Use ACME on Expressway-E

Use ACME on Expressway-E

From X12.5 the Cisco Expressway Series supports the ACME protocol (Automated Certificate Management Environment) which enables automatic certificate signing and deployment to the Cisco Expressway-E from a certificate authority such as Let's Encrypt. The main benefit of this feature is to generate low-cost server certificates to identify the Expressway-E, thereby reducing the cost of Expressway-based deployments like MRA (Mobile and Remote Access).

Due to the underlying validation mechanism this feature is most likely to be useful for MRA deployments. For Business to Business (B2B) applications, it's not always practical to include your primary domain in ACME certificates.

The configuration process is simple. You enter some information on the Cisco Expressway-E to create a certificate signing request (CSR), then the Expressway's ACME client interacts with the certificate authority to request the certificate. Expressway downloads the certificate and you click a button to deploy it. After this manual step, you can schedule renewal so that the certificate does not expire—because ACME certificates are deliberately short-lived.

One compromise of the ACME protocol is that it requires an inbound HTTP connection to port 80 on the Cisco Expressway-E. You can manage this risk with the Expressway's security features or, for highly secure environments, you can disable ACME and use the traditional CSR procedure with your preferred certificate authority.

No Jabber Guest support with ACME.

Currently, Expressway does not support ACME with Jabber Guest deployments.

ACME Deployment Overview

1. Deploy ACME Certificate Service

2. Configure ACME Certificate Service on Expressway-E
3. Generate a Certificate Signing Request for ACME
4. Sign the CSR using ACME Provider
5. [Optional] Check the Signed ACME Certificate
6. Deploy the ACME Certificate
7. Enable Automated Renewal of the ACME Certificate

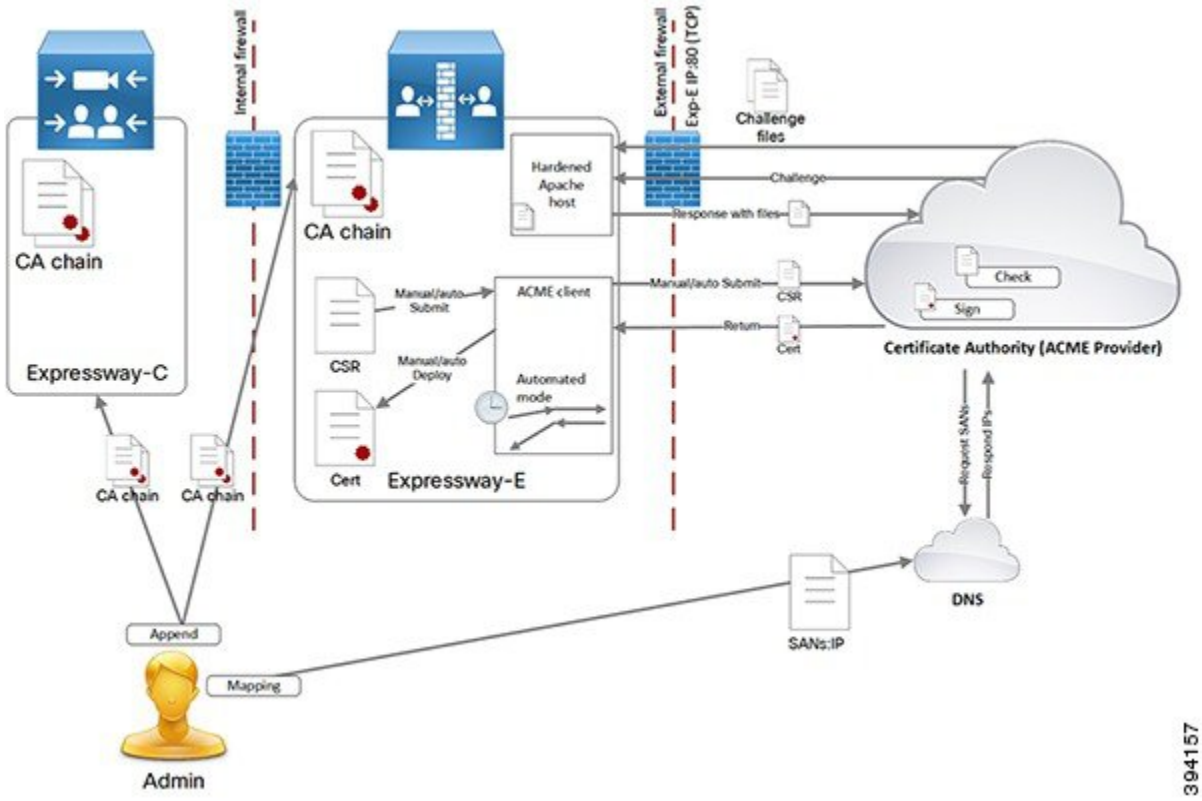
For clustered deployments, ACME **must be enabled individually on each peer** rather than at cluster level. Most certificate operations are performed per node.

