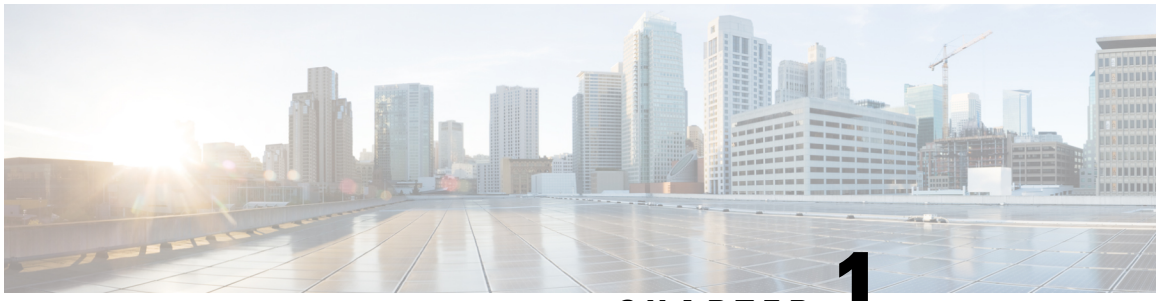
Cisco Expressway 証明書作成および仕様に関する導入ガイド（X14.3）

First Published: 2023-03-12

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS



CHAPTER 1

このマニュアルについて

Important ソフトウェアバージョン X12.5 以降の新機能は、Cisco TelePresence Video Communication Server（VCS）製品ではサポートされません。これらの新機能は Cisco Expressway シリーズ製品（Expressway）にのみ適用されます。このソフトウェアバージョンはメンテナンスおよびバグ修正のみを目的として VCS に用意されています。

バージョン X12.5 以降、このガイドは、Cisco Expressway シリーズ（Expressway）製品のみに適用され、Cisco TelePresence Video Communication Server（VCS）製品には適用されなくなります。Cisco.com の古い VCS は、各ガイドのタイトル ページで指定されている VCS バージョンで引き続き有効です。

この導入ガイドでは、Cisco Expressway（Expressway）で使用する X.509 暗号化証明書を作成する方法と、それを Expressway にロードする方法について説明します。

この章では、次の内容について説明します。

変更履歴

次の表では、製品で追加または変更された情報について説明します。

表 *1:* 変更履歴

リリース日	変更内容	理由
2023 年 4 月	「Certificate Manager ECDSA サポート」という新しいシナリオを追加。 「証明書署名要求の生成」および「Expressway を使用した証明書署名要求の作成」の項を更新。	X14.3 リリース
2020 年 6 月	「PKI の概要」項から偏った表現を削除。	ドキュメントの訂正
2020 年 6 月	X12.6 用に更新	X12.6 リリース
2020 年 2 月	マルチ SAN 証明書に関する「Expressway を使用した証明書署名要求の作成」項を更新。	ドキュメントの訂正
2019 年 12 月	ACME 証明書サービスを展開するための前提条件を更新。	ドキュメントの訂正
2019 年 4 月	メンテナンスリリース X12.5.2 を更新。	X12.5.2 リリース
2019 年 1 月	ACME 証明書管理の X12.5 用に更新。その他のマイナー修正。	X12.5 リリース
2018 年 9 月	X8.11 が使用できなくなったため、ソフトウェアバージョンを X8.11 から X8.11.1 に変更しました。	X8.11.1 リリース
2018 年 7 月	X8.11 用に更新。	X8.11 リリース（破棄）
2017 年 9 月	999 文字の SAN 制限を削除。	X8.10 リリースで修正済み
2017 年 7 月	サーバー証明書のアップロードに関する新しい警告メッセージの説明を追加。UI メニューパスを変更。VCS バージョンと Expressway バージョンを統合。	X8.10 リリース
2016 年 12 月	MRA 証明書の要件を明確化。	X8.9 リリース
2016 年 6 月	X8.8 用に更新。	X8.8 リリース
2015 年 11 月	新しいテンプレートを適用。X8.7 用に再発行。	
2015 年 7 月	X8.6 用に更新。	
2015 年 4 月	X8.5.2 用に更新。CRL 情報の変更、証明書署名要求生成ページのデフォルト、SAN の 999 文字制限。	
2015 年 1 月	X8.5.1用に更新。ユーザーインターフェイスにダイジェストアルゴリズムを選択させるオプションを導入。デフォルトは、SHA-256（ハッシュアルゴリズム）に設定されている。	

リリース日	変更内容	理由
2014 年 12 月	X8.5 用に再発行。2050 年の日付管理とサポートされていない OID の注釈を挿入。付録 2「OpenSSL のみを使用する証明書の生成」の手順を変更。	
2014 年 7 月	X8.2 用に再発行。Unified Communications 展開時のサーバー証明書用の推奨オプションを変更。	
2014 年 6 月	X8.2 用に再発行。Unified Communications 展開用のサーバー証明書要件を強化。	
2013 年 12 月	Expressway バージョンの初期リリース。 （以前の VCS 専用バージョンとの比較）X8.1 用に更新。「Microsoft OCS を使用した証明書の生成」の付録を削除。「OpenSSL のみを使用する証明書の生成」付録のさまざまな改善と明確化。	

このガイドに記載されていない情報

本書では、次の Expressway 構成のトピックについては説明しません。これらのトピックについては、『*Expressway* 管理者ガイド』を参照してください。

- Expressway で証明書ベースの認証を有効にする方法
- Expressway にプレインストールされているルート CA の詳細
- 最小限の TLS バージョンと暗号スイートの構成方法
- クライアント証明書のテスト方法
- mTLS 証明書の管理（モバイルおよびリモートアクセスの展開）
- マルチテナント用のドメイン証明書とサーバー名表示（ホステッドコラボレーションソリューション展開）

PKI の概要

Public Key Infrastructure（PKI）では、セキュアな通信を確立し（暗号化され完全性が保護される）、ID を確認できるメカニズムが提供されます。基本的な PKI は次のとおりです。

- **公開/秘密キーのペア：**公開キーがサーバーに送信されるデータを暗号化するために使用されますが、そのデータを復号化するには秘密キー（サーバーによって秘密が保持される）のみを使用できます。

- **データの署名**：データは、データおよびサーバーの秘密キーの暗号ハッシュの組み合わせを使用して「署名」できます。クライアントは、サーバーの公開キーと同じハッシュを使用して署名を検証できます。これにより、データが意図したサーバーから送信され、改ざんされていないことが保証されます。
- **証明書**：証明書は、公開キーのラッパーであり、キーの所有者に関する情報を X.509 フォーマットで提供します。これには通常サーバー名と連絡先詳細が含まれます。
- **証明書チェーン**：認証局（CA）は、独自の秘密キーを使用してサーバー証明書に署名します。次に、CA の証明書（公開キー）に対して署名をチェックすることで、証明書が署名されていることを確認できます。Web ブラウザと他のクライアントには、信用する CA 証明書のリストがあり、個々のサーバーの証明書を確認することができます。

Transport Layer Security（TLS）は、TCP/IP ネットワーク上のホスト間のセキュアな TCP 接続を確立する標準メカニズムです。たとえば、セキュアな HTTP（HTTPS）は TLS を使用してトラフィックを暗号化し確認します。TLS 接続を確立するには、次の手順に従います。

1. クライアントがそのキャパシティ（暗号スイートを含む）と乱数を送信し、初期 TCP 接続を確立します。
2. サーバーは、これらキャパシティの選択、その他乱数その証明書に応答します。
3. クライアントは、信頼できる CA がサーバー証明書を発行し（署名し）、廃止されていないかを検証します。
4. クライアントは、サーバーの公開キーで暗号化された「事前秘密」を送信します。
5. この事前秘密は、交換された乱数（リプレイアタックを防ぐため）と組み合わせて、「共有秘密」を生成するために使用されます。この共有秘密は、クライアントとサーバーの間で暗号化されたこの TLS セッションの残りの通信を保持します。

次の項では、これらの PKI コンポーネントを Expressway でどのように使用できるかについて説明します。

Expressway での証明書の使用の概要

Expressway は次に対して証明書を必要とします。

- TLS（HTTPS）接続によるセキュアな HTTP
- SIP シグナリング、エンドポイントおよびネイバーゾーンの TLS 接続
- Unified CM、Cisco TMS、LDAP サーバーおよび syslog サーバーなどの他のシステムへの接続

これは、は信頼された認証局（CA）証明書のリストおよび関連する証明書失効リスト（CRL）を使用して、接続するその他デバイスを検証します。

Expressway は、サーバー証明書と秘密キーを使用して、署名済み証明書を提供し、Expressway がそのデバイスであるという証拠を提示します。これは、Microsoft Lync または Unified CM などのネイバーデバイスおよび Web インターフェイスを使用する管理者が使用できます。

証明書は、Expressway を識別します。これには、名前が含まれ、この名前によって認識されて、トラフィックがルーティングされます。クラスタの一部である場合など、これらの目的でExpressway が複数の名前によって認識される場合は、RFC5922 のガイダンスに従って X.509 のサブジェクトデータでこれを表す必要があります。証明書には、Expressway 自体とクラスタの両方の FQDN が含まれている必要があります。次のリストには、選択された導入モデルに応じて X.509 サブジェクトに含める必要があるものを示します。

Expressway がクラスタ化されない場合：

- サブジェクトの共通名 = Expressway の FQDN
- サブジェクトの代替名 = 空欄のまま*

Expressway がクラスタ化され、Expressway ごとに個別の証明書がある場合：

- サブジェクトの共通名 = クラスタの FQDN
- サブジェクトの代替名 = Expressway ピアの FQDN とクラスタの FQDN*

[サーバー証明書（Server certificate）] ページ（**[メンテナンス（Maintenance）] > [セキュリティ（Security）] > [サーバー証明書（Server certificate）]**）から Expressway のサーバー証明書を管理します。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 を識別するためにこの証明書を使用します。「サーバ証明書（Server 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
- 証明書署名要求の生成
- 新しいサーバ証明書のアップロード

証明書生成の概要

X.509 証明書がサードパーティから提供されることがあります。または、OpenSSL などの証明書発行システムやMicrosoft認証局などのアプリケーションで使用できるツールで生成されることがあります。管理された環境またはテスト環境での Expressway の導入では内部で生成された証明書を使用できますが、認識された認証局から提供されたサードパーティ証明書を推奨します。

Expressway は Automated Certificate Management Environment（ACME）もサポートしており、*Let's Encrypt*® 認証局によって署名された証明書を自動的に要求して展開するように設定できます。

Cisco Expressway の以前のリリースでは、RSA 証明書のみがサポートされていました。ただし、Cisco Expressway X14.3 リリース以降では、楕円曲線デジタル署名アルゴリズム（楕円曲線 DSA）証明書が既存の RSA 証明書とともに追加されています。

証明書マネージャでは、キー長の値が異なる ECDSA 証明書の生成がサポートされています。

Cisco Expressway を更新またはインストールすると、自己署名証明書が生成されます。

証明書生成には通常 3 段階のプロセスがあります。

- ステージ 1：秘密キーの生成
- ステージ 2：証明書要求の作成
- ステージ 3：証明書の承認と作成

本書では、ルート証明書、Expressway用のクライアント/サーバー証明書、および秘密キーを生成する代替方法を提示します。

- 証明書署名要求の生成では、Expressway 自体を使用して、秘密キーと証明書要求を生成する方法について説明します。
- OpenSSL のみを使用する証明書の生成では、サードパーティまたは内部管理された CA で使用できる OpenSSL 専用のプロセスについて説明します。

相互 TLS 認証の場合、Expressway サーバー証明書は、クライアント証明書としても使用できる必要があります。よって、Expressway が隣接サーバーに対しクライアントデバイスとして認証することができます（AD CS によるクライアント証明書とサーバー証明書の発行の有効化を参照）。

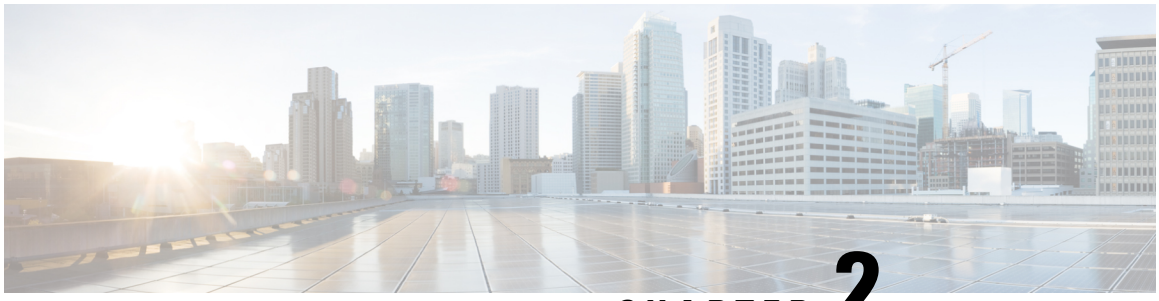
留意点

- 外部システムを使用して証明書署名要求を生成する場合は、証明書署名要求にサポートされていない OID が含まれていないことを確認します。現在、次の拡張検証 OID のみがサポートされています。
  - 1.3.6.1.4.1.311.60.2.1.1 jurisdictionOfIncorporationLocalityName
  - 1.3.6.1.4.1.311.60.2.1.2 jurisdictionOfIncorporationStateOrProvinceName
  - 1.3.6.1.4.1.311.60.2.1.3 jurisdictionOfIncorporationCountryName

  証明書にサポートされていない OID があるかどうかを確認する方法の詳細については、SSH 障害および未対応 OID に関する問題の項を参照してください。

  .
- ワイルドカード証明書では、複数のサブドメインと、それらがサポートするサービス名を管理します。SAN証明書よりも安全性が低い場合があり、Expresswayではサポートされません。
- 2050 年から日付の処理方法が変更されると、有効期限が 2050 年以降の証明書によって運用上の問題が発生する場合があります。
- CA 証明書チェックの Expressway メカニズムでは、BasicConstraints 拡張が存在する必要があります。
- 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。

- サーバー証明書を期限切れにしないでください。期限が切れるとほか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。



CHAPTER 2

証明書署名要求の生成

証明書署名要求（CSR）には、秘密キーの所有者に関するアイデンティティ情報が含まれています。また、署名済み証明書の生成のためにサードパーティまたは内部の認証局に渡すことができます。また、ACME、Microsoft 認証局または OpenSSL などのアプリケーションとともに使用できます。Expressway は、楕円曲線デジタル署名アルゴリズム（楕円曲線 DSA）または RSA ベースの公開キーアルゴリズムを使用した証明書署名要求の生成をサポートするようになりました。

