ユニファイド コミュニケーション

ユニファイドコミュニケーションの前提条件

ユニファイド コミュニケーションのためのセキュアなトラバーサル ゾーン接続の設定

ユニファイド コミュニケーション機能（Mobile & Remote Access、または Jabber Guest など）には、Expressway-C と Expressway-E 間にユニファイド コミュニケーション トラバーサル ゾーン接続が必要です。これには、以下が含まれます。

- Expressway-C と Expressway-E に適切なセキュリティ証明書をインストールする。
- Expressway-C と Expressway-E 間のユニファイド コミュニケーション トラバーサル ゾーンを設定する。

（注） ユニファイドコミュニケーショントラバーサルゾーンは Expressway のトラバーサルペアごとに 1 つだけ設定します。つまり、Expressway-C クラスタに 1 つのユニファイド コミュニケーション トラバーサル ゾーンと、Expressway-E クラスタに対応する 1 つのユニファイド コミュニケーション トラバーサル ゾーンです。

Expressway のセキュリティ証明書のインストール

Expressway-C と Expressway-E 間の信頼を設定する必要があります。

1. Expressway-C と Expressway-E の両方に適したサーバ証明書をインストールします。

   - 証明書には、**Client Authentication** 拡張子を含める必要があります。システムにより、ユニファイドコミュニケーション機能が有効になっている場合、この拡張子を指定せずにサーバ証明書をアップロードすることはできません。
   - Expressway には、証明書署名要求（CSR）を生成する機能が組み込まれており、CSR を生成する場合に推奨される方法です。
     - 要求に署名する CA がクライアント認証拡張子を除外していないことを確認します。
     - 生成した CSR には、クライアント認証要求と有効化されたユニファイド コミュニケーション機能に関連するサブジェクト代替名が含まれます（ユニファイドコミュニケーションのサーバ証明書要件を参照してください）。
   - CSR を生成するか Expressway にサーバ証明書をアップロードするには、**[メンテナンス（Maintenance）]** > **[セキュリティ（Security）]** > **[サーバ証明書（Server certificate）]** に移動します。新しいサーバ証明書を有効にするには、Expressway を再起動する必要があります。

2. 両方の Expressway に Expressway のサーバ証明書に署名した CA の信頼できる認証局（CA）証明書をインストールします。

   展開されるユニファイドコミュニケーション機能に基づいて、次のように信頼要件が追加されます。

   Mobile & Remote Access を導入する場合：

   - Expressway-C は Unified CM と IM&P の Tomcat 証明書を信頼する必要があります。
   - 状況に応じて、Expressway-C と Expressway-E の両方で、エンドポイントの証明書に署名した認証局を信頼する必要があります。

   Jabber Guest を導入する場合：

   - Jabber Guest サーバがインストールされると、自己署名証明書がデフォルトで使用されます。ただし、信頼できる認証局によって署名された証明書をインストールできます。Expressway-C に Jabber Guest サーバの自己署名証明書、または Jabber Guest サーバの証明書に署名した CA の信頼済み CA 証明書をインストールする必要があります。

   信頼できる認証局（CA）証明書を Expressway にアップロードするには、**[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）]** を選択します。新しい信頼できる CA 証明書を有効にするには、Expressway を再起動する必要があります。

Expressway 構成ガイドページの『*Cisco Expressway* 証明書作成および使用導入ガイド』を参照してください。

暗号化された Expressway トラバーサル ゾーンの設定

Expressway-C と Expressway-E 間のセキュアなトラバーサル ゾーン接続によってユニファイド コミュニケーション機能をサポートするには、次の手順を実行します。

- ゼロタイプの *Unified Communications* トラバーサルを使用して Expressway-C と Expressway-E を構成します。これは自動的に適切なトラバーサル ゾーン（Expressway-C 上で選択されたときは、トラバーサル クライアント ゾーン、Expressway-E 上で選択されたときは、トラバーサル サーバ ゾーン）を設定します。そのゾーンは、[TLS 検証モード（TLS verify mode）] が [オン（On）] かつ [メディア暗号化モード（Media encryption mode）] が [強制暗号化（Force encrypted）] の状態で SIP TLS を使用します。
- 両方の Expressway はサーバ証明書を相互に信頼する必要があります。各 Expressway は、クライアントとサーバーの両方として動作するので、各 Expressway の証明書がクライアントとサーバーの両方で有効であることを確認します。
- Expressway は、CN（共通名）ではなく SAN 属性（サブジェクトの別名）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が必要な場合は、トラバーサルゾーンの別のペアを構成します。

（注） Expressway-C と Expressway-E の間で ICMP がブロックされている場合、「<Exp-E FQDN> cannot be reached」 というエラーが表示され、セキュアテストに失敗します。（TAC ラボで、Expressway-C から ICMP クエリをドロップするように Expressway-E でファイアウォールルールを作成してシミュレート）。

安全なトラバーサルゾーンをセットアップするには

セキュアなトラバーサル ゾーンを設定するには、Expressway-C と Expressway-E を次のように設定します。

ステップ 1 **[設定（Configuration）]** > **[ゾーン（Zones）]** > **[ゾーン（Zones）]** へ移動します。

ステップ 2 [新規（New）] をクリックします。

ステップ 3 次のようにフィールドを設定します（他のすべてのフィールドはデフォルト値のままにします）。

	Expressway-C	**Expressway-E**
名前（Name）	「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		

	Expressway-C	Expressway-E
ユーザ名（**Username**）	「exampleauth」など	「exampleauth」など **注**：ローカル認証データベースのユーザーを作成する場合は、このフィールドにスペースを含めないでください。
パスワード（**Password**）	「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）]**をクリックし、ポップアップ ダイアログで **[新規（New）]** をクリックして、**[名前（Name）]** に名前（例：「「exampleauth」」）、**[パスワード（Password）]** にパスワード（例：「「ex4mpl3.c0m」」）を入力し、**[クレデンシャルの作成（Createcredential）]**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 シリーズ設定ガイドのページに用意されている、ご使用のバージョンに対応する『*Cisco Expressway IP Port Usage Configuration Guide*』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（SAN（サブジェクトの別名）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		

	Expressway-C	Expressway-E
ピア 1 アドレス	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。	**対象外**
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。	**対象外**

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

ユニファイド コミュニケーションのサーバ証明書要件

Cisco Unified Communications Manager の証明書

Mobile & Remote Access で重要な Cisco Unified Communications Manager 証明書は、次の 2 つです。

- *CallManager* 証明書
- *tomcat* 証明書

これらの証明書は Cisco Unified Communications Manager に自動的にインストールされ、デフォルトで自己署名されて同じ一般名（CN）を持ちます。

