Configure and Troubleshoot Collaboration Edge (MRA) Certificates

Contents

Introduction
Prerequisites
Requirements
Components Used
Background Information
Public vs. Private Certificate Authority (CA)
How Certificate Chains Work
SSL Handshake Summary
Configure
Expressway-C and Expressway-E Traversal Zone / Trust
Generate and Sign CSRs
Configuring the Expressway-C and Expressway-E to Trust Each Other
Secure Communication Between Cisco Unified Communications Manager (CUCM) and Expressway-C
Overview
Configuring Trust Between CUCM and Expressway-C
CUCM Servers Using Self Signed Certificates
Expressway-C and Expressway-E Cluster Considerations
Cluster Certificates
Trusted CA Lists
Verify
Checking Existing Certificate Information
Reading/Exporting a Certificate In Wireshark
Troubleshoot
Testing If A Certificate Is Trusted On The Expressway
Synergy Light Endpoints (7800/8800 Series Phones)

Introduction

This document describes certificates with respect to Mobile Remote Access (MRA) deployments.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used
Background Information

Public vs. Private Certificate Authority (CA)

There are a number of options to sign certificates on the Expressway-C and E servers. You can opt to have the Certificate Signing Request (CSR) signed by a public CA such as GoDaddy, Verisign, or others, or you can sign it internally using your own Certificate Authority (CA) (can either be self signed using openSSL or an internal enterprise CA such as a Microsoft Windows server). For more information on how to create and sign the CSRs using any of these methods please see the Video Communication Server (VCS) Certificate Creation Guide.

The only server that is really required to be signed by a public CA is the Expressway-E. This is the only server that clients will see the certificate from when singing in via MRA therefore using a public CA will ensure that users do not have to manually accept the certificate. Using an internal CA to sign the Expressway-E will work but first time users will be prompted to accept the untrusted certificate. MRA registration of 7800 and 8800 series phones also will not work with internal certificates because their certificate trust list cannot be modified. For simplicity it is suggested that your Expressway-C and Expressway-E certificates both be signed by the same CA however this is not a requirement as long as you properly configured the trusted CA lists on both servers.

How Certificate Chains Work

Certificates are linked together in a chain of two or more used to verify the source that signed the servers certificate. There are three types of certificates in a chain, the client/server certificate, intermediate certificates (in some cases), and the root certificate (also referred to as the root CA as this is the highest level authority that signed the certificate).

Certificates contain two primary fields that build the chain, the subject and issuer. The subject is the name of the server or authority that this certificate represents. In the case of an Expressway-C or Expressway-E (or other Unified Communications (UC) devices) this is built from the Fully Qualified Domain Name (FQDN). The issuer is the authority that validated that specific certificate. Since anyone can sign a certificate (including the server that created the certificate to begin with, also known as self-signed certificates), servers and clients have a list of issuers or CAs that they trust as authentic.

A certificate chain will always end with a self signed top level or root certificate. As you move through the certificate hierarchy, each certificate having a different issuer in relation to the subject, you will eventually encounter the root CA where the subject and issuer will match, indicating this is the top level cert and thus the one that needs to be trusted by a client or servers trusted CA list.

SSL Handshake Summary

You can see this flow diagram for a detailed signaling flow of the SSL handshake process including key exchange and generation which may be useful when looking at packet captures. In the case of the traversal zone, the Expressway-C will always act as the client while the Expressway-E will always be the server. The simplified exchange works as follows:

Expressway-C          Expressway-E
The key here is in the exchange, since the Expressway-C always initiates the connection and thus is always the client, the Expressway-E is the first one to send its certificate. If the Expressway-C cannot validate this certificate, it will tear down the handshake and will not send its own to the Expressway-E.

Another important thing to note is the Transport Layer Security (TLS) web client authentication and TLS web server authentication attributes on certificates. These attributes are determined on the CA that is signing the CSR (if using a Windows CA this is determined by the template selected) and indicate if the certificate is valid in the role of the client or server (or both). Because for a VCS or Expressway it can need to be either depending on the situation (it’s always the same for a traversal zone) the certificate must have both client and server authentication attributes. The Expressway-C and Expressway-E will give you an error when uploading a new server certificate if it does not have both applied.

If you are unsure if a certificate has these attributes, you can open the certificate details in a browser or in your OS and check the Extended Key Usage section (see screenshot). The format may vary and depends on how you are looking at the cert. Example:
Configure

Expressway-C and Expressway-E Traversal Zone / Trust

Generate and Sign CSRs

As described earlier, the Expressway-C and Expressway-E certificates must be signed either by an internal or external CA, or using openSSL to self sign. Using the temporary certificate that comes on the Expressway server is not supported. Using wild-card certificates where you have a CA sign a certificate where the subject line is not specifically defined is also not supported.

