、ルート アカウント、パスワードを保存
- SSH キーを保存
- オプション キーを保存
- HTTPS アクセスが有効
- SSH アクセスが有効

注意：Expressway クラスタの編成、変更、またはアップグレードにあたっては、公開されているクラスタリングのガイダンスに必ず従ってください。**クラスタが回復不能である可能性があり、正しい順序に従わないとデータが失われる可能性があります。**ご使用のバージョンについては、Cisco Expressway シリーズ設定ガイド ページの『*Cisco Expressway Cluster Creation and Maintenance Deployment Guide*』を参照してください。

（プレビュー）Smart Call Home

この機能は現在プレビュー ステータスにあります。

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：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：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。

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 Hybrid 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。

REST API 拡張

リモート構成を簡素化するため、シスコは引き続き REST API の拡張を行います。新機能の追加にあたって、REST API から構成、コマンド、およびステータス情報にアクセスする手段を追加していますが、同時に、以前のバージョンで導入された機能に REST API を選択的に組み込んでいます。

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
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概要については、Expressway インストール ガイド ページの『*Cisco Expressway REST API 要約ガイド*』で利用できます。

Cisco Webex ハイブリッド サービスと X8.11

- 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 N 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。「クラスタから離脱したピアの初期設定へのリセット、20 ページ」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、「Cisco Webex ハイブリッド サービスのコネクタ ホスト サポート」を参照してください。
- X8.11 では新しい「Webex」ゾーン タイプが導入されています。これは、Cisco Webex への接続用として特別に設計された DNS ゾーンです。この機能により、Cisco Webex Hybrid コール サービスの設定が簡素化されます。Webex ゾーンを 1 つ作成または削除することはできますが、変更することはできません。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。

その他のソフトウェアの変更と機能拡張

- 新しい CLI コマンド *RetainConnectionOnParseErrorMode* を使用して、形式が不正な、または破損した SIP メッセージを Expressway で処理する方法を管理できます。デフォルトでは、Expressway 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。このコマンドを使用すると、接続を維持する対象のメッセージを、必須以外のヘッダーのみを含むメッセージにするか、または必須ヘッダーを含むすべてのメッセージにするかを選択できます。

注：この設定に関係なく、形式が不正なメッセージを 10 個以上連続して受信した場合、または *Content-Length* ヘッダーが欠落しているか形式が不正な場合、Expressway は常に接続を閉じます。

- Cisco UCS C シリーズ サーバを実行している Expressway アプライアンスでは、Cisco Host Upgrade Utility（HUU）を使用したファームウェア アップグレードがサポートされています。これにより、『*Expressway 管理者ガイド*』に HUU のユーザ向け手順へのリンクが記載されるようになりました。
- SNMP の DES 暗号化オプションはなくなりましたが、以前は Expressway のユーザ インターフェイスとドキュメントに記載されていました。このオプションは削除されました。
- 診断ログを収集するプロセスが異なります。生成されたログ エントリを取得するには、新しい [ログの収集（Collect log）] ボタンを使用します。その後はこれまでどおり [ログのダウンロード（Download log）] ボタンを使用します。この変更は診断ロギングにのみ影響し、他のログプロセスには影響しません。[ログの収集（Collect log）] ボタンをもう一度使用することで、診断ログを繰り返しダウンロードできます。

お客様向けマニュアルの変更

- **X8.11 では 2 つのユーザ ガイドが廃止されています。**次のドキュメントが、このリリースで廃止され、維持されなくなります。『*Cisco Jabber と Microsoft Lync の相互運用性インフラストラクチャ設定虎の巻*』（「SIP ブローカ」の導入）および『*Microsoft のインフラストラクチャを使用した Cisco Expressway 導入ガイド*』（「Lync ゲートウェイ」の導入）。

  Meeting Server を使用した Microsoft 環境とのインターワーキングに関するガイドラインについては、『*Cisco Meeting Server と Cisco Expressway 導入ガイド*』を参照してください。

