Cisco Expressway X12.6.4

リリース ノート

First Published: 2020 年 6 月

Last Updated: 2020 年 10 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

Preface

変更履歴

表 1　リリース ノート変更履歴

日付	変更内容	理由
2020 年 10 月	メンテナンス リリースの更新。	X12.6.4
2020 年 10 月	メンテナンス リリースの更新。	X12.6.3
2020 年 8 月	メンテナンス リリースの更新。	X12.6.2
2020 年 7 月	ソフトウェアのダウングレード (サポート対象外) に関する問題について誤解を招くセクションを削除しました。	ドキュメントの訂正
2020 年 7 月	メンテナンス リリースの更新。OAuth トークン認証のエンドポイント要件も明確化。	X12.6.1
2020 年 6 月	初版。	X 12.6

対応プラットフォーム

表 2　Expressway プラットフォーム(このリリースでサポートされる)

プラットフォーム名	シリアル番号	ソフトウェア バージョンのサポート範囲
小規模 VM(OVA)	(自動生成)	X8.1 以降
中規模 VM(OVA)	(自動生成)	X8.1 以降
大規模 VM(OVA)	(自動生成)	X8.1 以降
CE1200 Hardware Revision 2(UCS C220 M5L にプレインストール)	52E1####	X12.5.5 以降。
CE1200 Hardware Revision 1(UCS C220 M5L にプレインストール)	52E0####	X8.11.1 以降。
CE1100(ExpresswayUCS C220 M4L にプレインストール)	52D#####	サポートが制限 (メンテナンスおよびバグ修正目的のみでの限られたサポートを除き、X12.5.9 以降ではサポートされません。新機能はサポートされていません。)
CE1000(ExpresswayUCS C220 M3L にプレインストール)	52B#####	サポート対象外(X8.10. x 以降)
CE500(ExpresswayUCS C220 M3L にプレインストール)	52C#####	サポート対象外(X8.10. x 以降)

VCS 製品サポートに関する通知

シスコは、Cisco TelePresence Video Communication Server(VCS) 製品の**販売終了日およびサポート終了日**を発表しました。詳細については https://www.cisco.com/c/en/us/products/collateral/unified-communications/telepresence-video-communication-server-vcs/eos-eol-notice-c51-743969.html [英語] をご覧ください。この通知は Cisco Expressway シリーズ製品には影響しません。

CE1100、CE1000、および CE500 アプライアンスのハードウェア サポートに関する通知

このセクションは、**ハードウェア** サポート サービスのみに適用されます。

CE500 および CE1000 アプライアンス - 撤回するハードウェア サービス サポートの事前通知

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ハードウェア 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。

CE1100 アプライアンス: 2018 年 11 月 13 日からの販売終了および撤回するハードウェア サービス サポートの事前通知。

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。今後のリリースでアプライアンス用のハードウェア サポート サービスを撤回します。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、「販売終了のお知らせ」を参照してください。

X12.6.x の機能履歴の概要

表 3　リリース番号別の機能

機能/変更	ステータス
MRA での複数のプレゼンスドメイン	X12.6.3 からサポート (以前のリリースではプレビュー ステータスとして利用可能)
カスタマイズされたアラーム ベースの電子メール通知のテスト ボタン	X12.6.3 以降でサポート
診断ロギング API	X12.6.3 以降でサポート
カスタマイズ可能なアラーム ベースの電子メール通知	X12.6.2 以降でサポート
MRA を介したウィスパーコーチング/ウィスパーアナウンスメント	X12.6.2 以降でサポート
MRA を介したエージェント グリーティング	X12.6.2 以降でサポート
アクティブな MRA 登録数の表示	X12.6.1 以降でサポート
MRA を介したサイレント モニタリング	X12.6.1 以降でサポート
セキュリティ機能の拡張	X12.6 以降でサポート
スマート ライセンス	X12.6 以降でサポート
オプション キーではなく UI 設定による、タイプおよびシリーズの設定	X12.6 以降でサポート
アラームベースの電子メール通知	X12.6 以降でサポート
ハードウェア セキュリティ モジュール(HSM) のサポート	プレビュー
IM&P 用の Android プッシュ通知パブリッシャー	プレビュー (X12.6.2 からはデフォルトで無効化)
Cisco Contact Center のヘッドセット機能	プレビュー
Expressway 転送プロキシ	X12.6.2 から削除
Smart Call Home	X12.6.2 から削除
Advanced Media Gateway	X12.6 から削除

撤回または廃止された機能とソフトウェア

Expressway 製品セットは見直しが続けられており、機能が製品で取り消しまたは廃止され、機能のサポートが以降のリリースで取り消されることが示される場合があります。この表は、現在廃止済みステータスである機能または X12.5 以降で取り消された機能の一覧です。

表 4　廃止および取り消された機能

機能/ソフトウェア	ステータス
Cisco Jabber Video for TelePresence(Movi) 注 : Cisco Jabber Video for TelePresence(ビデオ通信用に Cisco Expressway と連携して動作) 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 ソフトウェア クライアントとは関連していません。	非推奨メソッド
Findme デバイス/ロケーション プロビジョニング サービス: Cisco TelePresence FindMe/Cisco TelePresence Management Suite プロビジョニング拡張機能 (Cisco TMSPE)	非推奨メソッド
Expressway Starter Pack	非推奨メソッド
Smart Call Home のプレビュー機能	X12.6.2 で取り消し済み
Expressway 組み込み転送プロキシ	X12.6.2 で取り消し済み
Cisco Advanced Media Gateway	X12.6 で取り消し済み
VMware ESXi 仮想ハードウェア バージョン ESXi5.x(VM ベースの展開)	X12.5 で取り消し済み

関連資料

表 5　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 Expressway 構成手順については、「Expressway/VCS スクリーンキャスト ビデオ リスト」ページにあります。
仮想マシンのインストール	*Expressway 設置ガイド* ページの『Cisco Expressway 仮想マシン設置ガイド』
物理アプライアンスのインストール	*Expressway 設置ガイド* ページの『Cisco Expressway CE1200 アプライアンス設置ガイド』
レジストラ / 単一システムの基本設定	*Expressway 構成ガイド* ページの『Cisco Expressway レジストラ導入ガイド』
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 シリーズ 構成ガイド* ページの『Cisco Expressway-E および Expressway-C 基本設定導入ガイド』
管理およびメンテナンス	*Expressway シリーズメンテナンスおよび操作ガイド* ページの『Cisco Expressway 管理者ガイド』 *Cisco Expressway シリーズメンテナンスおよび操作ガイド* ページの『Cisco Expressway 保守ガイド ページ』
クラスタ	*Expressway 構成ガイド* 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	*Cisco Expressway シリーズ構成ガイド* ページの『*Cisco Expressway 証明書の作成と使用に関する導入ガイド*』
ポート	*Expressway 構成ガイド* ページの『*Cisco Expressway IP ポートの使用構成ガイド*』
ユニファイド コミュニケーション	*Expressway 構成ガイド* ページの『*Cisco Expressway 経由のモバイルおよびリモート アクセス*』
Cisco Meeting Server	*Expressway 構成ガイド* ページの『*Cisco Expressway による Cisco Meeting Server 導入ガイド*』 *Cisco Meeting Server プログラミングガイド* ページの『*Cisco Meeting Server API リファレンスガイド*』 その他の Cisco Meeting Server ガイドは、Cisco Meeting Server 構成ガイド ページから参照できます。
Cisco Webex ハイブリッド サービス	ハイブリッド サービス ナレッジ ベース
Cisco Hosted Collaboration Solution (HCS)	HCS のお客様用マニュアル
Microsoft インフラストラクチャ	*Expressway 構成ガイド* ページの『*Cisco Expressway with Microsoft Infrastructure 導入ガイド*』 *Expressway 構成ガイド* ページの『*Cisco Jabber and Microsoft Skype for Business Infrastructure Configuration Cheatsheet*』
REST API	Expressway コンフィギュレーション ガイド ページの『Cisco Expressway REST API サマリー ガイド』(API が自己文書化されている高レベル情報のみ)
MultiWay 会議	*Expressway 構成ガイド* ページの『*Cisco TelePresence Multiway 導入ガイド*』

Cisco Expressway のライセンスについて

Cisco Expressway X12.6 以降では 2 つのライセンス モードがサポートされます。

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

スマート ライセンスを使用すると、お客様が自社の Expressway ノードまたはクラスタからライセンスを使用する柔軟性が得られます。これに対し、従来の PAK ベースのライセンスでは、個別のノードまたはクラスタに対してライセンスが固定されます。

任意の Expressway ノードまたは Expressway クラスタで任意の時点でサポートされるライセンス モードは 1 つだけです。

Expressway は、デフォルトでは PAK ベースのライセンスに設定されています。スマート ライセンスへの切り替えは Web インターフェイスから実行します([メンテナンス(Maintenance)] > [スマート ライセンス(Smart licensing)]) 。PAK に戻すには初期設定へのリセットが必要です。

PAK ベースのライセンス モードとスマート ライセンス モードの両方で、以下のオプションがサポートされます。ライセンス登録ポータルで、これらの PAK ベースのオプションをスマートに変換できます。

表 6　両方のライセンスモードでサポートされるオプション キー

PID	キー	オプション
LIC-EXP-RMS*	116341Yn-m-########	リッチ メディア セッション ライセンス
LIC-EXP-DSK (LIC-EXP-DSK-EA を含む)	116341Bn-m-########	Expressway デスクトップ システム登録ライセンス/UC Manager の Enhanced ライセンス
LIC-EXP-ROOM (LIC-EXP-ROOM-EA を含む)	116341An-m-########	Expressway ルーム システム登録ライセンス/UC Manager TP ルーム ライセンス

* LIC-EXP-RMS-CPW、LIC-EXP-RMS-HCS、LIC-EXP-RMS-MIG、LIC-EXP-RMS-PMP、LIC-EXP-RMS-EA、および LIC-EXP-RMS= を含む

以下のキーは、Expressway X12.5.4 以降では必要ありません。この機能はデフォルトで有効になっています。PAK ベースのライセンス モードで実行している場合は必要ありませんが、キーを適用しても問題ありません。**スマート ライセンス モードでは、この機能はデフォルトで有効になっているため、キーは必要ないかまたはサポートされません。また、**ライセンス登録ポータルで変換できない場合があります。

