Product Support Notice

PSN #	PSN002181u				
Original publication date: 18-Dec-08. This is Issue #01, published date: 18-Dec-08.		Severity/risk level	Medium	Urgency	Immediately
Name of problem	Microsoft Windows 2008 Enterprise Certification Authority server does not support web enrollment for version 3 certificate templates.				

Products affected

Application Enablement Services (AES) 4.x.x using Microsoft Windows 2008 Enterprise Certification Authority (CA) server.

Problem description

The server certificates exchanged between Avaya AES and Microsoft Live Communications Server (LCS) / Microsoft Office Communications Server (OCS) must support both Server Authentication and Client Authentication key usage. The certificate template is used to create server certificates for both AES and LCS/OCS.

Note: In case of OCS server pool, the load balancer must have certificate with both Server Authentication and Client Authentication.

Microsoft Windows 2008 Enterprise CA Server does not support web enrollment for version 3 certificate templates.

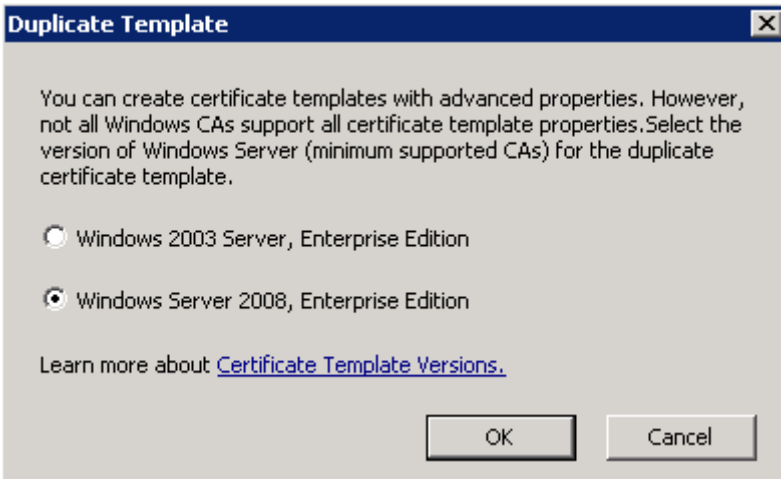
Resolution

Following are the steps to create and use a version 3 certificate template on the Windows Server 2008 Enterprise CA.

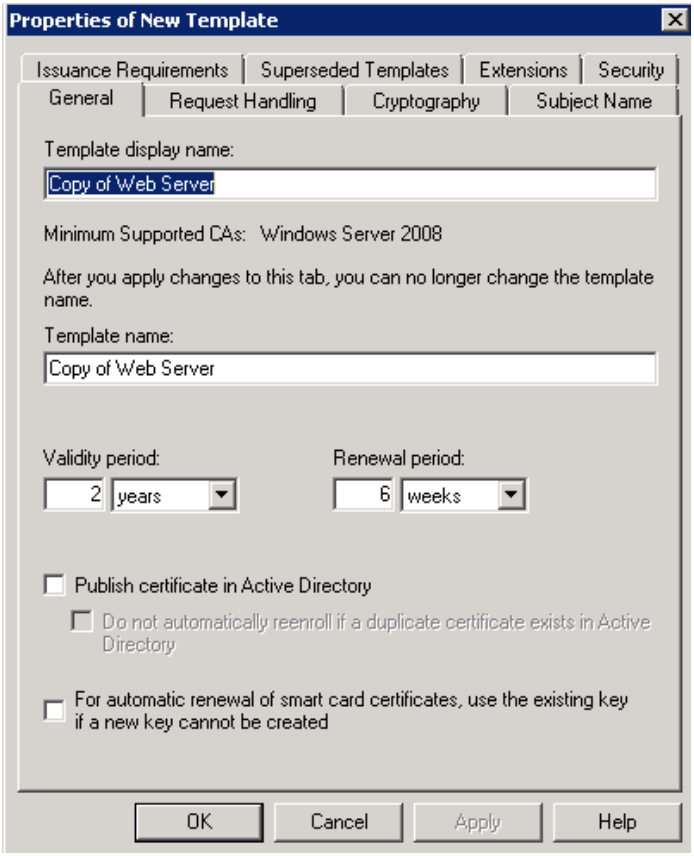
To create a template:

Follow the steps given below:

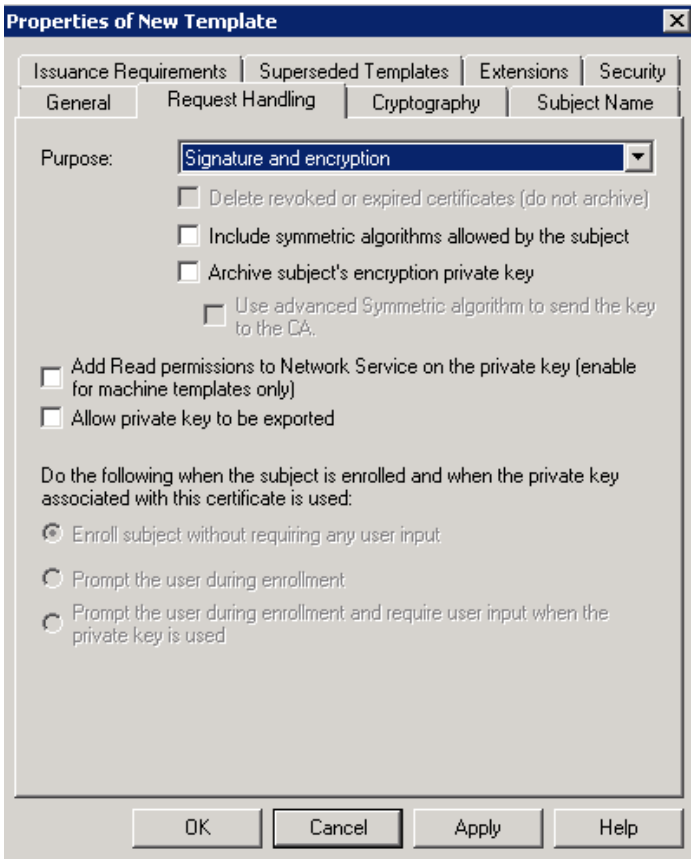
1. On the windows 2008 Enterprise CA server, launch the CA Microsoft Management Console (MMC) snap-in.
2. In the left pane of the Certification Authority MMC snap-in, expand the CA node, right-click on Certificate Templates, and select "Manage" to launch the Certificate Templates MMC snap-in.
3. In the right pane of the Certificate Templates MMC snap-in, right-click on the Web Server template, and select "Duplicate Template".
4. In the Duplicate Template dialog box, select **Windows Server 2008, Enterprise Edition.**



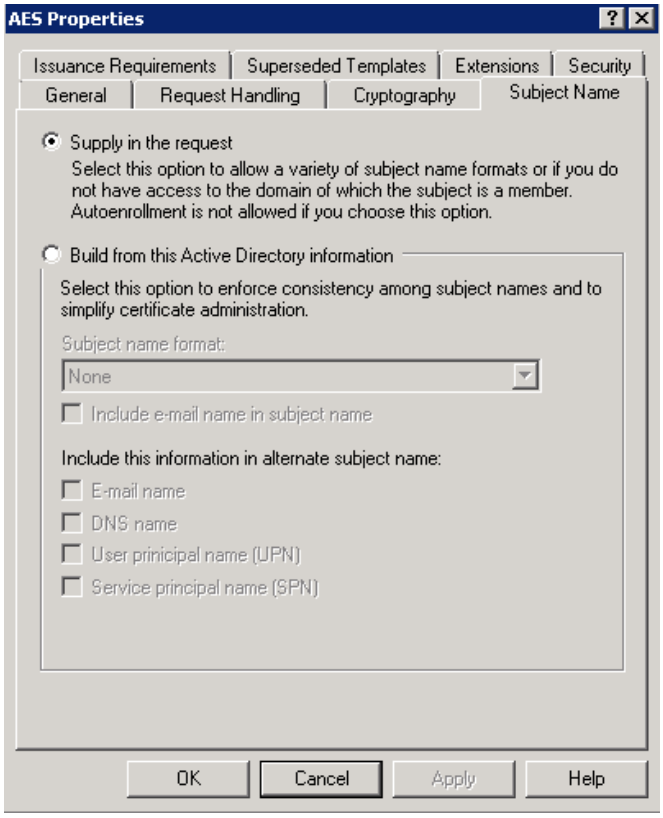
5. In the Properties of New Template dialog box, select the **General** tab, and enter a descriptive Template display name and Template name.



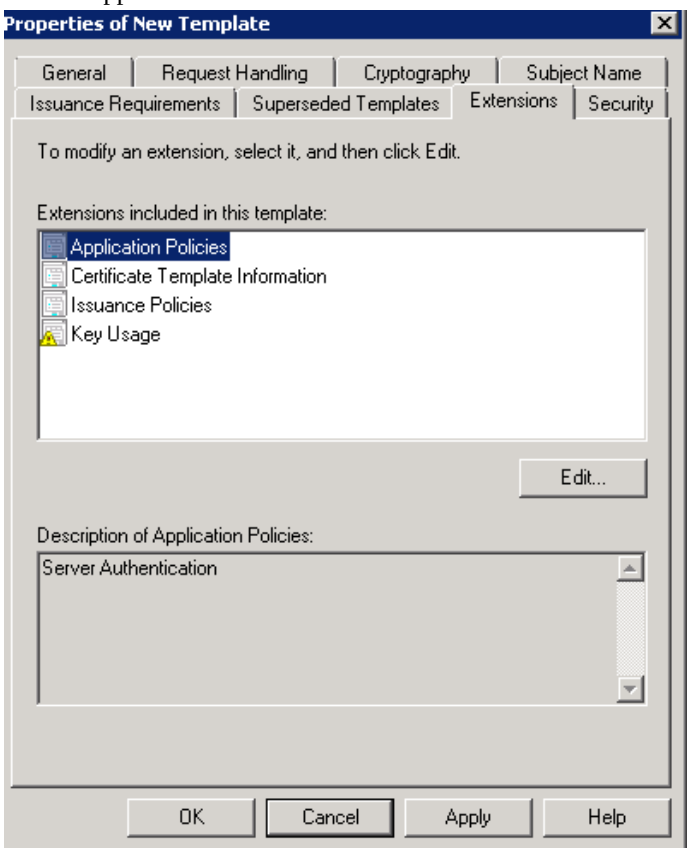
6. In the Properties of New Template dialog box, select the **Request Handling** tab, and ensure that Purpose is set to "Signature and encryption".



