CUCMへのExpressway-Coreのルート/中間証明書のアップロード

内容

はじめに

このドキュメントでは、Expressway-C証明書に署名したCAのルート証明書と中間証明書をCUCMパブリッシャにアップロードする方法について説明します。

背景説明

X14.0.2でのExpressway上のトラフィックサーバサービスの改善により、CUCMが非セキュアモードであっても、サーバ(CUCM)が8443以外のポート（6971、6972など）で実行されるサービスを要求するたびに、Expressway-Cはクライアント証明書を送信します。この変更により、Expressway-C証明書署名認証局(CA)をtomcat-trustおよびcallmanager-trustの両方としてCUCMに追加する必要があります。

CUCMにExpressway-C署名CAをアップロードしないと、ExpresswayをX14.0.2以降にアップグレードした後にMRAログインが失敗します。

CUCMがExpressway-Cから送信される証明書を信頼するようにするには、tomcat-trustおよびcallmanager-trustに、ルートCAと、Expressway-C証明書の署名に関与するすべての中間CAを含める必要があります。

コンフィギュレーション

ステップ 1：Expressway-Cサーバ証明書に署名したルート証明書と中間証明書の取得

そのサーバ証明書に署名したCAから最初にサーバ証明書を受け取った場合は、そのサーバ証明書のルート証明書と中間証明書も取得し、それらを安全な場所に保存します。これらのファイルが残っている場合、またはCAから再度ダウンロードできる場合は、ステップ2に進み、CUCMにアップロードする手順を確認できます。

これらのファイルがなくなった場合は、Expressway-CのWebインターフェイスからダウンロードできます。これは少し複雑であるため、可能であれば、CAに連絡して信頼ストアをダウンロードすることを強くお勧めします。

Expressway-Cで、Maintenance > Security > Server certificateの順に移動し、Server certificateの横にあるShow (decoded)ボタンをクリックします。Expressway-Cサーバ証明書の内容を含む新しいウィンドウまたはタブが開きます。次のようにIssuerフィールドを探します。

<#root>

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            55:00:00:02:21:bb:2d:41:60:55:d7:b2:27:00:01:00:00:02:21
    Signature Algorithm: sha256WithRSAEncryption