Note 新しいサーバー証明書署名要求（CSR）を生成しても、Expressway にインストールされている既存のアクティブなサーバー証明書は無効になりません。

この章では、次の内容について説明します。

Expressway を使用する証明書署名要求の作成

Expressway はサーバの証明書署名要求を生成できます。これにより、証明書要求を生成し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。

CSR を生成するには、次の手順を実行します。

手順

Step 1 [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。

Step 2 **[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。

Step 3 証明書に必要なプロパティを入力します。

1. **[追加情報（Additional Information）]** セクションで、**[公開キーアルゴリズム（Public key algorithm）]** を選択します。ドロップダウンで [RSA] または [ECDSA] を選択します。

2. 公開キーアルゴリズムに基づいて、ドロップダウンで目的の**キー長**（ビット単位）を選択します。

   （注） ECDSA – 256、384、521、RSA：2048、4096 の定義済みキー長（ビット単位）

3. Expressway がクラスタの一部である場合、サーバ証明書とクラスタ化システムを参照してください。
4. Expressway が Unified Communications ソリューションの一部である場合は、「Unified Communications 向けサーバー証明書要件」項を参照してください。
5. 証明書要求には、証明書で使用される公開キーと、クライアントおよびサーバー認証の Enhanced Key Usage（EKU）の拡張が自動的に含まれます。

Step 4 [CSR の作成（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。認証局に対しても秘密キーを開示してはなりません。

Step 5 [サーバ証明書（Server 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。

1. 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）。
2. 現在の要求の表示（人間可読フォーマットで表示するには**[表示（復号化（Show (decoded)）]** をクリック、または raw フォーマット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）。
3. 手動または自動 ACME の証明書に署名する CA に CSR を送信するには、ACME を使用します。

（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。
- バージョン X8.5.1 から、ユーザ インタフェースにダイジェスト 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-1、SHA-384、または SHA-512 に変更するオプションがあります。
- バージョン X8.10 以降では、SHA-1 を選択できません。
- Let's Encrypt から返される証明書の [発行元（Issuer）] と [件名（Subject）] フィールドには、都道府県、国、組織などの属性は含まれません。Expressway UI では CSR のこれらのフィールドにも入力する必要がありますが、入力した値は認証局では無視されます。

署名済みPEM証明書ファイルを生成するには、証明書署名要求を使用する必要があります。サードパーティまたは内部認証局に渡したり、Microsoft 認証局（Microsoft 認証局を使用する要求の承

認と証明書の生成）や OpenSSL（OpenSSL を使用する認証局としての操作）などのアプリケーションと連動して使用できます。

SAN に複数のエントリまたは FQDN がある場合（MRA 展開など）、単一の証明書ではなく、認証局からマルチドメイン/マルチ SAN 証明書を要求していることを確認します。一部の認証局は、特に要求しない限り、このオプションを推奨しません。

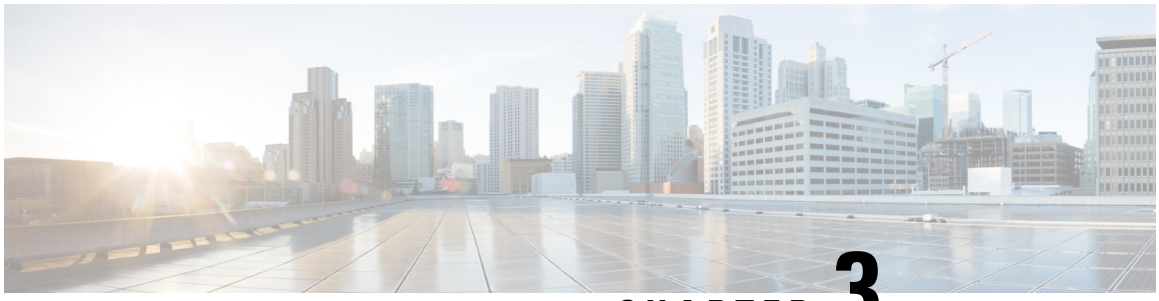
署名済みのサーバー証明書を認証局から受信したときは、Expressway に証明書をキーをロードするで説明されている Expressway にアップロードします。

サーバ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、返されたサーバ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。

正しいサーバ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。



CHAPTER 3

ユニファイド コミュニケーションのサーバ証明書要件

この章では、次の内容について説明します。

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 サーバーと IM and Presence Service サーバー間の 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	—

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			
IM and Presence チャットノードエイリアス （フェデレーション 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 サーバー証明書には、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。

- **Unified CM 電話機セキュリティ プロファイル**：暗号化された Transport Line Signaling（TLS）用に構成され、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**電話機セキュリティ 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。

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 サーバーで設定される**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* の証明書署名要求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

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 で構成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* フォーマットを選択でき、これは、入力するドメインにプリフィックス collab-edge を追加するだけである。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）。

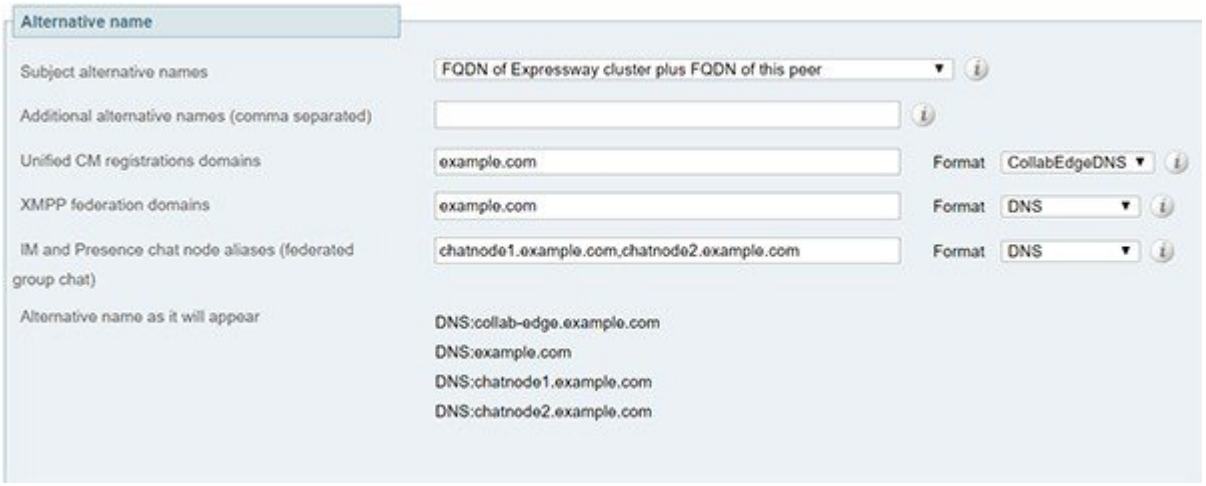
- **XMPP フェデレーションドメイン**：ポイントツーポイント XMPP フェデレーションに使用するドメイン。これらは、IM&P サーバで設定され、XMPP フェデレーション用のドメインとして Expressway-C でも設定する必要があります。

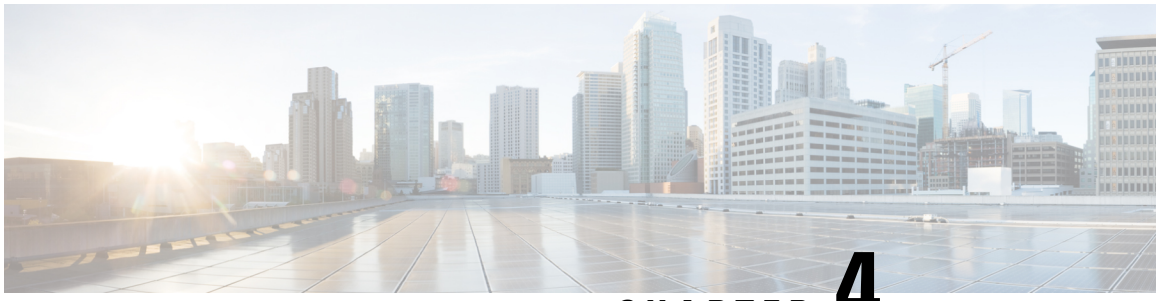
  DNS 形式を選択し、必要な FQDN を手動で指定します。複数のドメインが必要な場合は FQDN をカンマで区切ります。*XMPPAddress* 形式を使用しないでください。この形式は CA によってサポートされない可能性があり、Expressway ソフトウェアの将来のバージョンでは廃止される可能性があります。

- **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。

  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 証明書署名要求ジェネレータでの *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





CHAPTER 4

Expressway-E での ACME の使用

X12.5 以降、Cisco Expressway シリーズでは、ACME（AutomatedCertificate Management Environment）プロトコルをサポートするようになっています。このプロトコルにより、Let's Encrypt などの認証局から Cisco Expressway-E に署名済みの証明書を自動的に導入することが可能になります。この機能の主な利点は、Expressway-E を識別するサーバ証明書を低コストで生成できることです。したがって、MRA (モバイルおよび Remote Access) などの Expressway-E ベースの導入環境のコストを削減できます。

基礎となる検証メカニズムにより、この機能は MRA 導入環境に最も役立つ可能性があります。ビジネス ツー ビジネス (B2B) アプリケーションでは、ACME 証明書にプライマリ ドメインを含めるのが常に実用的であるとは限りません。

設定プロセスはシンプルです。Cisco Expressway-E で、証明書署名要求 (CSR) を作成するための情報を入力します。これにより、Expressway の ACME クライアントが認証局とやり取りして証明書を要求します。Expressway が証明書をダウンロードするので、ボタンをクリックするだけで展開できます。ACME 証明書の有効期間は意図的に短くされているため、この手動による手順を行った後、証明書が期限切れにならないように更新をスケジュールできます。

ACME プロトコルに伴う潜在的なセキュリティ侵害の 1 つとして、Cisco Expressway-E 上のポート 80 でのインバウンド HTTP 接続が必要になることです。このリスクを管理するには Expressway のセキュリティ機能を使用できますが、極めてセキュアな環境では、ACME を無効にして、任意の認証局で従来の CSR 手順を使用することもできます。

ACME での Jabber Guest サポートなし。

現在、Expressway では Jabber Guest 展開で ACME をサポートしていません。

この章では、次の内容について説明します。

ACME 展開の概要

1. ACME 証明書サービスの展開
2. Expressway-E で ACME 証明書サービスを構成
3. ACME に証明書署名要求を生成
4. ACME プロバイダーを使用して証明書署名要求に署名
5. （オプション）署名付き ACME 証明書の確認
6. ACME 証明書の展開
7. ACME 証明書の自動更新の有効化

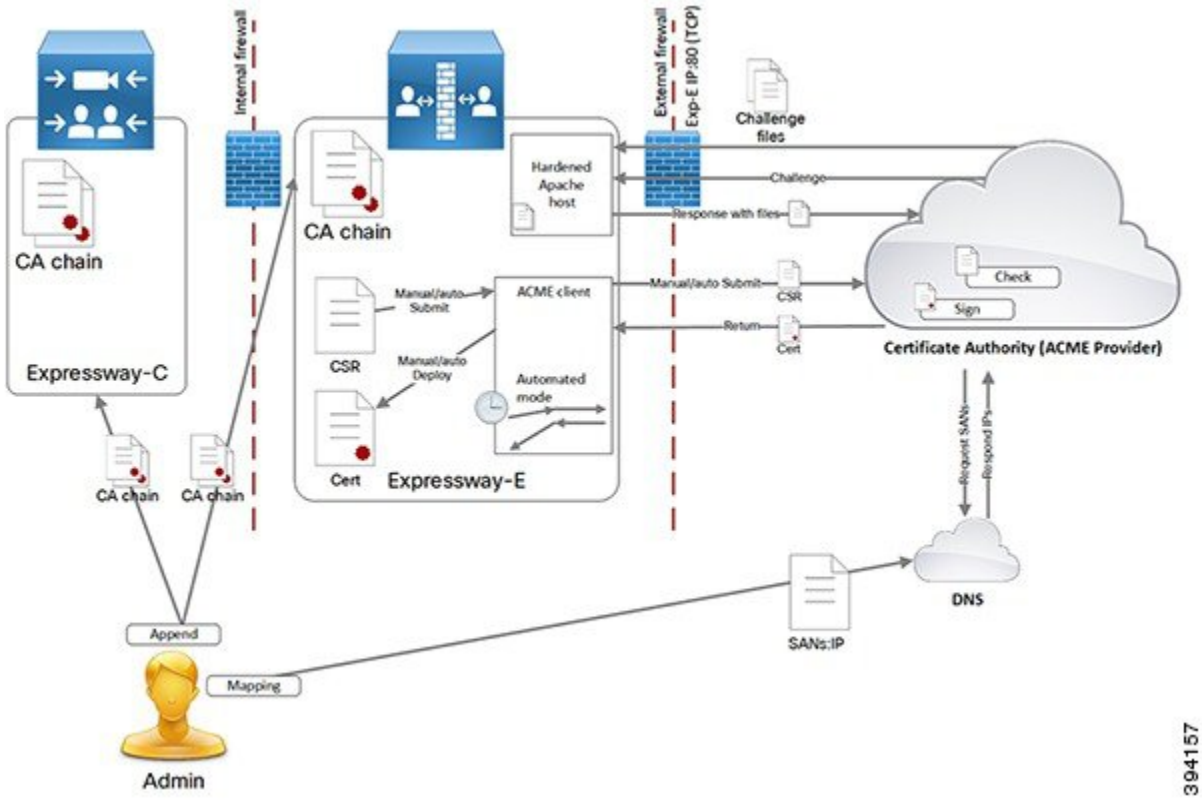
クラスタ展開の場合、ACME はクラスタレベルではなく**各ピアで個別に有効にする必要があります。**ほとんどの証明書操作はノードごとに実行されます。

ACME の仕組み

ACME は、Web ホストの自動証明書管理を可能にするクライアント サーバー プロトコルです。Expressway-E には、認証局の制御下にある ACME プロバイダーと双方向対話する ACME クライアントがあります。

現在、Let's Encrypt 機関と協力してサーバー証明書を生成しています。

また、ACME を使用して SNI（マルチテナンシー）のドメイン証明書を生成します。このプロセスは基本的にサーバー証明書プロセスと同じです。マルチテナンシーはHCS展開でのみサポートされており、SNI での ACME の使用に関する詳細は、Collaboration Knowledge ポータルの [証明書管理とサービス検出（Certificate Management and Service Discovery）] エリアを参照してください。