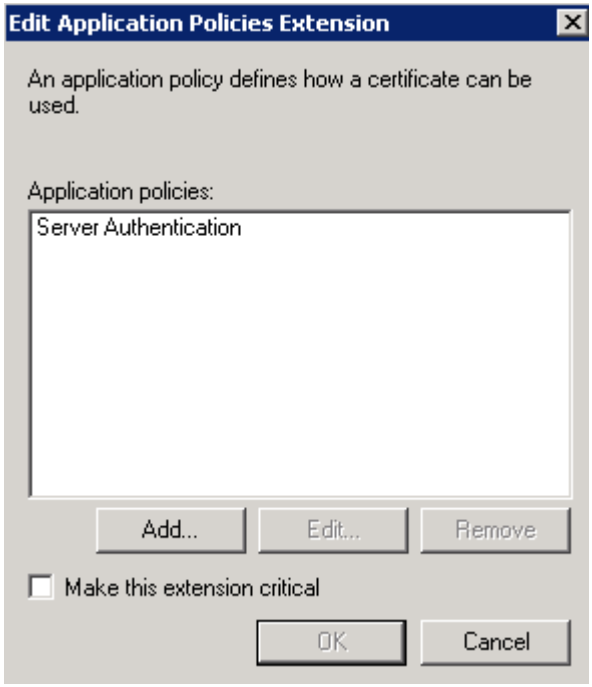
7. In the Properties of New Template dialog box, select the **Subject Name** tab and ensure that "Supply in the request" is selected.



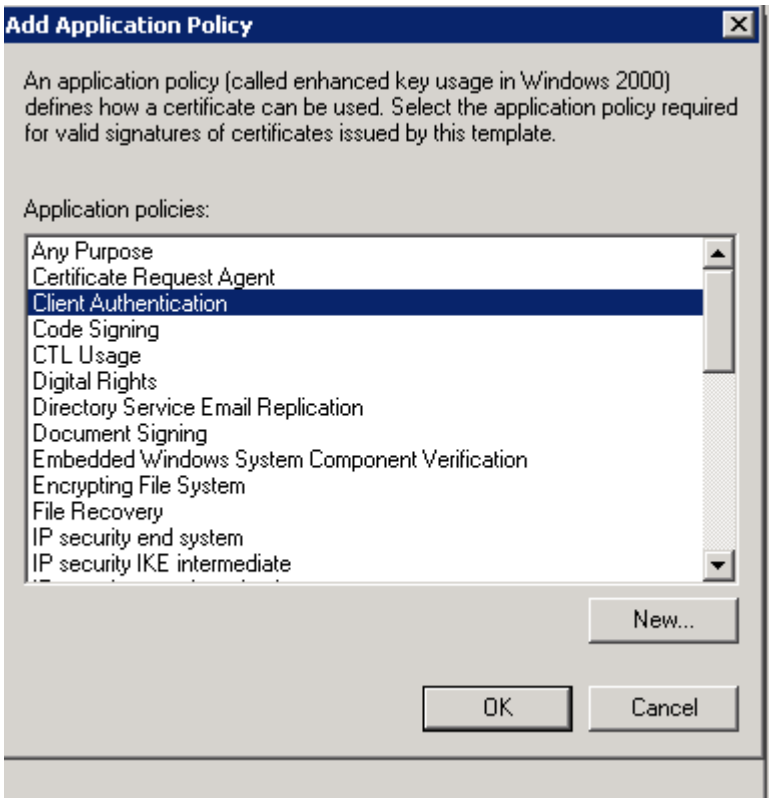
8. In the Properties of New Template dialog box, select the **Extensions tab**. In the Extensions included in this template section, select “Application Policies” and click on "Edit".



