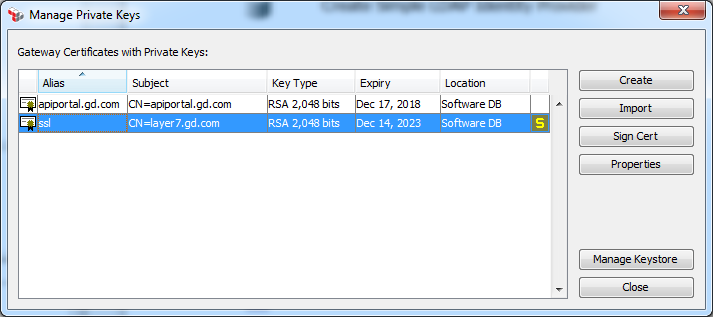
## Securing Communication Between CA Identity Manager and CA API Gateway for SCIM provisioning calls

***NOTE:*** *This procedure is for the CA Identity Manager administrator. If CA IM CS already has the CA API Gateway certificate, please do not import again*.

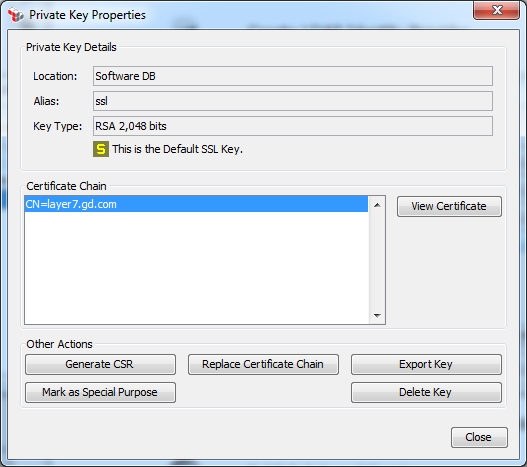
*Only import the CA API Gateway certificate into the CA Identity Manager Connector Server keystore after the CA API Gateway administrator has confirmed that the gateway is configured to use SSL*.

**Follow these steps to import the CA API Gateway Certificate into CA Identity Manager Connector Server:**

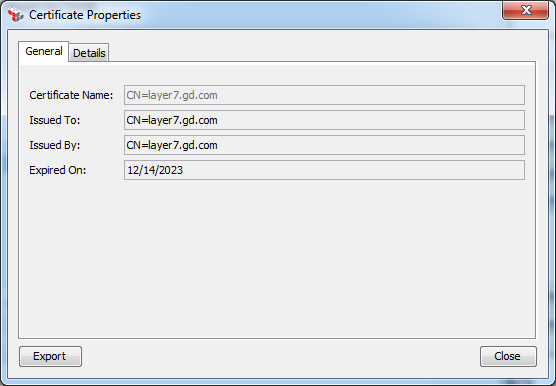
1. Export certificates from CA API Gateway:
2. Login CA API Gateway Policy Manager
3. Select menu **Tasks | Manage Private Keys**
4. Select the certificate **ssl** and click the **Properties** button

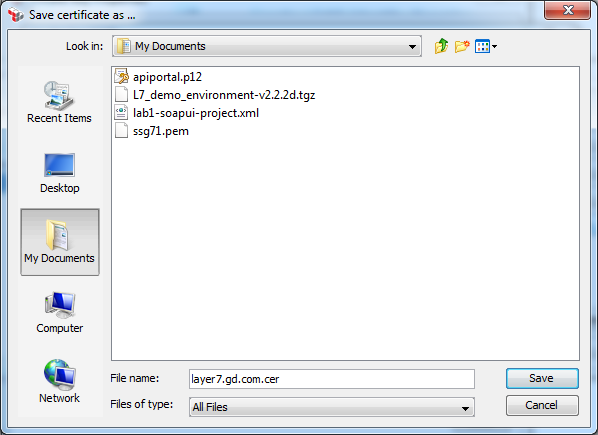


1. Highlight the certificate in the Certificate Chain list and click the **View** **Certificate** button.



1. Click the **Export** button to export the certificate to a file





1. Log in to CA IM CS Management Console.
2. At the top, click the **Certificates** tab.

*This tab lists all the certificates in the CA Identity Manager Connector Server keystore. To filter the list of certificates by their names, user the Certificate Filter box.*

1. To add a certificate, click **Add**, then enter the details of the certificate.

Add a certificate:

■ **Certificate**—Enter the path to the certificate file

■ **Alias**—Enter an alias for storing the certificate

1. Repeat step 4 for each certificate to be added to CA IM CS.

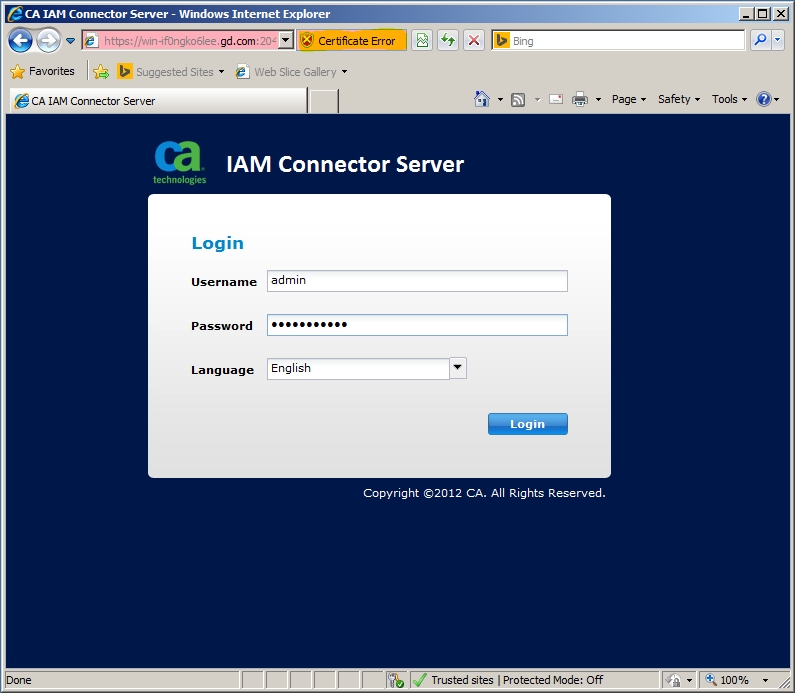
For detailed information about configuring HTTPS, see the help in the CA API Gateway Administration Guide and CA Identity Manager Administration Guide.

## Configuring CA API Gateway Client Certificate Authentication

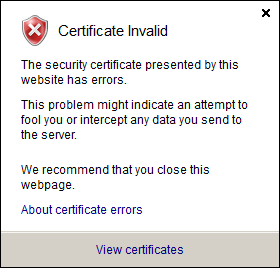
This section includes the steps to configure HTTPS client certificate authentication for accessing CA API Gateway from CA Identity Manager Connector Server.

1. Locate the CA Certificate for CA Identity Manager Connector Server from the Connector Server console:

1. Using Internet Explorer, access the Connector Server console at https://<connector\_server\_host>:20443/main.
2. Advance through the security warnings.
3. Click **Certificate** or **Certificate Error** to the right of the address field



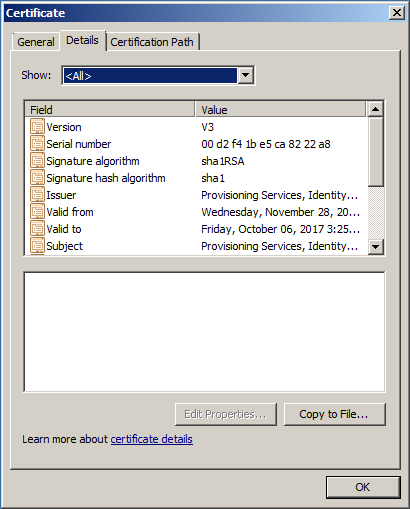
1. **View Certificate**.



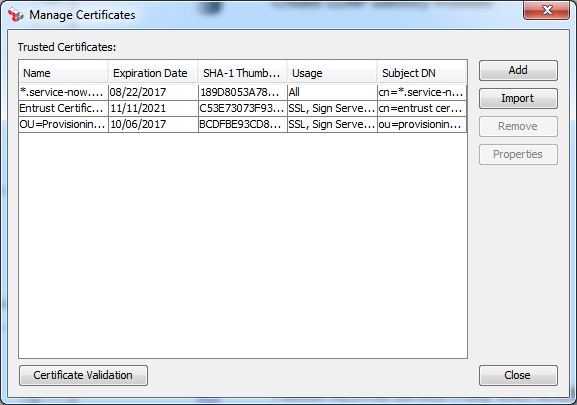
1. From the Certificate dialog, select the tab **Certification Path**. Select **Provisioning Services**, and click **View Certificate**.



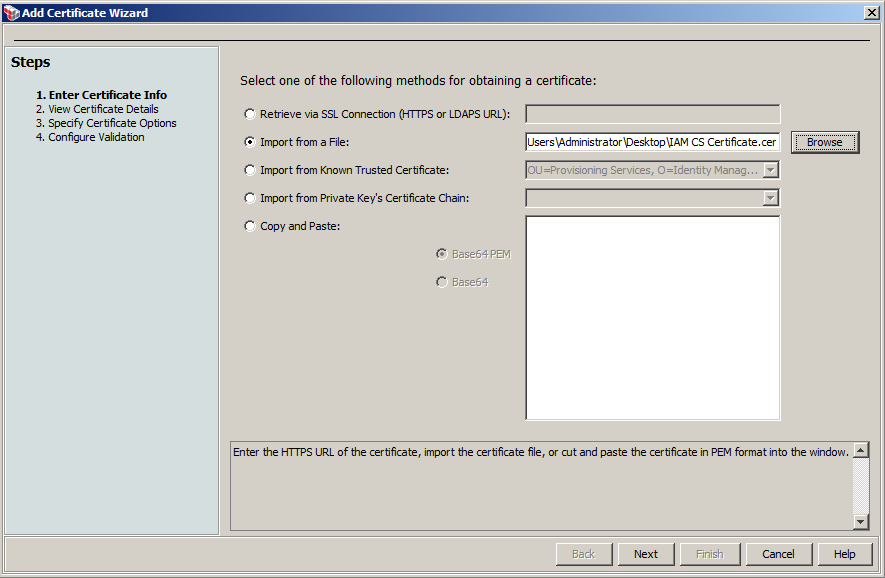
1. Click the **Details** tab, select **Copy to File**, and save the CA Certificate of CA Identity Manager Connector Server in **DER encoded binary X.509 (>CER)** format.