表 7　いずれのライセンスモードでも不要なオプションキー

PID	キー	オプション
LIC-SW-EXP-K9	16 桁の数	リリース キー(Release Key)
LIC-EXP-SERIES	116341E00-m-########	Expressway シリーズ
LIC-EXP-TURN	116341In-m-########	TURN リレー ライセンス(Expressway-E のみ)
LIC-EXP-E	116341T00-m-########	トラバーサル サーバ機能 (Expressway-E のみ)
LIC-EXP-GW	116341G00-m-########	インターワーキング ゲートウェイ機能
LIC-EXP-AN	116341L00-m-########	高度なネットワーキング機能 (Expressway-E のみ)

以下のキーを使用する場合は、この機能はスマートライセンスモードではまだサポートされていないため、**PAK ベースのライセンスからスマートライセンスモードに切り替えないでください**。

表 8　現在 PAK ベースモードでのみサポートされているオプション キー

PID	キー	オプション
LIC-EXP-JITC=	116341J00-m-########	高度なアカウントのセキュリティ機能
LIC-EXP-HSM	116341H00-m-########	ハードウェア セキュリティ モジュール機能 (現在はプレビュー ステータスのみ)
LIC-EXP-MSFT	116341C00-m-########	Microsoft 相互運用性

スマート ライセンスの仕組み

スマート ライセンスは、複数のシスコ製品で利用できます。ライセンスを簡素化し、ライセンス所有権と使用量を明確にします。デバイスは、ライセンス消費を自己登録およびレポートするため、オプション キー(製品アクティベーション キー) を使用する必要がなくなります。ライセンスの付与は 1 つのアカウントにプールされているため、Expressway または Expressway の複数のクラスタにわたって使用できます。会社が所有しているすべての互換性のあるデバイスでライセンスを使用して、組織のニーズに合わせてライセンスを移動することができます。

スマート ライセンスを使用して、CSSM(または Smart Software Manager オンプレミス) でのユーザの登録 / 登録解除を行い、ライセンスの使用状況、カウント、ステータスを表示し、ライセンスの承認を更新できます。

CSSM は Cisco Software Manager でホストされており、製品インスタンスで登録およびライセンスの消費をレポートできるようにします。

オンプレミスのアプローチ - Smart Software Manager オンプレミスの使用

ポリシーまたはネットワーク可用性のために、Cisco Smart Software Manager を使用したシスコ製品の直接管理を希望されない場合は、Smart Software Manager オンプレミスを利用できます。Cisco Smart Software Manager と同じ方法で、製品登録およびライセンス消費の報告は Smart Software Manager オンプレミスに対して行います。

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

- 接続済み。cisco.com への直接接続がある場合に使用されます。スマート アカウントの同期が自動的に実行されます。
- 切断済み。cisco.com への直接接続がない場合に使用されます。ファイルのアップロード/ダウンロードによりサテライトを Cisco SSM と同期可能

スマート ライセンスの重要な設定情報

注意 : スマートライセンスをオンに設定した後に、Web インターフェイスを使用してオフに戻すことはできません。PAK ベースのライセンスに戻すには(またはシステムを VCS に変更するには) 、工場出荷時の状態へのリセットが必要です。リセットによってソフトウェア イメージが再インストールされ、Expressway の設定がデフォルトにリセットされるので、スマート ライセンスを有効にする前に、Expressway のデータのバックアップを作成することを強く推奨します。

- スマート ライセンスを有効にした後は、お使いの Expressway でオプション キーを使用することはできません。つまり、高度なアカウント セキュリティ、ハードウェア セキュリティ モジュール(HSM) 、または Microsoft 相互運用性を使用するために(または、RMS やルーム / デスクトップの登録用のライセンスを追加するために) 、オプション キーは適用できません。
- Expressway で HSM デバイスを展開したい場合は、現在スマート ライセンスを使用することはできません。
- Expressway 製品インスタンスの登録の際に登録サーバで通信の問題が発生すると、登録が失敗して次のようなメッセージが表示されます。**次の理由により、スマート ソフトウェア ライセンスの登録の前回の試行が進行中です: HTTP サーバエラー: 操作タイムアウト** `(The last attempt to renew smart software licensing registration is in progress because of the following reason: HTTP Server Error 200: Operation timed out)`。

  製品インスタンスは、15 分間隔で再登録を試みます。現在の登録ステータスを確認するには、再試行するたびにページを最新の情報に更新します。再試行中に通信の問題が解決した場合は、製品が登録されます。製品が複数回の再試行後に登録されない場合は、登録サーバに何らかの通信問題があるかどうかを確認し、手動で製品インスタンスを再登録します。

- システムを復元する場合、復元されるスマート ライセンス設定は、バックアップを同じシステムに復元するか、あるいは別のシステムに復元するかによって異なります。
  - 同じシステムに復元する場合は、スマート ライセンスが有効になり、復元されたシステム上で登録設定が復元されます。
  - 別のシステムに復元する場合は、復元されたシステム上でスマート ライセンスが有効になりますが、登録キーを使用して製品を再度登録する必要があります。

詳細の表示

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

スマートライセンスの設定方法の詳細については、*Expressway 管理者ガイド*を参照してください。

H.323-SIP インターワーキング用 DH キー長さの X12.6.4

の設定の変更

この変更は、ExpresswayH.323-SIP インターワークコール(バグ ID CSCvv92477 参照) で使用する場合に適用されます。

X12.6では、Expressway のセキュリティ強化の一環として、H.323 コール暗号化用 2048 ビット Diffie-Hellman キーのサポートを導入しました。そのため、Expresswayデフォルトの動作として、1024 ビットと 2048 ビットの暗号キーの長さを提供します。これにより、展開されたファイアウォールの ALG 機能またはエンドポイントが、Diffie-Hellman キー交換の新しいオファー(1024 ビットと 2048 ビットの両方) を処理できなかった場合に、予期しない H.323 呼び出しエラーが発生しました。

X12.6.4 から、H.323-SIP インターワーキングのデフォルトの暗号化は 2048 ビット/1024 ビットのままですが、この新しい CLI コマンドで、管理者に 1024 ビット暗号化に戻すオプションが提供されています。

xConfiguration インターワーキング暗号キーサイズ 2048: <オン/オフ>

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

X12.6.3 での変更

アラーム ベースの電子メール通知のテスト ボタン

[メンテナンス(Maintenance)] > [電子メール通知(Email Notifications)] ページの新しい [今すぐテストする(Test Now)] ボタンにより、特定のアラームの通知電子メールが期待通り受信されるのを確認できます。

MRA での複数のプレゼンスドメイン

この機能は以前はプレビュー ステータスでしたが、X12.6.3 以降でサポートされています。IM and Presence Service 10.0.x 以降の場合、互換性のあるクライアントを、ユーザ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に展開できます。

Unified Communications のデフォルトの展開では、ドメインを 75 以下にすることをお勧めします。

注: Expressway 経由の XMPP/チャット &プレゼンス フェデレーションでは、XMPP フェデレーションが**単一の Expressway クラスタ**上でのみサポートされるという既存の要件が引き続き適用されます。これは、この変更の影響を受けません。

診断ロギング用の新しい API

診断ロギングのスナップショットを有効化、無効化、および収集するために API コマンドを使用できるようになりました。

仮想システム - 小規模 VM 向けの ESXi 6.7 アップデート 3 認定

ESXi 6.7 アップデート 3 バージョンは、小規模 VM での Expressway のホストについて正常にテストされています(X12.6.1 以降、中規模および大規模 VM でサポートされています) 。

X12.6.3 での MRA マニュアルの拡張

*Expressway MRA 導入ガイド*は、次の新しいトピックで更新され、拡張されました。

- *マルチドメインのシナリオ*–複数ドメイン環境に複雑なトポロジを導入する際に顧客を支援するために設計された概要、図、および構成のサマリー。
- *複数クラスタのシナリオ*–構成のヒントと複数クラスタのシナリオに関する要件を示すベストプラクティス セクション。
- *セキュリティ要件*– Mobile & Remote Access を導入する Unified CM のセキュリティ前提条件を明確に示します。

また、次のセクションの更新と編集も含まれます。

- コール録音とサイレント モニタリングのサポート
- キー拡張モジュールのサポート
- サポート対象クライアント
- サポートされるエンドポイント

X12.6.3 でのその他の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。
- このメンテナンスリリースの未解決および解決済みの問題, ページ 21の検索リストが更新されました。

X12.6.2 での変更

カスタマイズ可能なアラーム通知

X12.6.2 から、特定のアラーム ID の通知を特定の電子メール アドレスに送信するか、特定のアラーム ID の通知を無効にするように、アラーム ベースの電子メール通知機能を構成できます。たとえば、指名された個人にしきい値警告アラームを送信したり、不要なアラームによる通知を停止したりする(アクションを*無効*に設定する) ことができます。これまでは、特定の重大度のアラームはすべて同じ接続先に送信される必要がありました。Expressway 管理者ガイドで説明しているように、この機能は **[メンテナンス (Maintenance)] > [電子メール通知 (Email Notifications)]** ページの [カスタム通知 (Custom notifications)] 設定で構成します。

注 : X12.6.2 以降、宛先電子メール ID は 254 文字以内である必要があります。

MRA を介したウィスパーコーチングとウィスパーアナウンスメントのサポート

この項目は、MRA を展開する場合に適用されます。X12.6.2 から、Expressway は、展開された Unified Communications 製品が互換性のあるバージョンを実行していることを条件として、互換性のある MRA 接続エンドポイント向けのウィスパーコーチング/ウィスパーアナウンスメント機能をサポートします。

MRA を介したエージェント グリーティングのサポート

この項目は、MRA を展開する場合に適用されます。X12.6.2 から、Expressway は、展開された Unified Communications 製品が互換性のあるバージョンを実行していることを条件として、互換性のある MRA 接続エンドポイント向けのエージェント グリーティング機能をサポートします。

MRA を介した Android PUSH がデフォルトで無効になっている

IMP メッセージング用のプッシュ通知を、MRA 接続 Android デバイスに拡張する Expressway X12.6 の最近のプレビュー機能は、X12.6.2 ではデフォルトでは無効になっています(Apple プッシュ通知は影響を受けしません) 。これは、Cisco Jabber for Android 12.9 以降を使用する展開の予期しない結果 (バグ ID CSCvv12541) が原因です。