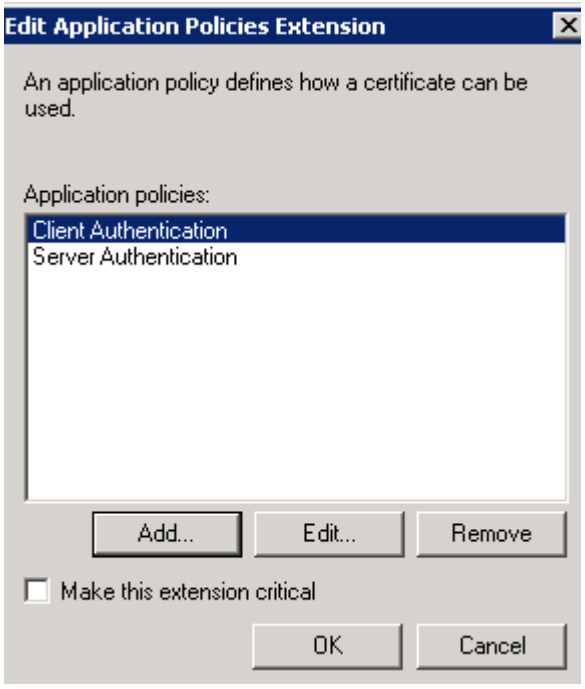
9. In the Edit Application Policies Extension dialog box, click **Add**.



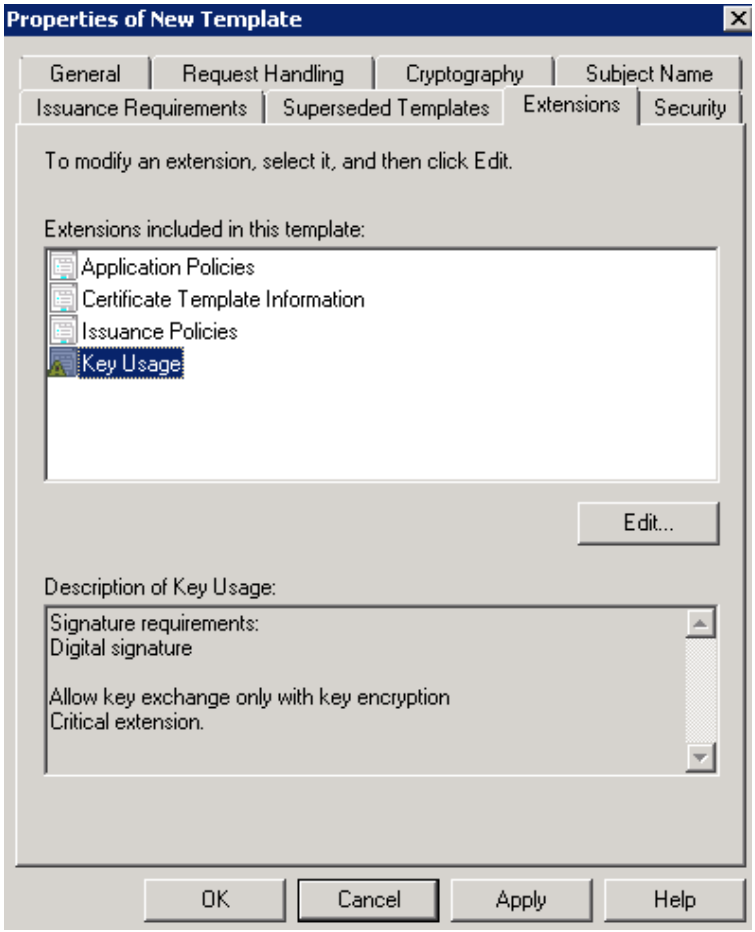
10. In the Add Application Policy dialog box, select **Client Authentication** and click **OK**.



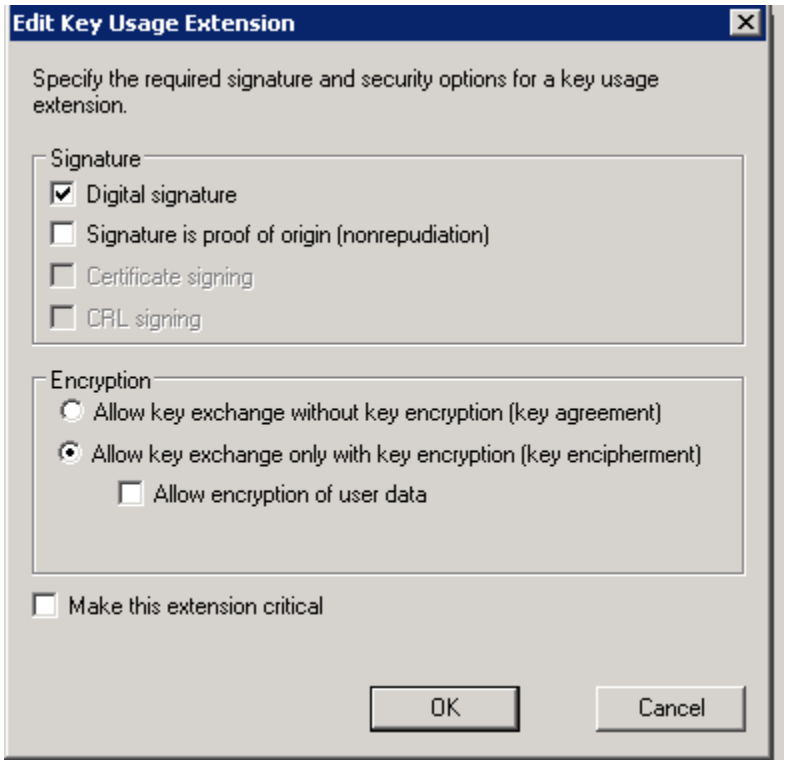
11. In the Edit Application Policies Extension dialog box, ensure that both Server Authentication and Client Authentication are included in the Application Policies list then click **OK**.