Expressway-E の ACME 証明書サービスは、このドキュメントの他の部分で説明されている方法とは異なる方法で、サーバー証明書を要求して Expressway-E に適用します。

重要な署名プロセスは次のとおりです。

- [要求の定義（Define request]）> [CA に送信（Submit to CA）] > [CA の生成（CA generates）] の順に選択し、[証明書にサイン（signs the certificate）] > [証明書の適用（Apply certificate）] の順に選択します。
- ACME証明書サービスはこのプロセスに従いますが、費用と手動作業の一部を取り除きます。
- このプロセスに関する注意点の1つは、CAが送信ホストに問い合わせて、証明書署名要求内のドメインを制御していることを確認する必要があることです。

共通の設定

ACME 証明書サービスを使用する場合は、常に次のタスクが必要です。

1. Expressway-E で証明書署名要求を作成します。
2. 証明書署名要求のドメインを使用してドメインネームシステム（DNS）を構成し、それらを Expressway-E のパブリック IP アドレスにマッピングします。
3. 各ドメインには、FQDN だけでなく、A レコードが必要です。

4. プロバイダーの詳細と電子メールアドレスを使用して ACME クライアントを設定します。

検証プロセスの暗号化

Let's Encrypt は、証明書署名要求で要求されたすべてのドメインが要求元の制御下にあることを確認するために、それぞれに対してチャレンジを実行します。要求元が証明書署名要求の各ドメインのポート 80 でサービスを提供できる必要があるランダムな文字列を含むファイルを提供します。

Let's Encrypt は、すべてのチャレンジファイルを正常に読み取った後にのみ証明書を発行します。

プロセスを手動で制御する場合の動作は次のとおりです。

手順

Step 1 署名プロセスを開始します。

1. ACME クライアントは、Let's Encrypt への HTTPS 接続を開き、証明書署名要求をアップロードします。
2. Let's Encrypt は、証明書署名要求内のドメインごとに 1 つずつ、チャレンジファイルのリストで応答します。
3. クライアントは、Expressway-E クラスタ内のすべてのピアにチャレンジファイルを配置します。
4. 各 Expressway-E ピアは、チャレンジファイルのみを提供するように設定された仮想 Apache ホストを起動します。
5. クライアントは、チャレンジファイルを提供する準備ができたことを Let's Encrypt に通知します。
6. Let's Encrypt は、チャレンジファイルの取得を試みます。
7. クライアントは、Let's Encrypt をポーリングして、チャレンジプロセスが成功したかどうかを確認します。
8. チャレンジ交換が成功した場合、クライアントは署名済み証明書をダウンロードしてステージングエリアに保存し、証明書を展開する準備ができたことを通知します。
9. Expressway-E ピアは仮想 Apache ホストを閉じます。

Step 2 展開プロセスを開始します。

1. Expressway-E は、既存のサーバー証明書にステージングされた証明書をコピーします。
2. 証明書署名要求に関連付けられた秘密キーを既存の秘密キーに上書きコピーします。

3. Expressway-Eは、サーバー証明書をリロードする必要があることを他の内部プロセスに通知します。（Expressway-E を再起動する必要はありません）。

Expressway-E は、TLS 接続を行うときに ACME 証明書を提示するようになりました。

頻繁な有効期限切れと影響の少ない更新

Let's Encrypt証明書は、設計上90日間のみ有効です。これは、証明書をより頻繁に更新する必要があることを意味します。ACME 証明書サービスでは、次のように対処しています。

- 有効期間の3分の2が期限切れになったときに新しい証明書を取得する自動更新モードを提供します。

  サービスが自動モードでない場合、3 分の 2 の時点で通知はありません。新しい署名要求を送信する必要があります。Let's Encrypt は、Expressway-E で ACME クライアントを構成するために使用するアカウントに期限切れ警告電子メールを送信します。

- ACME 証明書サービスを使用して新しい証明書を展開するときに Expressway-E を再起動する必要がなくなります（自動展開または手動展開）。

  証明書を使用する Expressway プロセスは、再起動せずに新しい証明書をロードできます。Expressway-E は TLS 接続をドロップせず、新しい接続試行に対して新しい証明書を提示します。

  モバイルおよびリモートアクセス クライアントのサービスは中断されません。

（注） 別の方法を使用して新しいサーバー証明書をアップロードする場合は、Expressway-E を再起動する必要があります。この動作は、ACME 証明書サービスの導入でも変更されていません。

自動更新モード

自動更新を構成するときに、1 週間のうち 1 日以上の特定の時刻をスケジュールできます。スケジュールは、新しい証明書の要求ではなく、証明書の展開にのみ使用されます。

サービスを自動モードにすると、サービスは最初の証明書を要求して受信し、次にスケジュールされた機会に証明書を展開します。その証明書の有効期間の 3 分の 2 が経過すると、ACME 証明書サービスは、保存されている証明書署名要求を自動的に再送信して新しい証明書を取得します。

1 日に 2 回の自動再送信の機会があります。これらは、チャレンジプロセスのセキュリティを向上させるために、意図的にランダムな時間に設定されています。このような場合、Expressway-E はポート 80 で要求を受け入れる必要があるため、予測不能にすることをお勧めします。

自動署名が成功すると、ACME 証明書サービスは、次にスケジュールされた機会にステージングされた証明書を自動的に展開します。これには数秒かかり、証明書を使用する実行中のプロセスには影響しません。

仮想 Apache ホストの詳細

Let's Encrypt は、上記のチャレンジと検証プロセスを使用して、証明書要求者が証明書署名要求のドメイン名を制御していることを確認する必要があります。ドメインが複数の IP アドレスに解決されると、Let's Encrypt はそれらのいずれかにランダムに接続するため、Let's Encrypt はクラスタ内のすべてのピアのポート 80 にアクセスできる必要があります。

送信元アドレスに基づいて Expressway-E ポートへのアクセスを制限することは実用的ではありません。これは、Let's Encrypt には、すべてのサーバーを含む簡潔なリストまたは CIDR がないためです。

悪意のあるアクセスのリスクを軽減するために、Apache 仮想ホストはチャレンジフェーズ中にのみ実行され、チャレンジファイルへの HTTP アクセスのみを許可するように制限されます。

Apache は、ポート 80 でリッスンするように構成され（そのポートでまだリッスンしていない場合）、ACME チャレンジトラフィック（のみ）を仮想 Apache ホストに転送します。

仮想ホストは、localhost インターフェイス上の 1 つの非特権ポートでのみリッスンします。仮想ホストは通常の方法で強化されます。ディレクトリの参照、シンボリックリンク、すべてのオプション、.htaccess ファイルの使用を拒否します。このため、HTTP から HTTPS へのリダイレクトは、Expressway E の Web 管理ポートがデフォルトの 443 ポートとして構成されている場合にのみサポートされます。

Expressway-E がポート 80 を 443 にリダイレクトするように構成されている場合：

- ACME チャレンジトラフィックの 80 から 443 へのリダイレクトルールに例外を追加します。この例外はバックグラウンドで自動的に追加され、手動で構成することはできません。
- 例外は、必要なパス（.well-known/acme-challenge/）への GET 要求でのみフィルタリングされます。

  したがって、特定のファイルパスへのポート 80 での GET 要求のみが仮想ホストに到達します。他のすべての要求は、通常どおりポート 443 にリダイレクトされます。

Expressway-E でポート 80 が有効になっていない場合：

- ポート 80 でリッスンするように Apache を構成します。
- ACME チャレンジファイルの GET 要求をポート 80 で仮想 Apache ホストにリダイレクトするルールを追加します。
- 他のすべての要求は、HTTP エラー 404（not found）を返します。

チャレンジプロセスは、証明書署名要求内のドメインの数と Expressway クラスタ内のピアの数に応じて、数分間続くことがあります。

チャレンジが完了すると、次のようになります。

- チャレンジファイルを削除します。
- 80 から 443 へのリダイレクトルールの例外を削除します。
- 443 へのリダイレクトを許可するように構成されていない場合、Apache がポート 80 でリッスンしないようにします。
- Apache 仮想ホストを停止します。

ACME 証明書サービスの展開

前提条件

- 法定代理人に連絡して、Let's Encrypt の利用規約を確認してください。
- 証明書で CN または SAN として必要な Expressway-E へのマッピングを使用してドメインネームシステム（DNS）を設定します。
- Let's Encrypt CA で使用する電子メールアカウントを作成します。
- Let's Encrypt ルート CA 証明書を Expressway の信頼ストアに追加します。
- Let's Encrypt 中間 CA 証明書を Expressway の信頼ストアに追加します。
- インターネットから Expressway-E のパブリックアドレスへの TCP 80 インバウンドを有効にします。
- SAN 上のすべてのドメインに（FQDN だけでなく）有効な A レコードがあることを確認します。**ドメイン**のレコードが別の Web サーバーによってすでに使用されている場合は、証明書署名要求で *collab-edge* ドメインを構成し、その A レコードを設定できます。

Expressway 信頼ストアへの Let's Encrypt ルート CA 証明書の追加

Let's Encrypt は比較的新しい CA であるため、独自の CA ルート証明書は、確立された IdenTrust CA によってクロス署名されます。次の手順に従って、すべての Expressway が Internet Security Research Group Root X1 を信頼していることを確認します。

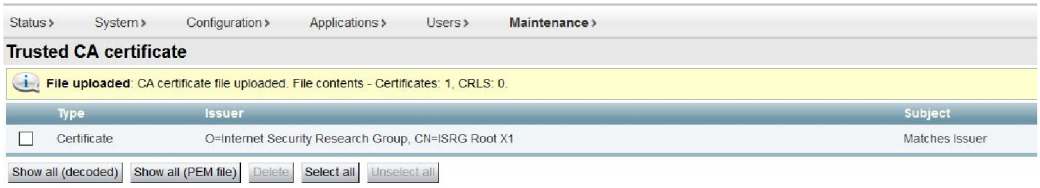
手順

Step 1 「https://letsencrypt.org/certs/isrgrootx1.pem」に進みます。

Step 2 展開内の各 Expressway-E（およびトラバーサル Expressway-C）の場合、Let's Encrypt が署名した証明書で保護します。

1. Expressway の Web インターフェイスにログインします。
2. **[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）]** の順に選択します。
3. ページの **[アップロード（Upload）]** セクションで、作成した証明書ファイルを選択します。
4. [CA 証明書の追加（Append CA certificate）] をクリックします。

   これで、信頼できる CA 証明書リストに、Internet Security Research Group のルート証明書が含まれます。



394147

Expressway 信頼ストアへの Let's Encrypt 中間 CA 証明書の追加

手順

Step 1 「https://letsencrypt.org/certs/lets-encrypt-r3.pem」に進みます。

Step 2 展開内の各 Expressway-E（およびトラバーサル Expressway-C）について、Let's Encrypt によって署名された証明書で保護します。

1. Expressway の Web インターフェイスにログインします。
2. **[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）]** の順に選択します。
3. ページの **[アップロード（Upload）]** セクションで、作成した証明書ファイルを選択します。
4. [CA 証明書の追加（Append CA certificate）] をクリックします。

   信頼できる CA 証明書リストには、Internet Security Research Group のルート証明書と Let's Encrypt CA 証明書の両方が含まれている必要があります。

394148

Expressway-E で ACME 証明書サービスを構成

手順

Step 1 Expressway-E のサインインし、**[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。

Step 2 **[ACME 証明書サービス（ACME Certificate Service）]** セクションまで下にスクロールします。

Step 3 ドロップダウンリストで、ACME **プロバイダー**を選択します。

これは、証明書に署名する CA です。現在、Let's Encrypt® でのみ動作します。

Step 4 プロバイダーで使用する**管理者の電子メールアドレス**を入力します。

これは、必要に応じてACMEプロバイダーからの通信を受信できるように、実際のアドレスである必要があります。

このアドレスは、プロバイダーのアカウント名であり、このプロバイダーで行うすべての証明書署名要求にリンクされています。

Step 5 利用規約をお読みください。

法定代理人がまだ確認していない場合は、コピーを保存して確認することをお勧めします。

Step 6 **[利用規約に同意します（I accept the terms and conditions）]** をクリックします。

Expressway-E の ACME クライアントは、選択したプロバイダーでアカウントを作成します。

これで、Expressway-E クライアントの ACME 証明書サービスが ACME プロバイダーと対話する準備が整いました。

各ドメイン証明書の ACME 構成

Expressway-E での ACME サービスでは、バージョン X12.5 以降から、（SNI で使用する）ドメイン証明書を要求して導入できるようになっています。

[メンテナンス（Maintenance）] > [セキュリティ（Security）] > [ドメイン証明書（Domain certificates）] の順に選択し、ドメインのリストに [ACME] 列が表示され、ここに各ドメインの ACME サービスのステータスが表示されます。

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。

ACME に証明書署名要求を生成

証明書署名要求を作成するプロセスは、ACME クライアントを使用する場合と変わりません。証明書署名要求の生成のガイダンスに従います。

ACME プロバイダーを使用して証明書署名要求に署名

Expressway-E に証明書署名要求を保存し、ACME サービスを構成したら、証明書署名要求を ACME プロバイダーに送信して検証および署名できます。

手順

Step 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。

Step 2 [ACME サービス構成（ACME Service Configuration）] までスクロールします。

Step 3 **[ACME プロバイダーで証明書署名要求に署名（Sign CSR with ACME Provider）]** をクリックします。

Expressway-E の ACME クライアントは、選択したプロバイダーに保存された証明書署名要求を送信します。

Step 4 署名プロセスが完了するまで、数分待ちます。

プロバイダーは、証明書署名要求の CN および SAN 属性のドメインネームシステム（DNS）をチェックし、署名要求を受信した Expressway-E アドレスと一致することを確認します。プロバイダーは証明書に署名して返します。ACME クライアントはこの証明書を Expressway-E に保存し、展開を待機します。

Step 5 **[サーバー証明書（Server certificate）]** ページを手動で更新します。

証明書が署名され、使用できる状態になると、成功バナーが表示されます。

（オプション）署名付き ACME 証明書の確認

手順

Step 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、**[ACME Certificate Service（ACME 証明書サービス）]** セクションに移動します。

[ステータス（Status）] フィールドには、署名付き証明書を展開する準備ができていることが示されます。

Step 2 **[保留中の ACME（Pending ACME Certificate）]** フィールドで、**[表示（復号化）（Show (decoded)）]** をクリックします。