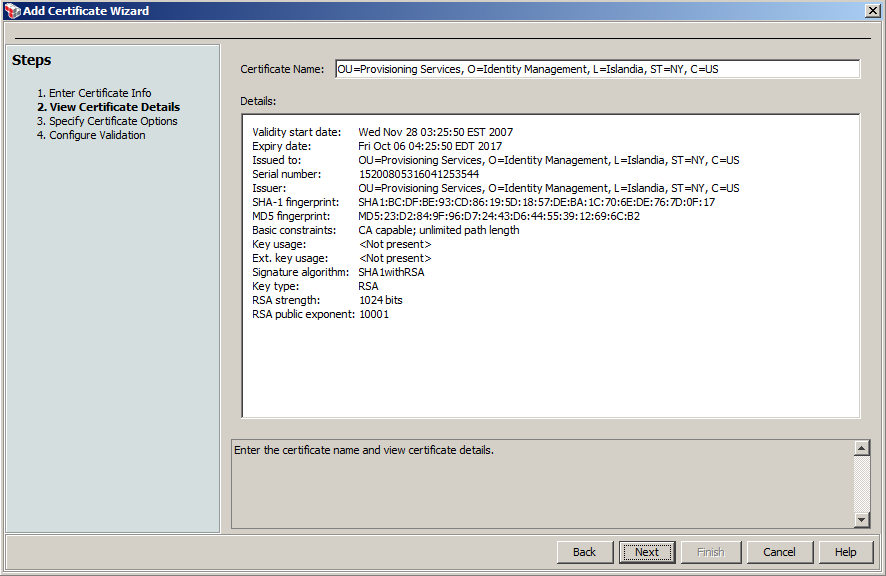
1. In CA API Gateway Policy Manager, select **Tasks | Manage Certificates** and click the **Add** button.