The first step is to generate the CSR and have it signed by the preferred CA type. The process for this is given specifically in the certificate creation guide. While creating the CSR its important to keep in mind the necessary Subject Alternative Names (SANs) that need to be included in the
certificates. This is also listed in the certificates guide and the Mobile Remote Access Deployment Guide. Check the most recent versions of the guide as more may be added as new features arrive. List of common SANs that need to be included depending on the features used:

Expressway-C

- Any domains (internal or external) added into the domains list.
- Any persistent chat node aliases if using XMPP federations.
- Secure device profile names on CUCM if using secure device profiles.

Expressway-E

- Any domains configured on the Expressway-C.
- Any persistent chat node aliases if using XMPP federations.
- Any domains advertised for XMPP federations.

Note: If the base domain used for external Service record (SRV) lookups is not included as a SAN in the Expressway-E certificate (either xxx.com or collab-edge.xxx.com) jabber clients will still require the end user to accept the certificate on first connection and TC endpoints will fail to connect at all.

Configuring the Expressway-C and Expressway-E to Trust Each Other

In order for the Unified Communications traversal zone to establish a connection the Expressway-C and Expressway-E must trust each others certificates. For this example assume the Expressway-E certificate was signed by public CA using the following hierarchy.

Certificate 3
Issuer: GoDaddy Root CA
Subject: GoDaddy Root CA

Certificate 2
Issuer: GoDaddy Root CA
Subject: GoDaddy Intermediate Authority

Certificate 1
Issuer: GoDaddy Intermediate Authority
Subject: Expressway-E.lab.com

The Expressway-C needs to be configured with trust certificate 1 above. In most cases, depending on the trusted certificates applied to the server actually sending its certificate, that
server will only send its lowest level server cert. That means that for the Expressway-C to trust certificate 1 you must upload both certificate 2 and 3 to the Expressway-C’s trusted CA list (Maintenance> Security > Trusted CA List). If you leave out the intermediate certificate 2, when the Expressway-C receives the Expressway-E certificate, it will have no way to tie it to the trusted GoDaddy Root CA, therefore it will be rejected.

Certificate 3
Issuer: GoDaddy Root CA
Subject: GoDaddy Root CA

Certificate 1
Issuer: GoDaddy Intermediate Authority - Not Trusted!
Subject: Expressway-E.lab.com

Additionally, if you only upload the intermediate certificate without the root to the trusted CA list of the Expressway-C, it will see that GoDaddy Intermediate Authority is trusted but it is signed by a higher authority, GoDaddy Root CA which is not trusted, therefore it will fail.

Certificate 2
Issuer: GoDaddy Root CA - Not Trusted!
Subject: GoDaddy Intermediate Authority

Certificate 1
Issuer: GoDaddy Intermediate Authority
Subject: Expressway-E.lab.com

With all intermediates and the root added to the trusted CA list, the certificate can be verified...

Certificate 3
Issuer: GoDaddy Root CA - Self signed top level certificate is trusted and chain complete!
Subject: GoDaddy Root CA

Certificate 2
Issuer: GoDaddy Root CA
Subject: GoDaddy Intermediate Authority
Certificate 1

Issuer: GoDaddy Intermediate Authority

Subject: Expressway-E.lab.com

If you are unsure what the certificate chain is, you can check your browser when logged into the web interface of the specific Expressway. The process varies slightly depending on your browser, but in Firefox, you can click the lock icon on the far left of the address bar. Then in the pop-up, click **More Information > View Certificate > Details**. Assuming your browser can piece together the full chain, you will see the chain from top to bottom. If the top level certificate does not have a matching subject and issuer, you know you are not seeing the full chain. You can also export each certificate in the chain by themselves by clicking export with the desired certificate highlighted. This is useful if you are not 100% certain you have uploaded the correct certificates to the CA trust list.

![Certificate View](image-url)
This certificate has been verified for the following uses:

<table>
<thead>
<tr>
<th>SSL Client Certificate</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL Server Certificate</td>
</tr>
</tbody>
</table>

**Issued To**

<table>
<thead>
<tr>
<th>Common Name (CN)</th>
<th>Organization (O)</th>
<th>Organizational Unit (OU)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Issued By**

<table>
<thead>
<tr>
<th>Common Name (CN)</th>
<th>Organization (O)</th>
<th>Organizational Unit (OU)</th>
</tr>
</thead>
<tbody>
<tr>
<td>DigiCert SHA2 High Assurance Server CA</td>
<td>DigiCert Inc</td>
<td></td>
</tr>
</tbody>
</table>

**Period of Validity**

<table>
<thead>
<tr>
<th>Begins On</th>
<th>Expires On</th>
</tr>
</thead>
<tbody>
<tr>
<td>3/25/2015</td>
<td>4/12/2017</td>
</tr>
</tbody>
</table>

**Fingerprints**

<table>
<thead>
<tr>
<th>SHA-256 Fingerprint</th>
<th>SHA1 Fingerprint</th>
</tr>
</thead>
</table>
Next, now that the Expressway-C trusts the certificate from the Expressway-E, ensure it works in the opposite direction. If the Expressway-C certificate is signed by the same CA that signed the Expressway-E, the process is simple, just upload the same certificates to the Trusted CA list on the Expressway-E as you already did to the C. If the C is signed by a different CA, you will need to follow the same process as above, except using the chain the signed the Expressway-C certificate instead.

