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:

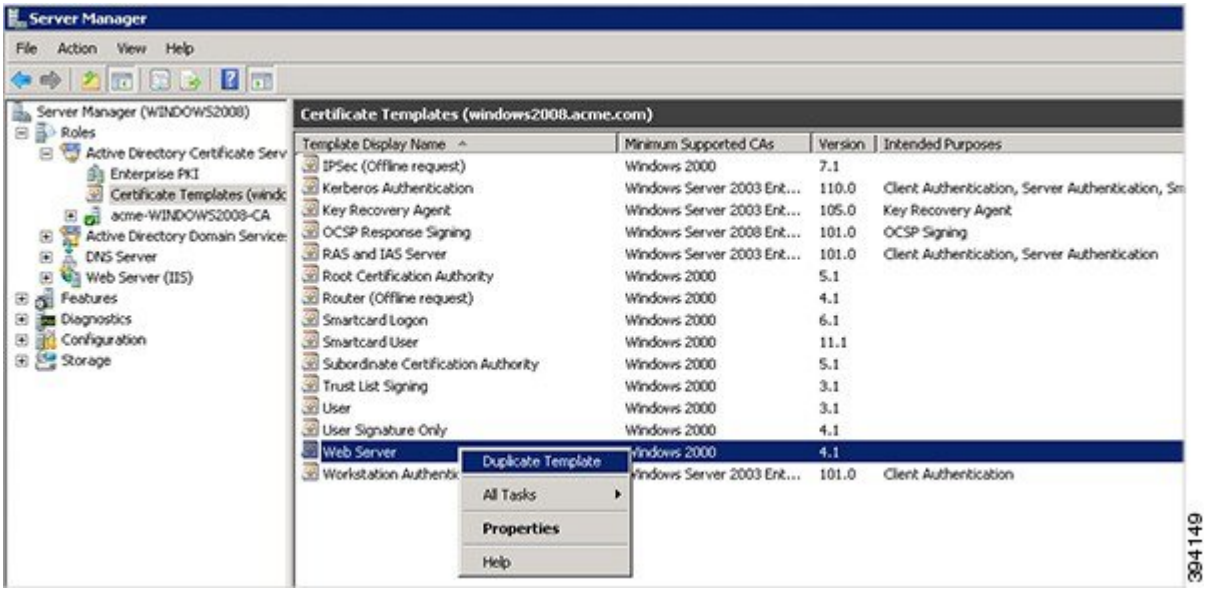
1. In Windows, launch **Server Manager** (**Start** > **Administrative Tools** > **Server Manager**).

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

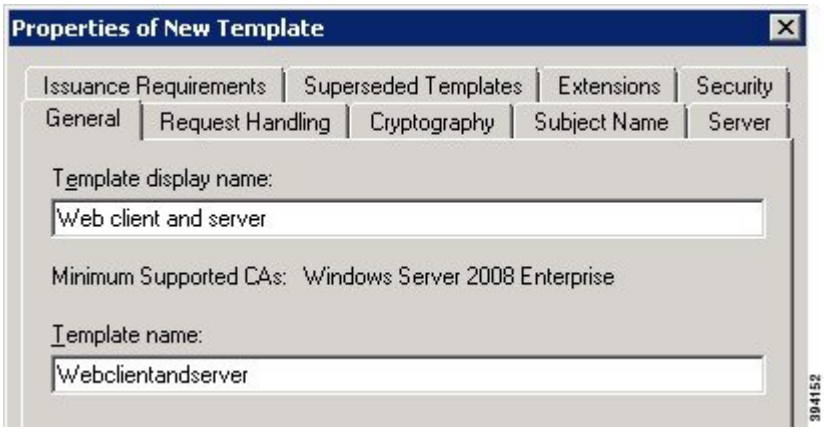
2. Expand the **Server Manager** navigation tree to **Roles** > **Active Directory Certificate Services** > **Certificate Templates (<domain>)**.