1. Import the CA certificate file that was exported from the CA Identity Manager Connector Server



1. Click the **Next** button and verify the certificate information

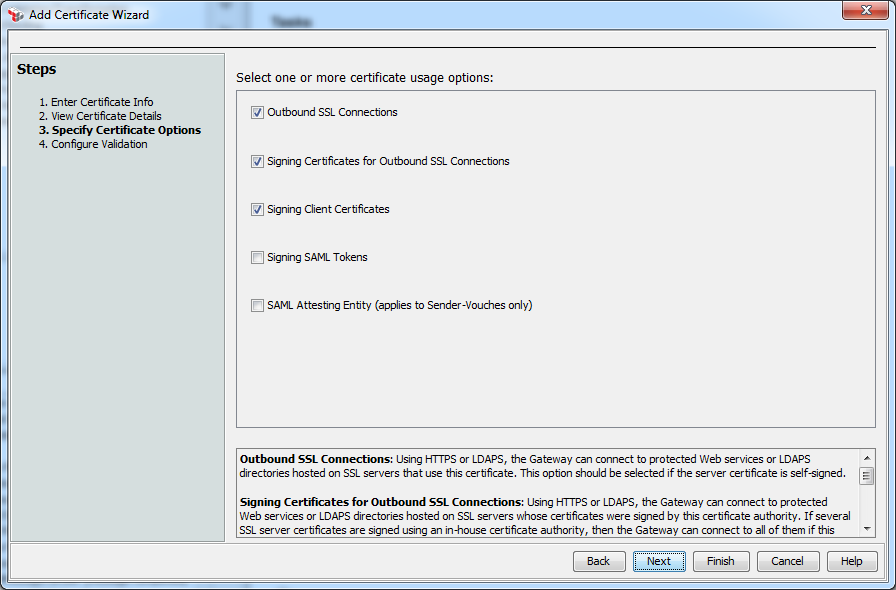


1. Click the **Next** button and select the following options:

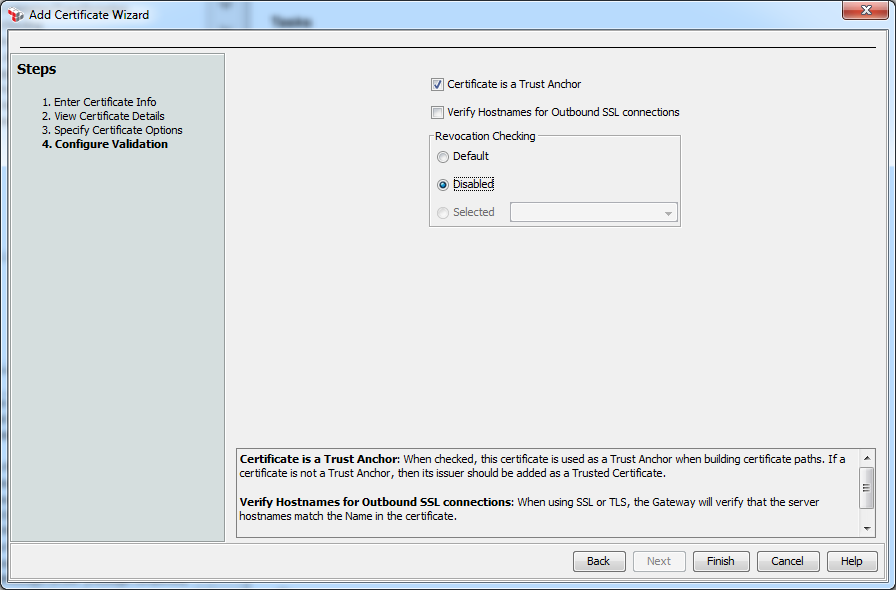
■ Outbound SSL Connections

■ Signing Certificates for Outbound SSL Connections

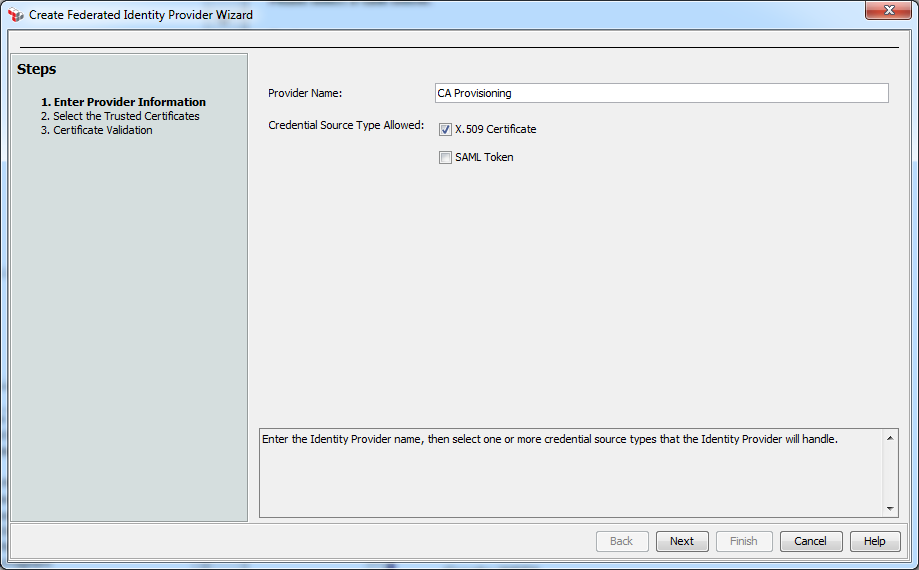
■ Signing Client Certificates



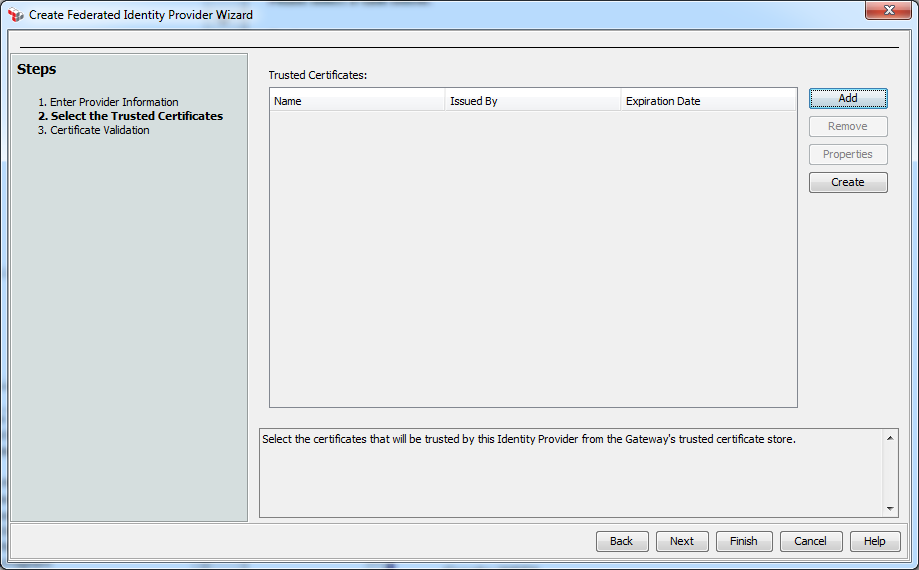
1. Click the **Next** button and select **Certificate is a Trust Anchor** and set **Revocation Checking** as **Disabled**.



