Cisco Expressway X12.7.1

リリース ノート

First Published: 2021 年 2 月

Last Updated:

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
2021 年 2 月	メンテナンス リリースの更新。	X12.7.1
2020 年 12 月	X12.7 リリースの初版。	X12.7
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#####	未サポート Expressway は X8.6.1 から X12.5.9、X12.6 はバグ修正のみサポートされていました。
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

Cisco TelePresence Video Communication Server (VCS) 製品は、現在**販売終了**となっています。**製品寿命**の日付およびその他の詳細については、https://www.cisco.com/c/en/us/products/collateral/unified-communications/telepresence-video-communication-server-vcs/eos-eol-notice-c51-743969.html 参照してください。

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。

X12.7.1 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
単一テナント環境での SNI のサポート	X12.7.1 以降でサポート
専用管理インターフェイス	X12.7 以降でサポート
MRA のファストパス登録(登録のためのキャッシング最適化)	X12.7 以降でサポート
Webex VDI for MRA	X12.7 以降でサポート
仮想化システム - ESXi 7.0 認定	X12.7 以降でサポート
ハードウェア セキュリティ モジュール(HSM) のサポート	プレビュー
Cisco Jabber の MRA SIP 登録フェールオーバー	プレビュー
MRA モバイルアプリケーション管理クライアント	プレビュー
IM&P 用の Android プッシュ通知パブリッシャー	プレビュー(X12.6.2 からはデフォルトで無効)
Cisco Contact Center のヘッドセット機能	プレビュー

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
VMware ESXi6.0(VM ベースの展開)	非推奨メソッド
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

Expressway は MLTS(マルチライン電話システム) ではありません。レイ・バウム法の要件を順守する必要があるお客様は、Cisco Unified Communication Manager を Cisco Emergency Responder と共に使用する必要があります。

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*』
モバイル& リモートアクセス(MRA)	*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*』

単一テナント環境の X12.7.1

サーバ名表示 (SNI) サポートの変更

X12.7.1 から、SNI のサポートは、以前サポートされていたマルチテナント HCS 環境に加えて、単一のテナント環境に拡張されるようになりました。

X12.7.1 のその他のソフトウェアの変更

クラスタ環境の X12.7.1 から、プライマリピアで自動侵入保護カテゴリのステータスが変更された場合、以前の場合は同じ状態が他のピアに反映されません。この予期しない動作が修正され、Expressway が設計どおりに機能するようになりました。

X12.7 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。

- より多くのサービスが Expressway でデフォルトで設定されるようになり、TLS の最小バージョンとして、TLS 1.2 が必要になります(詳細については、以下を参照) 。
- SMTP メールベースのサービスでは、TLS 証明書ベースの検証が必要になりました。この変更は、主にアラームベースの電子メール通知機能に影響します(詳細については、以下を参照) 。
- 「厳格なパスワードの適用」機能が有効の場合に追加のパスワード チェックが実行されるようになりました(**[ユーザ (Users)] > [パスワード セキュリティ(Password Security)]** ページ) 。X12.7 から、アカウント保持者がパスワードにユーザ名と同じ文字を(そのまま、あるいは逆順に、または小文字や大文字で) 使用しようとすると、エラーメッセージが表示されます。
  注: 厳格なパスワード機能は、ローカル認証データベース、および Expressway でローカルで管理されている管理者アカウントと FindMe ユーザアカウントに適用されますが、LDAP および外部に保存されているログイン情報には適用されません。

専用管理インターフェイス

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

DMI はデフォルトで無効です。DMI の有効化には、次の 2 つの側面があります。

1. DMI 機能の有効化: 管理トラフィックの LAN3 ポートをオンにします。ただし、専用ではなく、LAN1(および、設定している場合は LAN2) も使用できます。Expressway は、LAN3 ポートだけでなく、LAN1/LAN2 上の管理トラフィックも引き続きリッスンします。
2. 管理トラフィック用のインターフェイスを LAN3 のみにする場合は、Expressway で DMI 専用に個々の管理サービスを設定する必要があります。LAN3 サブネット外に管理サーバがある場合は、現在、これらのトラフィックを LAN3 に送信するにはスタティック IP ルートを設定する必要もあります。