CA によって署名された証明書を使用することを推奨します。ただし、自己署名証明書を使用する場合、2 つの証明書の一般名は異なる必要があります。Expressway では同じ CN を持つ 2 つの自己署名証明書は許可されません。そのため、Expressway の信頼される CA リストで *CallManager* と *tomcat* の自己署名証明書の CN が同じ場合、Expressway はそのうちの 1 つしか信頼できません。つまり、Expressway-C と Cisco Unified Communications Manager 間のセキュア HTTP またはセキュア SIP は失敗します。

また、シスコ コラボレーション システム リリース 10.5.2 内の製品に対して *tomcat* 証明書の署名要求を生成する場合、CSCus47235 に注意する必要があります。ノードの FQDN がサブジェクト代替名（SAN）エントリとして証明書に含まれるようにするため、この問題を回避する必要があります。「リリースノート」ページにある *Expressway X8.5.3* のリリースノートに回避策の詳細が記載されています。

IM and Presence Service の証明書

XMPP を使用する場合に重要となる IM and Presence Service 証明書は、次の 2 つです。

- *cup-xmpp* 証明書
- *tomcat* 証明書

CA によって署名された証明書を使用することを推奨します。ただし、自己署名証明書を使用する場合、2 つの証明書の一般名は異なる必要があります。Expressway では同じ CN を持つ 2 つの自己署名証明書は許可されません。*cup-xmpp* 証明書と *tomcat*（自己署名）証明書が同じ CN を持つ場合、Expressway はそのうちの 1 つしか信頼せず、Cisco Expressway サーバと IM and Presence Service サーバ間の一部の TLS 試行が失敗します。詳細については、CSCve56019 を参照してください。

Expressway 証明書

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、どのユニファイド コミュニケーションの機能にどの CSR 代替名の要素が適用されるかを示します。

サブジェクト代替名としてこれらの項目を追加します ↓	**これらの目的で CSR を生成する場合**			
	←			→
	モバイル & リモート アクセス	**Jabber Guest**	**XMPP フェデレーション**	**ビジネス ツー ビジネス コール**
Unified CM 登録ドメイン（ドメイン名にかかわらず、これらは Unified CM SIP 登録ドメインよりもサービス検出ドメインと共通点があります）	Expressway-E でのみ必要	-	-	-
XMPP フェデレーション ドメイン	-	-	Expressway-E でのみ必要	-
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）	-	-	必須	-
Unified CM 電話セキュリティ プロファイル名	Expressway-C でのみ必要	-	-	-
（クラスタ化されたシステムのみ）Expressway クラスタ名	Expressway-C でのみ必要	Expressway-C でのみ必要	Expressway-C でのみ必要	-

（注）
- チャット ノード エイリアスを追加するか、名前を変更する場合、Expressway-C 用の新しいサーバ証明書の作成が必要になることがあります。つまり、IM and Presence ノードが追加されるか名前が変更される場合、または新しい TLS 電話セキュリティ プロファイルが追加される場合などです。
- 新しいチャット ノード エイリアスがシステムに追加される場合、または CM か XMPP フェデレーション ドメインが変更される場合は、新しい Cisco Expressway-E の証明書を作成する必要があります。
- 新しくアップロードされたサーバ証明書を有効にするには、Expressway を再起動する必要があります。

Expressway-C/Expressway-E の個々の機能要件についての詳細は、次のとおりです。

Expressway-C のサーバ証明書の要件

Expressway-E サーバ証明書には、そのサブジェクト代替名（SAN）のリストに次の要素が含まれる必要があります。

- Un**ified CM 電話セキュリティ プロファイル名**：暗号化されたトランスポートライン（TLS）用に設定され、リモートアクセスを必要とするデバイスに使用される Unified CM の**電話セキュリティ プロファイル**の名前。完全修飾ドメイン名（FQDN）形式を使用し、複数のエントリをカンマで区切ります。

  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。

エンドポイントは OAuth 認証機能をサポートしています。電話セキュリティプロファイルの構成詳細は次のとおりです。

1. エンドポイントは、デバイスセキュリティモードが *[*暗号化（*Encrypted*）*]* に設定され、**OAuth 認証が有効**になっている電話セキュリティプロファイルにリンクされているため、電話のセキュリティプロファイル名が Expressway-C 証明書のサブジェクト代替名（SAN）リストに含まれている必要はありません。
2. エンドポイントは、デバイスセキュリティモードが *[*暗号化（*Encrypted*）*]* に設定されているが、OAuth 認証が**有効になっていない**電話セキュリティプロファイルにリンクされている場合、電話のセキュリティプロファイル名が Expressway-C 証明書のサブジェクト代替名（SAN）リストに含まれている必要があります。

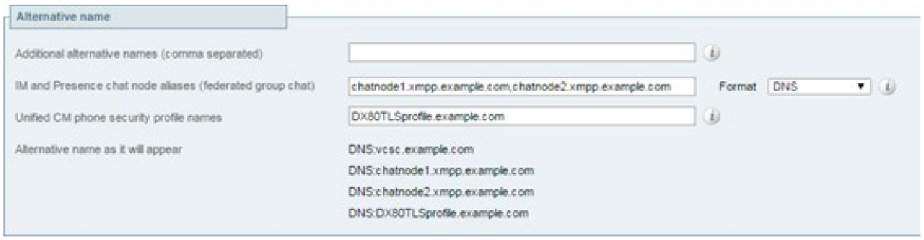
代替名としてセキュア電話プロファイルを持つことは、Unified CM がそのプロファイルを使用するデバイスからメッセージを転送する場合に、Expressway-C とトランスポートラインシグナリング（TLS）経由で通信できることを意味します。

- **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）**：IM and Presence サーバで設定される**チャットノードエイリアス**（たとえば **`chatroom1.example.com`**）。これらは、フェデレーテッド連絡先との TLS を介したグループ チャットをサポートするユニファイド コミュニケーション XMPP フェデレーション導入にのみ必要です。

  Expressway-C は一連の IM&P サーバを検出すると、CSR にチャット ノード エイリアスを自動的に含めます。

  CSR を生成するときは、チャット ノードエイリアスに DNS 形式を使用することを推奨します。Expressway-E サーバ証明書の代替名には、同一のチャット ノード エイリアスを含める必要があります。

図 *1: Expressway-C* の *CSR* ジェネレータでのセキュリティプロファイルおよびチャットノードエイリアスに対するサブジェクト代替名の入力



454313

Expressway-E のサーバ証明書の要件

Expressway-E サーバ証明書には、そのサブジェクト代替名（SAN）のリストに次の要素が含まれる必要があります。Expressway-E が他の FQDN によって知られている場合は、**すべてのエイリアス**がサーバ証明書 SAN に含まれている必要があります。