IM and Presence サービスがバージョン 12.5(1)SU3 以降で実行されている場合は、Expressway コマンド ライン インターフェイスでこの機能を手動で有効にできます。方法については、「このバージョンで特に重要な問題, ページ 21を参照してください。

ユーザインターフェイスから削除されたサポートされていない機能 (継続中)

使いやすさと一貫性を向上させるために、廃止された項目を Expressway ユーザインターフェイスから削除しています。次の機能は、X12.6.2 から削除されます。

- Smart Call Home(SCH) のプレビュー機能
- 組み込み転送プロキシ

X12.6.2 でのその他の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。
- このメンテナンスリリースの未解決および解決済みの問題, ページ 21の検索リストが更新されました。

X12.6.2 のお客様向けマニュアルの機能拡張

簡単に参照できるように、『*Expressway 保守ガイド*』に以前記載されていた情報を『*Expressway 管理者ガイド*』の「有用性、ロギング、監視およびメトリック」の章に移動しました。

『*Expressway 管理者ガイド*』の診断およびトラブルシューティング情報が再編されました。

X12.6.1 での変更

アクティブな MRA 登録数の表示

この項目は、ExpresswayExpressway を使用して Cisco Unified Communications モバイルおよびリモートアクセス(MRA) を展開する場合に適用されます。X12.6.1 以降では、MRA を介して現在登録されている SIP デバイスに関する使用状況情報が Expressway-E に表示されます。(該当する Expressway に対して MRA サービスを有効にする必要があります) 。この情報は、[ステータス(Status)] > [概要(Overview)] ページの [MRA 登録(MRA Registrations)] セクションで確認でき、現在のアクティブな MRA デバイス数と、Expressway が最後に再起動した時点以降の MRA 登録の最大数が表示されます。

この情報は、CLI で ResourceUsage xStatus 要素を使用して取得できます。システムメトリックの収集が有効である場合は([メンテナンス(Maintenance)] > [ロギング(Logging)]) 、Expressway が収集する統計にもこの情報が含まれます。

MRA を介したサイレント モニタリングのサポート

この項目は、MRA を展開する場合に適用されます。X12.6.1 以降、展開された Unified Communications 製品が互換性のあるバージョンを実行していることを条件として、Expressway は互換性のある MRA 接続エンドポイント向けのサイレント モニタリング機能をサポートします。

Expressway TURN は STUN サーバとして動作しない

X12.6 でのセキュリティ強化により、Expressway-E TURN サーバは汎用 STUN サーバとして動作しなくなり、認証されていない STUN バインド要求を受け入れません。以下のいずれかの項目を展開する場合は、この変更の結果として発生する可能性のあるコールの失敗について、「制限事項」セクションを参照してください。

- Microsoft との相互運用性を目的とした TURN クライアントとしての B2BUA。
- Cisco Meeting Server WebRTC。

ソケット プロセスの修正

X12.6.1 には、バグ ID CSCvt55506 ソケット プロセスによる CPU 使用率の上昇(Socket process causing High CPU) に対する修正が含まれます。このバグの回避策を以前に実装した場合は、必要であれば EPOLL モードを再び使用するように Sockhandler を設定し直すことができます。これを行うには、次のコマンドを実行します。

1. *xConfiguration Sockhandler EPOLL Mode: "On"*
2. *xCommand Restart*

X12.6.1 でのその他の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。
- このメンテナンスリリースの未解決および解決済みの問題, ページ 21の検索リストが更新されました。
- ESXi 6.7 アップデート 3 バージョンで、Expressway の中規模 VM および大規模 VM のホスティングに関するテストが正常に完了しました。

X12.6 の機能と変更点

セキュリティの強化

このリリースでは、継続的なセキュリティ機能拡張の一部として、さまざまなセキュリティ関連の機能向上が適用されています。この大部分はバックグラウンドで動作しますが、次のように、ユーザ インターフェイスに影響を与える変更もあります。

- ランダムの安全なパスフレーズを、パスワードの代わりに生成するための新しいオプション。生成されたパスフレーズでの最小のエントロピーのビットの数は、[**パスワード セキュリティ (Password Security)**] ページから設定できるようになりました。
- 「禁止パスワード」ディクショナリを設定するための新しいオプションが [ユーザと禁止パスワード (User & Forbidden password)] ページから利用できます。
- クラスタからピアを削除した後に、自動リセットによって証明書とキー情報が削除されるようになりました。詳細についてはこの通知で後述します。
- *Cisco インターセクション CA バンドル*の一部として、2 つの信頼されたルート CA がインストールされています。
  - O=Internet Security Research Group, CN=ISRG Root X1
  - O=Digital Signature Trust Co., CN=DST Root CA X3
- HSM のサポート (プレビューベースでのみ) 。

UI 設定によるシリーズの設定 - シリーズのオプション キー(PAK ベースのライセンス) を使用しない

この変更は、(Cisco VCS ではなく) Cisco Expressway シリーズのみをサポートする CE1200 シリーズ以降のハードウェアに搭載された、アプライアンスベースのシステムには該当しません。

X12.6 からは、*Expressway シリーズ*のオプション キーが廃止され、そのキーを使用して Cisco Expressway シリーズ システムを Cisco VCS に変更したり、その逆を行ったりはできません。何らかの理由で、X12.6 以降を実行しているシステムを Cisco VCS または Cisco Expressway シリーズズ製品に変更する必要がある場合は、サービスの選択ページで [シリーズの選択 (Selece Series)] 設定を使用します。このページは、インストール時に [サービスのセットアップウィザード (service setup wizard)] からアクセスできます。また、後からいつでも [**ステータス >概要 (Status > Overview)**] で行えます。オプション キーのメニューにキーを適用しようとすると、サービスの選択ページにリダイレクトされます。

システムでスマート ライセンスを使用している場合、ユーザインターフェイスを使用して Cisco Expressway シリーズから Cisco VCS に変更することはできません。唯一の方法は、初期設定にリセットしてから VCS ソフトウェアのイメージをインストールすることです。

UI 設定によるタイプおよびロールの設定 - 非トラバーサル サーバのオプション キー

X12.6 以降では、*トラバーサル サーバ*のオプション キーは廃止され、システムを Cisco Expressway-E 製品タイプに変更するためにこのキーは必要なくなります。その代わりに、サービス選択ページの [タイプの選択 (Select Type)] 設定を使用します(この設定には、インストール時にサービスのセットアップウィザードからアクセスするか、それ以降はいつでも [ステータス(Status)] > [概要 (Overview)] からアクセスできます) 。オプション キーのメニューにキーを適用しようとすると、サービスの選択ページにリダイレクトされます。

クラスタ システムの場合は、各ピアの [**タイプの選択 (Select Type)**] の設定を個別に適用します。ウィザードにはクラスタ内の他のピアは表示されません。現在設定されているピアだけが表示されます

タイプ設定を CLI から変更することはできません。

X12.6 以降のリリース キー、オプション キー、および一般的なライセンス

このセクションでは、X12.6 におけるライセンス、リリース キー、およびオプション キーに関する重要なポイントをまとめています。一部は X 12.6 の新機能であり、一部は以前のリリースで最近行われた変更点です。ここでは便宜上再度紹介します。

- Cisco Expressway シリーズ製品では、X8.6.x 以降のソフトウェア上のシステムを X12.6.x ソフトウェアにアップグレードするためにリリース キーを使用する必要はありません(変更は X12.5.4 で導入されています) 。Cisco VCS 製品では、すべてのソフトウェア アップグレードにリリースキーを引き続き必要とします。
- 必要に応じて、Cisco Expressway シリーズ製品にスマート ライセンスを使用することもできます(Cisco VCS 製品では利用できません) 。このトピックについては、Cisco Expressway のライセンスについて, ページ 9 ページ) で説明しています。
- オプション キーは、スマート ライセンスを使用する Expressway システムで使用することはできません。オプション キーの機能の使用は PAK ベースのシステムでは徐々に減少していますが(ライセンス オプション キーが未変更) 、次の Expressway 機能には引き続きオプション キーが必要です。次のいずれかの機能を使用する場合は、PAK ベースのライセンスを使用してください。
  - 詳細アカウント セキュリティ
  - HSM(ハードウェア セキュリティ モジュール)
  - Microsoft 製品との相互運用性
- これまでオプションキーを使用していたのは、システム(つまり Cisco Expressway シリーズまたは Cisco VCS) およびそのタイプ(「-E」または「-C」のロール) のシリーズを設定するためです。これらの機能は、Web UI の設定によって管理されるようになりました。また、次の関連オプションキーは使用されなくなりました。
  - *Expressway シリーズ*
  - *トラバーサル サーバ(Traversal Server)*

  この変更は、CE1200 アプライアンスベースの Expressway に対してすでに実装されており、X12.6 以降では VM システムにも適用されます

アラームベースの電子メール通知

生成されたアラームとそのアラームの重大度に基づいて、電子メール通知をメインの連絡先に設定できるようになりました。最新の『*Expressway 管理者ガイド [英語]*』では、新しい Web UI ページの**保守 > 電子メール通知 (Maintenance > Email Notifications)**を通して通知を設定するために必要な設定について説明しています。

米国内では、この機能は、連邦通信委員会に義務付けられている最近の「Kari's Law」にも適用されます。このためには、複数回線の電話システムが必要であり、直接 911 への通話(プレフィックスなし) を可能にして、そのような通話を中央のコンタクト ポイントに通知する必要があります。Expressway では、要件の最初の部分(直通ダイヤル) がバージョン X12.5.7 からサポートされていました。バージョン X12.6 以降の Expressway では、ユーザが 911 コールを開始した場合に中央の連絡先への電子メール通知もサポートされます。これは、米国における 911 緊急コールの発信を含め、PSTN コールを可能にする B2B 環境に Expressway と共にゲートウェイを導入する場合に適用されます。

新しいアラーム ID 90001 は、Expressway を通じた 9-1-1 ダイヤルの基準を満たす、米国での緊急コールに使用されます。このアラームの重大度は*緊急*に分類されています。

