Cisco Expressway リリース ノート（X14.0）

初版：2021 年 4 月 14 日

最終更新：2021 年 5 月 25 日

このマニュアルについて

このドキュメントでは、以下のトピックを扱います。

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。

はじめに

変更履歴

表 *1:* リリース ノートの変更履歴

日付	変更内容	理由
2021 年 6 月	X14.0.1 用の初版	X14.0.1 リリース
2021 年 5 月	「MRA に関する制限事項」セクションに制限事項を追加。	X14.0 リリース：再発行
2021 年 4 月	X14.0 用の初版	X14.0 リリース
2020 年 12 月	X12.7 用の初版	X12.7
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	X12.6 用の初版	X 12.6

サポートされるプラットフォーム

表 *2:* このリリースでサポートされている *Expressway* プラットフォーム

プラットフォーム名	シリアル番号	ソフトウェア バージョンのサポート範囲
小規模 VM（OVA）	（自動生成）	X8.1 以降
中規模 VM（OVA）	（自動生成）	X8.1 以降
大規模 VM（OVA）	（自動生成）	X8.1 以降

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
CE1200 Hardware Revision 2（UCS C220 M5L にプレインストール）	52E1####	X12.5.5 以降。
CE1200 Hardware Revision 1（UCS C220 M5L にプレインストール）	52E0####	X8.11.1 以降。
CE1100（UCS C220 M4L にプレインストールされた Expressway）	52D#####	メンテナンスとバグ修正のみを目的とする X12.6.x バージョンでの限定的なサポートを除き、（X12.5.x 以降）サポートされていません。
CE1000（UCS C220 M3L にプレインストールされた Expressway）	52B#####	サポート対象外（X8.10. x 以降）
CE500（UCS C220 M3L にプレインストールされた Expressway）	52C#####	サポート対象外（X8.10. x 以降）

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。詳細は https://www.cisco.com/c/en/us/products/collateral/unified-communications/telepresence-video-communication-server-vcs/eos-eol-notice-c51-743969.html で確認できます。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：販売終了のお知らせ

Cisco Expressway CE500 および CE1000 アプライアンスのハードウェア プラットフォームは、シスコによるサポートが終了しています。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：販売終了およびハードウェア サービス サポート終了の事前通知。

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、アプライアンスのハードウェア サポート サービスを終了します。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、「販売終了の通知」[英語] を参照してください。

相互運用性および互換性

製品の互換性情報

詳細マトリックス

Cisco Expressway は標準ベースであり、シスコ製とサードパーティ製の両方の標準ベース SIP 機器および H.323 機器と相互運用できます。特定のデバイスとの相互運用性については、シスコの担当者にお問い合わせください。

モバイル & リモートアクセス（MRA）

特に MRA に関して互換性のある製品については、『Cisco Expressway 経由での Mobile and Remote Access 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に記載しています。

どの Expressway サービスを同時に実行できますか。

『Cisco Expressway 管理者ガイド』で、どの Expressway サービスが同じ Expressway システムまたはクラスタで共存できるかについて詳細に説明しています。「概要」セクションにある「同時にホストできるサービス」「」の表を参照してください。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。

X14.0 の機能のサマリー

Note この表は変更される場合があります。

Table 3: リリース番号別の機能

機能/変更	ステータス（Status）
SSO/OAuth サインインでの URI リダイレクトのサポート	X14.0 以降でサポート
AV1 のサポート	X14.0 以降でサポート
“Jabber のゼロ ダウンタイム”での XCP サポート	X14.0 以降でサポート
P2P からミーティングへのエスカレーション	X14.0 以降でサポート
Expressway クラスタのロード バランシングは SIP フェデレーションには適用されない	X14.0 以降でサポート

機能/変更	ステータス（Status）
Cisco Jabber の MRA SIP 登録フェールオーバー	X14.0 以降でサポート
ハードウェア セキュリティ モジュール（HSM）のサポート	プレビュー
MRA 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

削除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、機能が製品から削除されることや、以降のリリースで機能のサポートが終了することを意味する廃止となることがあります。この表は、現在廃止ステータスである機能、または X12.5 以降で削除された機能の一覧です。

表 *4*：廃止および削除された機能

機能/ソフトウェア	ステータス（Status）
VMware ESXi 6.0（VM ベースの展開）	非推奨メソッド
Cisco Jabber Video for TelePresence（Movi） （注） TelePresence 版 Cisco Jabber Video（ビデオ コミュニケーションで Cisco Expressway と連携して動作）に関連するものであり、Unified CM と連携して動作する Cisco Jabber ソフトウェア クライアントには該当しません。	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 で削除
Expressway 組み込み転送プロキシ	X12.6.2 で削除
Cisco Advanced Media Gateway	X12.6 で削除
VMware ESXi 5.x（VM ベースの展開）	X12.5 で削除

レイ・バウム法に対するサポートなし

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 Communications 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 エンジニアが提供する、Expressway の一般的な構成手順に関するビデオは、Expressway/VCS スクリーンキャスト ビデオ リスト ページで利用できます（「Expressway videos」 で検索）。
インストール：仮想マシン	Expressway インストール ガイド ページの『仮想マシンでの Cisco Expressway インストレーション ガイド』
物理アプライアンスのインストール	Expressway インストール ガイド ページの『Cisco Expressway CE1200 アプライアンス インストール ガイド』
シングルボックス システムの基本設定	Expressway コンフィギュレーション ガイド ページの『Cisco Expressway Registrar Deployment Guide（Cisco Expressway レジストラ導入ガイド）』
ペアリングされたボックス システムの基本設定（ファイアウォール トラバーサル）	Expressway コンフィギュレーション ガイド ページの Cisco Expressway-E および Expressway-C の『基本設定導入ガイド』
管理およびメンテナンス	*Expressway* メンテナンスとオペレーション ガイド ページの『Cisco Expressway 管理者ガイド』http://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-maintenance-guides-list.html（有用性情報を含む）
クラスタリング	Expressway コンフィギュレーション ガイド ページの『Cisco Expressway クラスタの作成とメンテナンス導入ガイド』
証明書	Expressway コンフィギュレーション ガイド ページの『Cisco Expressway 証明書の作成と使用に関する導入ガイド』
ポート	Expressway コンフィギュレーション ガイド ページの『Cisco Expressway IP Port Usage Configuration Guide（Cisco Expressway IP ポートの使用コンフィギュレーション ガイド）』
モバイル & リモート アクセス	Expressway コンフィギュレーション ガイド ページの『Cisco Expressway 経由の Mobile and Remote Access 導入ガイド』

