# Expressway証明書のトラブルシューティング

## 内容



## はじめに

このドキュメントでは、証明書の仕組みと、Expresswayサーバの証明書に関する最も一般的な問題とヒントについて説明します。

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- ExpresswayおよびVideo Communications Server(VCS)サーバ
- セキュアソケットレイヤ(SSL)
- 証明書
- Telepresenceデバイス
- モバイルおよびリモート アクセス
- コラボレーションの導入

### 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いています。

- Expressway x14

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

## 背景説明

SSLと証明書は標準であり、他のデバイスやブランドでも同じように機能します。このドキュメントでは、Expresswayで使用される証明書について説明します。

### 定義

証明書は、2つのデバイス間でセキュアな接続を確立するために使用されます。サーバまたはデバイスのIDを認証するデジタル署名です。Hypertext Transfer Protocol Secure(HTTPS)やSession Initiation Protocol(SIP)Transport Layer Security(TLS)などのプロトコルが機能するには、証明書を使用する必要があります。

証明書について説明する際に使用されるさまざまな用語：

- 証明書署名要求(CSR)：後で署名してクライアント証明書またはサーバ証明書に変換するためにデバイスを識別する名前で作成されるテンプレート
- 証明書：署名済みのCSR。これらは一種のIDであり、SSLネゴシエーションで使用するためにデバイスにインストールされます。これらの証明書は、それ自体または認証局によって署名できます。
- 証明書の署名：対象の証明書を検証するIDは正当なものであり、別の証明書の形式で提示されます。
- 自己署名証明書：自身で署名されたクライアントまたはサーバの証明書
- 認証局(CA)：証明書に署名するエンティティ
    - 中間証明書：自身ではなく、別のCA証明書によって署名されるCA証明書。通常はルート証明書によって署名されますが、別の中間証明書によって署名されることもあります
    - ルート証明書：自身で署名されたCA証明書

### 基本原則

クライアントがサーバと通信し、SSL通信を開始すると、クライアントは証明書を交換します。証明書は、後でデバイス間のトラフィックを暗号化するために使用されます。交換の一環として、デバイスは証明書が信頼できるかどうかも判断します。証明書が信頼できるかどうかを判断するには、次のような複数の条件を満たす必要があります。

- サーバに接続するために最初に使用される完全修飾ドメイン名(FQDN)が、サーバによって提示される証明書内の名前と一致します。
    - たとえば、ブラウザでWebページを開くと、cisco.comは証明書を提供するサーバのIPアドレスを解決します。この証明書は、信頼されるためには名前としてcisco.comを含める必要があります。

- サーバから提示されたサーバ証明書に署名したCA証明書（または自己署名の場合は同じサ

ーバ証明書）が、デバイスのCA信頼できる証明書リストに存在します。
    - デバイスには信頼できるCA証明書のリストがあり、コンピュータにはよく知られたパブリック認証局があらかじめ作成されたリストが含まれていることがよくあります。

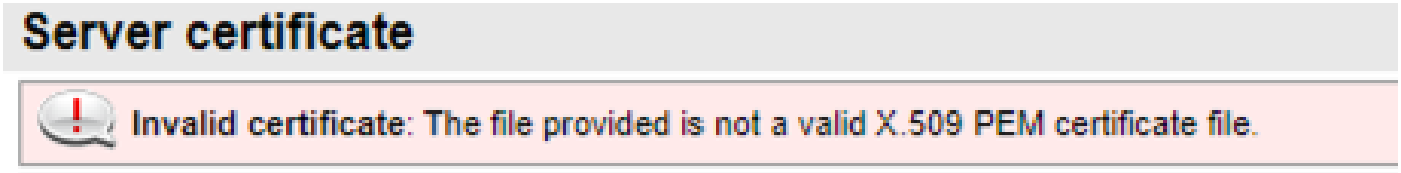
- 現在の日付と時刻は、証明書の有効期間内です。
    - 認証局はCSRに一定時間だけ署名します。これはCAによって決定されます。

- 証明書は失効していません。
    - 多くの場合、パブリック認証局では、証明書内部に証明書失効リスト(CRL)URLが含まれています。これにより、証明書を受信したパーティは、証明書がCAによって失効されていないことを確認できます。