Secure Communication Between Cisco Unified Communications Manager (CUCM) and Expressway-C

Overview
Unlike the traversal zone between the Expressway-C and Expressway-E, secure signaling is NOT required between the Expressway-C and CUCM. Unless it is not allowed by internal security policies, you should always configure MRA to work with non-secure device profiles on CUCM first to confirm the rest of the deployment is correct before moving to this step.

There are two main security features that can be enabled between CUCM and Expressway-C, TLS Verify and Secure Device Registrations. There is an important distinction between these two because they use two different certificates from the CUCM side in the SSL handshake.

TLS Verify - tomcat certificate

Secure SIP Registrations - callmanager certificate

**Configuring Trust Between CUCM and Expressway-C**

The concept in this case is exactly the same as between the Expressway-C and Expressway-E. The CUCM must first trust the server certificate of the Expressway-C. That means that on the CUCM, the intermediates and root certificate of the Expressway-C need to be uploaded as a tomcat-trust certificate for the TLS verify feature and a callmanager-trust for secure device registrations. This is done by going to **Cisco Unified OS Administration** in the upper right of the CUCM web GUI, then clicking **Security> Certificate Management**. Here you can click **Upload Certificate/Certificate Chain** and select the correct trust format or click **Find** to see the list of currently uploaded certificates.

![Upload Certificate/Certificate Chain](image)

You will also need to ensure that the Expressway-C trusts the CA that singed the CUCM.
certificates by adding them to the trusted CA list. In almost all cases, if you signed the CUCM certificates with a CA, the tomcat and callmanager certificates should be signed by the same CA. If they are different you will need to trust both if you are using TLS Verify and Secure Registrations.

For secure SIP registrations you also must ensure that the secure device profile name on the CUCM that is applied to the device is listed as a SAN on the Expressway-C certificate. If this is missing secure register messages will fail with a "403" from the CUCM indicating a TLS failure.

**Note:** When the SSL handshake takes place between the CUCM and Expressway-C for a secure SIP registration, two handshakes will take place. First the Expressway-C will act as the client, initiating the connection with the CUCM. Once that has completed successfully, the CUCM will initiate another handshake as the client to reply. This means that just like the Expressway-C, the callmanager certificate on CUCM must have both TLS Web Client and TLS Web Server authentication attributes applied. The difference is CUCM will allow these certificates to be uploaded without both, and internal secure registrations will work fine if the CUCM only has the server authentication attribute. You can confirm this on CUCM by finding the callmanager certificate on the list and clicking on it. There you can look at the usage oids under the Extension section. You will see 1.3.6.1.5.5.7.3.2 for Client Authentication and 1.3.6.1.5.5.7.3.1 for Server Authentication. You can also download the certificate from this window.
Note: Trust certificates applied to the publisher in a cluster should replicate over to subscribers, but it is good to confirm by logging into them separately on a new configuration.

Note: In order for the Expressway-C to properly validate the certificate from CUCM, the CUCM servers MUST be added in the Expressway-C using the FQDN, not IP address. The only way the IP address will work is if the IP of each CUCM node is added as a SAN in the certificate, which is almost never done.

CUCM Servers Using Self Signed Certificates
By default, a CUCM server comes with self signed certificates. If these are in place it is not possible to use both TLS Verify and Secure Device Registrations at the same time. Either feature can be used on its own, but because the certificates are self signed, it means both the self signed Tomcat and self signed CallManager certificates need to be uploaded to the trusted CA list on the Expressway-C. When the Expressway-C searches its trust list to validate a certificate, it will stop once it finds one with a matching subject. Because of this, whichever is higher on the trust list, tomcat or callmanager, that feature will work. The lower one will fail just as if it was not present. The solution to this is to sign your CUCM certificates with a CA (public or private) and trust that CA alone.

**Expressway-C and Expressway-E Cluster Considerations**

**Cluster Certificates**

It is strongly recommended that if you have a cluster of Expressway-C or Expressway-E servers for redundancy that you generate a separate CSR for each server and have it signed by a CA. Most deployments will use the server name for the subject and list all peers and the cluster ID as SANs. It is possible for you to use the cluster-id as the subject to use the same certificate for all nodes in the cluster, therefore avoiding the cost of multiple certs signed by a public CA. If absolutely necessary, this can be done with the following process or by using OpenSSL to generate both the private key and CSR manually:

Step 1. Generate a CSR on the master of the cluster and configure it to list the cluster-alias as the subject. Add all peers in the cluster as alternative names, along with all other required SANs.