Cisco Meeting Server	Expressway コンフィギュレーション ガイド ページの『Cisco Meeting Server with Cisco Expressway Deployment Guide（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 Reference Guide（Cisco Meeting Server API リファレンス ガイド）』 Cisco Meeting Server のその他のガイドは、Cisco Meeting Server コンフィギュレーション ガイド ページに用意されています。
Cisco Webex ハイブリッド サービス	ハイブリッド サービス ナレッジ ベース
Cisco Hosted Collaboration Solution（HCS）	HCS のお客様用マニュアル
Microsoft インフラストラクチャ	Expressway コンフィギュレーション ガイド ページの『Cisco Expressway with Microsoft Infrastructure Deployment Guide（Microsoft インフラストラクチャを使用した Cisco Expressway 導入ガイド）』 Expressway コンフィギュレーション ガイド ページの Cisco Jabber およびビジネス版 Microsoft Skype のインフラストラクチャ構成チートシート
REST API	Expressway コンフィギュレーション ガイド ページの『Cisco Expressway REST API Summary Guide（Cisco Expressway REST API サマリー ガイド）』（API は自己記述されているため概要レベルの情報のみ）
MultiWay 会議	Expressway コンフィギュレーション ガイド ページの『Cisco TelePresence Multiway Deployment Guide（Cisco TelePresence Multiway 導入ガイド）』

X14.0 の機能と変更点

セキュリティ機能の拡張

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。その大半については目に見える変化はありませんが、ユーザ インターフェイスや構成に影響を与える変更もあります。

- 管理者は、TCP ポート 22 で SSH 暗号を構成できるようになりました。これは、Web インターフェイスから構成可能であり、Expressway SSH 構成を更新するのに CLI コマンドを使用する必要はありません。
- シスコ製品セキュリティ ベースラインを満たすために、以下のサービスの暗号フィルタが更新されています。

- リバース プロキシで使用される SSL 暗号
- Apache で使用される SSL 暗号
- UC サービス検出で使用される SSL 暗号
- XMPP で使用される SSL 暗号
- LDAP 用の SSL 暗号

- シスコ製品セキュリティ ベースラインを満たすために、SSH キー構成の暗号アルゴリズムが更新されています。許可されない一部のキー交換アルゴリズムは削除されています。
  - ecdh-sha2-nistp521
  - ecdh-sha2-nistp384

  以下のキー交換アルゴリズムが追加されています。
  - ecdh-sha2-nistp256
  - diffie-hellman-group14-sha256
  - diffie-hellman-group14-sh1

- Expressway-E は、サイレント SIP スキャン（SIP OPTIONS を使用）およびスパム コール（SIP INVITE を使用）の対象になります。これは DoS 攻撃と似ています。この SIP ベースの DOS 攻撃から保護するために、次の条件で Fail2Ban での SIP 認証の失敗が有効になります。
  - X14.0 以降のバージョンからの Expressway の新規インストール
  - X14.0 以降のバージョンでの初期設定へのリセット

- X14.0 リリースから、SIP トランザクションのレート制限を構成できます。Web UI から、1 秒あたりの接続数および限界値を、有効化/無効化するか、変更することができます。デフォルトでは、1 秒あたりの接続数は 100 で、限界値は 20 です。
- X14.0 リリースから、自動保護、または SIP 登録の失敗の検出システムが拡張され、以下の状況に対応しました。
  - ライセンス制限の超過
  - メンテナンス モード
  - ポリシーによる禁止
  - リソース不足
  - 登録の禁止

- X14.0 リリースから、CPU が低速でメモリ容量も少ないサブスペックのハードウェアで Expressway VM が実行されている場合、サポートされていないか非準拠のハードウェアに関する警告アラームが表示されます。

- X14.0 リリースから、MRA を介した CUCM/電話機のセキュリティ機能のサポートの一部として、OAuth 対応の MRA クライアントが構成ファイルをダウンロードするための HTTPS 許可リストにポート 6971 が追加されています。
- X14.0.1 以降のリリースでは、複数の管理者アカウントとグループに CLI アクセス権を設定できます。詳細については、「管理者アカウントとフィールド参照について」を参照してください。
- X14.0.1 リリースから、信頼ストアとオンボーディング信頼ストアに、管理者に通知するための 2 つの新しいアラームが導入されます。
  - 証明書が 21 日以内に期限切れになることを示すアラーム
  - 証明書の有効期限が切れたことを示すアラーム

リダイレクト URI のサポート

Webex クライアントの埋め込みブラウザのサポート

Expressway X14.0 リリースから、Webex 機能の SSO リダイレクト URI を有効化または無効化する切り替えが提供されます。この機能により、Cisco Jabber/Webex クライアントの埋め込みブラウザのサポートにおけるセキュリティが向上し、次のような利点が得られます。

- RFC7636 を使用して「認可コードの横取り攻撃」から保護します。
- iOS 以外のオペレーティング システムで実行されているクライアントで Android などの埋め込みブラウザを使用できます。
- Jabber クライアントと Webex クライアントで、Unified Communications Manager（および MRA）の OAuth フローに埋め込みブラウザを使用できます。
- Webex クライアントおよび Unified Communications Manager Calling を使用する際のユーザ エクスペリエンスが向上します。

詳細については、『Cisco Expressway 経由での Mobile and Remote Access 導入ガイド』を参照してください。

AV1 のサポート

Expressway X14.0 リリースから、メディアを確立するための AV1 コーデックのネゴシエーションとパススルーがサポートされます。コーデックは、SIP トラバーサル コール（Expressway がメディア ストリームを処理しているコール）でサポートされます。

