デバイス認証

ここでは、Expressway の認証ポリシーと、**[設定（Configuration）] > [認証（Authentication）]** メニューに表示されるページについて説明します。

デバイス認証について

デバイス認証では、デバイスまたは外部システムから Expressway に届く着信要求のクレデンシャルを検証します。これは、特定の機能を既知のユーザと信頼できるユーザ用に予約できるようにするために使用されます。

Mobile & Remote Access デバイス

Expressway を介して Unified CM に登録するデバイスの認証について、Expressway 上で明示的に設定する必要はありません。（外部 IdP ではなく）Expressway がこれらのデバイスの認証エージェントである場合は、ホーム Unified CM クラスタに対してこれらのデバイスの認証を自動的に処理します。

リッチ メディア セッション

リッチ メディア セッションに参加して、Expressway と通信するデバイスは、Expressway の設定可能な認証ポリシーの対象となります。

デバイス認証が有効になっている場合、その Expressway との通信を試みるデバイスはすべて、クレデンシャル（通常はユーザ名とパスワードに基づく）の提示を要求されます。Expressway はそれらのクレデンシャルをローカル データベースを使用するための認証の設定と照合します。

Expressway 認証ポリシーは、各ゾーンにそれぞれ独立して設定できます。つまり、認証済みと未認証の両方のデバイスに対して同じ Expressway への通信を必要に応じて許可することが可

能です。後続のコールルーティングの決定には、デバイスが認証されているかどうかに基づいたさまざまなルールを設定できます。

認証ポリシー（Authentication policy）

認証ポリシーの設定オプション

認証ポリシーの動作は、H.323 メッセージ、ローカル ドメインから受信した SIP メッセージ、および非ローカル ドメインから受信した SIP メッセージであるかによって異なります。

プライマリ認証ポリシーの設定オプションおよびそれぞれに関連付けられている動作は以下のとおりです。

- **[クレデンシャルを確認する（Check credentials）]**：該当する認証方式を使用してクレデンシャルを検証します。

  （注） 一部のシナリオでは、メッセージはチャレンジされません。以下を参照してください。

- **[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せずに、メッセージを処理します。
- **[認証済みとして扱う（Treat as authenticated）]**：クレデンシャルを確認せず、認証済みであるかのようにメッセージを処理します。このオプションは、それぞれの登録メカニズム内で認証をサポートしていないサードパーティ サプライヤからのエンドポイントに対応するために使用できます。

  （注） 一部のシナリオでは、メッセージは許可されても、未認証であるかのように扱われることがあります。以下を参照してください。

認証ポリシーは、メッセージを受信しているかどうかに基づき、ゾーン タイプごとに選択して設定できます。

- デフォルト ゾーン、ネイバー ゾーン、トラバーサル クライアント ゾーン、トラバーサル サーバ ゾーン、およびユニファイド コミュニケーション トラバーサル ゾーンはすべて、認証ポリシーを設定できます。
- DNS ゾーンと ENUM ゾーンはメッセージを受信しないため、認証ポリシーの設定はありません。

ゾーンの [認証ポリシー（Authentication policy）] を編集するには、**[設定（Configuration）]** > **[ゾーン（Zones）]** > **[ゾーン（Zones）]** に移動して、ゾーンの名前をクリックします。新しい

ゾーンを作成すると、ポリシーはデフォルトで *[クレデンシャルを確認しない（Do not check credentials）]* に設定されます。

以下の表に示されているように、H.323 メッセージと SIP メッセージの動作は異なります。

H.323

ポリシー	動作
クレデンシャルを確認する（Check credentials）	メッセージは、メッセージ内のいずれかのクレデンシャルを認証データベースで確認できるかどうかによって、認証済みまたは未認証として分類されます。 クレデンシャルが提供されていない場合、メッセージは常に未認証として分類されます。
クレデンシャルを確認しない（Do not check credentials）	メッセージのクレデンシャルはチェックされず、すべてのメッセージが未認証として分類されます。
認証済みとして扱う（Treat as authenticated）	メッセージのクレデンシャルはチェックされず、すべてのメッセージが認証済みとして分類されます。

SIP

ゾーン レベルでの SIP メッセージの動作は、SIP 認証信頼 の設定によって異なります。つまり、Expressway が受信メッセージに含まれている P-Asserted-Identity ヘッダーと呼ばれる既存の認証済みインジケータを信頼するかどうか、およびメッセージをローカル ドメイン（Expressway が信頼するドメイン）から受信したか、非ローカル ドメインから受信したかによって異なります。