How ACME Works

ACME is a client server protocol that enables automated certificate management of web hosts. The Expressway-E has an ACME client that interacts with an ACME provider, which is under the control of a certificate authority.

We currently work with the Let's Encrypt authority to generate server certificates.

We also use ACME to generate domain certificates for SNI (multitenancy), for which the process is essentially the same as the server certificate process. Multitenancy is only supported for HCS deployments and more information about using ACME with SNI is available in the Certificate Management and Service Discovery area of the Collaboration Knowledge Portal.



The ACME Certificate Service on the Expressway-E is a different method of requesting and applying server certificates to Expressway-E than the method described in the other parts of this document.

The essential signing process is:

- Define request > Submit to CA > CA generates and signs the certificate > Apply certificate.
- The ACME certificate service follows this process, but it removes the cost and some of the manual effort.
- One caveat about the process is that the CA has to interrogate the submitting host to verify that it controls the domains in the CSR.

Common Configuration

These tasks are always required when using the ACME Certificate Service:

1. Create a CSR on the Expressway-E.
2. Configure DNS with the domains from your CSR and map them to the Expressway-E public IP address.
3. Each domain must have an A record, not just the FQDNs.
4. Configure the ACME client with the provider details and your email address.

Lets encrypt verification process

For Let’s Encrypt to verify that all the domains requested in the CSR are under the control of requestor, it performs a challenge for each one. It provides files, containing random strings, that the requestor must be able to serve on port 80 for each domain in the CSR.

Let's Encrypt only issues the certificate after it successfully reads all the challenge files.

This is how it works when you manually control the process:

Procedure

Step 1 You initiate the signing process:

a. The ACME client opens an HTTPS connection to Let’s Encrypt and uploads the CSR.

b. Let’s Encrypt responds with a list of challenge files, one for each domain in the CSR.

c. The client places the challenge files on all the peers in the Expressway-E cluster.

d. Each Expressway-E peer starts a virtual Apache host, configured to serve only the challenge files.

e. The client notifies Let’s Encrypt it is ready to serve the challenge files.

f. Let’s Encrypt attempts to retrieve the challenge files.

g. The client polls Let’s Encrypt to see if the challenge process was successful.

h. If the challenge exchange was successful, then the client downloads the signed certificate, stores it in a staging area, and notifies you that the certificate is ready to deploy.

i. The Expressway-E peers close down the virtual Apache hosts.

Step 2 You initiate the deployment process:

a. The Expressway-E copies the staged certificate over the existing server certificate.

b. It copies the private key associated with the CSR over the existing private key.

c. Expressway-E signals to other internal processes that they need to reload the server certificate. (You do not need to restart the Expressway-E.)

The Expressway-E now presents the ACME certificate when making TLS connections.

Frequent expiry and low impact renewal

Let’s Encrypt certificates are only valid for 90 days, by design. This means you need to renew your certificates more frequently, which we address in the ACME Certificate Service by:

- Providing an automated renewal mode, that fetches a new certificate when two-thirds of the validity period has expired.

There is no notification at the two-thirds time if the service is not in automated mode. You are responsible for submitting a new signing request. Let's Encrypt sends expiration warning emails to the account that you use to configure the ACME client on Expressway-E.

- Removing the need to restart the Expressway-E when you use ACME Certificate Service to deploy a new certificate (either automated or manual deployment).

  The Expressway processes that use the certificate can load the new certificate without restarting. Expressway-E does not drop TLS connections, and presents the new certificate for new connection attempts.

  There is no interruption of service for Mobile Remote Access clients.

Note If you use a different method to upload a new server certificate, you must restart the Expressway-E. That behavior is unchanged with the introduction of the ACME Certificate Service.

Automated renewal mode

You can schedule a particular time, on one or more days of the week, when you configure automated renewal. The schedule is only used for deploying the certificate, not for requesting a new one.

