

2021-03-31でのCisco WebexルートCA証明書の更新

内容

[はじめに](#)

[使用するコンポーネント](#)

[問題](#)

[解決方法](#)

はじめに

このドキュメントでは、Cisco Webexを新しい認証局(IdentrustコマーシャルルートCA 1)に移行する方法について説明します。Expresswayを使用してWebex会議にダイヤルインするお客様、またはExpresswayを利用するコネクタの1つのお客様は、2021-03-31より前に新しい証明書をExpresswayデバイスにアップロードする必要があります。

使用するコンポーネント

このドキュメントの情報は、Video Communication Server(VCS)-ExpresswayまたはExpresswayに基づいています。

問題

ルートCA証明書がExpresswayのトラストストアにアップロードされていない場合、WebexとのTLSネゴシエーションが次の展開で失敗する可能性があります。

- エンドポイントを使用して、VCS-ExpresswayまたはExpressway Edge経由でCisco Webex Video Platformに接続します。新しい証明書をVCSまたはExpresswayの信頼されたルートストアに追加する必要があります。
- VCS-ControlまたはExpressway Coreでコネクタまたはハイブリッドサービスを使用しており、クラウド証明書管理を選択していない。新しい証明書をVCSの信頼されたルートストアに追加する必要があります。
- VCS-ExpresswayまたはExpressway Edge経由でCisco Webex Edge Audioを使用している。証明書をVCSまたはExpresswayの信頼されたルートストアに追加する必要があります。
- 2021-03-23更新：Cloud Certificate Managementを利用するお客様は、現在、証明書の一覧に新しいIdentrust証明書が表示されません。既存のQuovadis (O=QuoVadis Limited, CN=QuoVadis Root CA 2)証明書は引き続き有効です。identrust証明書は、Cloud Certificate Managementで後日利用可能になる予定です。Cloud Certificate Managementをご利用のお客様は、今回の発表の結果としてサービスの中断が発生することなく、この時点で何もする必要はありません。

- 証明書失効リスト(CRL)を確認するためのURLへのアクセスが制限されています。Webexクライアントが<http://validation.identrust.com/crl/hydrantidcao1.crl>でホストされている証明書失効リスト(CRL)に到達できるようにする必要があります。
また、証明書の検証で許可する必要があるURLのリストに*.identrust.comを追加しました。
- オペレーティングシステムにデフォルトの証明書信頼ストアを使用しないでください。信頼されたルートストアに証明書を追加する必要があります。この証明書は、すべての主要オペレーティングシステムのデフォルトの信頼ストアにデフォルトで含まれています。

解決方法

これらの手順については、『[Expressway用の2021年3月のCisco WebexルートCA証明書の更新](#)』ビデオでも説明されています。

新しい証明書をVCS-Control、VCS-Expressway、Expressway-Core、およびExpressway Edgeにアップロードするには、次の手順を実行します。

ステップ1:[Identrust商用ルートCA 1](#)をダウンロードし、[identrust_RootCA1.pem](#)または[identrust_RootCA1.cer](#)として保存します。

a. [Identrust Commercial Root CA 1](#)にアクセスします。

b. ボックス内のテキストをコピーします。

c. テキストをメモ帳に保存し、ファイルを保存します。ファイルにidentrust_RootCA1.pemまたはidentrust_RootCA1.cerという名前を付けます。