 Issuer: O=DigiCert Inc, CN=DigiCert Global CA-1

        Validity
            Not Before: Dec  8 10:36:57 2021 GMT
            Not After : Dec  8 10:36:57 2023 GMT
        Subject: C=BE, ST=Flamish-Brabant, L=Diegem, O=Cisco, OU=TAC, CN=vcs-c1.vngtp.lab
        Subject Public Key Info:
...
```

この例では、Expressway-Cサーバ証明書は、共通名DigiCert Global CA-1でDigiCert Inc.という組織によって発行されています。

ここで、Maintenance > Security > Trusted CA certificateの順に移動し、リストを調べて、Subjectフィールドにまったく同じ値を持つ証明書が存在するかどうかを確認します。この例では、SubjectフィールドがO=DigiCert Inc, CN=DigiCert Global CA-1です。一致が見つかった場合、これは中間CAであることを意味します。このファイルが必要です。ルートCAが見つかるまで探し続ける必要があります。

一致が見つからない場合は、Subject of Matches IssuerのIssuerフィールドで、この値を持つ証明書を検索します。一致するエントリが見つかった場合は、これがルートCAファイルであり、これが必要な唯一のファイルであることを意味します。

	Type	Issuer	Subject
☐	Certificate	CN=vngtp-ACTIVE-DIR-CA	Matches Issuer
☐	Certificate	O=IdenTrust, CN=IdenTrust Commercial Root CA 1	Matches Issuer
☐	Certificate	O=Baltimore, OU=CyberTrust, CN=Baltimore CyberTrust Root	Matches Issuer
☐	Certificate	O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert Global Root CA	Matches Issuer
☐	Certificate	O=The Go Daddy Group, Inc., OU=Go Daddy Class 2 Certification Authority	Matches Issuer
☐	Certificate	O=GoDaddy.com, Inc., CN=Go Daddy Root Certificate Authority - G2	Matches Issuer
☐	Certificate	O=QuoVadis Limited, CN=QuoVadis Root CA 2	Matches Issuer
☐	Certificate	O=thawte, Inc., OU=Certification Services Division, OU=(c) 2006 thawte, Inc. - For authorized use only, CN=thawte Primary Root CA	Matches Issuer
☐	Certificate	O=VeriSign, Inc., OU=VeriSign Trust Network, OU=(c) 2006 VeriSign, Inc. - For authorized use only, CN=VeriSign Class 3 Public Primary Certification Authority - G5	Matches Issuer
☐	Certificate	O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert Global Root CA	O=DigiCert Inc, CN=DigiCert Global CA-1

Show all (decoded) Show all (PEM file) Delete Select all Unselect all

Expresswayトラストストア

この例では、証明書が見つかった後、SubjectフィールドがIssuerフィールドと一致していないことがわかります。これは、これが中間CA証明書であることを意味します。ルート証明書に加えて、この証明書が必要です。Subject saidが発行者と一致する場合、これがルート認証局であり、信頼する必要がある唯一の証明書であることがわかります。

中間証明書がある場合、ルート証明書が見つかるまで続行する必要があります。これを行うには、中間証明書のIssuerフィールドを調べます。次に、Subjectフィールドで同じ値を持つ証明書を探します。この例ではO=DigiCert Inc, OU=www.digicert.com, CN=DigiCert Global Root CAです。Subjectフィールドでこの値を持つ証明書を探します。一致する証明書が見つからない場合は、Subject of Matches IssuerがあるIssuerフィールドでこの値を探します。

この例では、Expressway-Cサーバ証明書が中間CA O=DigiCert Inc, CN=DigiCert Global CA-1によって署名され、ルートCA O=DigiCert Inc. OU=www.digicert.com, CN=DigiCert Global Root CAによって署名されたことが確認できます。ルートCAが見つかったので、作業は完了です。ただし、別の中間CAが見つかった場合は、すべての中間CAとルートCAを特定するまで、このプロセスを続行する必要があります。

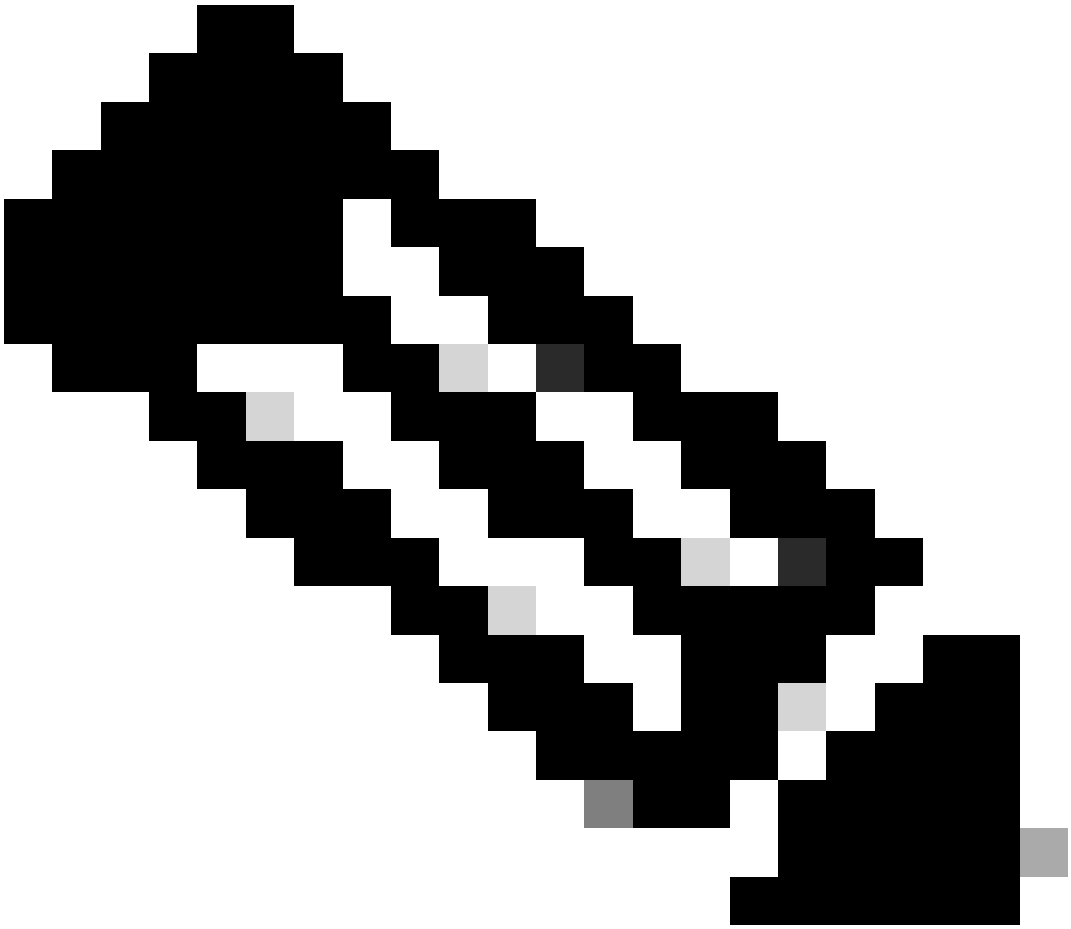
ルート証明書ファイルおよび中間証明書ファイルをダウンロードするには、リストの下にあるShow all（PEMファイル）ボタンをクリックします。これにより、すべてのルート証明書と中間証明書がPEM形式で表示されます。中間証明書またはルート証明書のいずれかに一致する証明書が見つかるまで下にスクロールします。この例では、最初にO=DigiCert Inc, CN=DigiCert Global Root CAが見つかりました。この証明書をファイルにコピーし、ローカルに保存します。