Step 2. Sign this CSR and upload to the master peer.

Step 3. Log into the master as root and download the private key located in /tandberg/persistent/certs.

Step 4. Upload both the signed certificate and matching private key to each other peer in the cluster.

**Note:** This is not recommended for the following reasons:
1. It is a security risk because all peers are using the same private key. If one is somehow compromised an attacker can decrypt traffic from any of the servers.
2. If a change needs to be made to the certificate, this entire process must be followed again rather than a simple CSR generation and signing.

**Trusted CA Lists**

Unlike CUCM subscribers in a cluster, the trusted CA list is NOT replicated from one peer to another in an Expressway or VCS cluster. That means that if you have a cluster, you will need to manually upload trusted certificates to the CA list on each peer.

**Verify**

Use this section to confirm that your configuration works properly.
Checking Existing Certificate Information

There are a number of ways you can check the information on an existing certificate. The first option is via the web browser using the method depicted in the previous section which can also be used to export a specific certificate in the chain. If you need to verify SANs or other attributes added to the Expressway server certificate, you can do this directly through the web Graphical User Interface (GUI) by going to Maintenance > Security Certificates > Server Certificate, then click Show Decoded.

Here you can see all the specific details of the certificate without the need to download. You can also do the same for an active CSR if the associated signed certificate has not yet been uploaded.

Reading/Exporting a Certificate In Wireshark

If you have a Wireshark capture of the SSL handshake including the certificate exchange wireshark will actually decode the certificate for you and you can actually export any certificates in the chain (assuming the full chain is exchanged) from within. Filter your packet capture for the
specific port of the certificate exchange (generally 7001 in the case of the traversal zone). Next, if you do not see the client and server hello packets along with the SSL handshake, right click on one of the packets in the TCP stream and select decode as Here, select SSL and click apply. Now, if you have captured the correct traffic, you should see the certificate exchange. Find the packet from the correct server containing certificate in the payload. Expand the SSL section in the lower pane until you see the list of certificates as shown below.

Here you can expand any of the certificate to see all of the details. If you want to export the certificate, right click on the desired certificate in the chain (if there are multiple) and select Export Selected Packet Bytes. Enter a name for the certificate and click save. Now you should be able to open the certificate in Windows Certificate Viewer (if you give it a .cer extension) or upload it to any other tools for analysis.

**Troubleshoot**

This section provides information you can use to troubleshoot your configuration.

**Testing If A Certificate Is Trusted On The Expressway**

While the best method is to manually check the certificate chain and ensure all members are included in the Expressway trusted CA list, you can quickly check to ensure the Expressway will trust a specific client’s certificate by using the Client Certificate Tested under Maintenance > Security Certificates in the web GUI. Leaving all the default settings the same, select Upload Test File (pem format) from the dropdown and select the client certificate you wish to verify. If the certificate is not trusted, you will get an error like the one below explaining the reason it was rejected. Below the error you will also be able to see the decoded information of the uploaded certificate for reference.
If you get an error that claims the Expressway is unable to get the certificate CRL but the Expressway is not using CRL checking, this means the certificate will be trusted and has passed all other verification checks.
Synergy Light Endpoints (7800/8800 Series Phones)

These new devices come with a pre-populated certificate trust list including a large number of well known public CAs. This trust list can not be modified which means your Expressway-E certificate MUST be signed by one of these matching public CAs in order to work with these devices. If it is signed by an internal CA or a different public CA the connection will fail. There is no option for the user to manually accept the certificate as there is with Jabber clients.

**Note:** It has been found for some deployments that the use of a device such as a Citrix NetScaler with a CA from the list included on the 7800/8800 Series Phones can register over MRA even if the Expressway-E uses an internal CA. The NetScalers root CA will need to be uploaded to the Expressway-E and the Internal root CA will need to be uploaded to the Netscaler in order for SSL authentication to work. This has been demonstrated to work but is best effort support.

**Note:** If the trusted CA list appears to have all the correct certificates in but it is still gets rejected. Ensure there is not another certificate higher on the list with the same subject that could be conflicting with the correct one. When all else fails, you can always export the chain directly from the browser or wireshark and upload all certificates to the opposite servers CA list. This will guarantee to be the trusted certificate.

**Note:** When you troubleshoot a traversal zone issue, sometimes the problem can appear to be certificate related but its actually something on the software side. Ensure that the account username and password used for the traversal is correct.

**Note:** The VCS or Expressway does not support greater than 999 characters in the SAN field of a certificate. Any SANs that are past this limit (which requires a lot of alternative names) will be ignored as if they were not there.