- **Unified CM 登録ドメイン**：Unified CM の登録用に Expressway-C で設定されているすべてのドメイン。エンドポイント デバイスと Expressway-E 間のセキュアな通信に必要です。

Expressway の設定と Expressway-E の証明書に使用される Unified CM 登録ドメインは、サービス検出時に **_collab-edge** DNS SRV レコードをルックアップするモバイルおよびリモート アクセス クライアントによって使用されます。これにより、Unified CM での MRA 登録が有効になり、サービス検出に役立ちます。

これらのサービス検出ドメインは SIP 登録ドメインと一致することもしないこともあります。これは展開方法により異なるため、一致する必要はありません。たとえば、社内ネットワークの Unified CM で .local または類似するプライベート ドメインを使用し、Expressway-E FQDN とサービス検出にパブリック ドメイン名を使用する展開の場合、Expressway-E の証明書にパブリック ドメイン名を SAN として含める必要があります。Unified CM で使用するプライベート ドメイン名を含める必要はありません。エッジ ドメインのみを SAN としてリストする必要があります。

DNS 形式を選択し、必要な FQDN を手動で指定します。複数のドメインが必要な場合は FQDN をカンマで区切ります。代わりに *CollabEdgeDNS* 形式を選択すると、入力したドメインにプリフィックス **collab-edge.** が追加されます。この形式は、トップ レベル ドメインを SAN として含めたくない場合に推奨されます（次のスクリーンショットの例を参照してください）。

- **XMPP フェデレーション ドメイン**：ポイントツーポイント XMPP フェデレーションに使用するドメイン。これらは、IM&P サーバで設定され、XMPP フェデレーション用のドメインとして Expressway-C でも設定する必要があります。

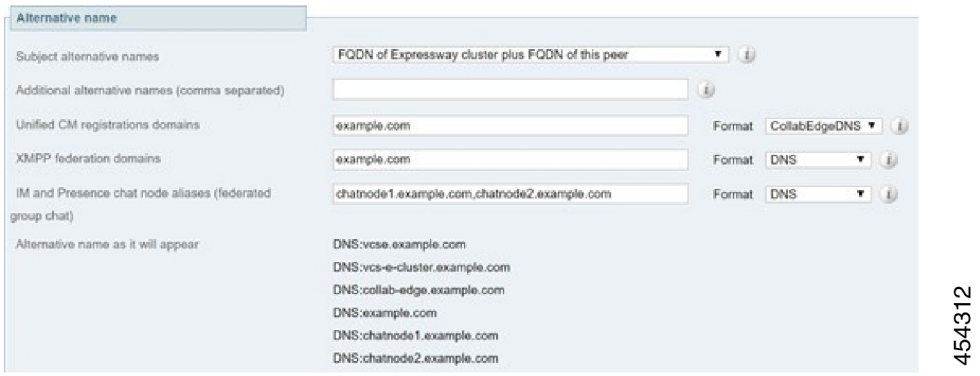
  DNS 形式を選択し、必要な FQDN を手動で指定します。複数のドメインが必要な場合は FQDN をカンマで区切ります。

（注） *XMPPAddress* 形式を使用しないでください。この形式は CA によってサポートされない可能性があり、Expressway ソフトウェアの将来のバージョンでは廃止される可能性があります。

- **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）**：Expressway-C の証明書で入力されたものと同じ**チャットノードエイリアス**のセット。フェデレーテッド連絡先との TLS を介したグループ チャットをサポートする音声とプレゼンスの導入にのみ必要です。

（注） チャットノードエイリアスのリストは、Expressway-C 対応の「**CSR の作成（Generate CSR）**」ページからコピーできます。

図 *2: Expressway-E* の *CSR* ジェネレータでの *Unified CM* 登録ドメイン、*XMPP* フェデレーション ドメイン、およびチャット ノード エイリアスに対するサブジェクト代替名の入力



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

MRA オンボードを使用する場合の mTLS 証明書

MRA 上でアクティベーション コード オンボードを有効にすると、相互 TLS に必要な CA 証明書が自動的に生成されます (相互 TLS はアクティベーション コード オンボードの必須要件です)。証明書は、信頼された CA 証明書のあるページからアクセスするための mTLS 用 CA 証明書ページで使用できます（**[メンテナンス（Maintenance）] > [セキュリティ（Security）] > [信頼された CA 証明書（Trusted CA certificate）]**）。

ドメイン証明書および Sever Name Indication の管理

Cisco Hosted Collaboration Solution（HCS）の一部であるマルチテナンシーにより、サービス プロバイダーは複数のテナント間で Expressway-E クラスタを共有できます。

TLS 内のサーバ名指定（SNI）プロトコル拡張を使用して、Expressway は、TLS ハンドシェイク中にクライアントに提供できるドメイン固有の証明書を保存および使用できるようになりました。この機能により、マルチテナント環境で MRA を介して登録したエンドポイントのシームレスな統合が可能になり、証明書のドメイン名がクライアントのドメインと一致するようになります。TLS ハンドシェイク中、クライアントは *ClientHello* 要求に SNI フィールドを含めます。Expressway は証明書ストアを検索し、SNI ホスト名との一致を探そうとします。一致が見つかった場合、ドメイン固有の証明書がクライアントに返されます。