サーバ/クライアント管理トラフィック

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

Expressway がサーバである管理トラフィックは、次のとおりです。

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

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

- Cisco TMS などの外部マネージャへのフィードバック イベント用の HTTP(S)
- NTP
- ディレクトリ(LDAP、Active Directory)
- リモート syslog
- 収集されたシステムメトリック

前提条件

DMI インターフェイスの新しい DNS 名は、Expressway サーバ証明書にサブジェクト代替名(SAN) として入力する必要があります。IP アドレスを使用してインターフェイス(または証明書の SAN エントリではない DNS) にアクセスする場合、証明書検証警告が

発行され、アクセスがブロックされる場合があります。

注意：DMI は Expressway 設定へのアクセスを提供するので、適切に保護することが重要です。

[SSOを有効にする(Enable DMI)]

1. Go to **[システム(System)] > [ネットワークインターフェイス(Network Interfaces)] > [IP]** に進み、[専用の管理インターフェイスを使用する(Use Dedicated Management Interface)] を [はい(Yes)]に設定します。
2. **[LAN3 - DMI]** セクションで、次を実行します。
   a. LAN3 ポートの IPv4 アドレスまたは IPv6 アドレスを指定します。
   b. IPv4 では、サブネットマスクも指定します。
   c. IPv6 の場合は、静的なグローバルアドレスを使用します。リンクローカルまたはステートレスの SLAAC は使用できません。
   d. 必要に応じて、ポートの**最大伝送ユニット(MTU)** を設定することで、DMI 経由で送信できるイーサネットパケットの最大サイズを変更します。デフォルト値は 1500 バイトです。
3. システムを再起動します。これらの変更を有効にするには、再起動が必要です。

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

注：Expressway VM の場合、OVF テンプレートに、DMI IP アドレスを定義するカスタマイズオプションがあります。

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

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

注意：これを行う前に、LAN3 で必要なサービスがアクセス可能であることを確認してください。そうしないと、DMI のみへの変更後にこれらのサービスがアクセスできなくなります。回復する唯一の方法は、コンソール(シリアル/VMWare) を使用して DMI をオフにすることであるため、これは管理サービスにとって特に重要です。

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

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

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

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

Expressway がクライアントとして動作する管理トラフィックでは、ターゲットサーバが DMI/LAN3 ポートと同じサブネット内にある場合、トラフィックは DMI に送信されます。LAN3 と同じサブネットにサーバを導入できない場合は、オプションで、サービスごとに LAN3 用のスタティック IP ルートを設定することで、Expressway 管理トラフィックに DMI の使用を強制できます。

例

この例では、次のサブネットを含む Expressway を想定しています。

- LAN3 サブネット範囲：a.b.128.0 ～ a.b.191.255
- LAN1 サブネット範囲：x.y.156.0 ～ x.y.159.255

Expressway で NTP を設定するとします。NTP サーバが LAN1 サブネット内にあります。Expressway からの発信 NTP トラフィックと NTP からの着信応答で DMI/LAN3 を使用します。これは、LAN3用のスタティックルートを次の設定で作成することで実現できます([システム(System)] > [ネットワーク インターフェイス(Network interfaces)] > [スタティックルート(Static routes)) 。

- IP アドレス: *x.y.151.0*
- プレフィックス長 : *24*
- ゲートウェイ : *172.22.128.1 (LAN3 サブネットのゲートウェイ)*
- インターフェイス: *LAN3*

スタティックルートの設定の詳細については、*Expressway 管理者ガイド*を参照してください。

MRA のファスト パス登録 (登録のためのキャッシング最適化)

X12.7 から、Expressway は、MRA ベースのデバイスのファスト パス登録をサポートしています。これによりルーティングプロセスが最適化され、サーバワークロードが軽減されてキャパシティが増加します。Expressway は、最初のルーティング計算をキャッシュしてから、事前にルーティングしたルートヘッダーを使用して、キャッシュされたルーティング結果を使用して後続のパケットを接続先に転送します。これには、次の利点があります。

- ルーティングワークロードが軽減されます。
- 登録キャパシティが増えます。
- 各メディアパケットが同じルートパスに従います。

重要: この機能は、MRA の導入にのみ適用されます。キャパシティの増加やその他の利点は、非 MRA Expressway 導入には適用されません。

高速パス登録は、次の SIP メソッドでサポートされています。登録。設定はコマンド ライン インターフェイスを通じて行う必要があります。詳細な手順については、最新の『*Expressway MRA 導入ガイド*』を参照してください。