ポリシー	信頼性	ローカル ドメイン内	ローカル ドメインの外
クレデンシャルを確認する（Check credentials）	オフ（Off）	メッセージは認証をチャレンジされます。 認証に失敗したメッセージは拒否されます。 認証に合格したメッセージは認証済みとして分類され、P-Asserted-Identity ヘッダーがメッセージに挿入されます。	メッセージは認証をチャレンジされません。 すべてのメッセージが未認証として分類されます。 既存の P-Asserted-Identity ヘッダーは削除されます。

ポリシー	信頼性	ローカル ドメイン内	ローカル ドメインの外
	オン（On）	既存の P-Asserted-Identity ヘッダーがあるメッセージは、追加のチャレンジなしに認証済みとして分類されます。P-Asserted-Identity ヘッダーは変更されずに渡されます（発信者の Asserted IDを保持）。 既存の P-Asserted-Identity ヘッダーがないメッセージはチャレンジされます。認証に合格すると、メッセージは認証済みとして分類され、P-Asserted-Identity ヘッダーがメッセージに挿入されます。認証に失敗すると、メッセージは拒否されます。	メッセージは認証をチャレンジされません。 既存の P-Asserted-Identity ヘッダーがあるメッセージは、認証済みとして分類され、ヘッダーは変更されずに渡されます。 既存の P-Asserted-Identity ヘッダーがないメッセージは未認証として分類されます。
クレデンシャルを確認しない（Do not check credentials）	オフ（Off）	メッセージは認証をチャレンジされません。 すべてのメッセージが未認証として分類されます。 既存の P-Asserted-Identity ヘッダーは削除されます。	メッセージは認証をチャレンジされません。 すべてのメッセージが未認証として分類されます。 既存の P-Asserted-Identity ヘッダーは削除されます。
	オン（On）	メッセージは認証をチャレンジされません。 既存の P-Asserted-Identity ヘッダーがあるメッセージは、認証済みとして分類され、ヘッダーは変更されずに渡されます。 既存の P-Asserted-Identity ヘッダーがないメッセージは未認証として分類されます。	メッセージは認証をチャレンジされません。 既存の P-Asserted-Identity ヘッダーがあるメッセージは、認証済みとして分類され、ヘッダーは変更されずに渡されます。 既存の P-Asserted-Identity ヘッダーがないメッセージは未認証として分類されます。
認証済みとして扱う（Treat as authenticated）	オフ（Off）	メッセージは認証をチャレンジされません。 すべてのメッセージが認証済みとして分類されます。 既存の P-Asserted-Identity ヘッダーは削除され、Expressway の発信者 ID を含む新しいヘッダーがメッセージに挿入されます。	メッセージは認証をチャレンジされません。 すべてのメッセージが未認証として分類されます。 既存の P-Asserted-Identity ヘッダーは削除されます。

ポリシー	信頼性	ローカル ドメイン内	ローカル ドメインの外
	オン（On）	メッセージは認証をチャレンジされません。 すべてのメッセージが認証済みとして分類されます。 既存の P-Asserted-Identity ヘッダーがあるメッセージは変更されずに渡されます。既存の P-Asserted-Identity ヘッダーがないメッセージにはヘッダーが挿入されます。	メッセージは認証をチャレンジされません。 既存の P-Asserted-Identity ヘッダーがあるメッセージは、認証済みとして分類され、ヘッダーは変更されずに渡されます。 既存の P-Asserted-Identity ヘッダーがないメッセージは未認証として分類されます。

認証済みデバイスおよび未認証デバイスに対するシステム動作の制御

認証済みデバイスおよび未認証デバイスからのコールおよびその他のメッセージの処理方法は、検索ルール、外部ポリシー サービス、および CPL の設定内容によって異なります。

検索ルール

検索ルールを設定する場合は、**[要求は認証が必要（Request must be authenticated）]** 属性を使用して、検索ルールが認証済みの検索要求にのみ適用されるのか、またはすべての要求に適用されるのかを指定します。

外部ポリシー サービス

外部ポリシー サービスは、通常、Expressway 自体にポリシー ルールを設定するのではなく、外部の集中型サービスによってポリシー決定が管理される導入で使用されます。次の領域でポリシー サービスを使用するように、Expressway を設定できます。

