# Certificate Enrollment Steps

The following document helps step you through the video entitled: “Managing Mobile Devices, Plan and Configure Security” To learn specific details about certification authorities, view my 70-412 series.

### Step 1: Create a Configuration Manager Web Server certificate template

1. In the Certification Authority console, select Certificate Templates.
2. Right-click the Certificate Templates folder, and click Manage.
3. Right-click Web Server, and click Duplicate Template.
4. On the Compatibility tab, ensure that the Windows Server 2003 option is selected.
5. On the General tab, type a name for the certificate template.
6. On the Subject Name tab, ensure that the Supply in the request option is selected.
7. On the Security tab, clear Enroll permissions for Domain Admins and Enterprise Admins. Then, add the Configuration Manager computer account or group to which it belongs. Give it the Read and Enroll permissions.

### Step 2: Create a Configuration Manager client certificate template

1. In the Certificate Templates console, right-click Workstation Authentication, and then Duplicate Template.
2. On the Compatibility tab, ensure that the Windows Server 2003 option is selected.
3. On the General tab, type a name for the certificate template.
4. On the Security tab, select Read, Enroll, and Autoenroll permissions for Domain Computers.

### Step 3: Create a Configuration Manager client distribution point certificate template

1. In the Certificate Templates console, duplicate the Workstation Authentication template.
2. On the Compatibility tab, ensure that the Windows Server 2003 option is selected.
3. On the General tab, type a name for the certificate template.
4. On the Request Handling tab, select Allow private key to be exported.
5. On the Security tab, clear Enroll permissions for Domain Admins and Enterprise Admins.
6. On the Security tab, add the Read and Enroll permissions to the Configuration Manager computer or group to which it belongs.

### Step 4: Create a Configuration Manager mobile device client certificate template

1. In the Certificate Templates console, duplicate the Authenticated Session template.
2. On the Compatibility tab, ensure that the Windows Server 2003 option is selected.
3. On the General tab, type a name.
4. On the Subject Name tab, ensure that the Build from this Active Directory information option is selected.
5. In the Subject name format list, select Common name. Under Include this information in alternate subject name, clear the User principal name (UPN) check box
6. Close the Certificate Templates console.

### Step 5: Enable the Configuration Manager certificate templates

In the Certification Authority console, right-click the Certificate Templates folder and issue issue all the certificate templates you have created.

### Step 6: Create an autoenrollment GPO

1. On your domain controller in the Group Policy Management console, create a GPO linked to the domain.
2. Edit the policy under Computer Configuration, Policies, Windows Settings, Security Settings, then Public Key Policies.
3. Edit the properties of Certificate Services Client – Auto-Enrollment. In the Configuration Model list, select Enabled, select the Renew expired certificates, update pending certificates, and remove revoked certificates check box. Select the Update certificates that use certificate templates check box.

### Step 7: Request a Configuration Manager IIS certificate on the management point

1. Restart the Configuration Manager server (if you have added it to a new security group. This is so that it will generate a token with the new group membership.)
2. After restarting, log in and right click the Start menu. In the Run box, type MMC and press enter. Add a snap-in for Local Computer Certificates.
3. Expand Certificates (Local Computer), and then click Personal.
4. Request a web server Certificate based on the template you created in Step 1.
5. You will see a “More information is required to enroll for this certificate” link. Click the link.
6. On the Subject tab, in the Alternative name area, select DNS.
7. In the Value box, add the FQDN of your Configuration Manager server.
8. On the General tab, enter a friendly name such as Configuration Manager Web Services.
9. Enroll the certificate.

### Step 8: Request a Configuration Manager client distribution point certificate

1. Enroll another New Certificate based on the template you created in step 3.
2. Select the enrolled certificate and export it along with the private key.

### Step 9: Assign the Configuration Manager IIS certificate to Web Services

1. In Internet Information Services (IIS) Manager, edit the bindings for the Default Web Site.
2. In the SSL certificate list, select your new certificate created in Step 7

### Step 10: Configure HTTPS for the Configuration Manager roles

1. On the Configuration Manager server, go to the Administration workspace.
2. In the navigation pane, expand Site Configuration, and then click Servers and Site System Roles.
3. In the Site system Properties of the site system server, select Specify an FQDN for this site system for use on the Internet.
4. In the Internet FQDN text box, type the FQDN of your Configuration Manager server and click OK.
5. On the properties of the Distribution Point role, Import file, and then click Open. Select the certificate that you exported in Step 8.
6. On the General tab, click HTTPS and Allow intranet and Internet connections.
7. Click the Management point, and then click Properties.
8. On the General tab, click HTTPS, and then then select Allow intranet and Internet connections.
9. Select the Allow mobile devices to use this management point check box, and then click OK.

### Step 11: Deploy certificate profiles to clients

1. On the domain controller, export its certificate to a CRT file in a location accessible to the Configuration Manager server.
2. On the Configuration Manager server, copy the certificate to the desktop.
3. In the Assets and Compliance workspace, expand Compliance Settings, and then expand Company Resource Access.
4. Right-click Certificate Profiles and create a certificate profile.
5. Import the certificate of the domain controller that is on your desktop.
6. Deploy the certificate profile to All Systems or a collection of your choosing.