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

MRA のポートについては、『Cisco Expressway シリーズ設定ガイド』の『*Cisco Expressway IP* ポート使用設定ガイド』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

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

ドメイン	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 *2:* 例：ローカルドメインネームシステム（*DNS*）

ドメイン	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* ポート使用設定ガイド』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 *3:* 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**: Unified CM は、IPv4 アドレスまたはデュアルスタックを有効にして（IPv4 および IPv6）、MRA 経由の IPv6 クライアントをサポートするように設定できます。X14.2 リリース以降、Expressway は MRA 経由の IPv6 クライアントをサポートします。

（注） MRA 経由の IPv6 クライアントをサポートするには、CUCM および IMP 関連の設定に対してデュアルネットワークを有効にします。デュアルネットワークは、必ずしも IPv4 アドレスと IPv6 アドレスの両方で構成することを意味しません。

- **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 （9 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」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。

- IM and Presence は、IPv4 アドレスまたはデュアルスタックを有効にして（IPv4 および IPv6）、MRA 経由の IPv6 クライアントをサポートするように設定できます。X14.2 リリース以降、Expressway は MRA 経由の IPv6 クライアントをサポートします。

（注） MRA 経由の IPv6 クライアントをサポートするには、CUCM および IMP 関連の設定に対してデュアルネットワークを有効にします。デュアルネットワークは、必ずしも IPv4 アドレスと IPv6 **アドレス**の両方で構成することを意味しません。

- 証明書の要件については、「証明書の要件 （9 ページ）」を参照してください。

自己署名証明書を使用する CUCM サーバー

デフォルトでは、CUCM サーバーに自己署名証明書が付属しています。これらが設定されている場合、**TLS 検証**と**セキュアデバイス登録**の両方を同時に使用することはできません。どちらの機能も独立して使用できます。ただし、証明書は自己署名であるため、自己署名の *Tomcat* および自己署名の *CallManager* 証明書を Expressway C の信頼できる CA リストにアップロードする必要があることを意味します。Expressway C は、証明書を検証するために信頼リストを検索すると、一致する件名を持つものが見つかったら停止します。このため、信頼リストの上位にある *tomcat* または *callmanager* のいずれかで、その機能が動作します。下の方は、存在しなかったかのように失敗します。

解決策: CA（パブリックまたはプライベート）で CUCM 証明書に署名し、その CA だけを信頼します。

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

新しい Expressway サーバー証明書をアップロードする前に、Expressway サーバー証明書に署名する、または証明書チェーンで参照されるすべての CA 署名付き証明書をアップロードします。Expressway の 信頼できるストアには、常に完全な CA 署名付き証明書チェーンが必要です。

メモ 不要になった CA 証明書を削除します。

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 *4:* 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）

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。
Unity Connection	Tomcat	Unified CM UC サービス設定（FQDN 推奨）のホスト名/IP アドレス内で Unity ノードを定義するために使用されるパラメータは、サブジェクト代替名（SAN）として *Unity Tomcat* 証明書内に存在する必要があります。

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-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。
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。

サーバー証明書の検証は、X14.2 以降のリリースのデフォルトです。Cisco Unified Communications Manager（CallManager、Tomcat）、モバイルおよびリモートアクセス用の IM and Presence Service（cup-xmpp、Tomcat）に自己署名証明書を使用する場合は、Expressway-C の信頼できる CA 署名付きストアにアップロードします。

Expressway-C のバージョンが X14.2 リリースより前の場合は、自己署名 Unified CM および IM and Presence Service 証明書を Expressway-C の信頼できる CA 署名付きストアにアップロードする必要はありません。

X14.2 以降のリリースでは、サーバー証明書の検証を無効にすることもできます。つまり、Unified CM、IM and Presence Service の証明書を Expressway-C の信頼できる CA 署名付きストアにアップロードする必要はありません。これは推奨オプションはありません。

