CSR Creation for Cisco Mobility Server

How to create a CSR for a Cisco Unified Mobility Server

For those who may not be familiar with SSL certificate management using an SSL keystore file, Cisco Unified Mobility Servers have a built in interface to help guide you through your CSR creation process.

During the initial server configuration you may have created a self signed certificate. These instructions aim not at creating a self signed certificate, but a fully functional, CA signed ssl certificate.

Create your Keystore/CSR

1. From the Cisco Unified Mobility Advantage Admin Portal, choose the "SSL Certificate Management" option, and then "Generate New Certificate".
2. Enter the requested information into the provided fields:

   Server Name: Also known as your **common name**, this is usually the fully qualified domain name through which your server will be accessed externally (e.g., www.yourdomain.com or *.yourdomain.com).
   Department Name: The name of your department within your organization. If this is not applicable, go ahead and enter the organization name twice.
   Company Name: The full legal name of your organization. For example, if your organization is named *Example Company Name Limited*, but goes by *Example*, enter *Example Company Name Limited*.
   City: Usually the main office of your organization. The city does not need to be the city where you or your server is located.
   State: Usually the location of your organization's main office. Once again, this does not need to have a bearing on your current location or the location of your server.
   Country Code: If this is not familiar to you, you can find you country codes here.
   Password: You will need your password to modify your keystore later. This password should be a minimum of six characters in length.
   Click the button to "Submit".

3. A screen should appear with a link to download your keystore file. You can name the keystore anything you like, give it a .keystore extension.
4. If there is also a link to download your CSR, download and save that file now. Otherwise, go back under "SSL Certificate Management" and choose to "Retrieve CSR".

   You will have to select the keystore file that was just created, enter your password, and then click "Submit".

   A CSR will usually be saved as a .csr or .txt file.

5. The entire body of your CSR file will need to save it to text file and submit to us.
   Please make sure to fill in Java as the server type in the application form.

Importing Your Signed SSL Certificate Files to The Keystore

1. Log onto your Admin Portal and select "SSL Certificate Management".
2. Choose the option to "Import SSL Certificate".

   Browse to the keystore file created during the CSR creation process. In the password field, enter the password you created when creating the keystore file.

   For Intermediate Certificate, choose false. Then, paste in the entire body of the your_domain_name.p7b file that you will have received.

   If you did not receive a .p7b format file, you may need to reissue your certificate, making sure to choose Java as your server type.

3. Click "Submit", then download the final SSL certificate keystore file. You can name the file anything you choose, such as mykey.keystore.

   Your keystore is now ready for use.

Enabling your SSL Certificate in the Cisco Unified Mobility Advantage Admin Portal

1. Log into the Admin Portal and select "SSL Certificate Management".
2. Choose the option to "Upload Certificate", browse to your newly created keystore, and enter the same password that you used when creating the keystore to enable the certificate for use by your server.
3. Go to Server Controls > Cisco > Control Server, and then stop and start your Managed Server.

   Your server should now be configured to use your newly created keystore and certificate files.

Your certificate file can be exported for use with other Cisco devices using keystores, including any applicable proxy servers.