Authorize a Request and Generate a Certificate Using Microsoft Certification Authority

This section describes how to authorize a certificate request and generate a PEM certificate file using Microsoft Certification Authority.

Note The CA component of Microsoft Active Directory Certificate Services (AD CS) must be able to issue a certificate that can be used for authentication of the Expressway as client or server.

AD CS in Windows Server 2008 Standard R2 (and later) can issue these types of certificates, if you create a certificate template for them. **Earlier versions of Windows Server Standard Edition are not suitable**.

1. Copy the certificate request file (for example, **certcsr.der** if generated via OpenSSL) to a location, such as the desktop, on the server where the Microsoft Certification Authority application is installed.
2. Submit the certificate request from a command prompt:
   - To generate a certificate with Server Authentication and Client Authentication, which is required if you want to configure a neighbor or traversal zone with mutual authentication (TLS verify mode), type:

     ```
     certreq -submit -attrib "CertificateTemplate:Webclientandserver"

     C:\Users\<user>\Desktop\certcsr.der
     ```

     See Appendix 5: Enable AD CS to Issue "Client and Server" Certificates for details about how to set up the `Webclientandserver` certificate template.
   - To generate a certificate with Server Authentication only, type:

     ```
     certreq -submit -attrib "CertificateTemplate:WebServer"
     C:\Users\<user>\Desktop\certcsr.der
     ```

   This triggers the Certification Authority window to open:

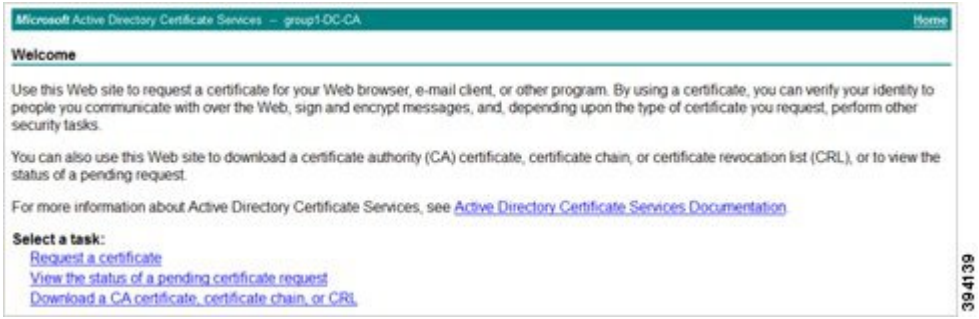
Authorize a Request and Generate a Certificate Using Microsoft Certification Authority

Note The command must be run as the administrator user.

3. Select the **Certification Authority** to use (typically only one is offered) and click **OK**.
4. When requested, save the certificate (browse to the required folder if the default **Libraries** > **Documents** folder is not to be used) calling it **server.cer** for example.
5. Rename **server.cer** to **server.pem** for use with the Expressway.

