Cisco Expressway X12.6

リリース ノート

初版発行日：2020 年 6 月

最終更新日：2020 年 7 月

プレビュー機能の免責事項

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

目次

はじめに

はじめに

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
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 6 月	初版。	X 12.6

対応プラットフォーム

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。
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######	サポートが制限（保守およびバグ修正目的のみでの限られたサポートを除き、X12.5.9 以降ではサポートされません。 新機能はサポートされていません。）
CE1000（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 以降ではサポートされません）
CE500（UCS C220 M3L にプレインストールされた Expressway）	52C######	サポート対象外 （X8.10.x 以降ではサポートされません）

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（アプライアンスのソフトウェア バージョンのサポートについては、この通知の他の箇所で説明されています）。

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、「販売終了の通知」[英語]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、「販売終了の通知」[英語]を参照してください。

関連資料

表 3 関連ドキュメントとビデオへのリンク

サポートビデオ	Cisco TAC エンジニアから 提供される特定の共 通の表現の設定手順 に関するビデオは、Expressway/VCS スクリーンキャスト ビデオリストページにあります。
仮想マシンのインストール	Expressway インストール ガイド ページの『Cisco Expressway 仮想マシン インストール 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 ページの『Cisco Expressway CE1200 アプライアンス インストール ガイド』
レジストラ / 単一システムの基本設定	Expressway インストール 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 基本設定 ガイドのページの『Cisco Expressway-E および Expressway-C 基本設定展開ガイド』
管理およびメンテナンス	Cisco Expressway シリーズ メンテナンスおよび 運用ガイドのページに用意されている『Cisco Expressway 管理者ガイド』 Expressway シリーズ運用ガイドのページに用意されている『Cisco Expressway 有用性ガイド』
クラスタ	Expressway 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導入ガイド』
証明書	Expressway コンフィギュレーション ガイド ページの『Cisco Expressway 証明書の作成と使用導入ガイド』
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 ポートの使用コンフィギュレーション ガイド』
ユニファイド コミュニケーション	Expressway コンフィギュレーション ガイド ページの『Cisco Expressway 経由の Mobile & Remote Access』
Cisco Meeting Server	Expressway コンフィギュレーション ガイド ページの『Cisco Expressway による Cisco Meeting Server 導入ガイド』 Cisco Meeting Server プログラミング ガイドのページの『Cisco Meeting Server API リファレンス ガイド』 その他の Cisco Meeting Server 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 および Microsoft インフラストラクチャ導入ガイド』 Expressway コンフィギュレーション ガイド ページの『Cisco Jabber およびビジネス版 Microsoft Skype インフラストラクチャ構成チートシート』

関連資料

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 コンフィギュレーション ガイド ページの『Cisco TelePresence Multiway 導入ガイド』

X12.6 の新機能

表 4 リリース番号別の機能履歴

機能/変更	X 12.6
セキュリティ機能の拡張	サポートあり
スマート ライセンス	サポートあり
オプション キーではなく UI 設定による、タイプおよびシリーズの設定	サポートあり
アラームベースの電子メール通知	サポートあり
高度なメディア ゲートウェイが UI から削除	未サポートの機能の削除
ハードウェア セキュリティ モジュール（HSM）のサポート	プレビュー
IM & 用の Android プッシュ通知パブリッシャー	プレビュー
Cisco Contact Center のヘッドセット機能	プレビュー
MRA での複数のプレゼンス ドメイン （X8.11 での新機能ではありません。以前はプレビュー ステータスであったため参照用に含めました）	プレビュー
Smart Call Home （X12.6 での新機能ではありません。以前はプレビュー ステータスであったため参照用に含めました）	X12.5 で非推奨にされました。 プレビュー

Cisco VCS は新機能の適用対象外。

ソフトウェアバージョン X 12.5 以降の新機能は、Cisco VCS ではサポートされていません。また、Cisco Expressway シリーズのみに適用されます。Cisco VCS システムでは、このバージョンは、保守およびバグ修正目的でのみ提供されています。これには、セキュリティ機能の強化、アラームベースの電子メール通知、および以下で説明するオプション キーの変更のサポートが含まれています。