When you put the service in automated mode, the service requests and receives an initial certificate, then deploys the certificate at the next scheduled opportunity. When two-thirds of that certificate's validity period has elapsed, the ACME Certificate Service automatically resubmits the stored CSR to get a new certificate.

There are two automated resubmission opportunities per day. These are deliberately at random times to improve security of the challenge process. At these times, the Expressway-E must accept requests on port 80, so it is better that they are unpredictable.

After the successful automated signing, the ACME Certificate Service automatically deploys the staged certificate at the next scheduled opportunity. This takes a few seconds and does not impact running processes that use the certificate.

More about the virtual Apache host

Let's Encrypt needs to verify that the certificate requestor controls the domain names in the CSR, using the challenge and validation process described above. Let's Encrypt must be able to access port 80 on all peers in the cluster because, when a domain resolves to several IP addresses, Let’s Encrypt will connect to any one of them, at random.

It is impractical to try and restrict access to the Expressway-E port based on the source address, because Let’s Encrypt does not have a concise list or CIDR containing all their servers.

To reduce the risk of malicious access, the Apache virtual host only runs during the challenge phase, and is also restricted to allow HTTP access only to the challenge files.

Apache is configured to listen on port 80 (if it is not already listening on that port) and forwards (only) ACME challenge traffic to the virtual Apache host.

The virtual host only listens on one unprivileged port on its localhost interface. The virtual host is hardened in the usual way. It denies: directory browsing, symbolic links, all options, and usage of .htaccess files.

If the Expressway-E is configured to redirect port 80 to 443:

- We add an exception to the 80 to 443 redirect rule for ACME challenge traffic.
- The exception filters only on GET requests to the required paths (.well-known/acme-challenge/).

  Therefore, only GET requests on port 80 to specific file paths will reach the virtual host. All other requests are redirected to port 443 as normal.

If port 80 is not enabled on Expressway-E:

- We configure Apache to listen on port 80.
- We add a rule to redirect GET requests, on port 80, for the ACME challenge files, to the virtual Apache host.
- All other requests return HTTP error 404 (not found).

The challenge process can last a few minutes, depending on the number of domains in the CSR and the number of peers in the Expressway cluster.

When the challenge is complete:

- We remove the challenge files.
- We remove the exception to the 80 to 443 redirection rule.
- We stop Apache from listening on port 80, if it was not configured to allow redirection to 443.
- We stop the Apache virtual host.

Deploy ACME Certificate Service

Prerequisites

- Check the Let's Encrypt terms and conditions with your legal representative.
- Configure DNS with any mappings to Expressway-E that you need as CN or SAN in your certificate.
- Create an email account to use with the Let's Encrypt CA.
- Append the Let's Encrypt root CA certificate to Expressway trust stores.
- Append the Let's Encrypt intermediate CA certificate to Expressway trust stores.
- Enable TCP 80 inbound from the internet to your Expressway-Es' public addresses.
- Ensure that all domains on the SAN have a valid A record (not just the FQDNs). If the record of a **domain** is already used by another web server, you can configure the *collab-edge* domain on the CSR and configure an A record for it.

Append Let's Encrypt Root CA Certificate to Expressway Trust Stores

Let's Encrypt is a relatively new CA, so their own CA root certificate is cross signed by the established IdenTrust CA. Follow these steps to make sure that all your Expressways trust the Digital Signature Trust X3 root CA:

Procedure

Step 1 Go to https://www.identrust.com/support/downloads and download the TrustID X3 root certificate. At the time of writing, the file is at https://www.identrust.com/node/935. This downloads the file trustidrootx3_chain.p7b.

Step 2 Open the .p7b archive file to convert the p7c certificate inside it to a format that you can upload to the Expressway:

a. On Windows 10:

1. Right-click the downloaded file, and select **Open with** > **Crypto Shell Extensions**.

   The .p7b file opens in Windows Certificate Manager.

2. Open the **Certificates** subfolder, right-click the "DST Root CA X3" certificate, select **All Tasks** > **Export...**.

3. Use the Certificate Export Wizard to export a Base-64 encoded X.509 (.CER) file.

4. Supply the wizard with a file name to save the exported file locally, eg. **DSTRootCAX3.cer**.

b. On Linux:

1. Use openssl to convert the PKCS7 file to PEM format, eg. `openssl pkcs7 -inform der -in dstrootcax3.p7c -print_certs -out dstrootcax3.pem`.