Step 3 詳細が期待どおりであることを確認します。そうでない場合は、保留中の証明書を破棄し、新しい証明書署名要求を生成する必要があります。

（注） Let's Encrypt CA は、証明書署名要求で指定した属性の一部を無視する可能性があります。

ACME 証明書の展開

手順

Step 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、**[ACME Certificate Service（ACME 証明書サービス）]** セクションに移動します。

[ステータス（Status）] フィールドには、署名済み証明書を展開する準備ができていることが示されます。

Step 2 **[保留中の証明書の展開（Deploy Pending Cert）]** をクリックします。

Expressway-E は、相手側に対して自身を認証する必要があるトランザクションで、この証明書の使用を開始します。Expressway-E を再起動する必要はありません。

ACME 証明書の自動更新の有効化

ACME 証明書は、セキュリティ上の予防措置として意図的に短命です。執筆時点では、有効期間は発行日から 90 日間です。

Expressway-E の ACME 証明書サービスは、証明書の有効期間をモニターし、有効期間の 3 分の 2 が経過すると警告します。前のトピックで説明した手順に従って、手動で応答できます。

この頻繁なタスクを回避するために、自動更新オプションを使用して、ACME 証明書サービスに証明書を更新して展開させることができます。

手順

Step 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、**[ACME Certificate Service（ACME 証明書サービス）]** セクションに移動します。

Step 2 **[ACME 自動スケジューラ（ACME Automated Scheduler）]** フィールドを *[オン（On）]* に変更します。

Step 3 1 つ以上の **[スケジュール日（Schedule Days）]** と **[スケジュール時刻（Schedule Time）]** を選択します。

証明書の有効期限の 3 分の 2 が経過すると、ACME 証明書サービスは、選択された翌日の指定時刻にサーバー証明書の更新と展開を試行します。

Step 4 [**Save**] をクリックします。

[ステータス（Status）]には、自動モードのサービスが表示されます。次に証明書を更新して展開するときに、**[最終展開ステータス（Last Deploy Status）]** と **[最終署名ステータス（Last Sign Status）]** を更新します。

ACME 証明書の取消

Expressway-E で ACME 証明書を取り消す理由の一部を次に示します。

- Expressway-E が侵害された。
- Expressway-E を初期設定にリセットした。
- Expressway-E の目的が変更された。
- ACME アカウントは無効になった。

ACME 証明書を取り消すには、Expressway-E のドメインネームシステム（DNS）アドレスを所有していること、および証明書の元のエントリを管理していることをプロバイダーに証明する必要があります。これを行うには、証明書に使用される署名証明書署名要求プロセスを繰り返す必要がありますが、結果の証明書を再展開する必要はありません。

元の証明書を取り消す前に、新しい証明書を展開する必要があります。取り消す証明書のコピーを保持します。

⚠

注意 使用中の証明書を取り消すと、この証明書を使用するすべてのサービスが中断されるため、取り消さないでください。

手順

Step 1 現在の証明書のバックアップを作成します。

この予防措置は、現在の証明書を失効させる予定の証明書で誤って上書きした場合に役立ちます。

Step 2 失効させる証明書を Expressway-E の一時的な場所にコピーします。場所へのパスを覚えておいてください。

取り消す証明書のコピーがない場合は、https://crt.sh/ から取得できる場合があります。

Step 3 失効させる証明書のすべてのドメイン名を含む証明書署名要求を作成します。ACME に証明書署名要求を生成を参照してください。

Step 4 元の証明書に署名した ACME プロバイダーによって署名される証明書署名要求を送信します。ACME プロバイダーを使用して証明書署名要求に署名を参照してください。

これで、失効させる証明書に一致する SAN エントリを持つ新しい保留中の証明書が作成されます。

このプロセスにより、元の証明書を取り消す権限があることが証明されました。

Step 5 Expressway-E の CLI に（管理者として）サインインします。

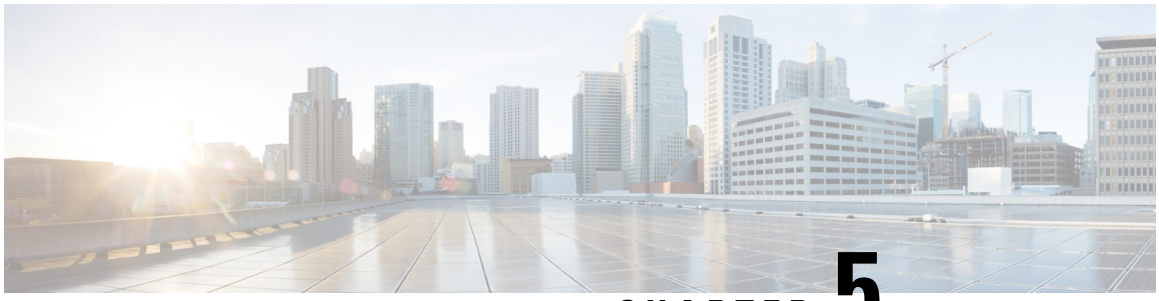
Step 6 次のいずれかの方法で acmerevoke コマンドを実行します。

- デフォルトのプロバイダーが証明書に署名した場合：`xcommand Acmerevoke "/path_to_cert_to_be_revoked"`
- 証明書に署名したプロバイダーを特定する場合：`xcommand Acmerevoke CertPath:"/path_to_cert_to_be_revoked" Provider:"ACME_Provider_Name"`

  （証明書に署名したのと同じプロバイダーが証明書を失効させる必要もあります）。

証明書の失効に成功すると、プロバイダーは 200 OK で応答します。

Step 7 失効した証明書の保存済みコピーを削除します。



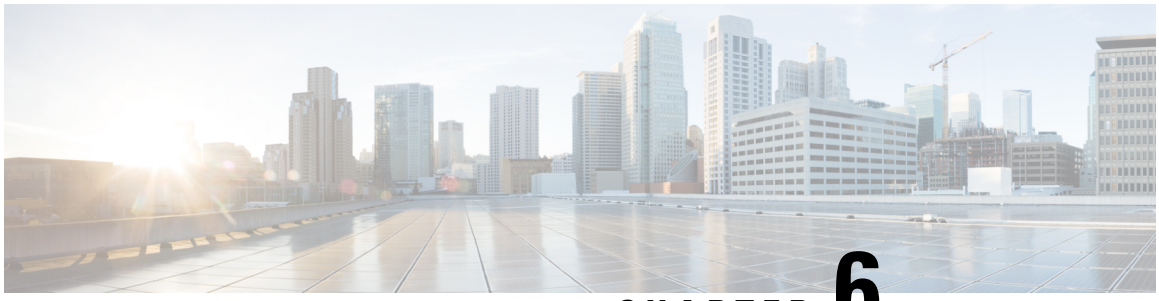
CHAPTER 5

現在アップロードされている証明書の表示

[サーバ証明書のデータ（Server certificate data）] セクションに、Expressway に現在ロードされているサーバ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サーバ証明書を表示する場合、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。

Note 現在アップロードされているサーバ証明書を Expressway の元の証明書に置き換えるには、[デフォルトのサーバ証明書にリセット（Reset to default server certificate）] をクリックします。



CHAPTER 6

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。）

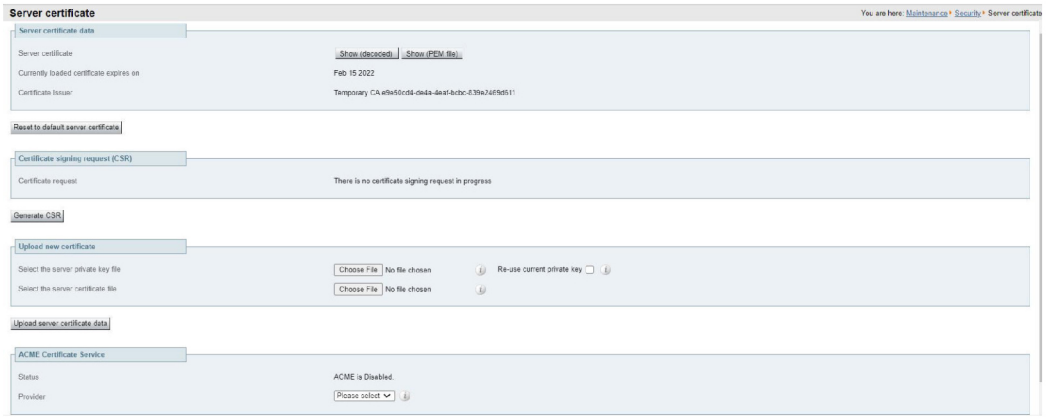
- **サーバー秘密キー** PEM ファイルはパスワードで保護しないでください。
- 証明書署名要求の進行中は、サーバ秘密キーをアップロードできません。

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。



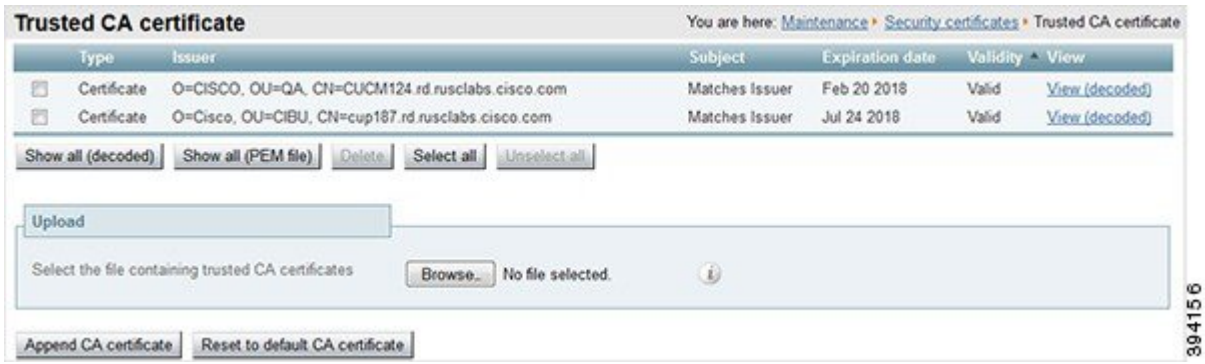
456940

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。

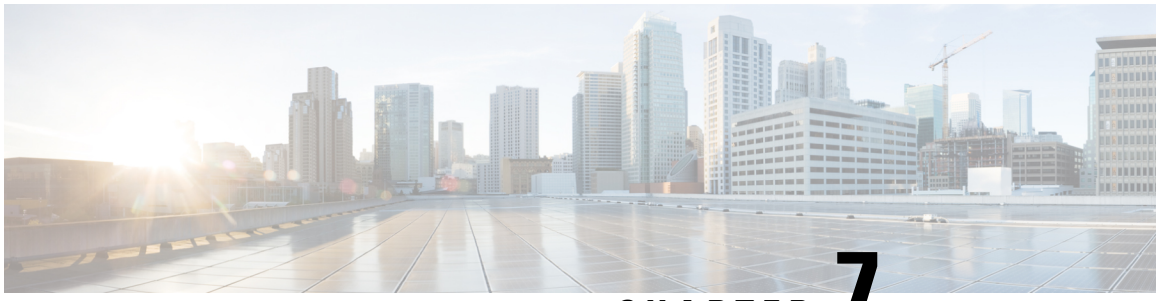
Step 3 クラスタ内のすべてのノードでサーバー証明書を更新します。

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。



CHAPTER 7

証明書失効リスト（CRL）の管理

証明書失効リストファイル（CRL）は、TLS/HTTPS を介して Expressway と通信するクライアントブラウザおよび外部システムにより提示される証明書を検証するために Expressway によって使用されます。CRL は、廃棄され Expressway との通信に使用できなくなった証明書を識別します。

TLS/HTTPS クライアントおよびサーバ証明書に署名する CA の CRL データをアップロードすることを推奨します。イネーブルの場合、CRL のチェックはトラスト チェーンのすべての CA に適用されます。

この章では、次の内容について説明します。

証明書失効ソース

Expressway は複数のソースから証明書失効情報を取得できます。

- CRL 分散ポイントからの CRL データの自動ダウンロード
- 証明書内のチェック対象 OCSP（Online Certificate Status Protocol）レスポンダ URI 経由（SIP TLS のみ）
- CRL データの手動アップロード
- Expressway の**信頼できる CA 証明書**ファイル内に組み込まれた CRL データ

制限事項と使用上のガイドライン

次の制約事項および使用上のガイドラインが適用されます。

- SIP TLS 接続を確立するときに、CRL データソースは、**[SIP 構成（SIP configuration）]** ページの **[証明書失効確認（Certificate revocation checking）]** 設定を必要とします。

- 自動的にダウンロードされた CRL ファイルが、手動でロードされた CRL ファイルを上書きする場合（SIP TLS 接続を確認する場合、手動でアップロードされた CRL データと自動でダウンロードされた CRL データの両方を使用する可能性がある場合は除く）
- 外部ポリシー サーバによって提示された証明書を検証する際に、Expressway は手動でロードされた CRL のみを使用します。
- リモート ログイン アカウント認証用に LDAP サーバーとの TLS 接続を検証する際、Expressway は **信頼できる CA 証明書（[ツール（Tools）] > [セキュリティ（Security）] > [信頼できる CA 証明書（Trusted CA certificate）]）**に組み込まれた CRL データのみを使用します。

  LDAP 接続の場合、Expressway はサーバの証明書配布ポイントの URL または発行する CA 証明書から CRL をダウンロードしません。また、[CRL 管理（CRL management）] ページの手動または自動更新設定も使用しません。

自動 CRL 更新

自動 CRL 更新を実行するように Expressway を構成することが推奨されます。これにより、最新の CRL が証明書の検証に使用できるようになります。

CRL の自動更新用に Expressway を構成するには次を実行します。

手順

Step 1 **[メンテナンス（Maintenance）] > [セキュリティ（Security）] > [CRL 管理（CRL management）]** の順に選択します。

Step 2 **[自動 CRL 更新（Automatic CRL updates）]** を *[有効（Enabled）]* に設定します。

Step 3 Expressway が CRL ファイルを取得できる **HTTP/HTTPS 分散ポイント**のセットを入力します。

- 新しい行にそれぞれ分散ポイントを指定する必要があります。
- HTTP/HTTPS 分散ポイントのみがサポートされます。HTTPS を使用する場合、分散ポイントのサーバ自体に有効な証明書が必要です。
- PEM および DER エンコード CRL ファイルがサポートされています。
- 分散ポイントは、CRL ファイルまたは複数の CRL ファイルを含む ZIP および GZIP アーカイブを直接示す場合があります。
- URL またはダウンロードしたアーカイブから解凍されたファイルのファイル拡張子は、Expressway がその基盤となるファイル タイプを決定するため、重要ではありませんが、代表的な URL は次の形式となります。
  - http://example.com/crl.pem
  - http://example.com/crl.der

