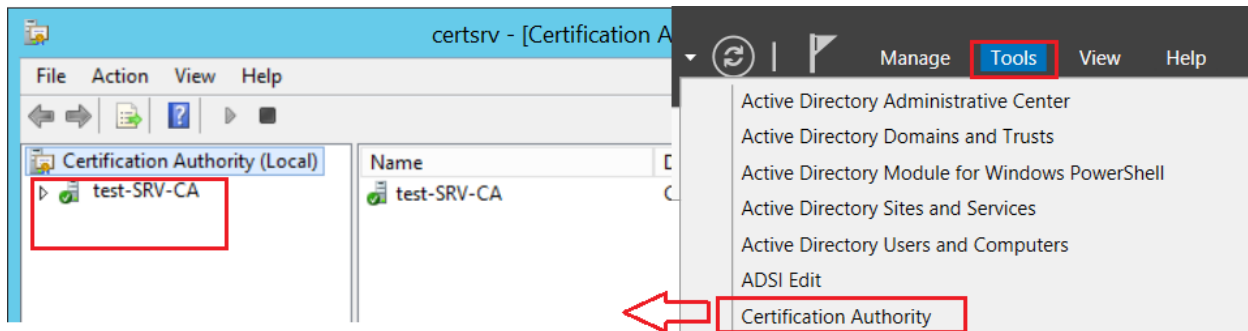
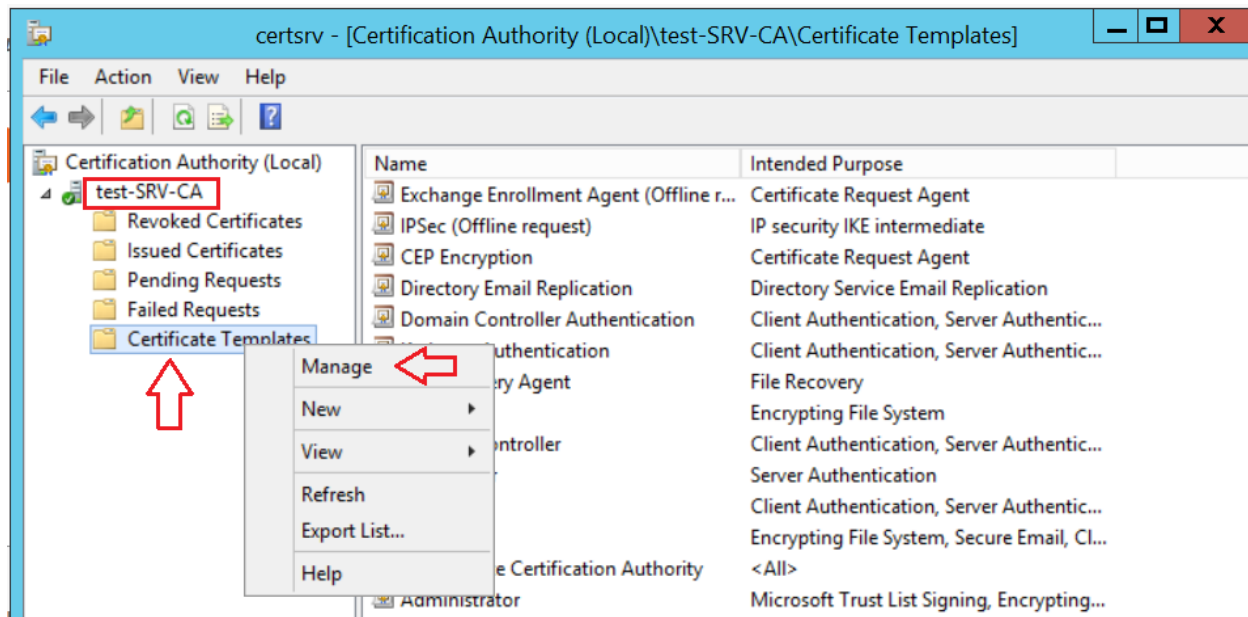