  - **いくつかの Cisco VCS のマニュアルを廃止しました。**以前は、VCS と Expressway においてほとんどのお客様のサポート マニュアルで 2 つのバリエーションを別々に提供していました。X8.10 以降では、特定のガイドについてのみ Expressway 版の提供を開始しました。この場合、Expressway 版には関連する VCS 固有の情報がすべて記載されます。
    - Cisco Expressway のマニュアルは http://www.cisco.com/c/en/us/support/unified-communications/expressway-series/tsd-products-support-series-home.html から入手できます。
    - Cisco VCS のマニュアルは http://www.cisco.com/c/en/us/support/unified-communications/telepresence-video-communication-server-vcs/tsd-products-support-series-home.html から入手できます。
- **最新情報とソフトウェア バージョン履歴情報が、管理者ガイドとオンライン ヘルプの要約形式になりました。**「最新情報」と「ソフトウェア バージョン履歴」の情報を編成し直し、Expressway の管理者ガイドとオンライン ヘルプにまとめました。機能の概要リストと、それらが導入されたリリースが掲載されており、合わせて、詳細な機能情報について説明するための、関連するリリース ノートへのリンクを紹介しています。
- **REST API ガイドで個々のコールの詳細説明がなくなりました。**Expressway API は RAML を使用して自己文書化されているため、『*Expressway REST API リファレンス ガイド*』から各コールの詳細説明を削除しました。このドキュメントでは、API インターフェイスへのアクセス方法や使用方法について概要情報のみを提供しています。
- **Cisco Meeting Server と Expressway。**『*Cisco Expressway セッション分類導入ガイド*』の名称を『*Cisco Meeting Server と Cisco Expressway 導入ガイド*』に変更しました。

  「2 つの標準ベース組織（B2B）間のビデオ コール」のシナリオについては、『*Cisco Expressway-E および Expressway-C 基本設定導入ガイド*』で説明しています。

  「Microsoft ベースの組織 における IM&P フェデレーション」のシナリオについては、『*Cisco Expressway を使用したチャットおよびプレゼンスのフェデレーション導入ガイド*』で説明しています。
- **XMPP フェデレーションと Expressway。**『*Cisco Unified Communications XMPP フェデレーション導入ガイド*』の名称を『*Cisco Expressway を使用したチャットおよびプレゼンスのフェデレーション*』に変更しました。
- **ドキュメントの小規模な拡張。**リリース機能の追加に加えて、ドキュメントの小規模な修正や変更をいくつか行いました。

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）
- X8.11.4 で解決した問題
- X8.11.3 で解決した問題
- X8.11.2 で解決した問題
- X8.11.1 で解決した問題
- X8.11 で解決した問題

このバージョンで特に重要な問題

エンドポイントが Expressway に登録されている場合に、Web ユーザ インターフェイスの [概要（Overview）] ページにおいて、アクティブ コール カウンタと登録済みコールのリンクで予期しない動作が発生する

Expressway がレジストラの場合、現時点では、2 つのコール関連の問題が [概要（Overview）] ページで正常に機能しません。

- 非トラバーサル コール（Expressway-C に登録されている両方のエンドポイント）では、アクティブ コール カウンタは増加しません。
- [登録済みコール（Registered calls）] リンクをクリックすると、Unified Communications のステータス ページが予期せずに表示されます。

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。CDETS CSCva36208 を参照してください。
- **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必要がありますが、実際には RMS ライセンスは Cisco Expressway-C で消費されます。この問題は X8.10 および CDETS CSCvf34525 の参照で明らかになりました。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：シスコは、Expressway の新機能を可能な限り迅速に提供することを目指しています。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。レビュー機能は使用できますが、**実稼働環境では使用を控えることを推奨します**（「プレビュー機能の免責事項、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 Expressway の機能については、下記の注意事項の最初にある「機能履歴表」に記載されています。

