Expressway に証明書をキーをロードする

Expressway は、標準の X.509 証明書を使用します。証明書情報は、PEM フォーマットで Expressway に提供される必要があります。通常、次の 3 つの要素がロードされます。

- サーバー証明書（証明書の所有者の ID を識別することで認証局によって生成され、クライアントおよびサーバー両方の証明書として機能できる必要があります）。
- 秘密キー（クライアントに送信されるデータに署名し、サーバー証明書の公開キーで暗号化されたクライアントから送信されたデータを複合化するために使用されます）。これは、Expressway 上でのみ保持し、安全な場所にバックアップする必要があります。TLS 通信のセキュリティはこの保持された秘密に依存します。
- 信頼できる認証局の証明書のリスト。

Note Expressway ソフトウェアの新規インストール（X8.1 以降）には、一時的に信頼された CA とその一時 CA が発行するサーバー証明書が付属します。サーバー証明書を信頼できる認証局により生成された証明書に置き換え、信頼する認証局の CA 証明書をインストールすることを強く推奨します。

Note Expressway-C および Expressway-E では、同じ共通名を持つ複数の CA 証明書をアップロードしないことを推奨します。これは、Expressway が外部 IdP を使用してエンドポイントを認証するように構成されている場合、エンドポイントがログインに失敗する可能性があるためです。

Warning 表示される可能性のある警告メッセージ

X8.10 以降の場合、証明書が特定の基準を満たさない場合、サーバー証明書のアップロードメカニズム（**[メンテナンス（Maintenance）]>[セキュリティ（Security）]>[サーバー証明書（Server certificate）]**）が警告を表示します。警告が表示されるケースは次のとおりです。

- 証明書に許容できるレベルのセキュリティがない。

- 証明書に共通名（CN）属性がない。この場合、アラームも発生します。Expressway サービスが共通名なしで機能しないためです（Cisco Meeting Server の MRA、Jabber Guest、Web プロキシ）。
- 認定機関（CA）または証明書失効リスト（CRL）が認識されていない。

証明書のアップロードは回避されません。

この章では、次の内容について説明します。

Expressway にサーバー証明書と秘密キーをロード

Expressway サーバー証明書は、TLS 暗号化を使用してクライアントシステムと通信するときや HTTPS を使用して Web ブラウザと通信するときに Expressway を識別するために使用されます。

これらの手順と Cisco TAC エンジニアが提供するプロセスのビデオデモは、[Expressway/VCS スクリーンキャスト ビデオ リスト（Expressway/VCS Screencast Video List）] ページにあります。

（注） サーバー証明書をインストールする前に、CA証明書をインストールすることをお勧めします。そうしないと、サーバー証明書のロードに失敗します。

サーバ証明書をアップロードするには、次の手順を実行します。

1. **[メンテナンス（Maintenance）]** > **[セキュリティ（Security）]** > **[サーバー証明書（Server certificate）]** の順に選択します。
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**サーバ証明書** PEM ファイルを選択し、アップロードします。

（注） 有効な FQDN を使用してサーバー証明書ファイルをアップロードしてください。

1. [SAN] フィールドのホスト名または IP を使用して証明書をアップロードする場合は、「File upload failed.: Subject alternative name must be a valid FQDN」 というエラーが表示されアップロードに失敗します。
2. CN（共通名）のホスト名またはIPを使用して証明書をアップロードする場合は、「File upload failed.: Common name must be a valid FQDN」 というエラーが表示されアップロードに失敗します。

3. 証明書署名要求（証明書署名要求）を生成するために外部システムを使用した場合は、サーバー証明書を暗号化するために使用された**サーバー秘密キー**の PEM ファイルもアップロード

する必要があります。（Expressway がこのサーバ証明書用の CSR を生成するために使用された場合、秘密キー ファイルがすでに自動的に生成され保存されています。）

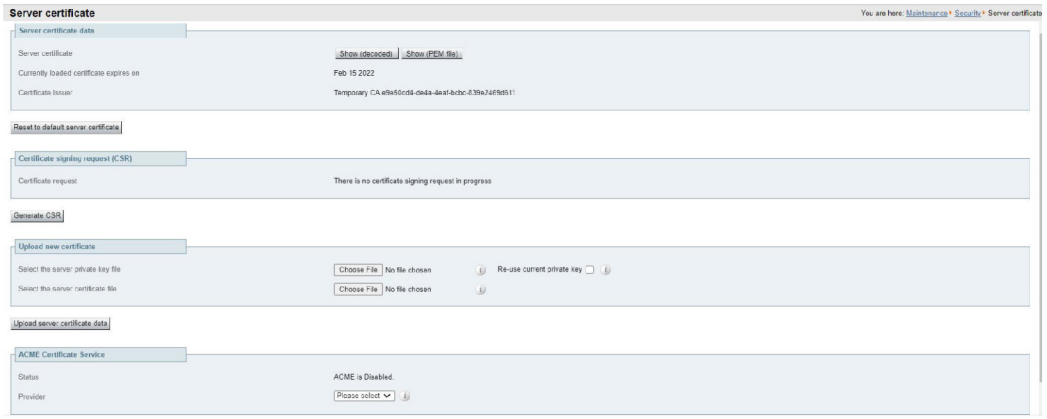
- **サーバー秘密キー** PEM ファイルはパスワードで保護しないでください。
- 証明書署名要求の進行中は、サーバ秘密キーをアップロードできません。