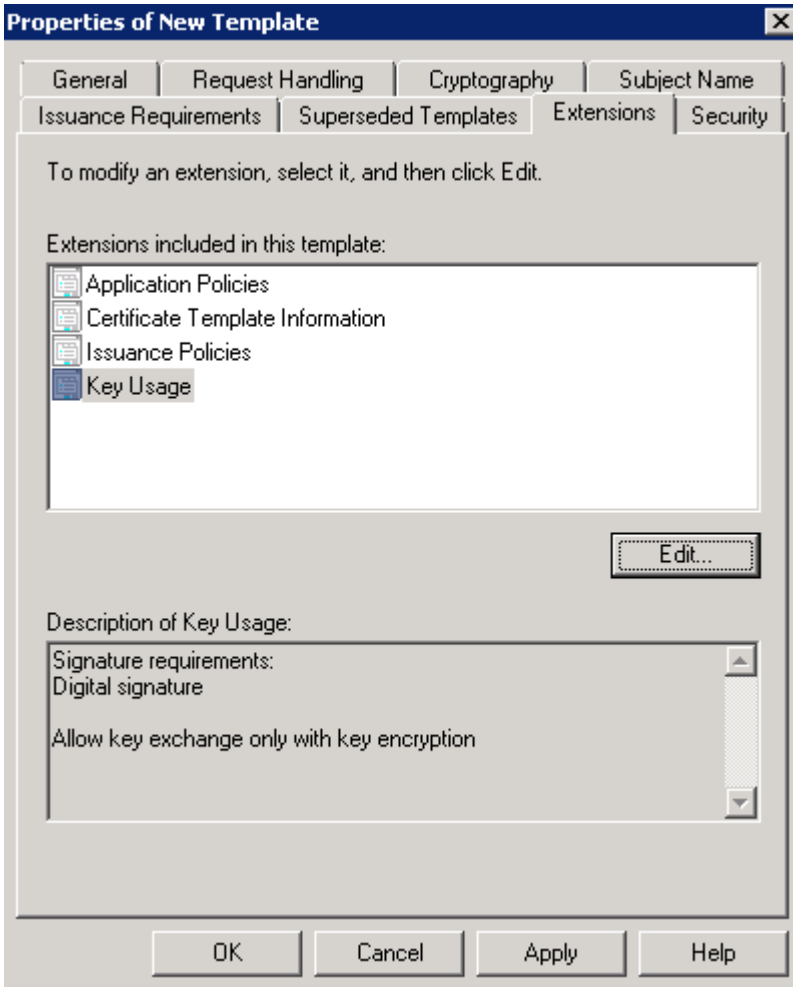
12. In the Properties of New Template dialog box, select the **Extensions** tab. In the Extensions included in this template section, select **Key Usage** and click **Edit**.



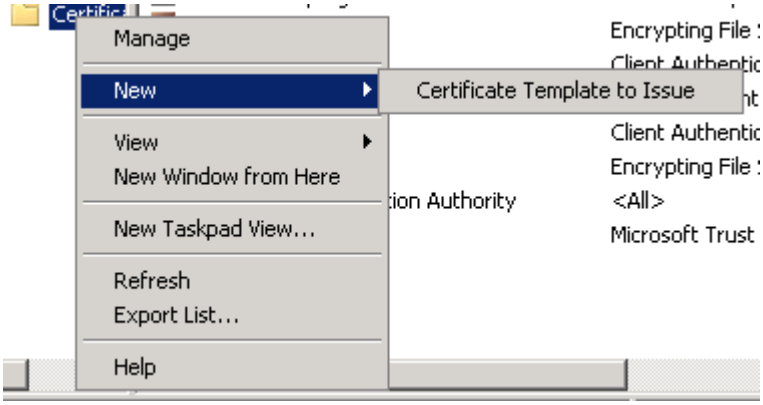
13. In the Edit Key Usage Extension dialog box, uncheck "Make this extension critical" and click **OK**.



14. In the Properties of New Template dialog box, click **OK**.



15. In the Certification Authority MMC snap-in, expand the Certification Authority node; right click on Certificate Templates, select **New** and point to **Certificate Template to Issue**.



16. In the Enable Certificate Templates dialog box, select the Certificate Template created in Steps 3 -14 and click **OK**.