Create User Certificate Template:

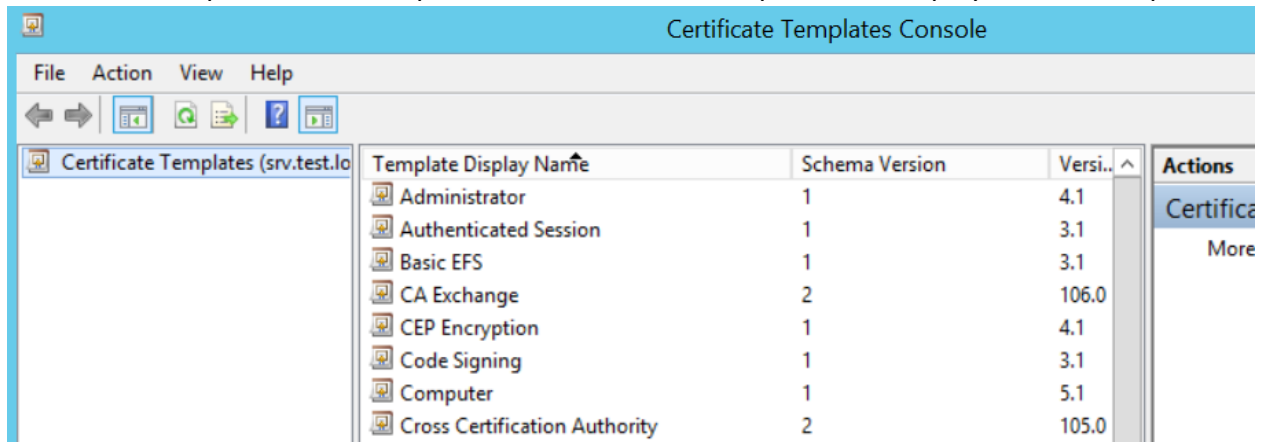
On CA, in **Server Manager**, click **Tools**, and then click **Certification Authority**. The Certification Authority Microsoft Management Console (MMC) opens.



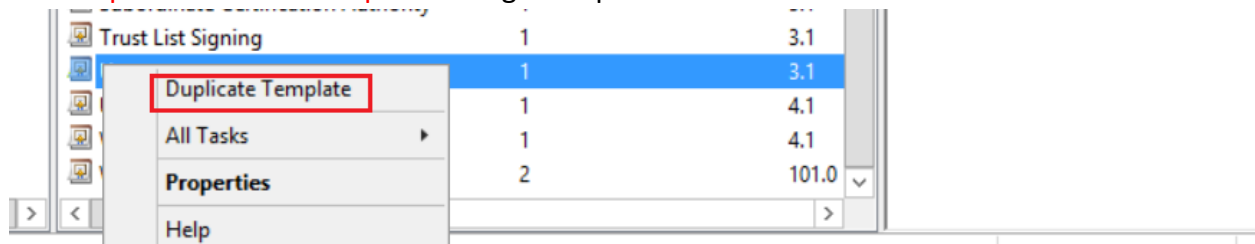
In the MMC, double-click the CA name, right-click **Certificate Templates**, and then click **Manage**.