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。この大部分はバックグラウンドで動作しますが、次のように、ユーザ インターフェイスに影響を与える変更もあります。

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

このリリースのリリース キー、オプション キー、および一般的なライセンス

このセクションでは、ライセンスに関する主なポイントについてまとめています。一部は X 12.6 の新機能であり、一部は以前のリリースで最近行われた変更点です。ここでは便宜上再度紹介します。X12.6 の変更の詳細については、後で説明します。

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

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

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

この変更は、（Cisco VCS ではなく）Cisco Expressway シリーズを何らかの方法でサポートする CE1200 シリーズ以降のハードウェアの、アプライアンスベースのシステムとは無関係です。

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

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

X12.6 の新機能

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

X12.6 から、トラバーサル サーバのオプション キーは使用されなくなります。また、システムを Cisco Expressway-E に変更する必要はありません。代わりに、サービスの選択ページの [**タイプの選択（Select Type）**] 設定を使用します（インストール時にサービスの設定ウィザードから、または後からいつでも [**ステータス> 概要（Status > Overview）**] からアクセス可能）。オプション キーのメニューにキー を適用しようとすると、 サービスの選択ページにリダイレクトされます。

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

タイプ設定を CLI から変更することはできません。

スマートライセンス

Cisco Expressway では、X12.6 から次の 2 つのライセンス モードのいずれかがサポートされています。

- PAK ベースのライセンス。従来の方法では、Expressway にインストールされたライセンス オプション キーを使用します（製品のアクティベーションキーとも呼ぶ）。
- スマート ライセンス。この新しい方法は通常、クラウドベースの Cisco Smart Software Manager（CSSM）によって管理されていますが、オンプレミスのアプローチが必要なデプロイでは、Smart Software Manager のオンプレミスの製品を使用することもできます。

常に 1 つのライセンス モードのみサポートされます。

Expressway は、デフォルトで、PAK ベース（従来）のライセンスに設定されています。Web インターフェイスからスマート ライセンスに切り替えられます[メンテナンス（Maintenance）] > [スマート ライセンス（Smart licensing）]） 。ただし、PAK へ切り替えて戻すには工場出荷時リセットが必要です。

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

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

詳細情報

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 ライセンスの設定方法の詳細については、『Expressway 管理者ガイド』[英語]を参照してください 。

アラームベースの電子メール通知

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

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

X12.6 の新機能

新しいアラーム ID 90001 は、Expressway を通した 9-1-1 ダイヤルの基準を満たす、 米国での緊急通話に使用されます。このアラームの重大度は緊急に分類されてい ます。

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

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

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

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

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

Expressway では、現時点では、nShield Connect が HSM プロバイダーとして (プレビューで) サポートされています。設定手順と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 デバイスの設定」(34 ページ) で詳しく説明します。

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

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

この機能は、モバイルおよび 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 (コンタクト センター向けのシスコ ヘッドセットと Finesse の統合)』(https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/cucm/whitePaper/CUCM_Headsets_for_ContactCenter_WP.pdf) [英語]をご覧ください。

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

この機能は、モバイルおよび Remote Access (MRA) を使用して Expressway を導入する場合に該当します。X12.6 では、外部の製品バージョンの依存関係によって、プレビュー のステータスのみで提供されます。

新しいデモの UC ソフトウェアは Android デバイスに対するプッシュ通知をサポートしています。X12.6 からは、関連するデバイス、Unified CM、および IM and Presence Service が、必要なソフトウェア バージョンを実行している場合は、これらの新しいプッシュ機能が自動的にサポートされます。Expressway での設定は一切不要です。この機能には、次のソフトウェアのバージョン以降が必要です。

- Unified CM バージョン 12.5 (1) SU3 またはバージョン 14 - 11.5 (1) SU8 では未サポート
- IM and Presence Service 12.5 (1) SU3 またはバージョン 14 - 11.5 (1) SU8 では未サポート

