Cisco Expressway 経由のモバイルおよびリモートアクセス導入ガイド（X14.2）

初版：2022 年 8 月 10 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

目 次

第 1 章

MRA の概要 1

モバイルおよびリモートアクセスについて 1

コア コンポーネント 2

プロトコル概要 3

VPN を使用しない Jabber クライアント接続 4

展開シナリオ 4

スタンドアロンネットワーク要素を使用した MRA 5

クラスタ化したネットワークを使用した MRA 6

複数のクラスタ化ネットワークを使用した MRA 6

サポートされていない展開 7

サポートされていない Expressway の組み合わせ 11

容量情報 11

第 2 章

MRA 要件および前提条件 13

モバイルおよびリモートアクセスポート 13

ネットワーク インフラストラクチャに関する要件 13

IP アドレス 13

ネットワークドメイン（Network Domain） 13

DNS 14

SRV レコード 15

パブリック ドメインネームシステム（DNS）（外部ドメイン） 16

ローカルドメインネームシステム（DNS）（内部ドメイン） 16

ファイアウォール設定 17

帯域幅の制限 18

ユニファイド コミュニケーションの要件 18
製品バージョン 18
Unified CM の要件 18
IM and Presence Service の要件 20
証明書の要件 21
エンドポイントの要件 26
MRA に互換性のあるクライアント 26
MRA に互換性のあるエンドポイント 27
EX、MX、SX シリーズエンドポイント（TC ソフトウェアを実行） 28
Android ベースの DX650、DX80、DX70 デバイスとサポートされている IP Phone 7800 および 8800 モデルに関する考慮事項 29
サポートされている MRA 機能 29
制限事項および機能サポート 30
UC 機能サポートおよび制限事項 30
サポートされていない Expressway 機能および制限事項 33
Cisco Jabber SKD の部分サポート 35
エンドポイント/クライアントとの MRA OAuth トークン認証 36
HSM のサポート 36

第 3 章 **MRA 構成** 37
MRA 構成の概要 37
MRA 設定タスクフロー 37
Expressway サーバーアドレスの設定 39
SIP の有効化 39
自動侵入保護の構成 40
モバイルおよびリモート アクセスを有効にします。 40
ドメインの追加 41
Unified CM クラスタの追加 42
自動生成されたゾーンと検索ルール 43
IM and Presence Service クラスタの追加 44
Cisco Unity Connection クラスタの追加 44

MRA アクセス制御の構成 45
Expressway（Expressway-C）アクセス制御の設定 46
エッジ経由の SAML SSO 認証 50
簡易 OAuth トークン認証について 51
更新を伴う自己記述 OAuth トークン承認について 52
OAuth トークンの前提条件 53
UC アプリケーションで OAuth を構成する 55
SIP OAuth モードの設定 56
SAML SSO の設定 57
Expressway-C から SAML メタデータをエクスポート 58
IdP から SAML メタデータをインポート 59
IdP とドメインの関連付け 60
SAML SSO に ADFS を構成 60
セキュアトラバーサルゾーンの構成 61
セキュア通信の構成 63
メディア暗号化 64

第 4 章 **ICE メディアパスの最適化 65**
ICE メディアパスの最適化 65
Expressway-C と Unified CM 間のシグナリングパスの暗号化 68
サポートされるコンポーネント 69
ICE メディアパスの最適化の前提条件 70
ICE メディアパス最適化のタスクフロー 71
ICE 設定の構成 72
サーバー証明書のインストール 73
CEtcp ネイバーゾーンを CEtls ネイバーゾーンに変更する 73
ICE パススルーサポート用 UC トラバーサルゾーンの設定 74
ICE パススルーサポート用 UC ネイバーゾーンの設定 74
CLI を使用して Cisco Expressway ゾーンで ICE パススルーを構成する 75
Cisco Expressway-E を TURN サーバーとして設定 75
ICE パススルーメトリックの使用 76

Expressway-C で ICE パススルーメトリックを表示 77
collectd デーモンを使用したメトリック収集 78
通話履歴で通話タイプを表示 78
帯域幅操作 79

第 5 章 機能と追加構成 81
展開パーティション 81
UC サービスの展開パーティションの割り当て 82
MRA 経由のプッシュ構成 83
MRA のプッシュ構成の構成 84
Android デバイスでプッシュ構成を有効化 85
ファストパス登録 86
ファストパス登録の構成 86
SIP パスヘッダーの有効化 86
Unified CM と Expressway-C 間の SIP トランク 87
トランク接続用の SIP ポートの構成 88
MRA 経由の BiB レコード 88
HTTP 許可リスト 90
HTTP 許可リストの編集 92
ルールを HTTP 許可リストにアップロード 93
MRA 経由の Dial via Office-Reverse 94
MRA 経由の Dial via Office-Reverse の構成 96
マルチクラスタのベストプラクティス 96
マルチドメインのベストプラクティス 99
マルチドメイン構成の概要 102
セッションの永続性 105

第 6 章 MRA デバイスの導入準備 107
アクティベーションコードによる MRA デバイスの導入準備 107
MRA 導入準備プロセスフロー 108
デバイスの導入準備の前提条件 109

MRA デバイス導入準備の構成フロー 111
電話機のアクティブ化 114
安全な導入準備のための追加オプション 115

第 7 章 MRA のメンテナンス 117
Expressway のメンテナンスモード 117
MRA 登録数 118
承認レートコントロール 118
クレデンシャルのキャッシング 119
Cisco Jabber 用 SIP 登録フェールオーバー 120
クラスタ化した Expressway システムとフェールオーバーの考慮事項 123
Expressway 自動侵入保護 123
例外の設定 124
Unified Communications サービス ステータスの確認 125
検出されたノードを更新する必要があるのはなぜですか? 125
Expressway-C でのサーバー更新 126

第 8 章 MRA のトラブルシューティング 127
一般的なテクニック 127
アラームとステータスメッセージ 127
Collaboration Solutions Analyzer の使用 128
診断ログ 128
Jabber for Windows 診断ログ 128
Cisco Expressway 診断ログ レベルの構成 128
診断ログキャプチャの作成 128
ログの作成後 129
ドメインネームシステム（DNS）レコードの確認 129
Cisco Expressway-E が到達可能であることを確認します 130
通話状況の確認 130
モバイルおよびリモートアクセス通話 ID 131
リッチメディアセッション（Cisco Expressway のみ） 131

Cisco Expressway 経由で Unified CM に登録されたデバイス 131
Unified CM のアイデンティティデバイス 131
Cisco Expressway-C でのプロビジョニングセッションを識別 132
Cisco Expressway-C が Unified CM と同期されていることを確認してください。 132
MRA 認証ステータスとトークンの確認 132
Registration Issues 133
Unified CM にエンドポイントを登録できない 133
Cisco Expressway 証明書と TLS 接続の問題 134
CiscoSSL 5.4.3 が 1024 ビット未満の Diffie-Hellman キーを拒否する 134
Cisco Jabber サインインの問題 134
Jabber が自動侵入保護をトリガーする 134
ネットワーク外からの接続時、Jabber ポップアップが無効な証明書を警告する 136
Jabber が電話サービスに登録しない 136
XMPP のバインド障害が原因で Jabber がサインインできない 136
SSH トンネル障害が原因で Jabber がサインインできない 137
Cisco Expressway-E のクラスタ内の異なるピアに接続すると Jabber がサインインできない 137
特定の問題 137
Cisco Expressway が 「401 Unauthorized」 のエラーメッセージを返します。 137
「「407 Proxy Authentication Required」」または「「500 Internal Server Error」」のエラーによる通話障害 138
通話のビットレートが 384 kbps に制限されているまたは、BFCP（プレゼンテーション共有）使用時のビデオの問題 138
IM and Presence Service レルムの変更 138
ボイスメールサービスがありません（「403 Forbidden」 応答） 138
サービスリクエストに対する 「403 Forbidden」 応答 139
Cisco Expressway がクライアント HTTPS リクエストをドロップする 139
失敗：アドレスが IM and Presence サーバーではない 139
無効な SAML アサーション 139
「502 Next Hop Connection Failed」 メッセージ 139
着信側エンドポイントが Expressway-E から 15 ホップ以上離れている場合、MRA コールは失敗します 140

第 I 部 : 付録 141

第 9 章 HTTP 許可リストのフォーマット 143

許可リストは、ファイルの参照を決定します 143

サンプルリストルール CSV ファイル 144

許可リスト テスト ファイル リファレンス 144

サンプルリストテスト CSV ファイル 145

第 10 章 MRA 導入のアップグレード後のタスク 147

MRA アクセス制御設定を再構成するには 147

MRA アクセス制御の設定 148

アップグレードによって適用される MRA アクセス制御値 157

第 11 章 Expressway での HSM デバイスの構成 161

重要：事前の確認事項 161

HSM を有効にして管理する方法 161

タスク 1：前提条件の設定 162

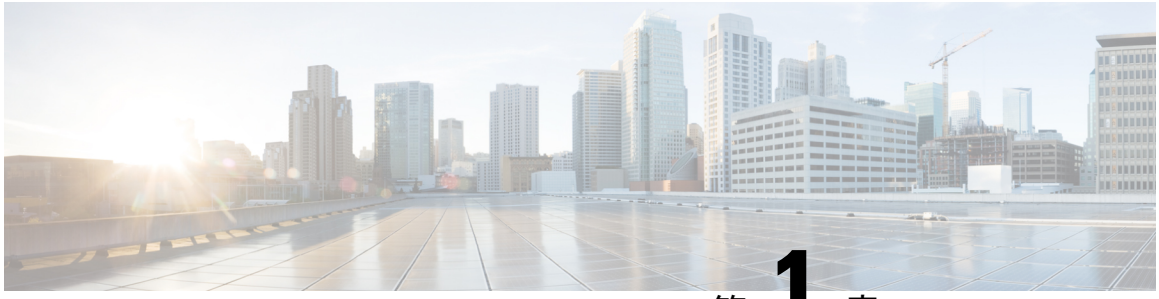
タスク 2：Expressway での HSM の有効化 163

タスク 3：HSM ステータス チェックのモニタリング 164

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 165

モジュールの削除方法 165

HSM の無効化方法 166



第 1 章

MRA の概要

- モバイルおよびリモートアクセスについて （1 ページ）
- 展開シナリオ （4 ページ）
- サポートされていない展開 （7 ページ）
- 容量情報 （11 ページ）

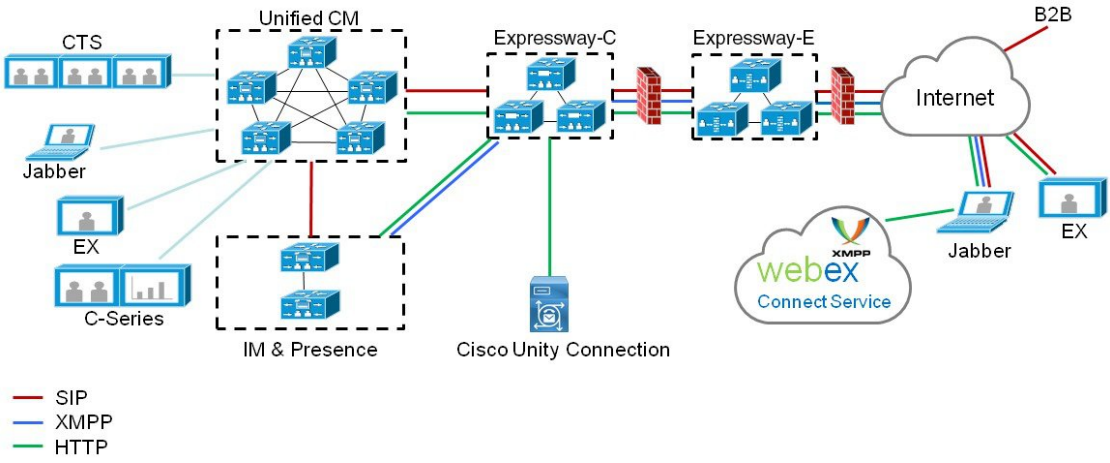
モバイルおよびリモートアクセスについて

Cisco Unified Communicationsモバイルおよびリモートアクセス（MRA） はシスコ コラボレーション エッジアーキテクチャの一部です。MRA によって、エンドポイントが企業ネットワークにある場合、 Cisco Jabber などのエンドポイントは、 Cisco Unified Communications Manager（Unified CM）が提供する登録、呼制御、プロビジョニング、メッセージおよびプレセンス サービスを設定できます。Expressway は、Unified CM 登録にセキュアなファイアウォール トラバーサルと回線側サポートを提供します。

MRA ソリューションは、次の機能を提供します。

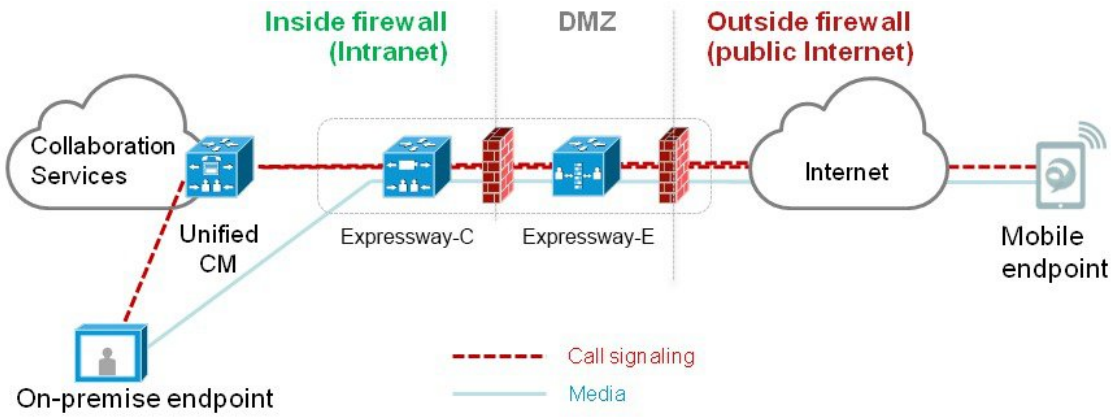
- **オンプレミスアクセス**：Jabber および EX/MX/SX シリーズクライアントに対してネットワーク外でも一貫したエクスペリエンスを提供
- **セキュリティ**：セキュアな Business-to-Business（B2B）コミュニケーション
- **クラウドサービス**：豊富な Cisco Webex 統合とサービスプロバイダー製品を提供する、柔軟で拡張性に優れたエンタープライズ クラスのソリューション
- **ゲートウェイおよび相互運用性サービス**：メディアおよびシグナリングの正規化、標準以外のエンドポイントのサポート

図 *1 : Unified Communications* : モバイルおよびリモート アクセス



（注） サードパーティのSIPまたはH.323デバイスはExpressway-Cに登録でき、必要に応じてSIPトランクを介して Unified CM 登録デバイスと相互運用することもできます。

図 *2 :* 一般的なコールフロー : シグナリングとメディアパス



Unified CM は、モバイルとオンプレミスの両方のエンドポイントに呼制御を提供します。シグナリングは、モバイルエンドポイントと Unified CM の間で Expressway ソリューションをトラバースします。メディアは、エンドポイント間で直接メディアをリレーする Expressway ソリューションをトラバースします。すべてのメディアは、Expressway-C とモバイル エンドポイント間で暗号化されます。

コア コンポーネント

MRA ソリューションには、MRA 互換のソフトクライアントや固定エンドポイントを備えた Expressway と Unified CM が必要です。これらのソリューションには、オプションで IM and

Presence サービスと Unity Connection を含めることができます。このガイドでは、次の設定が完了していることを前提としています。

- 『Expressway 基本設定導入ガイド』（このガイドは、DMZ で Expressway-E を展開するためのネットワークオプションが説明されています）で指定されている基本的な Expressway-C と Expressway-E
- Unified CM および IM and Presence Service が、『Cisco Unified Communications Manager 構成ガイド』にある該当バージョンの構成およびアドミニストレーションガイドで指定されている通りに構成されている。
- 使用されている場合、IM and Presence Service や Cisco Unity Connection が『Cisco Unified Communications Manager 構成ガイド』で説明されている通り構成されている。

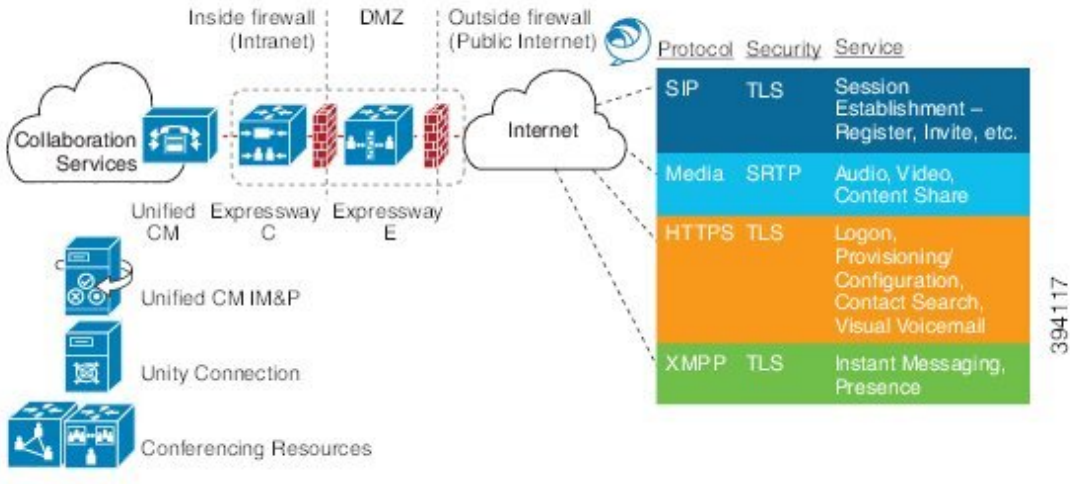
プロトコル概要

次の表では、Unified Communications ソリューションで使用するプロトコルと関連するサービスを一覧しています。

表 *1*：プロトコルと関連するサービス

プロトコル	セキュリティ	サービス
SIP	TLS	セッション確立 – Register、Invite など
HTTPS	TLS	ログオン、プロビジョニング、構成、ディレクトリ、ビジュアルボイスメール
メディア	SRTP	メディア - オーディオ、ビデオ、コンテンツ共有
XMPP	TLS	インスタントメッセージおよびプレゼンス、フェデレーション

図 *3:* プロトコルワークロード概要



VPN を使用しない Jabber クライアント接続

MRA ソリューションがオンプレミスとクラウドベースのハイブリッドサービスモデルをサポートし、企業内外で一貫したエクスペリエンスを提供します。MRA は、必要な機能を使用して、Jabber アプリケーショントラフィックおよび別のデバイスに安全な接続を提供し、VPN を経由した企業のネットワークに接続しないで通信します。これは、Windows、Mac、iOS および Android プラットフォームの Cisco Jabber クライアント向けのデバイスおよびオペレーティングシステムに依存しないソリューションです。

MRA は、企業外の Jabber クライアントで以下を実現します。

- Instant Messaging および Presence サービスの使用
- 音声/ビデオ通話
- 社内ディレクトリを検索する。
- コンテンツの共有
- Web 会議の開始
- ビジュアル ボイスメールへのアクセス

（注） TelePresence（Jabber Video）向け Cisco Jabber Video は MRA では機能しません。

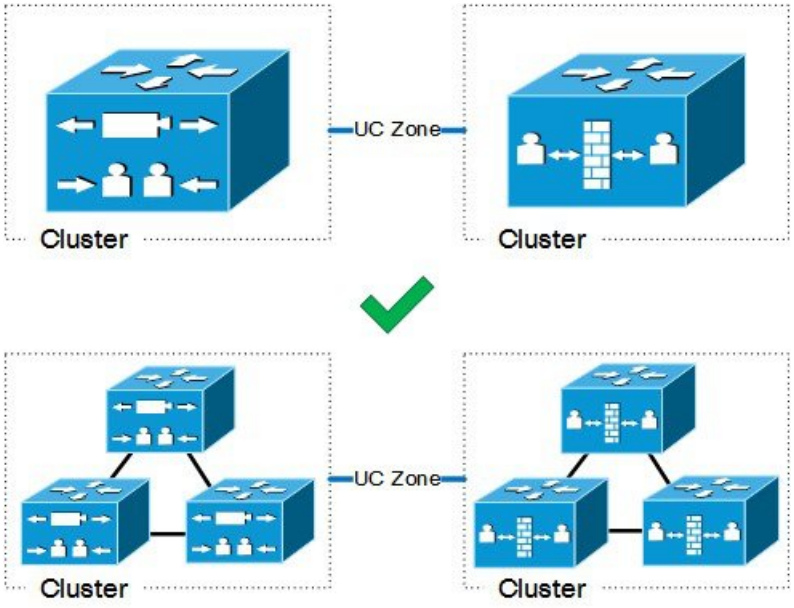
展開シナリオ

ここでは、サポートしている展開環境について説明します。

- 単一のネットワーク要素
- 単一のクラスタ化されたネットワーク要素
- 複数のクラスタ化されたネットワーク要素
- ハイブリッド展開

（注） サポートされている唯一のモバイルおよびリモートアクセスの展開は、Expressway-C クラスタと Expressway-E クラスタ間の 1 対 1 の Unified Communications ゾーンに基づいています。

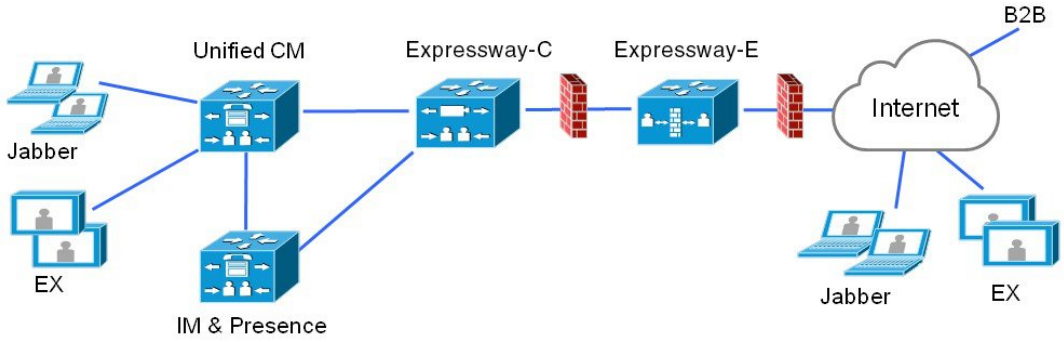
図 *4 :* サポートされる *MRA* トラバーサル接続



スタンドアロンネットワーク要素を使用した MRA

このシナリオには、スタンドアロン（非クラスター化）、Unified CM、IM and Presence Service、Expressway-C および Expressway-E サーバーが含まれます。

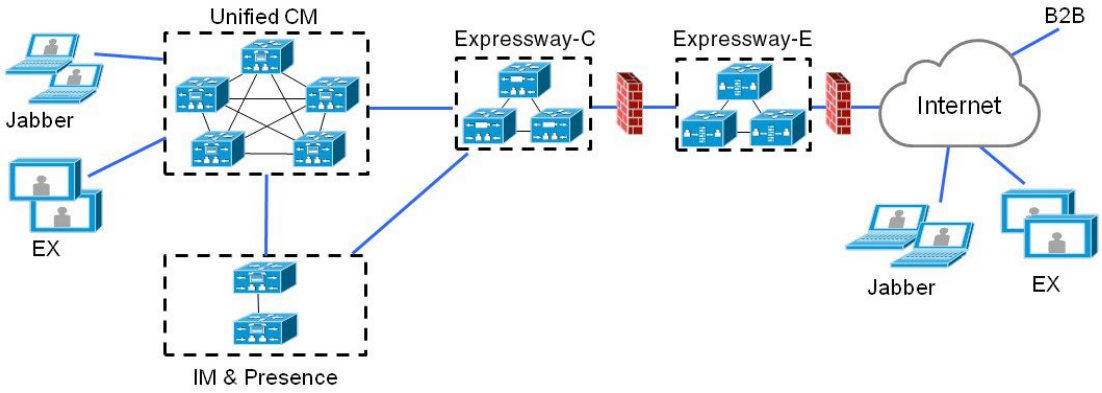
図 5: スタンドアロンネットワーク要素



クラスタ化したネットワークを使用した MRA

このシナリオでは、各ネットワーク要素がクラスタ化されています。

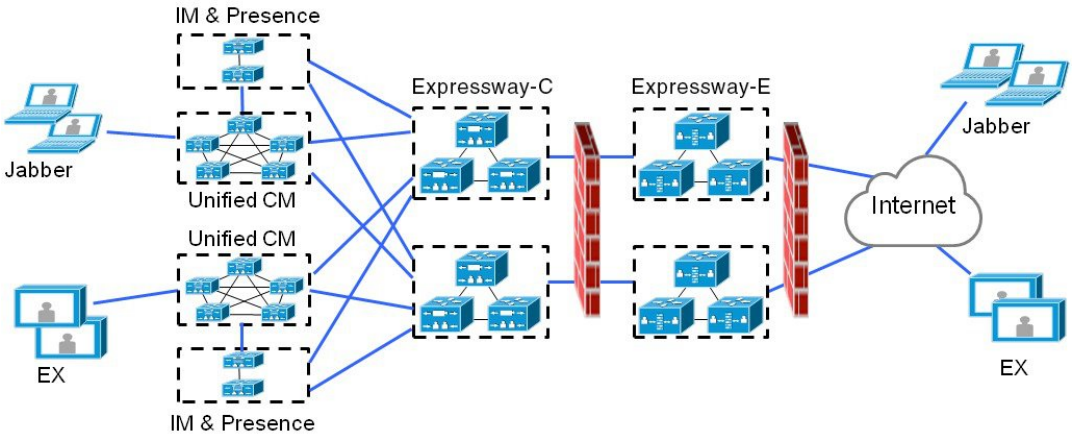
図 6: 単一のクラスタ化されたネットワーク要素



複数のクラスタ化ネットワークを使用した MRA

このシナリオでは、各ネットワーク要素に複数のクラスタが存在します。

図 7: 複数のクラスタ化されたネットワーク要素



- Jabber クライアントは、任意のルートを介して独自のクラスタにアクセスできます。
- Expressway-C は、ホームクラスタ検出要求をルーティングするときに、ラウンドロビンを使用してノード（パブリッシャまたはサブスクライバ）を選択します。
- Unified CM と IM and Presence Service クラスタの各組み合わせは、同じドメインを使用する必要があります。
- IM and Presence Service クラスタ間でクラスタ間ピアリングを設定し、クラスタ間同期エージェント（ICSA）をアクティブにする必要があります。

複数の Unified CM クラスタ

MRA 展開に複数の Unified CM クラスタが含まれている場合は、Unified CM のホームクラスタ検出を構成します。Expressway-C では、MRA ユーザーを正しいホーム Unified CM クラスタに誘導するために、この構成が必要です。次のいずれかの構成方法を使用します。

- リモート Unified CM クラスタ間にクラスタ間ルックアップサービス（ILS）ネットワークを構成します。ILS クラスタ検出は、リモートの Unified CM クラスタを検出してクラスタ間ネットワークに接続し、各クラスタのクラスタビューにデータを入力します。ILS は、大規模なクラスタ間ネットワークに適したオプションであり、すべての Unified CM クラスタで企業のダイヤルプランを複製する場合にも適しています。ただし、MRA ではダイヤルプランの複製が機能する必要がないことに注意してください。
- Unified CM **[高度な機能（Advanced Features）]** > **[クラスタビュー（Cluster View）]** メニューですべてのリモートクラスタのリストを使用して各 Unified CM クラスタを構成します。このオプションでは、ダイヤルプランの複製はできません。

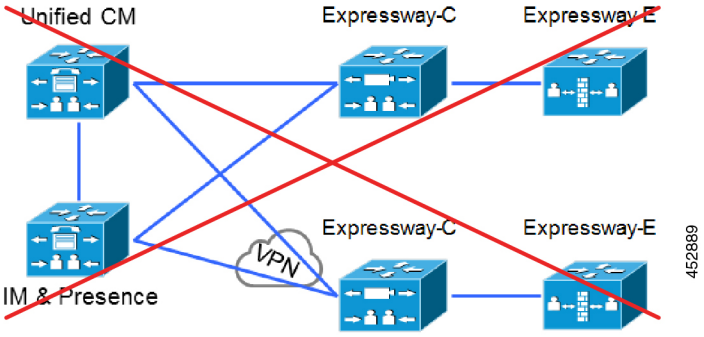
サポートされていない展開

このトピックでは、MRA でサポートされていないいくつかの展開について説明します。

VPN リンク

MRA は、Expressway-C と Unified CM サービス/クラスタ間の VPN リンクをサポートしていません。

図 *8 :* サポートされていない *VPN* リンク

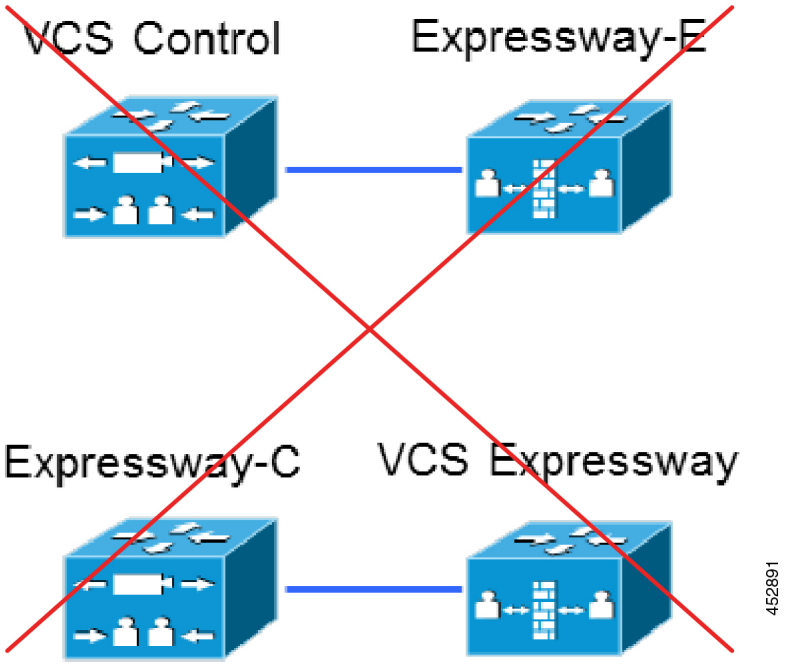


VCS シリーズと Expressway シリーズ間のトラバーサルゾーン

MRA は、「混合」トラバーサル接続をサポートしていません。Cisco VCS と Cisco Expressway 間にトラバーサルゾーンを設定することは可能ですが、MRA ではそれらをサポートしていません。

明確にすると、Expressway-E への VCS Control トラバーサルも、VCS Expressway への Expressway-C トラバーサルもサポートされません。

図 *9* : 混合トラバーサルゾーン

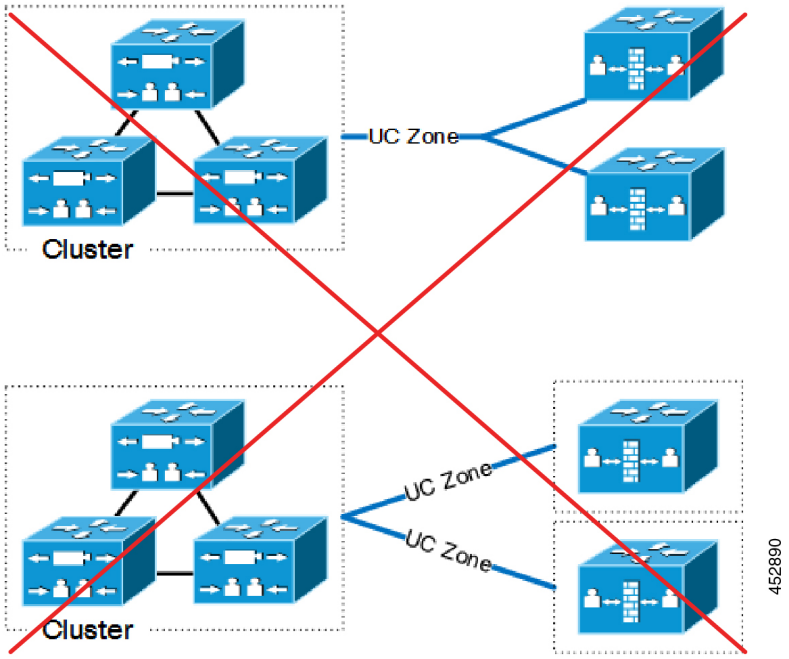


クラスタ化されていないまたは多対 1 のトラバーサル接続

1 つの Expressway-C クラスタから複数のクラスタ化されていない Expressway-E への Unified Communications ゾーンはサポートしていません。

また、1 つの Expressway-C クラスタから複数の Expressway-E または Expressway-E クラスタへの複数の Unified Communications ゾーンもサポートしていません。

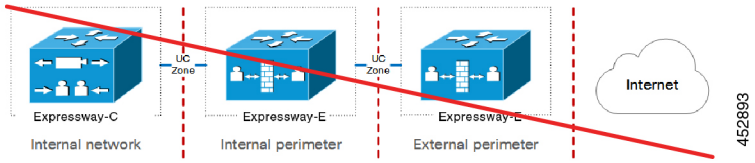
図 *10* : クラスタ化されていないまたは多対 *1* のトラバーサル接続



ネストされた境界ネットワーク

MRA は、（複数の Expressway-E を使用して複数のファイアウォールを通過する）チェーンされたトラバーサル接続をサポートしていません。Expressway-E を使用して、ネストされた境界ネットワークをトラバースして内部エンドポイントを呼び出す必要があるエンドポイントにモバイルおよびリモートアクセスを提供することはできません。

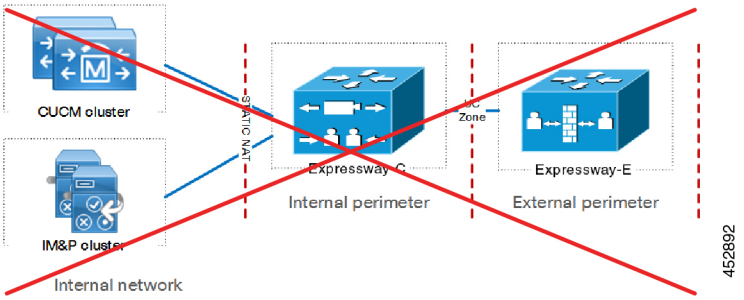
図 *11* : ネストされた境界ネットワーク



静的 NAT を使用した DMZ の Expressway-C

静的 NAT を使用する DMZ では Expressway-C はサポートされていません。静的 NAT ファイアウォール トラバーサルには SDP の書き換えが必要ですが、Expressway-C ではサポートされていません。代わりに Expressway-E を使用します。

図 *12 :* 静的 *NAT* を使用した *DMZ* の *Expressway-C*



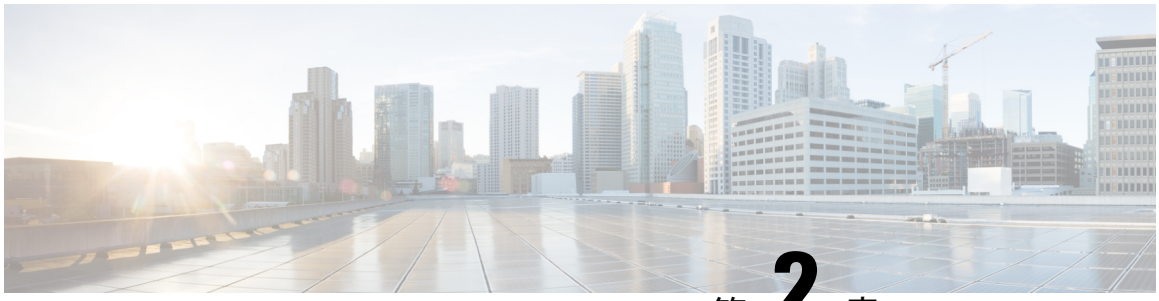
サポートされていない Expressway の組み合わせ

次の主要な Expressway ベースの展開は機能しません。これらを同じ Expressway（またはトラバーサルペア）に実装することはできません。

- モバイル & リモート アクセス
- Expressway-C ベースの B2BUA を使用した Microsoft 相互運用性
- Jabber Guest サービス

容量情報

MRA 登録制限およびその他キャパシティ情報については、『Expressway 構成ガイド』ページの『*Cisco Expressway*管理者ガイド』に記載されている「「クラスタライセンス利用およびキャパシティのガイドライン」」項を参照してください。



第 2 章

MRA 要件および前提条件

この章では、モバイルおよびリモートアクセスを構成して展開するために、展開が満たす必要がある要件と前提条件について説明します。

- モバイルおよびリモートアクセスポート （13 ページ）
- ネットワーク インフラストラクチャに関する要件 （13 ページ）
- ユニファイド コミュニケーションの要件 （18 ページ）
- 証明書の要件 （21 ページ）
- エンドポイントの要件 （26 ページ）
- 制限事項および機能サポート （30 ページ）

モバイルおよびリモートアクセスポート

MRA のポートについては、『Cisco Expressway シリーズ構成ガイド』の『*Cisco Expressway IP* ポート利用構成ガイド』を参照してください。このガイドでは、内部ネットワークの Expressway-C、DMZ の Expressway-E、およびパブリックインターネット間で使用できるポートについて説明します。

ネットワーク インフラストラクチャに関する要件

IP アドレス

Expressway-C と Expressway-E に別々の IP アドレスを割り当てます。ファイアウォールが区別できないため、両方の要素に共有アドレスを使用しないでください。

ネットワークドメイン（Network Domain）

MRA の理想的なシナリオは、分割ドメインネームシステム（DNS）構成を持つ単一のドメインを持つことであり、これが推奨されるアプローチです。これは常に可能というわけではないため、さまざまな代替シナリオに対処するために他のアプローチがいくつかあります。

（注） コールがルーティングされるドメインは、エンドポイントが登録されているMRAドメインと一致する必要があります。たとえば、エンドポイントがドメインexp.example.comに登録されている場合、コールはこのドメインにルーティングする必要があり、ドメインcluster1.exp.example.comにルーティングしてはなりません。

DNS

分割ドメインネームシステム（DNS）を使用した単一ドメイン - 推奨

単一ドメインとは、共通ドメイン（example.com）があり、内部と外部のドメインネームシステム（DNS）サーバーが存在することを意味します。これにより、ドメインネームシステム（DNS）構成に応じて、異なるネットワーク上でクライアントはドメインネームシステム（DNS）名を異なる方法で解決でき、基本 Jabber サービス検出要件に適合します。