- 登録ポリシー
- 検索ルール（ダイヤル プラン）
- コール ポリシー
- ユーザ ポリシー（FindMe）

Expressway は、ポリシー サービスを使用するときに、コール要求または登録要求に関する情報を POST メッセージでそのサービスに送信します。その際、名前と値のペアで構成される一連のパラメータを使用します。それらのパラメータには、要求の送信元が認証済みソースかどうかの情報が含まれています。

Cisco Expressway シリーズ構成ガイドページの『*Cisco Expressway* 外部ポリシー導入ガイド』を参照してください。

CPL

Expressway でコール ポリシー ルール ジェネレータを使用している場合、送信元の照合は、認証済みソースに対して実行されます。未認証のソースに対する照合を指定するには、空白フィールドを使用します。（送信元が認証されていない場合、その値は信頼できません）。

手作業で作成し、アップロードしたローカル CPL を使用してコール ポリシーを管理する場合は、認証済みと未認証のいずれの発信元を調べるかについて CPL を明確にすることを推奨します。

- CPL で未認証の送信元を調べる必要がある場合（たとえば、非認証の発信者をチェックする場合）は、「`unauthenticated-origin`」を使用する必要があります。（ただし、未認証のユーザは、自らを好きなように呼ぶことができるため、このフィールドでは、発信者は確認されません）。
- 認証済みの送信元（認証済みデバイスまたは「「認証済みとして扱う」」デバイスでのみ可能）をチェックするには、CPL で「`authenticated-origin`」を使用する必要があります。

（注） CPL スクリプトの記述は複雑なため、代わりに外部ポリシーサービスを使用することを推奨します。

SIP 認証信頼

デバイス認証についてを使用するように設定されている Expressway では、着信の SIP INVITE 要求が認証されます。その後、Expressway からネイバー ゾーン（別の Expressway など）に要求が転送されると、受信システムでもその要求が認証されます。このシナリオでは、すべてのホップでメッセージを認証する必要があります。

デバイスのクレデンシャルが（最初のホップで）一度だけ認証され、ネットワーク内の SIP メッセージの数が減るように簡素化する場合は、**[認証信頼モード（Authentication trust mode）]** の設定を使用するようにネイバー ゾーンを設定できます。

この設定は、ゾーンの認証ポリシーと組み合わせて使用されて、該当ゾーンから受信した事前認証済みの SIP メッセージが信頼されているかどうか、その後、Expressway 内で認証済みまたは未認証として扱われるかを制御します。事前認証済みの SIP 要求は、RFC 3326 で定義されている SIP メッセージ ヘッダー内の P-Asserted-Identity フィールドの存在によって識別されます。

[認証信頼モード（Authentication trust mode）] の設定は次のとおりです。

- *[オン（On）]*：事前認証済みメッセージは追加のチャレンジなしに信頼され、その後、Expressway内では認証済みとして扱われます。未認証メッセージは、**[認証ポリシー（Authentication policy）]** が *[クレデンシャルを確認する（Check credentials）]* に設定されている場合はチャレンジされます。
- *[オフ（Off）]*：既存の認証済みインジケータ（P-Asserted-Identityヘッダー）はすべてメッセージから削除されます。ローカル ドメインからのメッセージは、**[認証ポリシー**

（**Authentication Policy**）] が *[*クレデンシャルを確認する（*Check credentials*）*]* に設定されている場合はチャレンジされます。

（注）
- 認証信頼は、ネイバーゾーンが信頼できるSIPサーバのネットワークの一部である場合のみ有効にすることを推奨します。
- 認証信頼は、トラバーサル サーバ ゾーンとトラバーサル クライアント ゾーンの間では自動的に暗示されます。

デバイス プロビジョニングと認証ポリシー

プロビジョニング サーバが受信するプロビジョニング要求または電話帳要求は、Expressway へのゾーンまたはサブゾーン エントリ ポイントにおいて、すでに認証されている必要があります。プロビジョニング サーバは、自分自身で認証チャレンジを行うことはありません。未認証のメッセージはすべて拒否されます。