- http://example.com/ca.crl
- https://example.com/allcrls.zip
- https://example.com/allcrls.gz

Step 4 **[Daily update time]** を入力します（UTC 単位で）。これは、Expressway が分散ポイントからその CRL の更新を試行するおおよその時刻です。

Step 5 [保存（Save）] をクリックします。

手動 CRL 更新

CRL ファイルは Expressway に手動でアップロードできます。外部ポリシー サーバによって提示された証明書は、手動でロードされた CRL に対してのみ検証できます。

CRL ファイルをアップロードするには、次の手順を実行します。

（注） CRL ファイルのサイズが 16 MB 未満であることを確認します。

手順

Step 1 **[メンテナンス（Maintenance）] > [セキュリティ（Security）] > [CRL 管理（CRL management）]** の順に選択します。

Step 2 **[参照（Browse）]** をクリックして、ファイル システムから必要なファイルを選択します。また、PEM エンコード形式である必要があります。

Step 3 [CRL ファイルのアップロード（Upload CRL file）] をクリックします。

これによって、選択したファイルがアップロードされ、以前にアップロードしたCRLファイルが置換されます。

Expresswayから手動でアップロードされたファイルを削除する場合は、**[失効リストの削除（Remove revocation list）]** をクリックします。

注：認証局の CRL が期限切れの場合、その CA から発行されたすべての証明書が無効として扱われます。

オンライン証明書ステータス プロトコル（OCSP）

Expressway は OCSP レスポンダとの接続を確立して特定の証明書のステータスを照会することができます。Expressway は使用する OCSP レスポンダを、確認する証明書に示されているレスポン

ダURIから決定します。OCSPレスポンダは「良好（good）」、「失効（revoked）」、または「不明（unknown）」で証明書のステータスを送信します。

OCSPの利点は、失効リスト全体をダウンロードする必要がないことです。OCSPはSIP TLS接続のみでサポートされます。

OCSPレスポンダへ接続するには、Expressway-Eからのアウトバウンド通信が必要です。使用しているOCSPレスポンダのポート番号（ポート80または443）をチェックし、Expressway-Eからそのポートへのアウトバウンド通信が可能であることを確認します。

SIP TLS 接続を確認する失効の構成

証明書失効確認がSIP TLS接続でどのように管理されるかを設定する必要があります。

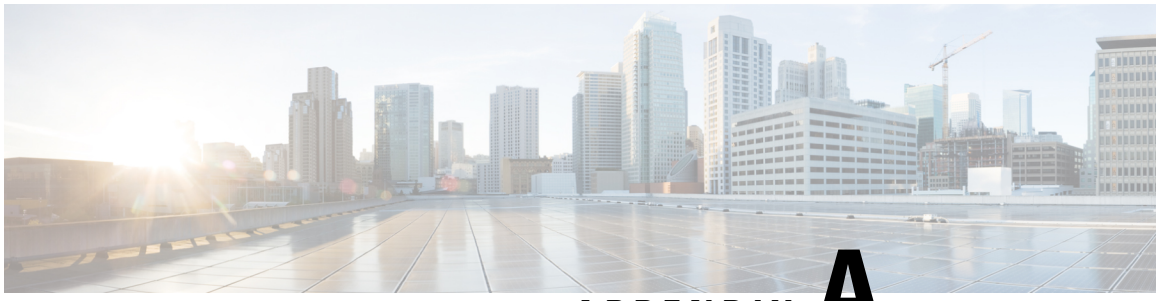
手順

Step 1 **[構成（Configuration）] > [SIP]** の順に選択します。

Step 2 **[証明書失効確認（Certificate revocation checking）]** セクションまでスクロールし、適宜設定を行います。

フィールド	説明	使用方法のヒント
Certificate revocation checking mode	失効確認がSIP TLS接続の確立時に交換された証明書に対し実行されるかどうかを制御します。	失効確認をイネーブルにすることを推奨します。
Use OCSP	Online Certificate Status Protocol（OCSP）を証明書失効確認を実行するために使用するかどうかを制御します。	OCSPを使用するには、以下の条件が必要です。 • チェック対象のX.509証明書にOCSPレスポンダのURIが含まれている必要があります。 • OCSPレスポンダーは、SHA-256ハッシュアルゴリズムをサポートしている必要があります。サポートされていない場合、OCSP失効チェックと証明書検証は失敗します。

フィールド	説明	使用方法のヒント
Use CRLs	証明書失効リスト（CRL）を証明書失効確認を実行するために使用するかどうかを制御します。	CRL は、証明書が OCSP をサポートしていない場合に使用できます。
Allow CRL downloads from CDPs	X.509 証明書に含まれる CDP URI からの CRL のダウンロードを許可するかどうかを制御します。	
Fallback behavior	たとえば、失効の送信元に連絡を取れないなど、失効ステータスを確立できない場合に、失効確認の動作を制御します。 *[*失効として処理（*Treat as revoked*）*]*：証明書を失効したとして処理します（そのため、TLS 接続を許可しません）。 *[*失効していないものとして処理（*Treat as not revoked*）*]*：失効していないものとして証明書を処理します。 デフォルト：[Treat as not revoked]	*[*失効していないものとして処理（*Treat as not revoked*）*]*では、失効の送信元に連絡をとれない場合、システムは通常の方法で稼働し続けますが、失効した証明書が承認される可能性があることを意味します。



APPENDIX A

トラブルシューティング

この章では、次の内容について説明します。

ネイバーとトラバーサルゾーンでの SIP TLS ネゴシエーションの失敗

TLS 検証モードが有効にされている場合、ゾーン構成の **[ピアアドレス（Peer address）]** フィールドに指定されたネイバーシステムのFQDNまたはIPアドレスがそのシステムで提示されたX.509証明書の証明書の所有者名と照合するために使用されます。（名前は証明書のSAN属性に含まれている必要があります）。証明書自体も有効であり、信頼された認証局によって署名されている必要があります。

そのため、証明書がピアまたはクラスタ FQDN で生成されている場合は、ゾーンの **[ピアアドレス（Peer address）]** フィールドが IP アドレスではなく FQDN で設定されていることを確認します。

8192 ビットキー長の証明書

証明書が 8192 ビットのキー長を使用する場合、SIP TLS ゾーンがアクティブになれない場合があります。4096 ビットのキー長を有する証明書を使用することを推奨します。

モバイルおよびリモートアクセスを使用する際のサービス障害

末尾の改行文字を含まない秘密キーファイルをアップロードした場合、証明書のエラーにより Unified Communications のモバイルおよびリモートアクセスサービスが失敗する場合があります。

秘密キーファイルに末尾の改行文字が含まれていることを確認してください。

SSH 障害および未対応 OID に関する問題

ssh トンネルの確立ができないなどの不明な ssh 障害が発生した場合は、証明書に不明な OID がないかを確認してください。これは、[発行者および件名（Issuer & Subject）] フィールドの CN に復号化されていない数値エントリがないかを確認することで対応できます（GUI の場合、**[メンテナンス（Maintenance）] > [セキュリティ証明書（Security Certificates）] > [サーバー証明書（Server Certificate）] > [表示（復号化）（Show (decoded)]** から確認。コンソールの場合、「`openssl x509 -text -noout -in /tandberg/persistent/certs/server.pem`」で確認）。

無効（Invalid）

```
subject=CN=blahdeblah,OU=IT
Security,O=BigBang,L=Washington,ST=District of
Columbia,C=US,1.3.6.1.4.1.6449.1.2.1.5.1 = #060C2B06010401B2310102010501
```

有効

```
subject=CN=blahdeblah,OU=IT
Security,O=BigBang,L=Washington,ST=District of
Columbia,C=US,jurisdictionOfIncorporationLocalityName=Dover
```

Expressway との Cisco Unified Communications Manager 暗号の相互運用性

Transport Layer Security（TLS）ハンドシェイク中のサーバーは、Rivest Shamir Adleman（RSA）/楕円曲線デジタル署名アルゴリズム（楕円曲線 DSA）暗号を送信します。クライアントとしての Expressway は、これらの暗号を受け入れることができます。

（注） Expressway の新規インストールでは、デフォルトで ECDSA 暗号が使用されます。

Expressway は ECDSA 暗号要求をネゴシエートできます。

メモ

- RSA を使用した証明書暗号化、UCM は *CallManager* または *Tomcat* 証明書のいずれかを送信します。
- ECDSA を使用した証明書暗号、UCM は *CallMananager-ECDSA* または *Tomcat-ECDSA* 証明書のいずれかを送信します。
- ユーザーは、UCM から受信した証明書を検証するために、署名済み Unified Call Manager（UCM）証明書を信頼できる認証局（CA）として Expressway-C に順番にアップロードする必要があります。

参考情報

- **暗号構成の場合**：ECDSA を構成してから RSA 暗号を構成します。

```
ECDHE-ECDSA-AES128-GCM-SHAdefault:ECDHE-ECDSA-AES128-SHAdefault:ECDHE-ECDSA-
AES128-SHA:ECDHE-ECDSA-AESdefault-GCM-SHA384:ECDHE-ECDSA-AESdefault-
AES128-SHA:ECDHE-ECDSA-AESdefault-GCM-SHA384:ECDHE-ECDSA-AESdefault-
GCM-SHA384
```

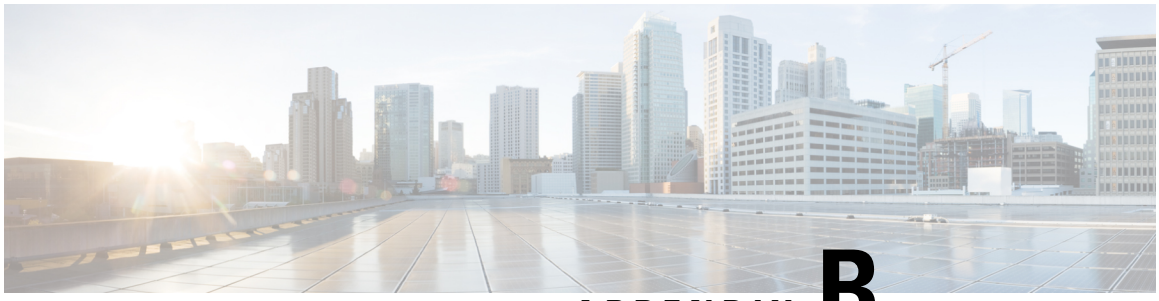
- **Expressway での構成の場合**

  [メンテナンス（Maintenance）] > **[セキュリティ（Security）]** > **[暗号（Ciphers）]**の順に選択し、以下の暗号を追加します。

（注） ECDSA を高優先度として送信するには、次の暗号の変更が必要です。

```
EECDH:EDH:HIGH:-
AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL:!aDH
```

トラブルシューティング



APPENDIX B

OpenSSL のみを使用する証明書の生成

このセクションでは、OpenSSL を使用した Expressway の秘密キーと証明書要求の生成プロセスについて説明します。これは、フリーの OpenSSL パッケージのみに依存する一般的なプロセスで、他のソフトウェアには依存しません。これは、証明書がテスト目的でネイバーデバイスとのインターフェイスを必要とする場合や、認証局と相互作用するために出力の提供を必要とする場合に適しています。

証明書要求の生成プロセスの出力は、組織の内部または外部の認証局に提供され、Expressway がネイバーデバイスとの認証に必要とする X.509 証明書を作成するために使用できます。

ここでは、プライベート認証局の管理に OpenSSL をどのように使用できるかについても簡単に説明しますが、包括的なものではありません。これらのプロセスのさまざまなコンポーネントは、サードパーティ CA とインターフェイスするときに使用されます。

OpenSSL および Mac OS X または Linux

OpenSSL はすでに Mac OS X にインストールされており、通常は Linux にインストールされています。

OpenSSL と Windows

OpenSSL をまだインストールしていない場合は、http://www.openssl.org/related/binaries.html から無料でダウンロードできます。

適切な 32 ビットまたは 64 ビットの OpenSSL を選択します。「Light」バージョンで十分です。

OpenSSL のインストール中に C++ ファイルを検出できないという警告を受信した場合は、このサイトでも使用可能な“「Visual C++ 再頒布可能パッケージ」”をロードし、OpenSSL ソフトウェアをリロードします。

この章では、次の内容について説明します。

OpenSSL を使用する証明書要求の作成

このプロセスでは、後で CA が検証する可能性があるサーバーの秘密キーと証明書要求が作成されます。これは、ローカルで作成および管理されている CA やサードパーティ CA にすることができます。

（注）
- 証明書署名要求を作成するこの方法は、コマンドが誤って入力される可能性があるため（特にSANエントリが多数ある場合）、OpenSSLでの作業に関する詳しい知識を持っている場合にのみ使用してください。関連するSANエントリが不足していると、証明書を後日再作成する必要があります。
- バージョン X8.5.1 から、ユーザー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-1、SHA-384、または SHA-512 に変更するオプションがあります。

OpenSSL のコマンドラインから証明書署名要求を生成するには、次の手順を使用します。

手順

Step 1 Expressway に SSH 接続し、root としてログインします。

Step 2 動作する新しいディレクトリを作成します：`mkdir /tmp/certtemp`

Step 3 ディレクトリを移動します：`cd /tmp/certtemp`

Step 4 編集する必要があるため、証明書署名要求に使用するOpenSSL構成ファイルをこのディレクトリにコピーします（**注：コマンドの末尾のドットもそのまま付けます**）：`cp /etc/openssl/csrreq.cnf`

Step 5 編集するためにファイルを開きます：`vi csrreq.cnf`

Step 6 「`default_md = sha1`」 の行を検索し、その行が 「`default_md = sha256`」 となるように編集します。

Step 7 「`# req_extensions = v3_req`」 行の先頭の **#** を削除して、コメントを解除します。

Step 8 「`extendedKeyUsage=serverAuth, clientAuth`」 行が、`[v3_req]` セクションで表示されていることを確認します。

Step 9 「`subjectAltName = ${ENV::CSR_ALT_NAME}`」 行を検索し、証明書内のサブジェクト代替名に希望するものがリストされるように置き換えます。例えば、「`subjectAltName = DNS:peer1vcs.example.com,DNS:peer2vcs.example.com,DNS:ClusterFQDN.example.com`」 にようにします。関連するすべてのエントリを追加したことを確認します。MRAの場合、次のように構成されます。

1. Expressway E: `DNS:<CM domain name>, DNS:<XMPP federation domain>, DNS:<federation chat alias 1>, DNS:<federation chat alias 2>`、など。
2. Expressway C: `DNS:<secure profile name 1>, DNS:<secure profile name 2>`、など。