分割ドメインネームシステム（DNS）のないデュアルドメイン

X12.5 から、Cisco Expressway シリーズ は、MRA クライアントが外部ドメインを使用して、*_collab-edge* SRV レコード、および Expressway-C が解決できないその同じドメインの *_cisco-uds* SRV レコードをルックアップするケースをサポートしています。通常、このケースは、外部ドメインで分割ドメインネームシステム（DNS）を利用できない場合です。X12.5 以前は、*_cisco-uds* レコードを解決するためのクライアント要件を満たすために、Expressway-C でピンポイントサブドメインまたはその他のドメインネームシステム（DNS）回避策が必要でした。

制限：このケースは、IP アドレスが識別する Unified CM ノードではサポートされず、FQDN のみでサポートされます。

また、この機能は、ユーザがオンプレミスで作業している場合でも、MRA 経由の Jabber アクセスのみを許可する MRA 展開のセカンダリケースもサポートします。この場合、必要なドメインは 1 つだけです。通常は、DNS レコードはパブリックに解決できます (ただし、オフプレミス時に MRA アクセスがユーザに許可されていない場合は必須ではありません)。X12.5 での変更は、Cisco Expressway-C または Jabber クライアントで利用できる *_cisco-uds._tcp.<external-domain>* ドメインネームシステム（DNS）SRV レコードが必要でないことを示します。

単一ドメインネームシステム（DNS）のないデュアルドメイン

Jabberクライアントが常にMRA経由で接続する必要がある展開では、Expressway-Cが *_cisco-uds* ドメインネームシステム（DNS）SRVレコードを解決する必要がなくなったX12.5アップデートのメリットも得られます。したがって、管理者は*_collab-edge* ドメインネームシステム（DNS）SRV レコードを構成するだけで済み、サービスディスカバリを使用する Jabber クライアントには、MRA 経由で接続するオプションしかありません。

Cisco Meeting Server Web プロキシと MRA ドメインの URL を同じにすることはできません

同じ Expressway で CMS Web プロキシサービスと MRA の両方を使用する場合、次の構成項目にサービスごとに異なる値を割り当てる必要があります。同じ値を使用しようとすると、最初に構成したサービスは機能しますが、もう一方は失敗します。

- MRA ドメイン。Expressway で構成され、Unified CM 登録が有効になっているドメイン
- CMS Web プロキシ URL リンク。**[Expressway] > [構成（Configuration）] > [Unified Communications] > [（Cisco Meeting Server）]** の順に選択し、Expressway「[ゲストアカウントクライアントURI（Guest account client URI）]」 設定で定義されます。

モバイルおよびリモートアクセス用の複数の外部ドメイン

Cisco Expressway は、複数の外部ドメインを使用してモバイルおよびリモートアクセスをサポートします。この展開では、MRA クライアントが存在する可能性のある外部ドメインが複数あります。MRA は、それらすべてに接続できる必要があります。この展開を構成するには、次の手順を実行します。

Expressway-E の場合

- パブリック ドメインネームシステム（DNS）で、各エッジドメインに対して `_collab-edge._tls.<domain>` ドメインネームシステム（DNS）SRV レコードを構成します。
- Expressway-E ホスト名を Expressway-E のパブリック IP アドレスにポイントする A レコードを設定します。

Expressway-C の場合：

- 内部ドメインネームシステム（DNS）の場合、Expressway-E FQDN を指す A および PTR レコードを追加します。これらのレコードをすべての Expressway-C ノードに追加します。
- すべてのドメインの `_cisco_uds` SRV レコードが、Unified Communications Manager クラスタを指すように設定します。
- Expressway-C の **[ドメイン（Domains）]** ページで、Unified Communications Manager クラスタを指す各内部ドメインを追加します。

複数ドメインのドメイン固有の構成タスクをまとめた構成チェックリストなどの詳細については、マルチドメイン構成の概要を参照してください。

SRV レコード

ここでは、MRA のパブリック（外部）とローカル（内部）ドメインネームシステム（DNS）の要件について説明します。詳細については、『Jabber インストールおよびアップグレードガイド』ページの『*Cisco Jabber* 計画ガイド』を参照してください。

パブリック ドメインネームシステム（DNS）（外部ドメイン）

エンドポイントがモバイルおよびリモートアクセスに使用する Expressway-E を検出できるようにするため、パブリックの外部ドメインネームシステム（DNS）は、*_collab-edge._tls.<domain>* SRV レコードで設定する必要があります。

表 *2：*例：*2* つの *Expressway-E* システムのクラスタ

[ドメイン（**Domain**）]	サービス	プロトコル	プライオリティ	ウェイト	ポート	ターゲット ホスト
example.com	collab-edge	tls	10	10	8443	expe1.example.com
example.com	collab-edge	tls	10	10	8443	expe2.example.com

ローカルドメインネームシステム（DNS）（内部ドメイン）

ローカルの内部 ドメインネームシステム（DNS）を _cisco-uds._tcp.<domain> SRV records で構成することが推奨されていても、これは、X12.5 以降で要件ではなくなりました。

重要 バージョン X8.8 以降、MRA（または Expressway-C および Expressway-E 間で XCP TLS を使用する XMPP フェデレーション）経由で IM and Presence Service を使用する場合、**各 Expressway-E システムで転送および reverse ドメインネームシステム（DNS）エントリを作成する必要があります**。これは TLS 接続を実行する Expressway-C システムが Expressway-E FQDN を解決し、Expressway-E 証明書を検証できるようにするためです。この要件は、内部の LAN 側インターフェイスにのみ影響し、外部 IP 側には適用されません。

表 *3：*例：ローカルドメインネームシステム（*DNS*）

[ドメイン（**Domain**）]	サービス	プロトコル	プライオリティ	ウェイト	ポート	ターゲット ホスト
example.com	cisco-uds	tcp	10	10	8443	cucmserver1.example.com
example.com	cisco-uds	tcp	10	10	8443	cucmserver2.example.com

MRA を使用するすべての Unified Communications ノードに対する正引きおよび reverse ルックアップの両方に内部ドメインネームシステム（DNS）を作成します。これにより、IPアドレスまたはホスト名が FQDNの代わりに使用されている場合に、のノードを検索することができます。

cisco-uds SRV レコードが内部ネットワーク外で解決できないことを確認します。解決できてしまうと、Jabber クライアントが Expressway-E 経由で MRA を開始しません。

ファイアウォール設定

- 関連するポートが内部ネットワーク（Expressway-C が配置されている）と DMZ（Expressway-E が配置されている）間、および DMZ とパブリック インターネット間のファイアウォールで設定されていることを確認します。

  内部ファイアウォールでインバウンドポートを開く必要はありません。内部ファイアウォールは、Expressway-C から Expressway-E への次のアウトバウンド接続を許可する必要があります。 SIP：TCP 7001。トラバーサルメディア：UDP 2776 から 2777（または大規模な VM/アプライアンスの場合は 36000 から 36011）; XMPP：TCP 7400; HTTPS（C と E の間の SSH 経由でトンネリング）：TCP 2222。

  外部ファイアウォールは、Expressway への次のインバウンド接続を許可する必要があります。 SIP：TCP 5061。 HTTPS：TCP 8443; XMPP：TCP 5222; メディア：UDP 36002 から 59999。

  詳細については、「Cisco Expressway シリーズ 構成ガイドページ」の『*Cisco Expressway IP* ポート使用状況構成ガイド』を参照してください。

- ファイアウォールが区別できないため、Expressway-E と Expressway-C に共有アドレスを使用しないでください。Expressway-E で IP アドレッシングにスタティック NAT を使用する場合は、Expressway-C 上の NAT が同じトラフィックの IP アドレスの解決を行わないことを確認します。Expressway-E と Expressway-C 間の共有 NAT アドレスはサポートされません。

- Expressway-C のトラバーサルゾーンは、Expressway-E サーバーのアドレスを指定するトラバーサルゾーンの **[ピアアドレス（Peer address）]** フィールドを介して Expressway-E を指します。

  - デュアル NIC の展開の場合、内部インターフェイスの IP アドレスに解決する FQDN を使用して Expressway-E アドレスを指定できます。分割ドメインネームシステム（DNS）を使用すると、必要に応じて、パブリック ドメインネームシステム（DNS）で利用可能になっているのと同じ FQDN を使用できます。分割ドメインネームシステム（DNS）を使用しない場合は、別の FQDN を使用する必要があります。

  - 静的 NAT を使用する単一の NIC の場合（この展開は非推奨です）、パブリック IP アドレスに解決する FQDN を使用して Expressway-E アドレスを指定する必要があります。これは、外部ファイアウォールが Expressway-C から Expressway-E の外部 FQDN へのトラフィックを許可する必要があることも意味します。この設計は NAT リフレクションと呼ばれており、一部のファイアウォールではサポートされていない場合があります。

詳細については、『Expressway 基本設定（Expressway-E がある Expressway-C）導入ガイド』の「「高度なネットワーク展開」」付録を参照してください。

帯域幅の制限

Cisco Unified Communications Manager のデフォルト地域の **[ビデオコールの最大セッションビットレート（Maximum Session Bit Rate for Video Calls）]** のデフォルト値は、384 kbps です。Expressway-C の **[デフォルトコール帯域幅（Default call bandwidth）]** のデフォルト値も、384 kbps です。これらの設定は、MRA 接続デバイスで想定されるビデオ品質を提供するには、低すぎる場合があります。

ユニファイドコミュニケーションの要件

製品バージョン

次の表は、MRA がさまざまな機能でサポートされるための Cisco UC 製品の最小リリースを示しています。

表 *4:* 製品バージョン

製品	**MRA** サポート	レガシー認証（**LDAP**）	**SSO** によるレガシー認証	**OAuth**（更新あり）	**SSO** による **OAuth** 更新	プッシュ構成
Expressway	X8.1.1	X8.1.1	X8.5.1	X 8.10.1	X 8.10.1	X 8.10.1
Unified CM	10.0	-	SAML SSO：10.5(1)	11.5(1) SU3	10.5(2)	11.5(1) SU3
IM and Presence Service（オプション）	10.0	-	SAML SSO：10.5(1)	11.5(1) SU3	10.5(2)	11.5(1) SU3
Cisco Unity Connection（オプション）	10.0	-	クラスタ全体の SSO：11.5(1) ノードごとの SSO：OpenAM: 8.6(2) SAML SSO: 10.0(1)	-	-	該当なし

Unified CM の要件

モバイルおよびリモートアクセス向けの次の Cisco Unified Communications Manager 構成要件に従います。

Unified CM の基本的な MRA 要件

- **IP アドレッシング** ー Expressway は IPv6 をサポートしていないため、Unified CM は IPv4 アドレッシングを使用する必要があります。
- **Cisco AXL Web サービス** ー このサービスはパブリッシャノードで実行する必要があります。
- **複数の Unified CM クラスタ** ー 複数の Unified CM クラスタがある場合は、**ホームクラスタディスカバリ**を設定します。Expressway-C が MRA ユーザーを正しい Unified CM クラスタに誘導できるように、エンドユーザーには **[エンドユーザー構成（End User Configuration）]** で **[ホームクラスタ（Home Cluster）]** フィールドが割り当てられている必要があります。次のいずれかの構成方法を使用します。
  - オプション 1：ILS ネットワーク — リモート Unified CM クラスタ間のクラスタ間ルックアップ サービス（ILS）ネットワークを設定します。ILS は、クラスタディスカバリを自動完了し、各クラスタの **[クラスタの表示（Cluster View）]** にデータを入力し、クラスタをクラスタ間ネットワークに接続します。ILS は、すべての Unified CM クラスタに企業ダイヤルプランを複製することもできますが、この機能は MRA では必要ありません。ILS は、特に大規模なクラスタ間ネットワークの場合に推奨されるアプローチです。
  - オプション 2：手動接続ー他のリモートクラスタへの接続を使用して、各 Unified CM クラスタを手動設定します。Cisco Unified CM Administration で、**[高度な機能（Advanced Features）]** > **[クラスタの表示（Cluster View）]** の順に選択します。このオプションでは、ダイヤルプランを複製できないので注意が必要です。
- **MRA アクセスポリシー** — MRA 経由で OAuth 認証を使用する Cisco Jabber クライアントがある場合は、Jabber ユーザーのユーザープロファイルでモバイルおよびリモートアクセスが許可されていることを確認してください。Unified CM の**ユーザープロファイル構成**内に次の設定が存在することを確認します。
  - **[モバイルおよびリモートアクセス（Mobile and Remote Access）]** チェックボックスをオンにする必要があります（デフォルト設定はオンになっています）。
  - **[Jabberデスクトップクライアントポリシー（Jabber Desktop Client Policy）]** と **[Jabber モバイルクライアントポリシー（Jabber Mobile Client Policy）]** フィールドは、展開に適切な Jabber サービスを許可するように設定する必要があります（デフォルト設定は **[IM & プレゼンス、音声およびビデオコール（IM & Presence, Voice and Video calls）]** です）。
- **プッシュ構成** — MRA 経由で iOS または Android クライアントに Cisco Jabber または Webex を展開している場合は、Unified Communications Manager でプッシュ構成と Cisco Cloud Onboarding を構成する必要があります。構成の詳細については、「プッシュ構成導入ガイド」を参照してください。
- **OAuth** — Expressway で OAuth を使用している場合は、Cisco Unified Communications Manager でも OAuth 更新ログインを有効にする必要があります。これは、Cisco Unified CM の管理

で **OAuth with Refresh Login Flow 企業パラメータ**を **[有効（Enabled）]** に設定することでオンにできます。

- MRA ユーザーおよびクライアントに SAML SSO を展開する場合は、Expressway で構成する前に Cisco Unified Communications Manager で構成する必要があります。
- MRA を介したビデオコールの場合、デフォルト値の 384 kbps ではビデオに十分でないため、**[リージョン構成（Region Configuration）]** 内の **[ビデオコールの最大セッションビットレート（Maximum Session Bit Rate for Video Calls）]** 設定を再構成することをお勧めします。
- Unified Communications Manager と Expressway が異なるドメインにある場合は、Cisco Unified Communications Manager サーバーアドレスに IP アドレスまたは FQDN を使用する必要があります。
- サービス拒否のしきい値 — 大量のモバイルおよびリモートアクセスでの通話は、すべての通話が同じ Expressway-C（クラスタ）から Unified CM に着信したときに、Unified CM でサービス拒否のしきい値をトリガーする場合があります。必要に応じて、**SIP Station TCP Port Throttle Threshold** サービスパラメータのレベルを **750 KB/秒**に上げることをお勧めします。このパラメータにアクセスするには、**[システム（System）]**>**[サービスパラメータ（Service Parameters）]**メニュー の順に選択し、**[Cisco CallManager]** サービスを選択します。
- 証明書の要件については、「証明書の要件 （21 ページ）」を参照してください。

ICE メディアパス最適化の追加要件

ICE メディアパス最適化を展開する場合は、追加の要件があります。詳細については、「ICE メディアパスの最適化の前提条件 （70 ページ）」を参照してください。

IM and Presence Service の要件

MRA 経由で IM クライアントを展開するには、IM and Presence Service に次の設定要件があります。

- **Cisco AXL Web サービス**は、IM and Presence Service データベース パブリッシャ ノードで実行されている必要があります。
- 同じドメイン内に複数の IM and Presence Service クラスタがある場合は、クラスタ間にクラスタ間ピアリングを設定する必要があります。
- Expressway は IPv6 アドレッシングをサポートしていないため、IPv4 アドレッシングを使用する必要があります。
- 証明書の要件については、「証明書の要件 （21 ページ）」を参照してください。

証明書の要件

このトピックでは、モバイルおよびリモートアクセス（MRA）の次の証明書要件について説明します。

- UC サーバーの証明書交換要件
- MRA を展開する Expressway サーバーの証明書署名要求（CSR）
- MRA 導入準備に向けた mTLS クライアント証明書の管理

証明書交換の要件

モバイルおよびリモートアクセスには CA 署名付き証明書を使用することをお勧めします。

次の表は、各アプリケーションがモバイルおよびリモートアクセスに使用する証明書と、それらのアプリケーションの証明書のアップロード要件を示しています。

この表は、MRA が使用するすべての証明書に CA 署名付き証明書を使用していることを前提としています。

表 *5：*証明書の交換要件（*CA* 署名付き証明書）

UC アプリケーション	MRA に対してこれらの証明書を提示する	交換要件

Unified CM	CallManager、
	Tomcat
		各 Unified CM クラスタは、Expressway-C 証明書を信頼する必要があります。クラスタごとに、次のことを確認してください。
		• **混合モードが有効な場合**—Expressway-C 証明書は、Unified CM の **CallManager 信頼**ストアと **Tomcat 信頼**ストアにインストールする必要があります。
		• **合モードが無効な場合**—Expressway-C を署名するルート CA 証明書は、Unified CM の **CallManager 信頼**ストアと **Tomcat 信頼**ストアにインストールする必要があります。そして、次を再起動します。
		  • Tomcat サービス
		  • CallManager サービス
		  • HA プロキシサービス（Tomcat で TLS を使用している場合）

UC アプリケーション	MRA に対してこれらの証明書を提示する	交換要件
IM and Presence Service	cup-xmpp Tomcat	各 IM and Presence Service クラスタは、Expressway-C 証明書を信頼する必要があります。クラスタごとに、次のことを確認してください。 • Expressway-C 証明書に署名するルート CA 証明書は、IM and Presence Service のストアの **cup-xmpp-trust** と **Tomcat-trust** にインストールする必要があります。
Expressway-C	Expressway-C 証明書（CA 署名）	Expressway-C は、各 Unified CM および IM and Presence Service クラスタによって提示された証明書を信頼する必要があります。さらに、Expressway-C は Expressway-E 証明書を信頼する必要があります。次の点を確認してください。 • Expressway-C の信頼できる CA リストには、Unified CM に署名するルート CA 証明書と、すべての UC クラスタの IM and Presence Service 証明書を含める必要があります。 • Expressway-C の信頼できる CA リストには、Expressway-E 証明書に署名する CA 証明書チェーン（ルートと中間証明書）を含める必要があります。 • 必要に応じて、Expressway-C の信頼できる CA リストにエンドポイント証明書を含める必要があります。 • **注意**：**UCM が 非セキュアモードで動作していても、Expressway-C 証明書に署名するために使用する**すべてのルートおよび中間証明書認証局 (CA) 証明書、または完全な認証局 (CA) チェーンを Cisco Unified Communications Manager（UCM）の *tomcat*-trust および *CallManager*-trust リストに追加することを確認してください。 **理由**：Expressway のトラフィック サーバー サービスは、サーバー（UCM）が要求するたびに証明書を送信します。これらの要求は、8443 以外のポート（例：ポート 6971、6972 ...）で実行されているサービスに対するものです。これにより、UCM が非セキュアモードでも、強制的に証明書が検証されます。

UC アプリケーション	MRA に対してこれらの証明書を提示する	交換要件
Expressway-E	Expressway-E 証明書（CA 署名）	Expressway-E は Expressway-C 証明書を信頼する必要があります。次の点を確認してください。 • Expressway-E の信頼できる CA リストには、Expressway-C 証明書に署名する CA 証明書チェーン (ルートおよび中間証明書) が含まれている必要があります。 • 必要に応じて、Expressway-E の信頼できる CA リストにエンドポイント証明書を含める必要があります。

各アプリケーションにすでにインストールされているので、同じ CA を使用してすべてのアプリケーションの証明書に署名すると、証明書管理が簡素化されます。ただし、Expressway-E にはパブリック CA を使用し、内部アプリケーションには企業 CA を使用して、証明書のコストを制限する場合があります。

（注） 事故証明書は Cisco Unified Communications Manager と IM and Presence Service に対しても使用できます。次に、証明書の要件は、1 つの例外を除いて上記の表と同じになります。Expressway-C では、Unified CM および IM and Presence Service 証明書に署名するルート CA 証明書をインストールするのではなく、Unified CM（CallManager、Tomcat）および IM and Presence Service（cup-xmpp、Tomcat）が実際にモバイルおよびリモートアクセスに使用する証明書をインストールします。

（注） Expressway-C と Expressway-E 間の UC トラバーサルゾーンの場合、他の Expressway アプリケーションが使用するルート CA 証明書をインストールするだけでは不十分です。他の Expressway アプリケーションが使用する CA 証明書チェーン（ルートと中間証明書）をインストールする必要があります。

Expressway サーバーの証明書署名要求要件

Expressway の証明書署名要求（CSR）ツールでは、Expressway でサポートされるユニファイドコミュニケーション機能に適した関連するサブジェクト代替名（SAN）について確認が求められ、組み込まれます。

次の表は、モバイルおよびリモートアクセス用の Expressway-C および Expressway-E 証明書を生成する際の証明書署名要求要件を示しています。

表 *6:* モバイルおよびリモートアクセスを備えた *Expressway* サーバーの証明書署名要求要件

証明書署名要求の拡張	Expressway-C の要件	Expressway-E の要件
サブジェクト代替名	Subject Alternative Names の Expressway-C リストには以下を含む必要があります。 • MRA エンドポイントが使用する電話機セキュリティプロファイル • Expressway クラスタ名（クラスタ化された Expressway のみ） • IM and Presence チャットノードエイリアス（フェデレーテッド グループ チャットのみ）	Subject Alternative Names の Expressway-E リストには、以下を含める必要があります。 • Unified CM 登録ドメイン • XMPP フェデレーションドメイン • IM and Presence チャットノードエイリアス（フェデレーテッド グループ チャットのみ）
クライアント認証	証明書には、Client Authentication 拡張子を含める必要があります。この拡張機能がないと、システムに証明書をアップロードできません。 （注） 要求に署名する CA がクライアント認証拡張機能を除外しないようにすることを確認してください。	証明書には、Client Authentication 拡張子を含める必要があります。この拡張機能がないと、システムに証明書をアップロードできません。 （注） 要求に署名する CA がクライアント認証拡張機能を除外しないようにすることを確認してください。

（注） 両方の Expressway に証明書署名要求を生成する際は、チャットノードエイリアスに対してドメインネームシステム（DNS）フォーマットを使用することを推奨します。

（注） Expressway-C は、一連の IM and Presence Service サーバーを検出すると、証明書署名要求（CSR）でチャートノードエイリアスを自動的に含めます。

証明書署名要求の生成と Expressway への証明書のアップロード

次の手順では、証明書署名要求の生成方法と Expressway に証明書をアップロードする方法を説明します。

1. **[メンテナンス（Maintenance）]** > **[セキュリティ（Security）]** > **[サーバー（Server）]**の順に選択し、証明書署名要求を生成し、Expressway にサーバー証明書をアップロードします。

2. **[メンテナンス（Maintenance）]** > **[セキュリティ（Security）]** > **[信頼できる CA（Trusted CA）]** の順に選択し、Expressway に信頼された証明機関（CA）証明書をアップロードします。
3. Expressway を再起動して、新しい信頼された証明機関（CA）を有効にします。

（注） Cisco Expressway 証明書用の証明書署名要求生成用の証明書署名要求ツールの使用方法およびExpresswayへの証明書のアップロード・ダウンロード方法については、『Expressway 構成ガイド』ページの「*Cisco Expressway* 証明書作成および仕様の導入ガイド」を参照してください。

MRA 導入準備に向けた mTLS クライアント証明書の管理

MRA クライアントがクライアント証明書を提示する場合は、クライアント証明書に署名する CA 証明書を mTLS CA 信頼リストに追加してください。

mTLS の [CA証明書（CA certificate）] ページは、[信頼できる CA 証明書（Trusted CA certificate）] ページ（**[メンテナンス（Maintenance）]** > **[セキュリティ（Security）]** > **[信頼できる CA 証明書（Trusted CA certificate）]**）からアクセスできます。

このページが適用されるのは、Cisco Unified Communications 製品でモバイルおよびリモートアクセス（MRA）用に Expressway を使用していて、アクティベーションコードによる導入準備が MRA に対して有効にされている場合のみです。

次の手順では、mTLS 証明書を Expressway にアップロードする方法について説明します。

1. **[メンテナンス（Maintenance）]** > **[セキュリティ（Security）]** > **[CA証明書（CA Certificate）]** の順に選択します。
2. 関連タスクの下にある **[信頼できるCA証明書でアクティベーションコードを導入準備（Activation Code onboarding trusted CA certificate）]** をクリックし、mTLS 接続用の CA 証明書をアップロードします。
3. CA 証明書をアップロードしたら、**[mTLSにCA証明書を付加する（Append CA certificate for mTLS）]** をクリックします。

エンドポイントの要件

MRA に互換性のあるクライアント

表 *7: MRA* に互換性のあるクライアントバージョン

Jabber	MRA サポート	レガシー認証（LDAP）	SSO によるレガシー認証	OAuth（更新あり）	SSO による OAuth 更新	APNS
Windows 版 Cisco Jabber	9.7	-	10.6	11.9	11.9	該当なし
iPhone および iPad 版 Cisco Jabber	9.6.1	-	10.6	11.9	11.9	11.9
Android 版 Cisco Jabber （Chromebook を含む）	9.6	-	10.6	11.9	11.9	該当なし
Mac 版 Cisco Jabber	9.6	-	10.6	11.9	11.9	該当なし

Jabber クライアントは、サーバー証明書の検証で接続している Expressway-E のアイデンティティを検証します。これを行うには、信頼できる CA リストで Expressway-E のサーバー証明書の署名に使用された認証局が必要です。

Jabber は、基盤となるオペレーティングシステムの証明書メカニズムを使用します。

- Windows：証明書マネージャ
- MAC OS X：キーチェーンアクセス
- IOS：信頼ストア
- Android：場所とセキュリティ設定

MRA の Jabber クライアント構成詳細については、関連するクライアントの『設置と構成ガイド』を参照してください。

- Windows 版 Cisco Jabber
- iPhone および iPad 版 Cisco Jabber
- Android 版 Cisco Jabber
- Mac 版 Cisco Jabber（X8.2 以降が必要）

Cisco Webex クライアント

Expressway は、互換性のあるソフトウェアバージョンを実行している MRA 接続 Webex クライアントでの通話をサポートしています。

- Cisco Webex for Windows
- Cisco Webex for Mac
- Cisco Webex for iPhone and iPad
- Cisco Webex for Android

MRA に互換性のあるエンドポイント

表 *8 : MRA* に互換性のあるエンドポイント

エンドポイント	MRA サポート
Cisco IP Phone 7800 シリーズ	11.0(1)
Cisco Wireless IP Phone 8821、8821-EX、Cisco Unified IP Conference Phone 8831 以外の Cisco IP Phone 8800 シリーズ	11.0(1)
Cisco IP Conference Phone 7832	12.1(1)
Cisco IP Conference Phone 8832	12.1(1)
Android ベースの Cisco DX650、DX70、および DX80 デバイス	10.2.4(99)
以下の Cisco Webex Desk シリーズ エンドポイント • Cisco Webex DX80 • Cisco Webex Desk Pro	ハードウェアがサポートするすべての CE リリース
以下の Cisco Webex Board シリーズ エンドポイント • Cisco Webex Board 55 • Cisco Webex Board 70 • Cisco Webex Board 85s	ハードウェアがサポートするすべての CE リリース

エンドポイント	MRA サポート
以下の Cisco Webex Room シリーズ エンドポイント • Cisco Webex Room 55 • Cisco Webex Room 70 G2 • Cisco Webex Room 55 Dual • Cisco Webex Room 70 Dual G2 • Cisco Webex Room Panorama • Cisco Webex Room 70 Panorama • Cisco Webex Room 70D Panorama アップグレード • Cisco Webex Room Kit • Cisco Webex Room Kit Pro • Cisco Webex Room Kit Plus • Cisco Webex Room Kit Mini • Cisco Webex Codec Plus	ハードウェアがサポートするすべての CE リリース
Cisco TelePresence エンドポイント：SX シリーズ、EX シリーズ、MX シリーズ、プロファイルシリーズ、C シリーズ	TC7.1
Cisco TelePresence および Webex エンドポイント： • DX70 • DX80 • MX700 • MX800 • MX800 デュアル • SX10 • SX20 • SX80 • MX200 G2 • MX300 G2	CE 8.2

EX、MX、SX シリーズエンドポイント（TC ソフトウェアを実行）

プロビジョニングモードが *[Expressway*経由の*Cisco UCM*（*Cisco UCM via Expressway*）*]* に設定されていることを確認します。

これらのデバイスでは、サーバー証明書の検証で接続している Expressway- E のアイデンティティを確認する必要があります。これを行うには、信頼できる CA リストで Expressway-E のサーバー証明書の署名に使用された認証局が必要です。

デバイスには、最も一般的なプロバイダー（Verisign や Thawte など）に対応するデフォルトの CA リストが付属しています。関連する CA が含まれていない場合は、追加する必要があります（手順については、『エンドポイント管理者ガイド』を参照してください）。

相互認証は任意です。これらのデバイスで、クライアント証明書を提供する必要はありません。相互 TLS を設定する場合、CAPF 登録を使用してクライアント証明書をプロビジョニングすることはできません。代わりに、デバイスに証明書を手動適用します。クライアント証明書は Expressway-E で信頼される認証局によって署名される必要があります。

Android ベースの DX650、DX80、DX70 デバイスとサポートされている IP Phone 7800 および 8800 モデルに関する考慮事項

これらのデバイスを展開して MRA 経由で Cisco Unified Communications Manager に録する場合は、次の点に注意してください。DX エンドポイントの場合、これらの考慮事項は Android ベースのデバイスにのみ適用され、CE ソフトウェアを実行している DX70 または DX80 デバイスには適用されません。

- **信頼リスト**：Cisco IP Phone 7800 シリーズ および Cisco IP Phone 8800 シリーズ デバイスのルート CA 信頼リストを変更することはできません。Expressway-E のサーバー証明書が、デバイスが信頼する CA の 1 つによって署名されていること、およびその CA が Expressway-C および Expressway-E によって信頼されていることを確認してください。
- **オフフック ダイヤル**：これらのデバイスと Unified CM の間で KPML ダイヤルが機能する方法は、MRA 経由でオフフックダイヤルを実行できるようにするために Cisco Unified Communications Manager 10.5(2)SU2 以降が必要であることを意味します。この依存関係を回避するには、オンフックダイヤルを使用します。

サポートされている MRA 機能

特定のクライアントおよびエンドポイントに対して MRA を介してサポートされる機能については、関連製品のドキュメントを参照してください。

エンドポイント	参照先
Cisco Jabber	『*Cisco Jabber* 向け計画ガイド』（お使いのバージョン）の「リモートアクセス」章の「サポートされているサービス」を参照してください。
Cisco IP Phone 7800 シリーズ	『*Cisco Unified Communications Manager* 向け *Cisco IP Phone 7800* シリーズ アドミニストレーション ガイド』の「電話機の機能と設定」章の「Expressway を介してモバイルおよびリモートアクセスで利用できる電話機の機能」を参照してください。

エンドポイント	参照先
Cisco IP Conference Phone 7832	『*Cisco Unified Communications Manager* 向け *Cisco IP Conference Phone 7832* アドミニストレーション ガイド』の「電話機の機能と設定」章の「Expressway を介してモバイルおよびリモートアクセスで利用できる電話機の機能」を参照してください。
Cisco IP Phone 8800 シリーズ	『*Cisco Unified Communications Manager* 向け *Cisco IP Phone 8800* シリーズ アドミニストレーション ガイド』の「電話機の機能と設定」章の「Expressway を介してモバイルおよびリモートアクセスで利用できる電話機の機能」を参照してください。
Cisco IP Conference Phone 8832	『*Cisco Unified Communications Manager* 向け *Cisco IP Conference Phone 8832* アドミニストレーション ガイド』の「電話機の機能と設定」章の「Expressway を介してモバイルおよびリモートアクセスで利用できる電話機の機能」を参照してください。

制限事項および機能サポート

MRA は、さまざまな展開シナリオ、およびさまざまなクライアントとエンドポイントが使用される場合に、さまざまな機能をサポートします。この項では、次の内容について説明します。

- クライアントとエンドポイントでサポートされていない主な機能
- 特定の MRA 状況で動作しない、サポートされていない Expressway 機能

UC 機能サポートおよび制限事項

このセクションでは、MRA 接続デバイスでは動作しないことがわかっている、いくつかの主要なクライアントおよびエンドポイント機能をリストします。

（注） 詳細については、エンドポイントまたはクライアントに関するドキュメントを参照してください。次のリストはすべてを説明しているわけではありません。

- **リリースが異なる複数の IM and Presence クラスタ**—Cisco Expressway-C で複数の IM and Presence Service クラスタを構成し、一部が 11.5 以前のソフトウェアで実行されている場合、MRA エンドポイントで 11.5 に必要な機能を使用できない場合があります。これは、ラウンドロビンアプローチを使用して、Cisco Expressway-C が古い方のソフトウェアバージョンのクラスタを選択する場合があるからです。
- **デュアル ネットワーク インターフェイスがある Expressway-E**—デュアル ネットワーク インターフェイスを使用する Expressway-E システムでは、XCP 接続（IM and Presence

Service XMPP トラフィック用）は常に内部インターフェイスで使用されます。Expressway-E 内部インターフェイスが別のネットワークセグメントにあり、システム管理のみに使用さ、Expressway-C トラバーサルゾーンが Expressway-E 外部インターフェイスに接続している場合、XCP 接続に障害が発生する場合があります。

- **E911 がある Cisco Jabber**—E911NotificationURL 機能を使用して、 Cisco Jabber クライアントを MRA に展開する場合は、通知用の静的 HTML ページを設定します。MRA は、Web ページ用のスクリプトとリンクタグをサポートしていません。
- **Cisco Jabber ディレクトリアクセス**—MRA は、Cisco User Data Services（UDS）を使用して、 Cisco Jabber ディレクトリアクセスをサポートします。MRA は、Jabber の他のディレクトリ アクセス メソッドをサポートしていません。
- **Unified Contact Center Express 機能サポート**—MRA は、一部の Cisco Unified Contact Center Express 機能をサポートしません。詳細については、「Unified Contact Center Express」 ドキュメントを参照してください。
- **エンドポイント フェールオーバー動作**：
  - MRA 経由で登録され、OAuth トークンを使用する 78XX/88XX シリーズの電話機は、Cisco Unified Communications Manager ノードがダウンすると登録解除される場合がありますが、別のアクティブノードとの通信は継続します。しばらくすると電話機が再登録されます。

    OAuth トークンを使用して MRA で経由で登録された Jabber は、Cisco Unified Communications Manager ノードがダウンし、「「セッションが有効期限切れです」というメッセージが表示されると登録解除される場合があります。Cisco Jabber」 を使用して再度サインインします。Jabber にサインインすると、サービスを引き続き使用できます。
  - Cisco Jabber クライアントは、IM and Presence Service および MRA を介した SIP 登録フェールオーバーをサポートします。詳細については、Cisco Jabber 用 SIP 登録フェールオーバーを参照してください。ただし、ボイスメールやユーザーデータサービス（UDS）など、他のタイプの MRA（関連する冗長性やフェールオーバー）はサポートしていません。クライアントは単一の UDS サーバーのみを使用します。

    Expressway-C または Expressway-E ノードに障害が発生した場合、障害が発生した Expressway ノードを介したアクティブな MRA コールも失敗します。この動作は、Jabber クライアントを含むすべてのデバイスタイプに適用されます。

    MRA を介した Unified CM フェールオーバーの場合、Cisco IP Phone にはクラスタ化された Expressway-C および Expressway-E サーバーが必要です。IP Phone には、少なくとも IP Phone で構成された CallManager グループ内の Unified CM 数と同じ数の Expressway-C および Expressway-E サーバがクラスタ内に必要です。TC または CE ソフトウェアを実行しているデバイスは、Unified CM フェールオーバー向けにクラスタ化された Expressway サーバーを必要としないことに注意してください。
- **OAuth 更新ログインを使用した MRA 経由のチャット**—OAuth 更新認証（自己記述トークン）を使用した MRA 経由およびIM and Presence Service プレゼンス冗長性グループを使用

した MRA 経由のチャット/メッセージサービスが必要な場合、 Cisco Jabber 12.5 以降が必要です。12.5 以前の Jabber では、このシナリオでユーザーは、ログインできません。

- **MRA 経由の通話録音**—次の制限が含まれます。
  - MRA は、 Cisco Jabber クライアントと Webex Unified CM 登録アプリケーション用の録音トーンをサポートします。また、Jabber モバイルデバイスの CTI モニタリングには、Unified CM 12.5(1)SU1 以降が必要であることにも注意してください。

- **MRA 経由のサイレントモニタリング**—次の監視機能は、互換性のある MRA 接続エンドポイントでサポートされます。ただし、展開された UC 製品が互換性のあるバージョンで実行されており、サイレントモニタリング機能が Cisco Unified Communications Manager で構成されており、SIP Path ヘッダーが Expressway で有効化されていることが条件です（「SIP パスヘッダーの有効化 （86 ページ）」で説明）。
  - サイレントモニタリングは X12.6.1 以降でサポートされています。
  - ウィスパーコーチングとウィスパーアナウンスメントは、X12.6.2 以降でサポートされています。

- **暗号化された iX チャネル**—Expressway は、別のエンティティに代わって iX プロトコルを暗号化しません。その結果、iX はエンドツーエンドで暗号化するか、エンドツーエンドで暗号化しない必要があります。iX が暗号化されている場合、エンドポイントと会議サーバーは暗号化を処理する必要があります。

（注） iX を MRA で機能させるには、暗号化されたトランクを使用して会議サーバーを Unified CM に構成し、エンドポイント/Jabber が適切かつ iX 対応のソフトウェアバージョンで実行されているかを確認する必要があります。

- **MRA 経由の認証局プロキシ機能（CAPF）**—MRA はリモートエンドポイント用の証明書プロビジョニングをサポートしていません。制限には、認証局プロキシ機能（CAPF）が含まれます。CAPF を使用するには、オンプレミス（ファイアウォール内）で、CAPF 登録を含む初回構成を完了します。後続の証明書操作を完了するには、エンドポイントをオンプレミスに戻す必要があります。

- **暗号化された TFTP**—MRA は、CAPF 登録がすでにオンプレミスで完了している場合、MRA 経由の TFTP 構成ファイルをサポートします。

- **セッション更新機能**—SIP UPDATE メソッド（RFC 3311）に依存する次のセッション更新機能は、MRA をフェールオーバーします。
  - 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

- **P2P ファイル転送**—IM and Presence Service と Jabber を使用する場合、MRA はピア間のファイル転送をサポートしません。
- **MRA 経由のマネージドファイル転送**—IM and Presence Service 10.5.2以降（制限されたバージョン）および Jabber 10.6 以降のクライアントを使用する場合、MRA は、MRA 経由のマネージドファイル転送をサポートします。MRA は、IM and Presence Service の無制限バージョンで MFT をサポートしていません。
- **Webex Messenger Service および Cisco Jabber 用ファイル転送** — MRA は、Webex Messenger Service と Cisco Jabber を使用したファイル転送をサポートします。
- **モビリティ機能のサポート**—MRA は、セッションハンドオフを含む追加のモビリティ機能をサポートしません。
- **ハントグループサポート**—Unified CM バージョン 11.5(1)SU5 または、関連する変更のあるそれ以降のバージョンを使用する場合、MRA は、ハントグループ（ハントパイロットとハントリストを含む）をサポートします。
- **セルフケアポータルアクセス**—MRA は、Cisco Unified Communications ルフケアポータルをサポートしません。
- **キー拡張モジュール（KEM）は、互換性のある電話をサポートします。**