Expresswayには、適切なデバイス認証設定が行われている必要があります。そうでなければ、プロビジョニング関連のメッセージは拒否されます。

- （サブスクライブ メッセージ）の初期プロビジョニングの認証は、デフォルト ゾーンの認証ポリシーの設定によって制御されます（デバイスがまだ登録されていないので、デフォルト ゾーンが使用されます）。
- デフォルトゾーンおよびトラバーサルクライアントゾーンの認証ポリシーは、*[*クレデンシャルを確認する（*Check credentials*）*]* または *[*認証済みとして扱う（*Treat as authenticated*）*]* のいずれかに設定されている必要があります。そうでなければ、プロビジョニング要求は失敗します。

それぞれの場合に、Expressway はその認証をローカル データベースと照合して検査を実行します。これには Cisco TMS によって提供されるすべてのクレデンシャルが含まれます。

一般的なプロビジョニング設定の詳細については、『Cisco TMS Provisioning Extension 導入ガイド』を参照してください。

認証方式

ローカル データベースを使用するための認証の設定

ローカル認証データベースは、Expressway システムの一部として組み込まれているため、固有の接続設定は必要ありません。ユーザアカウントの認証クレデンシャルを保存するために使用されます。各クレデンシャルのセットは**名前**と**パスワード**で構成されます。

ローカル データベース内のクレデンシャルは、デバイス（SIP）、トラバーサル クライアント、および TURN クライアントの認証に使用できます。

ローカル データベースへのクレデンシャルの追加

デバイス クレデンシャルのセットを入力するには、次の手順を実行します。

1. **[設定（Configuration）]** > **[認証（Authentication）]** > **[デバイス（Devices）]** > **[ローカル データベース（Local Database）]** に移動し、**[新規（New）]** をクリックします。
2. デバイスのクレデンシャルを表す**名前**と**パスワード**を入力します。
3. **[クレデンシャルの作成（Create credential）]** をクリックします。

（注） 2 台以上のデバイスで同じクレデンシャルを使用することができます。

Cisco TMS 内で管理されるクレデンシャル（デバイス プロビジョニング用）

Expressway が TMS Provisioning Extension サービスを使用している場合、ユーザ サービスから提供されたクレデンシャルは、手動で設定されたエントリとともに、ローカル認証データベースに保存されます。**[ソース（Source）]** カラムにより、ユーザ アカウント名が **TMS** から提供されたものか、**ローカル** エントリであるかが識別されます。編集できるのは、**ローカル** エントリのみです。

ローカル データベース内に Cisco TMS のクレデンシャルを組み込むことで、Expressway は Cisco TMS 内で使用されている同一のクレデンシャルのセットと照合して（プロビジョニング要求だけではなく）すべてのメッセージを認証できます。

H.350 ディレクトリ認証と組み合わせたローカル データベース認証

Expressway は、ローカル データベースと H.350 ディレクトリの両方を使用するように設定できます。

H.350ディレクトリが設定されている場合、Expresswayは、提示されたダイジェストクレデンシャルを検証する際は常に、最初にローカルデータベースと照合してから、H.350ディレクトリと照合します。

Active Directory（直接）認証と組み合わせたローカル データベース認証

Active Directory（直接）認証が設定されていて、[NTLM プロトコル チャレンジ（NTLM protocol challenges）] が *[自動（Auto）]* に設定されている場合、NTLM をサポートするデバイスに NTLM 認証チャレンジが提供されます。

- NTLM チャレンジは標準のダイジェスト チャレンジに加えて提供されます。
- NTLM をサポートするエンドポイントは、ダイジェスト チャレンジに優先して NTLM チャレンジに応答します。Expressway は、その NTLM 応答の認証を試みます。

外部システムによる認証

「アウトバウンド接続クレデンシャル（Outbound connection credentials）」ページ（**[設定（Configuration）]>[認証（Authentication）]>[アウトバウンド接続クレデンシャル（Outbound connection credentials）]**）は、外部システムとの認証が必要な場合にExpresswayが常に使用するユーザ名とパスワードを設定するために使用します。

たとえば、Expressway がエンドポイントから他の Expressway に招待を転送している場合、その別のシステムで認証が有効になっているために、ローカルExpresswayがユーザ名とパスワードをそのシステムに提供する必要があることがあります。

（注） これらの設定はトラバーサルクライアントゾーンでは使用されません。接続前に、トラバーサル サーバと常に認証する必要があるトラバーサル クライアントでは、トラバーサル クライアント ゾーンごとに接続のクレデンシャルを設定します。