サポートされていない機能

- Expressway は DTLS の終端にはなりません。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。コールの保護には代わりに SRTP を使用します。Expressway 経由で DTLS コールを発信しようとすると失敗します。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。
- Expressway では、SIP UPDATE メソッド（RFC 3311）はサポートされていません。このメソッドに依存する機能は、想定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。これらについては、X8.11『*Cisco Expressway 経由の Mobile and Remote Access*』ガイドの「*Mobile and Remote Access でサポートされている機能とサポートされていない機能*」で詳しく説明しています。

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 経由の Mobile and Remote Access*』ガイドの「*前提条件*」セクションを参照するか、Cisco の担当者にお問い合わせください。

このリリースで新たに追加された制限事項、または以前のドキュメントに含まれていなかった制限事項は次のとおりです。

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 サービスの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、このシナリオでユーザ ログインの障害が発生します。

BiB 録音を含む MRA 接続経由の録音については、次の制限があります。

- 録音は、個人どうしの直接コールの場合にのみ機能し、会議では機能しません。
- 現在、サイレント モニタリング機能とウィスパー コーチング機能では、録音はサポートされていません。

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。各問題の解決方法など、詳細についてはアップグレード手順を参照してください。
  - 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、Expressway ソフトウェア バージョン X8.11.1 以降が必要です。以前のソフトウェア バージョンへのダウングレードが妨げられることはありませんが、以前のバージョンを実行しているアプライアンスはシスコのサポート対象外になります。
- 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、[高度なネットワーク（Advanced Networking）] オプションを使用すると、設定したイーサネット ポートごとに速度とデュプレックス モードを設定できます。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 以降、[システム（System）] > [管理設定（Administration settings）] ページ（[導入設定（Deployment Configuration）] リストから [中（Medium）] を選択）を使用して、システム サイズを手動で [中（Medium）] 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、『*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。CDETS CSCvf78728 を参照してください。

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 and 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（Configuration）] > [プロトコル（Protocols）] > [SIP] で、SIP の最大サイズを介して定義します。

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。

「シングル ドメイン」、および、Expressway-E が Microsoft フロント エンド サーバに「直接接続」している構成では、Microsoft ベースの SIP ネットワークと標準ベースの SIP ネットワークを別々に展開します（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などの理由から）。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

ファイアウォールを通過するように Expressway-E を連結する場合（X8.10 以降で設定可能）、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 に接続する場合は、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」各 Expressway-E について、（コールごとに）リッチ メディア セッション ライセンスが消費されます。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）に接続する場合は、チェーン内の「すべての」Expressway-E（トラバーサル ペアのオリジナルを含む）によって（コールごとに）リッチ メディア セッション ライセンスが消費されます。以前と同様に、元の Expressway-C はライセンスを消費しません。

OAuth トークン認証（Jabber）

Jabber ユーザの場合、いくつかの制限が存在し、自己記述トークンによる OAuth 認証が許容される唯一の認証方式として適用される場合があります。古いバージョンの Jabber 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引き続き認証できます。

Expressway 転送プロキシ

注意：現時点では、組み込みの Expressway 転送プロキシは、Cisco Unified Communications Manager や IM and Presence サービスでの使用には適しておらず、これらの製品ではサポートされていません。転送プロキシは Expressway のユーザ インターフェイスに表示されますが、使用しないでください。そのため、転送プロキシの導入を必要とする場合は、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（Configuration）**] > [**トラバーサル（Traversal）**] > [（**TURN**）]）。

相互運用性

テスト結果

この製品の相互運用性テスト結果は http://www.cisco.com/go/tp-interop に掲載されています。ここでは、他の Cisco TelePresence 製品の相互運用性テスト結果も確認できます。

注目すべき相互運用性の考慮事項

X8.7.x（および以前のバージョン）の Expressway 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、このバージョンの IM and Presence サービスにおける意図的な変更に起因するもので、Expressway X8.8 以降では対応する変更が加えられています。