（注） **注意**：機能を展開するには、SIP パスヘッダーを Expressway で有効化し、パスヘッダー（リリース 11.5(1)SU4 以降を推奨）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。

- **MRA シングルサインオン** — MRA は、SAML アサーション署名用の IdP 証明書を 1 つのみサポートします。現時点では、IdP 署名証明書を複数サポートすることはできません。
- **MRA を介した負荷分散** — Expressway がノード間で負荷（登録数）が偏っていると特定した場合、負荷の再分散が実行されます。再分散中は、ロードされたパスを介して登録されたエンドポイントは、最小のロードされたパスを介して Cisco Unified Communications Manager にリダイレクトされます。このプロセスは、クラスタ全体で負荷が分散されるまで続きます。この負荷分散機能は、新しいバージョンの Jabber クライアントでのみサポートされます。この機能がサポートされているバージョンを確認するには、『Jabber ガイド』を参照してください。

サポートされていない Expressway 機能および制限事項

- 現時点では、クラスタ展開内の 1 つの Expressway ノードに障害が発生し、何らかの理由でネットワーク接続が失われた場合（Unified CM の再起動または障害がある場合を含む）、影響のあるノードを介するすべてのアクティブコールに障害が発生します。コールは別のクラスタ ピアに渡されません。Bug ID CSCtr39974 を参照してください。これは MRA 固有の問題ではなく、すべてのコールタイプに適用されます。

- MRA クライアントと Expressway-E 間のサードパーティ ネットワーク ロード バランサはサポートしていません。
- MRA 経由で接続された Cisco Jabber エンドポイントのカスタム埋め込みタブは、非常に基本的な HTML コンテンツ（JavaScript またはダイナミック HTML なし）に対してのみ機能します。
- Expressway がモバイルおよびリモートアクセス（MRA）に使用された場合、 Jabber Guest には使用できません。
- MRA の Expressway-C も Microsoft ゲートウェイサービスに使用できません。Microsoft ゲートウェイサービスには専用の Expressway-C が必要です。
- CE ソフトウェアを実行しているエンドポイントの MRA では、メンテナンスモードはサポートされていません。メンテナンス モードを有効にすると、Expressway はこれらのエンドポイントからの MRA コールをドロップします。
- Expressway は、MRA 接続に対して IPv4 モードのみサポートするため、IP 構成サポートの「IPv6 のみ」または「両方」は、サポートされていません。「両方」の場合、Expressway はクライアントから IPv6 MRA トラフィックをプロキシしないため、クライアントが IPv4 ではなく IPv6 を送信すると断続的な問題が発生する可能性があります。
- エンドポイント管理機能（SNMP、SSH/HTTP アクセス）はサポートされていません。
- **MRA を介した複数のプレゼンスドメイン**ーこの機能は、IM and Presence Service 10.0(x) 以降を備えた Expressway X12.6.3 からサポートされます。互換性のあるクライアントは、1 つ以上のドメインまたは、サブドメインのあるドメインのユーザーを持つインフラストラクチャに展開できます。Unified Communications のデフォルトの展開では、ドメインを 75 以下にすることをお勧めします。

  Expressway を介した XMPP/チャットおよびプレゼンスフェデレーションの場合、XMPP フェデレーションが単一 Expressway クラスタのみでサポートされているという既存用件のみが引き続き適用されます。

  X12.6.3 より前の Expressway リリースでは、複数のプレゼンスドメインのサポートはプレビュー機能であり、次の制限があることに注意してください。

  - X8.5 以前では、各 Expressway 展開は 1 つのプレゼンスドメインのみをサポートしていました。（ただし、IM and Presence Service 10.0 以降では複数のプレゼンスドメインがサポートされます。）
  - X8.5 では、Expressway-C で複数の展開を作成できますが、この機能も 1 展開あたり 1 つのドメインに制限されます。
  - X8.5.1 では、1 つの展開に複数のプレゼンスドメインを含めることができます。ただし、この機能は、プレビュー状態のみで機能します。また、50 ドメイン以上を保持しないことをお勧めします。

- 大規模 VM サーバーでの展開は、Unified CM へのプロキシ登録が 2500 に制限されています。

- Expressway は、コンタクトセンター エージェントまたは MRA を経由して接続する別のユーザーに対して、一部の Cisco Unified Contact Center Express 機能をサポートしません。Expressway ペアは、CTI-QBE プロトコルをトラバースしないため、Jabber for Mac および Jabber for Windows は、MRA 経由のデスクフォン制御を提供できません。

  ただし、これらの Jabber アプリケーションまたは別の CTI アプリケーションが、Unified CM CTIManager に接続できる場合（直接接続または VPN 経由での接続）、MRA 経由で接続されているクライアントのデスクフォン制御を提供できます。

- ICE パススルーコールの場合、ホストとサーバー再帰アドレスが正常にネゴシエートできない場合、エンドポイントは TURN サーバーのリレーアドレスを利用して、最適化されたメディア パスを確立できます。ただし、Expressway が TURN サーバーとして使用され、静的 NAT が Expressway-E で設定されている場合、メディアはリレーアドレスを使用して渡すことはできません（CDETS CSCvf85709 を参照）。この場合、デフォルトのトラバーサルパスがメディアのトラバースに使用されます。つまり、メディアは Expressway-C と Expressway-E を通過します。

- Expressway-E は、ICE パススルーコールの TCP 経由の TURN リレーをサポートしていません。

- 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。

- **リダイレクト URI サポート** — 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、クラスタ展開では機能しません。例えば、モバイルの Jabber または Webex クライアントに、モバイルの外部ブラウザの IP アドレスとは異なる IP アドレスが割り当てられた場合などが挙げられます。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

Cisco Jabber SKD の部分サポート

次のサポートされている Cisco Jabber SDK 機能は MRA 経由で使用できます。

- サインイン、サインアウト
- 電話サービスの登録
- 音声/ビデオ通話の発信および受信
- 保留と再開、ミュート/ミュート解除、通話転送

詳細については、『Cisco Jabber SDK のスタートアップガイド』を参照してください。

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、ユーザー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 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 導入ガイド』の「Expressway-C と Unified CM の間のシグナリング パスの暗号化」を参照してください）。エンドツーエンドの暗号化では通常、物理エンドポイント向けに Unified CM を混合モードにする必要があります。ただし Jabber クライアントについては、混合モードではない Unified CM クラスタで SIP OAuth を活用することによって、エンドツーエンドの暗号化の要件を満たすことができます。

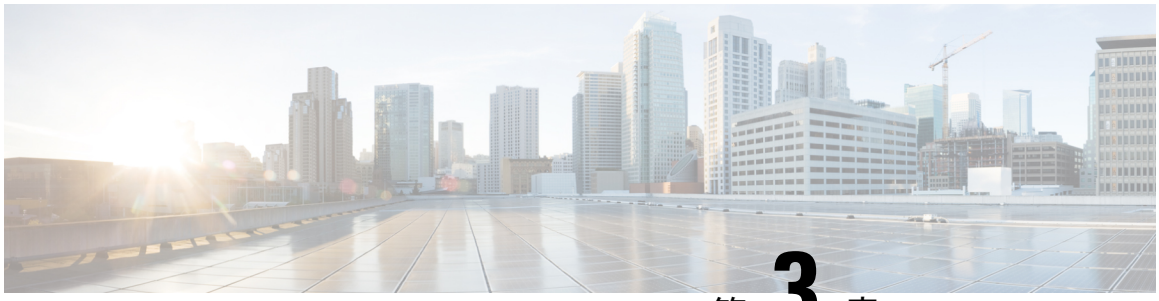
（注） Unified CM が混合モードでない場合は SIP OAuth を有効にする必要がありますが、標準のセキュア プロファイルを使用して登録できる場合は、Jabber には SIP OAuth は必要ありません。

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 Release 12.0（Cisco Collaboration Solution リリース 12.0 での OAuth の展開）』ホワイトペーパーを参照してください。

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。



第 3 章

MRA 構成

- MRA 構成の概要 （37 ページ）
- MRA 設定タスクフロー （37 ページ）
- セキュア通信の構成 （63 ページ）

MRA 構成の概要

この章には、互換性のあるエンドポイントにモバイルおよびリモートアクセスを提供する基本構成を完了する方法を説明する構成タスクが含まれています。これらの手順は、単一クラスタ、複数クラスタ、単一ドメイン、および複数ドメインのシナリオに使用できます。

MRA 設定タスクフロー

次のタスクを完了し、モバイルおよびリモートアクセスの基本設定を完了します。

始める前に

- MRA を構成する前に、MRA 要件の章を確認してください。
- MRA を展開するために必要な証明書がシステムにあることを確認してください。詳細については、証明書の要件 （21 ページ）を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	Expressway サーバーアドレスの設定 （39 ページ）	Expressway-C および E サーバーごとに、システムのホスト名、ドメイン名、および NTP ソースを設定します。
ステップ 2	SIP の有効化 （39 ページ）	Expressway-E と Expressway-C の両方で SIP が有効になっていることを確認します。

	コマンドまたはアクション	目的
ステップ 3	自動侵入保護の構成 （40 ページ）	推奨。Expressway-C で自動侵入保護を無効にし、Expressway-E で有効にします。
ステップ 4	モバイルおよびリモートアクセスを有効にします。（40 ページ）	Unified Communications モードをモバイルおよびリモートアクセスに設定します。
ステップ 5	ドメインの追加 （41 ページ）	Expressway-C で、内部 UC ドメインと、エッジドメインやプレゼンスドメインなどの他の関連ドメインを追加します。
ステップ 6	内部 UC クラスタの追加 • Unified CM クラスタの追加 • IM and Presence Service クラスタの追加 • Cisco Unity Connection クラスタの追加	各 Expressway-C クラスタから、内部 UC クラスタへの接続を作成します。
ステップ 7	MRA アクセス制御の構成 （45 ページ）	OAuth 認証や SAML SSO 設定など、MRA アクセス制御の設定を構成します。
ステップ 8	UC アプリケーションで OAuth を構成する （55 ページ）	推奨。システムがサポートしている場合は、OAuth 認証を構成します。
ステップ 9	SAML SSO の設定 （57 ページ）	オプション。SAML SSO を設定して、外部 Jabber クライアントとユーザーの Unified CM プロファイル間で共通アイデンティティを許可します。
ステップ 10	セキュアトラバーサルゾーンの構成 （61 ページ）	Expressway-C と Expressway-E の間に暗号化された UC トラバーサルゾーンを設定します。

次のタスク

基本的な MRA セットアップを完了したら、次の章を参照してください。

- ICE メディアパスの最適化 （65 ページ）—ICE は、MRA コールのメディアパスを最適化するオプション機能です。ICE により、MRA に登録されたエンドポイントは、メディアが WAN および Expressway サーバーをバイパスするように、メディアを相互に直接送信できます。
- 機能と追加構成 （81 ページ）— MRA 機能とオプションの構成については、この章を参照してください。
- MRA デバイスの導入準備 （107 ページ）—システムを構成した後、デバイスアクティベーションコードは、リモート MRA デバイスの導入準備をするための安全な方法を提供します。

Expressway サーバーアドレスの設定

この手順を使用して、Cisco Expressway-C および Expressway-E サーバーのそれぞれに FQDN と NTP サーバーを設定します。

（注） エッジドメインが複数ある場合でも、1つの Expressway サーバーは、1 つのホスト名とドメイン名を保持できます。

ステップ 1 Cisco Expressway-C で、サーバーアドレス情報を設定します。

a) **[システム（System）] > [ドメインネームシステム（DNS）（DNS）]**の順に選択します。
b) このサーバーに、**システムホスト名**と**ドメイン名**を割り当てます。
c) ドメインを検出する際に Expressway がクエリする 最大 5 台の ドメインネームシステム（DNS）サーバーに IP アドレスを入力します。これらのフィールドには FQDN ではなく、IP アドレスを使用する必要があります。

（注） 分割ドメインネームシステム（DNS）を展開する場合は、Expressway-C は内部サーバーを指し、Expressway-E は、パブリックドメインネームシステム（DNS）サーバーを指します。

ステップ 2 [NTP 設定の構成（Configure NTP Settings）] :

a) **[システム（System）] > [時刻（Time）]**メニューの順に選択し、信頼できる NTP サーバーを指します。
b) NTP 認証方式を入力する方法

- 無効 ー 認証が使用されていません
- Symmetric キーーこのメソッドを使用する際は、キー ID、ハッシュメソッドおよび Pass フレーズを指定する必要があります。
- 秘密キー—自動生成された秘密キーを使用します。

ステップ 3 Expressway-C クラスタにある各サーバーにこの手順を繰り返します。

ステップ 4 Expressway-C を設定したら、Expressway-E クラスタ内の各サーバに対してこの手順を繰り返します。

SIP の有効化

Expressway-C および Expressway-E クラスタで SIP を有効にします。

（注） SIP および H.323 プロトコルは、X8.9.2 以降のバージョンの新しいインストールで、デフォルトで無効になっています。

ステップ 1 Expressway-C プライマリピアで、**[構成（Configuration）]** > **[プロトコル（Protocols）]** > **[SIP]**の順に選択します。

ステップ 2 **[SIPモード（SIP mode）]** を**オン**にします。

ステップ 3 [保存（Save）] をクリックします。

ステップ 4 Expressway-E プライマリピアでこの手順を繰り返します。

自動侵入保護の構成

Expressway-C で自動侵入保護を無効にし、Expressway-E でサービスを有効にすることをお勧めします。

（注） Expressway-C が X8.9 以降で新しくインストールされた場合、自動侵入保護サービスはデフォルトで Expressway-C と Expressway-E の両方で実行されます（これをチェックします）。

ステップ 1 Expressway-C で、自動侵入保護を無効にします。

a) **[システム（System）]** > **[管理（Administration）]**の順に選択します。
b) **[自動保護サービス（Automated protection service）]** を **[オフ（Off）]** にします。
c) [保存（Save）] をクリックします。

ステップ 2 Expressway-E で、自動侵入保護を有効にします（サービスはデフォルトでオンになっています）。

a) **[システム（System）]** > **[管理（Administration）]**の順に選択します。
b) **[自動保護サービス（Automated protection service）]** を **[オン（On）]** に設定します。
c) **[保存（Save）]** をクリックします。

（注） 同じ IP アドレスを使用する複数の MRA ユーザーがいる場合（たとえば、同じパブリック IP アドレスを持つ NAT の背後に複数の MRA ユーザーがいる場合）、同じ IP アドレスからのすべてのトラフィックが原因で、自動侵入保護がトリガーされる可能性があります。この場合、IP アドレスに除外を設定します。詳細については、「例外の設定 （124 ページ）」を参照してください。

モバイルおよびリモート アクセスを有効にします。

ドメインとトラバーサルゾーンを構成設定する前に、Expressway でモバイルおよびリモートアクセス モードを有効にする必要があります。

ステップ 1 Expressway-C で、**[構成（Configuration）] > [Unified Communications] > [構成（onfiguration）]** の順に選択します。

ステップ 2 **[Unified Communicationsモード（Unified Communications mode）]** を **[モバイルおよびリモートアクセス（Mobile and Remote Access）]** に設定します。

ステップ 3 [保存（Save）] をクリックします。

ステップ 4 Expressway-E でこの手順を繰り返します。

ドメインの追加

Expressway-C で、MRA 展開が使用するドメインを追加します。システムの複雑さに応じて、これは単一の企業全体のドメインになる場合もあれば、次のような複数のドメインになる場合もあります。

- 企業ドメイン
- 内部 UC ドメイン（企業ドメインと異なる場合）
- エッジドメイン（他のドメインと異なる場合）
- プレゼンスドメイン（他のドメインと異なる場合）

ステップ 1 Expressway-C で、**[構成（Configuration）] > [ドメイン（Domains）]**の順に選択します。

ステップ 2 **ドメイン名**を入力します。

ステップ 3 次の各サービスの場合、サービスをこのドメインに適用するかどうかに応じて、対応するドロップダウンを **[オン]** か **[オフ]** にします。

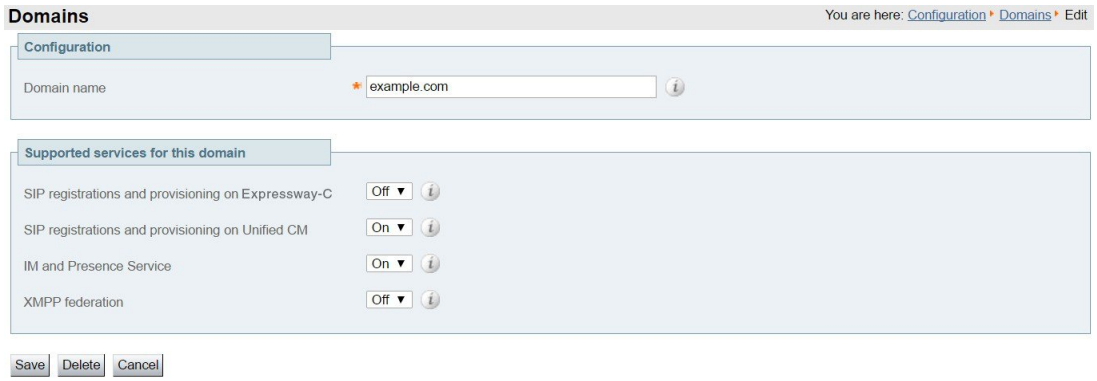
- **Expressway での SIP 登録およびプロビジョニング**—Expressway は、SIP レジストラとして機能し、任意の SIP ドメインの登録リクエストを承認します。
- **Unified CM での SIP 登録およびプロビジョニング**—Unified CM が終了登録と呼制御を処理します。Expressway は、UC サービスのゲートウェイとして機能します。
- **IM and Presence Service**—クライアントが IIM and Presence Service からサービスを取得します。
- **XMPP フェデレーション**—このドメインとパートナードメイン間で、XMPP フェデレーションを有効化します。

ステップ 4 複数の**展開**を構成した場合、このドメインを適用する展開を割り当てます。このフィールドは、複数ドメインを構成した時のみ表示されることに注意してください。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 追加を追加する場合はこの手順を繰り返します。

図 *13 :* ドメイン



Unified CM クラスタの追加

Expressway-C から各 Cisco Unified Communications Manager クラスタに接続を確立するには、この手順を使用します。各 Expressway-C クラスタは、各 Unified CM クラスタノードに到達できる必要があります。

（注）

- 登録エンドポイントにルーティング情報を戻す際、Unified CM が負荷分散を管理します。
- 負荷は、リソースの使用状況に基づいてノード全体に分散されます。エンドポイントは、Cisco Unified Communications Manager に到達するために最も負荷の少ないノードを受け取ります。コールのロードバランシングはなく、最初の登録のみが負荷分散されます。登録が負荷分散されるため、単一ノードでのコールの過負荷の可能性が減少します。

ステップ 1 Expressway-C プライマリピアで、**[構成（Configuration）]** > **[Unified Communications]** > **[Unified CMサーバー（Unified CM servers）]** の順に選択します。

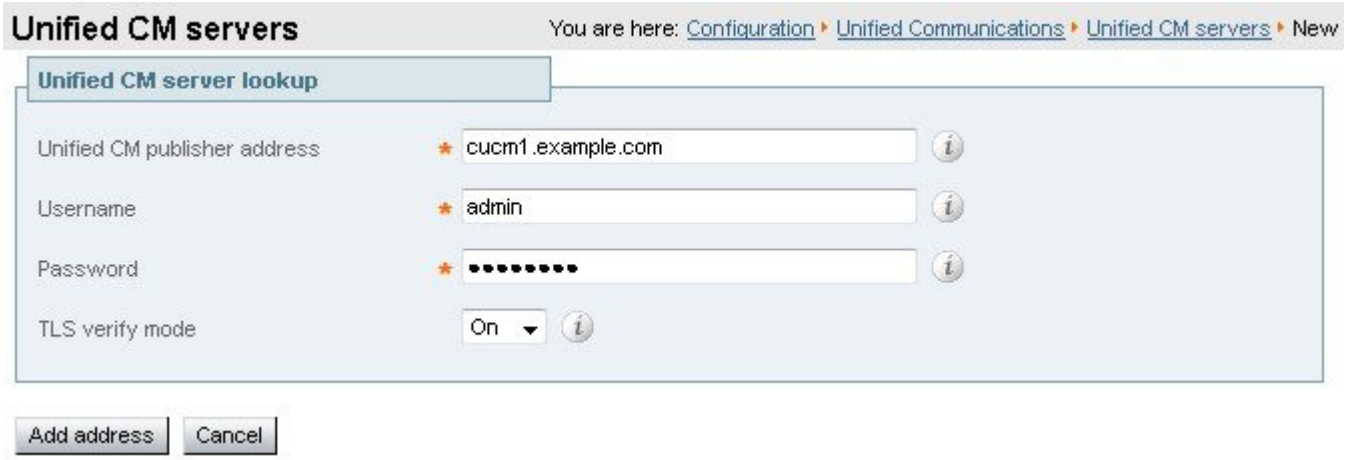
ステップ 2 **[新規（New）]** をクリックし、パブリッシャノードに関する次の詳細を追加します。

- **Unified CM パブリッシャアドレス**—パブリッシャノードのサーバーアドレス
- **ユーザー名**と**パスワード** —サーバーにアクセスできるアカウントのユーザー ID とパスワード。

  （注） これらのログイン情報は、Expressway データベースに恒久的に保管されます。対応する Unified CM ユーザーには、Standard AXL API Access ロールが必要です。

- **TLS 検証モード**
- **AEM GCM メディア暗号が**—AEM GCM サポートを有効化するには、これをオンにします。

- **展開**—複数の展開を構成した場合は、該当する展開を選択します。このフィールドは、展開を構成していない限り表示されません。



ステップ 3 **[アドレスを追加（Add Address）]** をクリックして、接続をテストします。

ステップ 4 複数の Unified CM クラスタがある場合は、手順 2 と 3 を繰り返して、追加の Unified CM クラスタのパブリッシャノードをこの Expressway-C クラスタに追加します。

ステップ 5 すべての Unified CM パブリッシャノードを追加したら、**[サーバーを更新（Refresh Servers）]** をクリックします。
Expressway-C は、各クラスタのサブスクライバノードを検出して追加します。

ステップ 6 Expressway-C クラスタが複数場合は、すべての Expressway-C クラスタがすべての Unified CM クラスタおよびノードに接続できるようになるまで、他の Expressway-C クラスタでこの手順を繰り返します。

自動生成されたゾーンと検索ルール

Expressway-C は、Expressway-C と検出された各 Unified CM ノード間で構成できないネイバーゾーンを自動生成します。TCP ゾーンは常に作成されます。TLS ゾーンは、Unified CM ノードがクラスタセキュリティモード（**[システム（System）]** > **[企業パラメータ（Enterprise Parameters）]** > **[セキュリティパラメータ（Security Parameters）]**）が 1（混合）で構成されている場合に作成されます（これにより、セキュアなプロファイルでプロビジョニングされたデバイスがサポートされます）。TLS ゾーンは、Unified CM が TLS 検証モードを有効になっている場合、**[TLS検証モード（TLS verify mode）]** が **[オン（On）]** の状態で構成されます。これは、Expressway-C が後続の SIP 通信用の CallManager 証明書を確認することを意味します。各ゾーンは「CEtcp-<node name>」または「CEtls-<node name>」の形式で作成されます。

X12.5 バージョンから、Unified CM 上で SIP OAuth モードが有効になっている場合、Expressway は、自身と検出された Unified CM ノード間に「CEOAuth <Unified CM name>」という名前のネイバーゾーンを自動的に生成します。詳細については、SIP OAuth モードの設定 （56 ページ）を参照してください。

また、同じ命名規則に従って、構成不可能な検索ルールが各ゾーンに自動作成されます。ルールは 45 の優先順位で作成されます。検索ルールの対象となる Unified CM ノード名が長い場合、検索ルールは正規表現を使ってアドレスのパターンマッチを行います。

IM and Presence Service クラスタの追加

この手順を使用して、Expressway-C から各 IM and Presence Service クラスタへの接続を作成します。各 Expressway-C クラスタは、各 IM and Presence Service クラスタ ノードに到達できる必要があります。

ステップ 1 Expressway-C で、**[構成（Configuration）]** > **[Unified Communications]** > **[IM and Presenceサービスノード（IM and Presence Service nodes）]** の順に選択します。

ステップ 2 **[新規（New）]** をクリックし、データベース パブリッシャ ノードに関する次の詳細を追加します。

- **IM and Presence データベースパブリッシャ名**—データベース パブリッシャ ノードのサーバーアドレス
- **ユーザー名**と**パスワード**—サーバーにアクセスできるアカウントのユーザー ID とパスワード。

  （注） これらのログイン情報は、Expressway データベースに恒久的に保管されます。対応する IM and Presence Service ユーザーには、Standard AXL API Access ロールを付与する必要があります。

- **TLS 検証モード**
- **展開**—複数の展開を構成した場合は、該当する展開を選択します。

  （注） このフィールドは、展開を構成していない限り表示されません。

ステップ 3 **[アドレスを追加（Add Address）]** をクリックし、接続をテストします。

ステップ 4 複数の IM and Presence クラスタがある場合は、手順 2 と 3 を繰り返して、これらの追加クラスタのデータベース パブリッシャ ノードを Expressway-C クラスタに追加します。

ステップ 5 すべての IM and Presence データベース パブリッシャ ノードを追加したら、**[サーバーを更新（Refresh Servers）]** をクリックします。
Expressway-C は、各 IM and Presence クラスタのサブスクライバノードを検出して追加します。

ステップ 6 複数の Expressway-C クラスタがある場合は、各 Expressway-C クラスタが各 IM and Presence クラスタノードに接続されるまで、他の Expressway-C クラスタでこの手順を繰り返します。

Cisco Unity Connection クラスタの追加

この手順を使用して、Expressway-C から各 Cisco Unity Connection クラスタへの接続を作成します。各 Expressway-C クラスタは、各 Cisco Unity Connection クラスタノードに到達できる必要があります。

ステップ 1 Expressway-C で、**[構成（Configuration）] > [Unified Communications] > [Unity Connection サーバー（Unity Connection servers）]**の順に選択します。

ステップ 2 **[新規（New）]** をクリックし、パブリッシャノードの次の詳細を追加します。

- **Unity Connection パブリッシャ名** — パブリッシャノードのサーバーアドレス
- **ユーザー名**と**パスワード** — サーバーにアクセスできるアカウントのユーザー ID とパスワード。

  （注） これらのログイン情報は、Expressway データベースに恒久的に保管されます。対応する Cisco Unity Connection ユーザーには、システム管理者ロールが必要です。

- **TLS 検証モード**
- **展開**—複数の展開を構成した場合は、該当する展開を選択します。

  （注） このフィールドは、展開を構成していない限り表示されません。

ステップ 3 **[アドレスを追加（Add Address）]** をクリックして、接続をテストします。

ステップ 4 複数の Unity Connection クラスタがある場合は、手順 2 と 3 を繰り返して、それらの追加クラスタのパブリッシャノードをこの Expressway-C クラスタに追加します。

ステップ 5 この Expressway-C にすべての Unity Connection クラスタを追加したら、**[サーバーを更新（Refresh Servers）]** をクリックします。
Expressway-C は、各クラスタのサブスクライバノードを検出して追加します。

ステップ 6 複数の Expressway-C クラスタがある場合は、各 Expressway-C クラスタが各 Unity Connection クラスタノードに接続されるまで、他の Expressway-C クラスタでこの手順を繰り返します。

MRA アクセス制御の構成

クライアントがモバイルおよびリモートアクセス（MRA）リクエストを認証する方法を定義します。

注意 X8.9 以前からアップグレードする場合は、アップグレード後に適用された設定はここで一覧されているものとは異なります。代わりに、「Expressway リリースノート」のアップグレード指示を参照してください。

ステップ 1 Expressway-C で、**[設定（Configuration）] > [Unified Communications] > [設定(Configuration)] > [MRAアクセスコントロール（MRA Access Control）]** に移動します。

ステップ 2 認証設定の構成

- **[認証パス（Authentication Path）]** フィールドで、SAML、SSO、LDAP または ローカルデータベースを使用して、認証ユーザーログイン情報を認証するかどうかを選択します。

- **[OAuthトークンで認証（Authorize by OAuth token）]** を選択すると Expressway で OAuth 認証が有効化されます。このオプションは、SAML SSO でのみサポートされています。

ステップ 3 追加フィールドを構成します。フィールド設定についての詳細は、「Expressway（Expressway-C）アクセス制御の設定 （46 ページ）」を参照してください。

Expressway（Expressway-C）アクセス制御の設定

次の表に MRA アクセス制御（**[構成（Configuration）]** > **[Unified Communications]** > **[構成（Configuration）]** > **[MRA アクセス制御（MRA Access Control）]**）で表示される説明を示します。この構成ページを使用して、モバイルおよびリモートアクセスの OAuth 認証設定と SAML SSO 設定を構成できます。

表 *9: MRA* アクセス制御の設定

フィールド	説明
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**—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**—Unified CM が、LDAP ログイン情報に対してクライアントをローカルで認証します。 • **SAML SSO および UCM/LDAP**—両方のメソッドを許可します。 • **[なし（None）]**—認証が適用されていません。MRA が最初に有効になるまでは、これがデフォルトです。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。**それ以外の場合はお勧めしません。** デフォルト設定：MRA がオンになる前は **[なし（None）]**。MRA をオンにすると、デフォルト値は、**UCM/LDAP** になります。

フィールド	説明
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。 OAuth は、 Cisco Jabber および Cisco Webex クライアントおよび MRA モードでデバイスアクティベーションコードを使用して導入準備をする Cisco IP Phones によってサポートされています。 **重要**：X8.10.1 から、Expressway は自己記述トークン（トークン更新、高速承認、アクセスポリシーサポートを含む）の利点を完全にサポートしています。ただし、実際にはすべての利点が広範なソリューション全体で利用できるわけではありません。使用する他の製品（Unified CM、IM and Presence Service、Cisco Unity Connection）およびそのバージョンによって、すべての製品が自己記述トークンのすべての利点を完全にサポートしているわけではありません。 Expressway でこのオプションを使用する場合は、**Unified CM および使用されている場合は Cisco Unity Connection で OAuth を更新して有効にする必要もあります**。このプロセスの概要は次のとおりです。 デフォルト設定：オン
OAuth トークンによる承認 （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 の場合、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、 Cisco Jabber および Cisco Webex クライアントのみが、この認証方式を使用しており、これは別の MRA エンドポイントではサポートされていません。 デフォルト設定：オフ
ユーザ クレデンシャルによる承認（Authorize by user credential）	**[認証パス（Authentication path）]** が UCM/LDAP または SAML SSO および UCM/LDAP の場合、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、サポートされている IP 電話機および TelePresence デバイスが含まれます。 デフォルト設定：オフ
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 の場合、利用可能。 詳細については、アイデンティティ プロバイダーの選択 （54 ページ）を参照してください。

フィールド	説明
SAML メタデータ	**[認証パス（Authentication path）]** が SAML SSO または SAML SSO および UCM/LDAP の場合、利用可能。 SAML 契約のメタデータファイルを生成する方法を決定します。設定可能なモードは、次のとおりです。 • **クラスタ**：単一のクラスタ全体の SAML メタデータファイルを生成します。SAML 契約のために、このファイルのみを IdP にインポートする必要があります。 • **ピア**：クラスタ内の各ピアに対してメタデータファイルを生成します。SAML 契約のために、各メタデータファイルを IdP にインポートする必要があります。
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 の場合、利用可能。 SAML データの操作の詳細については、「エッジ経由の SAML SSO 認証（50 ページ）」を参照してください。
Jabber iOS クライアントによる組み込みの Safari の使用の許可（Allow Jabber iOS clients to use embedded Safari）	iOS デバイスの場合、IdP または Unified CM 認証ページは、デフォルトで組み込み Web ブラウザ（Safari ブラウザではない）で表示されます。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。 この設定は、ネイティブ Safari ブラウザを使用するよう iOS デバイスの Jabber をオプションで許可します。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。 デフォルト設定：いいえ

フィールド	説明
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。 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：*get_edge_sso* リクエストは、OAuth トークンがサポートされているかどうかをユーザーのホーム 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* リクエストが送信するアイデンティティで判断します。 • 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 ノードが OAuth トークンをサポートする場合、*[いいえ（No）]* を選択すると応答時間とネットワーク全体のトラフィックを削減できます。または、ロールアウト中にクライアントがエッジ構成を取得するモードを使用するようにする場合や、すべてのノードで OAuth を保証できない場合は、*[*はい（*Yes*）*]* を選択します。 **注意：これを [はい（Yes）] に設定すると、認証されていないリモート クライアントからの不正なインバウンド要求が許可される可能性があります。**この設定に [いいえ（No）] を指定すると、Expressway は不正なリクエストを防止します。 デフォルト設定：いいえ
アクティベーションコードの導入準備を許可	**[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のみに利用可能。この設定により、Expressway のアクティベーションコードによる導入準備が有効になります。デフォルト値は **[いいえ（No）]** です。このオプションを有効にするには値を **[はい（Yes）]** に設定します。 デフォルト設定：いいえ

フィールド	説明
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。 デフォルト設定：0 秒
Webex クライアント埋め込みブラウザサポート	SSO リダイレクト URI を送信する Jabber および Webex クライアントに適用されます。 デフォルト値：いいえこのオプションを有効にするには値を [はい（Yes）] に設定します。 この機能により、Jabber と Webex クライアント組み込みブラウザサポートのセキュリティが強化されます。これにより、クライアントは、Unified Communications Manager（および MRA）OAuth フロー向けの埋め込みブラウザを使用できるようになり、ユーザーエクスペリエンスが改善されます。

（注） Expressway では、Unified CM サーバーがサポートする認証方法を確認できます。使用中のバージョン番号が表示されます。

Expressway で、**[構成（Configuration）] > [Unified Communications] > [Unified CMサーバー（Unified CM servers）]**の順に選択します。

エッジ経由の SAML SSO 認証

SAML ベースの SSO は、Unified Communications サービスリクエストを認証するためのオプションです。要求は、企業ネットワーク内、または（ここで説明されているように）外部から MRA 経由で Unified Communications サービスを要求するクライアントから発信されます。

エッジ経由の SAML SSO 認証には、**外部**アイデンティティ プロバイダー（IdP）が必要です。その認証は、エッジでの Expressway ペアのセキュアなトラバーサル機能と、内部のサービスプロバイダーと外部で解決可能なアイデンティティ プロバイダー（IdP）との間の信頼関係に依存します。

エンドポイントは VPN 経由で接続する必要はありません。これらは、複数の Unified Communications サービスにアクセスするために、1 つのアイデンティティと 1 つの認証メカニズムを使用します。認証は IdP によって所有され、 Expressway の認証も内部 Unified CM サービスもありません。

Expressway は、SAML SSO を使用した 2 種類の OAuth トークン認証をサポートします。

- シンプル（標準）なトークン。これらは常に SAML SSO 認証を必要とします。

- 更新を伴う自己記述トークン。これらは、Unified CM ベースの認証でも機能します。

（注）
- Jabber エンドポイントが更新なしで SSO を使用し、最初に Expressway/MRA を介してリモートで Unified CM を認証してからローカルネットワークに戻る場合、エンドポイント（エッジからオンプレミス）に再認証は必要ありません。
- Jabber エンドポイントが最初にローカルネットワークで Unified CM に直接認証し、次に Expressway/MRA を使用して Unified CM にリモートでアクセスする場合、エンドポイント（オンプレミスからエッジ）に再認証が必要です。

簡易 OAuth トークン認証について

前提条件

- Cisco Jabber 10.6 以降。Jabberクライアントは、モバイルおよびリモートアクセス（MRA）を介する OAuth トークン認証をサポートする唯一のエンドポイントです。
- Cisco Unified Communications Manager 10.5 (2) 以降
- Cisco Unity Connection 10.5 (2) 以降
- Cisco Unified Communications Manager IM and Presence Service 10.5(2) 以降

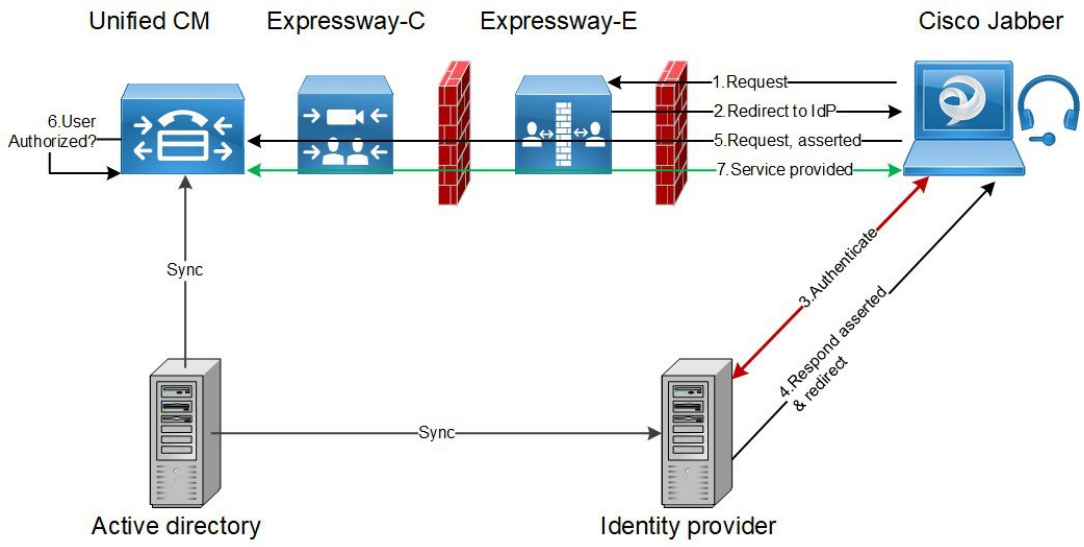
仕組み

Cisco Jabber は、ユニファイド コミュニケーション サービスを要求する前に、組織のネットワーク内にあるかどうかを判定します。Jabber がネットワークの外側にいる場合は、ネットワークのエッジにある Expressway-E からサービスを要求します。認証がエッジで有効な場合、Expressway-E はユーザーを認証するために署名した要求を使用して Jabber を IdP にリダイレクトします。

IdP は、クライアント自体を識別するためにクライアントにチャレンジを行います。このアイデンティティが認証されると、IdP は、Jabber のサービスリクエストを、アイデンティティが本物であるという署名済みアサテーションを付けて、Expressway-E にリダイレクトします。