Step 3 For each Expressway-E (and traversal Expressway-C) in the deployment you are securing with certificates signed by Let's Encrypt:

a. Sign on to the Expressway's web interface.

b. Go to **Maintenance** > **Security** > **Trusted CA certificate**.

c. In the **Upload** section of the page, select the certificate file you created.

d. Click **Append CA certificate**.

The trusted CA certificate list should now include the Digital Signature Trust root certificate.

Append Let's Encrypt Intermediate CA Certificate to Expressway Trust Stores

Procedure

Step 1 Go to https://www.letsencrypt.org/certs/lets-encrypt-x3-cross-signed.pem.txt.

Step 2 Copy the text and save it as a local text file, e.g. **lets-encrypt-x3-cross-signed.pem.txt**.

Step 3 For each Expressway-E (and traversal Expressway-C) in the deployment you are securing with certificates signed by Let's Encrypt:

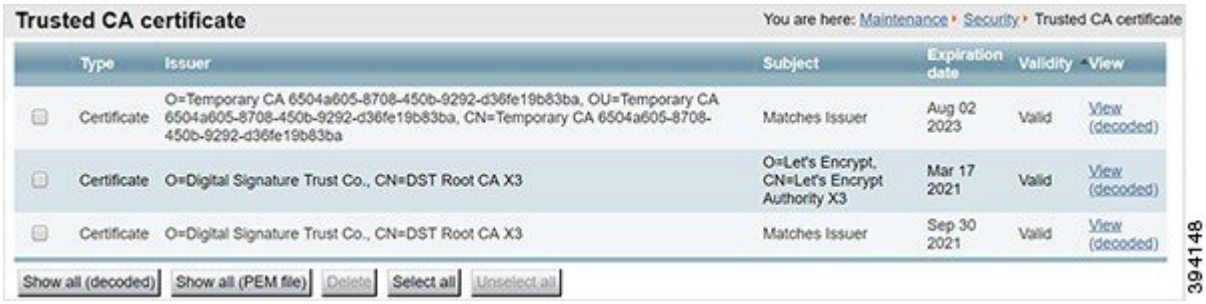
a. Sign on to the Expressway's web interface.

b. Go to **Maintenance** > **Security** > **Trusted CA certificate**.

c. In the **Upload** section of the page, select the certificate file you created.

d. Click **Append CA certificate**.

The trusted CA certificate list should now include both the Digital Signature Trust root certificate and the Let's Encrypt CA certificate.



Configure ACME Certificate Service on Expressway-E

Procedure

Step 1 Sign on to the Expressway-E and go to **Maintenance** > **Security** > **Server certificate**.

Step 2 Scroll down to the **ACME Certificate Service** section.

Step 3 Select the ACME **Provider** from the drop-down list.

This is the CA that signs your certificate. Currently, we only work with Let's Encrypt®.

Step 4 Enter an **Admin Email** address to use with the provider.

This should be a real address, so that you can receive communication from your ACME provider if necessary.

This address is your account name with the provider, and is linked to all certificate signing requests you make with this provider.

Step 5 Read the terms and conditions.

You may want to save a copy for your legal representatives to review, if they have not yet done that.

Step 6 Click **Accept Terms & Conditions**.

The ACME client on Expressway-E creates an account with your chosen provider.

The ACME Certificate Service on Expressway-E client is now ready to interact with your ACME provider.

Configure ACME for Each Domain Certificate

The ACME service on the Expressway-E, from version X12.5, can request and deploy domain certificates (used with SNI).

When you go to **Maintenance** > **> Security** > **Domain certificates**, the list of domains has an ACME column that shows the status of the ACME service for each domain.

Click **View/Edit** next to the domain name to enable the ACME service.

The process of configuring ACME service for domain certificates is the same as it is for the server certificate, only from a different place in the Expressway-E interface.

Generate a Certificate Signing Request for ACME

The process of creating your CSR is no different when you are using the ACME client. Follow the guidance in Generate a Certificate Signing Request (CSR).

Sign the CSR using ACME Provider

When you have a CSR saved on Expressway-E, and configured the ACME service, then you can submit the CSR to your ACME provider to verify and sign.

Procedure

Step 1 Go to **Maintenance** > **Security** > **Server certificate**.

Step 2 Scroll down to the ACME Service Configuration.

Step 3 Click **Sign CSR with ACME Provider**.

The ACME client on Expressway-E submits the saved CSR to the chosen provider.