Home - IdenTrust Commercial Root CA 1

Copy and Paste the following DST Root certificate into a text file on your computer.

```
MIIFYDCCA0igAwIBAgIQcGFCgAAAAUjyES1AAAAAjANBgkqhkiG9w0BAQsFADBK
MQswCQYDVQQGEwJVUzESMBAGA1UEChMJSWRlbiRydXN0MScwJQYDVQQDEEx5J
ZGVu
VHJ1c3QgQ29tbWVvY2lhbCBSb290IENBIDEwHhcNMTQwMTE2MTgxMjZWhcNMzQ
w
MTE2MTgxMjZWhcNjBKMzswCQYDVQQGEwJVUzESMBAGA1UEChMJSWRlbiRydXN0M
Scw
JQYDVQQDEEx5JZGVuVHJ1c3QgQ29tbWVvY2lhbCBSb290IENBIDEwggliMA0GCSqG
SIb3DQEBAQUAA4ICDwAwggIKAoICAQcnUBneP5k91DNG8W9RYYKyqU+PZ4ldhNIT
3Qwo2dfw/66VQ3KZ+bVdfIrbQuExUHTRgQ18zZshq0PirK1ehm7zCYofWjK9ouuU
+ehcCuz/mNKvcb00U590h++SvL3sTzIwiEsXXIfEU8L2ApeN2WlrvyQfYo3fw7gp
S0l4PJNgiCL8mdo2yMKi1CxUAGc1bnO/AljwpN3lsKlmesrgNqUZFvX9t++uP0D1
bVoE/c40yiTcdCMbXTMTEl3EASX2MN0CXZ/g1Ue9t0sbobtJSdifWwLziuQkkORi
T0/Br4sOdBeo0XKlanoBScy0RnnGF7Hamb4HWfp1IYVl3ZBWzvurpWCdxJ35UrCL
```

すべてのExpresswayデバイスで、Maintenance > Security > Trusted CA Certificateの順に選択します。

ステップ2: Expressway信頼ストアにファイルをアップロードします。



Cisco Expressway-E

The screenshot shows the Cisco Expressway-E web interface. The 'Maintenance' menu is open, and the 'Security' option is highlighted with a red box. Within the 'Security' sub-menu, the 'Trusted CA certificate' option is also highlighted with a red box. The main interface shows system information such as 'System mode: Generic', 'Up time: 4 hours 14 minutes 44 seconds', and 'Software version: X12.7'.

a. Expresswayの信頼ストアにCA証明書をアップロードするには、Append CA certificateをクリックします。

b. Browseをクリックします。identrust_RootCA1.pemまたはidentrust_RootCA1.cerファイルをア

アップロードします。CA証明書を追加します。

The screenshot shows the Cisco Expressway-E interface. The main content area is titled "Trusted CA certificate" and contains a table with the following data:

Type	Issuer
<input type="checkbox"/> Certificate	O=Temporary CA f80fac88-644e-48e8-b15c-38a14839ed12, OU=Temporary CA f80fac88-644e-48e8-b15c-38a14839ed12
<input type="checkbox"/> Certificate	CN=federation-AD-CA-1
<input type="checkbox"/> Certificate	O=QuoVadis Limited, CN=QuoVadis Root CA 2

Below the table are buttons: "Show all (decoded)", "Show all (PEM file)", "Delete", "Select all", and "Unselect all".

An "Upload" section contains a "Browse..." button.

At the bottom, there are buttons: "Append CA certificate" and "Reset to default CA certificate".

A "File Upload" dialog box is open, showing a file named "identrust_RootCA1.cer" selected in a folder named "CA webex cert".

ステップ3：証明書が正常にアップロードされ、VCS/Expressway信頼ストアに存在することを確認します。

The screenshot shows the Cisco Expressway-E interface after a successful upload. A yellow banner at the top says "File uploaded: CA certificate file uploaded. File contents - Certificates: 1, CRLS: 0." The main content area is titled "Trusted CA certificate" and contains a table with the following data:

Type	Issuer	Subject	Expiration date	Validity	View
<input type="checkbox"/> Certificate	O=Temporary CA f80fac88-644e-48e8-b15c-38a14839ed12, CN=Temporary CA f80fac88-644e-48e8-b15c-38a14839ed12	Matches Issuer	Feb 11 2023	Valid	View (decoded)
<input type="checkbox"/> Certificate	CN=federation-AD-CA-1	Matches Issuer	Apr 01 2022	Valid	View (decoded)
<input type="checkbox"/> Certificate	O=QuoVadis Limited, CN=QuoVadis Root CA 2	Matches Issuer	Nov 24 2031	Valid	View (decoded)
<input type="checkbox"/> Certificate	O=IdenTrust, CN=IdenTrust Commercial Root CA 1	Matches Issuer	Jan 16 2034	Valid	View (decoded)

Below the table are buttons: "Show all (decoded)", "Show all (PEM file)", "Delete", "Select all", and "Unselect all".

この操作の後、変更を有効にするために再起動や再起動は必要ありません。

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。