Unified Communications サービスが、IdP と Expressway-E を信頼すると、サービスを Jabber クライアントに提供します。

図 *14*：オンプレミス *UC* サービスに対するシンプルな *OAuth* トークンベースの承認



更新を伴う自己記述 OAuth トークン承認について

Expressway は、X8.10.1 からの MRA 承認オプションとしての自己記述トークンを使用してサポートします。（**[OAuth トークンによる承認（更新あり）（Authorize by OAuth token with refresh）]** を **[はい（Yes）]** に設定します。）自己記述トークンには、次のように大きな利点があります。

- トークン更新機能により、ユーザーは繰り返し再認証する必要がありません。
- 迅速な承認。
- アクセスポリシーのサポート。Expressway は、Unified CM のユーザーに適用された MRA アクセスポリシー設定を強制できます。
- ローミングのサポート。トークンはオンプレミスでもリモートでも有効なので、ローミングユーザーはオンプレミスとオフプレミスの間を移動する場合に再認証する必要がありません。

Expressway は、特に Cisco Jabber ユーザーを円滑に進めるため、自己記述トークンを使用します。モバイルまたははリモートの Jabber ユーザーは、ローカルネットワーク（オフプレミス）から離れていても認証できます。ユーザーが元々オンプレミスで認証していた場合、後でオフプレミスに移動した場合に再認証する必要はありません。同様に、ユーザーがオフプレミスで認証した後にオンプレミスに移動した場合、ユーザは再認証する必要はありません。どちらの場合も、構成されたアクセストークンまたは更新トークン制限の対象となり、再認証が適用される可能性があります。

Jabber iOS デバイスを使用するユーザーの場合、自己記述トークンでサポートされている高速度が、Apple Push Notifications（APN）の Expressway サポートを最適化します。

自己記述トークン承認をサポートするために必要なインフラストラクチャがあることを前提として、すべての展開に対して自己記述トークン承認を推奨します。適切な Expressway 構成に

従い、Jabber クライアントが、自己記述トークンを提示した場合、Expressway は単純にトークンを確認します。パスワードまたは証明書ベースの認証は必要ありません。構成された認証パスが外部 IdP によるものか、または Unified CM によるものかにかかわらず、トークンは Unified CM によって発行されます。コールフロー内のすべてのデバイスが自己記述トークン承認用に構成されている場合、自己記述トークン承認が自動的に使用されます。

Expressway-C は、トークン認証を実行します。これにより、認証と認証設定が Expressway-E で公開されるのを回避します。

前提条件

- Expressway は、すでに Cisco Jabber に対してモバイルおよびリモートアクセスを提供しています。
- コール フロー内の他のすべてのデバイスも同様に有効化されます。
- 次の最小製品バージョン（またはそれ以降）がインストールされている。
  - Expressway X8.10.1
  - Cisco Jabber iOS 11.9

    最大 Jabber デバイスを保持していて、その一部が古いソフトウェアバージョンの場合、古いソフトウェアバージョンは、単純な OAuth トークン認証を使用します（SSO と IdP が設定されていることが前提）。
  - Cisco Unified Communications Manager 11.5(SU3)
  - Cisco Unified Communications Manager IM and Presence Service 11.5(SU3)
  - Cisco Unity Connection 11.5(SU3)
- 自己記述認証が Cisco Expressway-C（**[OAuth トークン（更新あり）（OAuth token with refresh）]** 設定で認証）および Unified CM および/または IM and Presence Service（**OAuth with Refresh Login Flow** 企業パラメータ）でオンであることを確認します。
- Expressway で定義した Unified CM ノードを更新する必要があります。これにより、Expressway がトークンを復号化する Unified CM からキーをフェッチできます。

OAuth トークンの前提条件

このトピックでは、OAuth トークンに関して展開が満たす必要のある前提条件について説明します。

Expressway Pair 上

- Expressway-E と an Expressway-C はネットワークエッジで連携するように構成されています。
- Unified Communications トラバーサルゾーンは、Expressway-C と Expressway-E の間で構成されています。

- OAuth 経由でアクセスする SIP ドメインは、Expressway-C で構成されています。
- Expressway-C では MRA が有効化されており、必要な Unified CM リソースが検出されています。
- 必要な Unified CM リソースは、Expressway-C の HTTP 許可リストにあります。
- 複数の展開を使用する場合、OAuth がアクセスする Unified CM リソースは、Jabber クライアントからコールされるドメインと同じ展開にあります。

Cisco Jabber クライアント上

- クライアントは、正しいドメイン名/SIP URI/チャットエイリアスを使用して内部サービスを要求するように構成されている。
- デフォルトブラウザは Expressway-E および IdP を解決できます。

Unified CM での手順

非 OAuth MRA クライアントやエンドポイントに関連付けられているユーザーは、Unified CM にログイン情報を保存しています。または、Unified CM は、LDAP 認証用に構成されています。

アイデンティティ プロバイダー上

IdP 証明書のドメインは、クライアントが IdP を解決できるように、ドメインネームシステム（DNS）で公開する必要があります。

アイデンティティ 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 を正しく設定するアシストを受けてください。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

UC アプリケーションで OAuth を構成する

Expressway で MRA を使用して OAuth 認証を使用するには、Cisco Unified Communications Manager や Cisco Unity Connection（導入されている場合）などの内部 UC アプリケーションでも OAuth 認証を有効にする必要があります。

ステップ 1 Expressway-C で、MRA アクセス制御設定で OAuth トークンの更新が有効になっていることを確認します。

a) Expressway-C で、**[構成（Configuration）]** > **[Unified Communications]** > **[構成（onfiguration）]** > **[MRA アクセス制御（MRA Access Control）]** の順に選択します。
b) **[OAuth トークンによる承認（更新あり）（Authorize by OAuth token with refresh）]** チェックボックスをオンにします。
c) [保存（Save）] をクリックします。

ステップ 2 Cisco Unified Communications Manager パブリッシャノードで、**OAuth Refresh Login Flow** 企業パラメータを有効にします。

a) Cisco Unified CM Administration から、**[システム（System）]** > **[企業パラメータ（Enterprise Parameters）]** を選択します。
b) **OAuth with Refresh Login Flow** パラメータを **[有効（Enabled）]** に設定します。
c) [保存（Save）] をクリックします。

（注） Expressway が Cisco Unified Communications Manager とは異なるドメインで設定されている場合、Cisco Unified Communications Manager 管理者は、Exp-C の関連するシステムドメインを追加することにより、Exp-C ホスト名エントリを手動で FQDN に更新する必要があります。

ステップ 3 Cisco Unity Connection で、OAuth 更新ログインを有効にし、Authz サーバーを構成します 。

a) Cisco Unity Connection Administration から、**[システム設定（System Settings）]** > **[企業パラメータ] を選択します**。
b) **[SSO および OAuth 設定]** の下で設定を構成します。
c) **[更新ログイン フローを使用した OAuth（OAuth with Refresh Login Flow）]**エンタープライズ パラメータ を **[有効（Enabled）]** に設定します。
d) [保存（Save）] をクリックします。
e) **[システム設定（System Setting）]** > **[Authzサーバー（Authz Server）]**の順に選択します。
f) 既存の構成を編集するか、新しい Authz サーバーを追加します。
g) Authz サーバー設定に **`Cisco Unified Communications Manager パブリッシャ`**を追加します。

h) [保存（Save）] をクリックします。

次のタスク

システムが必要な要件を満たしている場合は、Cisco Unified Communications Manager で SIP OAuth モードを有効にします。

SIP OAuth モードの設定

この手順を使用して、Cisco Unified Communications Manager で SIP OAuth モードを有効にします。SIP OAuth モードは、安全な SIP 回線シグナリングが必要であり、システムがそれをサポートしている場合にお勧めします。

（注） X14.0 リリースから、SIP OAuth モードは 7800 および 8800 シリーズの Cisco IP Phone でサポートされます。SIP OAuth モードの詳細情報に関しては、『*Cisco Unified Communications Manager* の機能構成ガイド』の「「SIP OAuth モードの構成」」章を参照してください。

始める前に

Cisco Unified Communications Manager で、OAuth 更新ログインを有効にする必要があります。これは、**OAuth with Refresh Login Flow** 企業パラメータを **[有効（Enabled）]** にすることで設定できます。

ステップ 1 SIP OAuth を使用するサーバーごとに、SIP OAuth ポートを設定します。

a) Cisco Unified CM Administration で、**[システム（System）]** > **[Cisco Unified CM]** の順に選択します。
b) **[TCPポート設定（TCP Port Settings）]** を設定します。
c) [保存（Save）] をクリックします。

ステップ 2 Expressway-C への OAuth 接続の構成方法

a) Cisco Unified CM Administration で、**[デバイス（Device）]** > **[Expressway-C]**の順に選択します。
b) **[新規追加（Add New）]** をクリックします。
c) Expressway-C アドレスの追加
d) [保存（Save）] をクリックします。

ステップ 3 SIP OAuth モードを有効にする方法

a) ノードで、コマンド ライン インターフェイスにログインします。
b) `utils sipOAuth-mode enable` の CLI コマンドを実行します。

ステップ 4 **Cisco CallManager** サービスを再起動する方法

a) Cisco Unified Serviceability で、**[ツール（Tools）]** > **[コントロールセンター - 機能サービス（Control Center - Feature Services）]**の順に選択します。
b) **[サーバ（Server）]** ドロップダウン リストからサーバを選択します。

c) **Cisco CallManager** サービスを確認し、[再起動（Restart）] をクリックします。
d) エンドポイントが SIP OAuth モードで登録する各ノードを再起動します。

ステップ 5 電話機セキュリティプロファイルで OAuth 認証を有効化します。

a) Cisco Unified CM Administration で**[システム（System）] > [セキュリティプロファイル（Security Profile）] > [電話機セキュリティプロファイル（Phone Security Profile）]**の順に選択します。
b) **[検索（Find）]** をクリックして、MRA エンドポイントに関連付けられているプロファイルを選択します。
c) [OAuth 認証の有効化（Enable OAuth Authentication）] チェックボックスをオンにします。
d) ICE Media Path Optimization を使用している場合は、**[デバイスセキュリティモード（Device Security Mode）]** を **[暗号化（Encrypted）]** に設定し、**[転送タイプ（Transport Type）]** を **[TLS]** に設定します。
e) [保存（Save）] をクリックします。

SAML SSO の設定

モバイルおよびリモートアクセス用に Cisco Expressway で SAML SSO を設定する場合は、次のタスクを実行します。

始める前に

- 内部 UC アプリケーション用に SAML SSO を構成します。詳細については、『シスコ ユニファイドコミュニケーション ソリューション用*SAML SSO*導入ガイド』を参照してください。
- Expressway-C の MRA アクセス制御設定では、**[認証パス（Authentication path）]** フィールドを **[SAML SSO認証（SAML SSO authentication）]** または **[SAML SSOおよびUCM/LDAP（SAML SSO and UCM/LDAP）]** に設定する必要があります。

注意 次の変更では、SAML メタデータを更新する必要があります。

- Expressway の変更：Expressway-C 証明書、FQDN、クラスタの追加 (メタデータを送信して再度インポート)
- IDP の変更：FQDN、証明書、またはクライアントとの信頼関係に影響を与えるもの（最新のメタデータを再インポート）

手順

	コマンドまたはアクション	目的
ステップ 1	Expressway-C から SAML メタデータをエクスポート（58 ページ）	Expressway-C から メタデータファイルをエクスポートします。

	コマンドまたはアクション	目的
ステップ 2	アイデンティティ プロバイダの設定	Expressway メタデータをアイデンティティ プロバイダー（IdP）にインポートし、IdP を設定してから、IdP からメタデータファイルをエクスポートします。
ステップ 3	IdP から SAML メタデータをインポート （59 ページ）	Idp メタデータを Expressway-C にインポートし、構成を完了します。
ステップ 4	IdP とドメインの関連付け （60 ページ）	Expressway-C で、ドメインをアイデンティティ プロバイダーに関連付けます。
ステップ 5	SAML SSO に ADFS を構成 （60 ページ）	ADFS のみ。Active Directory フェデレーションサービスを使用している場合は、IdP でこれらの追加タスクを完了して構成を完了します。

Expressway-C から SAML メタデータをエクスポート

X12.5 から Cisco Expressway は、IdP との SAML 契約に対して単一のクラスタ全体のメタデータファイルを使用することをサポートしています。以前は、Expressway-C クラスタのピアごとにメタデータファイルを生成する必要がありました (たとえば、6 つのメタデータファイルなど)。クラスタ全体のオプションの場合、Expressway-C プライマリ ピアでこの手順を実行します。

（注） SAML SSO 展開で次のいずれかの Expressway 設定を変更する場合は、メタデータをプライマリピアから再エクスポートし、メタデータを IdP に再インポートする必要があります。

- プライマリピア
- サーバー証明書
- SSO 対応ドメイン
- Expressway-E ピアの IP アドレスまたはホスト名

（注） Expressway-C の SAML メタデータをエクスポートする前に、Expressway-C で、Expressway-E との有効な接続を確立する必要があります。

ステップ 1 **[構成（Configuration）]** > **[Unified Communications]** > **[構成（Configuration）]** の順に選択します。

ステップ 2 **[MRAアクセス制御（MRA Access Control）]** セクションの SAML メタデータリストでモードを選択します。

- **クラスタ**：単一のクラスタ全体の SAML メタデータファイルを生成します。このファイルのみを SAML 契約の IdP にインポートする必要があります。
- **ピア**：クラスタ内の各ピアに対してメタデータファイルを生成します。SAML 契約に対して、各メタデータファイルを IdP にインポートする必要があります。Expressway が以前の SAML SSO 対応リリースから 12.5 にアップグレードされると、[ピア（Peer）] オプションがデフォルトで選択されます。

新しい展開の場合、[SAMLメタデータ（SAML Metadata）]モードは常にデフォルトで**[クラスタ（Cluster）]**に設定されます。

既存の展開の場合、以前の Expressway リリースで SAML SSO が無効になっている場合、モードはデフォルトで**[クラスタ（Cluster）]**になり、SAML SSO が以前に有効になっている場合は**[ピア（Peer）]**になります。

ステップ 3 **[SAMLデータをエクスポート（Export SAML data）]** をクリックします。

このページには、接続された Expressway-E、またはクラスタの場合はすべての Expressway-E ピアが一覧されます。これは、これらのデータが、Expressway-C の SMAL メタデータに含まれるためです。

ステップ 4 SAML メタデータに **[クラスタ（Cluster）]** を選択した場合は、**[証明書の生成（Generate Certificate）]** をクリックします。

ステップ 5 次の手順を実行します。

- クラスタ全体のモードで、単一のクラスタ全体のメタデータファイルをダウンロードするには、**[ダウンロード（Download）]** をクリックします。
- ピアごとのモードで、個々のピアのメタデータファイルをダウンロードするには、ピアの横にある**[ダウンロード（Download）]** をクリックします。すべてを .zip ファイルにエクスポートするには、**[すべてダウンロード（Download All）]** をクリックします。

ステップ 6 生成されたファイルをコピーし、IdP に SAML メタデータをインポートする必要がある際にアクセスできる安全な場所にペーストします。

IdP から SAML メタデータをインポート

ステップ 1 Expressway-C で、**[構成（Configuration）]** > **[Unified Communications]** > **[アイデンティティプロバイダー（IdP）（Identity providers (IdP)）]** の順に選択します。

これを実行する必要があるのは、クラスタのプライマリ ピアのみです。

ステップ 2 **[SAMLから新しいIdPをインポート（Import new IdP from SAML）]** をクリックします。

ステップ 3 **[SAMLファイルをインポート（Import SAML file）]** コントロールを使用して、IdP から SMAL メタデータファイルを検索します。

ステップ 4 **[ダイジェスト（Digest）]** を必要な SHA ハッシュアルゴリズムに設定します。

Expressway はクライアントが IdP に提示する SAML 認証要求の署名にこのダイジェストを使用します。署名アルゴリズムは、SAML 認証要求の署名を検証するために IdP で想定されているものと一致している必要があります。

ステップ 5 [アップロード（Upload）] をクリックします。

Expressway-C は、IdP の通信を認証し、IdP に対する SAML 通信を暗号化できます。

（注） メタデータをインポートした後は、**[（Configuration）] > [Unified Communications] > [アイデンティティプロバイダ（IdP）（Identity providers (IdP)）]** の順に選択し、IdP 行を検索し、アクション列で **[ダイジェストの構成（Configure Digest）]** をクリックすると署名アルゴリズムを変更できます。

IdP とドメインの関連付け

ドメインの MRA ユーザーを IdP を介して認証する場合は、IdP にそのドメインを関連付ける必要があります。少なくとも 1 つのドメインを関連付けるまで IdP は値を追加しません。

ドメインと IdP 間には多対 1 の関係があります。1 つの IdP を複数のドメインに使用できますが、各ドメインに関連付けられる IdP は 1 つだけです。

ステップ 1 Expressway-C で、IdP リストを開き（**[構成（Configuration）] > [Unified Communications] > [アイデンティティプロバイダー（IdP）（Identity providers (IdP)）]**）、IdP がリストにあることを確認します。

IdP はそのエンティティ ID 別に表示されます。それぞれ関連付けられたドメインが ID の横に表示されます。

ステップ 2 IdP の行で **[ドメインの関連付け（Associate domains）]** をクリックします。

これにより、Expressway-C のすべてのドメインが一覧されます。IdP にすでに関連付けられているドメインの横には、チェックマークが表示されます。また、リスト内の他のドメインに関連付けられている別の IdP がある場合は、IdP エンティティ ID も表示されます。

ステップ 3 この IdP に関連付けるドメインの横にあるチェックボックスをオンにします。

チェックボックスの横に、（転送）と表示されている場合、ドメインの既存の関連付けが解除され、この IdP にドメインが関連付けられます。

ステップ 4 [保存（Save）] をクリックします。

選択したドメインがこの IdP に関連付けられます。

SAML SSO に ADFS を構成

アイデンティティ プロバイダーに Active Directory フェデレーションサービス（ADFS）を使用している場合は、ADFS でこれらの追加構成を完了します。

Expressway-E の信頼当事者証明を作成後、各エンティティに一部のプロパティを設定し、Active Directory フェデレーションサービス（ADFS）が Expressway-E の期待通りに SAML 応答を作成することを確認します。また、各信頼当事者証明にクレームルールを追加する必要があります。

ステップ 1 応答全体に署名するよう ADFS を構成します。信頼当事者証明が ADFS で作成されたら、Windows PowerShell® で、各 Expressway-E <Name> に対して次のコマンドを実行します。

`Set-ADFSRelyingPartyTrust -TargetName "<Name>" -SAMLResponseSignature MessageAndAssertion`。<Name> は、ADFS で設定されている Expressway-E の信頼当事者証明の名前に置き換えてください。

ステップ 2 各信頼当事者証明にクレームルールを追加する。

a) **[クレームルールの編集（Edit Claims Rule）]** ダイアログを開き、AD 属性にクレームとして送信される新規クレームルールを作成します。

b) 内部システムに対して OAuth ユーザーを識別するもの（通常は電子メールまたは SAMAccountName）に一致する AD 属性を選択します。

c) **[進行中のクレームタイプ（Outgoing Claim Type）]** として **`uid`** を入力します。

セキュアトラバーサルゾーンの構成

Expressway-C と Expressway-E の両方で、タイプ「Unified Communications traversal」の暗号化ゾーンを構成します。 Expressway-C と Expressway-E の両方で手順を完了します。

（注） この構成は、TLS 検証モードはオンに設定され、メディア暗号化モードは [暗号化を強制（Force encrypted）] に設定された状態で SIP TLS を使用する適切なトラバーサルゾーン（Expressway-C で選択した場合は、トラバーサルクライアントゾーン、Expressway-E で選択した場合は、トラバーサルサーバーゾーン）を自動設定します。

始める前に

- Expressway-C と Expressway-E が互いの証明書を信頼していることを確認してください。各 Expressway がクライアントとサーバの両方として機能すると同時に各 Expressway の証明書がクライアントとサーバとして有効であることを確認する必要があります。証明書交換要件の詳細については、「証明書の要件 （21 ページ）」を参照してください。
- Expressway は、CN ではなく、SAN 属性を使用して受信した証明書を検証することに注意してください。
- H.323 または暗号化されていない接続も必要な場合、別のトラバーサルゾーンペアを設定する必要があります。

ステップ 1 Expressway-C プライマリピアで、**[構成（Configuration）]** > **[ゾーン（Zones）]** > **[ゾーン（Zones）]**の順に選択します。

ステップ 2 [新規（New）] をクリックします。

ステップ 3 以下の表のフィールドを構成します。適切な Expressway サーバー（C または E）の設定を適用します。

表 *10 : UC* トラバーサルゾーンの設定

フィールド	**Expressway-C** の設定	**Expressway-E** の設定
名前	「「Traversal zone」」など	「「Traversal zone」」など
タイプ（Type）	Unified Communications traversal	Unified Communications traversal
[接続クレデンシャル（Connection credentials）] セクション		
ユーザー名（Username）	「「exampleauth」」など	「「exampleauth」」など
パスワード	「「ex4mpl3.c0m」」など	**[ローカル認証データベースの追加/編集（Add/Edit local authentication database）]** を選択します。ポップアップダイアログで、**[新規（New）]** をクリックし、**名前**（例：「exampleauth」）と**パスワード**（例：「ex4mpl3.c0m」）を入力し、**[ログイン情報を作成（Create credential）]** をクリックします。
SIP セクション		
ポート（Port）	Expressway-E の設定に一致する必要があります。	`7001`（デフォルト）『Cisco Expressway シリーズ構成ガイド』ページのご使用のバージョンの『*Cisco Expressway IP* ポート使用構成ガイド』を参照してください。
TLS サブジェクト名の確認（TLS verify subject name）	N/A	トラバーサルクライアントの証明書で、検索する名前を入力します（Subject Alternative Name 属性である必要があります）。トラバーサル クライアントのクラスタがある場合は、ここでクラスタ名を指定し、各クライアントの証明書に含まれることを確認します。
[認証（Authentication）] セクション		
[認証ポリシー（Authentication policy）]	[クレデンシャルを確認しない（Do not check credentials）]	[クレデンシャルを確認しない（Do not check credentials）]
[ロケーション（Location）] セクション		

フィールド	Expressway-C の設定	Expressway-E の設定
ピア 1 アドレス（Peer 1 address）	Expressway-E の FQDN を入力します。 注：IP アドレスを使用する場合（推奨していません）、そのアドレスが Expressway-E サーバ証明書に含まれている必要があります。 MRA のデュアル NIC インターフェイスで Expressway-E を構成している場合は、Expressway-E の内部インターフェイスの FQDN を入力します（IP アドレスではありません）。Expressway-C には、Expressway-E の内部 LAN の FQDN を指すローカルドメインネームシステム（DNS）レコードが必要です。	N/A
ピア 2 ～ 6 アドレス（Peer 2...6 address）	Expressway-E のクラスタである場合は、追加ピアの FQDN を入力します。	N/A

ステップ 4 [ゾーンの作成（Create zone）] をクリックします。

ステップ 5 Expressway-E プライマリピアでこれらの手順を繰り返し、Expressway-E 列の設定を適用します。

セキュア通信の構成

この展開には、Expressway-C と Expressway-E、および Expressway-E と企業外にあるエンドポイント間のセキュア通信が必要です。これには、HTTP、SIP、および XMPP の暗号化された TLS 通信の義務化、および該当する場合は証明書の交換とチェックが含まれます。Jabber エンドポイントは、Unified CM で保持されているログイン情報に対して検証される有効なユーザー名とパスワードの組み合わせを提供する必要があります。すべてのメディアが SRTP で保護されます。

Expressway-C は、Expressway-C と検出された各 Unified CM ノード間で構成できないネイバーゾーンを自動生成します。TCP ゾーンは常に作成されます。TLS ゾーンは、 Unified CM ノードが**クラスタセキュリティモード（[システム（System）] > [企業パラメータ（Enterprise Parameters）] > [セキュリティパラメータ（Security Parameters）]**）が *1*（混合）で構成されている場合に作成されます（これにより、セキュアなプロファイルでプロビジョニングされたデバイスがサポートされます）。TLS ゾーンは、Unified CM が TLS 検証モードを有効になっている場合、**[TLS検証モード（TLS verify mode）]** が *[オン（On）]* の状態で構成されます。これは、Expressway-C が後続の SIP 通信用の CallManager 証明書を確認することを意味します。

（注） Unified CM が混合モードでない場合、セキュアプロファイルは TCP を使用するようにダウングレードされます。

Unified CM パブリッシャ が Expressway に追加（または更新）された場合、Unified CM への Expressway ネイバーゾーンは、Unified CM が返す Unified CM ノードの名前を使用します。Expressway は、これらの返された名前を使用して Unified CM ノードに接続します。その名前がホスト名だけの場合

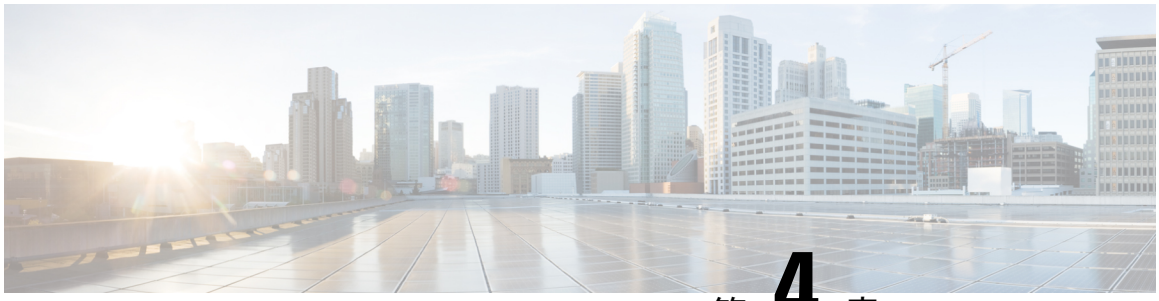
- その名前を使用してルーティング可能である必要があります
- これは、Expressway が Unified CM のサーバー証明書に公開されることを想定する名前です

セキュア プロファイルを使用している場合、 Expressway-C の証明書に署名した認証局のルート CA が CallManager の信頼証明書（Cisco Unified OS の管理アプリケーションの **[セキュリティ（Security）] > [証明書の管理（Certificate Management）]**）としてインストールされていることを確認します。

メディア暗号化

メディア暗号化は Expressway-C と Expressway-E 間、および企業外にある Expressway-E とエンドポイント間のコールレッグで実行されます。

暗号化は、メディアが Expressway-C の B2BUA にパススルーするときに物理的に適用されます。



第 4 章

ICE メディアパスの最適化

- ICE メディアパスの最適化 （65 ページ）
- ICE メディアパスの最適化の前提条件 （70 ページ）
- ICE メディアパス最適化のタスクフロー （71 ページ）
- ICE パススルーメトリックの使用 （76 ページ）

ICE メディアパスの最適化

X12.5 から、Interactive Connectivity Establishment （ICE）Media Path Optimization がサポートされます。この機能により、MRA エンドポイントのメディアパスが最適化され、MRA に登録されたエンドポイントがエンドポイント間でメディアを直接渡すことができるため、WAN と Expressway サーバーをバイパスできます。

この機能は、ICE プロトコル（RFC 5245）を使用します。ICE に関する背景情報は、https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-maintenance-guides-list.html にある『*Cisco Expressway* 管理者ガイド』の「*ICE* と *TURN* サービスについて」項を参照してください。

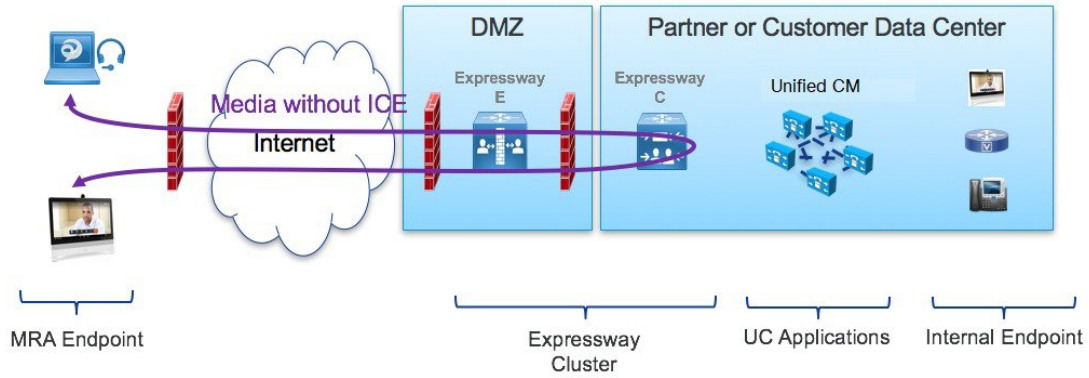
ICE の仕組み

Cisco Expressway X12.5 以前は、ICE は ICE エンドポイントの 1 つとして Cisco Expressway-C B2BUA のみサポートされていました。B2BUA がエンドポイントとして機能する場合、ICE 候補はエンドポイントと B2BUA の間でネゴシエートされます。したがって、メディアは常に Cisco Expressway-E と Cisco Expressway-C を介してトラバースします。

次の図は、メディアパスを最適化するために ICE を使用しない MRA コールを示しています。メディアは、Cisco Expressway-E と Cisco Expressway-C の両方を通過します。

ICE メディアパスの最適化

図 *15 : ICE* メディアパス最適化を使用しない *MRA* コールフロー



Cisco Expressway X12.5 で導入された ICE Media Path Optimization を使用すると、各エンドポイントは、SIP シグナリングをトラバースするゾーンを介して、ICE 候補を他のエンドポイントに渡すことができます。その結果、エンドポイントは ICE プロトコルを使用して、メディアの最適なパスをネゴシエートします。最適なパスは、次のいずれかです。

- **ホストアドレス**—NAT デバイスの背後にあるエンドポイントのホスト IP アドレスを表します。
- **サーバー再帰アドレス**—NAT デバイス上のエンドポイントのパブリックにアクセス可能なアドレスを表します。
- **リレーアドレス**—TURN サーバーで構成されたエンドポイントのリレーアドレスを表します。

すべての ICE コールでは、最初にメディアが Cisco Expressway-E と Cisco Expressway-C を通過し、ネゴシエートされた ICE 候補タイプに応じてメディアパスを切り替えます。これにより、エンドポイントが ICE に対応していない場合でも、 Cisco Expressway は、従来のトラバーサルパスを使用して、中断することなくメディアを渡すことができます。

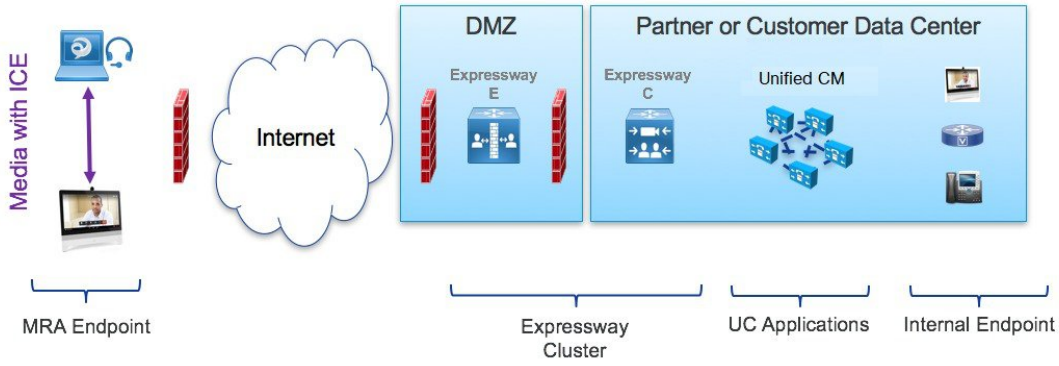
次のセクションでは、3 つの ICE 候補のそれぞれの MRA メディアパスを示します。

ホストアドレスを使用した ICE での MRA コールフロー

次の図は、メディアパスを確立するためにホストアドレスが使用される ICE を使用した MRA コールを示しています。エンドポイントは、ファイアウォールのない同じネットワーク内に存在するため、メディアはホストアドレスを使用してエンドポイント間を直接通過します。

ICE メディアパスの最適化

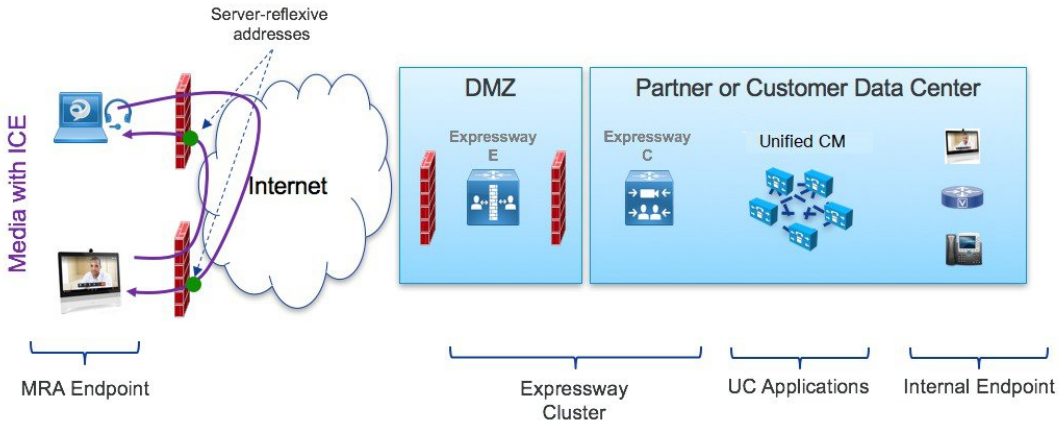
図 *16* : ホストアドレスを使用した *ICE* での *MRA* コールフロー



サーバー再帰アドレスを使用した ICE での MRA コールフロー

次の図は、両方のエンドポイントが異なるファイアウォールの背後にあるため、ホストアドレスが使用されないようになっている ICE を使用した MRA コールを示しています。代わりに、エンドポイントが異なるファイアウォールの背後にあるため、メディアはサーバー再帰アドレスを使用してエンドポイント間を通過します。

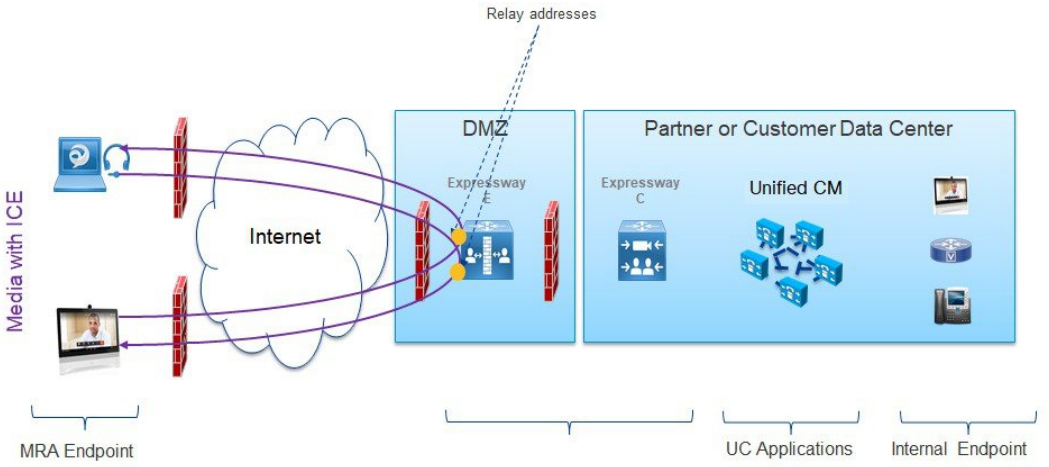
図 *17* : サーバー再帰アドレスを使用した *ICE* での *MRA* コールフロー



リレーアドレスを使用した ICE での MRA コールフロー

対称 NAT を使用した展開など、ホストとサーバー再帰アドレスが正常にネゴシエートできない場合、エンドポイントは ICE 最適化メディアパスとして TURN リレーを利用できます。次の図は、エンドポイントが Cisco Expressway TURN サーバーのリレーアドレスを使用してエンドポイント間でメディアを送信する、ICE を使用した MRA コールを示しています。

図 *18 :* リレーアドレスを使用した *ICE* での *MRA* コールフロー

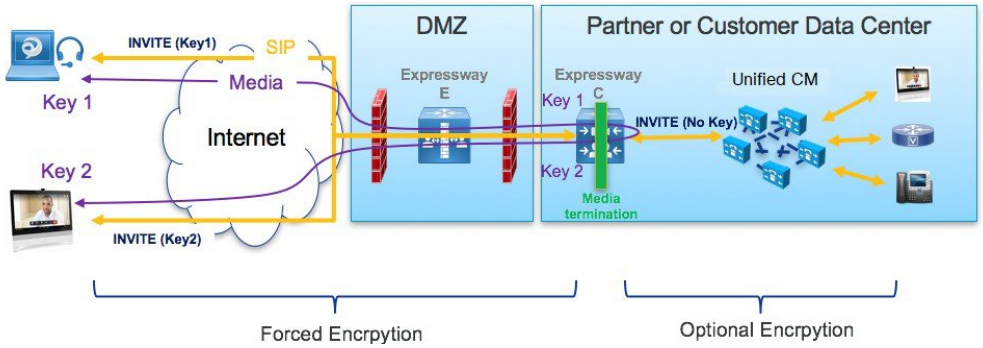


Expressway-C と Unified CM 間のシグナリングパスの暗号化

セキュリティと暗号化は、エンドポイント間の直接メッセージングを検討する際の重要な要素です。MRA エンドポイントはインターネット経由でシグナリングとメディアを送信しているため、暗号化モードでの動作が強制されます。通常の MRA モード（ICE なし）では、エンドポイントと Expressway-C の間では常に暗号化が必要ですが、Expressway-C と Unified CM の間ではオプションです。これが可能な理由は、内部レッグが暗号化されていない場合、Expressway-C がメディアストリームを終了してパケットを復号化できるためです。

次の図は、暗号化が MRA エンドポイントと Expressway-C の間で強制され、内部ネットワークではオプションである、ICE パススルーを使用しない暗号化を示しています。MRA コールでは、各レッグで異なる暗号化キー（キー 1 とキー 2）が交換され、Expressway-C は 2 つのレッグ間のメディアを復号化して再暗号化します。内部レッグが暗号化されていない場合、Unified CM への招待にキーは必要ありません。