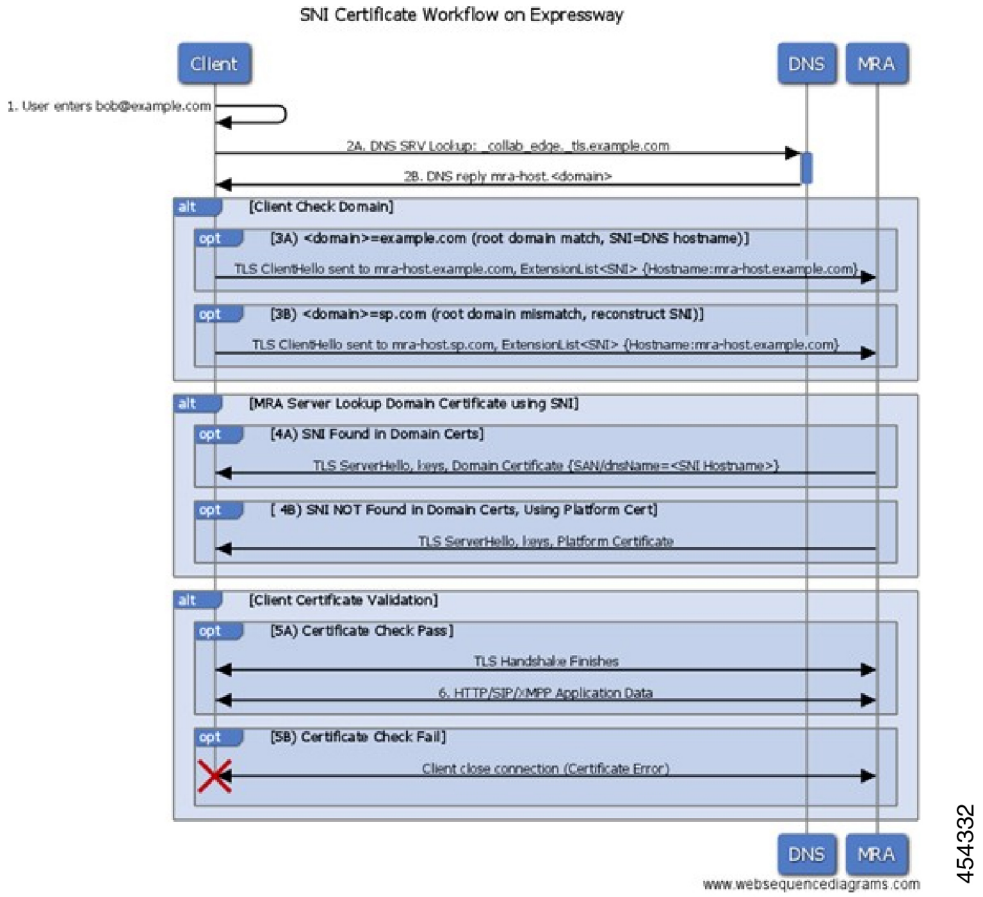
（注） マルチテナントモードでは、Cisco Expressway-E の **[システム（System）] > [DNS]** ページで、DNS に設定されているホスト名と一致するようにシステムのホスト名を設定する必要があります（X8.10.1 より前では大文字と小文字が区別されます。X8.10.1 以降は大文字と小文字は区別されません）。このようにしなければ、Cisco Jabber クライアントを MRA に正常に登録できません。

Cisco Hosted Collaboration Solution ページの『マルチテナントおよび *Cisco Expressway*』を参照してください。

SNI のコール フロー

1. 登録されている MRA クライアントで、ユーザが **bob@example.com** と入力します。ここで、**example.com** はユーザのサービス ドメイン（クラスタ ドメイン）です。
2. クライアントが DNS 解決を行います。
    1. **_collab-edge._tls.example.com** に対して DNS SRV 要求を送信します。
    2. DNS が要求に応答します。
        - 単一のテナント設定の場合：通常、DNS応答にはサービス ドメイン内のホスト名（たとえば、**mra-host.example.com**）が含まれます。
        - マルチテナント設定の場合：DNSが代わりに、サービスプロバイダーのドメイン内のサービスプロバイダーのMRAホスト名を返す場合があります。これは、ユーザのサービス ドメインとは異なります（たとえば、**mra-host.sp.com**）。
3. クライアントが SSL 接続を設定します。
    1. クライアントは、SSL ClientHello リクエストに SNI 拡張子を付けて送信します。
        - DNSによって返されたホスト名がユーザのサービス ドメインと同じドメインを持つ場合、DNS ホスト名は SNI server_name（変更なし）で使用されます。
        - それ以外の場合、ドメインが一致しなければ、クライアントはSNI server_name をDNS ホスト名とサービス ドメインに設定します（たとえば、DNS から **mra host.sp.com** が返されるのではなく、**mra-host.example.com** が返されます）。
    2. Expressway-Eが証明書ストアを検索し、SNIホスト名と一致する証明書を検索します。
        - 一致するものが見つかると、Expressway-E は証明書（SAN/dnsName=SNI ホスト名）を返信します。
        - それ以外の場合、MRA はプラットフォーム証明書を返します。
    3. クライアントがサーバの証明書を検証します。
        - 証明書が検証されると、SSL セットアップが続行され、SSL セットアップが正常に終了します。
        - それ以外の場合、証明書エラーが発生します。
4. アプリケーション データが開始されます。

（注） SIP と HTTPS の場合は、アプリケーションが SSL ネゴシエーションを即座に開始します。XMPP の場合は、クライアントが XMPP StartTLS を受信すると、SSL 接続が開始されます。



Expressway のドメイン証明書の管理

Expressway のドメイン証明書は、**「ドメイン証明書（Domain certificates）」**ページ（**[メンテナンス（Maintenance）] > [セキュリティ（Security）] > [ドメイン証明書（Domain certificates）]**）で管理します。これらの証明書は、マルチテナント環境で複数の顧客が TLS 暗号化と HTTPS 経由の Web ブラウザを使用してクライアントシステムと通信するために Expressway-E クラスタを共有している場合に、ドメインを識別するために使用されます。[ドメイン証明書（domain certificate）] ページを使用すると、次のことを実行できます。

- 現在ロードされている証明書に関する詳細の表示
- 証明書署名要求（CSR）を生成します。
- 新しいドメイン証明書のアップロード

- ACME（Automated Certificate Management Environment）サービスが自動的に CSR を ACME プロバイダーに送信して、生成された証明書を自動的に展開するように設定します。

（注） RSA キーに基づく証明書を使用することを強く推奨します。DSA キーに基づく証明書など他のタイプの証明書はテストされておらず、あらゆるシナリオで Expressway と連携するとは限りません。「**信頼できる CA 証明書（Trusted CA certificate）**」 ページを使用して、この Expressway で信頼されている認証局（CA）の証明書のリストを管理します。

現在アップロードされているドメイン証明書の表示

ドメインをクリックすると、ドメイン証明書データ セクションに、現在 Expressway にロードされている特定のドメイン証明書に関する情報が表示されます。

現在アップロードされているドメイン証明書ファイルを表示する場合、人間可読形式で表示するには **[表示（復号化）（Show (decoded)）]** をクリック、または RAW 形式でファイルを表示するには **[表示（PEM ファイル）（Show (PEM file)）]** をクリックします。

現在アップロードされているドメインを削除するには、**[削除（Delete）]** をクリックします。

（注） ドメイン証明書を期限切れにしないでください。期限が切れると他の外部システムが証明書を拒否し、Expressway がそれらのシステムに接続できなくなります。

新しいドメインの追加

ステップ 1 **[メンテナンス（Maintenance）]** > **[セキュリティ（Security）]** > **[ドメイン証明書（Domain certificates）]** に移動します。