(プレビュー) ハードウェア セキュリティ モジュール(HSM) のサポート

プレビューとしてのみ、X12.6 は HSM 機能のための Expressway のサポートを導入しています。

注 : プレビュー HSM デバイス(nShield CONNECT XC) が、X12.6 リリースのしばらく後に利用可能になります。

HSM は、強力な認証のためにデジタル キーを保護および管理し、アプリケーション、ID、およびデータベースで使用する暗号化、暗号解読、および認証などの重要な機能に対して crypto プロセスを提供します。HSM デバイスは、コンピュータまたはネットワーク サーバに直接接続するプラグイン カードまたは外部デバイスとして提供されます。これにより、アラームを出したり HSM を動作不能にしたりすることによって、ハードウェアおよびソフトウェアの改ざんを防ぐことができます。

新しい **[保守 (Maintenance)] > [セキュリティ(Security)] > [HSM 構成 (HSM configuration)]** ページが、Expressway の Web ユーザインターフェイスに追加されました。

Expressway では、現時点では、nShield Connect が HSM プロバイダーとして(プレビューで) サポートされています。設定手順と注意する必要があるいくつかの重要な警告と制限事項については、「付録 1: Expressway での HSM デバイスの構成 , ページ 38で詳細に説明します。

重要 :「SafeNet Luna」ネットワークデバイスは、ユーザインターフェイスでも参照されていますが、**このデバイスは、現在 Expressway ではサポートされていません 。**

(プレビュー) Cisco Contact Center のヘッドセット機能 : MRA 展開

この機能は、Mobile & Remote Access(MRA) を使用して Expressway を導入する場合に該当します。これは現在プレビュー ステータスで提供されています。

新しいデモンストレーション ソフトウェアにより、互換性のあるシスコ ヘッドセットに一部の Cisco Contact Center 機能が提供されるようになりました。X12.6 からは、関連するエンドポイント、ヘッドセット、または Unified CM で必要なソフトウェア バージョンが実行されている場合は、Expressway が自動でこれらのヘッドセットの新機能をサポートします。この機能は Unified CM インターフェイスから有効になっており、Expressway でのユーザによる設定は必要ありません。

詳細については、ホワイト ペーパー「*Cisco Headset and Finesse Integration for Contact Center*」(https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/cucm/whitePaper/CUCM_Headsets_for_ContactCenter_WP.pdf) をご覧ください。

(プレビュー) IMP メッセージ機能を Android デバイスに拡張するプッシュ通知 - MRA 展開

この機能は、Mobile & Remote Access(MRA) を使用して Expressway を導入する場合に該当します。X12.6 では、外部の製品バージョンの依存関係によって、プレビュー のステータスのみで提供されます。現在、この機能はデフォルトでオフになっています (「このバージョンで特に重要な問題, ページ 21」(1 ページ) を参照) 。

デモンストレーション用の UC ソフトウェアが Android デバイスへのプッシュ通知をサポートするようになりました。関係するデバイス、Unified CM、IM and Presence サービスが必要なソフトウェアバージョンを実行している場合、Expressway は、x12.6 からのサポートも含めて、これらの新しいプッシュ機能を自動的にサポートします。Expressway での設定は一切不要です。この機能には、次のソフトウェアのバージョン以降が必要です。

- Unified CM バージョン 12.5(1) SU3 またはバージョン 14 - 11.5(1) SU8 では未サポート
- IM and Presence Service 12.5(1)SU3 またはバージョン 14 - 11.5(1)SU8 ではサポートされていません
- Expressway X12.
- Cisco Jabber 12.9

(プレビュー) 互換性のある電話機の KEM サポート - MRA 展開

Cisco IP 電話 8800 シリーズのデバイス用のキー拡張モジュール(KEM) アクセサリ向けに、MRA を正式にはテストおよび検証していません。ただし、私たちは実験条件の下で、複数の DN を持つ KEM が MRA で満足できる程度に動作していることを確認しています。これらは公式なテストでは**ありません**が、COVID-19 危機管理の観点では、この情報は、サポートされていないプレビュー機能を使用することを希望するお客様にとって有用となっています。

SIP パス ヘッダーは、Expressway で有効にする必要があります。また、パス ヘッダーをサポートする Unified CM ソフトウェア バージョンが必要です(リリース 11.5(1) SU4 またはそれ以降を推奨) 。

クラスタからピアが削除された場合、工場出荷時の状態へのリセットによりセキュリティ情報が削除される

バージョン X12.6 から、ピアをクラスタから削除した後にピアを再起動すると、工場出荷時の状態へのリセットによってピアから次の情報も削除されます。

- サーバ証明書
- 証明書に関連付けられた秘密キー
- 保存された CA 信頼ストア

注 : この変更は、クラスタからピアを削除するために自動的にトリガーされる工場出荷時リセットにのみ適用されます。この場合、情報は必ず削除されます。ユーザインターフェイスから手動で行う工場出荷時の状態へのリセットの場合は、情報を保存するようにするオプションもあります。

CE1100 ハードウェア製品での本リリースの部分的サポート

COVID-19 による危機への対応のため、この X12.6 リリースの部分的なサポートは、(Cisco VSC ではなく) Cisco Expressway システムとして動作している、Cisco CE1100 アプライアンス用に提供されています。X12.6 以降の新機能は、CE1100 ではサポートされていません。ただし、CE1100 では、保守およびバグ修正目的でのみ、X12.6 がサポートされています。

ユーザインターフェイスから削除されたサポートされていない機能 (継続中)

使いやすさと一貫性を向上させるために、廃止された機能をユーザインターフェイスから削除しています。リリースごとの詳細は、撤回または廃止された機能とソフトウェア, ページ 7

仮想化システム - プロファイル情報がバックアップから削除

X12.6 から、Expressway バックアップファイルにはシステムプロファイル情報 (ProfileID 値) は含まれません。これは、異なる規模の展開でバックアップを復元した場合に、予期しないサイズへの変更に関する既知の問題を回避するためです。Bug ID CSCvs59766 を特定します。

仮想化システム - ESXi 6.0 の一般的なサポートの終了

この項目は、仮想化された Expressway システムに適用されます。VMware ESXi 6.0 仮想ハードウェア製品 (vSphere 6.0 を含む) は、2020 年 3 月から一般的なサポートが終了していることに注意してください。詳細については、VMware による通知を参照してください。

今回のリリースでのその他の変更点

コラボレーション ソリューション アナライザー ツールへのリンク

診断ロギング ページの新しい [**ログの分析 (Analyze log)**] ボタン (**[保守 (Maintenance)] > [診断 (Diagnostics)]**) を選択すると、コラボレーション ソリューション アナライザーのトラブルシューティング ツールへのリンクが開きます。

アラームとバナーの変更

- [*緊急 (Emergency)*] アラームの新しいカテゴリ。
- X12.6 またはそれ以降のソフトウェアが、サポートされていない CE ハードウェアアプライアンスにインストールされている場合、[準拠していないハードウェア (Non-compliant hardware)] メッセージが表示されるようになりました。

X12.6 でのお客様向けマニュアルの変更

Web ユーザインターフェイスからの Expressway のアップグレードに関する一部の手順は、以前は『*Expressway 管理者ガイド*』、『*クラスタの作成とメンテナンス ガイド*』、リリース ノートに記載されていました。すべての手順をこのノートの 1 つの場所にまとめました。

一部のキャパシティ情報は、以前は *Expressway 管理者ガイド [英語]* および *クラスタ作成とメインテナンス ガイド (Cluster Creation and Maintenance Guide)* に記載されていました。現在は、管理者ガイドにのみ記載されています。

Expressway 管理者ガイド [英語] には、次を含む細かい修正と改良があります。

- レイアウトと見出しの改善。
- ソフトウェアのダウンロード用 tar ファイルの名前の変更要件の明確化。
- デュアル ネットワーク インターフェイスが Expressway-E でのみサポートされていることの記述。

REST API への変更点

リモート構成を簡素化にするために、Expressway 用 REST API を使用できます。たとえば、Cisco Prime Collaboration Provisioning などのサードパーティのシステムなどがあります。新機能が追加される際には、構成、コマンド、およびステータス情報

に対する REST API アクセスを追加しますが、以前のバージョンの Expressway で導入された一部の機能に対しても REST API を選択的に後付けしています。

この API は、RAML を使用して自己記述されており、`https://<ip address>/api/raml` で RAML の定義にアクセスできます。API へのアクセス方法と使用方法の概要は、Expressway 設置ガイドページの『*Cisco Expressway REST API サマリー ガイド*』、VCS 構成ガイドページので説明しています。

構成 API	API が導入されたバージョン
Diagnostic Logging	X12.6.3
スマートライセンシング	X 12.6
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

未解決および解決済みの問題

バグ検索ツールのリンク

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)
- X12.6.4 で解決済みの問題
- X12.6.3 で解決済みの問題
- X12.6.2 で解決済みの問題
- X12.6.1 で解決済みの問題
- X12.6 で解決済みの問題

このバージョンで特に重要な問題

IMP メッセージ機能を Android デバイスに拡張するプッシュ通知 CSCvv12541

Android PUSH を MRA コネクテッド デバイスに拡張する X12.6 プレビュー機能には既知の問題が存在します。その結果、この機能は現在、デフォルトで無効になっています(X12.6.2 から)。これは、Expressway コマンドライン インターフェイスから手動で有効にすることができますが、**Android ユーザにサービスを提供しているすべての IM & Presence サービス ノードがバージョン 12.5(1)SU3 以上を実行している場合**にのみ実行してください。

MRA を介した Android 用の PUSH を有効にする CLI コマンド: *xConfiguration XCP Config FcmService: On*

注: このコマンドを使用すると MRA を介して現在サインインしているユーザの IM & Presence サービスは破壊されます。このため、これらのユーザは再度サインインする必要があります。

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。Bug ID CSCva36208 を特定します。
- **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、各 Jabber Guest コールごとに、Cisco Expressway-E で RMS ライセンスが消費されるはずが、実際には Cisco Expressway-C で RMS ライセンスが消費されます。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

Expressway の一部の機能はプレビューであるか、外部依存性があります

Expressway の新機能をできるだけ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シスコ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。このリリースでプレビュー ステータスでのみ提供される Expressway の機能は、こ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

