

## Enable AD CS to Issue "Client and Server" Certificates

• Enable AD CS to Issue "Client and Server" Certificates, on page 1

## **Enable AD CS to Issue "Client and Server" Certificates**



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.** 

The default "Web Server" certificate template in AD CS creates a certificate for Server Authentication. The server certificate for the Expressway also needs Client Authentication if you want to configure a neighbor or traversal zone with mutual authentication (where **TLS verify mode** is enabled).

To set up a certificate template with both Server and Client authentication:

1. In Windows, launch Server Manager (Start > Administrative Tools > Server Manager).

(Server Manager is a feature included with server editions of Windows.)

- Expand the Server Manager navigation tree to Roles > Active Directory Certificate Services > Certificate Templates (<domain>).
- 3. Right-click on Web Server and select Duplicate Template.

🗢 🌳 🛛 🔟 🔟 🖾 🔛 🔟 🗔 🗌					
Server Manager (WINDOWS2008)	Certificate Templates (windows2008.acme.com)				
Roles Active Directory Certificate Serv Enterprise PKI Certificate Certificate Serv	Template Display Name ~	Minimum Supported CAs	Version Intended Purposes		
	IPSec (Offline request)	Windows 2000	7.1		
	Rerberos Authentication	Windows Server 2003 Ent	110.0 Client Authentication, Server Authentication,		
Acme-WINDOWS2008-CA	Key Recovery Agent	Windows Server 2003 Ent	105.0 Key Recovery Agent		
F S Active Directory Domain Service	CCSP Response Signing	Windows Server 2008 Ent	101.0 OCSP Signing		
E L DNS Server	RAS and IAS Server	Windows Server 2003 Ent	101.0 Client Authentication, Server Authentication		
😥 🦥 Web Server (IIS)	Root Certification Authority	Windows 2000	5.1		
E of Features	Router (Offline request)	Windows 2000	4.1		
Diagnostics	Smartcard Logon	Windows 2000	6.1		
Configuration	Smartcard User	Windows 2000	11.1		
🛞 🚰 Storage	Subordinate Certification Authority	Windows 2000	5.1		
	Trust List Signing	Windows 2000	3.1		
	🔄 User	Windows 2000	3.1		
	General User Signature Only	Windows 2000	4.1		
	Web Server Durikate Terror	inter Vindovis 2000	4.1		
		Vindows Server 2003 Ent	101.0 Client Authentication		
	All Tasks	•			
	Properties				
	Hein				

- 4. Select Windows Server 2003 Enterprise and click OK.
- 5. On the General tab, enter the Template display name and Template name, for example Web client and server and Webclientandserver.

Issuance	Requirements   Sup	erseded Templates   Extensions	Security
General	Request Handling	Cryptography Subject Name	Server
Template	displau name:		
Web clie	ent and server Supported CAs: Win	dows Server 2008 Enterprise	

6. On the Extensions tab, select Application Policies and click Edit.

General	Request Hand	dling	Crypto	graphy	Su	bject Name	e Serve
ssuance	Requirements	Supe	rseded	Template	es l	Extensions	Securit
Extension	ns included in thi	is templ	Jate:	CITCUCK	<u> </u>		
Appli Appli	cation Policies						
Basic	c Constraints						
Certil	icate Template I	Informa	ition				
lissua 🛄	ince Policies						
Key I	Jsage						
							Edit

- 7. Add Client Authentication to the set of application policies:
  - a. Click Add
  - b. Select Client Authentication and click OK
  - c. Click OK

used.	itines how a cert	ficate can be
Application p <u>o</u> licies:		
Client Authentication Server Authentication		
<u>A</u> dd	<u>E</u> dit	<u>R</u> emove
<u>A</u> dd	<u>E</u> dit	<u>R</u> emove

- 8. Click OK to complete the addition of the new template.
- 9. Add the new template to the Certificate Authority:

- a. Go to Roles > Active Directory Certificate Services > <your certificate authority>.
- b. Right-click Certificate Templates and select New > Certificate Template to Issue

🗯 🔿 🙍 📷 🛛 🐽					
Server Manager (WINDO	W52008)	Certificate Templates			
Koles Active Directory	Certificate Serv	Name	Intended Purpose		
Enterprise Pi Certificate To Certificate To acme-WINDO Revoked Issued C Pending Failed Re Certific  Active Directory	(I emplates (windc )WS2008-CA Certificates ertificates Requests equests Manage	Directory Email Replication Domain Controller Authentication EFS Recovery Agent Basic EFS Domain Controller Web Server Computer User Subordinate Certification Authority	Client Authentication, Server Authenticatio File Recovery Encrypting File System Client Authentication, Server Authentication Server Authentication Client Authentication, Server Authentication Encrypting File System, Secure Email, Clien <all></all>		
DNS Server	New	Certificate Template to Issue	Microsoft Trust List Signing, Encrypting File		
Features	View	•			
Image Diagnostics Image Diagnostics Image Diagnostics Image Diagnostics	Refresh Export List				
	Help				

c. Select your new Web client and server template and click OK.

ote: If a certificate template that was re- ormation about this template has been	cently created does not appear on this list, you may need to wait until replicated to all domain controllers.	
or the certificate templates in the organ or more information, see <u>Certificate Tem</u>	nization may not be available to your CA. <u>plate Concepts.</u>	
Name	Intended Purpose	
OCSP Response Signing	OCSP Signing	
RAS and IAS Server	Client Authentication, Server Authentication	
🕺 Router (Offline request)	Client Authentication	
Smartcard Logon	Client Authentication, Smart Card Logon	
Smartcard User	Secure Email, Client Authentication, Smart Card Logon	
🕺 Trust List Signing	Microsoft Trust List Signing	
🕺 User Signature Only	Secure Email, Client Authentication	
Web client and server	Server Authentication, Client Authentication	
Workstation Authentication	Client Authentication	_
	an total and a second sec	č

The new **Web client and server** template can now be used when submitting a certificate request to the Microsoft Certification Authority.