（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 *5:* 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-E リストには、以下を含める必要があります。 • 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む必要があります。 • 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）

証明書署名要求の拡張	Expressway-C の要件	Expressway-E の要件
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。

（注） Expressway は、すべての MRA 接続に mTLS を使用します。アクティベーション コード オンボーディングが有効になると、mTLS はすべての MRA 接続に対して有効になります。これにより、オペレーティングシステムに応じて Jabber クライアントの動作が変わる可能性があります。

Apple コンピューターで Jabber を使用している場合、ポップアップが表示され、ローカルの信頼ストアから証明書を選択するように求められます。証明書が選択されていない場合でも、mTLS は Jabber MRA ログインを必要としないため、MRA ログインは引き続き機能します。IP 電話だけが mTLS を必要とします。

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 *6 : 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 *7: 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**：
  - CUCM ノードがダウンした場合、MRA 経由で登録された 78XX/88XX シリーズの電話機は、別のアクティブノードとの通信を継続します。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 は、Expressway-E の背後にあるデバイスのサーバーグループのフルメッシュではなく、2 つの静的サーバーグループを形成します。したがって、Expressway-C および CUCM ノードがダウンし、IP Phone に有効なサーバーグループがない場合、登録は失敗します。

    たとえば、クラスタ E1 と E2、C1 と C2、CUCM サブ、および CUCM pub を持つ顧客を考えてみます。IP 電話は、`getedgeconfigeresponse` に基づいて 2 つの静的サーバーグループを形成します。

    ```
    E1 > C1 > CUCM sub
    E2 > C2 > CUCM pub
    ```

顧客が C2 および CUCM サブを停止した場合、有効なサーバーグループがないため、登録は失敗します。電話機は、Expressway-E の背後にあるデバイスのフルメッシュ サーバー グループを作成しません。

- **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」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） 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。
- **MRA ログイン HA フェールオーバーを MRA-HTTP に拡張**

X14.2 リリース以降、Expressway MRA ログインは Unified CM の障害に対して復元力があります。

- Expressway がクラスタユーザーまたは authorize_proxy リクエストを送信する Unified CM ノードが機能していない場合、Expressway は同じクラスタ内の別のランダムノードを試行します。
- Expressway は、既知の不正な Unified CM/UDS をキャッシュから選択しません。そのため、Expressway は、サービス中であると考えられるが、これまでに障害が発生したノードを再試行しません。
- Expressway は、clusterUser の一部である `get_edge_config` レスポンスの一部として、既知の不正な UDS を含めません。
- 範囲は、Expressway で終了するフローのみを対象としています。これは、Expressway がプロキシであり、エンドポイント/Jabber が HTTP リクエストの発信元であるフローは対象外です。

- **Webex Unified CM Calling サポート自動拡張更新トークン**

  Webex アプリ（Unified CM Registered）は、電話サービスを維持するために 60 日ごとにログインするようにユーザーに求めます。管理者は、これらのプロンプトの周期を設定できます。デフォルトのタイミングは 60 日です。

  ユーザーは、Webex アプリへのログインをキャンセルできます。ただし、メッセージング、会議、および内部コールには引き続きアクセスできます。コールが適切に認証されていない場合、ユーザーは電話サービスが切断され、不在着信が発生します。さらに、内部（Call on Webex）コールは機能するが、PSTN コールは失敗するというユーザーエクスペリエンスが混乱する可能性があります。

  ユーザーの通話エクスペリエンスを向上させるために、Webex アプリケーション更新トークンの自動更新を設定します。この機能は、2023 年 11 月以降、Unified CM 15 とともに使用できます。Expressway X15 および Webex アプリ 6.8 もこの機能をサポートしています。

  この機能の **利点** には、エンドユーザーが Webex アプリでコールを見逃さないこと、および PSTN コールが失敗した場合にのみ Webex でコールを体験できることが挙げられます。

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。
- 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。

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。