

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.)

- 2. 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.

File Action View Help				
Server Manager (WINDOWS2008)	Certificate Templates (windows2008.acm	ne.com)	-	
Roles Greater Directory Certificate Serv	Template Display Name	Minimum Supported CAs	Version	Intended Purposes
Convertige Office Certificate Serv	IPSec (Offline request)	Windows 2000	7.1	
Certificate Templates (windc	Kerberos Authentication	Windows Server 2003 Ent	110.0	Client Authentication, Server Authentication, S
acme-WINDOWS2008-CA	Rey Recovery Agent	Windows Server 2003 Ent	105.0	Key Recovery Agent
E S Active Directory Domain Service:	CCSP Response Signing	Windows Server 2008 Ent	101.0	OCSP Signing
E 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	
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	
	G User Signature Only	Windows 2000	4.1	
	Web Server Duplicate Templat	Mindows 2000	4.1	
	Workstation Authentic	Vindows Server 2003 Ent	101.0	Client Authentication
	All Tasks	•		
	Properties			
	Help			

- 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 Su	iperseded Templates Extensions S	ecurity
General	Request Handling	and have been also been a second provide the second s	Server
Tomplate	display name:		
			-
	ent and server		
Web clie	ent and server	indows Server 2008 Enterprise	
Web clie	ent and server	indows Server 2008 Enterprise	

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

Issuance Requirements Superseded Templates Extensions Security To modify an extension, select it, and then click Edit. Extensions included in this template: Application Policies Basic Constraints Certificate Template Information Issuance Policies Key Usage	General	Request Hand	dling Cryp	otography	Subject Name	Server
Extensions included in this template: Application Policies Basic Constraints Certificate Template Information Issuance Policies	Issuance	Requirements	Supersede	d Templates	Extensions	Security
Basic Constraints Certificate Template Information Issuance Policies				(Hen Click E	uit.	
Certificate Template Information	Appli Appli	cation Policies				
Issuance Policies	📑 Basid	c Constraints				
	Certi	icate Template I	nformation			
Key Usage	📑 Issua	ance Policies				
		Jsage				
	🔣 Key I					
	Key I					
	Key					dit [

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

An application policy d used.	efines how a cert	ificate can be
Application p <u>o</u> licies:		
Client Authentication Server Authentication		
<u>A</u> dd	<u><u> </u></u>	<u>R</u> emove
<u>A</u> dd		<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 (WINDOWS2008)		Certificate Templates		
Roles G Roles G Roles	Certificate Serv	Name	Intended Purpose	
E 🛃 acme-WINDO Revoked Issued C Pending Failed Re	emplates (windc DWS2008-CA Certificates ertificates Requests	Directory Email Replication Domain Controller Authentication EFS Recovery Agent Basic EFS Domain Controller Web Server Computer User Subordinate Certification Authority	Directory Service Email Replication 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 <al></al>	
E 🥈 DNS Server	New	Certificate Template to Issue	Microsoft Trust List Signing, Encrypting File	
Web Server (II!	View	•		
Diagnostics Configuration Storage	Refresh Export List			
	Help			

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

of the certificate templates in the organ r more information, see <u>Certificate Temp</u>	eplicated to all domain controllers. ization may not be available to your CA. <u>Nate Concepts.</u>	
lame	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	

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