3. Right-click on **Web Server** and select **Duplicate Template**.

Enable AD CS to Issue Client and Server Certificates

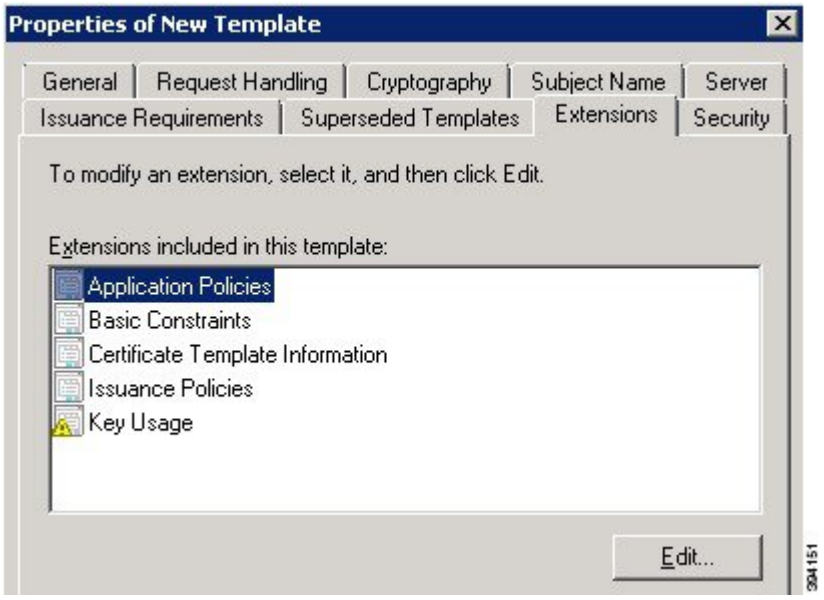


4. Select **Windows Server 2003 Enterprise** and click **OK**.
5. On the **General** tab, enter the **Template display name** and **Template name**, for example `Web client and server` and `Webclientandserver`.