1. Click the **Finish**.
2. Select menu **Tasks | Create Identity Provider | Create Federated Identity Provider**; Specify the name of the identity provider and set the **Credential Source Type Allowed** to **X.509 Certificate**

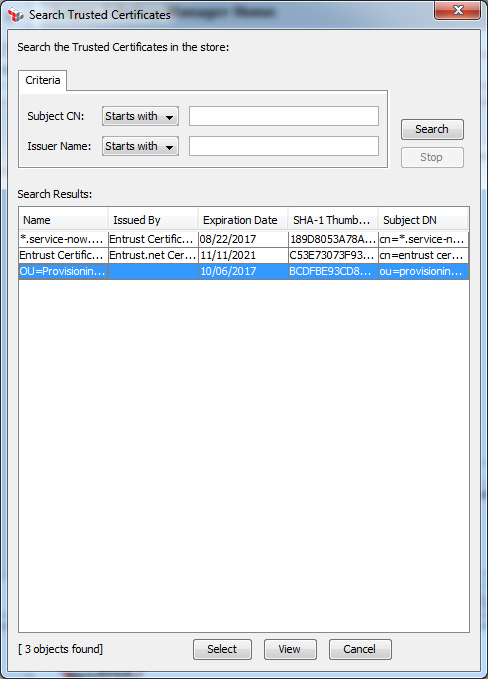


1. Click the **Next** button and then the **Add** button.

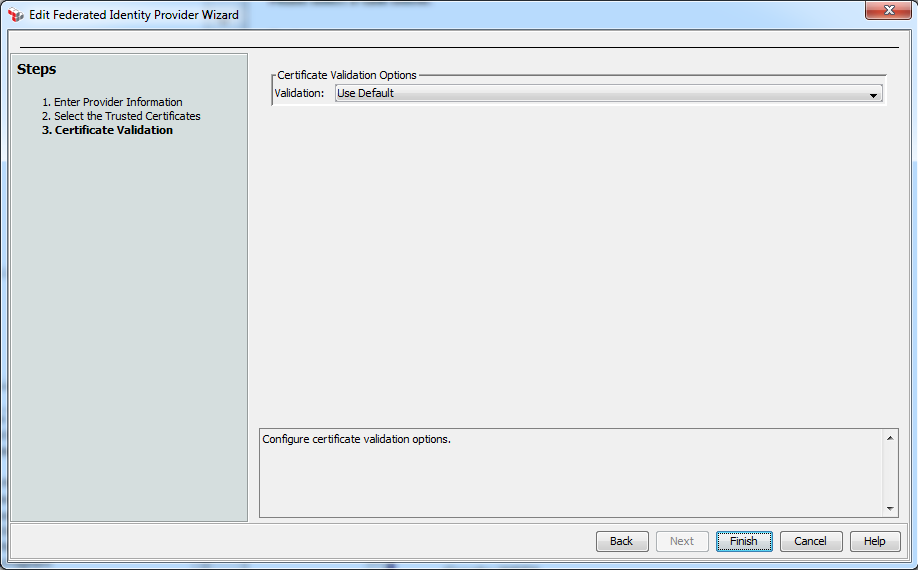


1. **Search** and **Select** the CA Identity Manager Connector Server certificate as a Trusted Certificate of the Identity Provider.

OU=Provisioning Services,O=Identity Management,L=Islandia,ST=NY,C=US

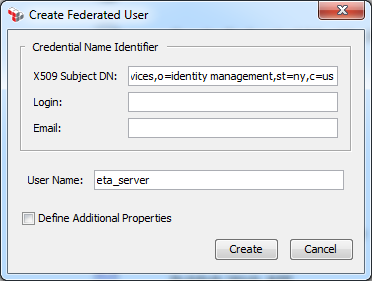


1. Click the **Next** button; keep the default settings then **Finish**.



1. Right click the Identity Provider just created and select the **Create User** in the context menu. Create a user with the following DN:

cn=eta\_server,ou=provisioning services,o=identity management,st=ny,c=us



SSL Client Certificate Authentication is now configured.

## Securing Communication between CA API Gateway Client and the Endpoint

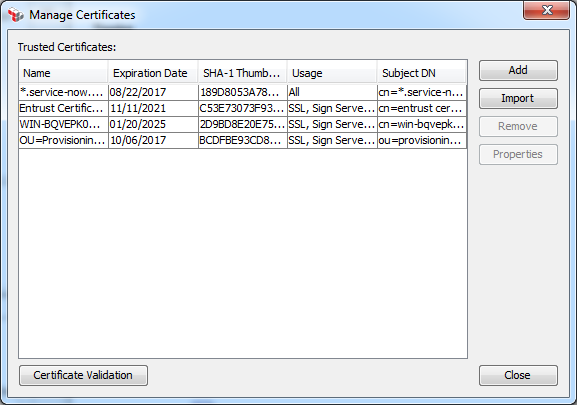
Sensitive information travels between the CA API Gateway and the endpoint. We recommend securing the communication channel between these components.