図 *19 : ICE* パススルーを使用しない暗号化

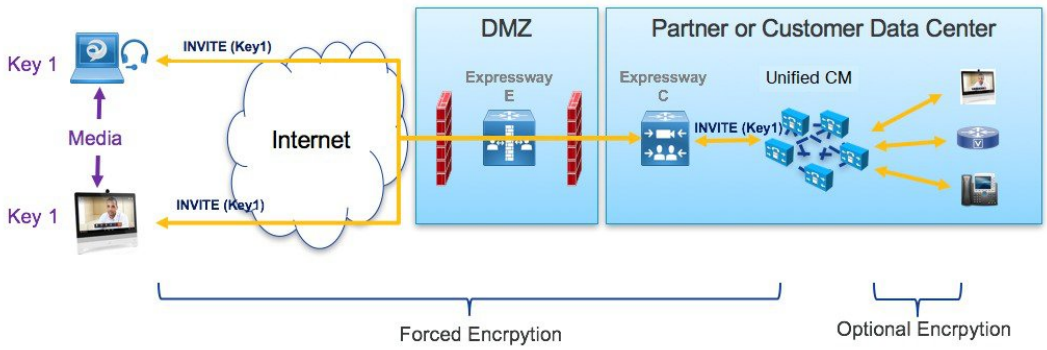


ただし、ICE パススルーモードでは、メディアパケットが Expressway-C 経由ではなく直接相互に送信されるため、エンドポイントはエンドツーエンドで暗号キーを交換できる必要があります。暗号キーが SIP メッセージに含まれる場合は常に、キーを保護するためにメッセージを

TLS 経由で送信する必要があります。暗号キーをエンドツーエンドで送信するには、SIP シグナリングパスをエンドツーエンドで暗号化する必要があるため、Expressway-C と Unified CM の間の内部レッグを暗号化する必要があります。シグナリングパスが暗号化されていない場合、暗号キーはコールセットアップ中にドロップされます。

次の図は、Expressway-C と Unified CM の間のシグナリングレッグも暗号化される ICE パススルーで必要な暗号化を示しています。

図 *20 : ICS* パススルーによる暗号化



サポートされるコンポーネント

Cisco Expressway ベースの展開

現在、ICE メディアパス最適化のサポートは MRA 展開にのみ存在します。次のサービス展開ではテストもサポートもされていません。

- Cisco Webex ハイブリッドサービス
- Jabber Guest
- Collaboration Meeting Room（CMR）クラウド
- ビジネス間コール

HCS 展開

ICE パススルーを使用して、次の HCS 展開タイプで MRA コールのメディアパスを最適化できます。

- HCS 共有アーキテクチャ
- HCS 専用サーバーと HCS 専用インスタンス
- お客様所有のコラボレーション アーキテクチャ

（注） HCS コンタクトセンターは ICE パススルーをサポートしていません。

サポートされるコンポーネント

ICE メディアパスの最適化は、次のコンポーネントでサポートされています。

- HCS 11.5 以降（HCS 展開用）
- Cisco Unified Communications Manager（Unified CM）11.5 以降
- Cisco Expressway-C および Cisco Expressway-E X12.5 以降

サポートされるエンドポイント

MRA に登録されていて、ICE メディアパスの最適化が有効になっている場合、次の ICE 対応エンドポイントは、メディアを相互に直接送信できます。

- Cisco Jabber クライアント、バージョン 12.5 以降、Unified Communications Manager 12.5 以降の使用が前提
- Cisco IP Conference Phone 7832、バージョン 12.5(1) 以降
- Cisco IP Phone 7800 シリーズ（MRA 互換モデルのみ）、バージョン 12.5(1) 以降
- Cisco IP Phone 8800 シリーズ（MRA 互換モデルのみ）、バージョン 12.5(1) 以降
- Cisco TelePresence DX、MX、SX シリーズ、CE バージョン 9.6.1 以降

ICE メディアパスの最適化の前提条件

ICE メディアパス最適化を使用して MRA エンドポイントを展開する場合、次の Cisco Unified Communications Manager の前提条件が存在します。

セキュアモードが Unified CM で実行されている必要がある

次のセキュアモードのいずれかが Cisco Unified Communications Manager で実行されていることが必須です。

- **SIP OAuth モード**は、それをサポートするエンドポイントに推奨されます。SIP OAuth モードは、以下に対してサポートされています。
  - Unified CM リリース 12.5(x) 以降の Cisco Jabber または Webex クライアント
  - Unified CM Release 14 以降の Cisco IP Phone 7800 または 8800 シリーズ
- ICE を使用して MRA 経由で SIP OAuth モードを展開していて、エンドポイントが SIP OAuth モードをサポートしていない場合は、**混合モード**を有効にする必要があります。こ

れには、サポートされていない Cisco IP Phone または TelePresence デバイスが含まれます。SIP OAuth モードを有効にしていない場合、または 12.5(x) 以前の Unified CM リリースを実行している場合は、Cisco Jabber クライアントにも混合モードが必要です。

混合モードを有効にするには、パブリッシャノードで `utils ctl set-cluster mixed-mode` CLI コマンドを実行します。

TLS 暗号化を含む電話セキュリティプロファイル

ICE メディアパス最適化を使用するすべての MRA エンドポイントは、TLS で暗号化された電話セキュリティプロファイルに関連付ける必要があります。電話セキュリティプロファイルには、次を設定する必要があります。

- **[デバイスセキュリティモード（Device Security Mode）]** を **[暗号化（Encrypted）]** にする
- **[転送タイプ（Transport Type）]** を **[TLS]** にする
- **[OAuth認証を有効化（Enable OAuth Authentication）]** をオンにする（SIP OAuth モードを使用している場合）—確認済み

さらに、Unified CM で混合モードが有効になっている場合、電話セキュリティプロファイル名は FQDN の形式である必要があります。

構成

SIP OAuth モードの構成方法については、「*Cisco Unified Communications Manager* 用構成ガイド」の「SIP OAuth モード」章を参照してください。

混合モードと TLS 暗号化電話セキュリティプロファイルの構成方法については、「*Cisco Unified Communications Manager* 用セキュリティガイド」を参照してください。

ICE メディアパス最適化のタスクフロー

次のタスクを実行して、MRA 展開用に ICE メディアパスの最適化を構成します。

手順

	コマンドまたはアクション	目的
ステップ 1	ICE 設定の構成 （72 ページ）	Unified CM で、MRA エンドポイントに適用できる ICE 設定を構成します。
ステップ 2	サーバー証明書のインストール （73 ページ）	Expressway-C で、適切なサーバー証明書と信頼できる CA 証明書をインストールします。
ステップ 3	CEtcp ネイバーゾーンを CEtls ネイバーゾーンに変更する （73 ページ）	Expressway-C で、既存の CEtcp ネイバーゾーンを CEtls ネイバーゾーンに変更します。

	コマンドまたはアクション	目的
ステップ 4	ICE パススルーサポート用 UC トラバーサルゾーンの設定 （74 ページ）	Expressway-C で、MRA の UC トラバーサルゾーンを設定します。
ステップ 5	ICE パススルーサポート用 UC ネイバーゾーンの設定 （74 ページ）	Expressway-C で、MRA の UC ネイバーゾーンを設定します。
ステップ 6	CLI を使用して Cisco Expressway ゾーンで ICE パススルーを構成する （75 ページ）	Expressway-C で、UC および CEtls ネイバーゾーンの ICE メディアパス最適化を設定します。
ステップ 7	Cisco Expressway-E を TURN サーバーとして設定 （75 ページ）	Expressway-E で、TURN リレーサービスを設定します。

ICE 設定の構成

Cisco Unified Communications Manager で、共通電話プロファイル内で ICE 設定を構成します。これは、プロファイルを使用する MRA 電話のグループに適用できます。

（注） 共通電話プロファイルを使用する代わりに、ICE設定は、製品固有の構成レイアウトの一部として、以下の [Unified CM] 設定画面のいずれかで適用できます。矛盾する構成が存在する場合、以下の優先順位によって、どの構成が電話機に適用されるかが決まります。

1. 電話機の構成—電話機ごとに ICE 設定を構成します。
2. 共通電話プロファイル—プロファイルを使用する電話機のグループに適用される ICE 設定を構成します。
3. 企業電話構成—これらの設定を使用する電話機にクラスタ全体に適用される ICE 設定を構成します。

使用する設定画面に関係なく、デフォルトでは ICE が**有効**になっており、**ホスト**がデフォルトの候補として使用され、サーバーの再帰アドレッシングも**有効**になっています。ただし、Expressway-E リレー TURN サービスを使用するには、これらのいずれかのウィンドウの ICE 設定で Expressway-E サーバーを指定する必要があります。

ステップ 1 Cisco Unified CM Administration で、**[デバイス（Device）] > [デバイス設定（Device Settings）] > [共有電話プロファイル（Common Phone Profile）]**の順に選択します。

ステップ 2 次のいずれかを実行します。

- 新しいプロファイルを作成するには、[新規追加（Add New）] をクリックします。
- **[検索（Find）]** をクリックし、既存のプロファイルを選択します。たとえば、デフォルトで新しい電話機に割り当てられるデフォルトの標準共通電話プロファイルなどです。

ステップ 3 **Interactive Connectivity Establishment（ICE）**で、次の ICE 設定を構成します。

- **ICE**—これが [有効（Enabled）] になっていることを確認します。
- **デフォルトの候補タイプ**ー**[ホスト（Host）]** が推奨値です。
- **サーバー再帰アドレス**—**[有効（Enabled）]** に設定されていることを確認します。
- **プライマリ TURN サーバーホスト名または IP アドレス**ーExpressway-E ノードの FQDN を入力して、プライマリ TURN サーバーとして機能させます。
- **セカンダリ TURN サーバーホスト名または IP アドレス**—Expressway-E ノードの FQDN を入力して、セカンダリ TURN サーバーとして機能させます。
- **TURN サーバー転送タイプ**—**[自動（Auto）]** が推奨値です。
- **TURN サーバーユーザー名**—Expressway-E サーバーにアクセスできるユーザー名を入力します。
- **TURN サーバーパスワード**—Expressway-E にアクセスするユーザーのパスワードを入力します。

ステップ 4 [保存（Save）] をクリックします。

ステップ 5 プロファイルを電話機に適用するには、次の手順を実行します。

a) **[デバイス（Device）]** > **[電話機（Phone）]** の順に選択します。
b) **[検索（Find）]** をクリックし、プロファイルを適用する電話機を選択します。
c) 作成する**共通電話プロファイル**を選択します。
d) [保存（Save）] をクリックします。

サーバー証明書のインストール

ここでは、サーバー証明書のインストール手順を説明します。

ステップ 1 サーバー証明書の新しい証明書署名要求を生成します（**[メンテナンス（Maintenance）]** > **[セキュリティ（Security）]** > **[サーバー証明書（Server Certificate）]**）。

詳細については、『Expressway 構成ガイド』ページの『*Cisco Expressway* 証明書作成と使用導入ガイド』を参照してください。

ステップ 2 証明書署名要求生成中、Subject Alternate Names（SAN）のエンドポイントに関連付ける電話機セキュリティプロファイルの名前を含めます。

詳細については、Expressway サーバーの証明書署名要求要件 （23 ページ）を参照してください。

ステップ 3 Cisco Expressway-C の信頼された証明機関から署名されたサーバー証明書をインストールします。

この証明書により、電話セキュリティ プロファイルを使用するエンドポイントは、 Cisco Expressway-C と Unified CM 間の TLS 接続を介して登録できます。

CEtcp ネイバーゾーンを CEtls ネイバーゾーンに変更する

Cisco Expressway-C で、MRA 用にすでに構成されている 既存の CEtcp ネイバーゾーンを CEtls ネイバーゾーンに変更します。

始める前に

Unified CM が次の有効になっている次のいずれかのモードでセキュアモードになっているかを確認します。

- 混合モード
- SIP OAuth モード

ステップ 1 **[構成（Configuration）] > [Unified Communications] > [Unified CMサーバー（Unified CM servers）]** の順に選択します。

ステップ 2 検出済みの Unified CM サーバーを選択し、**[サーバーを更新（Refresh Servers）]** をクリックして構成を更新します。

ステップ 3 Unified CM 状態が *TLS: Active* と表示されているかを確認します。

CEtcp ネイバーゾーンがまだ作成されていない場合は、Unified CM サーバーを追加してから、サーバーを更新する必要があります。「Unified CM クラスタの追加 （42 ページ）」に進みます。

Unified CM クラスタがセキュアモードの場合、Cisco Expressway-C は構成不可の CEtls ネイバーゾーンをそれ自体と検出した Unified CM ノードの間で自動生成します。詳細については、自動生成されたゾーンと検索ルール （43 ページ）を参照してください。

ICE パススルーサポート用 UC トラバーサルゾーンの設定

この手順では、ICE パススルーをサポートするために UC トラバーサルゾーンを設定する方法について説明します。

ステップ 1 Cisco Expressway-C で、**[構成（Configuration）] > [ゾーン（Zones）] > [ゾーン（Zones）]**の順に選択します。

ステップ 2 Cisco Expressway-E への Unified Communications ゾーンを選択します。

ステップ 3 SIP ペインで、**[ICEパススルーサポート（ICE Passthrough support）]** をオンに設定し、**[ICEサポート（ICE Support）]**をオフに設定します。

（注） ICE パススルーサポートは、ICE サポートより優先されます。ベスト プラクティスとして、ICE パススルー サポートをオンにして ICE サポートをオフにすることをお勧めします。

ICE パススルーサポート用 UC ネイバーゾーンの設定

この手順では、ICE パススルーをサポートするために UC ネイバーゾーンを設定する方法について説明します。

ステップ 1 Cisco Expressway-C で、**[構成（Configuration）] > [Unified Communications] > [Unified CMサーバー（Unified CM servers）]** の順に選択します。

ステップ 2 サーバを選択します。

ステップ 3 Unified CM サーバルックアップペインで**[ICEパススルーサポート（ICE Passthrough support）]** をオンにします。

CLI を使用して Cisco Expressway ゾーンで ICE パススルーを構成する

Cisco Expressway の ICE パススルーオプションは、ゾーンごとにセットアップします。各 Unified CM トラバーサル クライアント ゾーンおよび CEtls ネイバー ゾーンで ICE パススルーを有効にする必要があります。

Web インターフェイスの代わりに CLI を使用して、ICE パススルーのゾーンを構成できます。

ステップ 1 **[構成（Configuration）] > [ゾーン（Zones）]** の順に選択し、Cisco Expressway-E への Unified CM トラバーサルゾーンをクリックします。

ステップ 2 URL で、ゾーンの ID をメモします。たとえば、次の URL では、4 がゾーン ID です。

```
https://expressway.example.com/editzone?id=4
```

ステップ 3 CEtls ネイバーゾーンに対して手順 1 と 2 を繰り返します。

ステップ 4 管理者として Cisco Expressway-C の CLI にログインします。

ステップ 5 次のコマンドを実行して、Unified CM トラバーサル クライアント ゾーンで ICE パススルーを有効にします。

```
xConfiguration Zones Zone <Unified Communication Traversal client zone ID> TraversalClient SIP Media
 ICEPassThrough Support: On
```

ステップ 6 次のコマンドを実行して、CEtls ネイバーゾーンで ICE パススルーを有効にします。

```
xConfiguration Zones Zone <CEtls Neighbor zone ID> Neighbor SIP Media ICEPassThrough Support: On
```

Cisco Expressway-E を TURN サーバーとして設定

TURN サーバーが実行されている Cisco Expressway-E サーバーを使用して、リレーアドレスを検索し、サーバー再帰アドレスを取得できます。これは、通常 MRA に使用するクラスタの Cisco Expressway-E ですが、Cisco Expressway-E サーバーである必要はありません。準拠している TURN サーバーを使用できます。

次の手順は、Cisco Expressway-E TURN サーバーで必要な構成をまとめたものです。

ステップ 1 次の設定で TURN サーバー（**[構成（Configuration）] > [トラバーサル（Traversal）] > [TURN]**）を構成します

- **TURN サービス**：オンに設定。
- **TCP 443 TURN サービス**：オフに設定。
- **TURN ポート多重化**：オフに設定。このオプションは、大規模システムのみ利用できます。
- **TURN リクエストポート**：デフォルト値を使用。中小規模のシステムの場合、デフォルトポートは 3478 です。大規模システムの場合、デフォルトポート範囲は 3478 から 3483 です。

  （注） 大規模システムの **[TURNリクエストポート（TURN request port）]** フィールドは、**[TURN ポート多重化（TURN port multiplexing）]** がオンに設定されている場合のみ利用できます。

- **TURN リクエストポート範囲開始**：デフォルト値を使用。
- **TURNリクエストポート範囲終了**：デフォルト値を使用。

  （注） **TURN リクエストポート範囲開始**と **TURN リクエストポート範囲終了**オプションは、大規模システムの **[TURNポート多重化（TURN port multiplexing）]** がオフに設定されている場合のみ使用できます。

- **委任されたログインチェック**：デフォルト値を使用。
- **認証レルム**：デフォルト値を使用。デフォルト値は TANDBERG です。
- **メディアポート範囲開始**：デフォルト値を使用。デフォルト値は 24000 です。
- **メディアポート範囲終了**：デフォルト値を使用。デフォルト値は 29999 です。

ステップ 2 TURN クライアントが TURN サーバーで認証するためのログイン情報（**[構成（Configuration）] > [認証（Authentication）] > [デバイス（Device）] > [ローカルデータベース（Local database）]**）を構成します。

ステップ 3 [保存（Save）] をクリックします。

ステップ 4 TURN サーバーステータスが **[TURNサーバーステータス（TURN server status）]** で *[アクティブ（Active）]* に変更されたか確認します。

Cisco Expressway-E での TURN サービスの構成手順については、https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html の『*Cisco Expressway* 管理者ガイド』の「*TURN* サービスの構成」項を参照してください。

ICE パススルーメトリックの使用

このセクションでは、 Cisco Expressway で ICE パススルーのメトリックを使用する方法について説明します。

- Cisco Expressway-C で ICE パススルー メトリックを表示する
- collectd デーモンを使用してメトリクスを収集する
- 通話履歴で通話タイプを表示
- 帯域幅操作

Expressway-C で ICE パススルーメトリックを表示

Expressway-C では、完了した ICE パススルーコールのメトリックデータを表示できます。ICE パススルーコールをルーティングするように構成されているサーバーごとに、さまざまなメトリックを使用できます。値は 24 時間ごとに更新されます。

図 *21* : メトリクスの例

ICE Passthrough metrics

Metrics	
Peer	127.0.0.1
Start time	2018-10-22 20:43:45
End time	2018-10-23 20:43:45
B2BUA connected calls	4
Calls with optimized ICE media paths	2
% of calls with optimized ICE media paths	50%
Call types	
Host to host	100%
Host to server reflexive	0%
Host to relay	0%
Server reflexive to server reflexive	0%
Server reflexive to relay	0%
Relay to relay	0%
Advanced	
Calls with required Expressway ICE configuration	100%
Calls attempted with offered ICE candidates	100%
Calls with ICE candidates offered by one endpoint	0%
Calls without ICE candidates	0%
Calls with non-optimized media paths	50%
Calls with ICE candidates offered but without required Expressway ICE configuration	0%

- **[ピア（Peer）]** フィールドには、各ノードの IP アドレスまたはホスト名が表示されます。
- 最新の 24 時間間隔のデータが表示されます。
- 各ピアアドレスは、そのノードの履歴に移動するリンクです。
- 間隔の開始時刻は、最新のサーバー再起動の時刻を反映しています。
- 各列には、個別のクラスタの情報が表示されます。

ステップ 1 Expressway-C で、**[ステータス（Status）]** > **[ICEパススルーメトリック（ICE Passthrough metrics）]** の順に選択します。

このページは、これらのセクションで構成されています。

- **メトリクス**：各ピアのメトリクスが表示される時間間隔。この間隔で、B2BUA 接続されたコールの数、ICE コールの数、および B2BUA コールの合計に対する ICE の割合。N/A 値は、この 24 時間の間隔中に ICE コールが処理されなかった場合に発生します。
- **コールタイプ**：各コールタイプに対して、各コールタイプで発信された ICE コールの割合。
- **詳細**：トラブルシューティングに役立つその他のメトリック。

ステップ 2 フィールドの詳細な説明を表示するには、フィールド名の横にある **i** アイコンをクリックします。

ステップ 3 並べ替えるには、列名をクリックしてから、**上**矢印または**下**矢印をクリックして、その列でデータを並べ替えます。

ステップ 4 **[CSV にエクスポート（Export to CSV）]** をクリックして、表示しているページの値のスプレッドシートを作成します。

ステップ 5 クラスタの IP アドレスまたはホスト名をクリックして、そのクラスタの値の履歴を示す **[ICE コールメトリック履歴（ICE Call Metrics History）]** ページを表示します。

- 各列には個別のパラメータが表示されます。
- 各行には、異なる間隔の値が表示され、最新のものが最初に表示されます。
- 各値は、パーセンテージではなくローバリューです。
- このページには、最大 60 件のレコード（つまり、最新の 24 時間間隔で 60 件）を表示できます。

collectd デーモンを使用したメトリック収集

ICE パススルーコールのメトリックを表示する代わりに、*collectd* デーモンを使用してメトリックを収集できます。収集のためのサーバーのセットアップに関する詳細は、『Expressway の保持および運用ガイド』の『*Cisco Expressway* 有用性ガイド』の「「システム メトリック コレクションの導入」」項を参照してください。

通話履歴で通話タイプを表示

ICE パススルーコールの場合、コールタイプはコール履歴に表示されます。

ステップ 1 Cisco Expressway-C で、**[ステータス（Status）]** > **[コール（Calls）]** > **[履歴（History）]** の順に選択します。

ステップ 2 次のアクションのいずれかを選択します。

- **[開始時刻（Start Time）]** 列の値をクリックすると、通話詳細記録（CDR）が表示されます。

- **[アクション（Actions）]** 列でビューをクリックします。

ステップ 3 **[ICEパススルーコールタイプ（ICE Passthrough call type）]** フィールドの値を検証します。

次の値を使用できます。

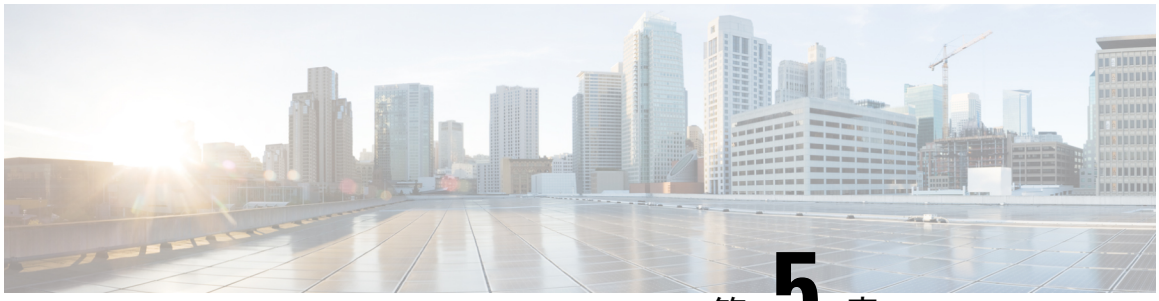
- *none*—最適化されたメディアパスがコールに使用されていないことを示します。 Cisco Expressway B2BUA を使用してコールが処理され、接続されます。
- *host_to_host*—コール用に最適化されたメディアパスが、エンドポイントのホストアドレスを使用して確立されたことを示します。
- *host_to_srvrflx*—コール用に最適化されたメディアパスがエンドポイントのいずれかのホストアドレスおよびサーバー再帰アドレスの間で確立されたことを示します。
- *host_to_relay*—コール用に最適化されたメディアパスが別のエンドポイントの TURN リレーアドレスの間で確立されたことを示します。
- *srvrflx_to_srvrflx*—コール用に最適化されたメディアパスがエンドポイントのサーバー再帰アドレスを使用して確立されたことを示します。
- *srvrflx_to_relay*—コール用に最適化されたメディアパスがエンドポイントのいずれかのサーバー再帰アドレスと別のエンドポイントの TURN リレーアドレスの間で確立されたことを示します。
- *relay_to_relay*—コール用に最適化されたメディアパスがエンドポイントのリレーアドレスを使用して確立されたことを示します。

ステップ 4 （任意） B2BUA コールレッグの詳細を確認するには、**[コールコンポーネント（Call components）]** セクションで、B2BUA タイプを表示されているコールレッグを選択します。

帯域幅操作

ICE がネゴシエートされると、メディアが Cisco Expressway に移動し、メディア帯域幅が減少します。**[状態（Status）]** > **[帯域幅（Bandwidth）]** > **[リンク（Links）]** ページに現在の帯域幅が表示されていて、ICE が使用されている場合、現在の使用量の合計は、より少ない使用率を表しています。

（注） 帯域幅の使用量には、TURN サーバーが使用する帯域幅は含まれません。



第 5 章

機能と追加構成

モバイルおよびリモートアクセスの基本設定が完了したら、この章を使用して MRA の機能とオプションの構成を構成します。

- 展開パーティション （81 ページ）
- MRA 経由のプッシュ構成 （83 ページ）
- ファストパス登録 （86 ページ）
- SIP パスヘッダーの有効化 （86 ページ）
- Unified CM と Expressway-C 間の SIP トランク （87 ページ）
- MRA 経由の BiB レコード （88 ページ）
- HTTP 許可リスト （90 ページ）
- MRA 経由の Dial via Office-Reverse （94 ページ）
- マルチクラスタのベストプラクティス （96 ページ）
- マルチドメインのベストプラクティス （99 ページ）
- セッションの永続性, on page 105

展開パーティション

展開は、ドメインと 1 つ以上の Unified Communications サービスプロバイダー (Unified CM、Cisco Unity Connection、IM and Presence Service ノードなど) を囲うために使用される抽象的な境界です展開を複数にする目的は、モバイルおよびリモートアクセス（MRA）ユーザーが使用できる Unified Communications サービスをパーティション化することです。よって、MRA ユーザーの異なるサブセットが同じ Expressway ペアを介してサービス一式にアクセスできます。

10 以上の展開はお勧めしません。

展開、関連ドメインおよびサービスは、Expressway-C で構成されます。

追加の展開を作成し、実装しない限り、1つのプライマリ展開（名前を変更しなければ「デフォルト展開」と呼ばれる）は、自動ですべてのドメインとサービスを自動包囲します。このプライマリ展開は、名前を変更してもメンバーがいなくても削除できません。

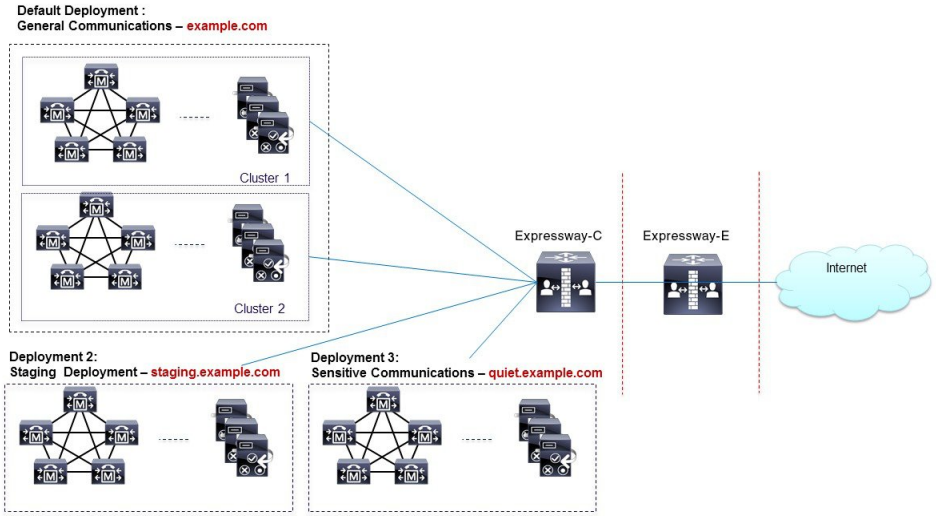
モバイルおよびリモートアクセスを介したサービスをパーティション化するには、必要な数の展開を作成します。それぞれに異なるドメインを関連付けたら、必要な Unified Communications リソースを各展開に関連付けます。

1 つのドメインを 1 つ以上の展開に関連付けることはできません。同様に、各 Unified Communications ノードには、1 つの展開のみ割り当てることができます。

例

2 つの Unified Communications インフラストラクチャを本運用 MRA 環境とステージング環境にそれぞれ実装するとします。この実装には、3 つ目のセットとして機密通信用の独立した環境も必要になる場合があります。

図 *22 :* ネットワーク外からアクセスする *Unified Communications* サービスをパーティション化する複数展開



UC サービスの展開パーティションの割り当て

複数の内部 UC クラスタがあり、境界を作成して内部 UC サービスを分割する場合は、このオプションの手順を使用します。これが役立つ例の 1 つは、企業 UC サービス用のクラスタと 2 つ目のステージングクラスタがある場合です。

（注） 新しい展開を作成しない場合、すべての内部 UC アプリケーションは、単一の企業全体のデフォルト展開に属します。

ステップ 1 Expressway-C で、展開を作成します。

a) **[設定（構成）]** > **[Unified Communications]** > **[展開（Deployments）]** の順に選択し、**[新規（New）]** をクリックします。

b) 新しい展開を作成します。
c) 追加する展開ごとに繰り返します。

ステップ 2 展開に UC ドメインを割り当てます。

a) **[構成（Configuration）]** > **[ドメイン（Domains）]** の順に選択します。
b) 割り当てるドメインを選択します。
c) このドメインに割り当てる**展開**を選択します。
d) **[保存（Save）]** をクリックします。
e) この手順をくりかえし、追加のドメインに展開を割り当てます。

ステップ 3 UC サービスを展開に割り当てます。

a) **[構成（Configuration）]** > **[Unified Communications]**の順に選択し、関連する UC アプリケーションを選択します。
b) 割り当てるサーバーを選択します。
c) **[展開（Deployment）]** フィールドで、割り当てる展開を選択します。
d) [保存（Save）] をクリックします。
e) 各 UC クラスタの各ノードにこれを繰り返します。

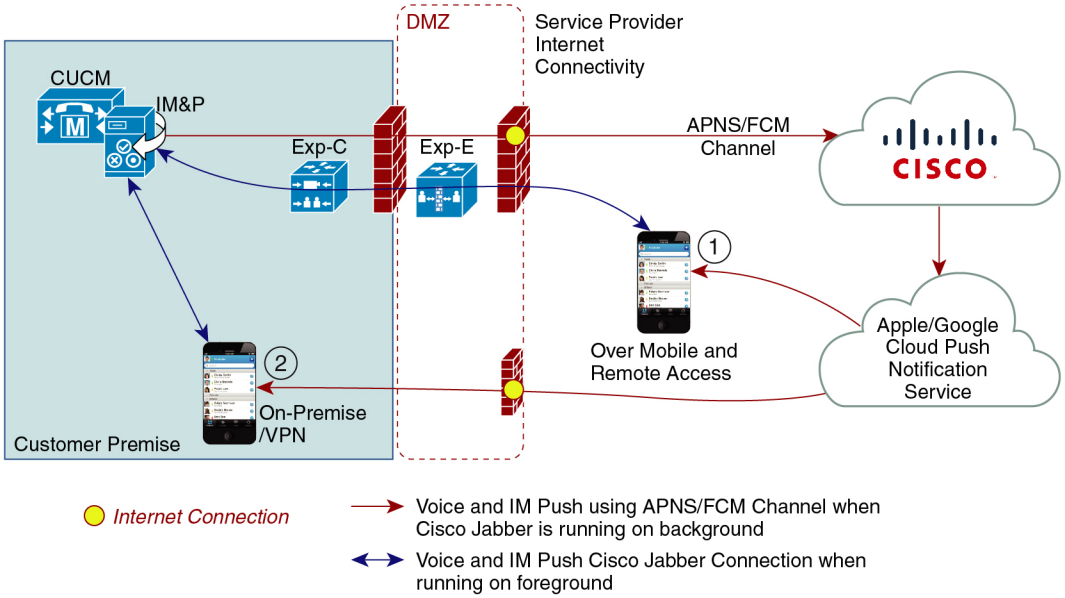
MRA 経由のプッシュ構成

MRA 展開に、iOS または Android デバイスで実行される Cisco Jabber または Webex クライアントが含まれている場合は、プッシュ構成を展開する必要があります。プッシュ構成がない場合、バックグラウンドモードに入ったクライアントにコールやメッセージを送信できない場合があります。

プッシュ構成の動作

クラスタでプッシュ構成が有効になっている場合、Cisco Unified Communications Manager と IM and Presence Service は、Apple または Google のいずれかのプッシュ構成サービスを使用してコールにプッシュ構成を、iOS または Android デバイスで実行する Cisco Jabber または Webex クライアントにメッセージを送信します。プッシュ構成を使用すると、システムがバックグラウンドモード（サスペンドモードとも呼ばれる）に入った後でも、クライアントと通信できます。プッシュ構成がない場合、バックグラウンドモードに入ったクライアントにコールやメッセージを送信できない場合があります。

起動時に、Android および iOS プラットフォームデバイスにインストールされているモバイルおよびリモートの Cisco Jabber または Cisco Webex クライアントは、Expressway-E を介して Cisco Unified Communications Manager および IM and Presence Service に登録されます。クライアントがフォアグラウンドモードのままである限り、新しいコールまたはメッセージを Expressway-E 経由でクライアントに送信できます。ただし、クライアントがバックグラウンドモードに移行すると、標準の通信チャネルは使用できなくなります。プッシュ構成は、該当するパートナークラウド（Apple または Google）を介してクライアントに到達するために大体チャネルを提供します。



プッシュ構成要件

Expressway-E が、Jabber iOS デバイス用にモバイルおよびリモートアクセス（MRA）をすでに提供している場合、プッシュ構成に対しては、Expressway での特定の構成は必要ありません。ただし、次の前提条件および推奨事項が適用されます。

- Expressway のプッシュ構成には、Apple クラウドの Cisco Jabber とプッシュ構成サーバー間でネットワークが必要です。

  インターネットに接続していないプライベートネットワークでは動作しません。

- Expressway は、すでに Jabber for iPhone/iPad に対してモバイルおよびリモートアクセスを提供しています。MRA は完全に構成されている必要があります（ドメイン、ゾーン、サーバ設定）。

- Unified CM 構成に応じて、プッシュ構成を Cisco コラボレーション クラウド に送信するためにフォワードプロキシが必要な場合があります。

- 自己記述トークン承認を使用することを推奨します。

- インスタントメッセージによるプッシュ構成には、Expressway-E の再起動が必要です。IM and Presence Service でプッシュ構成を有効化したら、Expressway-E を再起動する必要があります。再起動するまで、Expressway-E は、IM and Presence Service でプッシュ機能を認識できず、Jabber クライアントに PUSH メッセージを送信しません。

MRA のプッシュ構成の構成

MRA 経由でプッシュ構成を展開する場合は、次の要件があります。

- OAuth トークンの検証は、Expressway で構成する必要があります。
- Cisco Cloud サービスへの HTTPS 接続にフォワードプロキシ サーバーを使用するように Unified CM を構成する必要があります。

（注） Expressway の以前の組み込みフォワードプロキシは、X12.6.2 以降のバージョンの製品から削除されています。以前の Expressway バージョンでは、組み込みフォワードプロキシはサポートされていないため、使用しないでください。

詳細な手順については、『プッシュ構成導入ガイド』を参照してください。

Android デバイスでプッシュ構成を有効化

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。

MRA を介した Android 用の PUSH 対応 CLI コマンド： **xConfiguration XCP Config FcmService: On**

Note

- この操作は、Android ユーザー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。
- この機能を使用して、Expressway-E のみをオンにする必要があります。
- 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。

このテーブルは、Androidプッシュ構成用のExpressway CLI 対応/非対応コマンドを示しています。管理者は、CLI コマンドをオンにするかオフにするかを決定できます。

Table 11: ソリューションマトリックス

混合バージョンの IM&P クラスタ	Expressway X12.7 の FCM フラフの想定ステータス	コメント
12.5(1) SU2以降をの任意の 11.5(1) SU	オフ	Android プッシュ（FCM）はサポートされていません
11.5(1) SU8 以降または 12.5(1) SU2 以降と 12.5(1) SU3	オフ	Android プッシュ（FCM）はサポートされていません

混合バージョンの IM&P クラスタ	Expressway X12.7 の FCM フラフの想定ステータス	コメント
11.5(1) SU8 以降または 12.5(1) SU2 以降と 12.5(1) SU4 以降	オフ	12.5(1) SU4 以降のバージョンでサポートされている Android プッシュ（FCM）
11.5(1) SU9 以降または 12.5(1) SU4 以降と 12.5(1) SU3	ON	すべての 12.5(1) バージョンでサポートされている Android プッシュ（FCM）
11.5(1) SU9 以降と 12.5(1) SU4 以降	フラグは不要です （Expressway X12.7新しい検出メカニズムに完全に依存しています）	12.5(1) SU4 以降のバージョンでサポートされている Android プッシュ（FCM）

ファストパス登録

ファストパス登録の構成

ファストパス登録が有効な場合、Expresswayは、最初のルーティング計算をキャッシュしてから、事前にルーティングしたルートヘッダーを使用して、キャッシュされたルーティング結果を使用して後続のパケットをルートします。この機能は、サーバーのワークロードを削減し、キャパシティを増加させます。

Expressway-Eで、次のコマンドを使用して、ダイジェストキャッシュ間隔とダイジェストキャッシュライフタイムの両方を 7200 に設定します。

- `xConfiguration Authentication Remote Digest Cache ExpireCheckInterval：「7200」`
- `xConfiguration Authentication Remote Digest Cache Lifetime：「7200」`

SIP パスヘッダーの有効化

Expressway-C のデフォルト設定は、SIP REGISTER メッセージの Contact ヘッダーをリライトします。SIP Path ヘッダーを有効化すると、Expressway-C は Path ヘッダーにアドレスを追加しますが、Contactヘッダーには追加しません。この設定は、次のような一部の機能がMRAを介して動作するために必要です。

- 共有回線および複数回線
- BiB 通話録音

- サイレント モニタリング
- キー拡張モジュール

（注） 11.5(1)SU4 の最小の Unified CM リリースを展開することをお勧めします。詳細については、CSCvd84831 を参照してください。

ステップ 1 Expressway-C で、SIP Path ヘッダーをオンにする

a) Expressway-Cで、**[構成（Configuration）]** > **[Unified Communications]** > **[構成（Configuration）]**の順に選択します。
b) **[SIP Pathヘッダー（SIP Path headers）]** を **オン**にします。
c) [保存（Save）] をクリックします。

ステップ 2 設定を保存したら、Unified CM サーバーを更新します。

a) **[構成（Configuration）]** > **[Unified Communications]** > **[Unified CMサーバー（Unified CM servers）]** の順に選択します。
b) **[サーバーの更新（Refresh server）]** をクリックします。

Unified CM と Expressway-C 間の SIP トランク

モバイルおよびリモートアクセスの Expressway 展開では、Unified CM と Expressway-C 間の SIP トランク接続は必要ありません。 Expressway-C と検出された Unified CM ノードの間に自動生成されたネイバーゾーンは SIP トランクではないことに注意してください。