P2P からミーティングへのエスカレーション

Webex ユーザは、1:1 の SIP コール中に Webex ミーティングをコールし、次のようなミーティング機能を呼び出すことができるようになりました。

- ビデオ参加者の追加

- Webex Assistant の使用
- ホワイトボードの使用

エスカレーション プロセス中に、追加の参加者を招待するのか、単に 1:1 のコールを 1:1 のミーティングに移行するのかオプションを選択できます。既存のオーディオチャンネル（モバイルまたはデスクフォン）を維持しながら、別のデータ チャンネルを介してビデオを強化したり共有したりするオプションも選択できます。

Expressway クラスタのロード バランシングは SIP フェデレーションには適用されない

SIP フェデレーションに使用される Expressway 展開では、Expressway に対する SIP ボリュームの負荷が常に高くなり、SIP ボリュームを処理するために複数のピアが必要になります。Expressway では、このトラフィックを Expressway Edge トラバーサル サーバに均等に分散することができませんでした。

Expressway X14.0 リリースから、トラバーサル ゾーン接続全体でトラフィックを適切に負荷分散できます。

Jabber のゼロ ダウンタイムでの XCP サポート

Expressway X14.0 リリースから、Jabber クライアントとのデュアル接続がサポートされます。このタイプの接続をクライアント側で有効にすると、高可用性フェールオーバーイベント中のサービス ダウンタイムがゼロになります。

これは、次の場合に役立ちます。

- アップグレード中に Jabber クライアントのサービスの中断を最小限に抑えます。
- プライマリ ノードとセカンダリ ノードの間でユーザ セッションのシームレスな移行を実現します。

Cisco Jabber の SIP 登録フェールオーバー：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。

Expressway X14.0 は、クラスタ構成の Expressway 向けの既存のフェールオーバー機能を基に構築されており、MRA を介して接続する Cisco Jabber クライアントのフェールオーバー時間を大幅に改善する MRA フェールオーバーの更新が多数適用されています。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 クライアントで音声とビデオの MRA 高可用性（フェールオーバー）をサポートできます。

詳細については、『Cisco Expressway 経由での Mobile and Remote Access 導入ガイド』を参照してください。

（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 X12.6 リリースから、HSM 機能はプレビュー ベースでのみサポートされます。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、アイデンティティ、データベースで使用する暗号化、復号化、認証などの重要な機能向けに暗号処理を提供します。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、ハードウェアとソフトウェアの改ざんを防ぎます。

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

Expressway では現在、（プレビュー ベースで）HSM プロバイダーとしてのみ Entrust nShield Connect XC をサポートしています。

重要 Gemalto の 「SafeNet Luna」 ネットワーク デバイスは Expressway のユーザ インターフェイスでも参照されますが、**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 and Remote Access を使用して Expressway を展開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。

詳細は、次の場所にあるホワイト ペーパー『Cisco Headset and Finesse Integration for Contact Center（Contact Center 向けの Cisco ヘッドセットと Finesse の統合）』に記載されています。
https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/cucm/whitePaper/CUCM_Headsets_for_ContactCenter_WP.pdf

（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 展開

この機能は、Mobile and Remote Access を使用して Expressway を展開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。

この機能を使用すると、Jabberintune や Jabberblackberry などのモバイル アプリケーション管理（MAM）クライアントが、Mobile and Remote Access を介したプッシュ通知のサポート対象になります。その結果、Jabberintune クライアントや Jabberblackberry クライアントを実行しているすべてのデバイスでプッシュ通知サービスを利用できます。

（プレビュー）Android デバイスでのプッシュ通知：MRA 展開

この機能は、MRA を使用して Expressway を展開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り、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、既知の問題（バグ ID CSCvv12541 参照）により、この機能は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 は修正されました。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。**この操作は、Android ユーザにサービスを提供する IM and Presence Service のすべてのノードでサポート対象のリリースを実行している場合にのみ**実行します。

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 and Presence サービスが中断されます。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）。

サポートされていない機能の UI からの削除（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、「削除または廃止された機能とソフトウェア」を参照してください。

X14.0 リリースではこの点に変更はありません。

今回のリリースでのその他の変更点

- 『*Expressway* 経由の *Mobile and Remote Access* 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。

- Expressway X14.0 リリースから、UI ページの [診断ロギング（Diagnostic Logging）] セクションに次のフィールドが追加されました。
  - IP アドレスで tcpdump をフィルタリングする（Filter tcpdump by IP address）
  - ポートで tcpdump をフィルタリングする（Filter tcpdump by port）

  これらのフィールドは、[ロギングの進行中に tcpdump を採取する（take tcpdump while logging）] オプションを選択している場合に表示され、IP アドレスまたはポートで tcpdump をフィルタリングするのに役立ちます。
- Expressway X14.0 リリースから、PAK ベースのサポート終了を示す次のメッセージが PAK のライセンス ページに表示されます。

  「PAK ベースのライセンスのサポートは、Expressway の今後のリリースで終了する予定です。スマート ライセンスを推奨します。詳細については、『Cisco Expressway 管理者ガイド』を参照してください。」

  スマート ライセンスは PAK ベースのライセンスよりも推奨されており、既存の PAK ベースのライセンスをスマート ライセンスに転換するオプションが用意されています。
- Expressway X14.0 リリースから、アップグレード中に表示される可能性のある構成エラー、Expressway をインストールした後の不良構成、必要な外部リソースの可用性を検出するのが困難であるといった問題をクライアントに通知するアラームが導入されました。このアラームは、構成エラーを特定するのに役立ち、発生する可能性のある問題の診断と修正を容易にします。

REST API への変更点

リモート構成を効率化するために、Expressway 用の REST API を利用できます。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。新機能の追加にあたって、REST API から構成、コマンド、およびステータス情報にアクセスする手段を追加していますが、同時に、以前の Expressway のバージョンで導入された一部の機能に REST API を選択的に改良しています。

API は、RAML を使用して自己記述されており、`https://<ipaddress>/api/raml` で RAML の定義にアクセスできます。

構成 API	API が導入されたバージョン
SNMP 構成	X14.0.1
アラーム：表示および確認	X14.0.1
専用管理インターフェイス（DMI）	X12.7
Diagnostic Logging	X12.6.3
スマート ライセンス	X 12.6
クラスタ	X8.11