X12.6 の新機能

- Expressway X12.6
- Cisco Jabber 12.9

（プレビュー）互換性のある電話機の KEM サポート：MRA 展開

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

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

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

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

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

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

CE1100 ハードウェア製品での本リリースの部分的サポート

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

仮想化システム - プロファイル情報がバックアップから削除

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

仮想化システム - ESXi 6.0 の一般的なサポートの終了

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

X12.6 の新機能

撤回または廃止された機能とソフトウェア

Cisco TelePresence Management Suite プロビジョニング拡張機能（Cisco TMSPE） によるデバイスのプロビジョニングは、Expressway の次回のリリースで廃止される予定です。

次の機能は、Expressway バージョン X12.5 以降で廃止されており、その後のリリースでは Expressway でのこれらの機能のサポートが取り消されます。

- Cisco Jabber Video for TelePresence（Movi）。この項目は、Cisco Jabber Video for TelePresence に関連しており、Unified CM と連携して動作する Cisco Jabberソフト クライアントには対応していません（ビデオ通信の Cisco Expressway と連携して動作します）。
- Findme デバイス / ロケーションのプロビジョニング サービス（Cisco TelePresence FindMe/TMSPE）
- Smart Call Home
- Expressway Starter Pack
- Expressway 転送プロキシ

X 12.6 から、Cisco Webex ハイブリッド サービスのコネクタとして Cisco VCS を使用すること はできません。この機能がサポートされるのは、Cisco Expressway シリーズのみです。

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

- Cisco Advanced Media Gateway
- VM ベースの展開の場合、VMware ESXi 仮想ハードウェアバージョン Esxi5.x

ユーザインターフェイスから削除されたサポートされていない機能（継続中）

使いやすさと一貫性を向上させるために、Expressway のユーザ インターフェイスから、 廃止される機能を削除しています。このリリースでは、アドバンス メディア ゲートウェイ（AM gateway および AM GW とも呼ばれます） が削除されました。関連付けられている 2 つの Web UI ページである**外部トランスコーダ**および**トランスコーダ ポリシー ルール**は、**Microsoft の相互運用性**メニューから削除されました 。

今回のリリースでのその他の変更点

コラボレーション ソリューション アナライザー ツールへのリンク

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

アラームとバナーの変更

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

X12.6 の新機能

お客様向けマニュアルの変更

Web ユーザ インターフェイスからの Expressway のアップグレードに関する一部の手順は、以前は『Expressway アドミニストレータ管理者 ガイド』、『Cluster Creation and Maintenance Deployment Guide（クラスタの作成とメンテナンス導入ガイド）』[英語]、リリース ノートに記載され ていました。すべての手順をこのノートの 1 つの場所にまとめました。

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

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

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

REST API への変更点

リモート設定を容易にするために、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。

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については、Expressway インストール ガイド ページの『*Cisco Expressway REST API Summary Guide*（*Cisco Expressway REST API サマリー ガイド*）』に記載されています。

構成 API	API が導入されたバージョン
スマート ライセンス	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

以前のリリースを含むすべてのプレビュー機能

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

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

（プレビュー - 現在廃止）Smart Call Home

この機能は、Expressway X12.5 で非推奨となり、**以降のリリースではサポートが終了します。**

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

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

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

（プレビュー）MRA を介した複数のプレゼンス ドメイン/複数の IM アドレス ドメイン

この機能は現在プレビュー ステータスでのみ提供されています。

Jabber 10.6 以降は、ユーザが複数のドメインに編成されているインフラストラクチャ、またはサブドメインを持つドメイン（IM and Presence Service 10.0.x 以降が対象）に展開できます。