継続的な相互運用性を確保するため、必ず IM and Presence サービス システムをアップグレードする「前に」Expressway システムをアップグレードしてください。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 ノード アドレス> 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 シリーズ保守および操作ガイド ページの『Cisco Expressway 管理者ガイド』では、Expressway サービスを同じ Expressway システムまたはクラスタ上で共存させることができることについて詳しく説明しています。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。

X8.11.4 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ついての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、X8.11.4 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 以降のソフトウェア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 X8.11.4 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 https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-release-notes-list.html で参照できます。

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。

X8.11.1 以降、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、X8.11.1 で導入された、すべてのソフトウェア インストールにおける一意の信頼のあるルートに起因します。

X 8.8 以降のバージョンは、以前のバージョンよりも安全性が高くなっています。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セキュア トラバーサル テストを試してください（[メンテナンス（Maintenance）] > [セキュリティ（Security）] > [セキュアトラバーサルテスト（Secure traversal test）]）。
  - ユニファイド コミュニケーション ノードで、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。TLS 検証モードを無効にすることは、たとえ失敗した展開を簡単に解決する方法となる可能性があっても、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 の順方向および逆方向ルックアップがありますか。

  バージョン X8.8 以降では、すべての 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、それらへの 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、MRA などの複雑な展開において、アップグレード後に予期したと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 検証は実行されず（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 タイプの以前の設定内容によっては Web インターフェイスのバナーに Expressway-C と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 ウィザードに移動し（[**ステータス（Status）**] > [**概要（Overview）**] ページ）、[**タイプ（Type）**] を [Expressway-E] に変更してから、システムを再起動してください。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た場合だけです。サービス セットアップ ウィザードを使用した場合には問題は発生しません。

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が適用されます。一部のバージョンの Unified CM、IM and Presence サービス、および Cisco Unity Connection には、CiscoSSL アップデートの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 コンフィギュレーション ガイド ページの「*Cisco Expressway 経由の Mobile and Remote Access*」を参照してください）。

IM and Presence サービス 11.5 は例外です。IM and 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。CDETS CSCvh97495 を参照してください。
  - TC7.3.11
  - CE8.3.3
  - CE9.1.2

注：X8.10.n 以降のバージョンでは、MRA 認証（アクセス制御）設定が Expressway-E から Expressway-C に移動し、デフォルト値が適用されるため、既存の設定を保持できません。システムを正常に動作させるため、アップグレード後に **Expressway のアクセス制御設定を再設定する必要があります。**アップグレード手順については後述します。

X8.7.x 以前を使用している環境と Cisco Unified Communications Manager IM and Presence Service 11.5（1）

X8.7.x（および以前のバージョン）の Expressway 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 Presence サービス ソフトウェアの前に、Expressway 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、30 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、「Cisco Webex ハイブリッド サービスのコネクタ ホスト サポート」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、31 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-E で、[設定（Configuration）] > [Unified Communications]> [設定（Configuration）] に移動し、[シングルサインオンのサポート（Single Sign-on support）] を探します。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（Single Sign-on support）] が [オン（On）] または [排他（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も控えておきます。
     - **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 の使用の許可（Allow Jabber iOS clients to use embedded Safari）**

クラスタ化システム

クラスタ化システムをアップグレードするには、Cisco Expressway シリーズ コンフィギュレーション ガイド ページの『*Expressway クラスタの作成およびメンテナンス導入ガイド*』に記載されているアップグレード手順を実行してください。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、「先にプライマリ ピアをアップグレード」してから、下位ピアを「一度に 1 つずつ順にアップグレード」することが不可欠です。