この機能を設定した場合、スタンドアロンの Expressway MRA 導入(Expressway-C + Expressway-E) でテストした結果は次のとおりです。

プラットフォーム	MRA 登録	MRA ビデオコール	MRA 音声通話
CE 1200	7000	500	1000
大規模 OVA	3500	500	1000
中サイズ OVA	3000	150	300
小規模 OVA	2,500	100	200
小規模 OVA BE6K	2,500	100	200

Webex VDI over MRA

この項目は、MRA を展開する場合に適用されます。X12.7 から、Expressway は、互換性のある MRA で接続されたクライアントによる仮想デスクトップ インフラストラクチャ(VDI) を Webex でサポートします。

デフォルトの最小バージョンとしての TLS 1.2 の拡張

次の表に示されているように、追加サービス用のデフォルトの最小 TLS バージョンは TLS 1.2 になっています。デフォルトバージョン (および関連暗号) は、[メンテナンス(Maintenance)] > [セキュリティ(Security)] > [暗号(Ciphers)] ページで低いバージョン(非推奨) に設定できます。

サービス	設定項目
証明書のチェック機能	*HTTPS の最小 TLS バージョン*

Cisco Meeting Server の検出	*リバース プロキシの最小 TLS バージョン*
LDAP	*LDAP の最小 TLS バージョン*
SMTP メール クライアント (X12.7 からの TLS 証明書ベースの認証)	*SMTP の最小 TLS バージョン*
TMS プロビジョニングサービス	*TMS プロビジョニングの最小 TLS バージョン*
UC サーバディスカバリ(AXX クエリ)	*UC サーバ ディスカバリの最小 TLS バージョン*

TLS の変更 : TMS と CMS への影響

X12.7 から、デフォルトの最小 TLS バージョンが TLS 1.2 であるサービスに Cisco TMS と Cisco Meeting Server が含まれます。つまり、TLS 1.1 以下で CISCO TMS または Cisco Meeting Server が導入されている場合、TLS ハンドシェイクは失敗します。

TLS の変更 : LDAP への影響

X12.7 から、デフォルトの最小 TLS バージョンが TLS 1.2 であるサービスに LDAP が含まれます。つまり、TLS 1.1 以下で LDAP サーバが導入されている場合、ローカルの管理者のみがサインインすることが可能で、TLS ハンドシェイクが失敗します。**LDAP サーバが TLS 1.2** をサポートするまで(およびそれに合わせて[暗号(Ciphers)] ページが更新されるまで) 、リモートの管理者はサインインできません。

アップグレード時の設定変更 : [リモートのみ(Remote-only)] が自動的に [両方(Both)] に設定

この変更は、現在(このリリースにアップグレードする前に) **[ユーザ(Users)] > [LDAP 設定(LDAP configuration)]** ページで、管理者認証ソースの設定に [リモートのみ(Remote only)] を指定している場合に適用されます。リモートの管理者が、Expressway から意図せずにロックアウトされるのを避けるために、X12.7 以降にアップグレードすると、この設定は自動的に [両方(Both)] に変更されます。

アップグレードが完了した後、リモートの管理者のみが認証されるように、管理者のサインインを再度制限したい場合は、次の操作を実行します。

1. LDAP 接続のステータスが [利用可能(Available)] であることを確認します。
2. [ユーザ(Users)] > [LDAP 設定(LDAP configuration)] ページで、管理者認証ソースを *[リモートのみ(Remote only)]* に再設定します 。

TLS の変更 : SMTP への影響

X12.7 から、Expressway では、TLS 1.2 証明書ベースの検証を使用するために SMTP サービスが必要です。これらの設定の前提条件が実装されている必要があります。それ以外の場合、**アラーム ベースの電子メール通知(および他の SMTP ベースの機能) は失敗します**。

- SMTP サーバ証明書はクライアントによって検証されるため、その IP アドレスまたは FQDN が証明書の CN/SAN にある必要があります。
- SMTP サーバ証明書発行者を信頼できる CA 証明書リストにインポートする必要があります**([メンテナンス (Maintenance)] > [セキュリティ(Security)] > [Expressway の信頼できる CA 証明書(Trusted CA Certificate)])** にインポートする必要があります。