未解決および解決済みの問題

バグ検索ツール

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

- 変更された日付順に並べられたすべての未解決の問題（最新のものが最初）
- X12.6 で解決済みの問題

このバージョンで特に重要な問題

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

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

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

デュアル NIC Jabber Guest の導入を推奨します。

制限事項

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

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

このリリースのプレビュー ステータスでのみ提供される Expressway の機能については、 下記の注意事項の最初にある「機能履歴表」に記載されています。

サポートされていない機能

- 現時点では、クラスタ展開内の 1 つの Expressway が失敗した場合、 何らかの理由でネッ トワーク接続が失われた場合、 または Unified CM を再起動した場合は、 該当ノードを通過したす べてのアクティ ブなコールは失敗します。コールは別のクラスタ ピアに渡されません。これは X12.5x の新しい 動作ではあ りませんが、見過ごされていたために、以前のリリースでは文書化されていませんでした。Bug ID CSCtr39974 を参照してください。
- DTLS は Expressway によって終了されません。メディアを保護するための DTLS はサポートされていません。 SRTP は、コールを保護するために使用されます。DTLS コールを発信しようとする試みは失敗します。DTLS プロトコルは SDP に挿入されますが、暗号化された iX プロトコルを通過する場合に限ります。
- X12.5 から、Expresswayは、RFC 4028で指定されているように、セッションの更新のみを目的として、MRA 接続を介した SIP UPDATE のサポート を限定的に提供します。 ただし、 この機能を使用す るための特別な要件がない場合は、この設定をオンにしないでください。SIP UPDATE のその他の使用はサポートされておらず、このメソッドに依存する機能は期待どおりに機能しません。
- 音声コールは、状況によってはビデオコールとしてライセンスされる場合があります。厳密な音声のみのコールは、ビデオ通話よりも少ないライセンスを消費します。ただし、音声通話には、ActiveControl を有効にする iX チャネルなどの非オーディオチャネルが含まれている場合、ライセンスのためにビデオ通話として扱われます。

Cisco Webex Hybrid コールサービス

Expressway X12.6 は Cisco Webex Hybrid コールサービスと互換性がありません。 以前にサポートされていた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）。

制限事項

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。

モバイルおよびRemote Accessに関する制限事項

重要：モバイルおよびリモートアクセス（MRA）向けに Expressway を使用する場合、現状では、サポートされないさまざまな機能と制限が存在します。MRA と連動しないことがわかっている主要なサポートされていない機能のリストは、『Cisco Expressway 経由の Mobile & Remote Access 導入ガイド』に記載されている、「Mobile & Remote Access を使用する場合にサポートされる機能とサポートされない機能」で詳しく説明します。

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 & Remote Access』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。

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（Cluster communication failure: Unable to establish...）」）*を発生させる可能性があります。*アラームは、クラスタ内の既存のピアに表示されます。通常、不要なアラームは、新しいピアが正常に追加された時点から 5 分以上経過した後に引き下げられます。

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

仮想システム

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

物理的な Expressway アプライアンスの場合、高度なネットワーキング機能を使用すると、設定したイーサネット ポートごとに速度とデュプレックス モードを設定できます。ただし、仮想マシンベースの Expressway システムに対して、イーサネット ポートごとに速度を設定することはできません。

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

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。

制限事項

- 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）。システムは以前のバージョンのソフトウェアのダウングレードを防ぐことはできませんが、Cisco では以前のバージョンのアプライアンスをサポートしていません。
- Expressway を使用すると、CLI を使用して Traversal Server または 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 を使用する中規模システムを X8.10 以降にアップグレードすると、Expressway は自動的にアプライアンスを大規模システムに変換します。これは、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設定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、これらのポート 36000 ~ 36011 はファイアウォールで開かれないため、Expressway-E はコールをドロップします。

回避策

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

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

Xmpp フェデレーション- IM&P ノード障害の動作

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

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

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

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

制限事項

デュアルホーム会議-SIP メッセージサイズ

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

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

Microsoft の相互運用性のために Meeting Server を使用する場合、現時点では次のドメイン内または企業内のシナリオに制限が適用されます。

「シングル ドメイン」の場合、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で）Expressway-E が Microsoft フロント エンド サーバに「直接接続」している構成では、Microsoft ベースの SIP ネットワークと標準ベースの SIPネットワークを別々に展開しま。たとえば、同じドメイン内の 1 つの（サブ）ネットワークに Cisco Unified Call Manager を、別の（サブ）ネットワークに Microsoft を展開します。