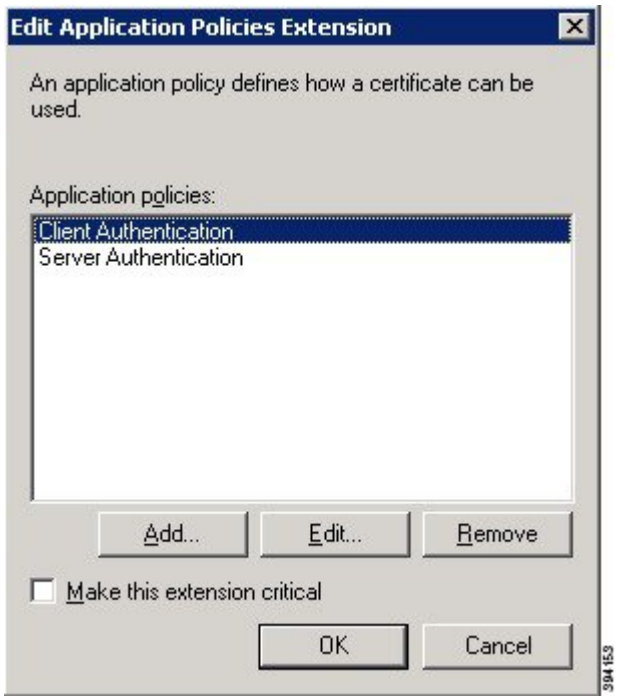


6. On the **Extensions** tab, select **Application Policies** and click **Edit**.

Enable AD CS to Issue Client and Server Certificates



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

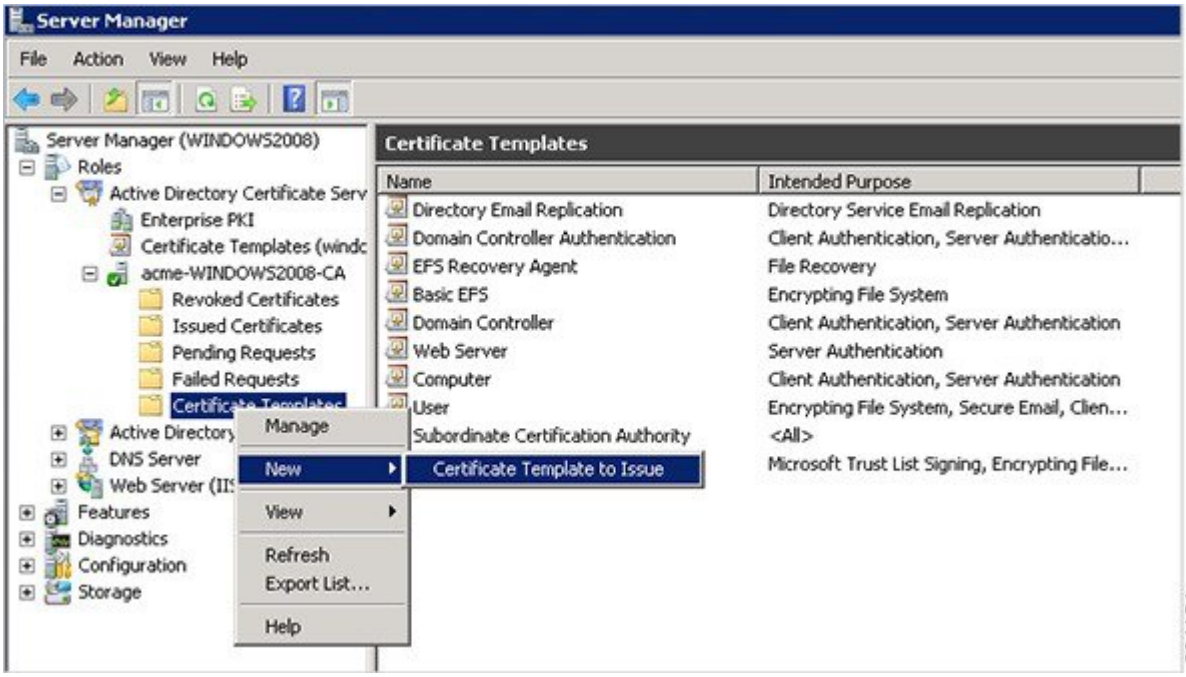


8. Click **OK** to complete the addition of the new template.
9. Add the new template to the Certificate Authority:

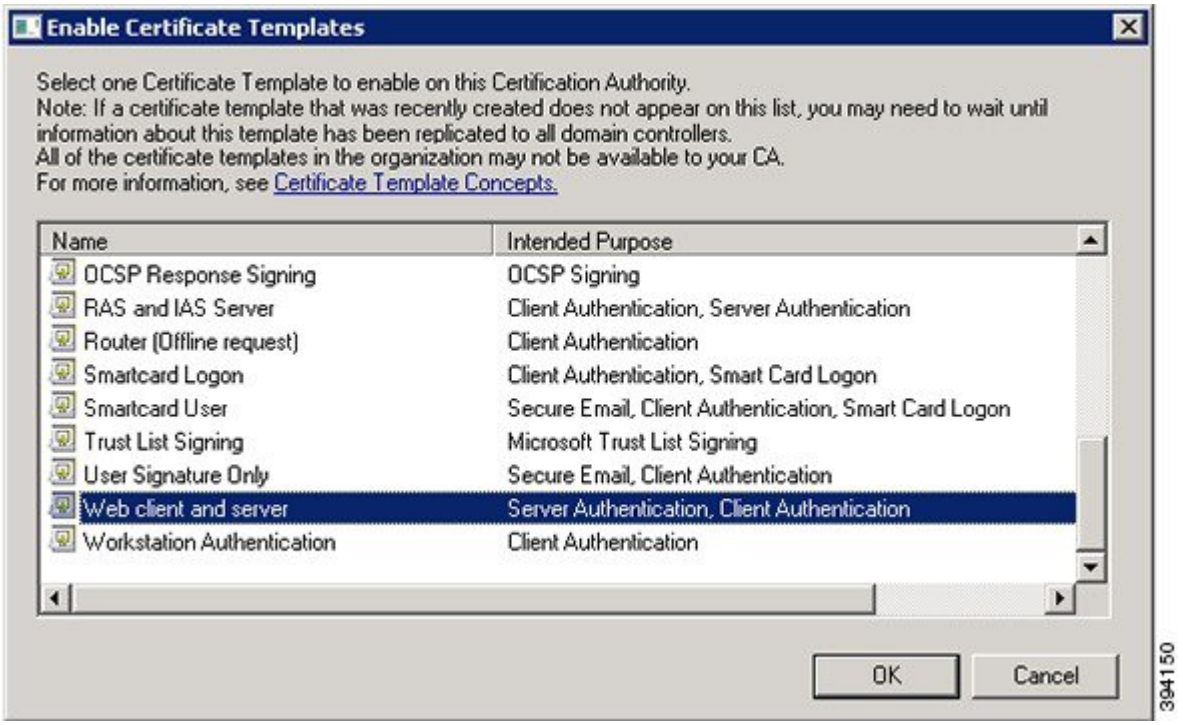
Enable AD CS to Issue Client and Server Certificates

a. Go to **Roles** > **Active Directory Certificate Services** > **<your certificate authority>**.

b. Right-click **Certificate Templates** and select **New** > **Certificate Template to Issue**



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



Enable AD CS to Issue Client and Server Certificates

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

Enable AD CS to Issue Client and Server Certificates