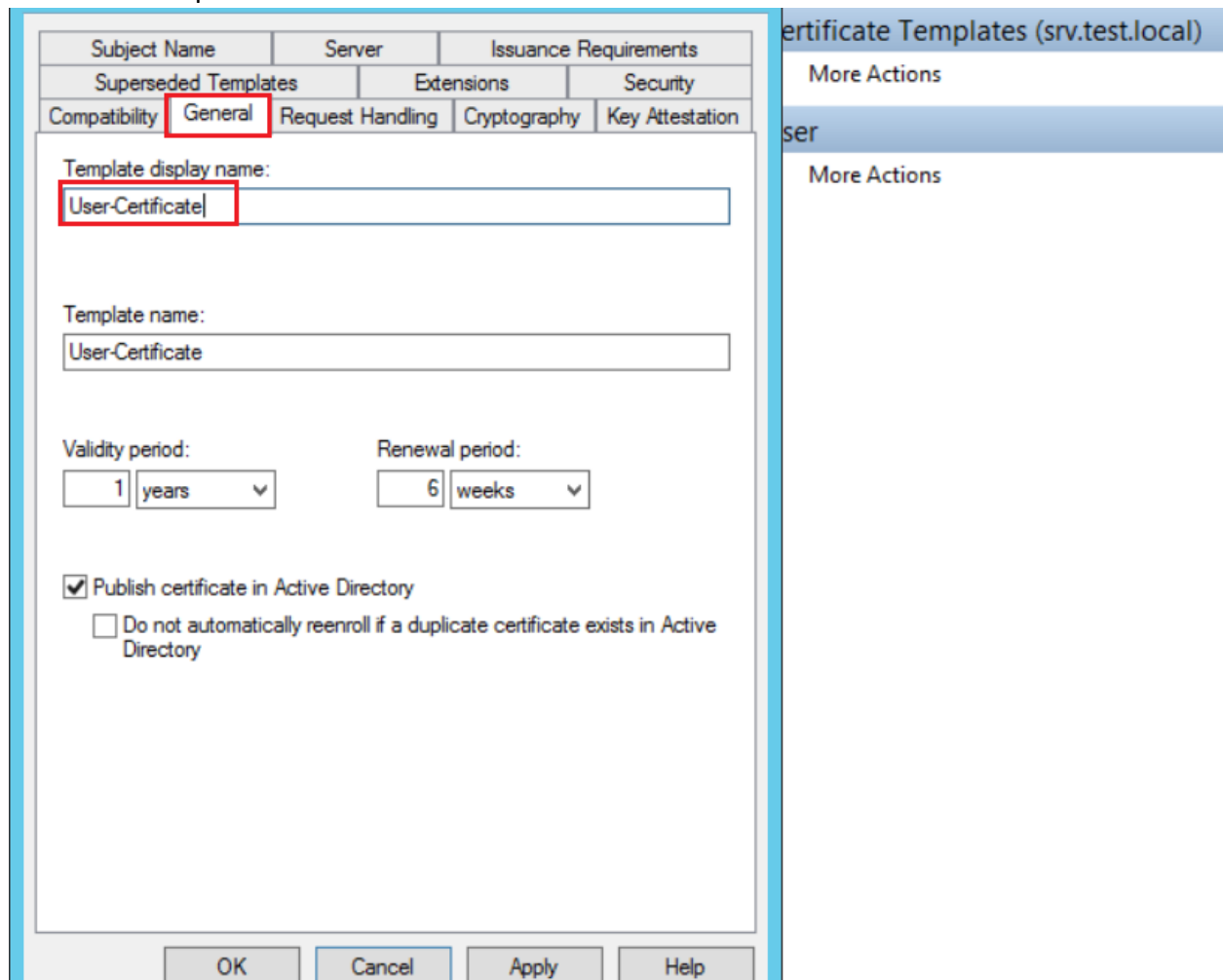
Certificate Templates console opens. All of certificate templates are displayed in details pane.



In the details pane, click the **User** template. On the **Action** menu, click **Duplicate Template**. The **Properties of New Template** dialog box opens.



In **Properties of New Template**, on the **General** tab, in **Display Name**, type a new name for the certificate template.



Click **Security** tab. In **Group or user names**, click **Domain Users**. In **Permissions for Domain Users**, under Allow, ensure that **Enroll** is selected, and then select **Read** and **Autoenroll** check boxes.