# 一般的な問題

## Expressway証明書のアップロードが失敗する

この問題は、いくつかの状況で発生します。これらは別の説明エラーを引き起こします。



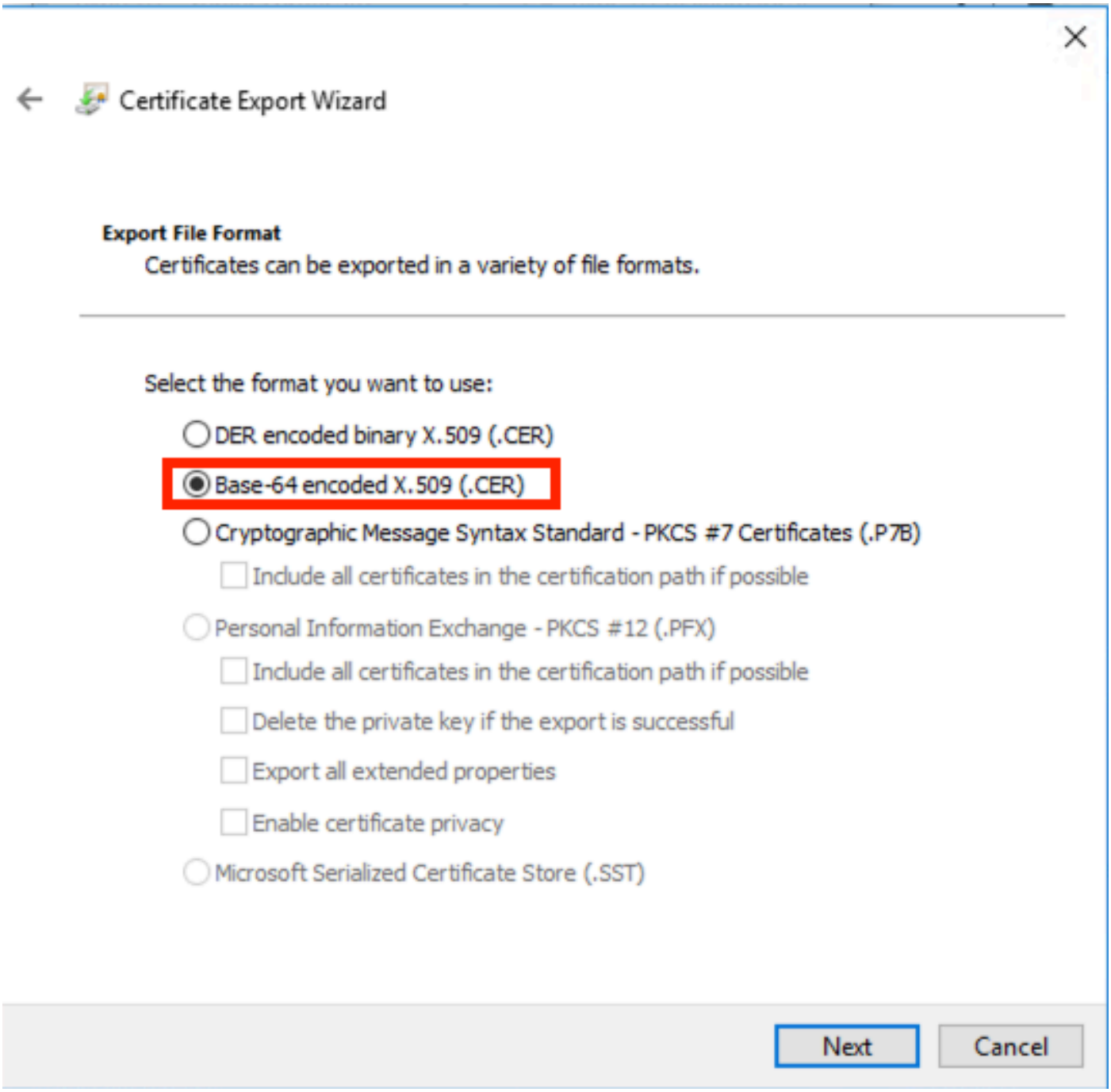

証明書の形式が無効

この最初のエラーは、証明書が有効な形式でない場合に発生します。ファイル拡張子は重要ではありません。

証明書が開かない場合は、正しい形式でCAから新しい証明書を要求できます

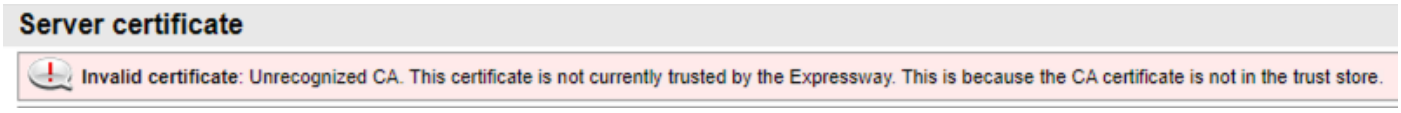
証明書が開いている場合は、次の手順を実行します。