To request and install server certificate on an AES server:

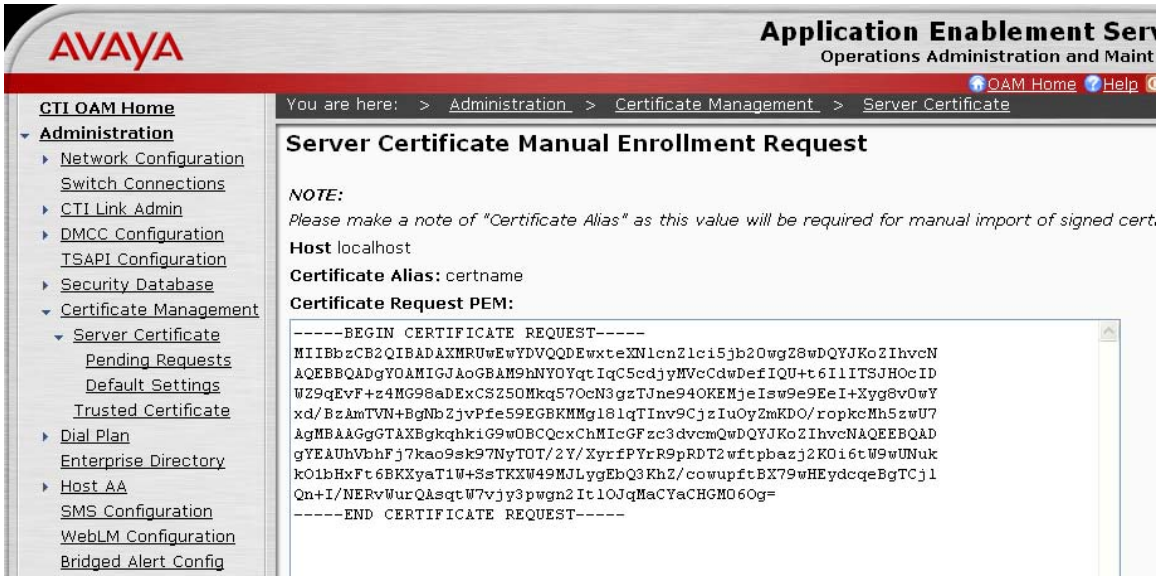
Follow the steps given below:

1. Launch a web browser and log into the Avaya AE Services OAM Web Interface. In the left pane, select **CTI OAM Home** > **Administration** > **Certificate Management** > **Server Certificate**. In the Server Certificates page, click **Add.**

2. In the Add Server Certificate page, configure the following and click **Apply**.
   - Certificate Alias – enter a descriptive name.
   - Password and Re-enter Password – enter an arbitrary password.
   - Distinguished Name – enter "**CN=<FQDN of Avaya AE Services server>,OU=<Department>,O=<Company>,L=<City>,S=<State>,C=<Country/Region>**" .

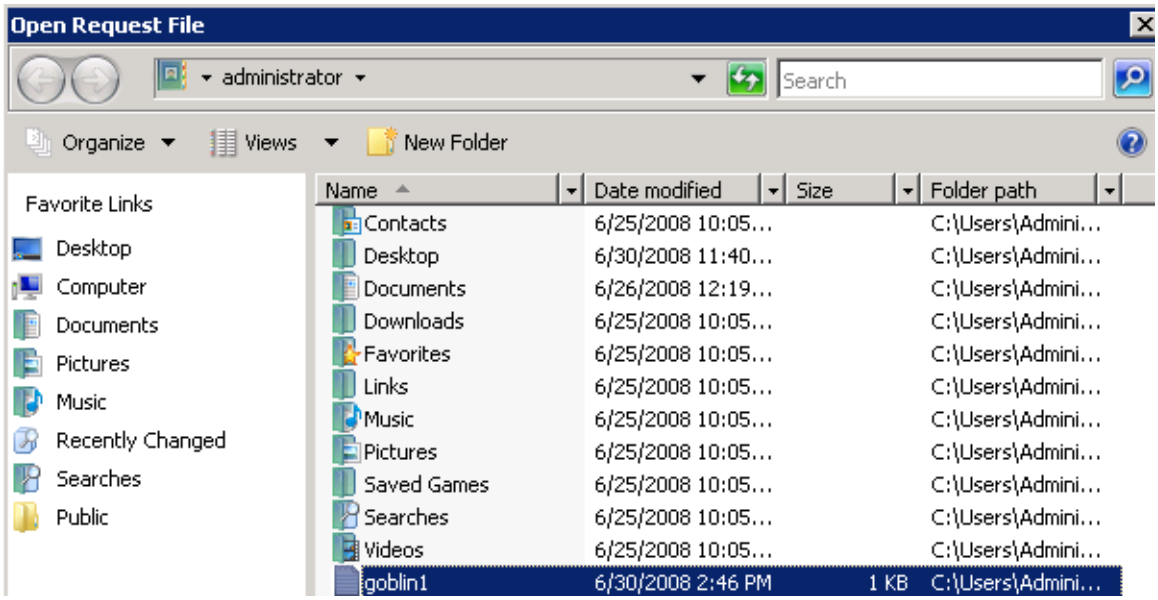
     Use the same Department, Company, City, State, and Country/Region values entered in Section 5.3 Step 5. In the below given example,"**CN=msavaes1.sitlms.net,OU=SITL,O=Avaya,L=Lincroft,S=New Jersey,C=US**" is entered.
   - Challenge Password and Re-enter Challenge Password – enter an arbitrary password.
   - Leave the other fields at the defaults.