Subject Name	Server	Issuance Requirements
Compatibility	General	Request Handling
Cryptography	Key Attestation	
Superseded Templates	Extensions	Security

Group or user names:

- Authenticated Users
- Administrator
- Domain Admins (TEST\Domain Admins)
- Domain Users (TEST\Domain Users)**
- Enterprise Admins (TEST\Enterprise Admins)

Permissions for Domain Users

	Allow	Deny
Full Control	<input type="checkbox"/>	<input type="checkbox"/>
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Write	<input type="checkbox"/>	<input type="checkbox"/>
Enroll	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Autoenroll	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Click the **Subject Name** Tab. Ensure that **Build from this Active Directory** information is selected. Also ensure that **Subject name format** has the value of **Fully distinguished name**. In **Include this information in alternate subject name**, ensure that **User principal name (UPN)** is selected.

Compatibility	General	Request Handling	Cryptography	Key Attestation
Superseded Templates	Extensions	Security		
Subject Name	Server	Issuance Requirements		

☐ Supply in the request

☐ Use subject information from existing certificates for autoenrollment renewal requests (*)

☒ Build from this Active Directory information

Select this option to enforce consistency among subject names and to simplify certificate administration.

Subject name format:

Fully distinguished name

☐ Include e-mail name in subject name

Include this information in alternate subject name:

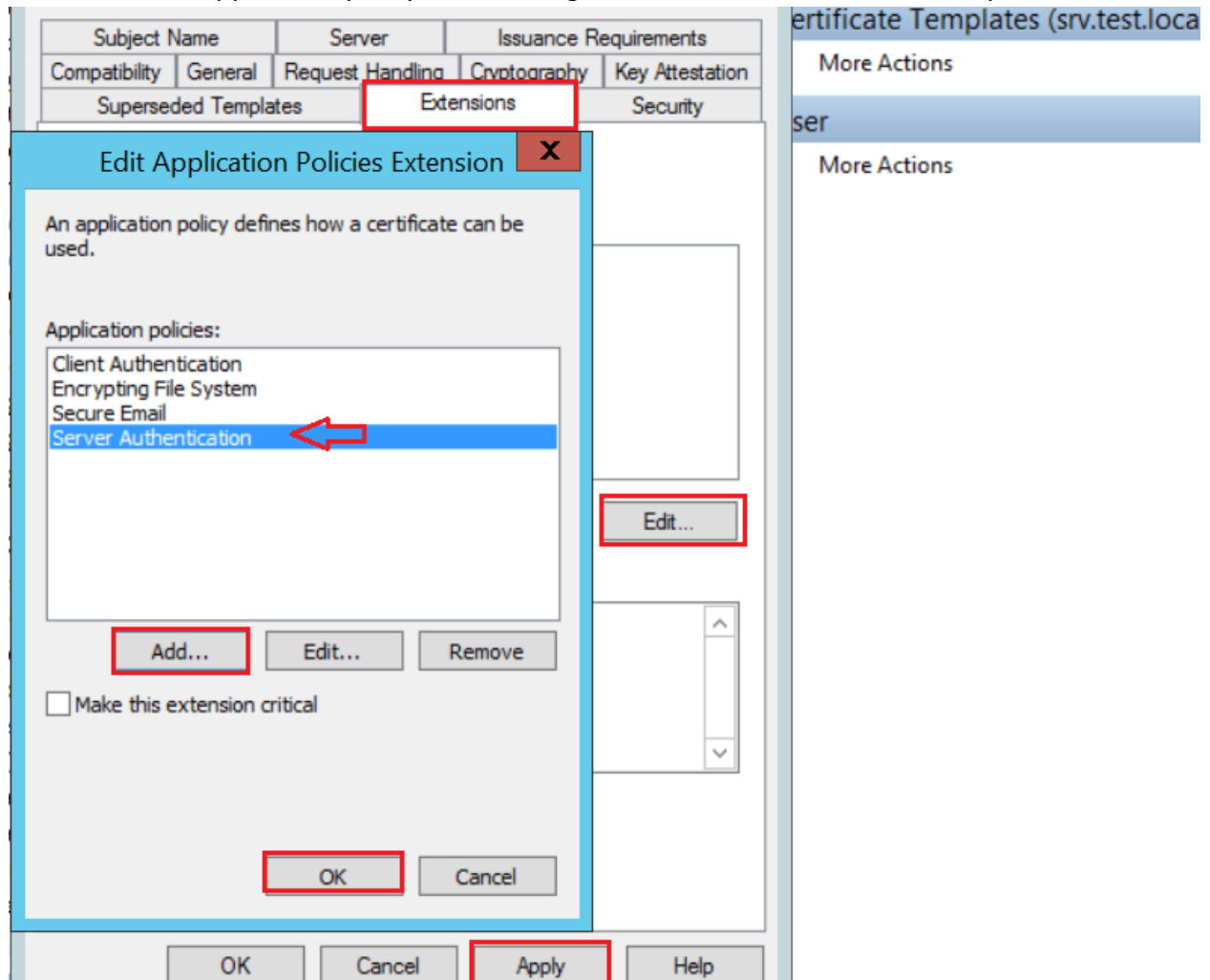
☐ E-mail name

☐ DNS name

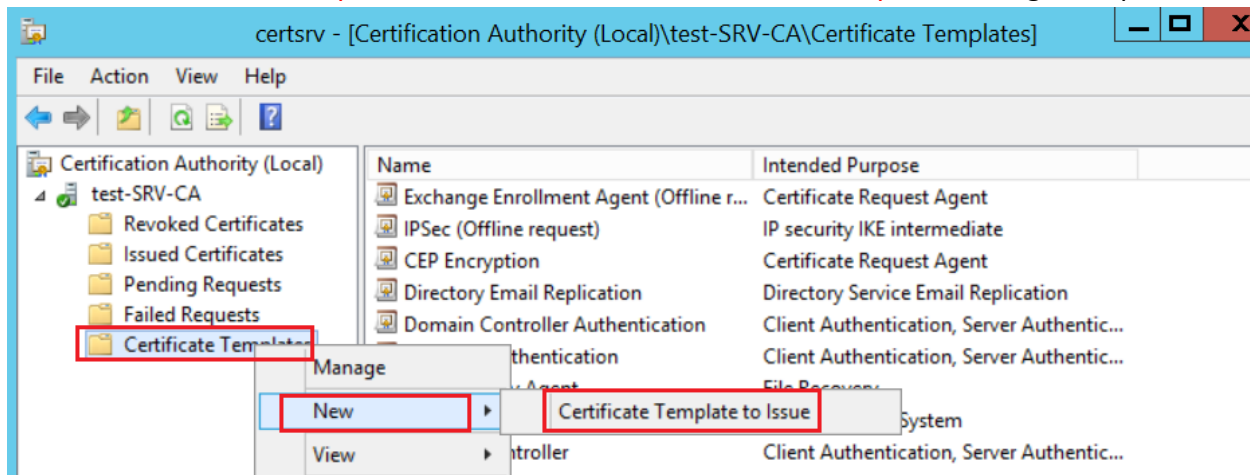
☒ User principal name (UPN)

☐ Service principal name (SPN)