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 クラスタの作成およびメンテナンス導入ガイド*』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（Maintenance）] > [バックアップと復元（Backup and restore）]**）。
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. 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。
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（Status）] > [コール（Calls）]、[すべて選択（Select all）] をクリックし、[切断（Disconnect）] をクリックします）。
- 必要に応じて、自動的にクリアされない登録を手動で削除します（[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、[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（Maintenance）]> [アップグレード（Upgrade）]）。

   新しい「メジャー」リリースにアップグレードする場合（たとえば、X7.x から X8.x へ）、最初にシスコからの新しいリリース キーが必要です。このキーは、アップグレードプロセス中に必要です。

   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 を使用する場合は、次のセクションに進み、MRA アクセス制御の設定を再設定します。

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。

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 経由の Mobile and Remote Access を使用していて、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 アクセス制御の設定を再設定する必要があります。

1. Expressway-C で、**[設定（Configuration）] > [Unified Communications] > [設定（onfiguration）] > [MRA アクセス制御（MRA Access Control）] に移動します。**
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**（更新を伴う OAuth トークンによる承認）を設定する場合は、Unified CM ノードを更新します。[設定（Configuration）] > [Unified Communications] > [UC サーバタイプ（UC server type）] 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）] オプションの設定では、SAML SSO 認証への認証パスを設定す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 [モバイルおよびリモート アクセス（Mobile and 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 basicauthentication）]: 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ります。**他のケースでは使用しないでください。**	MRA をオンにするまでは [なし（None）] MRA をオンにした後は [UCM/LDAP]
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。	[オン（On）]
[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

フィールド	説明	デフォルト
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エッジ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が許可され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）

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** シスコ 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。 シスコ 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、シスコ 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。	–
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。この場合、アプリケーションは URL の OAuth トークンへアクセスできます。 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)

フィールド	説明	デフォルト
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（SSO mode）] : 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（SSO mode）] : X8.9 の [エクスクルーシブ（Exclusive）] は、X8.10 の 2 つの設定になります。 ▪ **認証パス**=*SAML SSO* ▪ **OAuth トークンによる承認**=*オン* [SSO モード（SSO mode）] : X8.9 の [オン（On）] は、X8.10 の 2 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）	[オン（On）]	–	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

オプション	アップグレード後の値	の前	の現在
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）

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

Bug Searth Tool 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. Web ブラウザを使用して、Bug Search Tool 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（Search）]** フィールドにバグ ID を入力し、**[検索（Search）]** 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（Search）]** フィールドに製品名を入力し、**[検索（Search）]** をクリックします。
2. 表示されるバグ リスト**の [フィルタ（Filter）]**ドロップダウン リストを使用して、[キーワード（Keyword）]、[変更日（Modified Date）]、[重大度（Severity）]、[ステータス（Status）]、または [技術（Technology）]のいずれかでフィルタ処理します。

Bug Search Tool のホーム ページで **[詳細検索（Advanced Search）]** 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 フィードで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、シスコ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。

シスコの新しい技術情報や改訂された技術情報を直接デスクトップで受信することをご希望の場合は、What's New in Cisco Product Documentation RSS feed にご登録ください。RSS フィードは無料のサービスです。

シスコの法的情報

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、情報と推奨事項は、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となります。

対象製品のソフトウェア ライセンスと限定保証は、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。

シスコが導入する 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を適応したものです。All rights reserved. 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とソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコ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、シスコおよびその供給者は、このマニュアルの使用または使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、あらゆる可能性がシスコ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 アドレスと電話番号は、実際のアドレスと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 トポロジ図とその他の図は、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 IP 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。

ハード コピーおよびソフト コピーの複製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。

シスコは世界各国 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 番号は当社の Web サイト（www.cisco.com/go/offices）をご覧ください。

シスコの商標

Cisco およびシスコ ロゴは、シスコ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。シスコの商標の一覧については、www.cisco.com/go/trademarks をご覧ください。記載されている第三者機関の商標は、それぞれの所有者に帰属します。「パートナー」という用語の使用はシスコ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）