4. [サーバ証明書データのアップロード（Upload server certificate data）] をクリックします。
   - X7 で証明書署名要求を生成する際、アプリケーションは、**証明書署名要求.pem** および **privkey_証明書署名要求.pem** を **/tandberg/persistent/certs** に配置します。
   - X8 で証明書署名要求を生成する際、アプリケーションは、**証明書署名要求.pem** および **privkey.pem** を **/tandberg/persistent/certs/generated_証明書署名要求**に配置します。

   [現在の秘密キーを再利用（Re-use current private key）] チェックボックス ー 新しい秘密キーが不要な場合は、ローカルセキュリティ要件に従い、**[現在の秘密キーを再利用（Re-use current private key）]** チェックボックスをオンにします。現在の証明書の有効期間を延長する場合や、以前に生成された証明書署名要求を再発行する場合には、これを行うことができます

5. **[ACME 証明書サービス（ACME Certificate Service）]** セクションの **[プロバイダー（Provider）]** ドロップダウンリストを使用して、証明書署名要求の署名に使用する信頼できる ACME クライアントを選択します。

X7からアップグレードし、未送信の証明書署名要求が必要な場合は、アップグレードする前に証明書署名要求を破棄し、アップグレード後に証明書署名要求を再生成することを推奨します。

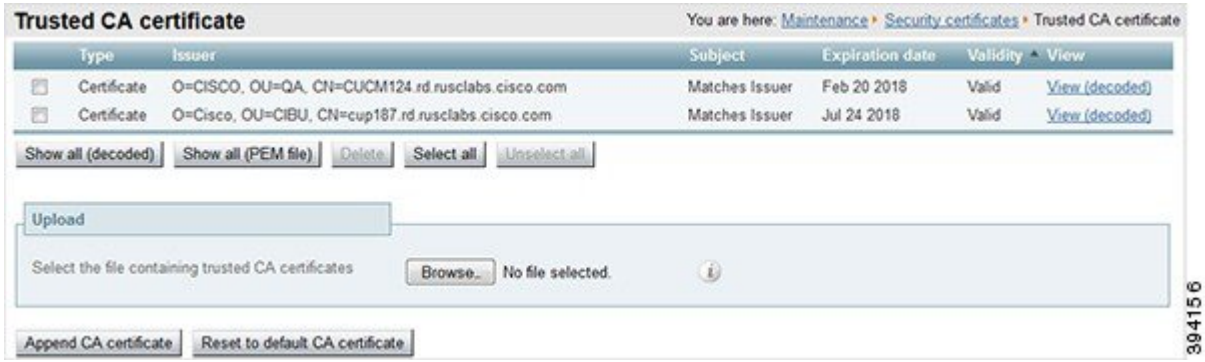


信頼された CA 証明書リストの管理

[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）]**）で、この Expressway が信頼する証明局（CA）の証明書のリストを管理できます。Expressway へ

の TLS 接続が証明書検証を要求したときは、Expressway に提示された証明書が、このリストの信頼できる CA によって署名され、ルート CA に対する完全なトラスト チェーン（中間 CA）がある必要があります。

- 1つ以上のCA証明書を含む新しいファイルをアップロードするには、[参照（Browse）] をクリックして必要な PEM ファイルの場所を指定し、[CA 証明書の追加（Append CA certificate）] をクリックします。これにより、新しい証明書がCA証明書の既存リストに加えられます。特定の発行者およびサブジェクトの既存の証明書を交換する場合は、手動で以前の証明書を削除する必要があります。
- 現在アップロードされたすべての CA 証明書をシステムの信頼できる CA 証明書の元のリストと交換するには、[Reset to default CA certificate] をクリックします。
- 現在アップロードされた信頼できるCA証明書のリスト全体を表示する場合、人間可読形式で表示するには **[Show all (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 all (PEM file)]** をクリックします
- 個別の信頼できる CA 証明書を表示するには、特定の CA 証明書の行で **[表示（復号化）（View (decoded）]** をクリックします。
- 1 つ以上の CA 証明書を削除するには、該当する CA 証明書の隣にあるボックスにチェックを入れて、[Delete] をクリックします。



注：これは推奨事項です。

Expressway の信頼ストアにアップロード/対応できる認証局（CA）の最大数は、1000 です。

既存サーバー証明書の変更

Important “既存のサーバー証明書の変更”に関するこの手順は、“Let's Encrypt” 認証局によって生成されたサーバー証明書には適用されません。

Before you begin

サーバー証明書を変更する前に、証明書署名要求（証明書署名要求）を生成します。詳細については、「証明書署名要求の生成」を参照してください。

Note サーバー証明書を変更する前に、[Transport Line Signaling (TLS) 検証（Transport Line Signaling (TLS) verify）] モードを *[許可（Permissive）]* に設定します。これにより、証明書の変更中に発生したエラーから保護されます。変更後、[TLS 検証（TLS verify）] モードを *[強制（Enforce）]* に戻します。

Procedure

Step 1 クラスタ内のすべてのノードに新しい信頼できる CA 証明書を追加します。

Step 2 **[システム（System）] > [クラスタリング（Clustering）]** の順に選択し、[TLS 検証（TLS Verification）] モードを、*[強制（Enforce）]* に設定し、[TLS 検証（TLS Verification）] を *[許可（Permissive）]*に変更します。**[Save]** をクリックします。

Step 3 クラスタ内のすべてのノードでサーバー証明書を更新します。

Step 4 一度に 1 つずつノードを再起動します。

Note 次のノードを再起動する前に、各ノードが回復できるようにします。

Step 5 ステップ 2 で [TLS 検証（TLS Verification）] モードを *[強制（Enforce）]* から *[許可（Permissive）]* に変更した場合は、**捨てプロンプト 2** で、*[強制（Enforce）]* に戻します。

Step 6 不要になった CA 証明書は削除します。

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。