# Video Communication Server 認証局の設定例

## 目次

[概要](#)
[前提条件](#)
[要件](#)
[使用するコンポーネント](#)
[背景説明](#)
[設定](#)
[確認](#)
[トラブルシューティング](#)

## 概要

このドキュメントでは、Video Communication Server（VCS）での証明書認証について説明します。 VCS を識別する証明書には、その VCS を認識してトラフィックのルーティング先とする名前が含まれています。 この目的で VCS が複数の名前で認識される場合（クラスタの一部となっている場合など）、X.509 のサブジェクト データで、そのことを表す必要があります。 証明書には、VCS 自体とその VCS が一部となっているクラスタの両方の完全修飾ドメイン名（FQDN）が含まれている必要があります。 証明書がクラスタ ピアで共有される場合、考えられるすべてのピア FQDN をリストする必要があります。

VCS の証明書は次の目的で必要になります。

- Transport Layer Security（TLS）によるセキュア HTTP（HTTPS）接続
- Session Initiation Protocol（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
- Cisco Unified Communications Manager（CUCM）、Cisco TelePresence Management Suite（TMS）、Lightweight Directory Access Protocol（LDAP）サーバ、Syslog サーバなどの他のシステムとの接続

VCS 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、VCS に接続する他のデバイスを検証します。

## 前提条件

### 要件

このドキュメントに関しては個別の要件はありません。

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- VCS： リリース 8.1 および 8.1.1
- 認証局：Microsoft Windows 2008 R2 Enterprise

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

## 背景説明

VCS リリース 8.1.1 では、コラボレーション エッジ モバイル リモート アクセス（MRA）機能をサポートするため、VCS-Control と VCS-Expressway 間に TLS 接続が必要です。

TLS を設定するには、VCS に必要な証明書をアップロードする必要があります。 それには、次の 3 つの方式があります。

- OpenSSL
- エンタープライズ CA
- サードパーティ CA

VCS-Control と VCS-Expressway 間の TLS 接続には、次の 2 つの属性が必要です。

- TLS クライアント認証
- TLS Web サーバ認証

OpenSSL については『VCS 証明書導入ガイド』で説明しているので、このドキュメントではエンタープライズ CA 方式に重点を置きます。

CA をインストールすると、デフォルトで Web サーバ証明書がインストールされます。 ただし、このテンプレートを使用して VCS-Control と VCS-Expressway 間の TLS 接続用証明書を生成することはできません。 Web サーバ属性だけで生成された証明書を VCS にアップロードしようとすると、以下に示すエラーが発生します。

サーバ証明書を確認するには、[Maintenance] > [Server Certificate] を選択します。 [Decode Certificate] をクリックします。 [Extended Key Usage] セクションを確認します。

## 設定

前述のとおり、TLS 接続にはクライアント属性と Web サーバ属性が必要です。 デフォルトのテンプレートはないので、新規のテンプレートを作成できます。 TLS クライアント認証と TLS Web サーバ認証の両方の属性を持つ新規テンプレートを生成するには、以下の手順に従います。

1. [Certificate Authority] を開くか、Microsoft Management Console（MMC）コンソールに移動します。 [Add/Remove Snapin] をクリックし、[Certificate Authority] を選択します。 左ペインで CA を展開し、[Certificate Template] を選択します。 証明書テンプレートを右クリックし、[Manage] を選択します。

2. [Web Server] 証明書テンプレートを右クリックし、[Duplicate Template] を選択します。.
3. [Windows Server 2003 Enterprise] オプション ボタンをクリックします ( テンプレートを Web 登録で使用可能にする場合 ) 。 [OK] をクリックします。
4. [Template display name] フィールドにテンプレート名を入力します。 テンプレートには要件に応じた名前を付けます ( たとえば、「web server client 2003」 ) 。
5. [Extensions] タブをクリックし、[Application policy] を選択します。 [Edit] をクリックします。
6. [Add Application Policy] ダイアログボックスで、[Client Authentication] を選択します。 [OK] をクリックします。
7. [Edit Application Policies Extension] ダイアログボックスで、[OK] をクリックします。
8. MMC コンソールまたは CA ウィンドウで、[Certificate Template] を右クリックします。 [New] > [Certificate Template to Issue] を選択します。
9. [Enable Certificate Templates] ダイアログボックスで、新しく作成したテンプレートを選択します。 [Intended Purpose] 列でテンプレートを確認します。 [OK] をクリックします。

## 確認

ここでは、設定が正常に動作していることを確認します。

次の手順を実行します。

1. 新しい証明書を発行するために、要求した証明書テンプレートが使用可能であることを確認します。**注:** テンプレートが Web 登録で使用可能になるのは、証明書テンプレートを作成する際に、テンプレートを Windows 2003 として選択した場合のみです。
2. 手順に従って、VCS から証明書署名要求 ( CSR ) を生成し、新しいテンプレートで署名された証明書を取得します。
3. 取得した証明書に、クライアント属性と Web サーバ属性の両方があることを確認します。

# トラブルシューティング

このセクションでは、設定のトラブルシューティングに役立つ情報を提供します。

テンプレートを Web 登録で使用できない場合は、**certsrv** にアクセスするユーザに必要な権限が割り当てられているかどうかを確認します。

前述したように、Windows 2008 のテンプレートは Web 登録では使用できません。 詳細については、『2008 Web 登録およびバージョン 3 テンプレート』を参照してください。