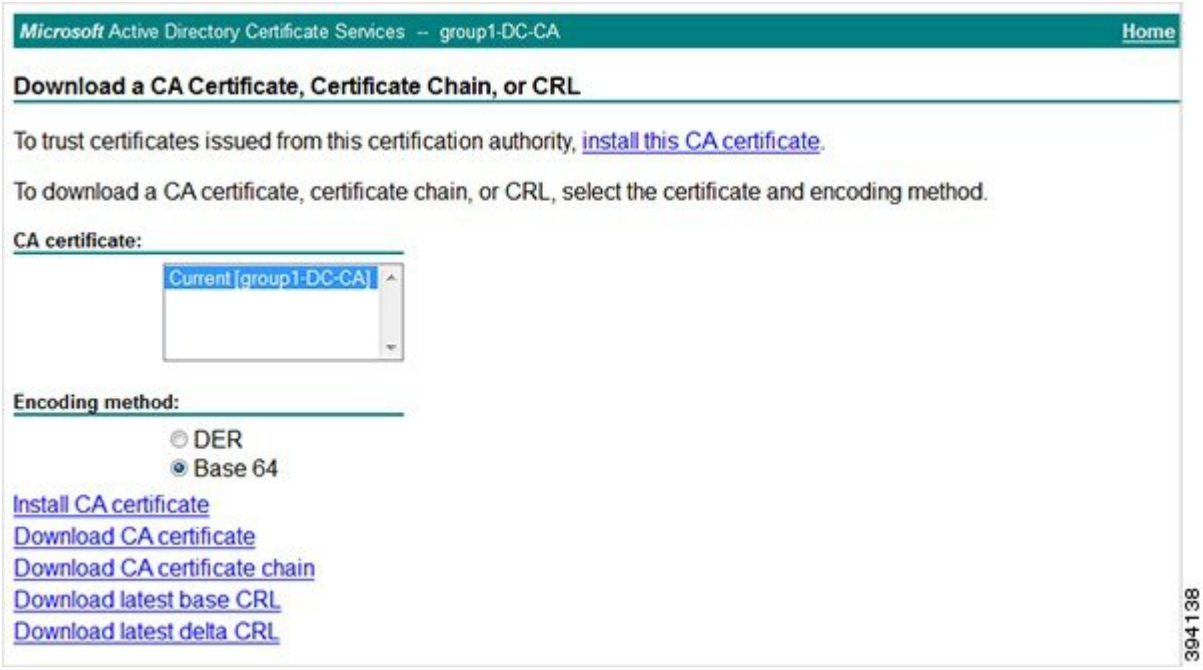
Get the Microsoft CA certificate

1. In your web browser, go to <IP or URL of the Microsoft Certificate Server>/certsrv and log in.

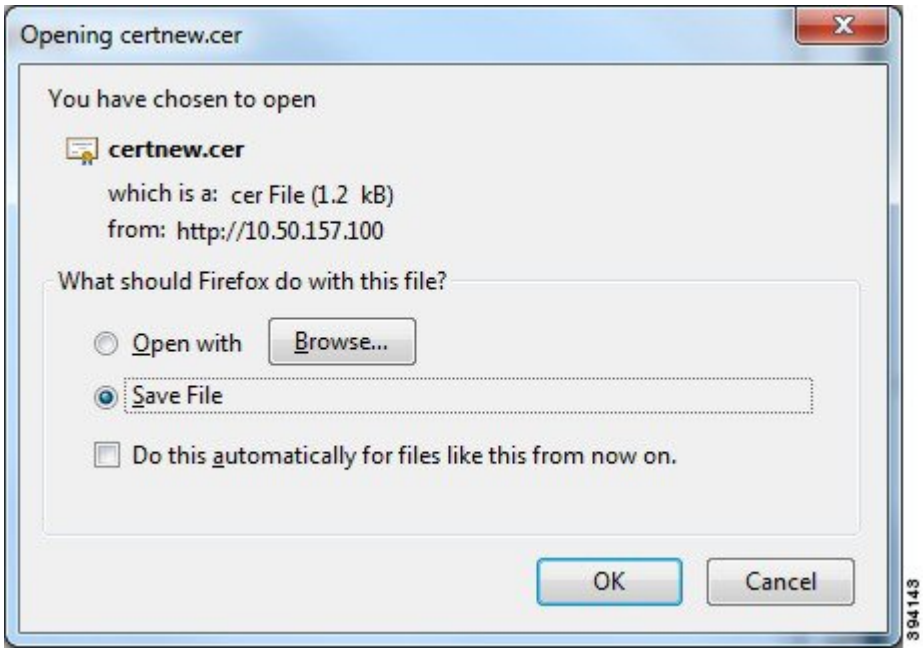


2. Select **Download a CA certificate, certificate chain or CRL**

Authorize a Request and Generate a Certificate Using Microsoft Certification Authority



3. Select the option **Base 64** under **Encoding method**.
4. Click **Download CA certificate** link.



5. Choose **Save File** and click **OK**.
6. Rename **certnew.cer** to **certnew.pem**.

Files **server.pem** and **certnew.pem** are now available.

Authorize a Request and Generate a Certificate Using Microsoft Certification Authority

Go to the Load Certificates and Keys Onto Expressway section in this document to know how to upload **server.pem** and **certnew.pem** to Expressway.