```
...
Epn3oOWC4zxe9Z2etiefC7IpJ5OCBRLbf1wbWsaY71k5h+3zvDyny67G7fyUIhz
ksLi4xaNmjICq44Y3ekQEe5+NauQrz4wlHrQMz2nZQ/1/I6eYs9HRCwBXbsdtTLS
R9I4LtD+gdwyah617jzV/OeBHRnDJELqYzmp
-----END CERTIFICATE-----

O=DigiCert Inc, CN=DigiCert Global Root CA
-----BEGIN CERTIFICATE-----
MIIDrzCCApegAwIBAgIQCDvgVpBCRrGhdWrJWZHHSjANBgkqhkiG9w0BAQUFADBh
```

```
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMSAwHgYDVQQDExdEaWdpQ2VydCBHbG9iYWwgUm9vdCBD
QTAeFw0wNjExMTAwMDAwMDBaFw0zMTExMTAwMDAwMDBaMGExCzAJBgNVBAYTAlVT
MRUwEwYDVQQKEwxEaWdpQ2VydCBJbmMxGTAXBgNVBAsTEHd3dy5kaWdpY2VydC5j
b20xIDAeBgNVBAMTF0RpZ2lDZXJ0IEdsb2JhbCBSb290IENBMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEA4jvhEXLeqKTTo1eqUKKPC3eQyaKl7hLOllsB
CSDMAZOnTjC3U/dDxGkAV53ijSLdhwZAAIEJzs4bg7/fzTtxRuLWZscFs3YnFo97
nh6Vfe63SKMI2tavegw5BmV/Sl0fvBf4q77uKNd0f3p4mVmFaG5cIzJLv07A6Fpt
43C/dxC//AH2hdmoRBBYMql1GNXRor5H4idq9Joz+EkIYIvUX7Q6hL+hqkpMfT7P
T19sdl6gSzeRntwi5m3OFBqOasv+zbMUZBfHWymeMr/y7vrTC0LUq7dBMtoM1O/4
gdW7jVg/tRvoSSiicNoxBN33shbyTApOB6jtSj1etX+jkMOvJwIDAQABo2MwYTAO
BgNVHQ8BAf8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUA95QNVbR
TLtm8KPiGxvDl7I90VUwHwYDVR0jBBgwFoAUA95QNVbRTLtm8KPiGxvDl7I90VUw
DQYJKoZIhvcNAQEFBQADggEBAMucN6pIExIK+t1EnE9SsPTfrgT1eXkIoyQY/Esr
hMAtudXH/vTBH1jLuG2cenTnmCmrEbXjcKChzUyImZOMkXDiqw8cvpOp/2PV5Adg
06O/nVsJ8dWO41P0jmP6P6fbtGbfYmbW0W5BjfIttep3Sp+dWOIrWcBAI+0tKIJF
PnlUkiaY4IBIqDfv8NZ5YBberOgOzW6sRBc4L0na4UU+Krk2U886UAb3LujEV0ls
YSEY1QSteDwsOoBrp+uvFRTp2InBuThs4pFsiv9kuXclVzDAGySj4dzp30d8tbQk
CAUw7C29C79Fv1C5qfPrmAESrciIxpg0X40KPMbp1ZWVbd4=
-----END CERTIFICATE-----