構成 API	API が導入されたバージョン
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 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展開の場合は、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。License Registration Portal 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 * [1]	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-ルーム（*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

[1] 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

（X12.5.4 以降）以下のキーは不要で、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、必要ではありませんが、キーを適用しても問題ありません。

（注） 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、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）

PID	キー	オプション
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）

（注） 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 製品との相互運用性

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報告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**。cisco.com への直接接続がない場合に使用されます。Smart Account の同期を手動でアップロードおよびダウンロードする必要があります。

スマート ライセンスの重要な設定情報

> **注意** Web インターフェイスを使用してスマート ライセンスを [オン（On）] に設定すると、[オフ（Off）] にリセットすることはできなくなります。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 製品インスタンスを登録するときに登録サーバとの通信に問題が発生した場合、次のメッセージが表示されて登録が失敗します。

  ```
  □□□□□ □□□□□□□ □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□HTTP Server
  Error 200□□□□□□□□ □□□□□□□□□
  ```

  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ーの詳細については、Smart Software Manager オンプレミスを参照してください。

スマートライセンスの構成方法の詳細については、『*Cisco 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

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）
- X14.0 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 サービスをホストする単一 NIC Expressway-E でリッチ メディア セッション ライセンスが消費されません。

CSCva36208

X8.8 のライセンス モデルを変更すると、Expressway-E サーバ上の Jabber Guest サービスのライセンスに関する問題が明らかになります。Expressway のペアが「単一 NIC」 Jabber Guest 展開の一部である場合、Expressway-E では 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、そうなっていません。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 の展開を推奨します。単一 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 のライセンスが正しく適用されていることを確認してください。

制限事項

一部の Expressway 機能はプレビューであるか、外部の依存関係がある

シスコでは、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。それでもこの機能を使用することでユーザがメリットが得られる場合は、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、**実稼働環境で業務に使用するのは推奨しません**（「プレビュー機能の免責事項」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、ノートの X14.0 の機能のサマリーの表に記載されています。

サポートされていない機能

現在、クラスタ展開内の Expressway のノードの 1 つ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、Unified CM が再起動した場合は、影響を受ける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、以前のリリースでは見落としによりドキュメント化されていませんでした。バグ ID CSCtr39974 を参照してください。

Expressway が DTLS を終了することはありません。メディアを保護する目的では DTLS はサポートされておらず、コールを保護するのには SRTP が使用されます。Expressway を介した DTLS コールの試行は失敗します。DTLS プロトコルは SDP に挿入されますが、暗号化された iX プロトコルを通過する場合に限ります。

X12.5 から、Expressway は、RFC 4028 で指定されているように、セッションの更新のみを目的として、MRA 接続を介した SIP UPDATE のサポートを限定的に提供します。ただし、この機能を使用するための特別な要件がない場合は、この設定をオンにしないでください。SIP UPDATE のその他の使用はサポートされておらず、このメソッドに依存する機能は期待どおりに機能しません。

Cisco VCS は SIP UPDATE メソッド（RFC 3311）をサポートしていないため、このメソッドに依存する機能は期待どおりには動作しません。

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 から、セキュリティ強化により、Expressway-E の 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 リクエストを受け付けません。

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 with Microsoft Infrastructure Deployment Guide（Microsoft インフラストラクチャによる Cisco Expressway 導入ガイド）』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、到達不能な 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 を使用している（かつ Expressway-E が TURN サーバとして構成されている）場合は、先に Meeting Server ソフトウェアをバージョン 3.0 にアップグレードするか、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。これは、他の Meeting Server バージョンでは、Expressway-E の TURN サーバに対して STUN バインド リクエストを使用することが理由です（Expressway-E の TURN サーバ構成の詳細については、『*Cisco Expressway Web Proxy for Cisco Meeting Server Deployment Guide*（*Cisco Meeting Server* 用 *Cisco Expressway Web* プロキシ導入ガイド）』を参照してください）。

Cisco Webex ハイブリッド コール サービス

Expressway X12.6 以降は、ハイブリッド コール サービスの展開で必要となるコール コネクタ ソフトウェアをホスティングする目的では機能せず、Expressway コネクタ ホスト用にサポートされている旧バージョンを使用する必要があります。詳細については、ハイブリッド コール サービスの既知の問題と Expressway バージョンのサポートに関するドキュメント（https://help.webex.com/）を参照してください。

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しないでください。既知の問題により、一部のライセンスだけ変換することを選択すると、残りのライセンスも自動的に無効になるか削除されます。そのため、変換しないライセンスも削除され、回復するためにはライセンス 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）] フィールドと [利用可能数量（Quantity Available）] フィールドの値が同じ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の状態です。

リダイレクト URI のサポート

クラスタ展開で、Expressway-E が 2 つの異なる送信元 IP アドレスを検出した場合、この機能は動作しません。たとえば、モバイルの Jabber クライアントまたは Webex クライアントの IP アドレスが、モバイルの外部ブラウザのアドレスと異なる場合です。これは次のことが原因で起こる場合があります。

- モバイル ローミング中に IP アドレスが変更された

- ユーザが、複数のパブリック IP アドレスを使用して NAT 用に設定されたファイアウォールの背後にいる場合
- 分割 VPN 構成

クラスタ化されたシステムのスタティック NAT

X 12.5.5 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 X 12.5.3 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

Mobile & Remote Access（MRA）用に 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、サポートされない主な機能のリストについては、『Cisco Expressway 経由の Mobile and Remote Access』ガイドで、Mobile and 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が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 Mobile and Remote Access』ガイドの MRA 要件に関するセクションを参照してください 。

1. 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リクエストします。
- 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 を変更するようにリクエストします。

2. Mobile and Remote Access（MRA）を介した Unity ボイスメールは、X14.0 リリースでは機能しません。この問題は今後のリリースで修正される予定です（バグ ID CSCvy29217 を参照）。

（注） Unity ボイスメール機能が重要である場合は、アップグレードしないでください。

MRA SIP 登録のフェールオーバー

7800/8800 シリーズの電話機および Jabber などのその他のエンドポイントが、最初に OAuth トークンを発行した CUCM サブスクライバ上の OAuth トークンを更新したが、トークンの更新中に到達できなかった場合、OAuth トークンの更新は行われません。