OpenSSL のみを使用する証明書の生成

Step 10 ファイルを保存して終了します。

Step 11 次の OpenSSL コマンドを実行して、必要に応じて、VCS 「`openssl req -nodes -newkey rsa:4096 -keyout privatekey.pem -out myrequest.csr -config csrreq.cnf`」 changing the `rsa:nnnn` 用に新しい証明書署名要求と秘密キーを生成します。（nnnn = キー長、推奨値は 4096）。

Step 12 情報を入力する必要がある次の例のような出力がコンソールに表示されます。すべてを入力する必要はありませんが、一部のフィールドは必須です。

- 国
- 都道府県
- 地域の名前
- 組織名
- 共通名
- 電子メール アドレス：任意、空欄のままでも可
- チャレンジパスワード：任意、空欄のままでも可
- 任意の会社名：任意、空欄のままでも可

```
Generating a 4096 bit RSA private key
.....++
.....++
writing new private key to 'privatekey.pem'
-----
証明書要求に記載する情報を入力するように求められています。
ここで入力するのは、識別名または DN と呼ばれる情報です。
入力するフィールドはごく限られており、一部は空白のままにすることもできます。
デフォルト値が入っているフィールドもあります。
「.」を入力すると空白のままになります。
-----
国名（2 文字コード） [AU]:GB
都道府県（フルネーム）[Some-State]:Berkshire
地域の名前（市など） []:Reading
組織名（例：会社名）[Internet Widgits Pty Ltd]:Cisco
組織の部署名（例：部門）[]:CIBU
共通名（例：自分の名前）[]:exp01.example.com
電子メールアドレス []:
```

フィールドに入力すると、**myrequest.csr** と **privatekey.pem** の 2 つの新しいファイルがあります。

Step 13 （オプション）ドメインネームシステム（DNS）エントリが正常に要求に入力されているかを確認する場合は、`openssl req -text -noout -in myrequest.csr` コマンドを使用して、**myrequest.csr** ファイルを復号化します。

Step 14 証明書署名要求を選択した認証局に送信します。その認証局からは公開証明書が提供されます。

Step 15 **[メンテナンス（Maintenance）] > [セキュリティ（Security）] > [サーバー証明書（Server certificate）]** Web ページの順に選択し、「**[サーバー証明書ファイルの選択（Select the server certificate file）]**」 入力ボックスから、公開証明書を VCS にアップロードします。

Step 16 **[メンテナンス（Maintenance）] > [セキュリティ（Security）] > [サーバー証明書（Server certificate）]** Web ページの順に選択し、「**[サーバー秘密キーファイルの選択（Select the server private key file）]**」 入力ボックスから、**privatekey.pem** を VCS にアップロードします。

---

privatekey.pem を安全な場所で保管します。

OpenSSL を使用する認証局としての操作

主要な展開では、サードパーティの認証局を使用するか、または組織の IT 部門にすでに内部認証局が 1 つ存在する可能性があります。ただし、次に説明するように、OpenSSL を使用してプライベート認証局で証明書を管理することができます。

CA として機能するようにすでに OpenSSL を構成している場合は、OpenSSL を使用する署名付き証明書の作成項に進みます。

OpenSSL を CA として構成する

OpenSSL は強力なソフトウェアで、CA として動作するには、発行された証明書を追跡するためのいくつかのディレクトリとデータベースの設定が必要です。

ディレクトリとファイルのリストは、OpenSSL 構成ファイルの `[CA_default]` セクションで確認できます。デフォルトでは、必要なファイル/ディレクトリを作成します。

- **certs**、**newcerts** および **private** の 3 つのサブディレクトリがある、現在のディレクトリ内の **demoCA** ディレクトリ。
- **demoCA** ディレクトリ内にある **index.txt** という空のファイル。
- 2 桁の番号（「10」 など）を保存している **demoCA** ディレクトリ内の **serial** というファイル。

たとえば、次のコマンドを使用します。

```
mkdir demoCA

cd demoCA

mkdir certs

mkdir newcerts
```

```
mkdir private

touch index.txt

echo 10 > serial
```

OpenSSL を使用する認証局の作成

このプロセスで、認証局（CA）の秘密キーと証明書が作成され、他の証明書を検証するために使用可能になります。これは明示的にインストールされるもの以外のデバイスから信頼されることはないことに注意してください。

コマンドプロンプトから次を実行します。

手順

Step 1 **demoCA** ディレクトリにいることを確認します。

Step 2 Windows の場合：OpenSSL が **demoCA** ディレクトリにインストールされているディレクトリから **openssl.cfg** をコピーし、その名前を **openssl_local.cfg** に変更します。

Mac OS X の場合：**/System/Library/OpenSSL/openssl.cnf** を **demoCA** ディレクトリにコピーし、名前を **openssl_local.cfg** に変更します。

Step 3 テキストエディタを使用して、上記のコピーコマンドで作成された **openssl_local.cfg** ファイルを編集します。`[CA_default]` セクションに次の修正を行います。

1. `copy_extensions = copy` 行の先頭に # が無いことを確認します。# がある場合は、削除します。行がコメントアウトされたままの場合は、証明書署名要求の属性が除去され、SSL サーバーと SSL クライアントの属性は証明書に表示されません。
2. `policy = policy_match` から `policy = policy_anything` に変更します。
3. `dir = ./demoCA` to `dir =` を変更します。
4. 任意で `default_days = 365`（生成された証明書の効力が 1 年）を `default_days = 3650`（10 年、または適切な値を選択）に変更します。
5. ファイルを保存します。

Step 4 次のコマンドを実行して、CA の秘密キーを生成します。

```
openssl genrsa -aes256 -out private/cakey.pem 4096
```

ここで、秘密キーを暗号化するパスワードが求められるので、強力なパスワードを選択し、安全な場所に記録します。cakey.pem ファイルが CA 証明書を作成し、他の証明書に署名するために使用されるので、安全に保持する必要があります。

Step 5 次のコマンドを実行して、CA 証明書を生成します。

Windows の場合：`openssl req -new -x509 -days 3650 -key private/cakey.pem -config openssl_local.cfg -sha1 -extensions v3_ca -out cacert.pem`

OS X の場合：`openssl req -new -x509 -days 3650 -key private/cakey.pem -config openssl_local.cfg -sha1 -extensions v3_ca -out cacert.pem`

Step 6 キーのパスフレーズを入力し、次の項目を含む要求されたデータを入力します。

- 国
- 都道府県
- 地域の名前
- 組織名
- 組織単位
- 共通名：通常は、この CA の担当者の名前になります
- 電子メールアドレス：任意、空欄のままでも可

要求されたデータを入力すると、処理が完了し、認証局の証明書 **cacert.pem** が使用可能になります。

OpenSSL を使用する署名付き証明書の作成

このプロセスでは、以前に生成された証明書要求を使用して生成された CA キーでサーバー証明書に署名します。

コマンドプロンプトから次を実行します。

手順

Step 1 **demoCA** ディレクトリにいることを確認します。

Step 2 証明書要求ファイル（**certcsr.pem**）が使用できることを確認します。

- Expressway を使用して証明書要求を作成する場合は、次の手順を実行します（推奨プロセス）。

  Expressway からダウンロードしたファイルを **demoCA** ディレクトリにコピーし、名前を **certcsr.pem** に変更します。

- OpenSSL を使用して証明書要求を作成する場合は、次の手順を実行します。

  以前に生成された証明書要求を **demoCA** ディレクトリにコピーして、次のコマンドを実行して PEM フォーマットに変換します。

  ```
  openssl req -in certcsr.der -inform DER -out certcsr.pem -outform PEM
  ```

Step 3 次のコマンドを実行して署名済みサーバー証明書を生成します。

```
openssl ca -config openssl_local.cfg -cert cacert.pem -keyfile private/cakey.pem -in
certcsr.pem -out certs/server.pem -md sha1
```

「failed to update database TXT_DB error number 2」というエラーメッセージを受信した場合、index.txt ファイルの内容を削除してからコマンドを再実行します。

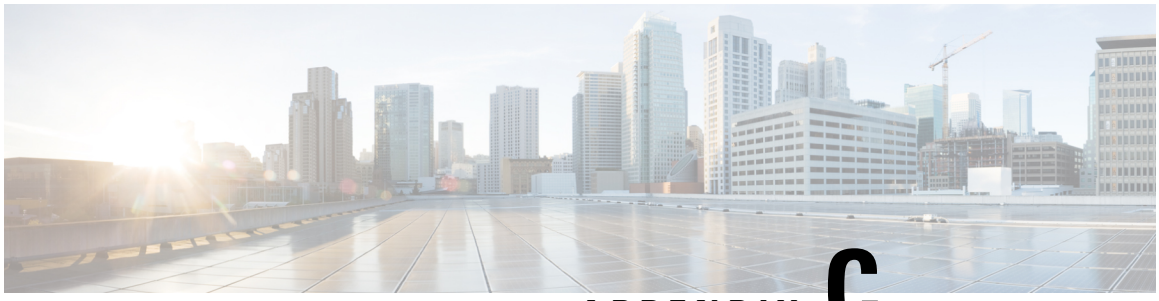
Step 4 CA の秘密キーのパスワードを入力するよう求められます。

サーバー用の署名済み証明書が **demoCA/certs/server.pem** として使用可能になります。

OpenSSL OpenSSL を使用する自己署名付き証明書の作成

自己署名証明書を作成することは推奨しません。Unified Communications 展開では動作しません。

その代わりに、前述のように OpenSSL を使用して認証局を作成する必要があります。



APPENDIX C

DER 証明書ファイルを PEM フォーマットに変換

秘密キー、ルート（CA）証明書およびサーバー/クライアント証明書は、サードパーティ製ツール（または認証局から購入したツール）を使用して生成でき、PEM（必須フォーマット、拡張子 .pem）または DER（拡張子 .cer）フォーマットのファイルとして生成できます。

証明書は、Expressway で使用するには PEM フォーマットにする必要があります。DER から PEM フォーマットへの変換は、次のセクションに説明されているように、OpenSSL または Windows を使用する 2 通りの方法のいずれかで行うことができます。

OpenSSL を使用した DER 証明書ファイルの PEM ファイルへの変換

DER から PEM フォーマットへ変換するには、openssl を実行しているシステム上で次のコマンドを実行します。

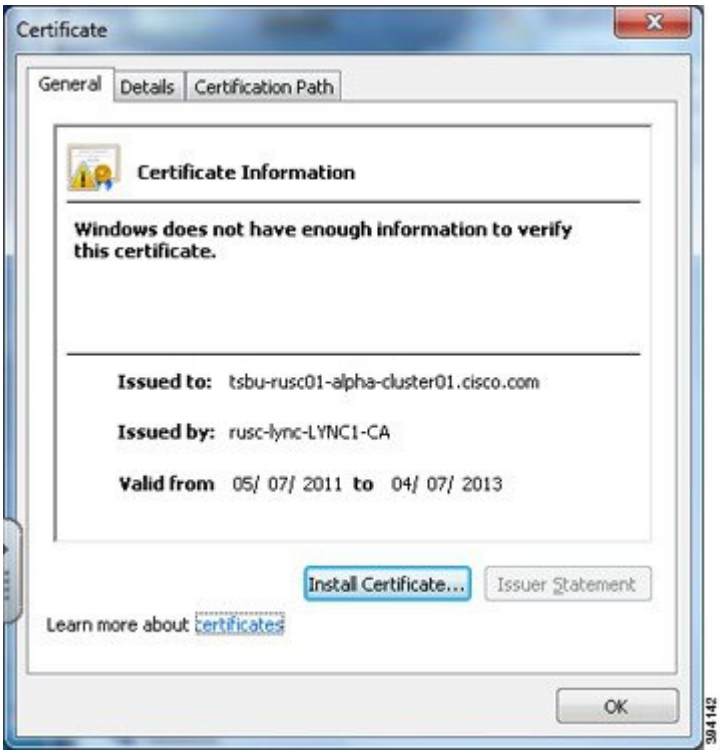
```
openssl x509 -in <filename>.cer -inform DER -out <filename>.pem -outform PEM
```

Microsoft Windows を使用した DER 証明書ファイルの PEM ファイルへの変換

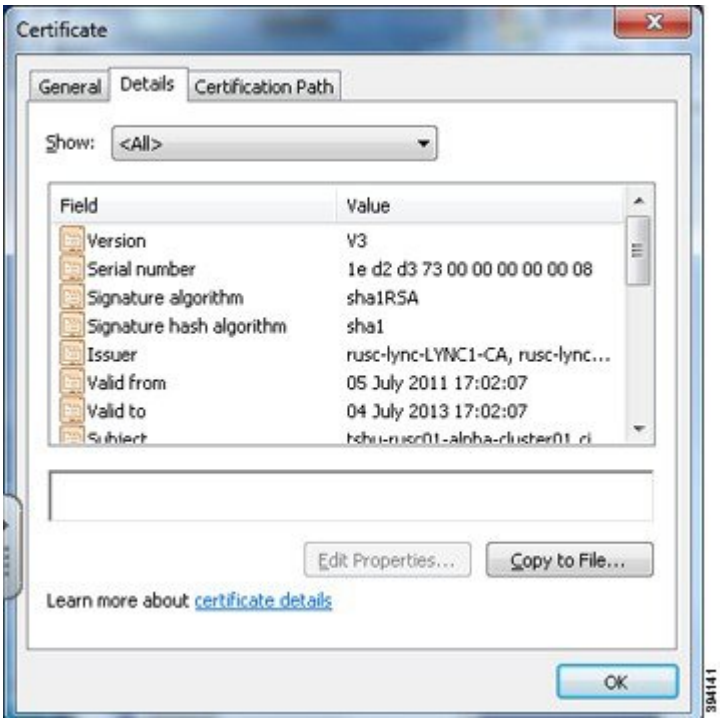
Microsoft Windows を使用して DER から PEM フォーマットへ変換するには、次の手順を実行します。