O=The Go Daddy Group, Inc.
-----BEGIN CERTIFICATE-----
MIIEADCCAuigAwIBAgIBADANBgkqhkiG9w0BAQUFADBjMQswCQYDVQQGEwJVUzEh
MB8GA1UEChMYVGhlIEdvIERhZGR5IEdyb3VwLCBJbmMuMTEwLwYDVQQLEyhHbyBE
...
```

ルート証明書と最終的な中間証明書のそれぞれに対して、（含まれる）-----BEGIN CERTIFICATE-----で始まり（含まれる）-----END CERTIFICATE-----で終わるものをすべてコピーします。それぞれを個別のテキストファイルに入れ、下部に空の行を1行追加します(-----END CERTIFICATE-----の行の後)。次のファイルを.pem拡張子を付けて保存します。root.pem、intermediate1.pem、intermediate2.pem、...ルート/中間証明書ごとに個別のファイルが必要です。前の例では、root.pemファイルに次の内容が含まれています。

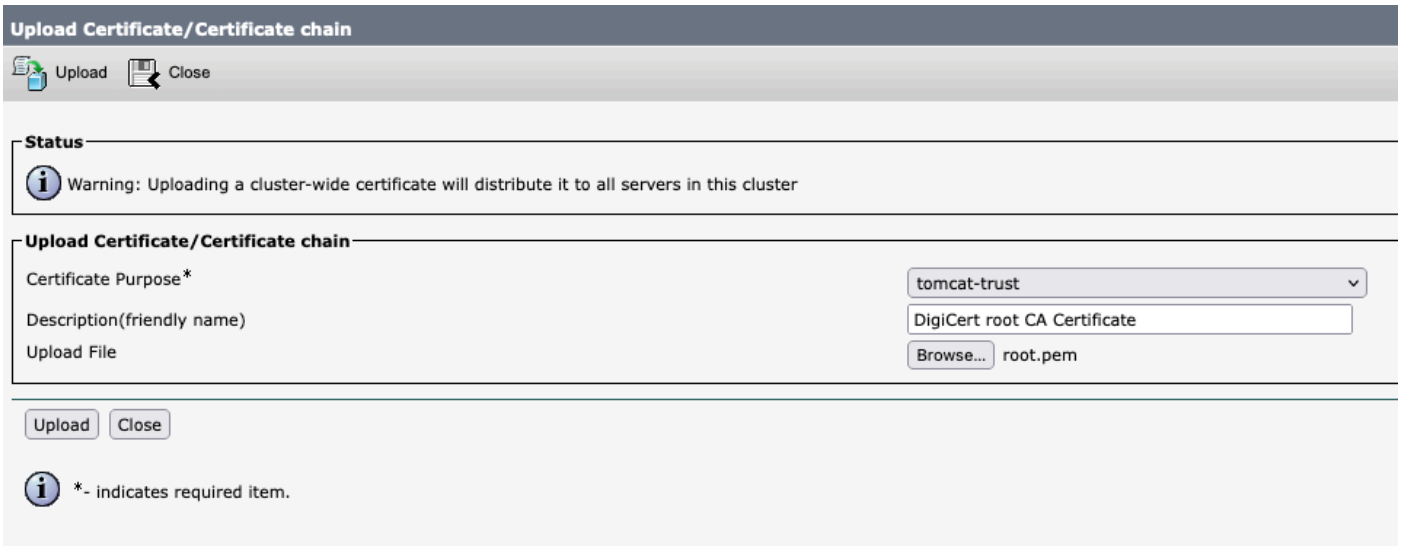
```
-----BEGIN CERTIFICATE-----
MIIDrzCCApegAwIBAgIQCDvgVpBCRrGhdWrJWZHHSjANBgkqhkiG9w0BAQUFADBh
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMSAwHgYDVQQDExdEaWdpQ2VydCBHbG9iYWwgUm9vdCBD
QTAeFw0wNjExMTAwMDAwMDBaFw0zMTExMTAwMDAwMDBaMGExCzAJBgNVBAYTAlVT
MRUwEwYDVQQKEwxEaWdpQ2VydCBJbmMxGTAXBgNVBAsTEHd3dy5kaWdpY2VydC5j
b20xIDAeBgNVBAMTF0RpZ2lDZXJ0IEdsb2JhbCBSb290IENBMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEA4jvhEXLeqKTTo1eqUKKPC3eQyaKl7hLOllsB
CSDMAZOnTjC3U/dDxGkAV53ijSLdhwZAAIEJzs4bg7/fzTtxRuLWZscFs3YnFo97
nh6Vfe63SKMI2tavegw5BmV/Sl0fvBf4q77uKNd0f3p4mVmFaG5cIzJLv07A6Fpt
43C/dxC//AH2hdmoRBBYMql1GNXRor5H4idq9Joz+EkIYIvUX7Q6hL+hqkpMfT7P
T19sdl6gSzeRntwi5m3OFBqOasv+zbMUZBfHWymeMr/y7vrTC0LUq7dBMtoM1O/4
gdW7jVg/tRvoSSiicNoxBN33shbyTApOB6jtSj1etX+jkMOvJwIDAQABo2MwYTAO
BgNVHQ8BAf8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUA95QNVbR
TLtm8KPiGxvDl7I90VUwHwYDVR0jBBgwFoAUA95QNVbRTLtm8KPiGxvDl7I90VUw
DQYJKoZIhvcNAQEFBQADggEBAMucN6pIExIK+t1EnE9SsPTfrgT1eXkIoyQY/Esr