OAuth トークンの更新を有効にする手順は次のとおりです。

- Jabber 側で Jabber に再ログインします。

- 7800/8000 シリーズの電話機で、電話機をリセットします。

クラスタ内の複数の Expressway ノードが到達不能な場合、Expressway は既存の MRA 登録の負荷分散を行えません。

Jabber クライアントが登録されている Expressway-E または Expressway-C のノードでサービスが停止すると、Jabber MRA クライアントは自動的に登録を代替パスに移動します。また、Expressway-E または Expressway-C のノードがオンライン状態に戻ったときに、既存の負荷はそのノードには分散されません。これは、一部の Expressway ノードの使用率が他のノードよりも高くなる可能性があることを意味します。

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 が設定されている場合。

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 Deployment Guide（Expressway MRA 導入ガイド）』 https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-and-configuration-guides-list.html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。

（注） 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 Deployment Guide（Expressway MRA 導入ガイド）』の「MRA アクセス制御の設定」セクション、および『Deploying OAuth with Cisco Collaboration Solution（Cisco Collaboration Solution 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偽アラーム

新しいピアがクラスタに追加されたときに、クラスタが実際に正しく構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（Cluster communication failure: Unable to establish...）」）が発生す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 バージョンを導入し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、VMware vCenter 7.0.1 と ESXi 6.7.0 を使用して Expressway OVA を展開するテスト中に特定されました。[OVFテンプレートの展開（Deploy OVF Template）] ウィザードの最終ページである [準備完了（Ready to complete）] に、その前のウィザード 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。この問題は表面的なものであり、[完了（FINISH）]「」をクリックすると、入力された値を使用して想定どおりに OVA が展開されます。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。
- 物理的な Expressway アプライアンスでは、[高度なネットワーク（Advanced Networking）] 機能を使用することで、構成したイーサネット ポートごとに速度とデュプレックス モードを設定できます。仮想マシンベースの Expressway システムでは、イーサネット ポートごとに速度を設定することはできません。

  また、仮想マシンベースのシステムでは、実際の物理的NIC速度に関係なく、Expressway とイーサネット ネットワークの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* インストール 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 インストール ガイド』に詳述されている Expressway ソフトウェアの最小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 を使用してトラバーサル サーバまたは Expressway シリーズの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場合、Expressway が、システムを自動的に大規模システムに変換します。これは、Expressway-E は、中規模システム用に構成された逆多重化ポートではなく、大規模システム用のデフォルトの逆多重化ポート（36000 ～ 36011）で多重化 RTP/RTCP トラフィックをリッスンすることを意味します。この場合、ポート 36000 ～ 36011 はファイアウォールで開かれていないため、Expressway-E はコールをドロップします。

回避策

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

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、X8.10.3 以降で、新しい Expressway 言語パックが提供されます。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.）。パックのインストールまたは更新の手順については、*Expressway* の管理者ガイドを参照してください。

IM&P ノード障害での XMPP フェデレーションの動作

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にフェールオーバーしても、影響を受けるユーザーは他のノードに動的に移動されないことに注意してください。Expressway はこの機能をサポートしておらず、テストされていません。

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

この問題は、デュアル NIC Expressway-E を使用して Expressway を展開する場合に該当します。Expressway-C を使用するインターフェイスと外部インターフェイスの両方に同じ（重複する）静的ルートが適用される場合に、Cisco Webex Calling リクエストが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という現在の Expressway-E のルーティング動作に起因します。

（注） 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 と Meeting Server を介してデュアルホーム会議を使用する場合は、最大 SIP メッセージサイズを 32768 バイト（デフォルト）以上に設定する必要があります。大規模な会議（つまり、約 9 人以上の参加者から）に対して、より大きな値が必要になる可能性があります。[構成（Configuration）] > [プロトコル（Protocols）] > [SIP] を選択し、[SIP最大サイズ（SIP max size）] で定義します。

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。

単一のドメイン内、および（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により）*Expressway-ECisco VCS Expressway* を *Microsoft* のフロントエンド サーバに**直接接続**する構成では、個別の *Microsoft* 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。たとえば、同じドメイン内で、*1* つの（サブ）ネットワークに *Cisco Unified Call Manager*、*2* つ目の（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することができない場合（Meeting Server <> Expressway-C <> Microsoft を構成できない場合）の回避策としては、各サブネットに Expressway-C を展開し、サブネット間を通過させるために Expressway-E を配置します。つまり、以下のようになります。

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

チェーン化される Expressway-Es によるライセンスの動作

ファイアウォールを通過させるために Expressway-E をチェーン接続する場合（X8.10 以降）は、このライセンスの動作に注意してください。

- ファイアウォールを介して Cisco Webex Cloud に接続する場合は、トラバーサル クライアント ロールでトラバーサル ゾーンを設定する「追加の」各 Expressway-E について、（コールごとに）リッチ メディア セッション ライセンスが消費されます。以前と同様に、元の Expressway-C と Expressway-E のペアはライセンスを消費しません。
- ファイアウォールを介してサードパーティの組織（ビジネスツービジネス コール）に接続する場合は、チェーン内の「すべての」Expressway-E（トラバーサル ペアのオリジナルを含む）によって（コールごとに）リッチメディアセッション ライセンスが消費されます。以前と同様に、元の Expressway-C はライセンスを消費しません。

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 の設定を構成しないでください。

オプションキーは 65 キー以下のみに対して有効

65 を超えるオプションキー（ライセンス）を追加しようとした場合、それらのキーは Expressway の Web インターフェイス（[メンテナンス（Maintenance）] > [オプションキー（Option keys）]）では正常に見えます。適用されるオプション キーは最初の 65 個のみです。66 個目以降のオプション キーは追加されているように見えても、実際には Expressway によって処理されません。Bug ID CSCvf78728 を参照してください。

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 の Web インターフェイスを使用します（[構成（Configuration）] > [トラバーサル（Traversal）] > [TURN]）。