- 現時点では、クラスタ展開内の 1 つの Expressway ノードで障害が発生した場合や、何らかの理由でネットワーク接続が失われた場合、または Unified CM を再起動した場合は、該当ノードを通過するすべてのアクティブなコールが失敗します。コールは別のクラスタピアに渡されません。これは X12.5x の新しい動作ではありませんが、見過ごされていたために、以前のリリースでは文書化されていませんでした。バグ ID CSCtr39974 を特定します。
- Expressway は DTLS を終了しません。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。Expressway を介して DTLS コールを発信しようとしても失敗します。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。

Expressway TURN は STUN サーバとして動作しない

X12.6.1 以降では、セキュリティ強化により、Expressway-E TURN サーバは汎用 STUN サーバとして動作しなくなり、認証されていない STUN バインドリクエストを受け入れません。

その結果、以下のシナリオが考えられます。

- シナリオ A:(『Cisco Expressway および Microsoft インフラストラクチャ導入ガイド』[英語] で説明されているように) Microsoft との相互運用性の目的で TURN クライアントとして B2BUA を使用する場合、B2BUA は、サーバが動作しているかどうかを確認するために STUN バインドリクエストを TURN サーバに送信することはありません。つまり、Expressway X12.6.1 以降では、到達可能でない TURN サーバの使用を B2BUA が試みた結果、**コールが失敗する可能性があります**。
- シナリオ B:Expressway X12.6.1 以降をインストールする前に Expressway と Meeting Server WebRTC を使用する(さらに Expressway-E が TURN サーバとして構成されている) 場合、最初に Meeting Server ソフトウェアをバージョン 3.0 またはバージョン 2.9.x または 2.8.x の互換性のあるメンテナンスリリースにアップグレードします。バグ ID CSCvv01243 を参照してください。この要件は、他の Meeting Server のバージョンが Expressway-E 上の TURN サーバに向けて STUN バインドリクエストを使用することによるものです(Expressway-E TURN サーバの構成の詳細については、『*Cisco Meeting Server 版 Cisco Expressway Web プロキシ導入ガイド*』を参照してください) 。。

Cisco Webex Hybrid コールサービス

Expressway X12.6 は、ハイブリッドコールサービスの導入に必要なコールコネクタソフトウェアのホストには機能しません。また、Expressway コネクタホストに以前のサポートされているバージョンを使用する必要があります。詳細については、https://help.webex.com でハイブリッドコールサービスの既知の問題のドキュメントをご覧ください。

プロダクト ライセンスの登録 - スマート ライセンスへの変換に関する問題

この項目は、既存の Expressway ライセンス(RMS、デスクトップ、またはルーム) をスマート ライセンスの利用資格に変換する場合に適用されます。この場合は、Cisco Product License Registration ポータルのオプションを使用して一部のライセンスだけを部分的に変換することはしないでください。既知の問題があるため、一部のライセンスのみを変換することを選択した場合、システムは残りのライセンスを自動的に喪失または削除します。つまり、変換されていないライセンスも削除されます(また、それらを取得するにはライセンスのケースが必要になります) 。

これを回避するには、[変換数量 (Quantity to Convert)] フィールドが [利用可能数量 (Quantity Available)] フィールドと同じ値であることを確認してください。これはページを開いたときのデフォルトになっています。

クラスタ化されたシステムのスタティック NAT

X12.5.5 から、スタティック NAT 機能のサポートはクラスタ化されたシステムに拡張されます(スタンドアロンシステムのサポートは X12.5.3 で導入されました) 。ただし、TURN サーバとして設定されているピアは、対応するパブリック インターフェイスのプライベート アドレスを使用して到達可能である必要があります。

MRA に関する制限事項

モバイルおよびリモート アクセス(MRA) に Expressway を使用する場合、現状では、サポートされない機能と制限がいくつか存在します。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については、『*Cisco Expressway 経由の Mobile & Remote Access*』ガイドの「*Mobile & Remote Access を使用する場合にサポートされる機能とサポートされない機能*」で詳しく説明されています。

7800/8800 シリーズのどの電話機とその他のエンドポイントが MRA をサポートしているかの詳細については、『*Cisco Expressway 経由のモバイルおよびリモート アクセス*』の「*MRA 要件*」のセクションを参照してください 。

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。

エンドポイント/クライアントとの MRA OAuth トークン認証

標準の MRA モード(ICE なし) では、Unified CM で設定されている MRA アクセス ポリシー設定に関係なく、Cisco Jabber のユーザは、次の場合に、ユーザ名とパスワードを使用するか、従来のシングル サインオンを使用して認証することができます。

- Jabber ユーザが(更新トークンがサポートされない) 11.9 より前のバージョンを実行しており、非トークン認証方式を許可するように Expressway が構成されている場合。

ICE パススルー モードでは、ICE MRA コール パスがエンドツーエンドで暗号化されている必要があります(『*Expressway MRA 導入ガイド*』の「*Expressway-C と Unified CM の間のシグナリング パスの暗号化*」を参照してください) 。エンドツーエンドの暗号化では通常、物理エンドポイント向けに Unified CM を混合モードにする必要があります。ただし Jabber クライアントについては、混合モードではない Unified CM クラスタで SIP OAuth を活用することによって、エンドツーエンドの暗号化の要件を満たすことができます。Unified CM が混合モードでない場合は SIP OAuth を有効にする必要がありますが、標準のセキュア プロファイルを使用して登録できる場合は、Jabber には SIP OAuth は必要ありません。

詳細については、『*Expressway MRA 導入ガイド*』の「*MRA アクセス制御の構成*」セクション、および『*シスコ コラボレーション ソリューション リリース 12.0 での OAuth の導入*』ホワイトペーパー [英語] を参照してください。

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引き下げられます。

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。

仮想システム

ESXi 側のチャンネル対応スケジューラが有効化されていて、CPU の負荷が 70% を超える場合、ビデオコールのキャパシティが制限される場合があります。

物理 Expressway アプライアンスでは、**高度なネットワーク**機能により、構成されたイーサネット 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。仮想マシンベースの Expressway システムのポート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。

CE1200 アプライアンス

- X710 ファームウェア バージョンに関する特定の要件が存在します。これは、利用可能な現在のバージョンに応じて変更される可能性があります。最新情報については、『*Expressway CE1200 設置ガイド*』の「必要なファームウェアバージョン」セクションを参照してください。
- アプライアンスには、*Cisco Expressway CE1200 設置ガイド*に詳述されている最小の Expressway ソフトウェアバージョンが必要です (バージョンはアプライアンスのリビジョンによって異なります)。システムには以前のバージョンのソフトウェアへのダウングレードを防止する機能はありませんが、シスコでは、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 Expressway 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 CE1200 アプライアンス(またはX12.6 以降を実行する VM ベースのシステム) の場合には効果がありません。サービス セットアップ Web UI ページでは、そのタイプ(Expressway-C または Expressway-E) またはシリーズ(Cisco Expressway または Cisco VCS) に対する変更を管理できるようになりました。

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 を使用する中規模アプライアンスを X8.10 以降にアップグレードすると、Expressway は自動的にシステムを大規模システムに変換します。これは、Expressway-E が大規模システム(36000 ~ 36011) のデフォルトの逆多重化ポートで多重化 RTP/RTCP トラフィックをリッスンし、中規模システム用に構成された逆多重化ポートではないことを意味します。この場合、ファイアウォール上でポート 36000 ~ 36011 が開かされていないため、Expressway-E はコールをドロップします。

回避策

X8.11.4 から、[System(システム)] > [Administration settings(管理設定)] ページ([Deployment Configuration(展開構成)] リストから [Medium(中)] を選択) を使用して、システム サイズを手動で [Medium(中)] に戻すことができます。

X8.11.4 より前の回避策は、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 の Web ユーザインターフェイスを翻訳する場合は、x8.10.3 以降で新しい Expressway 言語パックが提供されています。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。

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 Service ノードが別のノードへのフェイルオーバーに失敗した場合、影響を受けるユーザは他のノードに動的に移動しません。Expressway はこの機能をサポートしませんし、テストも行われていません。

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

この問題は、デュアル NIC Cisco 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) 静的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 リクエス

トは失敗する可能性があります。これは、Webex INVITE を非 NAT として扱うため、SIP Via ヘッダーから送信元アドレスを直接抽出する、現在の Expressway-E のルーティング動作に起因します。

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 AVMCU を起動した Expressway および Meeting Server を介してデュアルホーム会議を活用する場合は、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、現時点では次のドメイン内または企業内の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、同じドメイン内の 1 つの(サブ) ネットワークに Cisco Unified Call Manager を、別の(サブ) ネットワークに Microsoft を展開します。

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

チェーン付き Expressway-E を使用したライセンスの動作

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構成する「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。

オプションキー(HSM を含む) を使用する機能ではスマート ライセンスを使用できない

オプションキーにより、次の Expressway 機能が有効になります。オプションキーはスマート ライセンスと互換性がないため、これらの機能が必要な場合は、スマートライセンスではなく、PAK ベースのライセンスを使用する必要があります。

- 詳細アカウント セキュリティ
- HSM(ハードウェア セキュリティ モジュール)
- Microsoft 製品との相互運用性

HSM のサポート

現在のプレビュー ステータスのみで提供されている機能の 1 つに加え、次の追加のポイントが、Expressway の HSM サポートに適用されます。

- オプションキーで有効化されている他の機能と同様に(前のセクションを参照) 、スマート ライセンスを使用する Expressway とともに HSM を使用することはできません。
- 「SafeNet Luna」ネットワーク デバイスは、Expressway のユーザ インターフェイスに表示されますが、このデバイスは現在 Expressway によって一切サポートされていないため、SafeNet Luna 設定を行ってはいけません。

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(Maintenance)] > [オプションキー(Option keys)]) 。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。バグ ID CSCvf78728 を特定します。

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

この製品の相互運用性テストの結果は、https://tp-tools-web01.cisco.com/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の結果も確認できます。

同時に実行できる Expressway サービス

Cisco Expressway シリーズメンテナンスおよび操作ガイド ページの『*Cisco Expressway 管理者ガイド*』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することができる Expressway サービスについて詳しく説明しています。「概要」セクションにある「同時にホストできるサービス」の表を確認してください。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。

Expressway のアップグレード(アップグレード先 : X12.6.4

このセクションでは、推奨される方法である Web ユーザインターフェイスを使用して、Expressway にソフトウェアをインストールする方法について説明します。インストールを実行するために、SCP や PSCP などの安全なコピープログラムを使用する場合は、代わりに*管理者ガイド*を使用してください。

