

Authorize a Request and Generate a Certificate Using Microsoft Certification Authority

• Authorize a Request and Generate Certificate using Microsoft Certificate Authority, on page 1

Authorize a Request and Generate Certificate using Microsoft Certificate 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**.

- 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:

A	Computer	
arusc-ser1-CA (Kerberos)	ser1.cisco.com	
E.	1	



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.

Welcome	
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.	1
You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view to status of a pending request.	e
For more information about Active Directory Certificate Services, see Active Directory Certificate Services Documentation.	
Select a task:	
Request a certificate	
View the status of a pending certificate request	
Download a CA certificate, certificate chain, or CRI,	

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

Microsoft Active Directory Certificate Services group1-DC-CA	Home
Download a CA Certificate, Certificate Chain, or CRL	
To trust certificates issued from this certification authority, install this CA certificate.	
To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.	
CA certificate:	
Current [group1-DC-CA]	
•	
Encoding method:	
© DER	
Base 64	
Install CA certificate	
Download CA certificate	
Download CA certificate chain	
Download latest base CRL	
Download latest delta CRL	

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

You have chosen to	pen	
🔄 certnew.cer		
which is a: cer	File (1.2 kB)	
from: http://10	.50.157.100	
What should Firefor	do with this file?	
© Open with	<u>B</u> rowse	
Save File		
🔲 Do this <u>a</u> uto	natically for files like this from now on	

5. Choose Save File and click OK.

6. Rename certnew.cer to certnew.pem.

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

3

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.