CBC 暗号を SSH デフォルト設定から削除

現在進行中のセキュリティ機能拡張の一部として、CBC モード暗号は SSH 用のシステムのデフォルト暗号設定に含まれなくなりました。アップグレードでは、デフォルト値が自動的に変更され、CBC 暗号 (aes129-cbc、aes-256-cbc、aes192-cbc) が削除されます。これらの暗号が必要な場合(非推奨) 、*xconfiguration Ciphers sshd_ciphers* コマンドを使用して再設定できます。

仮想化システム: VMware HA および DRS(手動) がテスト済み

Expressway バージョン X12.7 は、次の VMware 機能で正常にテストされました。

- **vSphere HA**(high availability) 。Expressway X12.7 を使用したテストで、VMware は ESXi クラスタ内の代替ホスト上の Expressway VM を再起動しました。VM が起動すると、VM はクラスタに正常に再参加しました。Expressway VM を新しいホストに移動すると、すべてのアクティブコールと登録がドロップされます。
- **DRS (分散リソーススケジューラ)** による vSphere HA。Expressway は**手動モード**の場合にのみ DRS でテストされ、サポートされます。予定されているメンテナンス期間中に、推奨される変更を実行してください。

仮想化システム: より最近の VM ハードウェアバージョン

この項目は、仮想化システムとして実行されている Expressway に適用されます。Expressway X12.7 は、VM ハードウェアバージョン 11 と互換性があります。

仮想化システム: 大規模または中規模の VM の ESXi 7.0

この項目は、仮想化システムとして実行されている Expressway に適用されます。Expressway X12.7 は VMware ESXi バージョン 7.0 と互換性があります。

仮想化システム: ESXi 6.0 の廃止

この項目は、仮想化システムとして実行されている Expressway に適用されます。VMware ESXi6.0 は Expressway システムで廃止されました。

LDAP 認証検索の最適化

この項目は、Expressway 管理者のリモートアカウント認証を許可する場合に適用されます。これらの管理者は LDAP 接続を介してリモートディレクトリサービスを認証します。Expressway にサインインしようとしたユーザが、許可されている管理者グループのメンバーであること確認する LDAP 検索メカニズムは、特に多くのサブグループが関連している場合など、長時間かかる可能性があります(バグ ID CSCvs44968 参照) 。X12.7 には、LDAP 検索を最適化するための新しい設定が、**[ユーザ(Users)] > [LDAP 設定 (LDAP configuration)]** ページにあります。

検索するサブグループのネストレベル

LDAP 検索のグループの深さを制限するために使用されます。最適な検索パフォーマンスのために、リモート管理者の上位レベルのグループを Expressway の(管理者) グループとして定義し、検索深さを「1」に設定します。デフォルト値は「16」です。

すべてのメンバーのルックアップをスキップ

認証検索プロセス中に管理者グループのメンバールックアップを無効または有効にするために使用されます。デフォルトは [はい (Yes)] で、メンバールックアップをスキップします。

設定されているグループのメンバー数が相対的に多い場合は、この設定を [はい(Yes)] のままにしておくことをお勧めします。ただし、設定されているグループのメンバーが相対的に少ない導入では、[いいえ(No)](メンバールックアップを行う) に設定すると、認証の遅延が減少する場合があります。

コマンドライン インターフェイス

この設定は、Expressway CLI で次の 2 つの新しいコマンドを使用して設定することもできます。

- *xconfiguration Login Remote LDAP SearchOptimize NestedDepth: <1..16>*
- *xconfiguration Login Remote LDAP SearchOptimize SkipMembers: <Yes/No>*

(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

Expressway は、プレビューベースでのみ、X12.6 から HSM をサポートしています。

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 は、現在、(プレビュー ベースで)、HSM プロバイダーとして、Entrust nShield Connect XC をサポートしています。設定手順といくつかの重要な注意事項および制限については、付録 1: Expressway での HSM デバイスの構成 , ページ 36で詳しく説明します。

重要: Gemalto の「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 Jabber の SIP 登録フェールオーバー - MRA 導入