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

回避策

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

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

チェーン化される Expressway-Es によるライセンスの動作

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

- ファイアウォールを介して Cisco Webex Cloud に接続する場合は、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

制限事項

HSM のサポート

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

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

オプションキーは 65 キー以下のみに対して有効

65を超えるオプションキー（ライセンス）を追加しようとすると、それらはExpressway Webインタ ーフェイスに通常どおり表示されます（[メンテナンス（Maintenance）] > [オプションキー（Option keys）]）。適用されるオプション キーは最初の 65 個のみです。66 個目以降のオプション キーは追加されているように見えても実際には Expressway によって処理されません。Bug ID CSCvf78728 を参照してください。

Jabber を使用した OAuth トークン認証

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

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

Expressway 転送プロキシ

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

TURN サーバ

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

相互運用性

テスト結果

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

注目すべき相互運用性の考慮事項

X8.7.x（および以前のバージョン）の Expressway は、Cisco Unified Communications Manager IM and Presence Service 11.5（1）以降と相互運用できません。これは、このバージョンの IM and Presence サービスにおける意図的な変更に起因するもので、Expressway X8.8 以降では対応する変更が加えられています。

継続的な相互運用性を確保するため、必ず IM and Presence サービス システムをアップグレードする「前に」Expressway システムをアップグレードしてください。この問題の症状としては、次のような Expressway のエラーが挙げられます。

`Failed Unable to Communicate with` *`<IMRP node address >`*`.` **`AXL query HTTP error "'HTTPError:500'"`**

同時に実行できる Expressway サービス

Cisco Expressway シリーズ保守および操作ガイド ページの『Cisco Expressway 管理者ガイド』では、Expressway サービスを同じ Expressway システムまたはクラスタ上で共存させることができることについて詳しく説明しています。「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 X12.6 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。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 5 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	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」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のインストール（[アップグレードを続行する（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

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

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（たとえば X8.11.4 から X12.6.1）、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。なお、**リリースキーは Cisco VCS システムでも必要**です。

X8.11.4 より前の Expressway システムでは 2 段階アップグレードが必要

バージョン X8.11.4 よりも前のソフトウェアを実行しているシステムをアップグレードする場合は、 **まず中間リリースにアップグレードしてから、X12.6 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。

Expressway の X12.6 へのアップグレード

すべての導入の手順:

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

X8.11.1 以降、アップグレード後にシステムが再起動すると、 新しい暗号化メカニズムが使用されます。これは、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）]）。
  - ユニファイド コミュニケーション 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 の信頼できる CA リストには、 展開内のすべてのノードの自己署名証明書が含まれていますか。
  - Expressway の信頼できる CA リスト内のすべてのエントリは一意ですか。重複をなくします。
  - 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 はリブート時に新しいソフトウェア バージョンをインストールし、以前の設定を復元します。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。

Expressway の X12.6 へのアップグレード

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 バージョンを使用してシステムを再起動した時点で失われます。

注: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 を使用する導入

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

- ユニファイド コミュニケーション インフラストラクチャ ソフトウェアの最小バージョンが適用されます。一部のバージョンの Unified CM、IM and Presence サービス、および Cisco Unity Connection には、CiscoSSL アップデートのパッチが適用されています。Expressway のアップグレード前に、『*Cisco Expressway 経由の Mobile & Remote Access 導入ガイド*』に記載されている最小バージョンを実行しているかどうかを確認してください 。