Expressway の X14.0 へのアップグレード

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。SCP や PSCP などの安全なコピープログラムを使用してインストールを実行する場合は、『*Cisco Expressway* 管理者ガイド』を参照してください。

概要

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	どこから?
1	以下の「前提条件とソフトウェアの依存関係」および「はじめる前に」の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（Upgrade）]「」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をインストールします（[アップグレードの続行（Continue with upgrade）]「」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（Upgrade）] 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、展開に適用されるタスクを完了してください。

X8.11.4 より前の Expressway システムでは、2 段階の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 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で Expressway をこのリリースにアップグレードする場合（たとえば X8.11.4 から X12.7）、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）。

すべての展開

X12.6 または X12.6.1 からアップグレードする予定で、アラーム ベースの電子メール通知機能を使用する場合

（注） X12.6.2 では、電子メール ID の長さは最大 254 文字に制限されます。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。新しいバージョンを実行しているシステムに、以前のバージョンの Expressway をインストールしないでください。システム構成が失われます。

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

X8.8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、展開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で証明書の検証が強化されたため、検証の失敗を回避するために、以下の項目を確認する必要があります。
  - アップグレードの前後にセキュアなトラバーサル テストを試行して（**[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）]**）、TLS 接続を検証します。
  - Unified Communications ノードが展開されている場合、それらのノードで、Expressway-C の信頼リストにある CA が発行した有効な証明書を使用しているか。
  - 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、展開内のすべてのノードの自己署名証明書が含まれているか。
  - Expressway の信頼 CA リスト内のすべてのエントリが一意であるか。重複をなくします。
  - 他のインフラストラクチャとの接続で**TLS検証モード**が有効になっている場合（Unified Communications トラバーサル ゾーンではデフォルトで常時オン、Unified Communications ノードへのゾーンの場合は任意）、ホストの証明書の CN または SAN フィールドにホスト名が存在することを確認する必要があります。失敗した展開を解決するための簡単な方法であっても、TLS 検証モードを無効にすることは推奨されません。

- **DNS エントリ**：Expressway がやりとりするすべてのインフラストラクチャ システムについて、転送および逆引き DNS ルックアップを実行しているか。X8.8 から、すべての Expressway-E システムに対して正引きおよび逆引きの DNS エントリを作成して、それらのシステムと TLS 接続するシステムが FQDN を解決し、証明書を検証できるようにする必要があります。Expressway がシステムのホスト名と IP アドレスを解決できない場合、MRA などの複雑な展開は、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。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 が新しいソフトウェアバージョンをインストールし、以前の構成を復元するのは、このリブートのときだけです。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リブートの間に行った設定変更は、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 リブートは必要ありません。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 を使用する展開

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

- 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、Cisco Unity Connection には、CiscoSSL アップデートのパッチが適用されています。Expressway をアップグレードする前に、『Expressway 経由の Mobile and Remote Access 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 と Cisco Expressway-E の**両方**を同じアップグレード「ウィンドウ」/期間内にアップグレードする必要があります（これは非 MRA 展開の一般的な推奨事項でもあります）。Expressway-C と Expressway-E を異なるバージョンで長期にわたって運用することは推奨しません。
- この項目は、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構成の Unified CM とエンドポイントで、MRA に使用される Expressway をアップグレードする場合に適用されます。この場合、Expressway をアップグレードする前に、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を参照してください。
  - TC7.3.11
  - CE8.3.3
  - CE9.1.2

X8.10.x から、MRA 認証（アクセス制御）設定は、以前のリリースのように Expressway-E で設定するのではなく Expressway-C で設定します。また、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構成し直す必要があります。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 以前のバージョンと Cisco Unified Communications Manager IM and Presence Service 11.5(1) を使用する展開

Expressway X8.7.x（およびそれ以前のバージョン）は、Cisco Unified Communications Manager IM and Presence Service 11.5(1) 以降との相互運用性がありません。これは、IM and Presence Service の当該バージョンでの計画的な変更によるものであり、Expressway X8.8 以降でそれに対応する変更が行われています。継続的な相互運用性を確保するためには、IM and Presence Service システムをアップグレードする前に、Expressway システムをアップグレードする必要があります。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 クエリ HTTP エラー "'HTTPError:500'"*（*Failed Unable to Communicate with <IM&P node address>. AXL query HTTP error "'HTTPError:500'"*）

Cisco Webex ハイブリッド サービスを使用する展開

Expressway をアップグレードする前に、管理コネクタを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のホスティングがサポートされている Expressway のバージョンの詳細については、『Webex ハイブリッド サービス コネクタに対応可能な Expressway バージョン』を参照してください。

アップグレード手順

はじめる前に

- システムのアクティビティレベルが低い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。すべてのピアでソフトウェア バージョンが一致するまで、クラスタは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。
- MRA に対して Expressway を使用していて、X8.9.x より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 認証の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）設定を、Expressway-E から Expressway-C に移動しました。アップグレードでは、既存の Cisco Expressway-E 設定は保持されないため、アップグレード後は、それらを確認し、必要に応じて展開に合わせて調整する必要があります。既存の MRA 認証設定にアクセスするには、次のようにします。

  a. Expressway-E で、[構成（Configuration）] > [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。

  （注） 既存の値（[オン（On）]、[排他（Exclusive）]、[オフ（Off）]）

  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。

（注） 以下の関連フィールドの現在の値。

- 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」に記載されているすべての関連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 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）システムと Expressway-E（トラバーサル サーバ）システムでは、**両方で同じソフトウェア バージョンを実行する**ことを常に推奨します。Mobile & Remote Access 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

（注） クラスタ構成の 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。

手順

ステップ 1 Expressway の Web ユーザ インターフェイスに管理者としてログインします。

ステップ 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）]）。

ステップ 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。

ステップ 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 コールはすぐにクリアされない場合があります）。

（注） 会議ファクトリの登録（有効化されている場合）はそのままにしておいて構いません。これがコールのソースになることはなく、また他のピアには固有の会議ファクトリ登録があるため、削除しても他のピアにロールオーバーされることはありません。

ステップ 5 [メンテナンス（Maintenance）] > [アップグレード（Upgrade）] を選択して、[アップグレード（Upgrade）] ページにアクセスします。