ステップ 1：証明書を開き、Detailsタブに移動します。
ステップ 2：Copy to Fileを選択します。
ステップ 3：ウィザードに従って、Base-64 encodedが選択されていることを確認します。




証明書の形式の選択

ステップ 4：保存したら、Expresswayに新しいファイルをアップロードします。




信頼できないCA証明書チェーン

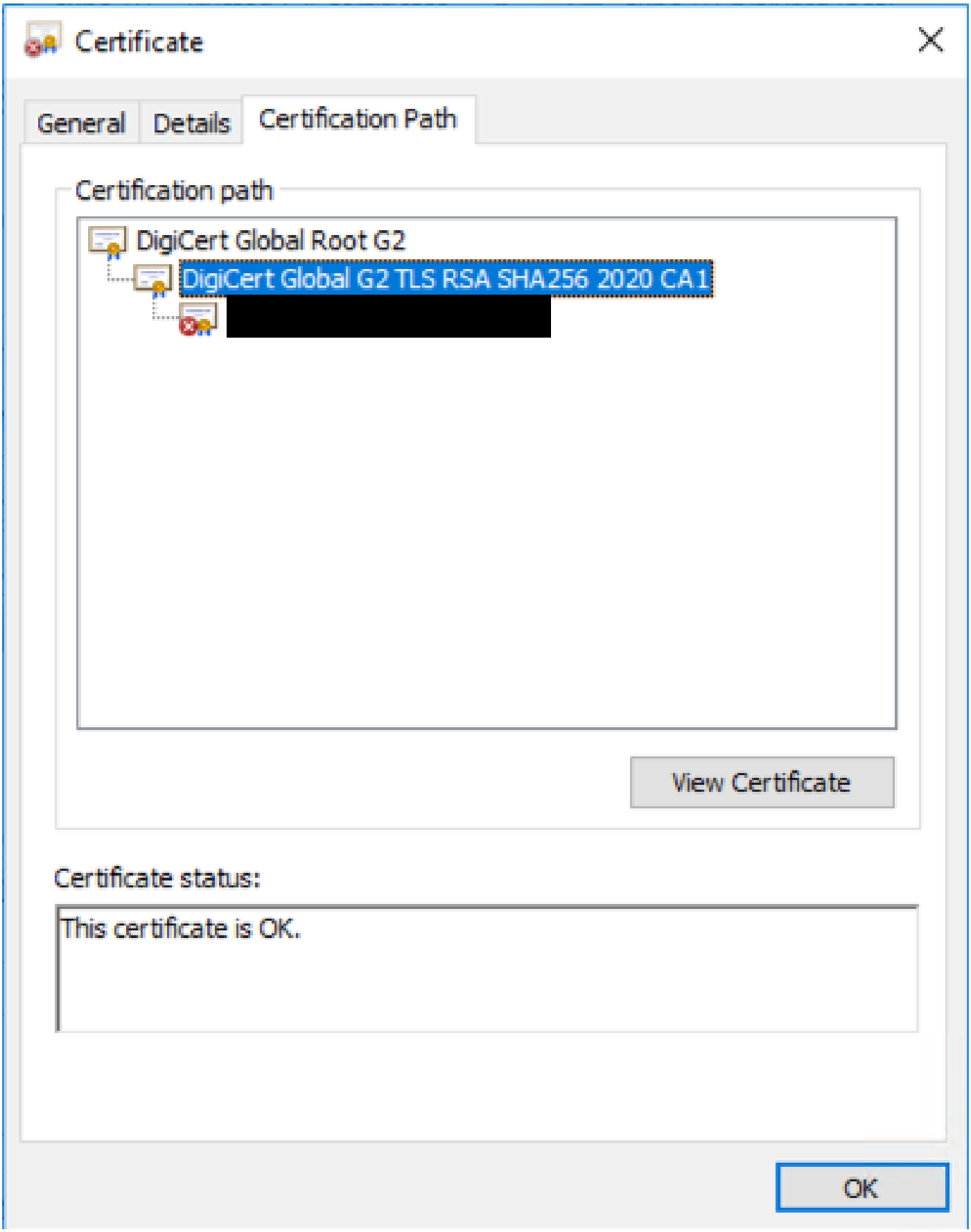
このエラーは、サーバ証明書に署名したCA証明書が信頼されていない場合に発生します。サーバ証明書をアップロードする前に、サーバはチェーン内のすべてのCA証明書を信頼する必要があります。