ステップ 2 **[新規（New）]** をクリックします。

ステップ 3 **[新しいローカルドメイン]**で、追加するドメインの名前を入力します。

例：

有効なドメインの例としては、`100.example-name.com` などがあります。

ステップ 4 [ドメインの作成（Create domain）] をクリックします。

ステップ 5 新しいドメインが **[ドメイン証明書（Domain certificates）]** ページに追加され、ドメインの証明書のアップロードに進むことができます。

証明書署名要求の生成

Expressway はドメイン CSR を生成可能で、これにより証明書要求を生成および取得するために外部メカニズムを使用する必要がなくなります。

（注）

- 1 回に 1 つの署名要求だけを進行させることができます。これは、Expressway が現在の要求に関連付けられた秘密キーファイルを追跡する必要があるためです。現在の要求を廃棄し、新しい要求を開始するには、[Discard CSR] をクリックします。
- ユーザインターフェイスにダイジェストアルゴリズムを設定するオプションがあります。デフォルトでは SHA-256 に設定されており、SHA-384 または SHA-512 に変更するオプションがあります。
- ユーザインターフェイスにキーの長さを設定するオプションがあります。Expressway は、1024、2048、および 4096 のキーの長さをサポートしています。

ステップ 1 **[メンテナンス（Maintenance）]** > **[セキュリティ（Security）]** > **[ドメイン証明書（Domain certificates）]** に移動します。

ステップ 2 CSR を生成するドメインをクリックします。

ステップ 3 **[CSR の作成（Generate CSR）]** をクリックして **[CSR の作成（Generate CSR）]** ページに移動します。

ステップ 4 証明書に必要なプロパティを入力します。

Expressway がクラスタの一部である場合、145 ページのドメイン証明書とクラスタ化システムを参照してください。

ステップ 5 [Generate CSR] をクリックします。システムが署名要求と関連する秘密キーを生成します。秘密キーは、Expressway に安全に保存され、表示またはダウンロードすることはできません。

（注） 認証局に対しても秘密キーを開示してはなりません。

ステップ 6 「**ドメイン証明書（Domain certificate）**」ページに戻ります。グローバル設定に関して実行できることは次のとおりです。

- 認証局に送信できるように、要求をローカルファイルシステムにダウンロードします。ファイルを保存するよう求められます（実際の表現はブラウザによって異なります）。
- 現在の要求の表示（人間可読形式で表示するには **[Show (decoded)]** をクリック、または raw 形式でファイルを表示するには **[Show (PEM file)]** をクリックします）。

新しいドメイン証明書のアップロード

署名付きドメイン証明書が認証局から送り戻されたら、Expressway にアップロードする必要があります。**[新規証明書のアップロード（Upload new certificate）]** セクションを使用して、現在のドメイン証明書を新しい証明書に置き換えます。

ステップ 1 **[メンテナンス（Maintenance）]** > **[セキュリティ（Security）]** > **[ドメイン証明書（Domain certificates）]** に移動します。

ステップ 2 **[新規証明書のアップロード（Upload new certificate）]** セクションの **[参照（Browse）]** ボタンを使用して、ドメイン証明書の PEM ファイルを選択し、アップロードします。

ステップ 3 外部システムを使用して CSR を生成する場合は、ドメイン証明書を暗号化するために使用した、サーバ秘密キー PEM ファイルもアップロードする必要があります。（Expressway を使用して、このドメイン証明書用の CSR が作成された場合、秘密キー ファイルは、前もって自動的に生成および保存されます）。

- サーバ秘密キー PEM ファイルはパスワードで保護しないでください。
- 証明書署名要求の進行中は、サーバ秘密キーをアップロードできません。

ステップ 4 [ドメイン証明書データのアップロード（Upload domain certificate data）] をクリックします。

自動証明書管理環境サービス

バージョン X12.5 から、Expressway-E の自動証明書管理環境（ACME）サービスは、（SNI で使用される）ドメイン証明書を要求して導入できます。

[メンテナンス（Maintenance）] > **[セキュリティ（Security）]** > **[ドメイン証明書（Domain certificates）]** に移動すると、ドメインのリストの **[ACME]** 列に、各ドメインの ACME サービスのステータスが示されます。

ACME サービスを有効にするドメイン名の横にある **[表示/編集（View/Edit）]** をクリックします。

ドメイン証明書用に ACME サービスを設定するプロセスは、サーバ証明書用に設定する場合と同じで、Expressway-E インターフェイスで使用する場所が異なるだけです。

Expressway 構成ガイドページの『*Cisco Expressway* 証明書作成および使用導入ガイド』を参照してください。

ドメイン証明書とクラスタ化システム

CSR の生成時には、1 つの要求および秘密キーの組み合わせがそのピア専用に生成されます。

Expressway のクラスタがある場合は、各ピアで個別の署名要求を生成する必要があります。これらの要求はその後、認証局に送信し、返されたドメイン証明書を関連する各ピアにアップロードする必要があります。

（注） 正しいドメイン証明書が適切なピアにアップロードされていることを確認する必要があります。そうでないと、各ピアに保存された秘密キーがアップロードされた証明書に対応しません。

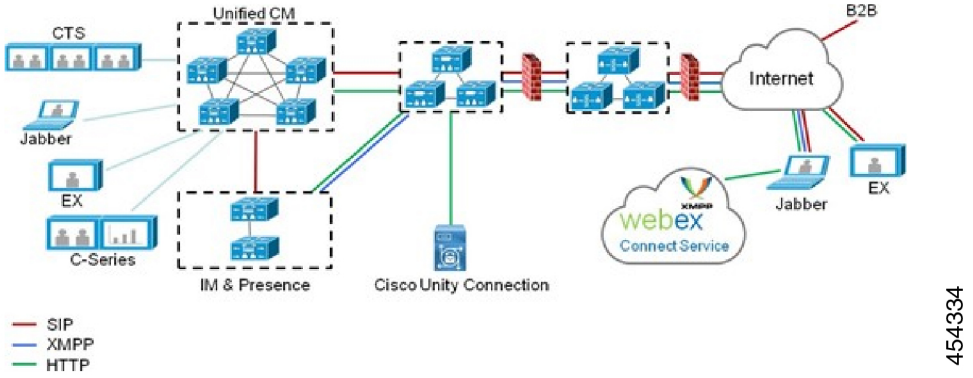
モバイルおよびリモート アクセスの概要

Cisco Unified Communications の Mobile & Remote Access は Cisco Collaboration Edge アーキテクチャの中核を成します。Cisco Jabber などのエンドポイントが企業ネットワーク外にある場合に、Cisco Unified Communications Manager（Unified CM）への登録、呼制御、プロビジョニング、メッセージング、およびプレゼンスの機能を使用することができるようになります。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。