1. 変換する DER ファイルをダブルクリックします（拡張子は「.cer」である可能性があります）。

DER 証明書ファイルを PEM フォーマットに変換



2. **[詳細（Details）]** タブを選択します。



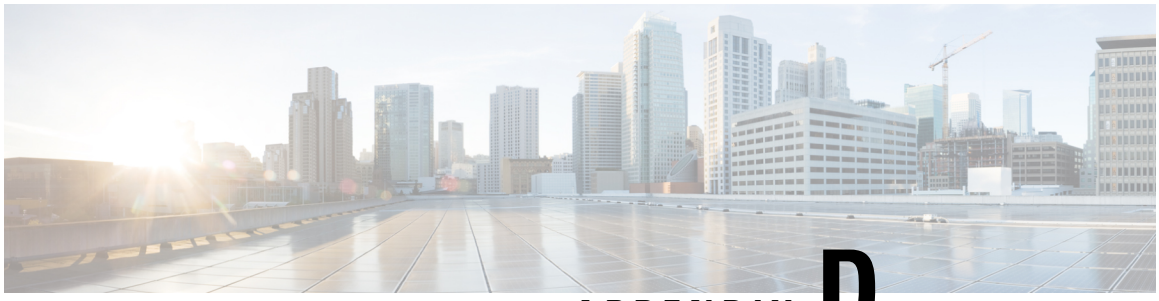
3. **[ファイルにコピー…（Copy to File…）]** をクリックします。
4. **[ようこそ（Welcome）]** ページで **[次へ（Next）]** をクリックします。

DER 証明書ファイルを PEM フォーマットに変換

5. *[Base-64 encoded X.509（.CER）]* を選択して、**[次へ（Next）]** をクリックします。

6. **[参照（Browse）]** をクリックして要求されるファイルの宛先（たとえば **server.pem**）を選択し、**[次へ（Next）]** をクリックします。
7. [完了（Finish）] をクリックします。
8. **server.pem.cer** から **server.pem** にファイル名を変更します。
9. これは、本書のExpressway に証明書をキーをロードする項で使用します。

DER 証明書ファイルを PEM フォーマットに変換



APPENDIX D

証明書のデコード

ここでは、証明書の内容を復号化して表示する方法についていくつか説明します。

OpenSSL

PEM ファイル（**cert.pem** など）は、次のコマンドによって復号化できます。

```
openssl x509 -text -in cert.pem
```

DER ファイル（**cert.cer** など）は、次のコマンドによって復号化できます。

```
openssl x509 -text -inform DER -in cert.cer
```

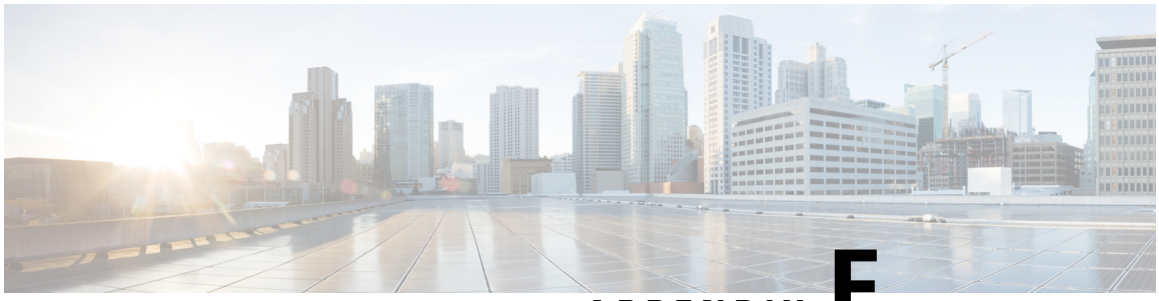
Firefox

Firefox の場合、アドレスバーの **[セキュリティ情報（Security Information）]** ボタンをクリックし **[詳細情報（More Information）]** > **[証明書を表示（View Certificate）]** の順に選択すると、Web サイトで使用中の証明書を表示できます。

Internet Explorer

Internet Explorer では、アドレスバーの右側にあるロックアイコンをクリックすると、Web サイトで使用されている証明書を表示できます。[Web サイトの識別（Website Identification）] ダイアログが表示されます。下にある **[証明書の表示（View Certificates）]** リンクをクリックします。

証明書のデコード



APPENDIX E

AD CSによるクライアント証明書とサーバー証明書の発行の有効化

Note Microsoft Active Directory Certificate Services（AD CS）の CA コンポーネントは、クライアントまたはサーバーとして Expressway の認証に使用できる証明書を発行できる必要があります。

Windows Server 2008 Standard R2（およびそれ以降）の AD CS は、証明書テンプレートを作成すると、これらのタイプの証明書を発行できます。**以前のバージョンの Windows Server Standard Edition は適していません。**

AD CS のデフォルトの「Web サーバー」証明書テンプレートは、サーバー認証用の証明書を作成します。相互認証でネイバーまたはトラバーサルゾーンを設定する場合（**[TLS 検証モード（TLS verify mode）]** が有効化）は、Expressway のサーバー証明書もクライアント認証が必要です。

サーバーおよびクライアント認証で証明書テンプレートを設定するには、次の手順を実行します。

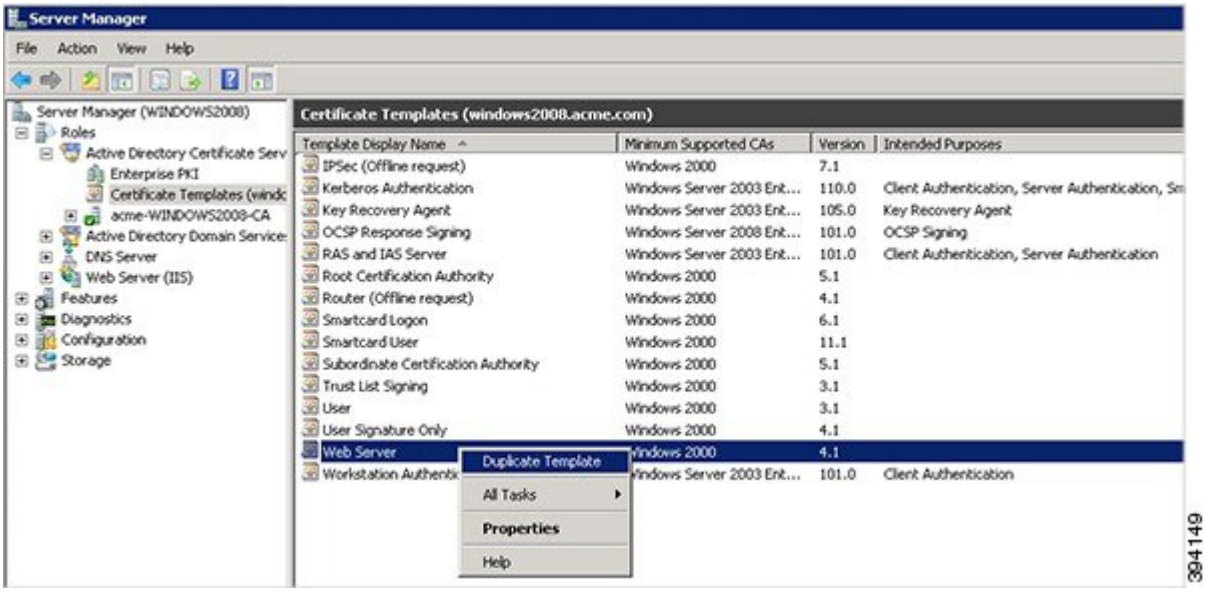
1. Windows で、**サーバーマネージャ** を開始します（**[開始（Start）]**>**[管理ツール（Administrative Tools）]** > **[サーバーマネージャ（Server Manager）]**）。

   （サーバーマネージャは、Windows のサーバーエディションに含まれる機能です。）

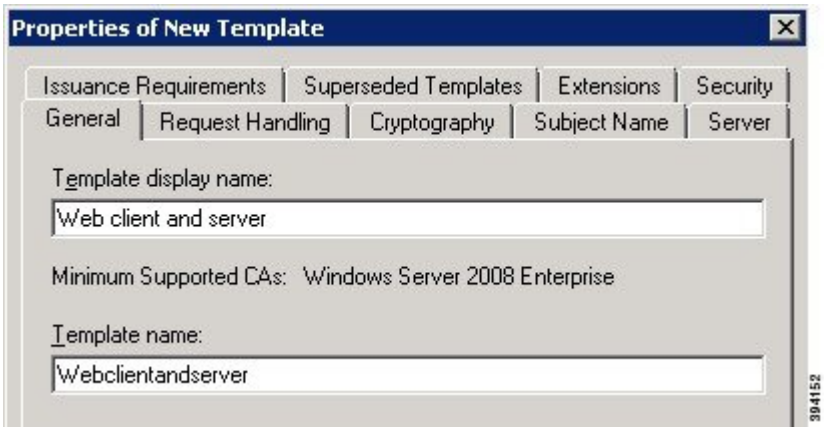
2. **[Server Manager]** ナビゲーションツリーを展開して、**[ロール（Roles）]** > **[Active Directory 証明書サービス（Active Directory Certificate Services）]** > **[証明書テンプレート（<ドメイン>）（Certificate Templates (<domain>)）]** の順に選択します。

3. **[Web サーバー（Web Server）]** を右クリックして、**[テンプレートの重複（Duplicate Template）]** を選択します。

AD CS によるクライアント証明書とサーバー証明書の発行の有効化

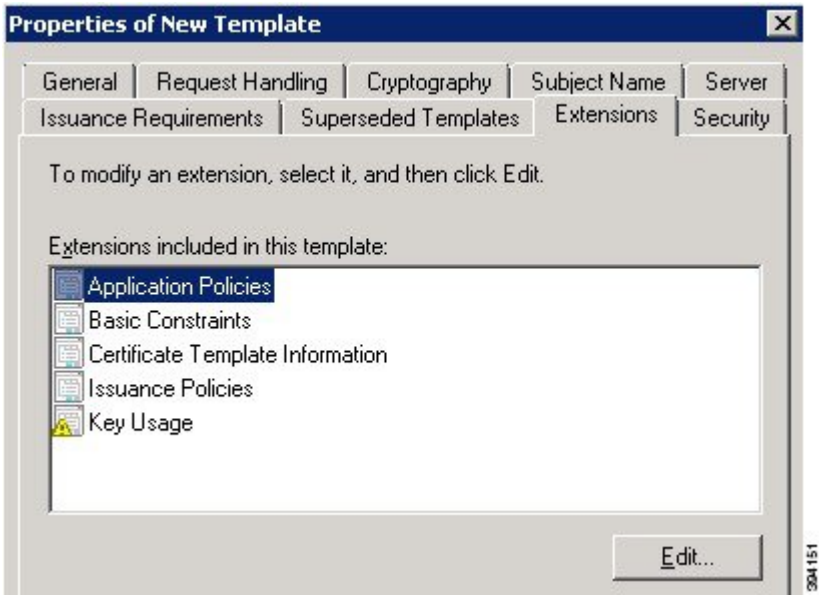


4. **[Windows Server 2003 Enterprise]** を選択し、**[OK]** をクリックします。
5. **[全般（General）]** タブで、**[テンプレートの表示名（Template display name）]** と **[テンプレート名（Template name）]** をたとえば `Web client and server` や `Webclientandserver` などのように入力します。

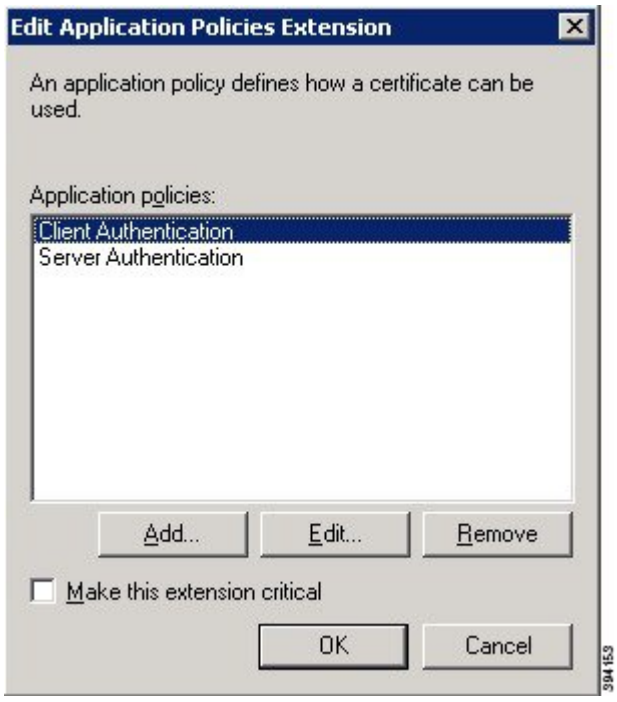


6. **[拡張（Extensions）]** タブで、**[アプリケーションポリシー（Application Policies）]** を選択し、**[編集（Edit）]** をクリックします。

AD CS によるクライアント証明書とサーバー証明書の発行の有効化



7. **[クライアント認証（Client Authentication）]** をアプリケーションポリシーに追加します。
   a. [Add] をクリックします。
   b. **[クライアント認証（Client Authentication）]** を選択し、**[OK]** をクリックします。
   c. [OK] をクリックします。