The endpoint may require additional configuration to enable HTTPS. Please contact the administrator of the endpoint about SSL communication and configure the CA API Gateway to trust the endpoint SSL certificate.

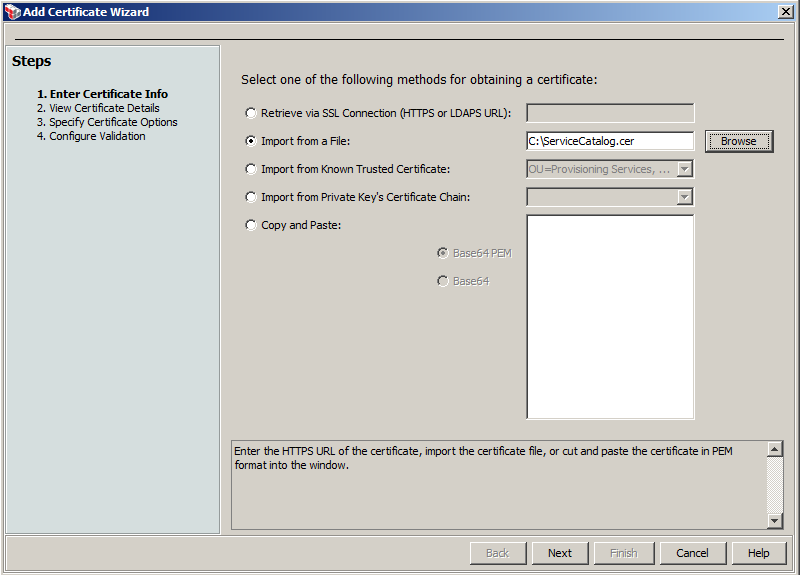
**Add the Endpoint SSL Certificate to the CA API Gateway Server**

Normally, the CA certificate used by the endpoint instance needs to be added to the CA API Gateway Server as a trusted anchor. For information on adding the server certificate as a trust anchor, please see the Help in the CA API Gateway Policy Manager. The following steps demonstrate the import of an SSL certificate into CA API Gateway Server.

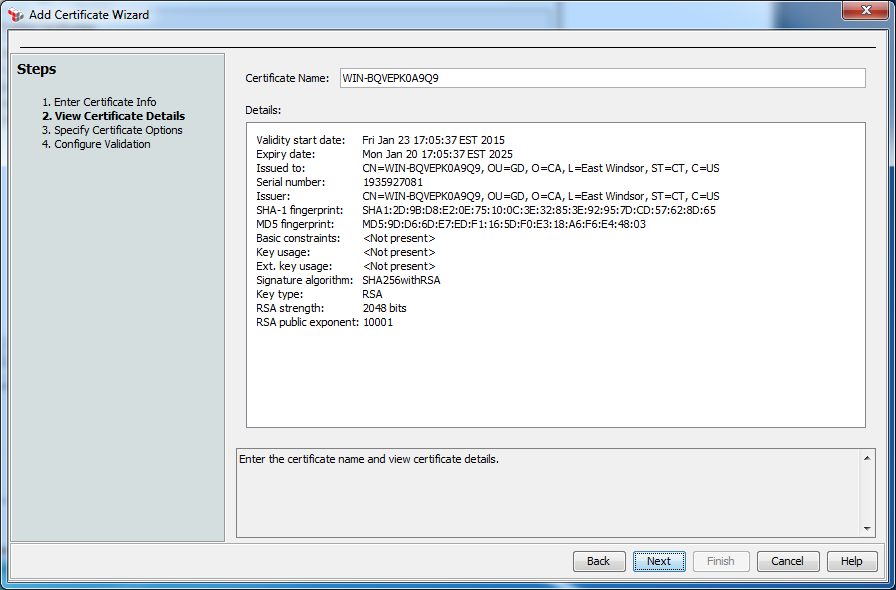
1. Login CA API Gateway Policy Manager
2. Select menu Tasks | Manage Certificates, and click the Add button