ソリューション全体で、次の機能が提供されます。

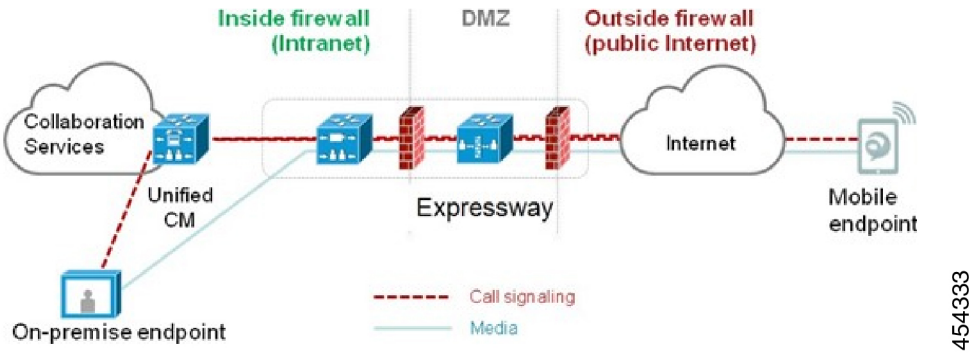
- **オフプレミスアクセス**：企業ネットワーク外においても、JabberおよびEX/MX/SXシリーズ クライアントで一貫したエクスペリエンスを提供。
- **セキュリティ**：セキュアな Business-to-Business（B2B）コミュニケーション
- **クラウドサービス**：エンタープライズクラスの柔軟性と拡張性に優れたソリューションにより、さまざまな Cisco Webex 統合およびサービス プロバイダ オファリングに対応。
- **ゲートウェイと相互運用性サービス**：メディアおよびシグナリングの正規化、非標準エンドポイントのサポート

図 *3 : 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トランクを介して統合されたCM登録デバイスと相互運用することもできます。

図 *4:* 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コール制御を提供します。

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 ソリューションを横断します。Expressway ソリューションをトラバースするメディアは、エンドポイント間で直接中継されます。

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。

導入範囲

次の主要な Expressway ベースの導入は機能しません。これらを同じ Expressway（またはトラバーサル ペア）で一緒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

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ページに用意されている『*Cisco Expressway IP Port Usage Configuration Guide*』を参照してください。このガイドに、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使用できるポートが記載されています。

VPN を使用しない Jabber クライアント接続

MRA ソリューションでは、ハイブリッド オンプレミス サービス モデルとクラウドベースのサービス モデルをサポートしています。これは、社内および社外で一貫したエクスペリエンスを提供します。MRA は、VPN で企業ネットワークに接続せずに Jabber アプリケーション トラ

フィックのセキュアな接続を提供します。Windows、Mac、iOS および Android プラットフォームでデバイスとオペレーティング システムに依存しない Cisco Jabber クライアントの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。

- インスタント メッセージングおよびプレゼンス 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

詳細な設定情報の取得場所

MRA 用に Expressway を使用する方法について詳しくは、「Expressway 設定ガイド」ページの『*Cisco Expressway* を使用したモバイルおよびリモートアクセス』を参照してください。このガイドでは、以下について説明します。

- Expressway-C と Expressway-E で MRA 機能を有効にして設定する方法。
- MRA サービスで使用する Unified CM サーバと IM&P サーバを検出する方法。
- MRA アクセス制御（認証の設定、SAML SSO、許可リストを含む）。
- プッシュ通知のサポートを有効にする方法

Expressway による XMPP フェデレーション

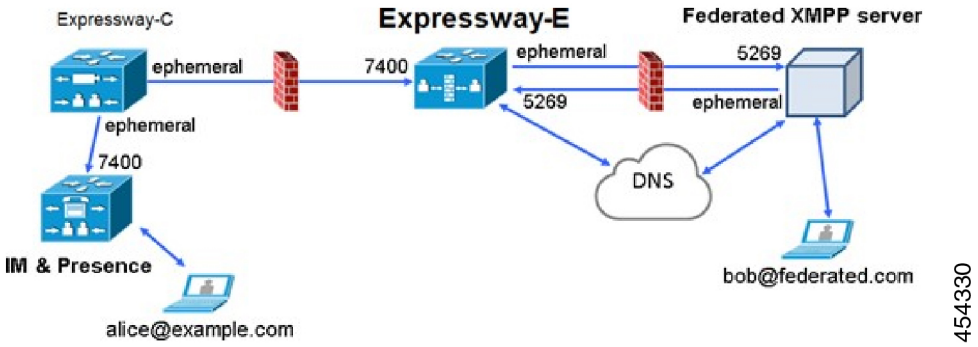
外部 XMPP フェデレーションでは、Cisco Unified Communications Manager IM and Presence Service に登録されたユーザが、異なる XMPP 導入環境からのユーザと Cisco Expressway-E を介して通信できます。

（注） このセクションでは、Expressway を使用して管理する XMPP フェデレーションについて説明しますが、このガイドで後述するように、IM and Presence Service を使用して管理することもできます。

次の図は、オンプレミス IM & Presence サーバから Expressway-C および Expressway-E コラボレーション エッジ ソリューションを介してフェデレーテッド XMPP サーバにルーティングされる XMPP メッセージを示しています。また、メッセージが DMZ ファイアウォールを通過するときに使用される接続とポートも示しています。「「example.com」」組織では Expressway

フェデレーション モデル（図の左側）を使用し、一方、「「federated.com」」組織（図の右側）では DMZ フェデレーション モデルの IM and Presence Service を使用しています。

図 *5 : XMPP* 連邦に対するメッセージのルーティング



サポートされるシステム

Expressway-E は次の製品との XMPP フェデレーションをサポートしています。

- Expressway X8.2 以降
- Cisco Unified Communications Manager IM and Presence Service 9.1.1 以降
- Cisco Webex Connect リリース 6.x
- Cisco Jabber 9.7 以降
- その他の XMPP 標準準拠サーバ

制限事項

- Expressway を XMPP フェデレーションに使用する場合、Expressway-E はリモート フェデレーション サーバへの接続を処理し、Jabber ID のみを使用して XMPP メッセージを管理できます。Expressway-E は（電子メール アドレスなどの）XMPP のアドレス変換をサポートしません。