要約

表 9　一般的なアップグレード プロセスのタスクの概要

ステージ(Stage)	タスク	条件
1	以下の*前提条件とソフトウェアの依存関係*と、*はじめる前に*セクションをご確認ください。	リリース ノート
2	システムのバックアップ	**[メンテナンス(Maintenance)] > [バックアップと復元(Backup and Restore)]**
3	メンテナンス モードを有効にし、現在のコールと登録が終了するまで待機します	**[メンテナンス(Maintenance)]> [メンテナンスモード(Maintenance mode)]**
4	新しいソフトウェアイメージをアップロードします (**アップグレード**オプション)	**[メンテナンス(Maintenance)] > [アップグレード(Upgrade)]**
5	新しいソフトウェアのインストール (「**アップグレードを続行する**」オプション)	**[メンテナンス(Maintenance)] > [アップグレード(Upgrade)]**
6	リブート	**アップグレード** ページから
7	クラスタ展開では、各ピアに対して順番に繰り返します	-

前提条件とソフトウェアの依存関係

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。

Expressway システム(X8.11.4 より前) では 2 段階アップグレードが必要です。

バージョン X8.11.4 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、X12.6.4 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) 。既存のシステムのバージョンによっては、アップグレードが失敗します。中間リリースとして X8.11.4 にアップグレードすることをお勧めします。

リリースキーが必要かどうか

X8.6.x 以降のソフトウェア上の Expressway をこのリリースにアップグレードする場合 (X8.11.4 から X12.6.4 へなど) 、リリースキーは必要ありません。この変更は X12.5.4 で導入されました。(Cisco VCS システムでは引き続きリリース キーが使用されています) 。

すべての導入の手順 :

X12.6 または X12.6.1 からアップグレードし、アラーム ベースの電子メール通知機能を使用する場合、X12.6.2 では、電子メール ID の長さは最大 254 文字に制限されることに注意してください。アップグレードする前に、すべての接続先電子メール ID が 254 文字未満であることを確認してください。

ダウングレードはサポートされません。より新しいバージョンの Expressway を実行しているシステムに古いバージョンをインストールしないでください。システム設定が失われます。

X8.11 以降では、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ることに注意してください。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。

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 : X8.8 で証明書の検証が厳しくなったため、検証に失敗しないように、次の項目を確認する必要があります。
  - 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)]) 。
  - Unified Communications ノードが展開されている場合、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 CA リストに、環境内のすべてのノードの自己署名証明書が記載されていますか。
  - Expressway の信頼 CA リスト内のすべてのエントリは一意ですか。重複をなくします。
  - 他のインフラストラクチャへの接続で **TLS 検証モード**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、Expressway-E システムに対して順方向および逆方向の DNS エントリが必要です。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 で、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、MRA などの複雑な展開がアップグレード後に期待どおりに動作しない可能性があります。
- 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。デフォルトでは、TLS 検証はアップグレード後に強制的に実行されず、実行するようにアラームによって通知されます。

アップグレードの一部としてリブートが必要な場合とそのタイミング

*システム プラットフォーム*のコンポーネントのアップグレードは 2 段階のプロセスで行います。まず、新しいソフトウェア イメージを Expressway にアップロードします。これと同時に、システムの現在の設定が記録されるため、アップグレード後にこれを復元することができます。この最初の段階ではシステムは引き続き既存のソフトウェア バージョンで稼働しており、すべての正常なシステム プロセスが継続します。

アップグレードの第 2 段階では、システムをリブートする必要があります。Expressway は再起動時に新しいソフトウェアバージョンをインストールし、以前の構成を復元します。リブートによって、現在のすべてのコールが終了し、現在のすべての登録も終了します。つまり、新しいソフトウェアはいつでもアップロードできるため、タイミングが合うまで(コールがまったく実行されていないときなど) 待機してからシステムをリブートすることで、新しいバージョンに切り替えることができます。**ソフトウェアのアップロードと再起動の間に行った構成変更は、新しいソフトウェアバージョンでシステムを再起動した時点で失われます**。

システム プラットフォーム以外のコンポーネントのアップグレードでは、システムの再起動は必要ありません。ただし、そのコンポーネントが提供するサービスはアップグレードが完了するまで、一時的に中断されます。

MRA を使用する導入

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

- Unified Communications 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 Service、および シスコ ユニティ コネクション(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 のアップグレード前に、『*Expressway 経由のモバイルおよびリモート アクセス導入ガイド*』に記載されている最小バージョンが実行されていることを確認してください。

  IM and Presence Service 11.5 は例外です。IM and Presence Service 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 および Cisco Expressway-E は、同じアップグレードの「ウィンドウ(期間) 」で**アップグレードする必要があります**(これは非 MRA 展開に対する一般的な推奨でもあります) 。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、MRA に使用される Expressway を、TC またはコラボレーションエンドポイント (CE) ソフトウェアを実行するクラスタ化された Unified CM とエンドポイントで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、これ以降に記載されている関連する TC または CE の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

X8.10x 以降では、MRA 認証 (アクセス制御) の設定は、以前のリリースのように Expressway-E で構成するのではなく Expressway-C で構成します。既存の設定を維持できない場合は、デフォルト値が適用されます。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構成する必要があります。これらの手順については後述します。

FIPS モードの暗号を使用する展開

Expressway で FIPS モードが有効になっている場合、アップグレード後に、デフォルトの SIP TLS Diffie-hellman キーサイズをデフォルトの 1024 ビットから 2048 以上に手動で変更します。これらの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)

Expressway の X8.7.x(以前のバージョン) には、Cisco Unified Communications Manager IM and Presence Service 11.5(1) 以降との相互運用性はありません。これは、このバージョンの IM and Presence Service 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に、Expressway システムをアップグレードしてから IM and Presence Service システムをアップグレードしてください。Expressway で次のエラーが発生する場合は、この問題の兆候です。*<IM&P ノード アドレス> と通信できませんでした*。AXL query HTTP error "'HTTPError:500'"」

Cisco Webex ハイブリッド サービスを使用する導入

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 Cloud 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

始める前に

- システムのアクティビティレベルが低いときにアップグレードを実行します。
- システム アップグレードでは、プロセスを完了するためにシステム リブートが必要です。リブートによって、すべてのアクティブなコールと登録が強制終了されます。
- クラスタ システムの場合は、すべてのピアを同じ「ウィンドウ」でアップグレードするための十分な時間を割り当てます。クラスタは、ソフトウェア バージョンがすべてのピアで一致するまで、正常に再形成されません。
- [アラーム (Alarms)] ページ (**[ステータス (Status)] > [アラーム (Alarms)]**) を参照して、すべてのアラームが実行され、クリアされていることを確認します。クラスタをアップグレードする場合は、各ピアに対してこれを実行します。
- VM ベースのシステムをアップグレードする場合は、標準の *.tar.gz* ソフトウェアの イメージファイルを使用します。*.ova* ファイルは、VMware への Expressway ソフトウェアの初期インストールにのみ必要です。
- Expressway for MRA を使用していて、X8.9.x 以前のバージョンから X 8.10 以降にアップグレードする場合は、アップグレードする前に MRA 認証設定をメモしてください。バージョン X8.10 以降では、MRA 認証 (アクセス制御) 設定は 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 の設定は維持されないため、アップグレード後に Expressway-C で設定を確認し、必要であれば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、[構成 (Configuration)] > [ユニファイド コミュニケーション(Unified Communications)] > [構成 (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 ([オン (On)]、[排他 (Exclusive)]、または [オフ(Off)]) をメモします。
  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)**
- 前提条件とソフトウェアの依存関係, ページ 28にあるすべての関連するタスクが完了していることを確認します。

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 の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) システムのすべての場合では、**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。** モバイルおよびリモート アクセスなどの一部のサービスでは、両方のシステムで同じバージョンを実行する*必要*があります。

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 X12.5 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。

スタンドアロン システムをアップグレードするためのプロセス

クラスタ化された Expressway をアップグレードする場合は、このプロセスを使用しないでください。代わりに、クラスタ システムをアップグレードするプロセスを使用します。

1. 管理者として Expressway Web ユーザインターフェイスにサインインします。
2. 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)]) 。
3. メンテナンスモードを有効して、Expressway が新しい着信コールを一切処理しないようにします([メンテナンス(Maintenance)] > [メンテナンスモード(Maintenance mode)]) 。既存のコールはコールが終了するまで継続します。
4. 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。

   自動的にクリアされないコールまたは登録を手動で削除するには、**[ステータス(Status)] > [コール(Calls)]** ページまたは **[ステータス(Status)] > [登録(Registrations)] >[デバイスごと(By device)]** ページをそれぞれ使用します (SIP コールがすぐにクリアされない場合があります)。

   注 : Conference Factory の登録はそのままにしておいて構いません(有効化されている場合) 。これはコールの送信元ではなく、また他のピアが各自の Conference Factory 登録を所有しているため、これを削除しても別のピアにロールオーバーされることはありません。
5. **[メンテナンス(Maintenance)] > [アップグレード(Upgrade)]** に移動して、**[アップグレード(Upgrade)]** ページにアクセスします。
6. **[参照(Browse)]** をクリックし、アップグレードするコンポーネントのソフトウェア イメージ ファイルを選択します。
   Expressway は、選択したソフトウェア イメージ ファイルに基づいて、アップグレードするコンポーネントを自動的に検出します。
7. [アップグレード(Upgrade)] をクリックします。この手順では、ソフトウェア ファイルはアップロードされますが、インストールはされません。アップロードが完了するまで数分かかる場合があります。
8. **システム プラットフォーム** コンポーネントに対するアップグレードの場合は、「**アップグレードの確認(Upgrade confirmation)** 」ページが表示されます。
   a. 以下の詳細を確認してください。
      - **新しいソフトウェアバージョン**番号が想定どおりである。
      - **MD5 ハッシュ**と「SHA1 ハッシュ」の値が、ソフトウェアイメージファイルをダウンロードした cisco.com ページに表示された値と一致している。
   b. [アップグレードの続行(Continue with upgrade)] をクリックします。この手順では、新しいソフトウェアをインストールします。
      「**システム アップグレード(System upgrade)** 」ページが開き、ソフトウェアのインストール中は経過表示バーが表示されます。
      ソフトウェアのインストールが完了すると、アクティブなコールと登録の概要が表示されます(コールと登録は、次の手順でシステムをリブートすると失われます) 。
   c. [システムのリブート(Reboot system)] をクリックします。ソフトウェア tar ファイルのアップロードとリブートの間に設定変更を行った場合、それらの変更はシステムの再起動時にすべて失われます。