ただし、必要に応じて SIP トランクを構成することもできます。（たとえば、B2B 発信者または Expressway に登録されたエンドポイントを有効化して、Unified CM に登録されたエンドポイントにコールするなどが挙げられます。）

SIP トランクが構成されている場合、Unified CMUnified CM への SIP 回線登録に使用されるポートとは別のリスニング ポートを Unified CM で使用する必要があります。競合が起きると、Expressway-C でアラームが出ます。

SIP トランクで使用するポートは、Unified CM と Expressway の両方で構成されます。

SIP トランクの構成詳細については、『Cisco Expressway SIP トランクから Unified CM 導入ガイド』を参照してください。

SIP トランクに OAuth ベースの認証を設定する方法については、「UC アプリケーションで OAuth を構成する （55 ページ）」を参照してください。

トランク接続用の SIP ポートの構成

Expressway と Cisco Unified Communications Manager の間に SIP トランクを構成した場合は、この手順を使用して、トランクが使用するポート設定を構成します。

ステップ 1 Unified CM の回線登録リスニングポートの設定

a) Cisco Unified CM Administration で、**[システム（System）]** > **[Cisco Unified CM]** の順に選択します。
b) **[SIP 電話ポート（SIP Phone Port）]** を **5060** に設定します。
c) **[SIP 電話のセキュア ポート（SIP Phone Secure Port）]** を **5061** に設定します。
d) [保存（Save）] をクリックします。

ステップ 2 Unified CM のトランク リスニング ポートの設定

a) Cisco Unified CM Administration で、**[システム（System）]** > **[セキュリティ（Security）]** > **[SIPランクのセキュリティプロファイル（SIP Trunk Security Profile）]** の順に選択します。
b) **[検索（Find）]** をクリックして、SIP トランクに使用しているプロファイルを選択します。
c) **着信ポート**を回線ポートとは異なるように構成します。
d) **[保存（Save）]** をクリックして、**[構成を適用（Apply Config）]** をクリックします。

ステップ 3 Expressway で SIP トランクリスニング ポートを設定します。

a) Expressway-C で、**[構成（Configuration）]** > **[ゾーン（Zones）]** > **[ゾーン（Zones）]** の順に選択します。
b) SIP トランクに使用する Unified CM ネイバーゾーンを選択します。
c) **SIP ポート**を、SIP トランク セキュリティ プロファイルで構成された**着信ポート**と同じ値に設定します。
d) [保存（Save）] をクリックします。

MRA 経由の BiB レコード

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

提供内容の概要

- BiB を使用して、オフプレミスで作業しているユーザが発信または受信したコールの音声部分を録音できます。
- BiB は Expressway で常に有効になっています。
- BiB は Cisco Unified Communications Manager で設定できます。BiB が有効になっている場合、Unified CM は、エンドポイント間での発着コールをメディア録音サーバにフォークします。

帯域幅とキャパシティの要件

この機能を使用する場合は、帯域幅とコールキャパシティに大きな影響を与えることに注意してください。

- 追加のネットワーク帯域幅をプロビジョニングする必要があります。詳細については、「シスコ コラボレーション システム 12.x ソリューション リファレンス ネットワーク デザイン（SRND）」の「監視および録音用キャパシティプラン」項を参照してください。MRA エンドポイントに対して BiB を有効にするには、通常 2 倍の帯域幅が必要です。これは、コールの発信側と着信側の両方が録音されると仮定すると、BiB 対応の各コールが通常の 2 倍の帯域幅を消費するためです。
- MRA エンドポイントで BiB を有効にすると、Expressway ノードの全体的なコール キャパシティが元のキャパシティの約 3 分の 1 に減少します。これは、録音されている各通話に、それに関連付けられた 2 つの追加の SIP ダイアログがあるためです（したがって、本質的に 3 つの通話に相当します）。

設定要件

MRA を介して BiB Recording を展開するには、次のように構成します。

- BiB 録音を Cisco Unified Communications Manager で構成します。手順の詳細については、「*Cisco Unified Communications Manager* 向け機能構成ガイド」の「通話録音」章を参照してください。
- SIP パスヘッダーは、Expressway で有効にします。詳細については、SIP パスヘッダーの有効化 （86 ページ）を参照してください。

さらに、次の要件も満たす必要があります。

- 互換性のあるクライアントが必要です
  - Windows 版 Cisco Jabber 11.9
  - Mac 版 Cisco Jabber 11.9
  - iPhone および iPad 版 Cisco Jabber 11.9
  - Android 版 Cisco Jabber 11.9
  - MRA 対応の Cisco IP Phone 7800 シリーズ、Cisco IP Conference Phone 7832 または Cisco IP Phone 7800 シリーズ デバイス（これらすべての電話が MRA 対応であるとは限りません）
  - 現在 MRA に対応している電話に関しては、このガイドの「MRA インフラストラクチャ要件」項を参照するか、シスコ担当者にお問い合わせください。
- レジストラ/呼制御エージェント：Cisco Unified Communications Manager 11.5(1)SU3 BiB は、Expressway 登録エンドポイントではサポートされていません。
- エッジ トラバーサル：Expressway X8.11.1 以降

- レコーディング サーバ：このドキュメントの範囲外です。（Cisco Unified Communications Managerにおける録音の設定方法の詳細については、『*Cisco Unified Communications Manager* 機能設定ガイド』を参照してください。）

HTTP 許可リスト

HTTP 許可リストは、HTTP サービスのアクセスリストの一種です。Expressway-C は、インバウンドルールとアウトバウンドルールの両方を自動追加します。たとえば、Expressway は、MRA 構成中に検出されたUnified Communications ノードに外部クライアントがアクセスできるようにするインバウンドルールを自動追加します。これらには、Unified CM ノード（CallManager および TFTP サービスを実行する）、IM and Presence Service ノード、および Cisco Unity Connection ノードが含まれます。

ただし、場合によっては、特定のタイプのアクセスを許可するためにインバウンドルールを編集する必要があります。アウトバウンドルールは編集できません。

- インバウンドルールを表示するには、**[構成（Configuration）] > [Unified Communications] > [HTTP許可リスト（HTTP allow list）] > [自動インバウンドルール（Automatic inbound rules）]**の順に選択します。
- アウトバウンドルールを表示するには、**[構成（Configuration）] > [Unified Communications] > [HTTP許可リスト（HTTP allow list）] > [自動アウトバウンドルール（Automatic outbound rules）]**の順に選択します。

HTTP 許可リストの編集

リモートクライアントが企業内の他の Web サービスにアクセスする必要がある場合は、独自のインバウンドルールをHTTP許可リストに追加できます。たとえば、次のサービスでは許可リストの構成が必要になる場合があります。

- Jabber アップデート サーバ
- Cisco Extension Mobility
- ディレクトリ フォト ホスト
- マネージド ファイル転送
- Problem Report Tool サーバー
- ビジュアル ボイスメール

<link to Appendix and other places for more info>

HTTP 許可リストにアウトバウンドルールを追加することはできません。また、リストに自動追加されたルールを編集または削除することはできません。

（注） [マネージドファイル転送（Managed File Transfer）] 機能が Expressway 全体で機能するようにするには、手動または自動で追加されたかどうかにかかわらず、すべての Unified CM IM and Presence Service ノードが許可リストに表示されていることを確認してください。

自動インバウンドルール

Expressway は、Unified Communications ノードを検出または更新すると、HTTP 許可リストを自動編集します。このページには、検出されたノードと、それらのノードに適用されるルールが表示されます。

最初のリストは検出されたノードであり、この Expressway-C で現在認識されているすべてのノードが含まれています。各ノードのリストには、ノードのアドレス、タイプ、および発行元のアドレスが含まれています。

2 番目のリストは、さまざまなタイプの Unified Communications ノードへのクライアントアクセスを制御するために追加されたルールです。MRA 構成のノードのタイプごとに、このリストに 1 つ以上のルールが表示されます。編集可能なルールと同じ形式で表示されますが、これらのルールを変更することはできません。

表 *12 :* 自動追加された許可リストルールのプロパティ

列	説明
タイプ	このルールは、リストされているタイプのすべてのノードに影響します。 • Unified CM サーバー： Cisco Unified Communications Manager ノード • IM and Presence Service ノード： Cisco Unified Communications Manager IM and Presence Service ノード • Unity Connection サーバー：Cisco Unity Connection ノード • TFTP：TFTP ノード
[プロトコル（Protocol）]	クライアントがこれらのタイプのノードと通信することをルールが許可するプロトコル。
ポート	クライアントがこれらのタイプのノードと通信することをルールが許可するポート。
一致タイプ	*Exact* または *Prefix*。このルールを使用してクライアントがアクセスするサービスの性質に応じる。
パス	このルールを使用したクライアントがアクセスするリソースへのパス。ルールで *Prefix* 一致が許可されている場合、これは存在しないか、実際のリソースの部分一致のみである可能性があります。
仕組み	このルールが許可する HTTP メソッド（**GET** など）。

HTTP 許可リストの編集

ステップ 1 **[構成（Configuration）]** > **[Unified Communications]** > **[HTTP許可リスト（HTTP allow list）]** > **[編集可能なインバウンドルール（Editable inbound rules）]** の順に選択し、HTTP 許可リストルールを表示、作成、修正、削除します。

このページには 2 つの領域があります。1 つはデフォルトの HTTP メソッドを制御するためのもので、もう 1 つは編集可能なルールを表示するためのものです。

ステップ 2 （任意） チェックボックスを使用してデフォルトの HTTP メソッドのセットを変更し、**[保存（Save）]** をクリックします。

個々のルールを編集しているときに、デフォルトをオーバーライドできます。可能な限り安全にしたい場合は、デフォルトセットからすべてのメソッドをクリアし、ルールごとにメソッドを指定します。

デフォルトの方法を変更すると、以前にデフォルトの方法で作成したすべてのルールで新しいデフォルトが使用されます。

ステップ 3 [推奨]左側の列のチェックボックスをオンにし、**[削除（Delete）]** をクリックすると不要なルールを削除できます。

ステップ 4 **[新規（New）]** をクリックし、ルールを作成します。

ステップ 5 要件に合わせてルールを構成します。

ここでは、各フィールドに対するアドバイスをいくつか紹介します。

表 *13*：手動追加した許可リストルールのプロパティ

列	説明
説明	目的を認識しやすくするために、このルールの分かりやすい説明を入力します。
Url	MRA クライアントがアクセスできる URL を指定します。たとえば、**`http://www.example.com:8080/resource/path`** へのアクセスを許可するには、この URL をそのまま入力します。 • クライアントがホストにアクセスするために使用しているプロトコルは、http:// または https:// である必要があります。 • デフォルト以外のポートを使用する場合は、ポートを指定します（例：8080）。 （デフォルトポートは、80（http）と 443（https）です） • ルールの範囲を制限する（より安全な）パスを指定します（例：/resource/path）。 このルールで、**[プレフィックスの一致（Prefix match）]** を選択した場合、部分的なパスを使用するか、パスを省略できます。対象のリソースが不正な URL に対してレジリエンシがない場合、これはセキュリティリスクになる可能性があることに注意してください。

列	説明
許可された方式	**[デフォルトを使用（Use defaults）]** または **[方法を選択（Choose methods）]** を選択します。 このルールに特定の HTTP メソッドを選択すると、すべてのルールに対して選択したデフォルトがオーバーライドされます。
一致タイプ	**[完全一致（Exact match）]** または **[プレフィックス一致（Prefix match）]** を選択します。 ここでの判断は、環境によって異なります。[完全一致（Exact match）] を使用する方が安全ですが、より多くのルールが必要になる場合があります。[プレフィックス一致（Prefix match）] を使用する方が便利ですが、意図せずにサーバーリソースを公開するリスクがあります。
導入	MRA 環境で複数の展開を使用している場合は、新しいルールを使用する展開も選択する必要があります。複数の展開がない限り、このフィールドは表示されません。

ステップ 6 **[エントリの作成（Create Entry）]** をクリックしてルールを保存し、編集可能な許可リストに戻ります。

ステップ 7 （任意） ルールを変更するには、**[表示/編集（View/Edit）]** をクリックします。

ルールを HTTP 許可リストにアップロード

（注） アウトバウンドルールをアップロードすることはできません。

ステップ 1 **[構成（Configuration）]** > **[Unified Communications]** > **[HTTP許可リスト（HTTP allow list）]** > **[ルールをアップロード（Upload rules）]** の順に選択します。

ステップ 2 ルール定義を含む CSV ファイルを参照して選択します。

許可リストは、ファイルの参照を決定します （143 ページ）を参照してください。

ステップ 3 [アップロード（Upload）] をクリックします。

Expressway は成功メッセージで応答し、**[編集可能なインバウンドルール（Editable inbound rules）]** ページを表示します。

MRA 経由の Dial via Office-Reverse

モバイルワーカーは、オフィスで電話をかけるときと同じ高品質、セキュリティ、信頼性を必要としています。Dial via Office-Reverse（DVO-R）機能を有効にして、デュアルモードモバイル デバイスで Cisco Jabber を使用している場合は、そのことを保証できます。DVO-R は、企業を介して Cisco Jabber call を自動的にルーティングします。

DVO-R は、コールシグナリングと音声メディアを別々に処理します。Expressway でのモバイルおよびリモートアクセスのシグナリングを含むコールシグナリングは、クライアントと Cisco Unified Communications Manager 間の IP 接続を通過します。音声メディアは、企業の公衆電話交換網（PSTN）（PSTN）ゲートウェイのセルラーインターフェイスとヘアピンを通過します。オーディオをセルラーインターフェイスに移動すると、IP接続が失われた場合でも、高品質な通話とオーディオは安全に維持されます。

DVO-R を構成して、ユーザーが通話発信したときに、Cisco Unified Communications Manager からの折り返し通話が次のいずれかに送信されるようにすることができます。

- ユーザーのモバイル ID（携帯電話番号）。
- ユーザーの代替番号（ホテルの部屋など）。

DVO-R over MRA のコールフローの例

次のコールフローは、モバイル ID または代替番号のいずれかに折り返し通話を送信する場合の、MRA 通話経由の Dial via Office Reverse について説明します。コールフローの図については、後続の画像を参照してください。

1. 番号をダイヤルすると、信号が IP パス（WLAN またはモバイル ネットワーク）を介して Cisco Unified Communications Manager に送信されます。
2. Cisco Unified Communications Manager は、自分の携帯電話番号または設定した代替番号に電話をかけます。
3. 応答すると、Cisco Unified Communications Manager はダイヤルした番号に通話を転送し、呼び出し音が鳴ります。
4. その人が応答すると、進行中の通話は企業の PSTN ゲートウェイでヘアピンされ、次の処理が行われます。
    - モバイル ID を使用すると、通話は企業ゲートウェイに固定されます。通話は携帯電話とデスクフォンでアクティブであるため、この 2 つを切り替えることができます。
    - 代替番号を使用すると、進行中の通話は固定されず、デスクフォンには出られません。

図 *23* : モバイル *ID* を使用した *MRA* 経由の *DVO-R*

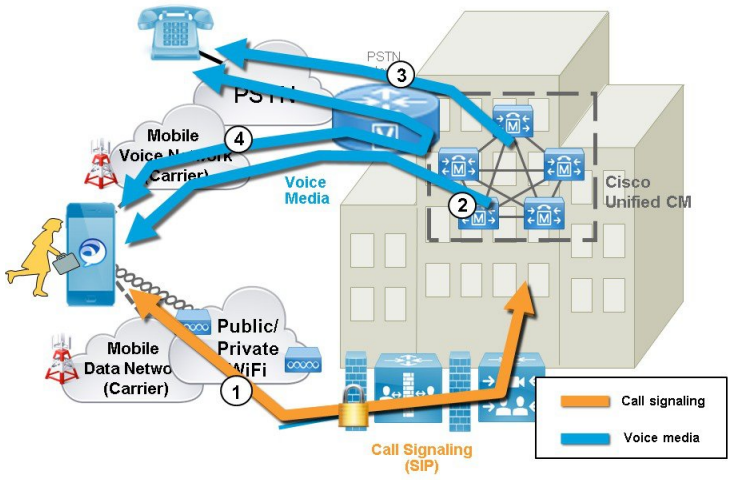
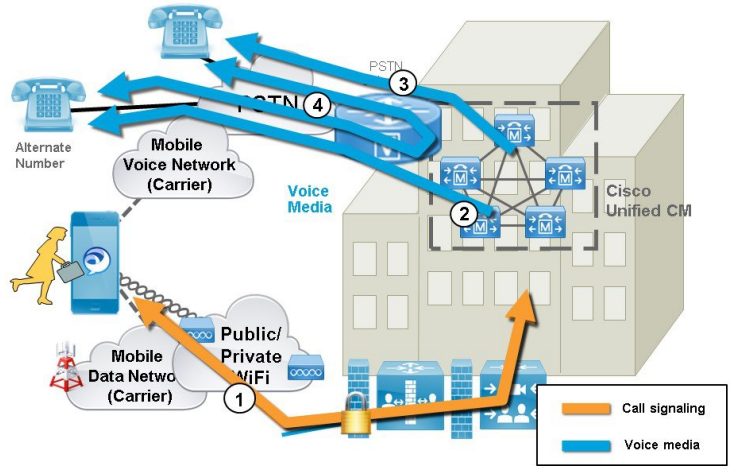


図 *24* : 代替番号を使用した *MRA* 経由の *DVO-R*



DVO の要件

この機能は、関連システムの次のバージョンで必要です。

- Cisco Unified Communications Manager 11.0(1) 以降
- Cisco Jabber 11.1 以降

補足事項

- PSTN ゲートウェイと Cisco Unified Communications Manager 間にアウトオブバンド DTMF リレーがある場合、アンカーされたコールで Dual Tone Multi Frequency（DTMF）ベースの通話中機能（例：保留は *81）を使用できます代替番号を使用している場合は、通話中機能を利用できません。

- Cisco Unified Communications Manager からのコールバックレッグがボイスメールにルーティングされるのを防ぎ、ダイヤルしている相手にボイスメールコールが届かないようにするには、DVO-R ボイスメール ポリシーを [ユーザ制御一（user controlled）] に設定することをお勧めします。これにより、通話を続行する前に、キーパッドのいずれかのキーを押して DTMF トーンを生成する必要があります。

MRA 経由の Dial via Office-Reverse の構成

DVO-R を MRA 上で機能させるための Expressway 構成要件はありません。ただし、Unified CM ノードと Cisco Jabber クライアントで必要な構成があります。ハイレベルでの構成は次のとおりです。

ステップ 1 DVO-R をサポートするように Cisco Unified Communications Manager を設定します。
ステップ 2 各デバイスに DVO-R を設定します。
ステップ 3 ユーザー制御によるボイスメールを無効に設定します。
ステップ 4 リモート接続先の追加（オプション）。
ステップ 5 Cisco Jabber クライアント設定を構成します。

（注） UC アプリケーションとクライアントを構成し、モバイルおよびリモートアクセスで Dial via Office-Reverse を機能させる方法について説明する詳細な構成例は、https://www.cisco.com/c/en/us/support/docs/unified-communications/expressway/200198-Configuring-Dial-via-Office-Reverse-to-W.html の 「モバイルおよびリモートアクセスで *Dial via Office-Reverse* を機能するよう構成する」を参照してください。

マルチクラスタのベストプラクティス

このセクションでは、マルチクラスタ MRA 展開を構成するためのヒントとベストプラクティスについて概説します。次に、マルチクラスタ MRA 展開を構成する際に留意すべきいくつかのベストプラクティスを示します。

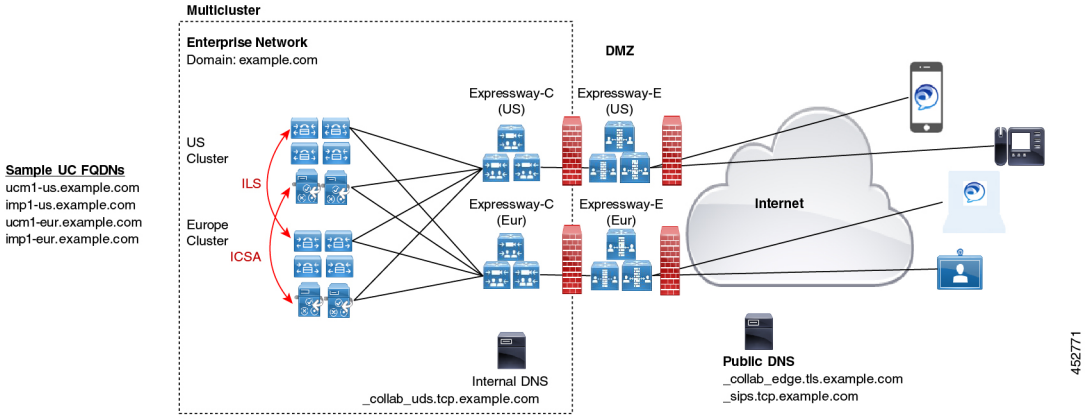
- すべての Expressway-C クラスタを、すべての UC クラスタに接続する必要があります。そうしないと、Expressway-C はすべての UC クラスタに要求をプロキシできません。各 Expressway-C クラスタのプライマリピアで、Expressway-C が到達する必要がある各 UC クラスタのパブリッシャ ノードを追加してから、サーバーを更新します。これにより、さまざまな UC クラスタからの残りのサブスクライバノードが Expressway-C に入力されます。
- 一部のクラスタが SIP ドメインを共有している場合：各ユーザーが特定のクラスタに割り当てられるように、各ユーザーの **[ホームクラスタ（Home Cluster）]** 設定を有効にする必要があります。この設定は、Cisco Unified Communications Manager の **[エンドユーザー構成（End User Configuration）]** ウィンドウに表示されます。

- 同じドメイン内に複数の Unified CM クラスタがある場合、特に大規模なクラスタ間ネットワークでは、クラスタ間検索サービス (ILS) が推奨されます。初期設定後、ILS は ILS ネットワーク全体で自動クラスタ検出とダイヤルプラン レプリケーションを提供します。ただし、クラスタ検出は手動で構成できるため、ILS は必須ではないことに注意してください。ILS の構成方法については、『*Cisco Unified Communications Manager* 向け システム構成ガイド』を参照してください。
- 同じドメイン内に複数の IM and Presence Service クラスタがある場合は、同じドメインにある IM and Presence クラスタの Intercluster Sync Agent（ICSA）を使用してクラスタ間ピアリングを構成する必要があります。クラスタ間ピアリングの構成方法については、『*IM and Presence Service* 向け構成およびアドミニストレーション ガイド』を参照してください。
- 複数の Edge クラスタがある場合は、それらの間で負荷分散を構成します
  - これらのエッジが同じデータセンターにある場合は、負荷分散にドメインネームシステム（DNS）SRV を使用できます。
  - エッジが地理的境界（異なる都市または大陸）にまたがって分割されている場合は、GeoDNS を使用できます。GeoDNS SRV レコードを使用してリクエストを適切なエッジサーバーにルーティングする方法の例については、以下を参照してください。

マルチクラスタの GeoDNS の例

GeoDNS over MRA は、クライアントが MRA に使用される Expressway から比較的離れている場合に、最も近い Expressway を提供するという特定の目的でサポートされます。これにより、待ち時間とネットワーク遅延を最小限に抑えることができます。

次の例は、複数の Unified CM クラスタに接続する 2 つの Expressway-C クラスタを使用したマルチクラスタ展開を示しています。この例では、単一のドメインを使用していますが、地理的に離れた 2 つの Expressway クラスタを使用しているため、2 つのエンタープライズエッジが提供されます。DNS プロバイダーによっては、GeoDNS を SRV または CNAME レコードに適用できます（SRV が使用可能な場合は優先されます）。以下は、2 つの Edge ドメイン（1 つはヨーロッパにあり、もう 1 つは米国にある Edge）がある場合に、GeoDNS を使用する方法の 2 つの例です。



ドメインネームシステム（DNS）プロバイダーがサポートしている場合、推奨される SRV アプローチは、ユーザーの場所（たとえば、米国またはヨーロッパ）に基づく優先度設定での SRV レコード作成です。SRV は、ユーザーの場所と、各エッジサーバーに割り当てられている優先度設定を使用して、要求の送信先のサーバーを決定します。その要求が失敗した場合、他のサーバーはバックアップオプションを提供します。

表 *14 : SRV* レコードの *GeoDNS*（推奨アプローチ）

SRV レコード	ユーザの場所	にルート...（優先）
`_collab-edge.tls.example.com` `_sips_tcp.example.com`	US	• `us-expc.example.com (10)` • `eur-expc.example.com (20)`
	ヨーロッパ	• `eur-expc.example.com (10)` • `us-expc.example.com (20)`

以下は、2 つの CNAME エイリアス（メインエイリアスと優先度の低いバックアップ CNAME）にルーティングする GeoDNS SRV 構成レコードの例です。各 CNAME レコードは、ユーザーの場所に基づいて異なるサーバーに通話をルーティングします。メイン CNAME に障害がある場合、バックアップ CNAME は通話を別のリージョンのサーバーに送信します（NA ユーザーはヨーロッパベースの Expressway にルーティングされます）。

表 *15 : CNAME* 経由の *GeoDNS* ルーティング

SRV レコード	CNAME へのルーティング（優先）	ユーザの場所	にルート...
_collab-edge.tls.example.com _sips_tcp.example.com	alias1.example.com (10)	US	us-expc.example.com
		ヨーロッパ	eur-expc.example.com
	backup-alias1.example.com (20)	US	eur-expc.example.com
		ヨーロッパ	us-expc.example.com

（注） SRV アプローチでは、SRV の重み設定をすべてのレコードで同じままにします。

（注） 発信者のロケーションに基づいて通話をルーティングできるように、Unified CM で地理ベースのコーリングサーチスペースとパーティションを設定する必要がある場合もあります。たとえば、地理ベースのコーリングサーチスペース（特定の都市の CSS）を作成し、その都市にあるすべての電話をその CSS 内に配置できます（1 つの CSS は「New_York_CSS」と呼ばれ、別の CSS は「Chicago_CSS」と呼ばれる場合があります)」）

詳細については、https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Collaboration/enterprise/12x/120/collbcvd/edge.html#pgfId-1081382 の「シスコ コラボレーション *12.x* 企業オンプレミス展開向け優先アーキテクチャ」に記載されている「コラボレーションエッジソリューションのスケーリング」を参照してください。

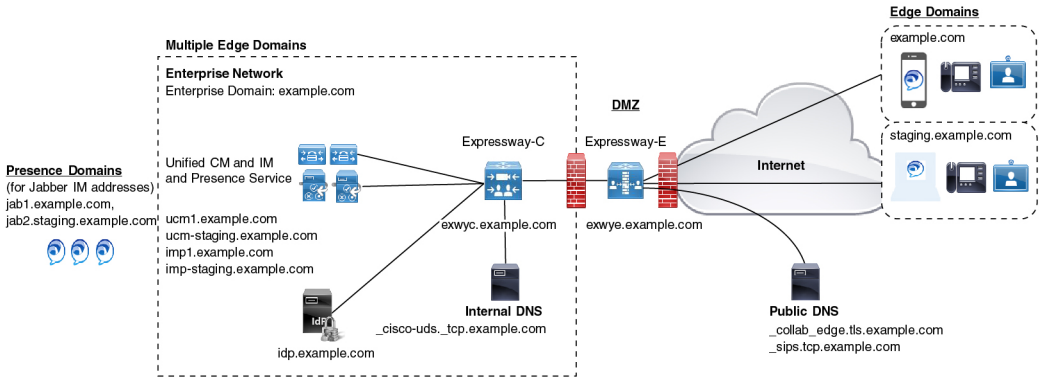
マルチドメインのベストプラクティス

このセクションでは、複数のドメインで MRA を展開するお客様向けに、ドメイン関連の情報と構成プロセスの概要を説明します。モバイルおよびリモートアクセスの理想的なシナリオは、すべてのコラボレーションアプリケーションとエンドポイントに対して単一ドメインを割り当てることですが、これがすべての場合に可能であるとは限りません。ネットワークによっては、マルチドメイン設定の複雑さのレベルが異なる場合があるため、ドメイン設定を使用できるさまざまなコンテキストを理解することが重要です。

複数エッジドメイン

次の図は、内部 UC ドメインが外部ドメインと異なる基本的なマルチドメインシナリオを示しています。

図 *25* : 複数エッジドメイン

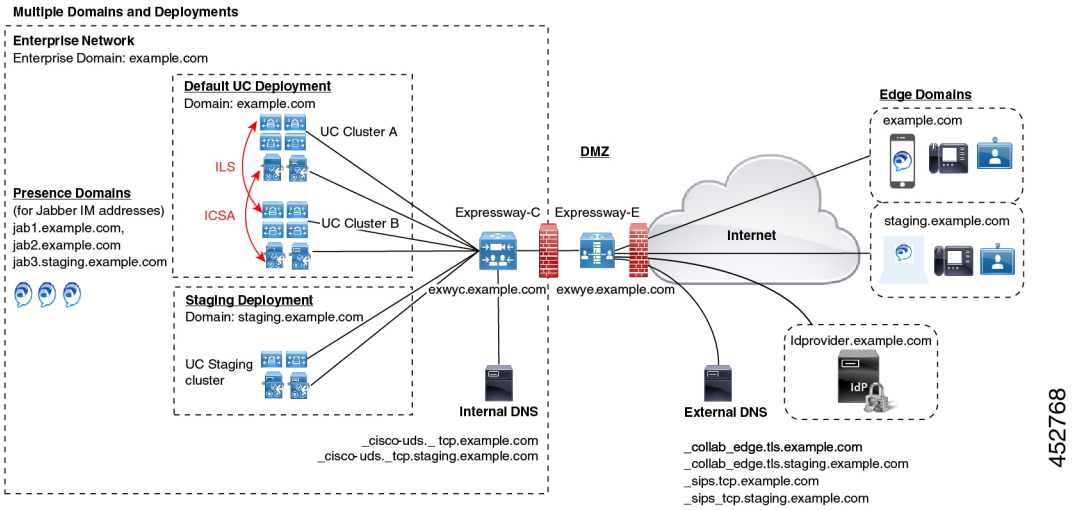


（注） MRA エンドポイントは、Expressway-E に到達できるように、外部パブリック ドメイン ネームシステム（DNS）サーバーに接続できる必要があります。

個別のデプロイメントを持つ複数のドメイン

次の例は、内部 UC 環境が 2 つの展開（デフォルトの UC 展開）に分割されている、より複雑なマルチドメインシナリオを示しています。これには、Expressway と 2 番目のステージング展開の両方を含む、メインの UC アプリケーションが含まれます。2 つの展開は、異なるドメインにあります。デフォルトの展開には、ILS と ICSA を使用して内部クラスタ間でデータを同期する複数の UC クラスタがあります。この例では、別の外部 IdP ドメインにあるクラウドベースの ID プロバイダーも使用しています。

図 *26* : 個別のデプロイメントを持つ複数のドメイン



ドメイン用語一覧

次の表は、MRA 展開内でドメイン用語を使用できるさまざまなコンテキストと、それらを Expressway で設定する方法を概説しています。展開によっては、これらすべてのコンテキストに同じドメインが適用される場合があります。

表 *16*：ドメイン用語一覧

用語	説明
エッジ ドメイン	この用語は、リモート MRA エンドポイントがオンプレミスの UC ネットワークに接続するリモートドメインを指します。これは、**[構成（Configuration）] > [ドメイン（Domain）]**メニューの Expressway-C で構成し、UC トラバーサルゾーンを経由して Expressway-E に通信されます。
Expressway サーバードメイン	Expressway-C と Expressway-E の場合、ドメインは各サーバーの FQDN アドレスの一部であり、それぞれのサーバーの **[システム（System）] > [ドメインネームシステム（DNS）（DNS）]** でプロビジョニングされます。各サーバーは、単一のドメインのみをサポートします。
内部 UC ドメイン	これは、Cisco Unified Communications Manager や IM and Presence Service などの内部 UC アプリケーションのドメインです。これらのアプリケーションは、Expressway と同じドメインにある場合もあれば、別のドメインにある場合もあります。 （注） 内部 UC アプリケーションが Expressway とは異なるドメインにある場合は、UC サーバーアドレスのサーバーアドレスとして FQDN または IP アドレスを使用する必要があります。FQDN が優先されます。
[プレゼンス（Presence）] [ドメイン（Domains）]	プレゼンスドメインは IM and Presence Service で設定され、クライアントの IM アドレスで使用される場合があります（たとえば、user@domain）。 （注） MRA クライアントの場合、プレゼンスドメインがエッジドメインと同じでない場合は、プレゼンスドメインを Expressway-C のドメインリストに追加します。 （注） MRA を介した複数のプレゼンスドメインは、IM and Presence Service、リリース 10.0(1) 以降を備えた Expressway X12.6.3 でサポートされます。ただし、1 回の展開内で 75 ドメインを超えないようにすることをお勧めします。
MRA アクティベーションドメイン	MRA エンドポイントのアクティベーションコード導入準備を使用している場合、MRA アクティベーションドメインは、クラウドの導入準備プロセス中に Unified CM で設定され、最初のデバイスアクティベーションのためにそのクラスタの MRA エンドポイントが接続する必要があるドメインを表します。各クラスタは、単一の MRA アクティベーションドメインのみを持つことができます。

用語	説明
MRA サービスドメイン	MRA エンドポイントのアクティベーションコード導入準備を使用している場合、MRA サービスドメインは Unified CM で設定され、エンドポイントが通常の MRA 使用のために接続するリモートエッジドメインを表します。複数の Expressway クラスタがある場合、MRA サービスドメインでは、通常の MRA 操作に使用する Expressway クラスタを指定できます。 MRA デバイスが MRA アクティベーションドメイン内でアクティブ化されたら、デバイスは、割り当てられた MRA サービスドメインへのリダイレクトを含む構成ファイルをダウンロードします。次に、デバイスはそのドメインの `_collab_edge` SRV を検索し、ドメインに割り当てられている Expressway クラスタを介して登録を試行します。 MRA サービスドメインは、クラスタ、デバイスプール、または個々のデバイスレベルでエンドポイントに適用できます。 （注） MRA アクティベーションドメインは、Unified CM クラスタで使用可能な MRA サービスドメインのリストに自動追加されます。

マルチドメイン構成の概要

次の表は、マルチドメイン MRA シナリオのドメイン固有タスクの構成概要を示しています。

（注） この概要は、基本的な MRA 展開を設定するための主要な構成フローを置き換えるものではありません。主要な構成フローに従うことで、複数のドメインで MRA をサポートするようにシステムを構成できます。ただし、複雑なマルチドメインシナリオの場合、この概要は、ドメイン設定が正しいことを確認するために使用するドメイン固有タスクの便利なチェックリストとして使用できます。

表 *17 : MRA* マルチドメイン構成の概要

手順	タスク
ステップ 1	Expressway サーバーのホスト名とドメイン名を構成します。 Expressway サーバーアドレスの設定 （39 ページ）を参照してください。

手順	タスク
ステップ 2	Expressway-C で、Unified CM にルートする MRA 登録、呼制御、プロビジョニング、メッセージングおよびプレゼンスサービスに対してドメインを追加します。次も含まれます。 • 内部 UC ドメイン • エッジドメイン（内部ドメインと異なる場合） • プレゼンスドメイン（他のドメインと異なる場合） ドメインの追加 （41 ページ）を参照してください。
ステップ 3	(オプション)。展開を内部 UC アプリケーションに割り当てます。このオプション設定により、内部 UC サービスをパーティション化できます。たとえば、この構成を使用して、メインの本運用クラスタを別のステージングクラスタから切り離すことができます。 UC サービスの展開パーティションの割り当て （82 ページ）を参照してください。
ステップ 4	内部 DNS エントリの構成方法 1. `_cisco-uds._tcp.<domain>` SRV レコードを各 Unified CM ドメインに構成します。 2. Unified CM および IM and Presence ノードに対して正引きおよび reverse ルックアップを作成します。 3. Expressway-C を Expressway-E に向ける A および PTR レコードを設定します。 （注） X12.6 の時点で、MRA エンドポイントが正しい UC クラスタに到達できるようにするために、`_cisco_uds.tcp.example.com` 内部 SRV レコードは必須ではなくなりました。ただし、オンプレミスの Cisco Jabber および Webex クライアントを展開している場合は、この SRV レコードが引き続き必要であることに注意してください。 ローカルドメインネームシステム（DNS）（内部ドメイン） （16 ページ）を参照してください。

手順	タスク
ステップ 5	パブリック ドメインネームシステム（DNS） の構成方法 1. Expressway-E で、エッジドメインに対して `_collab-edge._tls.<domain>` および `_sips_tcp.<domain>` ドメインネームシステム（DNS）SRV レコードを構成します。 2. Expressway-E ホスト名を Expressway-E のパブリック IP アドレスにポイントする A レコードを設定します。 （注） MRA エンドポイントは、Expressway-E に到達できるように、パブリック ドメインネームシステム（DNS）サーバーへの接続が必要です。 パブリック ドメインネームシステム（DNS）（外部ドメイン） （16 ページ）を参照してください。 警告 Expressway-E の完全修飾ドメイン名（FQDN）は、SRV A レコードと一致して、MRA エンドポイントとパブリック ドメインネームシステム（DNS）サーバー間の接続を確立して、それらが Expressway-E に到達できるようにする必要があります。
ステップ 6	Expressway-E 証明書を設定します。Expressway-E 証明書に各 Unified CM 登録ドメインが含まれていることを確認してください。 詳細については、証明書の要件 （21 ページ）を参照してください。
ステップ 7	SAML SSO を展開している場合は、適切なドメインをアイデンティティプロバイダーに関連付けます。 IdP とドメインの関連付け （60 ページ）を参照してください。
ステップ 8	デバイス アクティベーションコードを使用して MRA クライアントをプロビジョニングする場合は、MRA導入準備のために Unified CM でクラスタ全体の MRA アクティベーション ドメインをプロビジョニングします。 さらに、デバイスがアクティブ化された後にユーザーが使用できるようにするエッジドメインを持つ MRA サービスドメインをプロビジョニングします。 MRA デバイス導入準備の構成フロー （111 ページ）を参照してください。

（オプション）SRV を使用して Expressway-E のエイリアス FQDN を作成する

複数のエッジドメインがある場合のオプションのアプローチは、SRV レコードを使用して、複数の Expressway-E FQDN をシミュレートする Expressway-E のエイリアスドメインを作成することです。たとえば、example.com に Expressway-E サーバーがあり、example.com と staging.com の 2 つのエッジドメインがある場合

- エッジドメインごとに、エッジドメインの一部であるかのように Expressway-E FQDN アドレスを指す _collab_edge SRV を構成します（例：expe.example.com を指す SRV や expe.staging.com を指す別の SRV）。

