1. **A new Client Cert will need to be issued against your CA**
   1. Run mmc.exe on my PC
   2. Press Ctrl + M OR File -> Add/Remove Snap-in…
   3. Click Certificates -> Add
   4. My user account -> Finish
   5. Ok

Machine generated alternative text:



1. Expand Certificates – Current User -> Personal -> Certificates
   1. IF Certificates does not exist under Personal just move on to step **vii.**
2. Right-Click on Certificates -> All Tasks -> Request new Certificate…

Machine generated alternative text:



1. Click Next -> Next
2. You should have an option for User, select that then click Enroll
3. If you don’t see that option you will need to talk to you PKI team and have them publish that template for use.

Machine generated alternative text:



1. Now Double-Click on the new cert that was installed in your cert store
2. You will need to record the Thumbprint and Serial Number for later use
3. If there are spaces in either string please remove them

Machine generated alternative text:



1. Now we need to export that cert out to install it on the CCP server
2. Right-click on the new cert click All Tasks -> Export…

Machine generated alternative text:



1. Click Next -> Yes, export the private key -> Next

Machine generated alternative text:



1. Select PKCS #12
2. Check Include all certificates in the certification path if possible
3. Check Export all extended properties -> Next

Machine generated alternative text:



1. Check Password then type in a password -> Next

Machine generated alternative text:



1. Click Browse then choose a path to save the .pfx to -> Next

Machine generated alternative text:



1. Click Finish
2. **Now we are ready to install the new cert on your CCP server**
   1. Copy the .pfx file you exported to your CCP server and import it to the local cert store
   2. Please follow step **1i** from the beginning of these instructions to create the MMC console. When you get to sub-step **iii** come back and follow the below instructions
      1. Select Computer account -> Next -> Select Local computer -> Finish
      2. Expand Personal > Certificates
      3. Right-click on Certificates -> All Tasks > Import

Machine generated alternative text:



1. Next -> Browse
2. Browse and select the .pfx you copied to this server. You will have to change the file name filter on the Open File Dialog
3. Next -> Type the password you set when you exported the cert -> Next -> Next -> Finish
4. **Now we are ready to configure IIS**
   1. Install the *IIS Client Certificate Mapping Authentication* Role on your CCP server
   2. Add Roles and Features
   3. Server Roles -> Web Server (IIS) -> Web Server -> Security, and then select IIS Client Certificate Mapping Authentication -> Next -> Next -> Install
      1. In IIS select the **AIMWebService** then double click the **Configuration Editor**

Machine generated alternative text:



1. Select *system.webServer/security/authentication/iisClientCertificateMappingAuthentication*

Machine generated alternative text:



1. In the Configuration Editor set enabled = True then click the ellipsis button on the **manyToOneMappings** line.

Machine generated alternative text:



1. Now click **Add**
2. Fill in **description** and **name**. These can be arbitrary values.
3. Click the ellipsis button on the **rules** line

Machine generated alternative text:



1. Click **Add**
2. Fill in the fields as below

Machine generated alternative text:



1. Close those screens back to Configuration Editor in IIS
   1. Now **Apply** those changes then click on the **AIMWebService** again
   2. Double click on **Authentication**
2. Validate **Anonymous Authentication = Enabled**
   1. Click on **AIMWebService**
   2. Double click on **SSL Settings**
3. For Cert Auth ONLY, check **Require SSL** and select **Require** -> Apply
4. For Cert Auth OR Machine Identity Auth, select **Accept** -> Apply
5. Apply the correct permissions to the safe for the AppID and add the Certificate Serial Number to the application authentication section