  外部ユーザとして、フェデレーションを介して企業内のユーザとチャットを試みる場合は、エンタープライズユーザの Jabber ID を使用して XMPP を介してユーザと連絡をとる必要があります。エンタープライズ ユーザの Jabber ID が電子メール アドレスと一致しない場合（特に Jabber ID に内部ユーザの ID またはドメインを使用している場合）、エンタープライズ ユーザの電子メール アドレスがわからないため、フェデレーションを設定することはできません。このため、Expressway を XMPP フェデレーションに使用する場合、企業は Unified CM ノードを設定して、ユーザの Jabber ID と電子メールに同じアドレスを使用することを推奨します。この制限は、フェデレーションが Expressway-E で処理されているとしても、企業内で（フェデレーションを使用せず）互いに連絡を取り合うユー

ザには適用されません。このようなフェデレーションされていないユース ケースでは、Jabber ID またはディレクトリ URI（通常は電子メール）を使用するように IM and Presence Service を設定できます。

ユーザの Jabber ID をユーザの電子メール アドレスに似せて、フェデレーテッド パートナーがフェデレーション用に電子メールアドレスを近いものにできるようにするには、次のように設定します。

a. ユーザ ID がユーザの sAMAccountName になるように、Unified CM Lightweight Directory Access Protocol（LDAP）属性を設定。

b. 電子メール ドメインと同じになるように Unified CM IM and Presence Service プレゼンス ドメインを設定。

c. samaccountname@presencedomain と同じになるように電子メール アドレスを設定。

- IM and Presence Service によって管理される内部フェデレーションと Cisco Expressway によって管理される外部フェデレーションは同時にサポートされません。内部フェデレーションのみが必要な場合に、IM and Presence Service 上でドメイン間フェデレーションを使用する必要があります。使用可能なフェデレーション導入の設定オプションは次のとおりです。
  - 外部フェデレーションのみ（Expressway で管理）。
  - 内部フェデレーションのみ（IM and Presence Service によって管理）。
  - IM and Presence Service によって内部および外部フェデレーションが管理されますが、インバウンド接続を許可するようにファイアウォールを設定する必要があります。

前提条件

- Expressway 上で XMPP フェデレーションを有効にする前に、IM and Presence Service 上のドメイン間 XMPP フェデレーションが**無効**にされている必要があります。

  [Cisco Unified CM IM and Presence サービス管理（Cisco Unified CM IM and Presence Service Administration）] > [プレゼンス（Presence）] > [ドメイン間フェデレーション（Inter Domain Federation）] > [XMPP フェデレーション（XMPP Federation）] > [設定（Settings）] に移動して、**[XMPP フェデレーション ノードのステータス（XMPP Federation Node Status）]** が *[オフ（Off）]* に設定されていることを確認します。

- XMPP フェデレーションは単一の Expressway クラスタでのみサポートされます。
- Expressway-C（クラスタ）と Expressway-E（クラスタ）は、『*Mobile and Remote Access via Cisco Expressway Deployment Guide*』で説明されているように、ユニファイド コミュニケーション サービスに対するモバイルおよびリモート アクセス用に設定する必要があります。XMPP フェデレーションのみが必要となる場合（Unified CM へのビデオ コールとリモート登録は不要な場合）、次の項目を設定する必要はありません。
  - *Unified CM* 上での *SIP* 登録とプロビジョニングをサポートするドメイン、または *Unified CM* 上での *IM and Presence Service* をサポートするドメイン。

- Unified CM サーバ（IM&P サーバは設定する必要があります）。
- HTTP サーバ許可リスト。

（注） フェデレーテッドコミュニケーションは、オンプレミスクライアント（IM and Presence Service に直接接続）とオフプレミスクライアント（MRA を介して IM and Presence Service に接続）の両方で使用できます。

- SIP および XMPP フェデレーションは独立していて、相互に影響を与えません。たとえば、IM and Presence サービスの SIP フェデレーションと Expressway の外部 XMPP フェデレーションを展開することができます。
- Expressway を通じて外部 XMPP フェデレーションを導入する場合、IM and Presence Service に対して Cisco XCP XMPP Federation Connection Manager 機能サービスをアクティブ化しないでください。
- Transport Layer Security（TLS）とグループ チャットの両方を使用する場合は、Expressway-C および Expressway-E サーバ証明書のサブジェクト名代替名リストに、IM and Presence Service サーバで設定された**チャット ノード エイリアス**を含める必要があります。XMPPAddress または DNS の形式を使用します。

（注） Expressway-C は、一連の IM and Presence Service サーバを検出すると、その証明書署名要求（CSR）にチャット ノード エイリアスを自動的に含めることに注意してください。Expressway-E 用の CSR を生成する場合は、Expressway-C 対応の「**CSR の作成（Generate CSR）**」ページからチャット ノード エイリアスをコピー、ペーストすることを推奨します。

設定情報の詳細

IM and Presence Service で管理する XMPP フェデレーションの設定については、『Cisco Unified Communications Manager の IM and Presence Service 用インタードメインフェデレーション』を参照してください。

Expressway で管理する XMPP フェデレーションの設定については、Expressway 設定ガイド ページの『*XMPP* フェデレーションに関する *Expressway* または *IM and Presence Service* の使用方法』を参照してください。

Cisco XCP ルータの遅延再起動

Cisco Hosted Collaboration Solution（HCS）の一部である、Cisco XCP ルータの遅延再起動機能は、Expressway-E がマルチテナント モードの場合にのみ使用できます。新しい SIP ドメインを持つ 2 つ目の Unified CM トラバース ゾーンを追加すると、Expressway-E はマルチテナント モードに入ります。

（注） マルチテナントモードでは、Cisco Expressway-E の **[システム（System）]** > **[DNS]** ページで、DNS に設定されているホスト名と一致するようにシステムのホスト名を設定する必要があります（X8.10.1 より前では大文字と小文字が区別されます。X8.10.1 以降は大文字と小文字は区別されません）。このようにしなければ、Cisco Jabber クライアントを MRA に正常に登録できません。

マルチテナンシーにより、サービス プロバイダーは複数のテナント間で Expressway-E クラスタを共有できます。各テナントには、共有 Expressway-E クラスタに接続する専用の Expressway-C クラスタがあります。

Expressway-E クラスタ、または顧客の Expressway-C クラスタで特定の設定を変更すると、共有クラスタ内の各 Expressway-E で Cisco XCP ルータを再起動する必要があります。マルチテナント Expressway-E クラスタのすべてのノードにわたって Cisco XCP ルータの設定の変更が有効になるには、再起動が必要です。再起動は、すべての顧客のすべてのユーザに影響します。