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。保留中のソフトウェア依存関係のため、現在、これはプレビューステータスで提供されています。

Expressway X12.7 は、MRA を経由して接続する Cisco Jabber クライアントのフェールオーバー時間が大幅に改善される多数の MRA フェールオーバー更新など、クラスタ化された Expressway に対する既存のフェールオーバー機能を基に構築されています。更新には、適応型ルーティング、STUN キープアライブのサポート、改善されたエラー レポートが含まれます。

これらの新しい機能により、Jabber クライアントは音声とビデオの MRA 高可用性(フェールオーバー) をサポートできます。

適応型ルーティング

Expressway X12.7 の適応型ルーティングの更新により、Expressway はルーティングパスを動的に変更することができます。ノード障害が検出されると、パケットは稼働中のピアノードに再ルーティングされます。たとえば、リモート Jabber クライアントが、特定の Expressway-E(EXWY-E1) 、Expressway-C(EXWY-C1) 、Unified CM(CUCM1) の組み合わせを経由する SIP REGISTER を送信し、指定された Expressway-C ノードがダウンしているか、メンテナンスモードにあるとします。この場合、メッセージはピア Expressway-C ノード(EXWY-C2) に再ルーティングされ、目的の Unified CM 接続先に転送されます。登録後、Cisco Jabber はルーティングテーブルも更新し、今後の SIP メッセージで登録パスが使用されます。

注: フェールオーバーにはコールの保存は含まれません。Jabber の登録は新しい登録パスにフェールオーバーされますが、失敗時のアクティブコールはドロップされます。

STUN キープアライブのサポート

Expressway X12.7 は、適応型ルーティングに加えて、MRA で接続された Jabber クライアントによる STUN キープアライブの使用をサポートします。リモート Jabber クライアントは、Expressway-E を介して STUN キープアライブをエンタープライズ ネットワークに送信し、接続の問題を前もって学習します。その結果、登録パス内のノードが失敗した場合、Jabber は STUN 応答の受信後の失敗について学習し、今後の SIP メッセージ用に別のルートパスを選択できます。

要件

特定の設定は必要ありません(当然ながら、必要なクラスタリング/バックアップノードが存在していることを条件とします) 。ただし、次の最小リリースを実行している必要があります。

ルーティング機能	最小リリーズ
適応型ルーティング	Expressway X12.7 Cisco Jabber 12.9 MR
STUN キープアライブ	Expressway X12.7 Cisco Unified Communications Manager 14 Cisco Jabber 12.9MR

すべてのソフトウェア要件による多くの利点

3 つのコンポーネント(クライアント、Expressway、Unified CM) すべてが、高い登録フェールオーバー機能で更新されたソフトウェアを実行している場合、次の利点があります。

- フェールオーバーにユーザアクション不要
- フェールオーバー時間の短縮：従来の 120 秒の標準から最長で 30 ～ 60 秒
- ルートパスが動的に更新され、サーバの障害を処理
- 目的の接続先に到達するために利用可能なルートの数が多い
- リモート Jabber クライアントは、STUN キープアライブを使用してサーバの障害を学習し、ルーティングを前もって調整できます。

Unified CM アップグレードなしの適応型ルーティングの利点

新しい Unified CM ソフトウェアなしでも(ただし、新しい Expressway および Jabber ソフトウェアを使用) 、この機能は Jabber クライアントがパスの障害を検出できる利点があります。このアクションには 2 分を超える時間がかかる場合があること。および実際はサーバがアイドル状態にあるか、その時点での使用が少ない一部のシナリオで、Expressway は、Unified CM サーバを非アクティブとしてフラグを立てる可能性があることに注意してください。

(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) モバイルアプリケーション管理クライアントを使用したプッシュ通知：MRA 導入

この機能は、MRA を使用する Expressway を導入する場合に適用されます。これは現在プレビュー ステータスで提供されています。

この機能により、MRA を介したプッシュ通知サポートには、Jabberintune や Jabberblackberry のようなモバイルアプリケーション管理(MAM) クライアントのサポートが含まれるようになりました。この結果、プッシュ通知サービスは、Jabberintune および Jabberblackberry クライアントを実行しているすべてのデバイスで使用できます。