ステップ 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。

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 Expressway が自動的に検出します。

ステップ 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。

ステップ 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。

1. 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**番号が予定どおりのものであること。
   - **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こと。
2. [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）。
3. [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。

   リブートが完了すると、[ログイン（Login）] ページが表示されます。

ステップ 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、アップグレードが完了し、Expressway の設定が期待どおりになります。[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 を使用しており、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 展開のアップグレード後のタスク」で説明されているように、MRA アクセス制御の設定を構成し直します。

有効にするためにオプション キーが必要な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）] ページからその処理を実行します。

Expressway で FIPS モードが有効な場合（つまり、FIPS140 暗号化システムである場合）、X12.6 から、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。これを実行するには、Expressway コマンド ライン インターフェイスで次のコマンドを入力します（キー サイズが 2048 を超える場合は最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は、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 つずつ順番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。

手順

ステップ 1 Expressway の Web ユーザ インターフェイスに管理者としてログインします。

ステップ 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） クラスタの複数のピアで実行しているExpresswayのバージョンが異なる場合は、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。プライマリExpresswayと異なるバージョンで実行されている下位のピアに対しては、構成変更は複製されません。

ステップ3 メンテナンス モードを有効にして、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。

ステップ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 コールはすぐにクリアされない場合があります）。

（注） 会議ファクトリの登録（有効化されている場合）はそのままにしておいて構いません。これがコールのソースになることはなく、また他のピアには固有の会議ファクトリ登録があるため、削除しても他のピアにロールオーバーされることはありません。

ステップ5 [メンテナンス（Maintenance）] > [アップグレード（Upgrade）] を選択して、[アップグレード（Upgrade）] ページにアクセスします。

ステップ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。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 Expressway が自動的に検出します。

ステップ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。

ステップ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。

1. 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**番号が予定どおりのものであること。
   - **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こと。
2. [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）。

3. [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。

   リブートが完了すると、[ログイン（Login）] ページが表示されます。

ステップ 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。

ステップ 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. Expressway（プライマリを含む）の新しいステータスを確認します。
   1. [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）] であることを確認します。
   2. [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 を再度バックアップします（[メンテナンス（Maintenance）] > [バックアップおよびリストア（Backup and restore）]）。
3. MRA を使用しており、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 展開のアップグレード後のタスク」で説明されているように、MRA アクセス制御を再構成します。
4. 有効にするためにオプション キーが必要な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）] ページからその処理を実行します。
5. Expressway で FIPS モードが有効な場合（つまり、FIPS140 暗号化システムである場合）、X12.6 から、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。これを実行するには、Expressway コマンド ライン インターフェイスで次のコマンドを入力します（キー サイズが 2048 を超える場合は最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。

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、展開の検証を支援するため、また、Expressway のログ ファイル解析することでトラブルシューティングを支援するために、Cisco Technical Assistance Center （TAC）が作成したものです。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。

はじめに

手順

ステップ 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。

ステップ 2 https://cway.cisco.com/tools/CollaborationSolutionsAnalyzer/ にサインインします。

X12.6 から、[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）]）を使用して、コラボレーション ソリューション アナライザのトラブルシューティング ツールへのリンクを開くことができます。

ステップ 3 使用するツールをクリックします。たとえば、ログを使用するには、次のようにします。

1. [ログ分析（Log analysis）] をクリックします。
2. ログファイルをアップロードします。
3. 分析するファイルを選択します。
4. [分析の実行（Run Analysis）] をクリックします。

   ツールはログファイルを分析し、生のログよりも理解しやすい形式で情報を表示します。たとえば、ラダー図を生成して SIP コールを表示することができます。

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、バグ検索ツールに移動します。https://tools.cisco.com/bugsearch/
2. cisco.com のユーザ名とパスワードでログインします。
3. **検索**フィールドにバグ ID を入力して、**検索**をクリックします。

ID がわからない場合に情報を検索するには、次の手順を実行します。

1. [検索（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。

バグ検索ツールのホーム 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、更新情報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、更新情報の RSS フィード [英語] をご購読ください。RSS フィードは無料のサービスです。

付録 1：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。

初期設定へのリセット。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 設定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（HSM configuration）] ページ（**[メンテナンス（Maintenance）]** > **[セキュリティ（Security）]** > **[HSM構成（HSM configuration）]**）で、Expressway に必要な情報を構成します。

設定はクラスタ全体に複製されます。

[HSM 設定（HSM configuration）]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：前提条件の設定

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、オプション 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、Security World とリモート ファイル システム（RFS）を設定します。 **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.	署名認証局にアクセスします。	-
e.	HSM 互換の証明書を作成します。	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。

手順

ステップ 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。

ステップ 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。

ステップ 3 nShield の設定

1. 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。
2. [構成を保存（Save Configuration）] をクリックします。

   ページの上部に次のメッセージが表示されます。

   HSM □□□□□□□□□□□

3. [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。
4. [モジュールの追加（Add Module）] をクリックします。

   ページの上部に次のメッセージが表示されます。

   HSM □□□□□□□□□□□□□□□□□□

5. [HSMモード（HSM Mode）] タブの下のテーブルにデバイスが表示されます。
6. 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。

ステップ 4 [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。

ページの上部に次のメッセージが表示されます。

HSM □□□□□□□□□□□□□□□□

（注） HSM モードのオン/オフを切り替えると、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 の使用が有効になります。

次のタスク

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 チェックのモニタリング」を参照してください。

タスク 3：HSM ステータス チェックのモニタリング

HSM モードを有効にすると、[HSM構成（HSM configuration）]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

1. **TRUE**：Expressway で HSM モードを有効にした後に、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。
2. **FALSE**：プロセスが Expressway で実行されておらず、HSM の障害のアラームが発行された場合。

使用中の HSM 証明書

1. 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。
2. 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

1. 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。
2. 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

1. 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。
2. ハードウェアまたは HSM ボックスの設定に問題があり、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