  IM and Presence サービス 11.5 は例外です。IM and Presence サービスを 11.5 にアップグレードする「前に」、Expressway を X8.8 以降にアップグレードする必要があります。
- Expressway-C 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、TC または Collaboration Endpoint（CE）ソフトウェアを実行しているクラスター化された Unified CM とエンドポイントで、MRA に使用される Expressway をアップグレードする場合に適用されます。この場合、Expressway をアップグレードする「前に」、以下に（または後続で）リストされている関連する TC または CE メンテナンス リリースをインストールする必要があります。これは、フェールオーバーに関する既知の問題を回避するために必要です。推奨される TC / CE メンテナンスリリースがない場合、エンドポイントが登録された元の Unified CM が何らかの理由で失敗した場合、エンドポイントは別の Unified CM へのフェールオーバーを試行しません。Bug ID CSCvh97495を参照してください。
  - TC7.3.11
  - CE8.3.3
  - CE9.1.2

注：X8.10x からは、MRA 認証（アクセス制御）設定は、旧リリースでは Expressway-E ではなく Expressway-C で設定します。既存の設定を保持することが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設定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）

X8.7.x（および以前のバージョン）の Expressway は、Cisco Unified Communications Manager IM and Presence Service 11.5（1）以降と相互運用できません。IM and Presence サービス ソフトウェアの前に、Expressway ソフトウェアをアップグレードする必要があります。詳細については、「相互運用性、23 ページ」を参照してください。

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 クラウドによっ てアドバタイズされた管理コネクタのアップグレードを承認して受け入れます。そうでない場合、アップグレード後にコネクタで問題が発生する場合があります。ハイブリッド コネクタ ホスティングでサポートされる Expressway のバージョンの詳細については、「Connector Host Support for Cisco Webex Hybrid Services（Cisco Webex ハイブリッド サービスのコネクタ ホスト サポート）」を参照してください。

アップグレード手順

はじめる前に

- システムのアクティビティレベルが低いときに 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。
- 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。

  1. Expressway-E で、[設定（Configuration）] > [Unified Communications] > [設定（Configuration）] に移動し、[シングルサインオンのサポート（Single Sign-on support）] を探します。既存の値（[オン（On）]、[排他（Exclusive）]、または [オフ（Off）]）をメモします。
  2. [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メモしておきます。
     - **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 24 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 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 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

クラスタ化された Expressway をアップグレードする場合は、 この手順を使用しないでください。
代わりに、このプロセスを使用してクラスタシステムを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ログインします。
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）。 これはコールのソースではなく、また他のピアが各自の Conference Factory 登録を所有しているため、 これを削除しても別のピアにロールオーバーされることはありません。
5. **[メンテナンス（Maintenance）] > [アップグレード（Upgrade）]** に移動して、**[アップグレード（Upgrade）]** ページにアクセスします。
6. **[参照（Browse）]** をクリックし、アップグレードするコンポーネントのソフトウェア イメージ ファイルを選択します。Expressway が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。
   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。
   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、Ex pressway 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。
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 を使用していて、X8.9.x 以前のバージョンからアップグレードする場合は、「付録 1：MRA 導入のアップグレード後のタスク」（38 ページ）の説明に従って、MRA アクセス制御設定を設定し直します。

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：設定データが失われるリスクを回避し、サービスの継続性を維持するために、「先にプライマリピアをアップグレード」してから、下位ピアを「一度に 1 つずつ順にアップグレード」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ログインします。
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設定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、設定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）。これはコールのソースではなく、また他のピアが各自の Conference Factory 登録を所有しているため、これを削除しても別のピアにロールオーバーされることはありません。
5. **[メンテナンス（Maintenance）] > [アップグレード（Upgrade）]** に移動して、**[アップグレード（Upgrade）]** ページにアクセスします。
6. **[参照（Browse）]** をクリックし、アップグレードするコンポーネントのソフトウェア イメージ ファイルを選択します。Expressway が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。
   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。
   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。

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. 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 再度を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 を使用していて、X8.9.x 以前のバージョンからアップグレードする場合は、「付録 1：MRA 導入のアップグレード後のタスク」（ 38ページ）の説明に従って、MRA アクセス制御設定を設定し直します。
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。