通常、CAは署名付きサーバ証明書とともにCA証明書を提供します。これらがある場合は、次の

ステップ6に進んでください。

CA証明書が使用できない場合は、サーバ証明書から取得できます。手順は以下のとおりです。

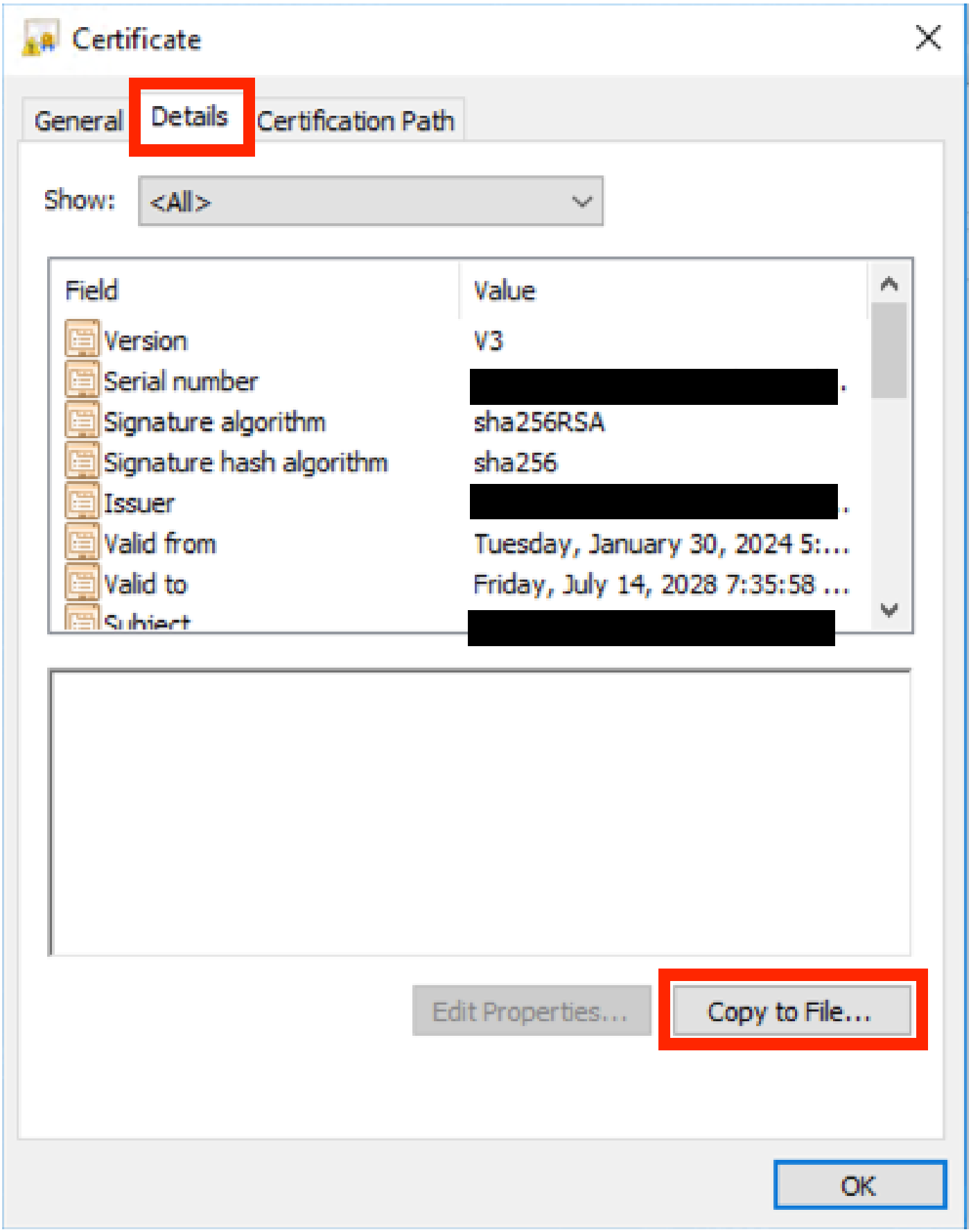
ステップ 1：サーバ証明書を開きます。
ステップ 2：Certification Pathタブに移動します。最上位の証明書は、ルートCA証明書と見なされます。下の方はサーバ証明書で、中間のすべての証明書は中間CA証明書と見なされます。
ステップ 3：CA証明書を選択し、View Certificateを選択します。