(プレビュー) Android デバイスでのプッシュ通知 - MRA 導入

この機能は、MRA を使用する Expressway を導入する場合に適用されます。X12.6 では、外部の製品バージョンの依存関係によって、プレビューステータスのみで導入されました。

X12.6.2 では、この機能は既知の問題(バグ ID CSCvv12541 参照) のため、デフォルトでオフに切り替えられました。

X12.7 で、バグ ID CSCvv12541 は修正されています。ただし、この機能はソフトウェアの依存関係が保留中のため、プレビューステータスのままです。

Android デバイスのプッシュ通知を有効にする方法

この機能は、Expressway コマンド ライン インターフェイスを介して有効化されます。Android ユーザにサービスを提供する IM and Presence Service のすべてのノードがサポートされるリリースを実行している場合にのみ、これを行います。

CLI コマンドは、xConfiguration XCP Config FcmService: On です。

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。

(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) 。

UI からのサポートされていない機 能 の継 続 的 な削 除

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 6

今 回 のリリースでのその他 の変 更 点

接続マネージャーログが改善されました。

*Expressway MRA 導入ガイド*のレイアウトとコンテンツが拡張されました。

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

構成 API	API が導入されたバージョン
専用管理インターフェイス(DMI)	X12.7
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

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 モードで実行する場合は、必要ありませんし、適用しないことを推奨します。**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。

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)
- X12.7.1 で解決済みの問題
- X12.7 で解決済みの問題

このバージョンで特に重要な問題

Jabber Guest サービスをホスティングしているホスティングしている単一の NIC Expressway-E でリッチ メディア セッション ライセンスが使用されない CSCva36208

X8.8 でライセンス モデルを変更すると、Expressway-E サーバの Jabber Guest サービスのライセンスに関する問題が発生します。Expressway ペアが「単一の NIC」Jabber Guest 展開の一部である場合、Expressway-E は Jabber Guest コールごとに 1 つの RMS ライセンスをカウントする必要がありますが、そうではありません。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。

デュアル NIC Jabber Guest の導入を推奨します。単一の NIC 展開を使用している場合は、今後のアップグレードでサービスの継続性を確保するために、Expressway-E のサーバが正しくライセンスされていることを確認してください。

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**(「プレビュー機能の免責事項, ページ 1」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

- 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。
- 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 以降は、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。詳細については、*「シスコ高速道路を介したモバイルおよびリモートアクセス」*の*「モバイルおよびリモートアクセスを使用したサポートされているキー機能とサポートされていない機能 」*を参照してください。

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。

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

- この問題は、Expressway が VMWare vCenter 7.0.x を使用して特定の ESXi バージョンを備えた仮想化システムとして実行されている場合に適用されます。これは、ESXi 6.7.0 で VMWare vCenter 7.0.1 を使用して Expressway OVA を導入するテスト中に検出されました。[OVF テンプレートの導入 (Deploy OVF Template)] ウィザードの [準備完了 (Ready to complete)] 最終ページには、前のウィザード ページで入力された実際の値ではなく、テンプレートの値が表示されます。問題は表面的であり、[完了 (FINISH)] をクリックすると、OVA は入力された値を使用して期待通り展開されます。バグ ID CSCvw64883 を参照してください。
- 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。

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。

相互運用性および互換性

詳細マトリックス

Expressway および他の Cisco Telepresence 製品の相互運用性テストの結果は、次の場所で入手できます。https://tp-tools-web01.cisco.com/interop/

Cisco Collaboration Systems Release (CSR) セット内の製品互換性マトリックスは、次の場所で入手できます。https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/unified/communications/system/Compatibility/CSR-Compatibility-Matrix-InteractiveHTML.html Expressway のエントリは、「Enterprise Edge」セクションにあります。

モバイル & リモート アクセス

MRA 向けの互換製品に関する情報は、*Expressway MRA 導入ガイド*のインフラストラクチャ製品およびエンドポイントのバージョン表を参照してください。

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：X12.7.1

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、X12.7.1 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 X12.7.1 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 26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の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. [システムの再起動(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 39

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の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. [システムの再起動(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 39
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)] フィールドにバグ識別子を入力し、[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 37」(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 (continued)

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 (continued)

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 (continued)

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

Cisco の商標または登録商標