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の場合は、最初に、お使いの Expressway のログを収集します。
2. https://cway.cisco.com/tools/CollaborationSolutionsAnalyzer/にログインします

   X12.6 以降では、[**診断のロギング（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。
   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。
2. cisco.com のユーザ名とパスワードでログインします。
3. [検索（Search）]フィールドにバグ ID を入力し、[検索（Search）]をクリックします。

ID がわからない場合に情報を検索するには、次の手順を実行します。

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

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。

マニュアルの入手方法およびテクニカル サポート

付録 1：Expressway での HSM デバイスの設定

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 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 設定（HSM configuration）] ページ（**[メンテナンス（Maintenance）] > [セキュリティ（Security）] > [HSM 設定（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 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。

マニュアルの入手方法およびテクニカル サポート

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、クラスター内の各ピアに 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 設定（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. [設定の保存（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. [**モジュールの追加（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。

1. [**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36」 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 設定ページに [**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）」という警告が 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 ボックスの設定に問題があり、アラームが発生すると、**Failed となります。**

マニュアルの入手方法およびテクニカル サポート

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

オプションで Expressway HSM 設定からデバイス（モジュール）を削除するには:

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。

マニュアルの入手方法およびテクニカル サポート

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

1. Expressway-C で、[設定（Configuration）] > [Unified Communications] > [設定（onfiguration）] > [MRAアクセス制御（MRA Access Control）] に移動します。
2. 次のいずれかを実行します。
   - 新しい MRA アクセス制御方式を 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、このページで適切な値を設定して、Expressway-E の以前のバージョンの設定に一致させます。古い Expressway-E 設定を Expressway-Cの 新しい同等の設定にマッピングする方法については、下の 2 番目の表を参照してください。
3. 自己記述トークン（更新を伴う OAuth トークンによる承認）を設定する場合は、Unified CM ノードを更新します。[設定（Configuration）] > [Unified Communications] > [<UCサーバタイプ>] 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 [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。

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。

マニュアルの入手方法およびテクニカル サポート

表 6 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 SSOauthentication）]：クライアントは外部 IdP によって認証されます。 [UCM/LDAP 基本認証（UCM/LDAP basic authentication）]：クライアントは、LDAP クレデンシャルに対して Unified CM によってローカルに認証されます。 [SAML SSO および UCM/LDAP（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]
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）]

マニュアルの入手方法およびテクニカル サポート

フィールド	説明	デフォルト
内部認証の可用性の確認（Check for internal authentication availability）	[OAuth トークンによる承認（更新あり）（Authorize by OAuth token with refresh）]または [OAuth トークンによる承認（Authorize by OAuth token）]が有効になっている場合に利用可能。 最適なセキュリティとネットワーク トラフィックの削減のため、デフォルトは [いいえ（No）] です。 Expressway-C がホーム ノードをチェックす るかどうかを選択することにより、Expressway-E がリモート クライアント認証要求にどのように反応するかを制御します。 要求は、クライアントが OAuth トークンによってユーザを認証 しようとする可能性があるかどうかを尋ね、その要求には Expressway-C がユーザのホーム クラスタを見つけるためのユーザ ID が含まれています。 [はい（Yes）] *: get_ Edge _sso* 要求は、OAuth トークンがサポー トされているかどうかをユーザのホーム Unified CM に尋ねます。ホーム Unified CM は、Jabber クライアントの *get_edge_sso* 要求によって送信された ID から決定されます。 [いいえ（No）] : Expressway が内部的に見えないように設定されている場合、 Edge の認証設定に応じて、すべてのクライアントに同じ応答が送信されます。 選択するオプションは、実装およびセキュリティ ポリシーによって異なります。すべての Unified CM ノードで OAuth トークンがサポートされて いる場合は、[いいえ（No）]を選択して応答時間とネットワーク全体のトラフィックを減らすことができます。または、ロールアウト中にクライアントがエッジ構成を取得するモードを使用するようにする場合や、すべてのノードで OAuth を保証できない 場合は、[はい（Yes）]を選択します。 **注意：これを [はい（Yes）] に設定すると、認証されていないリモート クライアントからの不正な着信要求が許可される可能性があります。** この設定に [いいえ（No）] を指定すると、Expressway は不正な要求を回避します。	[いいえ（No）]