認証パス

ステップ 4：Detailsタブに移動し、前の手順に従って証明書を別のファイルに保存します。

ステップ 5：存在するすべてのCA証明書に対して、これらの手順を繰り返します。




Certificate Detailsタブ

すべてのCA証明書が使用可能になったら、Expresswayの信頼済みCA証明書リストにアップロー

ドします。

手順 6：Expresswayサーバで、Maintenance > Security > Trusted CA Certificateの順に選択します。
手順 7：Choose File and uploadを選択します。
ステップ 8：各CA証明書について手順7を繰り返します。
ステップ 9：すべてのCA証明書が信頼リストにアップロードされたら、サーバ証明書をサーバにアップロードします。

## エラー「TLS Negotiation Error」によるトラバーサルゾーンのダウン

このエラーは、Expressway-CとExpressway-Eの間のSSL交換が正常に完了していない場合に発生します。この問題を引き起こす可能性のあるいくつかの例を次に示します。

- ホスト名が、提示された証明書の名前と一致しません。
  - Expressway-Cトラバーサルゾーンに設定されたピアアドレスが、Expressway-Eサーバ証明書の名前の少なくとも1つと一致していることを確認します
- TLS検証名が、提示された証明書の名前と一致しません。
  - Expressway-Eトラバーサルゾーンで設定されたTLS検証名が、Expressway-Cサーバ証明書の名前の1つと一致することを確認します。クラスタ設定の場合は、Expressway-CクラスタのFQDNをTLSとして設定することをお勧めします。この名前はクラスタのすべてのノードに存在する必要があるため、名前を確認します。
- CA証明書がサーバによって信頼されていない
  - サーバ証明書をアップロードする前に各サーバが独自のCA証明書を信頼する必要があるのと同様に、他のサーバもサーバ証明書を信頼するためにこれらのCA証明書を信頼する必要があります。このためには、両方のExpresswayサーバの認証パスからのすべてのCA証明書が、関係するすべてのサーバの信頼済みCAリストに存在することを確認します。CA証明書は、このドキュメントで前述した手順で抽出できます。

## 証明書の更新後にトラバーサルゾーンはアップするがSSHはダウンする


SSHトンネル障害

このエラーは、通常、証明書の更新後に1つ以上の中間CA証明書が信頼されていない場合、ルートCA証明書の信頼によってトラバーサルゾーン接続が可能になる場合に発生しますが、SSHトンネルはより詳細な接続であるためチェーン全体が信頼されていない場合に失敗する可能性があります。証明書の更新によってこの問題が引き起こされるように、証明機関によって中間CA証明書が変更されることがあります。すべての中間CA証明書がすべてのExpressway信頼リストにアップロードされていることを確認します。

## アップグレードまたは証明書の更新後にモバイルおよびリモートアクセスログイン

が失敗する

証明書が原因でログインが失敗する方法は数多くありますが、Expresswayソフトウェアの新しいバージョンでは、セキュリティ上の理由から、以前は行われていなかった場所で強制的に証明書を検証するソフトウェア変更が実装されています。

これについては、次のページで詳しく説明します。トラフィックサーバが証明書検証を実施する

回避策からわかるように、Expressway-C CA証明書がCisco Unified Communications Managerにtomcat-trustおよびcallmanager-trustとしてアップロードされていることを確認し、必要なサービスを再起動します。

## モバイルおよびリモートアクセス(MRA)ログイン時のJabberの証明書アラーム


Jabberの信頼できない証明書の警告

この動作は、アプリケーションで使用されているドメインがExpressway-Eサーバ証明書のサブジェクト代替名と一致しない場合に発生します。
例の.comまたは代替collab-edge.example .comが、証明書に存在するサブジェクト代替名の1つであることを確認します。

# 関連情報

シスコのテクニカルサポートとダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。