この再起動の頻度およびユーザへの影響を軽減するには、Cisco XCP ルータの遅延再起動機能を使用できます。

（注） 遅延再起動機能が有効になっていない場合、再起動は自動的に行われ、Cisco XCP ルータに影響を与える構成変更を保存するたびに発生します。複数の設定変更が必要な場合に、Cisco XCP ルータを数回再起動すると、ユーザに悪影響を及ぼす可能性があります。マルチテナントのお客様は、Cisco XCP ルータの遅延再起動機能を有効にすることを強く推奨します。

詳細については、Expressway 構成ガイドページの『*Cisco Unified Communications XMPP Federation using IM and Presence Service or Expressway*』を参照してください。

Jabber Guest サービスの概要

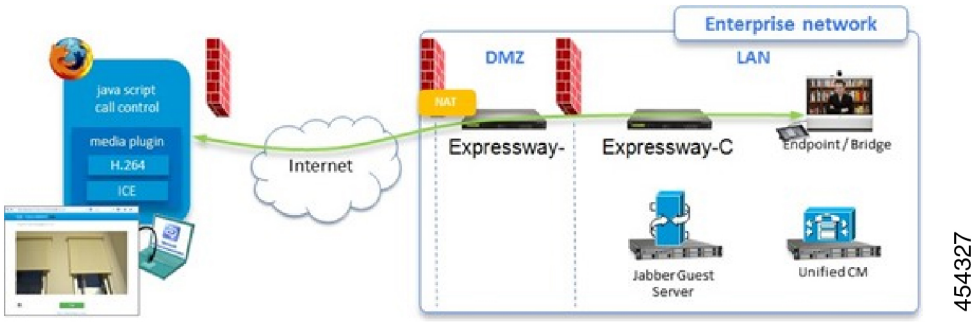
Cisco Jabber Guest は消費者企業間（C2B）ソリューションであり、電話機を Cisco Unified Communications Manager で登録していない企業のファイアウォール外の人々にシスコの企業テレフォニー範囲を拡張します。

これにより、外部ユーザはハイパーリンク（電子メールまたは Web ページ内）をクリックすると、H.264 プラグインをユーザのブラウザにダウンロードし、インストール（最初の使用時）

することができます。次に、ユーザは http ベースのコール制御を使用して URL を「「ダイヤル」」し、企業内に事前に定義された宛先にコールを発信します。ユーザがアカウントを開いたり、パスワードを作成したり、あるいは認証を行ったりする必要はありません。

コールを発信するには、インターネット内の Jabber Guest クライアントと企業内の Jabber Guest サーバ間のファイアウォールを通過して宛先のユーザエージェント（エンドポイント）に到達するために、Expressway ソリューションをユニファイド コミュニケーションのゲートウェイ（Expressway-C と Expressway-E 間のセキュアなトラバーサル ゾーン）として使用します。

図 *6 : Jabber Guest* のコンポーネント



情報の範囲

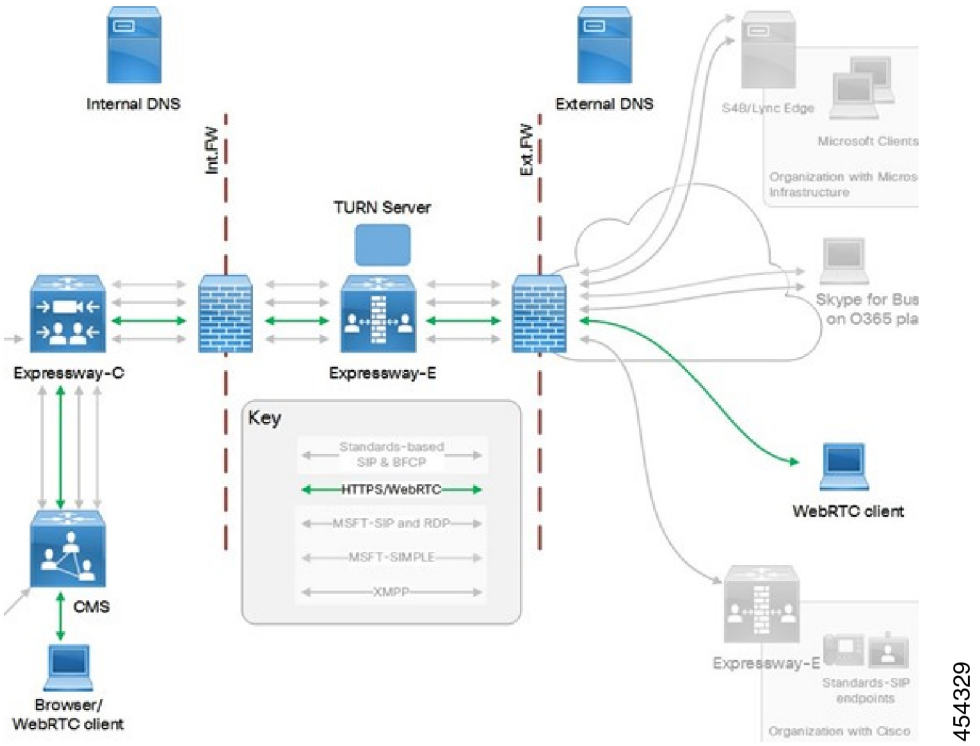
バージョン X8.7 以前では、Jabber Guest の導入に必要な Expressway のすべての設定項目は管理者ガイドに記載されていました。X8.8 以降から、この情報は個別の導入ガイドに記載されています。Jabber Guest の詳細については、次のドキュメントを参照してください。

- Expressway 設定ガイドのページに用意されている『*Cisco Expressway with Jabber Guest Deployment Guide*』。
- Jabber Guest インストールおよびアップグレードガイドのページに用意されている、ご使用のバージョンに応じた『*Cisco Jabber Guest Server Installation and Configuration Guide*』。
- Jabber Guest メンテナンスおよびオペレーションガイドのページに用意されている、ご使用のバージョンに応じた『*Cisco Jabber Guest Administration Guide*』。
- Jabber Guest リリースノートのページに用意されている、ご使用のバージョンに応じた『*Cisco Jabber Guest Release Notes*』。

Expressway の Meeting Server Web プロキシ

このオプションにより、外部ユーザは各自のブラウザを使用して Meeting Server スペースに参加したり、管理したりすることができます。すべての外部ユーザには、Meeting Server スペースへの URL と Meeting Server にアクセスするためのクレデンシャルが必要です。

図 *7 : Expressway の Meeting Server Web* プロキシ



「Expressway 設定ガイド」ページの『*Cisco Meeting Server* および *Cisco Expressway* 導入ガイド』（旧称『*Cisco ExpresswayTraffic Classification* 導入ガイド』）。

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。