マニュアルの入手方法およびテクニカル サポート

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。	–

マニュアルの入手方法およびテクニカル サポート

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**しません。**	[いいえ（No）]
SIP トークンの余分なパケット存続時間（SIP token extra time to live）	[OAuth トークンによる承認（Authorize by OAuth token）]が[オン（On）]の場合に利用可能。 必要に応じて、簡単な OAuth トークンの存続可能時間（秒）を延長します。クレデンシャルの有効期限が切れた後、コールを受け入れるための短い時間枠をユーザに提供します。ただし、潜在的なセキュリティ リスクが増加します。	0 秒

マニュアルの入手方法およびテクニカル サポート

表 7 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 クレデンシャルによる承認（Authorize by user credentials）**=オン [SSOモード（SSO mode）] : X8.9 の [排他（Exclusive）] は、X8.10 では 2 つの設定になっています。 • **認証パス**=SAML SSO • **OAuth トークンによる承認**=オン [SSOモード（SSO mode）] : X8.9 の [オン（On）] は、X8.10 の 2 つの設定になります。 • **認証パス**=SAML SSO/および UCM/LDAP • **OAuth トークンによる承認**=オン • **ユーザクレデンシャルによる承認（Authorize by user credentials）**=オン	両方（Both）	Expressway-C
OAuth トークンによる承認（更新あり）（Authorize by OAuth token with refresh）	点灯	–	Expressway-C
[OAuth トークンによる承認（Authorize by OAuth token）]（以前は SSO モード）	アップグレード前の設定が適用されます	両方（Both）	Expressway-C
ユーザクレデンシャルによる承認（Authorize by user credentials）	アップグレード前の設定が適用されます	両方（Both）	Expressway-C
内部認証の可用性の確認（Check for internal authentication availability）	いいえ（No）	Expressway-E	Expressway-C

マニュアルの入手方法およびテクニカル サポート

オプション	アップグレード後の値	従来	現在
ID プロバイダー：IdP の作成または変更（Identity providers: Create or modify IdPs）	アップグレード前の設定が適用されます	Expressway-C	Expressway-C（変更なし）
ID プロバイダー：SAML データのエクスポート（Identity providers: Export SAML data）	アップグレード前の設定が適用されます	Expressway-C	Expressway-C（変更なし）
Jabber iOS クライアントによる組み込みの Safari の使用の許可（Allow Jabber iOS clients to use embedded Safari）	いいえ（No）	Expressway-E	Expressway-C
SIP トークンの余分なパケット存続時間（SIP token extra time to live）	アップグレード前の設定が適用されます	Expressway-C	Expressway-C（変更なし）

Cisco の法的情報

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

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

Cisco が採用している TCP ヘッダー圧縮機能は、UNIX オペレーティング システムの UCB（University of California, Berkeley）のパブリック ドメイン バージョンとして、UCB が開発したプログラムを採用したものです。All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよび上記代理店は、商品性、特定目的適合、および非侵害の保証、もしくは取り引き、使用、または商慣行から発生する保証を含み、これらに限定することなく、明示または暗黙のすべての保証を放棄します。

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

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

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

シスコは世界各国 200 箇所にオフィスを開設しています。各オフィスの住所、電話番号、FAX 番号は当社の Web サイト（www.cisco.com/jp/go/offices/）をご覧ください。

シスコの商標

Cisco および Cisco のロゴは、米国およびその他の国における Cisco およびその関連会社の商標を示します。シスコの商標の一覧については、www.cisco.com/go/trademarks をご覧ください。Third-party trademarks mentioned are the property of their respective owners. 「パートナー」という用語の使用は Cisco と他社との間のパートナーシップ関係を意味するものではありません。（1110R）。