Step 4 Wait a few minutes for the signing process to complete.

The provider checks DNS for CN and SAN attributes in your CSR, to verify that they match up with the Expressway-E address from which it received the signing request. The provider signs and returns the certificate, which the ACME client stores on Expressway-E, waiting for you to deploy it.

Step 5 Manually refresh the **Server certificate** page.

You see a success banner when the certificate is signed and ready to use.

[Optional] Check the Signed ACME Certificate

Procedure

Step 1 Go to **Maintenance** > **Security** > **Server certificate** and down to the **ACME Certificate Service** section.

The **Status** field shows that you have a signed certificate ready to deploy.

Step 2 In the **Pending ACME Certificate** field, click **Show (decoded)**.

Step 3 Verify the details are as you expected. If they are not, you may have to discard the pending cert and generate a new CSR.

Note It's possible that Let's Encrypt CA may ignore some of the attributes you provided in the CSR.

Deploy the ACME Certificate

Procedure

Step 1 Go to **Maintenance** > **Security** > **Server certificate** and down to the **ACME Certificate Service** section.

The **Status** field shows that you have a signed certificate ready to deploy.

Step 2 Click **Deploy Pending Cert**.

The Expressway-E starts using this certificate in transactions that require it to authenticate itself to the other party. There is no need to restart the Expressway-E.

Enable Automated Renewal of the ACME Certificate

ACME certificates are deliberately short-lived as a security precaution. At the time of writing, the validity period is 90 days from the date of issue.

The ACME Certificate Service on Expressway-E monitors the certificate validity, and warns you when two-thirds of the validity period has elapsed. You can manually respond by following the procedure outlined in previous topics.

To avoid this frequent task, you can use the automated renewal option to have the ACME Certificate Service renew and deploy your certificate for you.

Procedure

Step 1 Go to **Maintenance** > **Security** > **Server certificate** and down to the **ACME Certificate Service** section.

Step 2 Change the **ACME Automated Scheduler** field to *On*.

Step 3 Select one or more **Schedule Days** and a **Schedule Time**.

When two-thirds of the certificate's validity has elapsed, the ACME Certificate Service attempts to renew and deploy the server certificate at the given time on the next selected day.

Step 4 Click **Save**.

The **Status** shows that the service is in Automated mode. The next time it renews and deploys the certificate, it updates the **Last Deploy Status** and **Last Sign Status**.

Revoke an ACME Certificate

These are some of the reasons why you might want to revoke an ACME certificate on your Expressway-E:

- The Expressway-E has been compromised.
- You factory reset the Expressway-E.
- The purpose of the Expressway-E changed.
- The ACME account is no longer valid.

To revoke an ACME certificate, you need to prove to the provider that you own the Expressway-E's DNS address and that you control the original entries in the certificate. To do that you need to repeat the signing CSR process used for the certificate, but you do not need to redeploy the resulting certificate.

You should deploy a new certificate before you revoke the original certificate. Keep a copy of the certificate you want to revoke.

Caution Do not revoke a certificate that is in use, because that will interrupt all services that use this certificate.

Procedure

Step 1 Take a backup of the current certificate.

This precaution helps if you inadvertently overwrite your current certificate with one that you intend to revoke.

Step 2 Copy the certificate that you want to revoke into a temporary location on the Expressway-E. Remember the path to the location.

If you do not have a copy of the certificate you want to revoke, you may be able to retrieve it from https://crt.sh/.

Step 3 Create a CSR that contains all the domain names of the certificate you want to revoke. See Generate a Certificate Signing Request for ACME.

Step 4 Submit the CSR to be signed by the ACME provider that signed the original certificate. See Sign the CSR using ACME Provider.

You should now have a new, pending certificate that has matching SAN entries to the certificate you want to revoke.

This process has proved that you are entitled to revoke the original certificate.

Step 5 Sign in (as an administrator) to the CLI of the Expressway-E.

Step 6 Run the acmerevoke command in one of the following ways:

- If the default provider signed the certificate: `xcommand Acmerevoke "/path_to_cert_to_be_revoked"`
- Otherwise, specify the provider that signed the certificate: `xcommand Acmerevoke CertPath:"/path_to_cert_to_be_revoked" Provider:"ACME_Provider_Name"`

  (The same provider that signed the certificate must also revoke the certificate.)

The provider responds with 200 OK if it successfully revoked the certificate.

Step 7 Delete any saved copies of the revoked certificate.