      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。

      再起動が完了すると、[**ログイン(Login)**] ページが表示されます。
9. (システム プラットフォームではなく) 他のコンポーネントへのアップグレードの場合、ソフトウェアは自動的にインストールされ、再起動する必要はありません。

次のステップ

MRA を使用しない場合は、これでアップグレードが完了し、Expressway の構成が想定どおりに行われています。[概要(Overview)] ページと [アップグレード(Upgrade)] ページに、アップグレードされたソフトウェアのバージョン番号が表示されます。

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 2: MRA 導入のアップグレード後のタスク, ページ 41

オプション キーを有効にする必要があるコンポーネントがある場合は、**[メンテナンス(Maintenance)] > [オプション キー(Option keys)]** ページから行います。

Expressway で FIPS モードが有効である場合 (つまり FIPS140-2 暗号化システムである場合) 、X12.6 以降では、デフォルトの SIP TLS Diffie-Hellman キー サイズをデフォルトの 1024 ビットから 2048 以上に手動で変更する必要があります。これを行うには、次のコマンドを Expressway のコマンドライン インターフェイスで入力します(キー サイズを 2048 より大きくする場合は、最後の要素の値を変更します) 。
「xconfiguration SIP Advanced SipTlsDhKeySize: "2048"」。この手順は、ほとんどのシステムには該当しません。これは、高度なアカウント セキュリティが設定され、FIPS が有効になっているシステムのみに適用されます。

クラスタ システムをアップグレードするためのプロセス

注意 : 構成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」します。

まず、Expressway-E クラスタを最初にアップグレードしてから、その後に Expressway-C をアップグレードすることを推奨します(どの場合もプライマリピアで開始します) 。これによって、Expressway-C で Expressway-E に対する新しいトラバーサル セッションを開始した場合に、Expressway-E でその処理の準備が整います。プライマリのピアから始めて、クラスタピアを次の順序でアップグレードします。

1. 管理者として Expressway Web ユーザインターフェイスにサインインします。
2. アップグレードする前に、Expressway 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)]) 。

   注 : クラスタのピアが異なるバージョンの Expressway を実行している場合は、アップグレードに必要な設定以外の構成変更は行わないでください。クラスタは、プライマリ Expressway とは異なるバージョン上で実行されている下位のピアに対しては、構成の変更を一切複製しません。
3. メンテナンスモードを有効して、ピアが新しい着信コールを一切処理しないようにします([メンテナンス(Maintenance)] > [メンテナンスモード(Maintenance mode)]) 。既存のコールはコールが終了するまで継続します。クラスタ内の他のピアは、コールの処理を続行します。
4. 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。

   自動的にクリアされないコールまたは登録を手動で削除するには、**[ステータス(Status)] > [コール(Calls)]** ページまたは **[ステータス(Status)] > [登録(Registrations)] >[デバイスごと(By device)]** ページをそれぞれ使用します (SIP コールがすぐにクリアされない場合があります)。

   注 : Conference Factory の登録はそのままにしておいて構いません(有効化されている場合) 。これはコールの送信元ではなく、また他のピアが各自の Conference Factory 登録を所有しているため、これを削除しても別のピアにロールオーバーされることはありません。
5. **[メンテナンス(Maintenance)] > [アップグレード(Upgrade)]** に移動して、**[アップグレード(Upgrade)]** ページにアクセスします。
6. **[参照(Browse)]** をクリックし、アップグレードするコンポーネントのソフトウェア イメージ ファイルを選択します。Expressway は、選択したソフトウェア イメージ ファイルに基づいて、アップグレードするコンポーネントを自動的に検出します。
7. [アップグレード(Upgrade)] をクリックします。この手順では、ソフトウェア ファイルはアップロードされますが、インストールはされません。アップロードが完了するまで数分かかる場合があります。

8. **システム プラットフォーム** コンポーネントに対するアップグレードの場合は、「**アップグレードの確認 (Upgrade confirmation)** 」ページが表示されます。
   a. 以下の詳細を確認してください。
      - **新しいソフトウェアバージョン**番号が想定どおりである。
      - **MD5 ハッシュ**と「SHA1 ハッシュ」の値が、ソフトウェアイメージファイルをダウンロードした cisco.com ページに表示された値と一致している。
   b. [アップグレードの続行 (Continue with upgrade)] をクリックします。この手順では、新しいソフトウェアをインストールします。
      「**システム アップグレード (System upgrade)** 」ページが開き、ソフトウェアのインストール中は経過表示バーが表示されます。
      ソフトウェアのインストールが完了すると、アクティブなコールと登録の概要が表示されます (コールと登録は、次の手順でシステムをリブートすると失われます) 。
   c. [システムのリブート (Reboot system)] をクリックします。ソフトウェア tar ファイルのアップロードとリブートの間に設定変更を行った場合、それらの変更はシステムの再起動時にすべて失われます。

      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。

      クラスタの通信の失敗やクラスタのレプリケーションのエラーなど、アップグレード プロセス中に発生するクラスタ関連のすべてのアラームと警告は無視します。これらは予測済みのものであり、すべてのクラスタピアがアップグレードされたとき、およびクラスタデータの同期後 (通常、完全なアップグレードから 10 分以内) に解決されます。

      再起動が完了すると、[**ログイン (Login)**] ページが表示されます。
9. (システム プラットフォームではなく) 他のコンポーネントへのアップグレードの場合、ソフトウェアは自動的にインストールされ、再起動する必要はありません。
10. すべてのピアが新しいソフトウェアバージョンになるまで、各ピアについて前の手順を繰り返します。

次のステップ

1. 各 Expressway (プライマリを含む) の新しいステータスを確認します。
   a. **[システム (System)] > [クラスタリング (Clustering)]** に移動し、クラスタデータベースのステータスが [**アクティブ (Active)**] とレポートされていることを確認します。
   b. [システム (System)]、[設定 (Configuration)]、[アプリケーション (Application)] メニューで、各項目の構成を確認します。
2. Expressway をもう一度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)]) 。
3. 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 2: MRA 導入のアップグレード後のタスク, ページ 41
4. オプション キーを有効にする必要があるコンポーネントがある場合は、**[メンテナンス (Maintenance)] > [オプション キー (Option keys)]** ページから行います。
5. Expressway で FIPS モードが有効である場合 (つまり FIPS140-2 暗号化システムである場合) 、X12.6 以降では、デフォルトの SIP TLS Diffie-Hellman キー サイズをデフォルトの 1024 ビットから 2048 以上に手動で変更する必要があります。これを行うには、次のコマンドを Expressway のコマンドライン インターフェイスで入力します (キー サイズを 2048 より大きくする場合は、最後の要素の値を変更します) 。
   「xconfiguration SIP Advanced SipTlsDhKeySize: "2048"」。この手順は、ほとんどのシステムには該当しません。これは、高度なアカウント セキュリティが設定され、FIPS が有効になっているシステムのみに適用されます。
6. (省略可) 何らかの理由でデフォルトの TLS バージョンを変更する必要がある場合は、『*Cisco Expressway 証明書の作成と使用に関する導入ガイド*』で、各ピアで TLS バージョンを設定する方法について説明されています。

これで、Expressway クラスタでのソフトウェアのアップグレードは完了しました。

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 Expressway ログ ファイル解 析) を支 援 するために作 成したものです。たとえば、ビジネス ツー ビジネス コール テスターを使 用して、コールの検 証 とテス トを行うことができます。これには、Microsoft インターワーキングコールが含 まれます。

コラボレーション ソリューション アナライザを使 用 するには、カスタマー アカウント またはパート ナー アカウント が必 要 です。

スタート ガイド

1. ログ分 析 ツールを使 用 する予 定 であれば、まず、Expressway のログを収 集します。
2. https://cway.cisco.com/tools/CollaborationSolutionsAnalyzer/ にサインインします

   X12.6 からは、[診 断 ロギング(Diagnostic logging)] ページの [ログの分 析 (Analyze log)] ボタン([メンテナンス (Maintenance)] > [診 断 (Diagnostics)]) を使 用し、コラボレーション ソリューション アナライザのト ラブルシューティング ツー ルへのリンクを開 けます。
3. 使 用 するツールをクリックします。たとえば、ログを使 用 するには、次 のようにします。
   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。

バグ検 索 ツールの使 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. 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 されるバグのリスト で [フィルタ(Filter)] ドロップダウン リストを使 用し、[キーワード (Keyword)] 、[変 更 日 (Modified Date)] 、[重 大 度 (Severity)] 、[ステータス(Status)] 、[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。

Bug Search Tool のホーム ページの [詳 細 検 索 (Advanced Search)] を使 用して、特 定 のソフト ウェア バージョンで検 索します。

バグ検 索 ツールのヘルプ ページには、バグ検 索 ツールの使 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。

マニュアルの入 手 、Cisco バグ検 索 ツール(BST) の使 用 、サービス リクエスト 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 されたシスコのテクニカルコンテンツをお手 元 で直 接 受 信 するには、What's New in Cisco Product Documentation の「RSS フィード 」に登 録 してください。RSS フィード は無 料 のサービスです。

付録 1: Expressway での HSM デバイスの構成

重要:事前の確認事項

HSM の障害。Expressway が HSM を使用するように設定されており、その後 HSM が失敗すると、**暗号化を必要とするすべてのサービスが利用できなくなります**。これには、MRA、コール、Web アクセスなどが含まれます。

設定初期化。何らかの理由で HSM が恒久的に利用できない場合は、Expressway の**初期設定化**を行ってから、Expressway で新しい HSM を設定する必要があります。初期設定化のリセットでは、**ソフトウェアイメージが再インストールされ、Expressway 構成がデフォルトで最も少ない機能がリセットされます**(リセットの実行方法については、『*Expressway 管理者ガイド*』を参照してください)。

HSM を有効にして管理する方法

HSM 構成ページ(**[メンテナンス(Maintenance)] > [セキュリティ(Security)] > [HSM 構成 (HSM configuration)]**)を使用して、Expressway 必要な情報を設定します。