3. In the Server Certificate Manual Enrollment Request page , copy the entire contents of the Certificate Request PEM textbox into the Windows clipboard, and past it into a text file <filename>

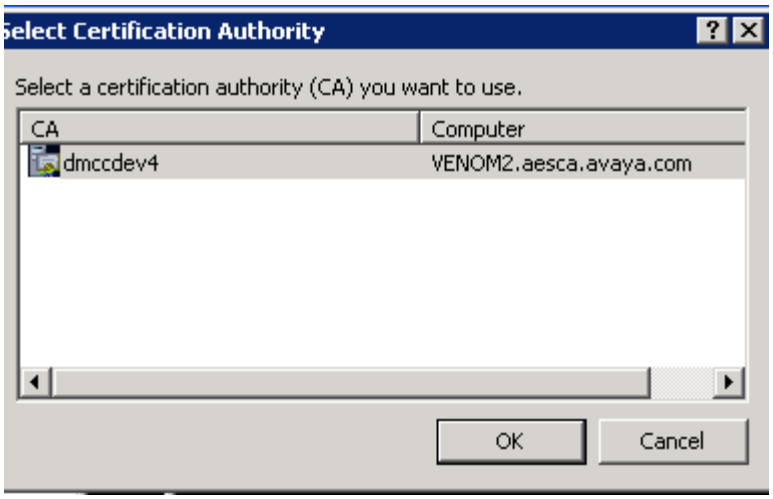


4. Copy the file created on the step 2.3 to Windows 2008 Enterprise CA server.
5. On the Windows 2008 Enterprise CA server, Click Start->Run, on Run dialog box, type “cmd” on the Open field, then click OK.
6. On the Command Prompt console, type
   certreq -attrib "CertificateTemplate:<template name created on step 1>", then press Enter.

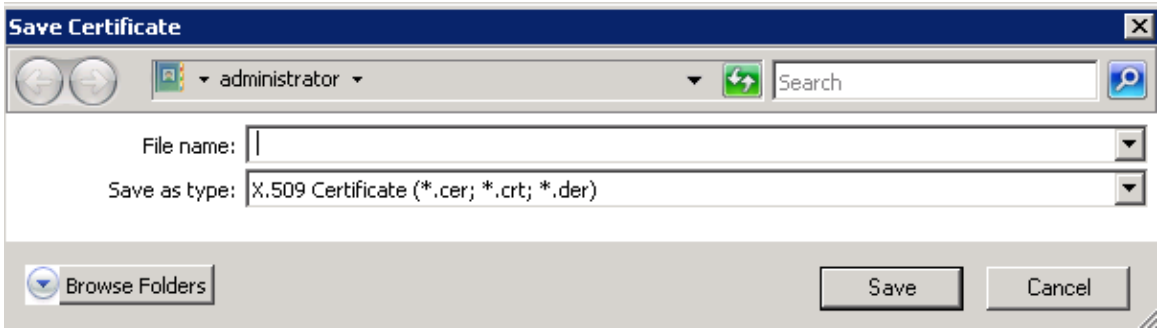
7. On the Open Request File dialog box, select the file created on step 2.4.



8. A window will appear where you can select the CA that will issue the certificate. Select the issuing CA and click **OK**.