- FQDN ごとに、Expressway-E のパブリック IP アドレスを指す A レコードを設定します。

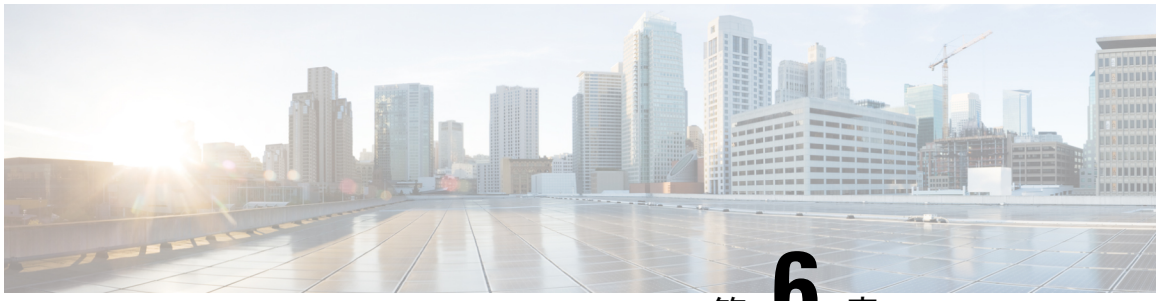
セッションの永続性

セッション持続性により、ローミング中のユーザーエクスペリエンスが向上し、Webex アプリで次のことができるようになります。

- ネットワーク内の異なるアクセスポイント間をローミングします。
- 再登録することなく、異なるネットワーク（Wi-Fi、VPN over 3G/4G など）間をローミングできます。
- 異なるネットワーク間をローミングしている間、SIP ベースのサブスクリプション ステータスを維持します。
- ネットワーク接続が失われた場合に備えて登録を維持します。
- アクティブな通話と保留中の通話の両方を、通話が途切れることなく、あるネットワークから別のネットワークにシームレスに転送します。

ネットワーク間のローミング中の接続を容易にするために、セッション持続性では、キープアライブ登録による動的な IP アドレス/ポートの変更が可能です。さらに、この機能には構成可能な TCP 再接続タイマーが含まれており、これは製品レベルで有効にする必要があり、一時的なネットワーク接続の切断またはローミングの場合に Webex アプリクライアントが接続を維持できるようにする必要があります。タイマーは、クライアントが元の TCP 接続を明示的に切断した場合にのみ有効です。セッション持続性機能を利用するには、シスコ定義の SIP インターフェイスに準拠する必要があります。

たとえば、オフィス内で Webex アプリクライアントで通話中に、Wi-Fi 接続を失って建物の外に出た場合、クライアントが Expressway 経由でモバイルおよびリモートアクセスに切り替えると、通話は続行されます。同様に、クライアントが Expressway 経由でモバイルおよびリモートアクセスからオフィスの Wi-Fi ネットワークに切り替えても、通話が切断されることはありません。



第 6 章

MRA デバイスの導入準備

- アクティベーションコードによる MRA デバイスの導入準備 （107 ページ）
- デバイスの導入準備の前提条件 （109 ページ）
- MRA デバイス導入準備の構成フロー （111 ページ）
- 電話機のアクティブ化 （114 ページ）
- 安全な導入準備のための追加オプション （115 ページ）

アクティベーションコードによるMRAデバイスの導入準備

アクティベーションコードは、モバイルおよびリモートアクセス（MRA）用のリモートエンドポイントの導入準備をするためのシンプルで安全な方法を提供します。この機能により、MRAユーザーが初めて電話を使用するときにオンプレミスにいる必要がなくなります。リモートユーザーは、電話を接続し、アクティベーションコードを入力すると、通話を開始できます。

この機能は、導入準備に対応するため、Cisco Cloud を活用します。管理者は Cisco Unified Communications Manager をクラウドに導入し、デバイスアクティベーション中にすべてのリモート MRA ユーザーが接続する Expressway クラスタでクラスタ全体の MRA アクティベーションドメインを指定します。

複数の Expressway クラスタがある場合、MRA サービスドメインを使用すると、電話機が登録する Expressway を指定できます。電話機がアクティブ化されると、電話機は構成ファイルをダウンロードします。このファイルには、その電話機に割り当てられている Expressway クラスタを持つ MRA サービスドメインへのリダイレクトが含まれています。

アクティベーションコードとは何ですか。

アクティベーションコードは、1 回だけ使用できる 16 桁の値であり、電話機を登録する前にユーザーが電話機に入力する必要があります。ユーザーは正しいコードを入力する必要があります。入力しないと、電話が登録されません。アクティベーションコードは、電話機を安全に導入するメソッドであり、管理者が手動で個々の電話機の MAC アドレスを収集して入力する必要がありません。

カスタム証明書（オプション）

独自の証明書を使用する場合は、クラウドを使用して証明書をMRA電話機に配布し、Expresswayとの信頼を確立できるようにします。このオプションでは、証明書を最初にExpresswayにアップロードしてから、Cisco Unified Communications Manager の **PhoneEdge-trust** ストアにアップロードする必要があります。証明書は Cisco Cloud にアップロードされるため、デバイスのアクティベーションプロセス中に電話機が証明書をダウンロードできます。

MRA 導入準備プロセスフロー

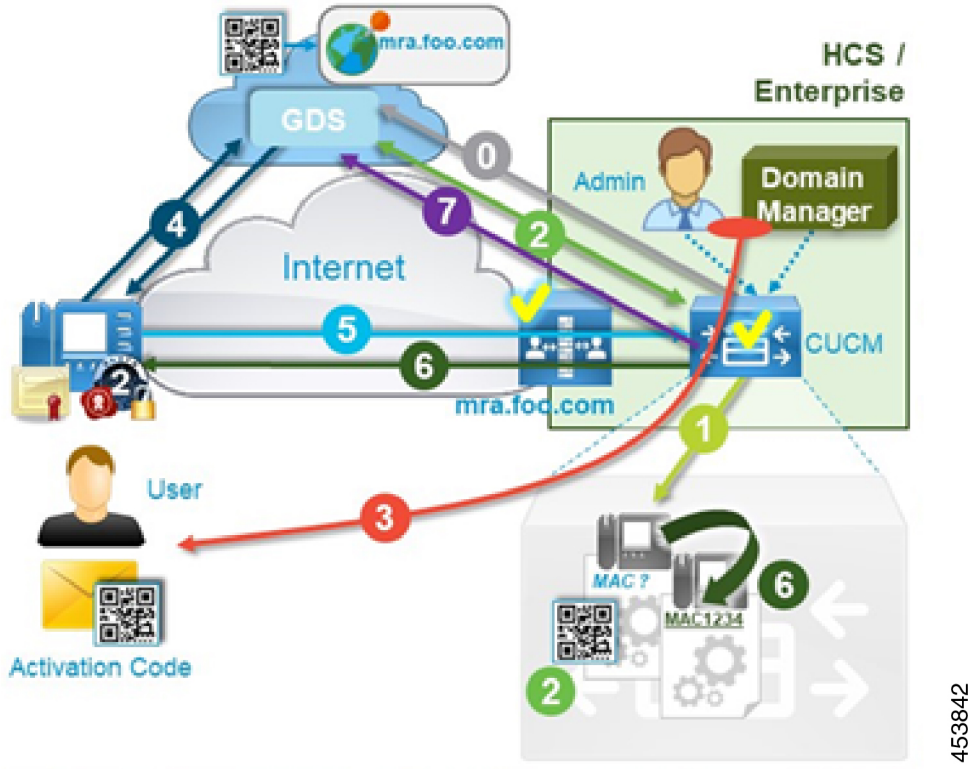
次の表には、MRAモードでのデバイスアクティベーションコード導入準備による新しいMRA電話の導入準備のプロセスフローが含まれています。プロセスの図については、番号の付いた各手順を後続の図と一致させてください。

（注） UCM パブリッシャでデバイス アクティベーション サービスを開始して、モバイルおよびリモートアクセス経由でクライアントの導入準備をする場合は、UDSおよびCCMサービスも開始する必要があります。サーバーが更新されない場合は、Expressway-C の Unified Communications 構成の UCM クラスタを削除または再検出します。

プロセス手順	プロセスの流れ
0	管理者は Cloud 導入準備を構成し、MRA アクティベーションドメインと MRA サービスドメインを指定します。
1	管理者は、MAC アドレスを指定せずに完全なデバイス構成をプロビジョニングします。デバイス名は、ランダムな BAT MAC アドレスになります。
2	管理者が、このデバイスのアクティベーション コードを要求します。デバイスアクティベーションサービスは、クラウドベースのデバイスアクティベーションサービスからコードを要求します。
3	アクティベーションコードがユーザーに送信されます（E メールまたはセルフケア ポータル経由）。
4	ユーザーがアクティベーションコードを入力します。電話機はクラウドからMRAターゲットを取得します。
5	電話機はExpresswayの場所を学習し、SRPハンドシェイクでMIC+アクティベーションコードを使用して認証します。
6	デバイス アクティベーション サービスが電話機の MAC を使用してデータベース内のデバイス構成を更新し、成功したことを電話機に送信します。

プロセス手順	プロセスの流れ
7	電話機が登録され、その電話機の TFTP からの固有構成ファイルを取得し、Unified CM に登録されます。電話機が別の MRA サービスドメインに割り当てられている場合、構成ファイルにリダイレクトされます。その後、電話機は MRA サービスドメインを使用して登録できます。
8	デバイスアクティベーションサービスは、クラウドからアクティベーションコードをリリースします。コードは今後再利用できます。

図 *27* : アクティベーションコードによる *MRA* デバイス導入準備プロセス



デバイスの導入準備の前提条件

次の表に、MRA エンドポイントのアクティベーションコード導入準備のサポート情報を示します。

表 *18 : MRA* アクティベーションコード導入準備サポート情報

サポート	詳細
最小リリーズ	Expressway X12.5.1 Cisco Unified Communications Manager 12.5(1)SU1 Cisco IP Phone ファームウェア 12.5(1)SR3
サポートされるエンドポイント	Cisco IP Phones 7811、7821、7832、7841、7861、8811、8832、8832NR、8841、8845、8851、8851NR、8861、8865、8865NR

（注） リリースX14.0の時点で、モバイルおよびリモートアクセス用にサポートされているCisco IP Phone 78xx シリーズおよび88xx シリーズを導入準備している場合、 電話は、**Cisco Unified Communications Manager** の **[電話構成（Phone Configuration）]** ウィンドウで **[MRAを介したアクティベーションコードを許可（Allow Activation Code via MRA）]** チェックボックスがオンになっている場合のみ、MRA モードに切り替えられます。

このアプローチを使用して、MRA 電話のアクティベーションコード導入準備を設定する必要があります。さらに、MRA 電話のユーザーは、電話機をアクティブにして使用するために正しいアクティベーションコードを入力する必要があります。

アクティベーションコードの導入準備についての詳細は、『*Cisco Unified Communications Manager* 向け機能構成ガイド』の「「アクティベーションコードを介したデバイスの導入準備」」章を参照してください。

さらに、次の前提条件があります。

- X12.5 より前のリリースから Expressway をアップグレードした場合は、この機能を設定する前に Expressway-C の Unified CM サーバーを更新してください。Expressway-C で、**[構成（Configuration）]** > **[Unified Communications]** > **[Unified CMサーバー（Unified CM servers）]** の順に選択し、**[サーバーを更新（Refresh servers）]** をクリックします。
- **Cisco デバイス アクティベーション サービス**—このサービスは、Cisco Unified Communications Manager で実行する必要があります（サービスはデフォルトで実行されます）。Cisco Unified Serviceability のサービスのリストをチェックして、サービスが実行されていることを確認します。
- **OAuth リフレッシュ ログイン**—この機能は、**OAuth Refresh Login Flow** 企業パラメータを **[有効（Enabled）]** に設定し、Cisco Unified Communications Manager で有効にします。
- **セルフケアポータル**—ユーザーがセルフケアポータルを使用して、電話をアクティブ化させる場合に使用します。
  - **Show Phones Ready to Activate** 企業パラメータは、Cisco Unified Communications Manager で **[True]** に設定します。

- エンドユーザーはポータルへのログインアクセスが必要です。セルフケア構成詳細の「*Cisco Unified Communications Manager* 用機能構成ガイド」の「セルフケアポータル」章を参照してください。
- セルフケアポータルは、MRA ではサポートされていないので、リモートユーザーは、VPN を使用してポータルにアクセスする必要があります。

- **ドメインネームシステム（DNS）SRV レコード**—MRA アクティベーション ドメインと MRA サービスドメインの場合、適切な Expressway クラスタを指す *_collab_edge* SRV を構成する必要があります。

MRA デバイス導入準備の構成フロー

以下の手順に従って、MRA モードでアクティベーションコードを使用して MRA デバイスの導入準備を構成します。

手順	手順
ステップ 1	Cisco Unified Communications Manager および Expressway で OAuth 認証を有効にします。 **1.** Cisco Unified Communications Manager で OAuth を有効にする方法 **1.** Cisco Unified CM Administrationで、**[システム（System）]** > **[企業パラメータ（Enterprise Parameters）]**の順に選択します。 **2.** **OAuth Refresh Login Flow**パラメータを **[有効（Enabled）]** に設定します。 **3.** [保存（Save）] をクリックします。 **2.** Expressway で OAuth 更新認証を有効にする方法 **1.** **[構成（Configuration）]** > **[Unified Communications]** > **[構成（Configuration）]** > **[MRAアクセス制御（MRA Access Control）]**の順に選択します。 **2.** **[OAuth トークンによる承認（更新あり）（Authorize by OAuth token with refresh）]** を **オン**にします。 **3.** **[保存（Save）]** をクリックします。

手順	手順
ステップ2	MRA アクティベーションコードの導入準備のために、Cisco Unified Communications Manager をクラウドに導入準備します。 **1.** Cisco Unified CM の管理から、**[詳細機能（Advanced Features）]** > **[Cisco Cloud 導入準備（Cisco Cloud Onboarding）]** を選択します。 **2.** **[バウチャーを生成（Generate Voucher）]** ボタンをクリックします。 **3.** **[Cisco Cloudでアクティベーションコードの導入準備を有効化（Enable Activation Code Onboarding with Cisco Cloud）]** チェックボックスをオンにします。 **4.** **MRA アクティベーションドメイン** を指定します。 **5.** [保存（Save）] をクリックします。 （注） • MRA アクティベーションドメインの Collab-edge ドメインネームシステム（DNS）レコードが存在する必要があります。 • クラスタごとに 1 つの MRA アクティベーションドメインの制限があります。MRA アクティベーションは、MRA サービスドメインのリストに自動的に追加されます。
ステップ3	MRA サービスドメインを設定します。 **1.** Cisco Unified CM Administrationで、**[高度な機能（Advanced Features）]** > **[MRA サービスドメイン（MRA Service Domains）]**の順に選択します。 **2.** 複数の Expressway クラスタがある場合は、MRA エンドポイントが動作する各ドメインを追加します。 **3.** ドメインをクラスタ全体のデフォルト MRA サービスドメインとして適用する場合は、**[IsDefault]** チェックボックスをオンにします。 **4.** [保存（Save）] をクリックします。
ステップ4	オプション。MRA サービスドメインを既存のデバイスプールに割り当てます。これにより、デバイスプールを使用するすべての MRA デバイスに特定の Expressway クラスタを割り当てることができます。 **1.** Cisco Unified CM Administration で、**[システム（System）]** > **[デバイスプール（Device Pool）]**の順に選択します。 **2.** **[検索（Search）]** をクリックして、適切なデバイスプールを選択します。 **3.** **[MRAサービスドメイン（MRA Service Domain）]**ドロップダウンから、このデバイスプールを使用するデバイスに割り当てるドメインを選択します。 **4.** [保存（Save）] をクリックします。

手順	手順
ステップ 5	アクティベーションコードの導入準備を許可するように MRA アクセス制御を構成します。 **1.** Expressway-C で、**[構成（Configuration）] > [Unified Communications] > [構成（Configuration）]**の順に選択します。 **2.** **[OAuth トークンによる承認（更新あり）（Authorize by OAuth token with refresh）]** を **オン**にします。 **3.** **[アクティベーションコードの導入準備を許可する（Allow activation code onboarding）]** を **[はい（Yes）]** に設定します。
ステップ 6	インストールされている信頼できるシスコ製造証明書（MIC）を確認します。これは、アクティベーションコードの導入準備機能にアクセスするために必要です。 **1.** Expressway-E で、**[メンテナンス（Maintenance）] > [セキュリティ証明書（Security certificates）] > [信頼できるCA証明書（Trusted CA certificates）]** の順に選択します。 **2.** **[信頼できるCA証明書を導入準備するコードをアクティブ化する（Activate code onboarding trusted CA certificates）]** をクリックします。
ステップ 7	オプション。独自のカスタム証明書を使用する場合 (: **1.** Expressway に証明書をアップロードします。 **2.** Unified Communications Manager の PhoneEdge-trust に証明書をアップロードします。 Unified Communications Manager がクラウドに証明書をアップロードします。アクティベーションプロセス中に、電話機はクラウドから証明書をダウンロードするため、電話機が Expressway と通信できるようになります。

手順	手順
ステップ 8	許可されているプロビジョニング方法を使用して、Cisco Unified Communications Manager データベースで電話機をプロビジョニングします。どちらのオプションを選択する場合でも、次のチェックボックスが両方ともオンになっていることを確認してください。 • **アクティベーションコードの導入準備が必要（Requires Activation Code Onboarding ）** • **MRA 経由のアクティベーションコードを許可（Allow Activation Code via MRA）** （注） 電話機にダミーの MAC アドレスをプロビジョニングできます。導入準備プロセスでは、電話機の実際の MAC アドレスを使用して**デバイス名**を更新します。 GUI または バルク管理者のどちらかを使用したサンプルプロビジョニング手順については、 *Cisco Unified Communications Manager* システム構成ガイド、リリース *12.5(1)SU1* 以降の「アクティベーションコードによるデバイス導入準備」章を参照してください。
ステップ 9	電話を MRA ユーザーに発送します。

電話機のアクティブ化

管理者には、電話機ユーザーにアクティベーションコードを送信するための2つのオプションがあります。

- セルフケアポータル — 電話機ユーザーはポータルにログインして、電話のアクティベーションコードと付随するバーコードを表示できます。アクティベーションコードを電話機に入力するか、電話機のビデオカメラを使用してバーコードをスキャンします。どちらの方法でも機能します。セルフケアの要件については、デバイス導入準備の前提条件を確認してください。
- CSV ファイルのエクスポート — 管理者は、Cisco Unified Communications Manager で、未処理のアクティベーションコードと関連するユーザの csv ファイルをエクスポートできます。このファイルの内容を使用して、MRA ユーザーにアクティベーションコードを通知できます。csv ファイルをエクスポートする方法

  1. Cisco Unified CM Administration から、**[デバイス（Device）]** > **[電話（Phone）]** を選択します。
  2. [関連リンク（Related Links）] から [アクティベーションコードのエクスポート（Export Activation Codes）] を選択し、[移動（Go）] をクリックします。

（注） アクティベーションコードのデフォルトの有効期間は 168 時間（7 日間） です。この値は、Cisco Unified Communications Manager の **Activation Time to Live (Hours)** サービスパラメータを使用して再構成できます。アクティベーションコードの有効期限が切れた場合、管理者は **[アクティベーションコードの解放（Release Activation Code）]** をクリックし、**[電話機の構成（Phone Configuration）]** ウィンドウの **[新しいアクティベーションコードを生成（Generate New Activation Code）]** をクリックすると、アクティベーションコードをリセットできます。

アクティベーションコードの入力

MRA ユーザーが電話機を接続すると、アクティベーションコードを入力するように求められます。アクティベーションコードを入力するか、セルフケアポータルに表示されるバーコードをスキャンすると、電話機が起動するので、構成ファイルをダウンロードして登録します。

これで、電話機を使用できる状態になりました。

安全な導入準備のための追加オプション

次のオプションは、セキュリティを強化するために構成プロセスをわずかに変更します。

オプション 1：管理者が実際の MAC アドレスを使用して電話をプロビジョニングする

管理者は、ダミーの MAC アドレスを使用するのではなく、実際の MAC アドレスを使用して電話機を Cisco Unified Communications Manager に追加します。この方法では、アクティベーションコードが実際の電話機の MAC アドレスに関連付けられ、アクティベーションコードがその電話機でのみ機能するため、セキュリティが強化されます。ただし、この方法では、管理者が各電話機の MAC アドレスを個別に収集して入力する必要があります。

オプション 2：管理者は、MRA モードでの再導入準備のためにリモートユーザーに送信する前に、オンプレミスの電話をアクティブ化します。

この方法では、管理者は、アクティベーションコード要件をリセットして MRA ユーザーに出荷する前に、オンプレミスモードで電話をアクティブ化します。MRA ユーザーは、電話を MRA モードでアクティブ化します。

- 管理者はアクティベーションコード導入準備（オンプレミスモード）を設定し、電話機にダミーの MAC アドレスをプロビジョニングします。
- 管理者は、オンプレミス環境で電話の導入準備をして登録します。このプロセスにより、Cisco Unified Communications Manager の**デバイス名**が実際の電話機の MAC アドレスで更新され、電話機がファームウェアロードを更新できるようになります。
- 管理者は MRA モードのアクティベーションコード導入準備を設定し、アクティベーションコード要件をリセットして、新しいコードが入力されるまで電話をロックします。

（注） **[電話機の構成（Phone Configuration）]** ウィンドウで、アクティベーションコードをリセットして電話をロックするため、次の両方のチェックボックスをオンにする必要があります。

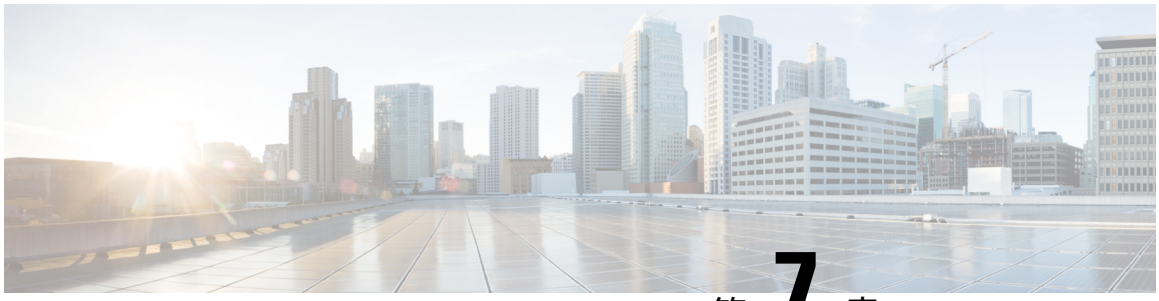
- **アクティベーションコードの導入準備が必要（Requires Activation Code Onboarding ）**
- **MRA 経由のアクティベーションコードを許可（Allow Activation Code via MRA）**

- 管理者は電話機を MRA ユーザーに発送し、ユーザーに新しいアクティベーションコードを通知します。
- リモート MRA ユーザーは、電話機を使用するために新しいアクティベーションコードを入力する必要があります。

このオプションには次の利点があります。

- アクティベーションコードは MAC アドレスに関連付けられ、その電話でのみ機能するため、セキュリティが向上します。
- ユーザーが電話機を受け取ったときに、電話機のファームウェアがすでに最新であることを確認します。
- 管理者が個別の MAC アドレスを収集して入力する必要はありません。

オンプレミスモードでのアクティベーションコード導入準備の構成方法については、『*Cisco Unified Communications Manager* 向けシステム構成ガイド』「アクティベーションコード」章の「オンプレミスタスク」を参照してください。



第 7 章

MRA のメンテナンス

- Expressway のメンテナンスモード （117 ページ）
- MRA 登録数 （118 ページ）
- 承認レートコントロール （118 ページ）
- クレデンシャルのキャッシング （119 ページ）
- Cisco Jabber 用 SIP 登録フェールオーバー, on page 120
- クラスタ化した Expressway システムとフェールオーバーの考慮事項 （123 ページ）
- Expressway 自動侵入保護 （123 ページ）
- Unified Communications サービス ステータスの確認 （125 ページ）
- 検出されたノードを更新する必要があるのはなぜですか? （125 ページ）
- Expressway-C でのサーバー更新 （126 ページ）

Expressway のメンテナンスモード

Expressway のメンテナンスモードは、管理された方法で MRA システムを停止できるように強化されました。

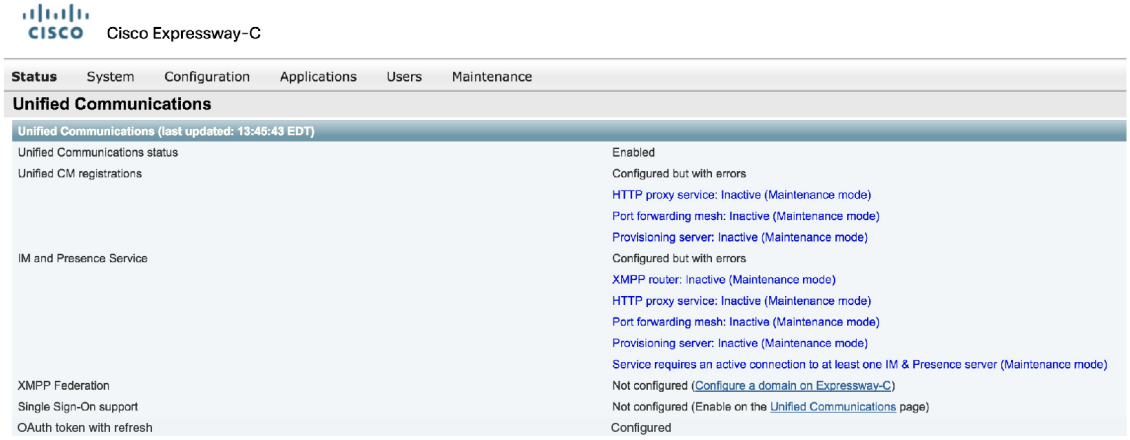
メンテナンスモードを実行すると、 Expressway は、新規通話またはプロキシ（MRA）トラフィックを受け入れを停止します。既存のコールとチャットセッションは影響を受けません。

ユーザがセッションを正常に終了すると、システムは、特定のタイプのトラフィックを処理していない時点に到達し、そのサービスをシャットダウンします。

Expressway がメンテナンスモード中、ユーザが新しいコールを発信または新しいチャットセッションを開始しようとすると、クライアントはサービス利用不可応答を受信し、他のピアを使用するように選択できます（可能な場合）。このフェールオーバーの動作はクライアントによって異なりますが、クラスタ内に実行中のピアがある場合、クライアントの再起動により、接続の問題を解決する必要があります。

[ユニファイドコミュニケーションのステータス（Unified Communications status）]ページには、MRA サービスが影響を受けるすべての場所（メンテナンスモード）が示されます。

図 *28 : Expressway-C* のメンテナンス モード



502281

CE エンドポイントの制限

CE ソフトウェアを実行しているエンドポイントの MRA では、メンテナンスモードはサポートされていません。メンテナンス モードを有効にすると、Expressway はこれらのエンドポイントからの MRA コールをドロップします。

MRA 登録数

X12.6.1 以降、Cisco Expressway-E の**[状態（Status）]** > **[概要（Overview）]** ページでは、MRA 経由で登録された SIP デバイスの最新の使用状況情報を監視できます。**[概要（Overview）]** ページには次のフィールドが含まれます。

MRA 登録

- **現在** — MRA を介して現在登録されているデバイスの総数。
- **ピーク**— 最後の Expressway 再起動以降の MRA 登録のピーク数。

承認レートコントロール

Expressway は、任意のユーザーのrpグイン情報を使用して、特定の構成可能な期間内に、ユーザーにコラボレーションサービスを許可する回数を制限できます。この機能は、同じユーザーを認証する複数のクライアントデバイス、または必要以上に頻繁に再承認するクライアントから発生する可能性のある、不注意または実際のサービス拒否攻撃を阻止するように設計されています。

クライアントがユーザーを認証するためのログイン情報を提供するたびに、Expressway は、この試行が**レートコントロール期間**によって指定された前の秒数内の**期間あたりの最大認証**を超えるかどうかを確認します。

試行が選択した最大数を超える場合、Expressway は試行を拒否し、HTTP エラー 429 「Too Many Requests」 を発行します。

認証レートコントロール設定は、**[構成（Configuration）]** > **[Unified Communications]** > **[構成（Configuration）]** ページの **[詳細設定（Advanced）]** セクションで構成できます。

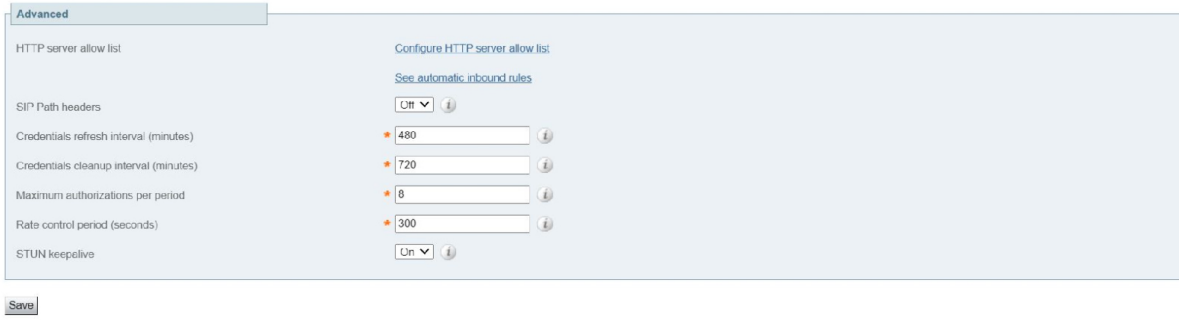
クレデンシャルのキャッシング

（注） これらの設定は、MRA 経由の認証に SSO（共通アイデンティティ）を使用しているクライアントには適用されません。

Expressway は、Unified CM が認証したエンドポイントログイン情報をキャッシュします。このキャッシュにより、Expressway が常に、認証目的で Unified CM にエンドポイントログイン情報を送信しなくても良くなるため、全体的なパフォーマンスが向上します。

キャッシュ設定は、**[構成（Configuration）]** > **[Unified Communications]** > **[構成（Configuration）]** ページの **[詳細設定（Advanced）]** セクションで構成できます。

図 *29 :* 詳細設定



ログイン情報更新間隔は、クライアントの認証に成功するために送信する認証トークンのライフタイムを指定します。正常に認証されたクライアントは、このトークンが期限切れになる前に更新を要求する必要があります。更新しないと、再認証が必要になります。デフォルト値は、480 分（8 時間）です。

ログイン情報削除間隔は、Expressway がキャッシュクリアの動作の間に待機する時間を指定します。キャッシュがクリアされると、期限切れのトークンのみが削除されるため、この設定は期限切れトークンをキャッシュに保持できる最長時間となります。デフォルトは 720 分（12 時間）です。

Cisco Jabber 用 SIP 登録フェールオーバー

モバイルおよびリモートアクセス（MRA）を使用して Expressway を展開する場合は、Cisco Jabber 用の SIP 登録フェールオーバーを適用します。

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

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

適応型ルーティング

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

Note 注記

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

STUN キープアライブのサポート

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

[設定（Settings）]

STUN キープアライブ設定は、**[構成（Configuration）]** > **[Unified Communications]** > **[構成（Configuration）]**ページの **[詳細設定（Advanced）]** セクションで構成できます。図 29 : 詳細設定 を参照してください。

フィールド	説明
STUN キープアライブ	Unified CM ハイアベイラビリティの STUN キープアライブを有効にします。 デフォルト：オン

要件

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

ルーティング機能	必要最小リリース
適応型ルーティング	**1.** Expressway X12.7 **2.** Cisco Jabber 12.9 MR **3.** Cisco Webex App
STUN キープアライブ	**1.** Expressway X12.7 **2.** Cisco Unified Communications Manager 14 **3.** Cisco Jabber 12.9 MR **4.** Cisco Webex App

Note 注記

-
- STUN キープアライブはクライアント（Jabber）から 30 秒ごとに送信され、3 秒以内に応答がなかった場合、クライアントはフェールオーバーを開始します。
- Expressway が Cisco Unified Communications Manager とは異なるドメインで設定されている場合、Cisco Unified Communications Manager 管理者は、Exp-C の関連するシステムドメインを追加することにより、Exp-C ホスト名エントリを手動で FQDN に更新する必要があります。

ノード復旧後の負荷分散

MRA-HA では、ノードに障害が発生するたびに、障害が発生したノードの負荷がクラスタ内の他の使用可能なノードにシフトされます。次のセクションでは、ノードがクラスタ内でアクティブになった後の負荷分散手順について説明します。

Expressway-C ノードの負荷分散

X14.1 リリース以降、Expressway-C ノードは、Expressway-E ノードで適応型ルーティングを使用して負荷分散されます。

Expressway-C ノードの障害後、トラフィック/登録はクラスタ内の他のノードによって処理されます。障害が発生したノードが回復してアクティブになると、新しい登録がそのノードを通過しても、そのノードは既存の負荷を処理しません。このシナリオで Expressway-C クラスタを負荷分散するために、Expressway-E には AR メカニズムが導入されています。

メッシュアーキテクチャでは、Expressway-E ノードと Expressway-C ノードの間にキープアライブメカニズムがあります。キープアライブメッセージ内で、Expressway-C はリソース使用状況やアクティブな登録を Expressway-E に送信します。次に、Expressway-E は、Expressway-C 内のすべてのノードでアクティブな登録を評価し、ノードでアンバランスな負荷を識別した場合、負荷分散をトリガーします。

負荷分散は、Register メッセージ（新規/更新）を最も負荷の少ないノードに適応的にルーティングすることによって実現されます。これは、適応型ルーティングをサポートするクライアントに対して行われます。負荷が分散されると、Expressway-E はプロセスを停止します。これにより、アイドル状態のノードがなくなり、負荷が分散されます。

Expressway-E ノードの負荷分散

Expressway-E ノードは、クラスタ内のすべてのノードの登録総数を維持します。クラスタに不均衡がある場合、登録数の多いノードは常に、200 応答メッセージの警告ヘッダーを使用して登録メッセージに応答し、負荷が不均衡であることを示します。

Note 負荷分散は均等または固定比率で共有されませんが、ノードの 0 ～ 100 の共有状況を回避しようとします。

すべてのソフトウェア要件によるメリット

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

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

Unified CM アップグレードなしの適応型ルーティングの利点

新しい Unified CM ソフトウェアなしでも（ただし、新しい Expressway および Jabber ソフトウェアを使用）、この機能は Jabber クライアントがパスの障害を検出できる利点があります。

Note このアクションは 2 分以上かかります。サーバーがアイドル状態またはその時点で使用が少ない一部のシナリオの場合、Expressway は、Unified CM サーバを非アクティブとしてフラグを立てる場合があります。

クラスタ化した Expressway システムとフェールオーバーの考慮事項

フェールオーバー（冗長性）サポートと向上した拡張性を提供するよう Expressway-C のクラスタおよび Expressway-E のクラスタを構成できます。

Expressway クラスタの構成方法に関しては、「Expressway クラスタ作成およびメンテナンス導入ガイド」を、Jabber エンドポイントおよびドメインネームシステム（DNS）の構成に関しては、「「Cisco Jabber 用のドメインネームシステム（DNS）の構成」」を参照してください。

Expressway-C で Unified CM および IM and Presence Service を検出する際は、これをプライマリピアで実行する必要があります。

Expressway 自動侵入保護

X8.9 以降、次のカテゴリについて自動侵入保護がデフォルトで有効になっています。

- http-ce-auth
- http-ce-intrusion
- sshpfwd-auth
- sshpfwd-intrusion
- xmpp-intrusion

この変更は新しいシステムに影響します。アップグレードされたシステムは既存の防御設定を維持します。

Expressway-C

Expressway-C をモバイルおよびリモートアクセスに使用すると、Unified CM と Expressway-E から多くのインバウンドトラフィックを受信します。

Expressway-C の自動保護を使用するには、自動的に作成されたネイバー ゾーンとユニファイド コミュニケーションのセキュアなトラバーサル ゾーンを使用するすべてのホストについて免除を追加する必要があります。Expressway は、検出された Unified CM または関連ノードの免除を自動では作成しません。

Expressway-E

まだ実行されていない場合は、[自動保護サービス（Automated protection service）]（**[システム（System）]** > **[システム管理（System administration）]**）を有効化する必要があります。

HTTP プロキシに対する悪意のある試行から保護するには、Expressway-E で自動侵入保護を設定できます（**[システム（System）]** > **[保護（Protection）]** > **[自動検出（Automated detection）]** > **[構成（Configuration）]**）。

Expressway-E で、次のカテゴリを有効にすることを推奨します。

- HTTP プロキシの認証の失敗と HTTP プロキシプロトコル違反。HTTP プロキシリソースアクセスの失敗カテゴリを有効化しないでください。
- XMPPプロトコル違反

（注） 自動保護サービスは Fail2ban ソフトウェアを使用します。これは、単一の送信元 IP アドレスから発信された総当たり攻撃から保護します。

例外の設定

自動侵入保護が構成されている場合は、この手順を使用して、1 つ以上の保護カテゴリからの IP アドレス範囲の除外を構成します。

免除が必要になる 1 つの例は、同じパブリック IP アドレスを使用して NAT の背後で複数の MRA ユーザーが接続されている場合です。これにより、単一の IP アドレスからの着信トラフィックが原因で保護がトリガーされる場合があります。

（注） この手順では、自動侵入保護が Expressway-E で有効化され、Expressway-C で無効化されていることを前提としています。これは、推奨される展開です。

ステップ 1 Expressway-E で、**[システム（System）]** > **[保護（Protection）]** > **[自動検出（Automated detection）]** > **[例外（Exemptions）]**の順に選択します。

ステップ 2 構成する**[アドレス（Address）]**をクリックするか、新規アドレスを構成する場合は、**[新規（New）]**をクリックします。

ステップ 3 **アドレス**と**プレフィックス長**を入力し、除外する IP アドレスの範囲を定義します。

ステップ 4 免除を適用するカテゴリから選択します。NAT の背後に複数のユーザーがいる例では、次のカテゴリが適用されます。

- HTTP プロキシ認証の失敗
- HTTP プロキシリソースアクセスの失敗
- SIP 認証エラー

ステップ 5 [住所の追加（Add Address）] をクリックします。

Unified Communications サービス ステータスの確認

Expressway-C と Expressway-E の両方で、Unified Communications サービスのステータスを確認できます。

ステップ 1 **[ステータス（Status）]** > **[Unified Communications]** の順に選択します。

ステップ 2 ドメイン、ゾーンおよび（Expressway-C のみ）Unified CM と IM and Presence Service サーバーの状態リストを確認します。

このページには、構成エラーと、問題に対処するためにアクセスする関連する構成ページへのリンクが表示されます。

検出されたノードを更新する必要があるのはなぜですか?