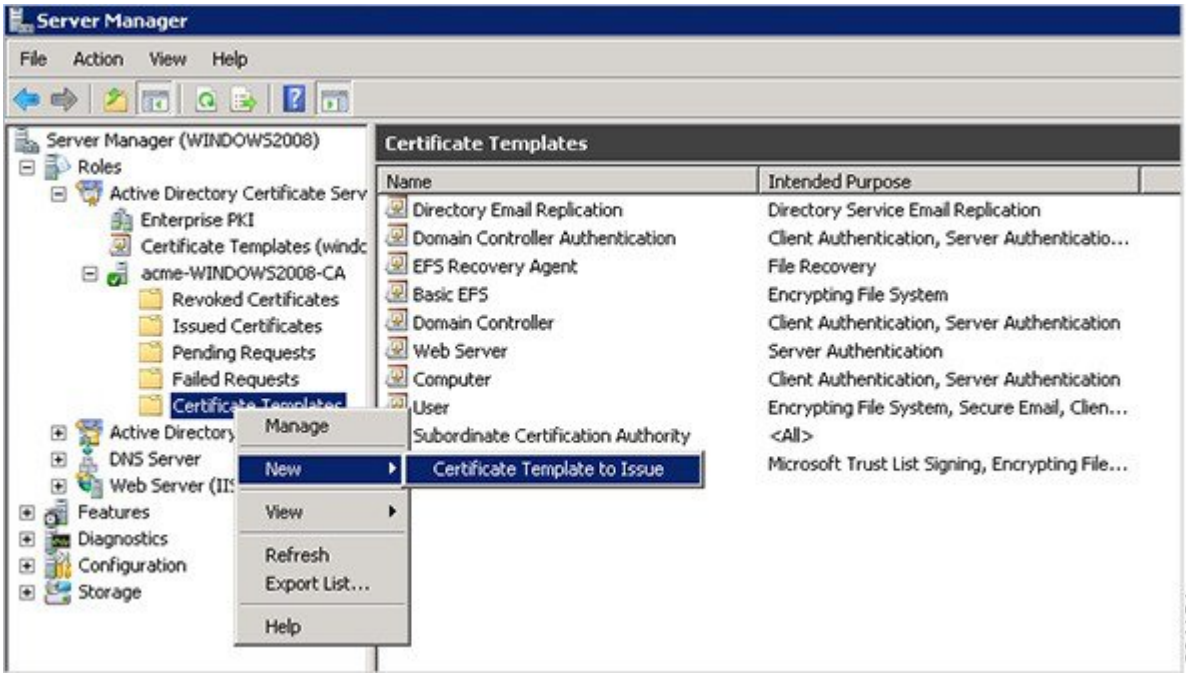


8. **[OK]** をクリックして、新しいテンプレートの追加を完了します。
9. 認証局に新しいテンプレートを追加するには、次の手順を実行します。

AD CS によるクライアント証明書とサーバー証明書の発行の有効化

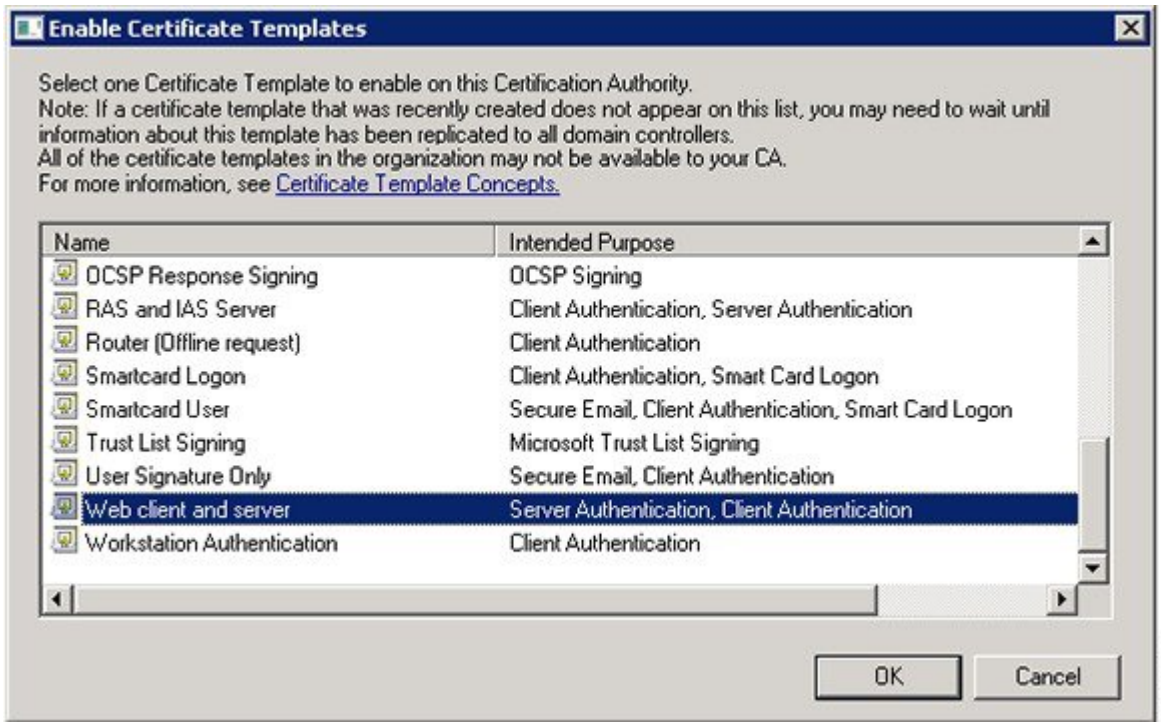
a. **[ロール（Roles）]** > **[Active Directory 証明書サービス（Active Directory Certificate Services）]** > **[<ご自身の証明機関>]** を選択します。

b. **[証明書テンプレート（Certificate Templates）]** を右クリックして、**[新規（New）]** > **[発行する証明書テンプレート（Certificate Template to Issue）]** を選択します。



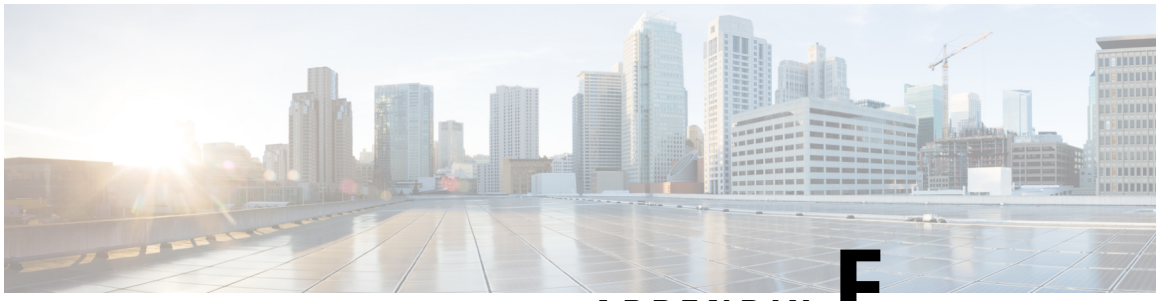
c. 新しい **[Web クライアントとサーバー（Web client and server）]** テンプレートを選択し、**[OK]** をクリックします。

AD CS によるクライアント証明書とサーバー証明書の発行の有効化



新しい **[Web クライアントとサーバー（Web client and server）]** テンプレートが証明書要求をその Microsoft 認証局に送信するときに使用できるようになります。

AD CS によるクライアント証明書とサーバー証明書の発行の有効化



APPENDIX F

Microsoft 認証局を使用する要求の承認と証明書の生成

ここでは、Microsoft 認証局を使用して、証明書要求を承認し PEM 証明書ファイルを生成する方法について説明します。

Note Microsoft Active Directory Certificate Services（AD CS）の CA コンポーネントは、クライアントまたはサーバーとして Expressway の認証に使用できる証明書を発行できる必要があります。

Windows Server 2008 Standard R2（およびそれ以降）の AD CS は、証明書テンプレートを作成すると、これらのタイプの証明書を発行できます。**以前のバージョンの Windows Server Standard Edition は適していません。**

1. 証明書要求ファイル（たとえば、OpenSSL 経由で生成した場合は **certcsr.der** など）を、Microsoft 認証局のアプリケーションがインストールされているサーバーのデスクトップなどの場所にコピーします。
2. コマンドプロンプトから証明書要求を送信します。
   - サーバー認証とクライアント認証で証明書を生成するには（これはネイバーまたはトラバーサルゾーンを相互認証（TLS 確認モード）で構成する場合に必要になります）、次を入力します。

     ```
     certreq -submit -attrib "CertificateTemplate:Webclientandserver"

     C:\Users\<user>\Desktop\certcsr.der
     ```

     `Webclientandserver` 証明書テンプレートの設定方法の詳細については、AD CS によるクライアント証明書とサーバー証明書の発行の有効化証明書を発行するための AD CS の有効化」を参照してください。
   - サーバー認証のみを使用して証明書を生成するには、次を入力します。

     ```
     certreq -submit -attrib "CertificateTemplate:WebServer"
     C:\Users\<user>\Desktop\certcsr.der
     ```

   これにより [認証局（Certification Authority）] ウィンドウが開きます。

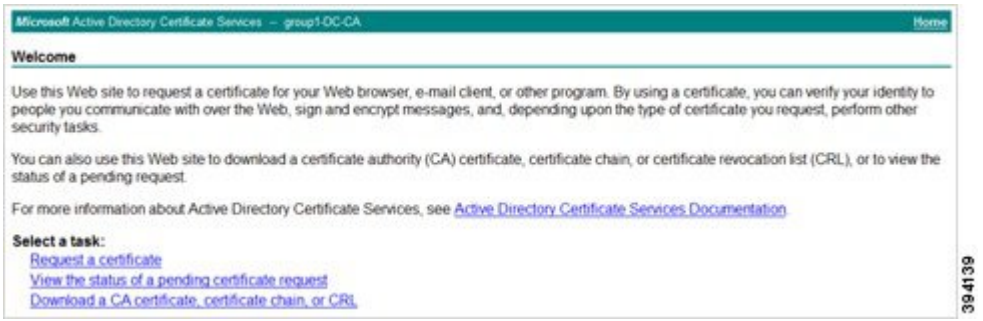
Microsoft 認証局を使用する要求の承認と証明書の生成

Note コマンドは、管理者ユーザーとして実行する必要があります。

3. 使用する**認証局**を選択し（通常は 1 つのみ提供されます）、**[OK]** をクリックします。
4. 要求されたら、**server.cer** などの名前を付けてその証明書を保存します（デフォルトの**[ライブラリ（Libraries）]**>**[ドキュメント（Documents）]**フォルダが使用されない場合は必要なフォルダを閲覧してください）。
5. Expressway で使用するために、名前を **server.cer** から **server.pem** に変更します。

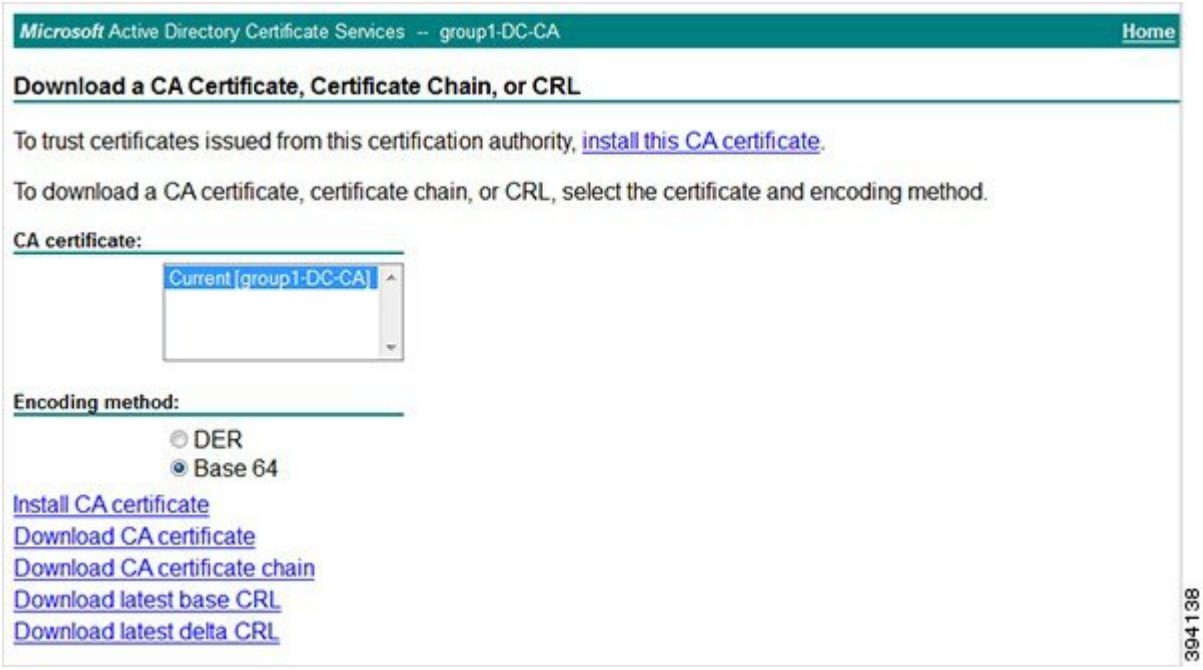
Microsoft の CA 証明書の取得

1. Web ブラウザで、[<Microsoft Certificate Server の IP または URL>/certsrv（<IP or URL of the Microsoft Certificate Server>/certsrv）] に移動し、ログインします。

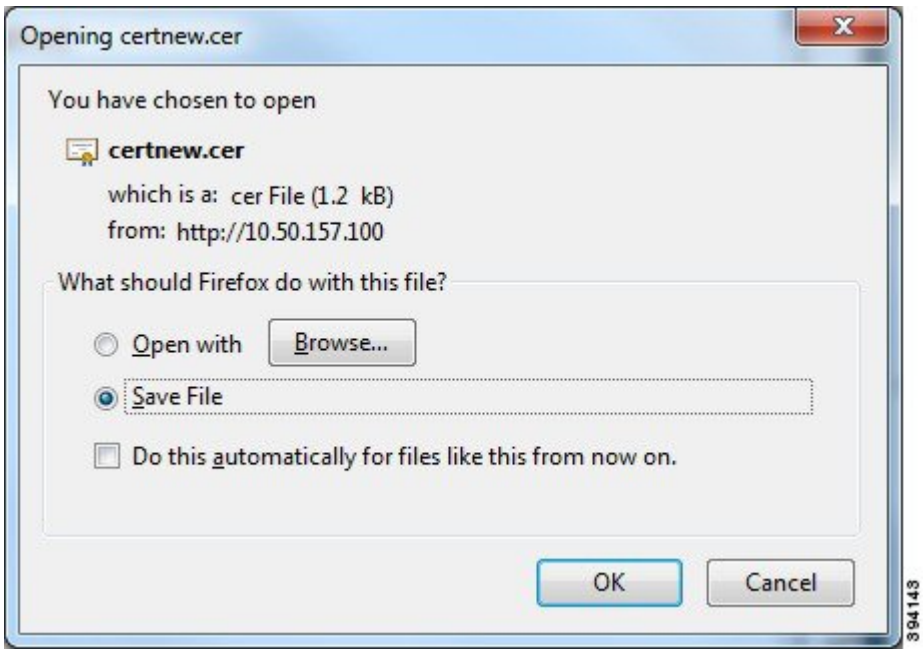


2. [CA 証明書、証明書チェーン、または CRL のダウンロード（Download a CA certificate, certificate chain or CRL）] を選択します。

Microsoft 認証局を使用する要求の承認と証明書の生成



3. **[エンコードメソッド（Encoding Method）]** で **[Base 64]** を選択します。
4. **[CA 証明書のダウンロード（Download CA certificate）]** リンクをクリックします。



5. **[ファイルの保存（Save File）]** を選択し、**[OK]** をクリックします。
6. 名前を **certnew.cer** から **certnew.pem** に変更します。

ファイル **server.pem** と **certnew.pem** が使用可能になります。

Microsoft 認証局を使用する要求の承認と証明書の生成

本書のExpressway に証明書をキーをロードする項を読み、**server.pem** および **certnew.pem** を Expressway にアップロードする方法を確認します。

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。