hMAtudXH/vTBH1jLuG2cenTnmCmrEbXjcKChzUyImZOMkXDiqw8cvpOp/2PV5Adg
06O/nVsJ8dWO41P0jmP6P6fbtGbfYmbW0W5BjfIttep3Sp+dWOIrWcBAI+0tKIJF
PnlUkiaY4IBIqDfv8NZ5YBberOgOzW6sRBc4L0na4UU+Krk2U886UAb3LujEV0ls
YSEY1QSteDwsOoBrp+uvFRTp2InBuThs4pFsiv9kuXclVzDAGySj4dzp30d8tbQk
CAUw7C29C79Fv1C5qfPrmAESrciIxpg0X40KPMbp1ZWVbd4=
-----END CERTIFICATE-----
```



注：下部に空の行が1行表示されている必要があります。

ステップ 2：CUCMでのルート証明書と中間証明書のアップロード（該当する場合）

- CUCMパブリッシャのCisco Unified OS Administrationページにログインします。
- Security > Certificate Managementの順に移動します。
- Upload Certificate/Certificate chainボタンをクリックします。
- 新しいウィンドウで、手順1のルート証明書のアップロードを開始します。これをtomcat-trustにアップロードします。



- Uploadボタンをクリックすると、次にSuccess: Certificate Uploadedが表示されます。今はTomcatを再起動するように求めるメッセージを無視します。
- 証明書の目的で、CallManager-trustを使用して同じルートファイルをアップロードします。
- Expressway-Cで使用されているすべての中間証明書について、前の手順（tomcat-trustおよびCallManager-trustへのアップロード）を繰り返します。

ステップ 3：CUCMで必要なサービスを再起動する

CUCMクラスタ内の各CUCMノードで、次のサービスを再起動する必要があります。

- Cisco CallManager
- Cisco TFTP
- Cisco Tomcat

Cisco CallManagerとCisco TFTPは、CUCMのCisco Unifiedサービスアビリティページから再起動できます。

- CUCMパブリッシャのCisco Unifiedサービスアビリティページにログインします。
- Tools > Control Center - Feature Servicesの順に選択します。
- サーバとしてパブリッシャを選択します。
- Cisco CallManager serviceを選択し、Restartボタンをクリックします。
- Cisco CallManagerサービスの再起動後、Cisco TFTP serviceを選択し、Restartボタンをクリックします。

Cisco TomcatはCLIからのみ再起動できます。

- CUCMパブリッシャへのコマンドライン接続を開きます。
- utils service restart Cisco Tomcatコマンドを使用します。

関連情報

[テクニカルサポートとドキュメント - Cisco Systems]

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。