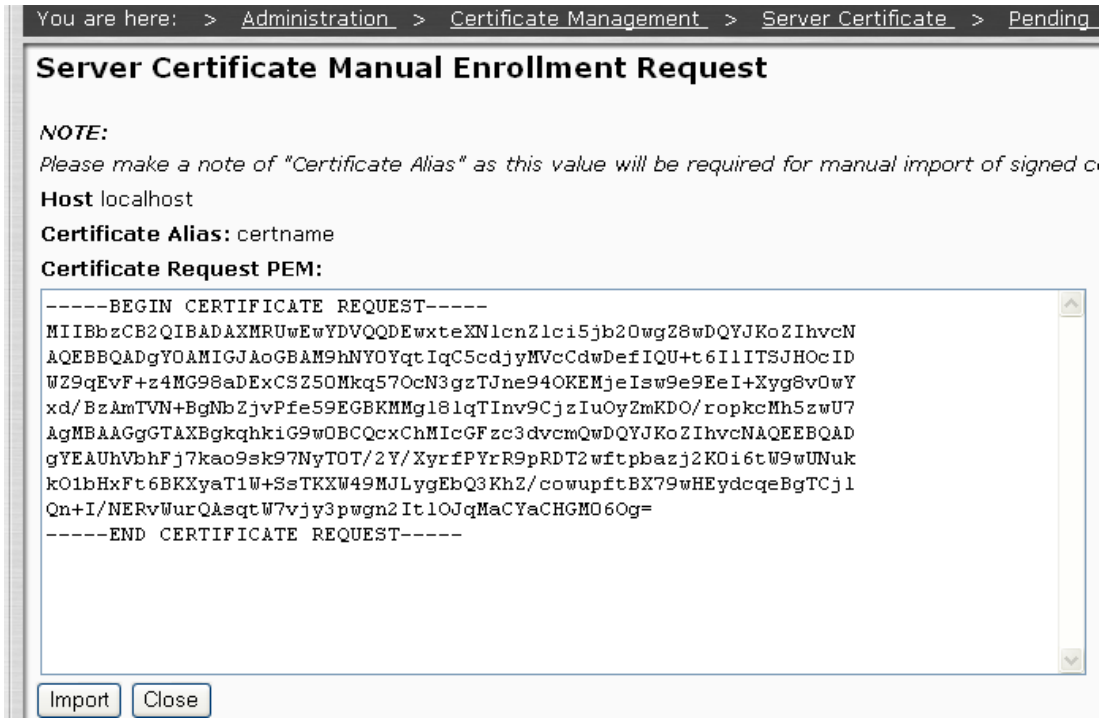


9. On the Save Certificate window, enter the output file name.

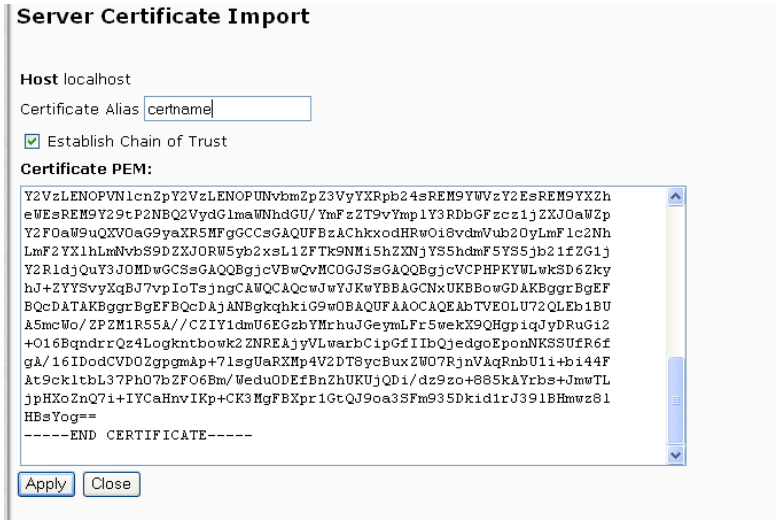


10. Copy the created file on your local machine.
11. In the left pane of the Avaya AE Services OAM Web Interface, select **CTI OAM Home** >**Administration** > **Certificate Management** > **Server Certificate** > **Pending Requests**. In the Pending Server Certificate Requests page, select the **Alias** for the certificate request created in Steps 1 – 3 and click **Manual Enroll**.

12. In the Server Certificate Manual Enrollment Request page, click **Import**.



13. In the Server Certificate Import page, enter the same Certificate Alias, ensure that the 'Establish Chain of Trust' checkbox is checked, paste the copied contents from Step10 into the Certificate PEM textbox, and click **Apply**. If the import is successful, the message "Certificate imported successfully" is displayed on the Server Certificate Import page.



To Install a Microsoft Certificate Services-based certificate on the Microsoft LCS 2005 or OCS 2007:

Please use Chapter 3 of the AE Services Implementation Guide for Microsoft LCS 2005 or OCS 2007 Issue 5 - December 2007
http://support.avaya.com/elmodocs2/AES/4.1/02-601893_i5.pdf

Workaround or alternative remediation

Version 2 certificate templates can be used for the web enrollment procedure.

Remarks

n/a

Patch Notes

The information in this section concerns the patch, if any, recommended in the Resolution above.

Backup before applying the patch

n/a

Download

n/a

Patch install instructions

Service-interrupting?

n/a

No

Verification

n/a

Failure

n/a

Patch uninstall instructions

n/a

Security Notes

The information in this section concerns the security risk, if any, represented by the topic of this PSN.

Security risks

n/a

Avaya Security Vulnerability Classification

Not Susceptible

Mitigation

n/a

For additional support, contact your Authorized Service Provider. Depending on your coverage entitlements, additional support may incur charges. Support is provided per your warranty or service contract terms unless otherwise specified.

Avaya Support Contact	Telephone
U.S. Remote Technical Services – Enterprise	800-242-2121
U.S. Remote Technical Services – Small Medium Enterprise	800-628-2888
U.S. Remote Technical Services – BusinessPartners for Enterprise Product	877-295-0099
BusinessPartners for Small Medium Product	Please contact your distributor.
Canada	800-387-4268
Caribbean and Latin America	786-331-0860
Europe, Middle East, and Africa	36-1238-8334
Asia Pacific	65-6872-8686