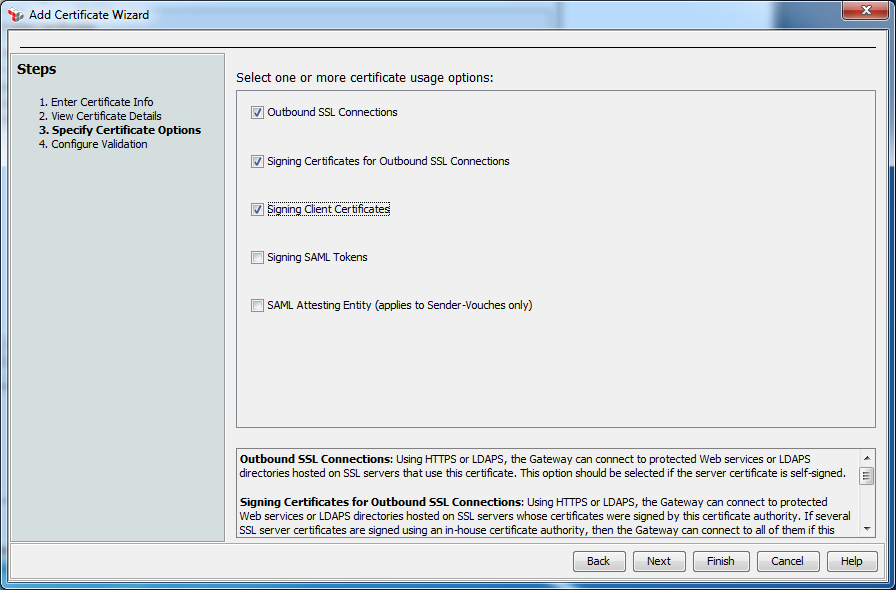
1. Import the certificate file and click the Next button



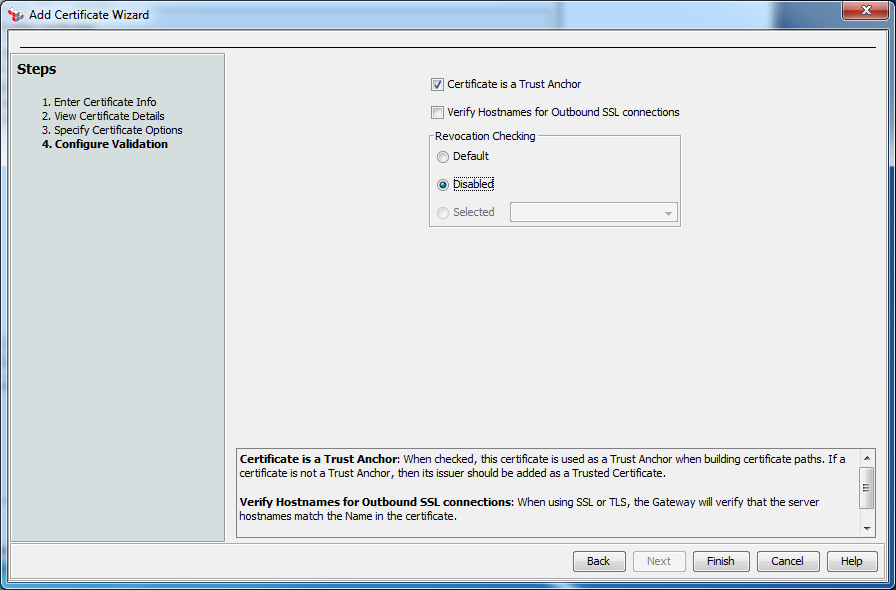
1. Review the certificate details and click the Next button



1. Select at least the Outbound SSL Connections option and click the Next button



1. Select Certificate is a Trust Anchor and Disable Revocation Checking and click the Finish button



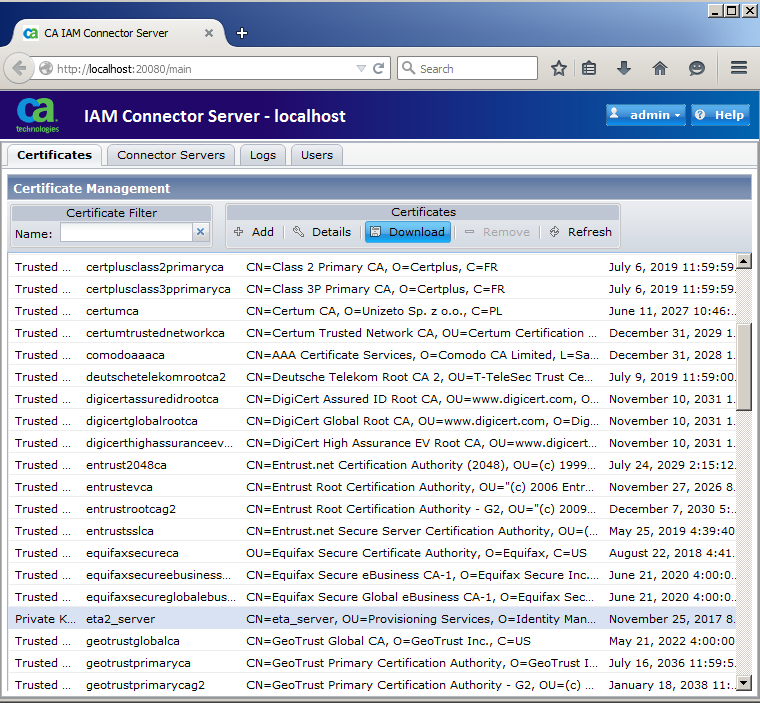
The SSL connection between the CA API Gateway and the endpoint is now enabled.