Expressway-C が Unified Communications ノードを検出すると、接続を確立して、ゾーンに必要な情報を読み取り、ルールを検索し、ネットワークの外部から発信されたリクエストをそのノードにプロキシします。**この構成情報は静的です。**Expressway は、新しいノードの検出を手動で開始したとき、または以前に検出されたノードの構成を更新したときにのみ、それを読み取ります。ノードを検出した後に関連する構成がノードで変更された場合、新しい構成とそのノードについて Expressway-C が認識している情報の不一致により、何らかの障害が発生する可能性があります。

Expressway-C が Unified Communications ノードから読み取る情報は、ノードタイプやロールごとに異なります。これらは、Expressway からの更新が必要になると予想される UC 構成の例です。これはすべてを網羅した完全なリストではありません。ノードの構成変更が MRA サービスに影響していると思われる場合は、それらのノードを更新して、潜在的な問題の既知の原因を 1 つ排除する必要があります。

- クラスタの変更（ノードの追加または削除など）
- セキュリティパラメータの変更（混合モードの有効化など）
- 接続ソケットの変更（SIP ポート構成など）
- TFTP サーバー構成の変更
- ノードソフトウェアのアップグレード

更新中にデバイスが接続できない

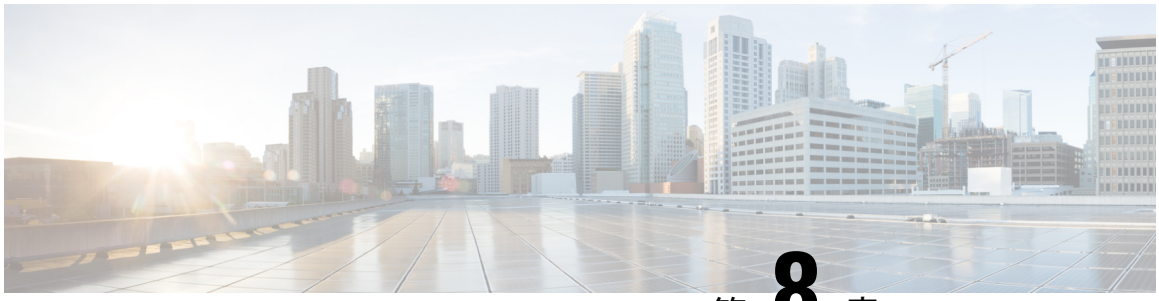
サーバーの更新後にサービスを復元するには時間がかかり、更新中、Jabber クライアントと他のエンドポイントは MRA 経由で接続できません。展開によって異なるため、正確なタイミングはお伝えできません。単純なデプロイメントの場合、更新には通常 5 ～ 10 秒かかりますが、非常に複雑な構成では 45 秒以上かかる場合があります。

Expressway-C でのサーバー更新

Expressway-C で定義した Cisco Unified Communications Manager と Cisco Unity Connection ノードを更新する必要があります。更新することで、Expressway がトークンを暗号化するために必要なキーをフェッチできます。

ステップ 1 Unified CM で、**[構成（Configuration）]** > **[Unified Communications]** > **[Unified CMサーバー（Unified CM servers）]** の順に選択し、**[サーバーを更新（Refresh servers）]** をクリックします。

ステップ 2 Cisco Unity Connection の場合は、**[構成（Configuration）]** > **[Unified CMサーバー（Unified CM servers）]** > **[Unity Connectionサーバー（Unity Connection servers）]** の順に選択し、**[サーバーを更新（Refresh servers）]** をクリックします。



第 8 章

MRA のトラブルシューティング

- 一般的なテクニック （127 ページ）
- Registration Issues （133 ページ）
- Cisco Expressway 証明書と TLS 接続の問題 （134 ページ）
- Cisco Jabber サインインの問題 （134 ページ）
- 特定の問題 （137 ページ）

一般的なテクニック

アラームとステータスメッセージ

トラブルシューティングを行うときは、最初にアラームが発生していないかどうかを確認します（**[ステータス（Status）] > [アラーム（Alarms）]**）。アラームが発生している場合、**[アクション（Action）]** 列の指示に従います。Cisco Expressway-C と Cisco Expressway-E の両方でアラームを確認します。

次にステータスの概要と構成情報を表示します（**[ステータス（Status）] > [Unified Communications]**）。Cisco Expressway-C と Cisco Expressway-E の両方でステータスページを確認します。必要な構成がないか、無効な場合、エラーメッセージと関連構成ページにアクセスするリンクが表示されます。

Cisco Expressway で次の項目を変更すると、無効なサービスまたはエラーが表示される場合があります。この場合、構成変更を有効にするため、システムを再起動する必要があります。

- サーバーまたは CA 証明書
- DNS 構成
- ドメインの設定

Collaboration Solutions Analyzer の使用

TAC が提供するCollaboration Solutions Analyzer（CSA）ツール 一式を使用して、MRA の展開とトラブルシューティングを行うことができます。（CSA にアクセスする方法については、Cisco Expressway リリースノートを参照してください。）

ステップ 1 CollabEdge **バリデータ ツール**を使用して、MRA 展開を検証します。

これは、Jabber クライアントのサインインプロセスをシミュレートし、結果に関するフィードバックを送信します。

ステップ 2 CollabEdge バリデータが問題を識別できない場合は、サインインの試行中に Cisco Expressway からログを収集することをお勧めします。次に、CSA の**ログ分析**コンポーネントを使用してログを分析します。

診断ログ

Jabber for Windows 診断ログ

Jabber for Windowsログファイルは、`C:\Users\<UserID>\AppData\Local\Cisco\Unified Communications\Jabber\CSF\Logs` で `csf-unified.log` として保存されます。

Cisco Expressway 診断ログ レベルの構成

Cisco Expressway の診断ロギングツールは、システムの問題をトラブルシューティングするために使用できます。また、長時間に渡ってシステムアクティビティの診断ログを生成し、ログをダウンロードすることができます。

始める前に

診断ログを実行する前に、適切なロギングモジュールのログレベルを設定する必要があります。

ステップ 1 **[メンテナンス（Maintenance）] > [診断（Diagnostics）] > [詳細設定（Advanced）] > [サポートログの構成（Support Log configuration）]** の順に選択します。

ステップ 2 発生している問題に対して推奨されるログを選択します。これらは、Log Advisor ツールを使用して見つけることができます。https://logadvisor.cisco.com/logadvisor/collaboration/unifiedcommunications/mra を参照してください。

ステップ 3 **[デバッグに設定（Set to debug）]** をクリックします。

診断ログキャプチャの作成

Cisco Expressway 診断ログ レベルを構成したら、診断ログキャプチャを開始できます。

ステップ 1 **[メンテナンス（Maintenance）]** > **[診断（Diagnostics）]** > **[診断ロギング（Diagnostic logging）]** の順に選択します。

ステップ 2 （任意） **[ロギング中にtcpdumpを取る（Take tcpdump while logging）]** を選択します。

ステップ 3 [Start new log] をクリックします。

ステップ 4 （任意） **マーカー**テキストを入力して、**[マーカーの追加（Add Marker）]** をクリックします。

- 特定のアクティビティが実行される前にマーカー機能を使用して、ログ ファイルにコメント テキストを追加することができます。これは、ダウンロードされた診断ログ ファイルで該当するセクションを識別するのに役立ちます。
- 診断ログの進行中に、必要に応じた数のマーカーを追加できます。
- マーカーのテキストは「**DEBUG_MARKER**」タグでログに追加されます。

ステップ 5 診断ログにトレースするシステムの問題を再現します。

ステップ 6 [Stop Logging] をクリックします。

ステップ 7 [ログの収集（Collect Logs）] をクリックします。

ステップ 8 ログの収集が完了したら、**[ログのダウンロード（Download log）]** をクリックして、ローカル ファイル システムに診断ログ アーカイブを保存します。

アーカイブを保存するように促されます（実際の表現はブラウザによって異なります）。

ログの作成後

ログを再度ダウンロードする場合は、**[ログ収集（Log Collection）]** ボタンを使用することで再度収集できます。ボタンがグレー表示されている場合は、まず、ブラウザでページを更新してください。

診断ログを完了した後、**[サポートログの構成（Support Log configuration）]** ページに戻り、*INFO* レベルに変更されたロギングモジュールをリセットします。

ドメインネームシステム（DNS）レコードの確認

Cisco Expresswayのドメインネームシステム（DNS）ルックアップ ツールを使用すると、システムの問題をトラブルシューティングできます。

[メンテナンス（Maintenance）] > **[ツール（Tools）]** > **[ネットワークユーティリティ（Network utilities）]** > **[ドメインネームシステム（DNS）ルックアップ（DNS lookup）]** の順に選択します。

SRV レコードのルックアップには、H.323、SIP、Unified Communications、および TURN サービスに固有のものが含まれます。

（注） Cisco Expressway-C からドメインネームシステム（DNS）ルックアップを実行すると、企業内からのビューが返され、Cisco Expressway-E で実行すると、DMZ 内から表示できる内容が返されます。これは、必ずしもパブリックインターネットのエンドポイントで使用可能なレコードと同じレコード一式であるとは限りません。

ドメインネームシステム（DNS）ルックアップには、Unified Communications に使用する次の SRB サービスが含まれます。

- _collab-edge._tls
- _cisco-uds._tcp

Cisco Expressway-E が到達可能であることを確認します

この手順では、 Cisco Expressway-E が到達可能であることを確認する方法について説明します。

Cisco Expressway-E の FQDN がパブリック ドメインネームシステム（DNS）で解決可能であることを確認します。

[システム（System）] > **[ドメインネームシステム（DNS）（DNS）]** で FQDN を **<System host name>.<Domain name>** として構成します。

通話状況の確認

通話状況情報には、現在の通話と完了した通話の両方を表示できます。

コール ステータス情報の同じセットは、「**登録ごとのコール（Calls by registration）**」ページ（「**登録の詳細（Registration details）**」ページ経由でアクセス可能）でも表示できます。

Cisco Expressway がクラスタの一部の場合、リストが各ピアに対して最新の 500 通話に制限されていても、クラスタ内でピアに適用できるすべての通話が表示されます。

ステップ 1 現在の通話に関する情報を取得する場合は、**[通話状態（Call status）]**ページ（**[状態（Status）]** > **[通話（Calls）]** > **[通話（Calls）]**）にアクセスします。

[通話状態（Call status）] ページには、現在進行中のすべての通話または Cisco Expressway で登録されているデバイスからの通話、または Cisco Expressway をパススルーしている通話が一覧されます。

ステップ 2 完了した通話に関する情報を取得する場合は、**[通話履歴（Call history）]** ページ（**[状態（Status）]** > **[通話（Calls）]** > **[履歴（History）]**）にアクセスします。

[通話履歴（Call history）] ページには、非アクティブのすべての通話が一覧されます。このリストは、最新の 500 通話に制限されており、 Cisco Expressway が最後に再開されてから発生した通話が含まれます。

モバイルおよびリモートアクセス通話 ID

[通話状態（Call Status）] と [通話履歴（Call History）] ページには。Unified CM リモートセッション（モバイルおよびリモートアクセスが有効な場合）と Cisco Expressway RMS セッションを含むすべての通話タイプが表示されます。

コール タイプを区別するにはコール コンポーネントをドリルダウンする必要があります。モバイルおよびリモートアクセス通話には、通話が Cisco Expressway-C または Cisco Expressway-E で表示されているかによって、異なるコンポーネントの特性があります。

- Cisco Expressway-C では、Unified CMリモートセッションには、（メディア暗号化を強制するために B2BUA が使用されるため）3 つのコンポーネントがあります。 Cisco Expressway コンポーネントの 1 つは、 Cisco Expressway と Unified CM 間で自動生成されたネイバーゾーン（名前の前に **CEtcp** または **CEtls**が付きます）の 1 つを介して通話をルートします。
- Cisco Expressway-E では、1 つのコンポーネントがあり、これは **CollaborationEdgeZone** を介して通話をルートします。

両方のエンドポイントが企業外（つまりオフプレミス）にある場合は、2 つの独立したコールとして扱われます。

リッチメディアセッション（ Cisco Expressway のみ）

システムにリッチ メディア セッション キーがインストールされ、Business-to-Business（B2B）コール、サードパーティ製ソリューションへのインターワーク コールまたはゲートウェイ コールなどをサポートする場合、これらのコールは、コール状態やコール履歴のページに記載されています。

Cisco Expressway 経由で Unified CM に登録されたデバイス

Unified CM のアイデンティティデバイス

この手順では、 Cisco Expressway を介して Unified CM にアイデンティティデバイスを登録する方法を説明します。

ステップ 1 Unified CM で、**[デバイス（Device）]** > **[電話機（Phone）]** の順に選択し、**[検索（Find）]** をクリックします。

ステップ 2 **[IP アドレス（IP Address）]** 列をチェックします。

Cisco Expressway 経由で登録されたデバイスが、Cisco Expressway-C で登録された IP アドレスを表示します。

Cisco Expressway-C でのプロビジョニングセッションを識別

この手順では、Cisco Expressway-C を経由してプロビジョニングされるセッションの識別方法について説明します。

ステップ 1 Cisco Expressway-C で、**[ステータス（Status）] > [Unified Communications]** の順に選択します。

ステップ 2 **[詳細ステータス情報（Advanced status information）]** セクションで、**[プロビジョニングセッションの表示（View provisioning sessions）]** をクリックします。

これは、現在および最近の（赤色で表示）すべてのプロビジョニングセッションのリストを表示します。

Cisco Expressway-C が Unified CM と同期されていることを確認してください。

Unified CM クラスタまたはノード構成を変更すると、Unified CM と Cisco Expressway-C 間で通信の問題が発生する場合があります。これには、次の項目への変更が含まれます。

- Unified CM クラスタ内のノード数
- 既存クラスタのホスト名または IP アドレス
- リスニングポート番号
- セキュリティ パラメータ
- 電話機セキュリティプロファイル

そのような変更が Cisco Expressway-C で反映されることを確認する必要があります。手順は次のとおりです。

ステップ 1 Cisco Expressway で、**[構成（Configuration）] > [Unified Communications]** の順に選択します。

ステップ 2 すべての Unified CM と IM and Presence Service ノードで再検出します。

MRA 認証ステータスとトークンの確認

この手順では、MRA 認証ステータスとトークンを確認する方法について説明します。

ステップ 1 （任意） 標準（更新無し）OAuth ユーザートークンを確認してクリアするには、**[ユーザー（Users）] > ビューを選択し、トークン所有者を更新せずに OAuth を管理します。**

これは、特定のユーザーの OAuth アクセスに関する問題を特定するのに役立ちます。

ステップ 2 （任意） MRA 認証の統計を確認するには、**[状態（Status）] > [Unified Communications] > [詳細なMRA認証統計を表示（View detailed MRA authentication statistics）]** の順に選択します。

このページでの予期しないリクエストまたは応答は、構成または承認の問題を特定するのに役立つ場合があります。

Registration Issues

Unified CM にエンドポイントを登録できない

次の理由でエンドポイントが登録できない場合があります。

- Unified CM と Cisco Expressway-C の間で SIP トランクが構成されている場合、Unified CM にエンドポイントを登録できない場合があります。SIP トランクが構成されている場合、Unified CMUnified CM への SIP 回線登録に使用されるポートとは別のリスニング ポートを Unified CM で使用する必要があります。詳細については、Unified CM と Expressway-C 間の SIP トランク （87 ページ）を参照してください。

- Cisco Expressway-C のサーバー証明書に、Subject Alternate Name リスト、暗号化された TLS に対して構成された Unified CM のすべての電話機セキュリティプロファイルの名前、リモートアクセスに必要なデバイスに使用するすべての電話機セキュリティプロファイルの名前が含まれていない場合、登録を安全にできない場合があります（「SSL 接続確立の失敗」メッセージ）。Unified CM と Cisco Expresswayの証明書の両方にあるこれらの名前は、FQDN フォーマットにしなければなりません。

  Expressway-C の既存のクラスタに新しい Expressway-C ノードを追加する間は、新しいノードの証明書署名要求（CSR）を生成する必要があります。CUCM でモバイルおよびリモートアクセス（CUCM）クライアントの安全な登録が必要な場合、CUCM に安全なプロファイル名を付ける必要があります。「Unified CM Phone のセキュリティプロファイル名」が CUCM デバイスのセキュリティプロファイルの名前またはホスト名だけである場合、新しいノードでの CSR の作成は失敗します。これにより、管理者は **[安全な電話機プロファイル（Secure Phone Profile）]** ページの下で、CUCM で 「Unified CM Phone のセキュリティプロファイル名」の値を変更する必要があります。

  X12.6 から、Unified CM のセキュリティプロファイル名は完全修飾ドメイン名（FQDN）である必要があります。名前、ホスト名、または値だけでは使用できません。

  たとえば、`jabbersecureprofile.domain.com`、`DX80SecureProfile.domain.com`

（注） FQDN は複数レベルで構成できます。各レベルの名前に使用できるのは文字、数字、ハイフンのみで、各レベルはピリオド（ドット）で区切ります。レベル名はハイフンで開始または終了できません。また、最後のレベル名は文字で開始する必要があります。

Cisco Expressway 証明書と TLS 接続の問題

Cisco Expressway のサーバー証明書または信頼できる CA 証明書を変更するには、変更を有効にするために Cisco Expressway を再起動する必要があります。

セキュアなプロファイルを使用している場合、Cisco Expressway-C 証明書に署名した認証局のルート CA を CallManager の信頼証明書（**[Cisco Unified OS の管理（Cisco Unified OS Administration）]** アプリケーションの **[セキュリティ（Security）]** > **[証明書管理（Certificate Management）]**）としてインストールする必要があります。

CiscoSSL 5.4.3 が 1024 ビット未満の Diffie-Hellman キーを拒否する

バージョン 9.x 以前、または Unified CM または Unified CM IM and Presence Service の Cisco Expressway バージョン X8.7.2 以降を実行している場合、2 つのシステム間の SSL ハンドシェイクはデフォルトで失敗します。

これは、 Cisco Expressway X8.7.2 以降にアップグレードした後、すべての MRA エンドポイントが登録または呼び出しに失敗する症状です。

これは、CiscoSSL コンポーネントを 5.4.3 以降にアップグレードしたことが原因です。このバージョンは、D-H キー交換を使用するときに Unified CM が提供するデフォルト（768 ビット）キーを拒否します。

インフラストラクチャをアップグレードするか、Cisco Technical Assistance Center に問い合わせて、Unified CM や Unified CM IM and Presence Service のデフォルト設定を修正し、 TLS をサポートできるかを確認する必要があります（CSCuy59366）。

Cisco Jabber サインインの問題

Jabber が自動侵入保護をトリガーする

条件（Conditions）

- MRA ソリューションは、OAuth トークンによる認証用に構成されています（更新の有無にかかわらず）。

- Jabber ユーザーのアクセストークンの有効期限が切れた
- Jabber は、次のいずれかを行います。
  - デスクトップの休止状態からの再開
  - ネットワーク接続の回復
  - 数時間サインアウトした後の高速ログインの試行

動作

- 一部の Jabber モジュールは、有効期限切れのアクセストークンを使用して Cisco Expressway-E で認証を試行します。
- Cisco Expressway-E がこれらのリクエストを（正しく）拒否する
- 特定の Jabber クライアントからそのようなリクエストが 5 つ以上ある場合、Cisco Expressway-E は、（デフォルトで）10 分間、IP アドレスをブロックします。

Symptoms

影響のある Jabber クライアントの IP アドレスは、*HTTP* プロキシ認証障害カテゴリにある Cisco Expressway-E の **[ブロックされたアドレス（Blocked addresses）]** リストに追加されます。**[システム（System）]** > **[保護（Protection）]** > **[自動検出（Automated detection）]** > **[ブロックされたアドレス（Blocked addresses）]** の順に選択すると、これらを表示できます。

回避策

この問題に対処するには、2 つの方法があります。1 つ目は、特定のカテゴリに対して検出しきい値を増加させる方法、2 つ目は、影響のあるクライアントに対して例外を作成する方法です。例外は実際の環境で実用的ではない場合があるので、ここではしきい値オプションについて説明します。

1. **[システム（System）]** > **[保護（Protection）]** > **[自動検出（Automated detection）]** > **[設定（Configuration）]**の順に選択します。
2. **[HTTPプロキシの認証の失敗（HTTP proxy authorization failure）]** をクリックします。
3. **トリガーレベル** を *5* から *10* に変更します。期限が切れたトークンを提示する Jabber モジュールを容認するには 10 で十分です。
4. 設定を保存すると、すぐに有効になります。
5. 影響を受けるクライアントのブロックを解除します。

ネットワーク外からの接続時、Jabberポップアップが無効な証明書を警告する

これは、Cisco Expressway-E 上で正しく構成されていないサーバー証明書の症状です。証明書が自己署名されているか、サブジェクトの別名（SAN）としてリストされている組織の外部ドメインネームシステム（DNS）ドメインがない可能性があります。

これは、Jabber で想定されている動作です。Jabber が信頼する CA が発行した証明書をインストールし、その証明書に Jabber が使用しているドメインが SAN のリストに含まれていることをお勧めします。「 証明書の要件 （21 ページ）」を参照してください。

Jabber が電話サービスに登録しない

Cisco Expressway と ユーザーデータサービス（UDS）の間には不一致を処理するケースがあり、提供されたユーザー ID が保存されている ID のケースと一致しない場合、電話サービスに Jabber を登録できなくします。Jabber は、継続してサインインできますが、電話サービスは使用できません。

ユーザーは、UDS で保存されているとおりのユーザー ID でサインインすることで、この問題を回避できます。

ユーザーは、サインアウトして Jabber をリセットすることで、この問題を解決できます。「CSCux16696」を参照してください。

XMPP のバインド障害が原因で Jabber がサインインできない

XMPP のバインド障害が原因で、Jabber クラインとにサインインできない場合があります（「サーバーに通信できない」エラーメッセージ）。

これは、Jabber クライアントログのリソース バインド エラーによって示されます。次に例を示します。

```
XmppSDK.dll #0, 201, Recv:<iq id='uid:527a7fe7:00000cfe:00000000' type='error'><bind
xmlns='urn:ietf:params:xml:ns:xmpp-bind'/><error code='409' type='cancel'><conflict
xmlns='urn:ietf:params:xml:ns:xmpp-stanzas'/></error></iq>

XmppSDK.dll #0, CXmppClient::onResourceBindError

XmppSDK.dll #0, 39, CTriClient::HandleDisconnect, reason:16
```

これは通常、IM and Presence Intercluster Sync Agent が正しく実行されない場合に発生します。詳細については、https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html の『Cisco Unified Communications Manager 構成ガイド』の「*IM and Presence* 情報」を参照してください。

SSH トンネル障害が原因で Jabber がサインインできない

SSH トンネルが確立できないことが原因で、Jabber がサインインできない場合があります。Cisco Expressway-C と Cisco Expressway-E の間のトラバーサルゾーンは、他のすべての点で正常に機能します。 Cisco Expressway は、「アプリケーションに障害発生 – `portforwarding.pyc` で予期しないソフトウェアエラーが検出されました」と報告します。

これは、Cisco Expressway-E ドメインネームシステム（DNS）ホスト名に下線を含めると発生する場合があります。**[システム（System）] > [ドメインネームシステム（DNS）（DNS）]**の順に選択し、**システムホスト名**に、文字、数字、ハイフンのみが含まれていることを確認します。

Cisco Expressway-E のクラスタ内の異なるピアに接続すると Jabber がサインインできない

Cisco Expressway-E ピア間でドメインネームシステム（DNS）ドメイン名に不整合があると、Jabber がサインインできない場合があります。ドメイン名は、クラスタ内のすべてのピアで、大文字と小文字の区別も含めて同一である必要があります。

各ピアで、**[システム（System）] > [ドメインネームシステム（DNS）（DNS）]**の順に選択し、ドメイン名が、すべてのピアで同じであるか確認します。

特定の問題

Cisco Expressway が 「401 Unauthorized」 のエラーメッセージを返します。

Cisco Expressway が、エンドポイントクライアントが提示したログイン情報を認証しようとした場合、「401 Unauthorized」 のエラーメッセージが表示される場合があります。エラーの理由には次のものが挙げられます。

- SAML アサーションで提供される IDP の userid にソリューションを構成する必要があることに注意してください。これは、トークン（アクセス/更新）に対して検証するために、Cisco Unified Communications Manager userid の sAMAccountName と一致する必要があります。
- クライアントが不明なユーザー名または間違ったパスワードを入力した。
- クラスタ間ルックアップサービス（ILS）がすべての Unified CM クラスタに設定されていない。これは、UDS クエリがクライアントのホームクラスタを検出するために Cisco Expressway が使用する Unified CM ノードに応じて、断続的な障害の原因となる場合があります。

「「407 Proxy Authentication Required」」または「「500 Internal Server Error」」のエラーによる通話障害

通話障害は、 Cisco Expressway のトラバーサルゾーンが *[*ログイン情報の確認（*Check credentials*）*]* の **[認証ポリシー（Authentication policy）]** で構成されていると発生する場合があります。モバイルおよびリモートアクセスに使用されているトラバーサルゾーンの **[認証ポリシー（Authentication policy）]** が *[*ログイン情報を確認しない（*Do not check credentials*）*]* に設定されていることを確認します。

通話のビットレートが 384 kbps に制限されているまたは、BFCP（プレゼンテーション共有）使用時のビデオの問題

これは、Unified CM で構成された地域内のビデオビットレート制限によって生じる可能性があります。

地域間と地域内で、**[ビデオ コールの最大セッション ビット レート（Maximum Session Bit Rate for Video Calls）]**（**[システム（System）]** > **[リージョン情報（Region Information）]** > **[リージョン（Region）]**）が 6000 kbps などのシステムの適切な上限に設定されていることを確認します。

IM and Presence Service レルムの変更

IM and Presence Service レルムが変更され、Cisco Expressway-C のレルムデータが更新されていない場合、プロビジョニングエラーが発生する可能性があります。

たとえば、これは、IM and Presence Service ノードのアドレスが変更された場合、または新しいピアが IM and Presence Service クラスタに追加された場合に発生する可能性があります。

診断ログには、Cisco Expressway-C でレルムが見つからないため、「`Failed to query auth component for SASL mechanisms`」のような 情報メッセージが含まれる場合があります

[構成（Configuration）] > **[Unified Communications]** > **[IM and Presence Service ノード（IM and Presence Service nodes）]**の順に選択し、**[サーバーを更新（Refresh servers）]** をクリックして、更新した構成を保存します。プロビジョニングエラーが解決されない場合は、IM and Presence Service ノード構成を確認して再度更新します。

ボイスメールサービスがありません（「403 Forbidden」 応答）

Cisco Unity Connection（CUC）のホスト名が Cisco Expressway-C の HTTP サーバー許可リストに含まれていることを確認します。

サービスリクエストに対する「403 Forbidden」 応答

Cisco Expressway-C および Cisco Expressway-E が信頼できる NTP サーバーに同期されていない場合、サービスに障害が発生する場合があります（「403 Forbidden」 応答）。すべての Cisco Expressway システムが信頼できる NTP サービスと同期されていることを確認してください。

Cisco Expressway がクライアント HTTPS リクエストをドロップする

Cisco Expressway-E の自動侵入保護機能によって、HTTP プロキシ経由でリソースにアクセスするクライアント IP アドレスから、不正な試行（404 エラー）が繰り返し検出された場合に発生することがあります。

クライアント アドレスがブロックされないようにするには、**[HTTP プロキシのリソース アクセスの失敗（HTTP proxy resource access failure）]**（**[システム（System）]** > **[保護（Protection）]** > **[自動検出（Automated detection）]** > **[構成（Configuration）]**）が無効になっていることを確認します。

失敗：アドレスが IM and Presence サーバーではない

このエラーは、リモートアクセスに使用する IM and Presence Service サーバーを構成しようとした場合に発生する可能性があります（**[構成（Configuration）]** > **[Unified Communications]** > **[IM and Presence サーバー（IM and Presence servers）]**）。これは IM and Presence Service サーバーに CA 証明書がないことが原因で、9.1.1 を実行するシステムに該当します。詳細と推奨ソリューションは、「CSCul05131」を参照してください。

無効な SAML アサーション

クライアントが SSO を介した認証をできなかった場合の 1 つの可能性のある理由として、Cisco Expressway-C が IDP からの無効なアサテーションを拒否した場合が挙げられます。

無効な `SAML 応答` のログを確認します。

1 つの例として、ユーザーの ID を Cisco Expressway-C に送信するクレームルールが ADFS にない場合が挙げられます。この場合、ログに `[IdPからのアサテーションにuid属性がありません（No uid Attribute in Assertion from IdP）]` と表示されます。

Cisco Expressway は、**`uid`** と呼ばれる属性にアイデンティティを持つ ADFS からのクレームがアサートされるユーザー ID を想定します。ADFS に移動して、各信頼当事者証明でクレームルールを設定し、「uid」 としてユーザーの E メールアドレス（または展開に応じて sAMAccountName）を他の信頼当事者に送信します。

「502 Next Hop Connection Failed」 メッセージ

Cisco Expressway-E の 502 メッセージは、次のホップに障害が発生したことを示します（一般的には Cisco Expressway-C）。次の手順を実行します。

1. Cisco Expressway-E で、**[ステータス（Status）]** > **[Unified Communications]** の順に選択します。Cisco Expressway-E レポートで問題が発生しましたか?
2. ステータスが正常に見える場合は、[ステータス（Status）] ページの下部にある **[SSH トンネルステータス（SSH tunnel status）]** リンクをクリックします。Cisco Expressway-C ノードへの 1 つ以上のトンネルがダウンしている場合、502 エラーが原因である可能性があります。

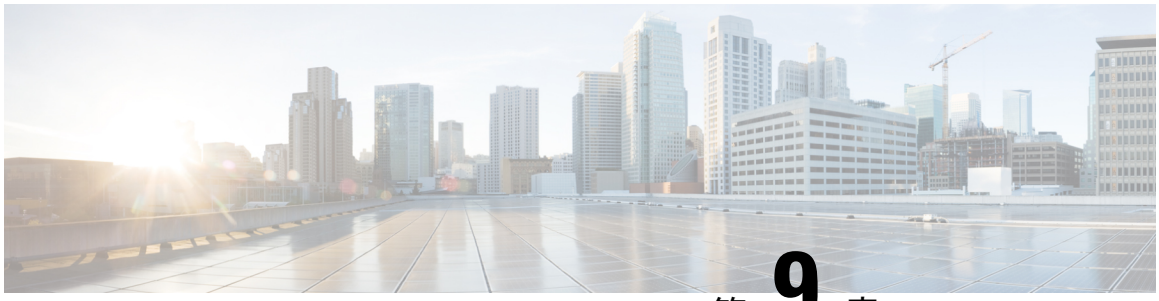
着信側エンドポイントが Expressway-E から 15 ホップ以上離れている場合、MRA コールは失敗します

Unified Communications トラバーサルゾーンのデフォルトのホップカウントは 15 です。これが原因であると思われる場合は、すべての MRA Expressway にサインインし、ホップカウントを 70 などの非常に大きな数に増やしてテストします。

第 部

付録

- HTTP 許可リストのフォーマット （143 ページ）
- MRA 導入のアップグレード後のタスク, on page 147
- Expressway での HSM デバイスの構成, on page 161



第 9 章

HTTP 許可リストのフォーマット

この付録には、HTTP 許可リストの生成とテストに使用できる情報が含まれています。

- 許可リストは、ファイルの参照を決定します （143 ページ）
- 許可リスト テスト ファイル リファレンス （144 ページ）

許可リストは、ファイルの参照を決定します

CSVファイルを使用してルールを定義できます。この項では、各ルールの引数に許容されるデータへの参照を提供し、CSV 形式のルールを示します。

表 *19*：リストルールの引数を許可する

引数インデックス	パラメータ名	Required/オプション	サンプル値
0	Url	必須	**`protocol://host[:port][/path]`** それぞれの説明は次のとおりです。 • protocol は **`http`** または **`https`** です。 • host には DNS 名または IP アドレスを指定できます。 • :port はオプションです。: の後に 0 ～ 65535 の範囲の 1 つの数値のみが続きます（例えば、**`:8443`** • /path はオプションです。HTTP 仕様に準拠する必要があります。
1	導入	任意	このルールを使用する導入の名前。複数の導入がある場合は必須です。それ以外の場合は空白の引数を入力します。
2		オプション	HTTP メソッドのカンマ区切りリスト。必要に応じて二重引用符で囲います。例：**`"GET,PUT"`**
3		任意	**`exact`** または **`prefix`**。デフォルトは **`prefix`** です。

引数インデックス	パラメータ名	Required/オプション	サンプル値
4		任意	ルールの説明。スペースを含む場合は二重引用符で囲みます。

サンプルリストルール CSV ファイル

```
Url,Deployment,HttpMethods,MatchType,Description
https://myServer1:8443/myPath1,myDomain1,GET,,"First Rule"
http://myServer2:8000/myPath2,myDomain200,"GET,PUT",exact,
https://myServer3:8080/myPath3,myDomain1,,prefix,"Third Rule"
https://myServer4/myPath4,myDomain1,,prefix,"Fourth Rule"
http://myServer5/myPath5,myDomain1,,prefix,"Fifth Rule"
```

- ファイルの最初の行にパラメータ名（記載のとおり）をリストします
- 1 行ごとに 1 つのルール、ルールごとに 1 行
- カンマで引数を区切ります
- 上記の表に示すように、ルール値は正しい順序にします
- スペースを含む値は二重引用符で囲みます

許可リスト テスト ファイル リファレンス

CSV ファイルを使用してテストを定義できます。この項では、各テストの引数に許容されるデータへの参照を提供し、CSV 形式のテストを示します。

表 *20 :* リストテスト引数の許可

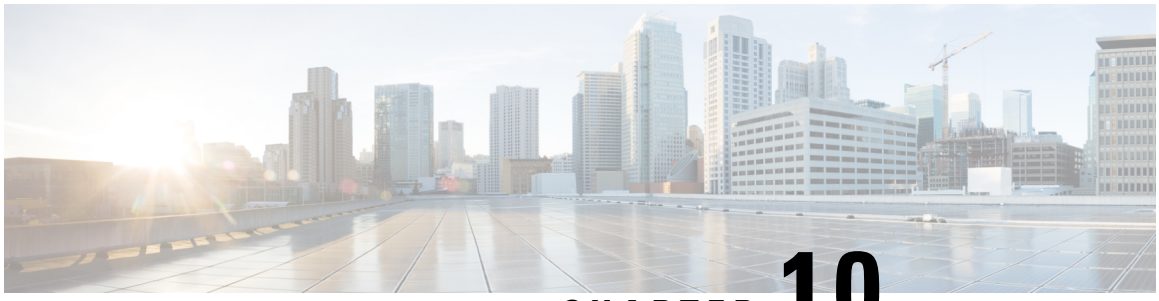
引数インデックス	パラメータ名	Required/オプション	サンプル値
0	Url	必須	**`protocol://host[:port][/path]`** それぞれの説明は次のとおりです。 • protocol は **`http`** または **`https`** です。 • host には DNS 名または IP アドレスを指定できます。 • :port はオプションです。：の後に 0 ～ 65535 の範囲の 1 つの数値のみが続きます。 • /path はオプションです。HTTP 仕様に準拠する必要があります。

引数インデックス	パラメータ名	Required/オプション	サンプル値
1	ExpectedResult	必須	**allow** または **block**。テストで、指定した URL をルールによって許可またはブロックする必要があると前提するかどうかを指定します。
2	導入	任意	この URL を使用してテストする導入の名前。この引数を省略すると、テストはデフォルトの導入を使用します。
3	説明	任意	ルールの説明。スペースを含む場合は二重引用符で囲みます。
4	HttpMethod	任意	テストする HTTP メソッドを 1 つ指定します。例：**PUT** 指定しない場合、デフォルトで **GET** に設定されます。

サンプルリストテスト CSV ファイル

```
Url,ExpectedResult,Deployment,Description,HttpMethod
https://myServer1:8443/myPath1,block,"my deployment","a block test",GET
http://myServer2:8000/myPath2,allow,"my deployment","an allow test",PUT
https://myServer4/myPath4,allow,,,GET
http://myServer4/myPath4,block,,,POST
```

- 最初の行にパラメータ名（記載のとおり）をリストします
- 1 行ごとに 1 つのテスト、テストごとに 1 行
- カンマで引数を区切ります
- 上記の表に示すように、テスト値は正しい順序にします
- スペースを含む値は二重引用符で囲みます



CHAPTER 10

MRA 導入のアップグレード後のタスク

- MRA アクセス制御設定を再構成するには （147 ページ）
- MRA アクセス制御の設定 （148 ページ）
- アップグレードによって適用される MRA アクセス制御値 （157 ページ）

MRA アクセス制御設定を再構成するには

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、ユーザー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。

ステップ 1 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、 の以前の設定に合わせて適切な値を設定します。従来の の設定と同等の 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、[サーバーの更新（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 *21 : 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 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）]

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。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

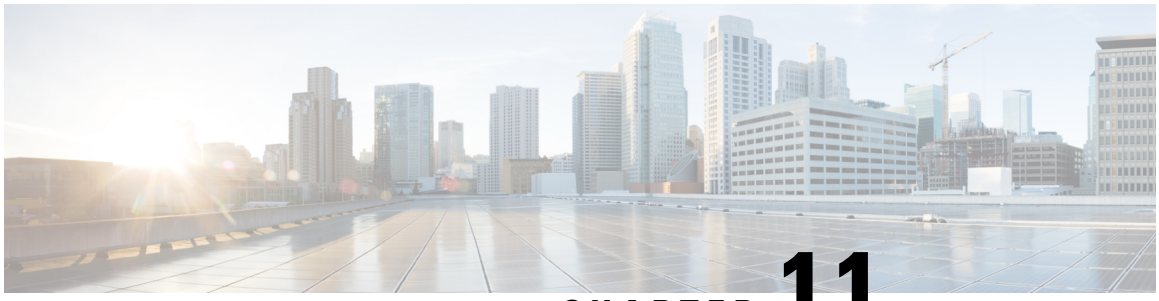
アップグレードによって適用されるMRAアクセス制御値

表 *22 :* 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）



CHAPTER 11

Expressway での HSM デバイスの構成

- 重要：事前の確認事項 （161 ページ）
- HSM を有効にして管理する方法 （161 ページ）
- モジュールの削除方法 （165 ページ）
- HSM の無効化方法 （166 ページ）

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 と互換性のある証明書の作成	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 での HSM の有効化

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。

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 設定が更新されました
   ```

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 モジュールが正常に追加されました
```

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 モードが正常に更新されました
```

（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。

ステップ 1 **[メンテナンス（Maintenance）]** > **[セキュリティ（Security）]** > > **[HSM構成（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。

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。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。