設定はクラスタ全体に複製されます。

HSM 構成ページの設定は、Expressway クラスタ内のすべてのピアにわたって複製されます。したがって、1 つのピアの設定を追加または削除すると、その変更は他のすべてのピアに複製されます。

タスク 1: 前提条件の構成

Expressway のハードウェア セキュリティ モジュール(HSM)機能を有効にする前に、次の手順を実行してください。

a.	HSM オプション キーを追加します。	i. **[メンテナンス(Maintenance)] > [オプション キー(Option keys)]** に移動します。 ii. [**ソフトウェア オプション(Software option)**] セクションで、option キーを入力します。 iii. [オプションの追加(Add option)] をクリックします。キーはページ上部のリストに表示されます。
b.	HSM TLP パッケージをインストールします。これは、Expressway ソフトウェア イメージと同じダウンロード サイトから入手できます。 HSM TLP は、Expressway が HSM を使用するために必要な HSM プロバイダー固有のバイナリのアーカイブです。	i. **[メンテナンス(Maintenance)] > [アップグレード(Upgrade)]** に移動します。 ii. [コンポーネントのアップグレード(Upgrade component)] セクションで、[ファイルの選択(Choose File)] をクリックして、ローカル マシンから TLP ファイルを選択します。 iii. [アップグレード(Upgrade)] をクリックします。[コンポーネントが正常にインストールされました(Component installation succeeded)] というメッセージがページ上部に表示され、HSM TLP もページ上部に表示されます。ドロップダウンで、インストールされているすべてのモジュールのリストを確認できます。 **注:** オプションキーを追加して、クラスタ内の各ピアに TLP をインストールする必要があります。すべてのピアにオプションキーと TLP がある場合を除き、クラスタで HSM モードを有効にすることはできません。

c.	Expressway での HSM ボックスの展開	nShield Connect XC HSM を設定するには、次のようにします。 i. nShield Connect のユーザ ガイドの説明に従って、セキュリティ環境とリモート ファイル システム(RFS) をセットアップします。 ii. HSM が必要とするすべてのファイルのマスター コピーを含む nShield Connect に RFS を設定します。通常、RFS はクライアント コンピュータ上に存在しますが、ネットワーク上でアクセス可能な任意のコンピュータ上に配置することもできます。 iii. RFS および nShield Connect ボックスを展開した後、RFS で次のコマンドを実行します: */opt/nfast/bin/rfs-setup --gang-client --write-noauth <Expressway_ip_address>* このコマンドが実行されていない場合、HSM 証明書管理は、Expressway で正しく機能しません。
d.	証明書の署名権限へのアクセス	
e.	HSM 互換の証明書の作成	手順については、『*Expressway 管理者ガイド*』のセキュリティの章を参照してください。

タスク 2: Expressway で HSM を有効にする

この手順は、Expressway で HSM を有効にするために推奨される手順です。

1. **[メンテナンス(Maintenance)] > [セキュリティ(Security)] > [HSM 構成(HSM configuration)]** に移動します。
2. [HSM 構成(HSM Settings)] で、[HSM モード(HSM Mode)] ドロップダウンリストから HSM プロバイダーを選択します。
3. nShield の設定
   a. RFS IP アドレスと RFS ポートを入力します。デフォルトのポートは 9004 です。
   b. [Save Configuration] をクリックします。
   「*HSM 設定が更新されました(HSM Settings updated)* 」というメッセージがページの上部に表示されます。
   c. [モジュールの追加(Add Module)] セクションで、デバイスの IP アドレス、ポート、ESN (電子シリアル番号)、および KNETI (ネットワーク整合性キー) を入力します。
   d. [Add Module] をクリックします。
   [*HSM モジュールが正常に追加されました(HSM Module successfully added)*] というメッセージがページ上部に表示されます。
   e. [HSM モード(HSM Mode)] タブの下の表にデバイスが表示されるようになりました。
   f. デバイスを追加するには、モジュールの追加手順を繰り返します。
4. a. [HSM モード(HSM Mode)] を [オン(On)] に設定して、[モードを設定(Set Mode)] をクリックします。
   [HSM モードが正常に更新されました(HSM Mode successfully updated)] というメッセージが表示されます(ページ上部) 。
   注 : HSM モードの On/Off を切り替えると、Web が利用できなくなる場合があります。この問題が発生した場合は、ブラウザページをリロードします。

結果 : Expressway で HSM の使用が可能になります。HSM の動作ステータスを確認するには、次のセクション「タスク 3: HSM ステータス チェックの監視, ページ 39」(1 ページ) を参照してください。

タスク 3: HSM ステータス チェックの監視

HSM モードを有効にすると、HSM 構成ページに [HSM ステータスチェック(HSM Status Check)] セクションが表示されます。このセクションには、すべての Expressway クラスタピア用の HSM サーバと HSM 証明書、および各ピアのすべてのモジュールに関する情

報が表示されます。

実行中の HSM サーバ

a. **HSM ボックスとの通信を担当するプロセスが Expressway で実行されている場合は、HSM モードを Expressway で有効にした後、TRUE** になります。
b. **プロセスが Expressway 上で実行中ではなく、HSM エラーアラームが発生した場合は、FALSE** になります。

使用中の HSM 証明書

a. **HSM 証明書と秘密キーが Expressway で使用されている場合は、TRUE** になります。
b. Expressway が HSM 証明書と秘密キーを使用していない場合は、**FALSE** になります。デフォルトの状態は FALSE です。[HSM 証明書が使用されていません(HSM certificate is not used)] というアラームが Expressway で表示されます。これは、HSM 証明書と秘密キーを使用していないことを警告するものです。

   HSM 証明書と秘密キーが Expressway に展開されると、このアラームは引き下げられ、表示されるステータスは TRUE に変更されます。

ESN セクションには、HSM の設定中に追加され、その ESN で区別される HSM モジュールがリストされます。その他の列は、**接続ステータス**と**ハードウェアのステータス**を定義します。

接続ステータス

a. **Expressway と HSM モジュール間にネットワークの問題が存在しない場合は、OK** となります。
b. **ネットワークまたは HSM サーバの接続に関する問題が発生し、アラームが発生した場合、Failed** となります。

ハードウェア ステータス

a. **ハードウェアに関する問題が HSM ボックス自体で検出されない場合は、OK** となります。
b. **ハードウェアまたは HSM ボックスの構成に問題があり、アラームが発生すると、Failed** となります。

タスク 4: 次のステップ - HSM 秘密キーの生成とインストール

HSM を有効にして正常に動作している場合は、HSM 秘密キーと証明書を生成し、Expressway にインストールする必要があります。詳しくは、『*Expressway 管理者ガイド*』の「*HSM を使用した Expressway サーバ証明書の管理*」を参照してください。

モジュールの削除方法

Expressway HSM 設定からデバイス(モジュール) を削除するには、次の手順を実行します。

1. **[メンテナンス(Maintenance)] > [セキュリティ(Security)] > [HSM 構成(HSM configuration)]** に移動します。
2. リストから必要なデバイスを選択し、**[削除(Delete)]** をクリックします。

注 : HSM モードが有効になっているときは最後のデバイスを削除することはできません。まず、HSM モードを無効にする必要があります。

HSM の無効化方法

いずれかの理由で HSM を無効にする場合は、次の手順を実行することを推奨します。

1. **[メンテナンス(Maintenance)] > [セキュリティ(Security)] > [HSM 構成(HSM configuration)]** に移動します。
2. [HSM モード(HSM Mode)] を [オフ(Off)] に設定し、[モードの設定(Set Mode)] をクリックします。これにより、Expressway での HSM の使用が無効になります。
3. 削除するテーブル内のすべてのモジュールを選択するには、個々のデバイスを確認するか、[すべて選択(Select all)] をクリックします。(テーブルのすべてのデバイスを選択解除するには、**[すべてを選択解除(Unselect all)]** をクリックします) 。
4. [削除 (Delete)]をクリックし、確認ダイアログボックスで [OK] をクリックします。

付録 2: MRA 導入のアップグレード後のタスク

このセクションは、モバイルおよびリモート アクセスに Expressway 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、[構成(Configuration)] > [ユニファイド コミュニケーション(Unified Communications)] > [構成(Configuration)] > [MRA アクセス制御(MRA Access Control)] に進みます。
2. 次のいずれかを実行します。
   - 新しい MRA アクセス制御方式を 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、このページの適切な値を Expressway-E の設定に合わせて設定します。古い Expressway-E の設定を Expressway-C の新しい同等物にマッピングする方法については、次の 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 CM ノードを更新します。[構成(Configuration)] > [ユニファイド コミュニケーション(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。Unified 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 10　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 ログイン情報に対して Unified CM によってローカルで認証されます。 *[SAML SSO および UCM/LDAP(SAML SSO and 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]

表 10　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 (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(Off)]
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(Off)]
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確認します。また、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アイデンティティを含んでいます。 *[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 に確認します。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アイデンティティから決定されます。 *[いいえ(No)]*: Expressway が内部的に見えないように構成されている場合、エッジ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全体のネットワーク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インバウンド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)]

表 10　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** 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。	–

表 10　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。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**しないでください。**	[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 11　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	従来	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 ログイン情報による承認(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 ログイン情報による承認(Authorize by user credentials)** =*オン*	両方	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	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	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となります。

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 が採用している TCP ヘッダー圧縮機能は、UNIX オペレーティング システムの UCB(University of California, Berkeley) のパブリックドメイン バージョンとして、UCB が開発したプログラムを採用したものです。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。シスコおよび上記代理店は、商品性、特定目的適合、および非侵害の保証、もしくは取り引き、使用、または商慣行から発生する保証を含み、これらに限定することなく、明示または暗黙のすべての保証を放棄します。

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。マニュアルの中の例、コマンド出力、ネットワークトポロジー図、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 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。

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。

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 (https://www.cisco.com/c/ja_jp/about/contact-cisco.html) をご覧ください。

Cisco の商標または登録商標

Cisco および Cisco のロゴは、米国およびその他の国における Cisco およびその関連会社の商標を示します。シスコの商標一覧は https://www.cisco.com/c/ja_jp/about/legal/trademarks.html をご覧ください。Third-party trademarks mentioned are the property of their respective owners.「パートナー」という用語の使用は 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) 。