## Securing Communication between CA API Gateway Client and Connector Xpress

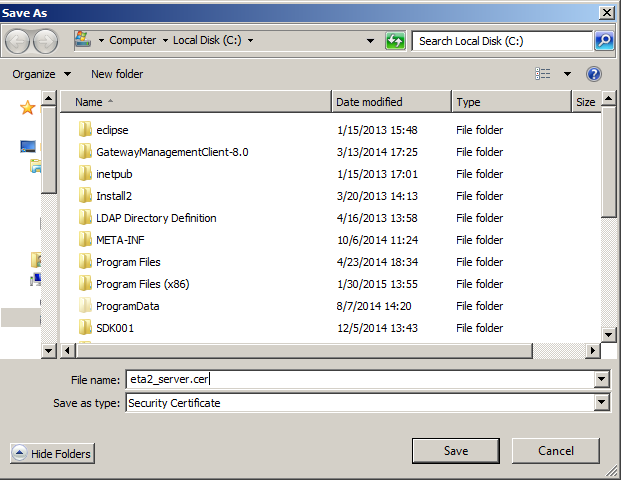
1. Login to the CA Identity Manager Connector Server.



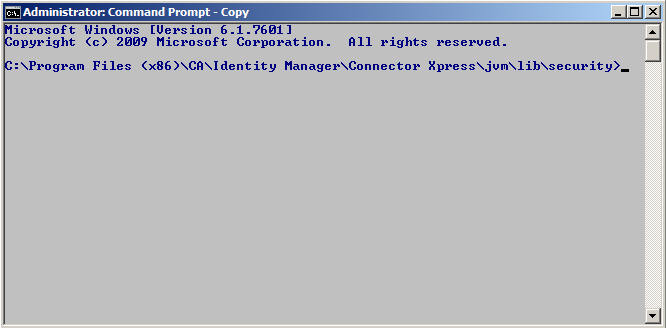
1. Select the ‘Certificates’ tab, scroll down and highlight the ‘eta2\_server’ private key, and click the ‘Download’ button.



1. Save the certificate to a convenient location and exit Connector Server.

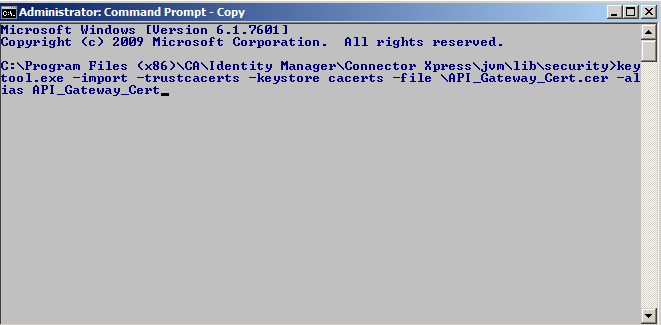


1. Locate the CA API Gateway certificate exported previously.
2. Open a Command Prompt window and navigate to the installed Connector Xpress directory. Navigate further to the ‘jvm\lib\security’ directory, E.g., “Program Files (x86)\CA\Identity Manager\Connector Xpress\jvm\lib\security”.

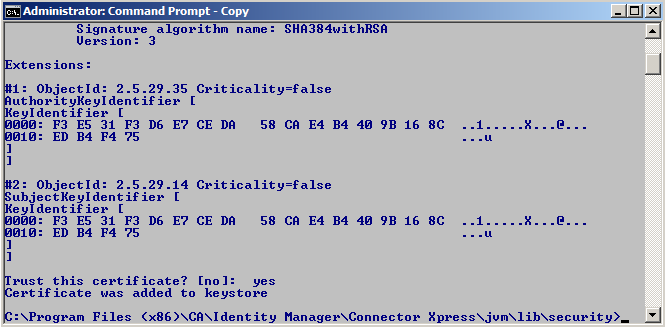


1. Import the CA API Gateway certificate into Connector Xpress using the Java keytool utility as follows:

keytool.exe -import -trustcacerts -keystore cacerts -file \API\_Gateway\_Cert.cer -alias API\_Gateway\_Cert

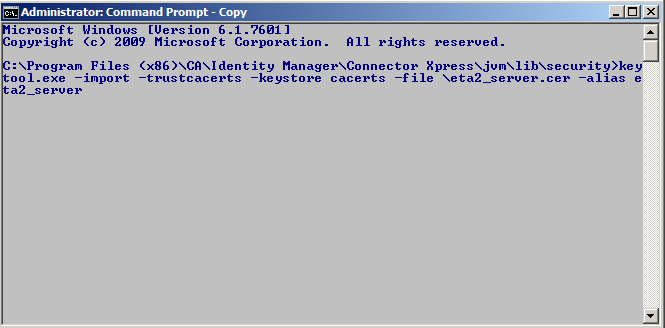


1. Enter ‘yes’ when asked whether to trust this certificate.



1. Now import the ‘eta2\_server’ certificate just exported from CA Identity Manager Connector Server as follows:

keytool.exe -import -trustcacerts -keystore cacerts -file \eta2\_server.cer -alias eta2\_server



1. Again, enter ‘yes’ when asked whether to trust this certificate.