（注） HSM モードが有効である場合、最後のデバイスは削除できません。まず、HSM モードを無効にする必要があります。

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。

手順

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

ステップ 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。

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。

手順

ステップ 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。

ステップ 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。

ステップ 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。）

ステップ 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 展開のアップグレード後のタスク

このセクションは、Expressway 経由の Mobile and Remote Access を使用していて、X8.9.x またはそれ以前から X8.10 以降にアップグレードする場合にのみ適用されます。システムを再起動した後、MRA アクセス制御の設定を再設定する必要があります。

MRA アクセス制御設定を再設定するには

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 [排他（Exclusive）] オプションの設定は、[認証パス（Authentication path）] で [SAML SSO 認証（SAML SSO authentication）] を指定することで設定します。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。

始める前に

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。

手順

ステップ 1 Expressway-C で、[構成（Configuration）] > [Unified Communications] > [構成（Configuration）] > [MRAアクセス制御（MRA Access Control）] に移動します。

ステップ 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方法を保持するには、このページで、Expressway-E の以前の設定に合わせて適切な値を設定します。従来の Expressway-E の設定と同等の Expressway-C の新しい設定を調べるには、次の 2 番目の表を参照してください。

ステップ 3 自己記述トークン（[OAuth トークンによる承認（更新あり）（Authorize by OAuth token with refresh）]）を構成する場合は、Unified CM ノードを更新します。[構成（Configuration）] > **[Unified Communications]** > ***[UCサーバタイプ（UC server type）]*** に移動し、[サーバの更新（Refresh servers）] をクリックします。

MRA アクセス制御の設定

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（[Unified Communications 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）] に設定されているかどうか）、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 Basic 認証（UCM/LDAP basic authentication）：クライアントは、Unified CM によって LDAP 資格情報に対してローカルに認証されます。 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。単に MRA をオフにするのではなく [なし（None）]「」オプションが用意されているのは、展開によっては、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です。（Meeting Server の Web プロキシ、XMPP フェデレーションなど）。[なし（None）]「」は、そのような場合にのみ使用してください。 （注） 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]

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 ログイン情報による承認（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 ログイン情報によって認証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）

フィールド	説明	デフォルト
内部認証の可用性の確認（**Check for internal authentication availability**）		[いいえ（No）]

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）] 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 クライアント認証リクエストにどのように反応するかを制御します。 リクエストは、クライアントが OAuth トークンによってユーザを認証しようとする可能性があるかどうかを尋ね、そのリクエストには Expressway-C がユーザのホーム クラスタを見つけるためのユーザ ID が含まれています。 はい（Yes）：*get_edge_sso* リクエストで、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* リクエストによって送信されたアイデンティティから判別されます。 いいえ（No）：Expressway が内部を参照しないように構成されている場合に、Edge の認証設定に応じて、すべてのクライアントに同じ応答が送信されます。 選択するオプションは、実装およびセキュリティ ポリシーによって異なります。すべての Unified CM ノードで OAuth トークンがサポートされている場合は、[いいえ（No）] を選択して応答時間とネットワーク全体のトラフィックを減らすことができます。または、ロールアウト中にクライアントがエッジ構成を取得するモードを使用するようにする場合や、すべてのノードでOAuthを保証できない場合は、[はい（Yes）] を選択します。 **注意** これを[はい（Yes）]に設定すると、認証されていないリモートクライアントからの不正なインバウンドリク	

フィールド	説明	デフォルト
	エスト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 は不正なリクエストを防止します。	

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）		-

フィールド	説明	デフォルト
	[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）	

フィールド	説明	デフォルト
	• 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」を参照してください。	-
Jabber iOS クライアントによる組み込みの Safari の使用の許可（Allow Jabber iOS clients to use embedded Safari）	デフォルトでは、IdP または Unified CM の認証ページは、iOS デバイスの組み込み Web ブラウザ（Safari ブラウザではない）に表示されます。このデフォルトのブラウザは iOS の信頼ストアにアクセスできないので、デバイスに導入された証明書を使用することはできません。 この設定では、オプションで、iOS デバイス上の Jabber がネイティブの Safari ブラウザを使用することができます。Safari ブラウザでは、デバイスの信頼ストアにアクセスできるため、OAuth 導入時にパスワードレス認証または二要素認証を有効化できるようになりました。 このオプションには潜在的なセキュリティの問題が存在します。認証が完了した後で、Safari から Jabber にブラウザ制御を返す機能は、カスタムプロトコルハンドラを呼び出すカスタム URL 方式を使用します。Jabber 以外の別のアプリケーションがこの方式を妨害し、iOS から制御を取得できます。この場合、アプリケーションはURLのOAuthトークンへアクセスできます。 すべてのモバイル デバイスが管理されているなどの理由で、iOS デバイスに Jabber のカスタムURL形式を登録する他のアプリケーションがないと確信する場合、オプションを有効にしても安全です。別のアプリケーションがカスタム Jabber URL を妨害する可能性が心配な場合、組み込み Safari ブラウザを有効にしないでください。	[いいえ（No）]

フィールド	説明	デフォルト
SIP トークンの余分なパケット存続時間（SIP token extra time to live）	[OAuth トークンによる承認（Authorize by OAuth token）] が [オン（On）] の場合に利用可能。 必要に応じて、簡単な OAuth トークンの存続可能時間（秒）を延長します。ログイン情報の有効期限が切れた後、コールを受け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

アップグレードによって適用される MRA アクセス制御値

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（Authentication path）** = *UCM/LDAP* • **ユーザ ログイン情報による承認（Authorize by user credentials）** = オン（*On*） [SSOモード（SSO mode）]：X8.9 の [排他（Exclusive）] は、X8.10 では 2 つの設定になっています。 • **認証パス（Authentication path）** = *SAML SSO* • **OAuth トークンによる承認（Authorize by OAuth token）** = オン（*On*） [SSOモード（SSO mode）]：X8.9 の [オン（On）] は、X8.10 では 2 つの設定になっています。 • **認証パス（Authentication path）** = *SAML SSO* および *UCM/LDAP* • **OAuth トークンによる承認（Authorize by OAuth token）** = オン（*On*） • **ユーザ ログイン情報による承認（Authorize by user credentials）** = オン（*On*）	両方	Expressway-C

オプション	アップグレード後の値	従来	現在
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）

オプション	アップグレード後の値	従来	現在
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）