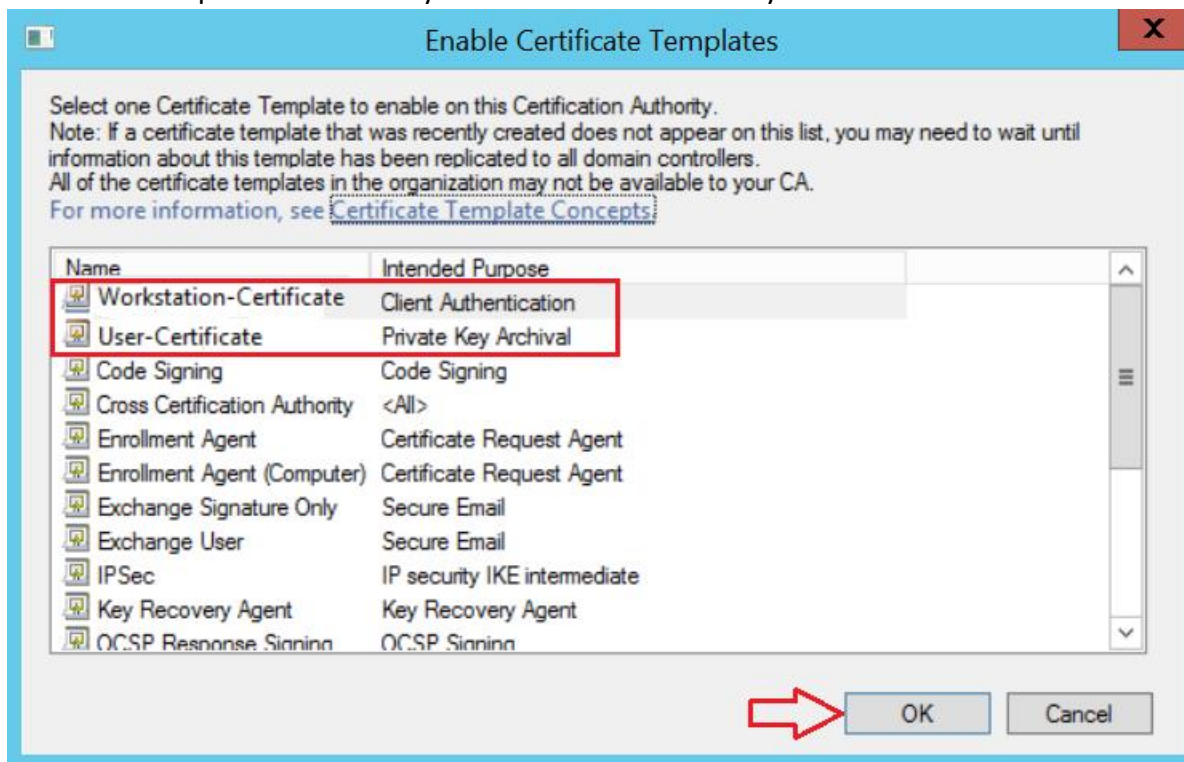
Click the **Extensions** tab, Select the **Application Policies extension**, and click **Edit**. Add Server Authentication application policy. Click **OK**, Again and close the Certificate Templates MMC.



In Certification Authority MMC, click **Certificate Templates**. On **Action** menu, point to **New**, & then click **Certificate Template to Issue**. The **Enable Certificate Templates** dialog box opens.

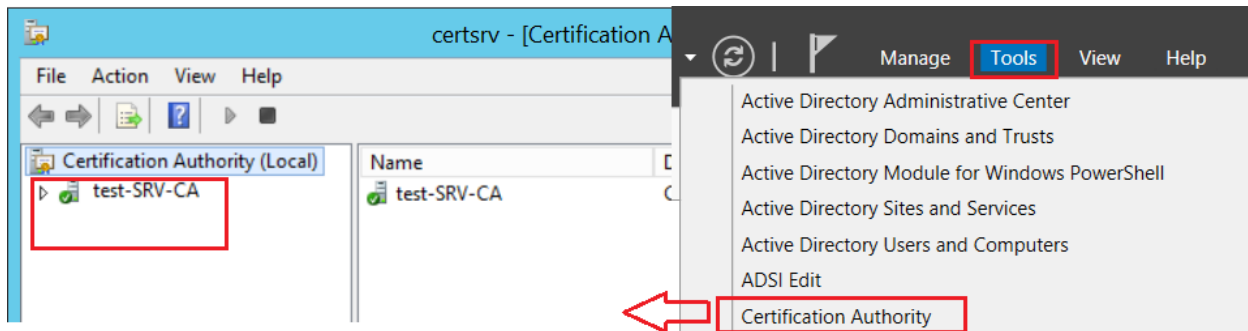


Click the name of the certificate template you just configured, and then click **OK**. Ensure the certificate template is added to your Certification Authority.

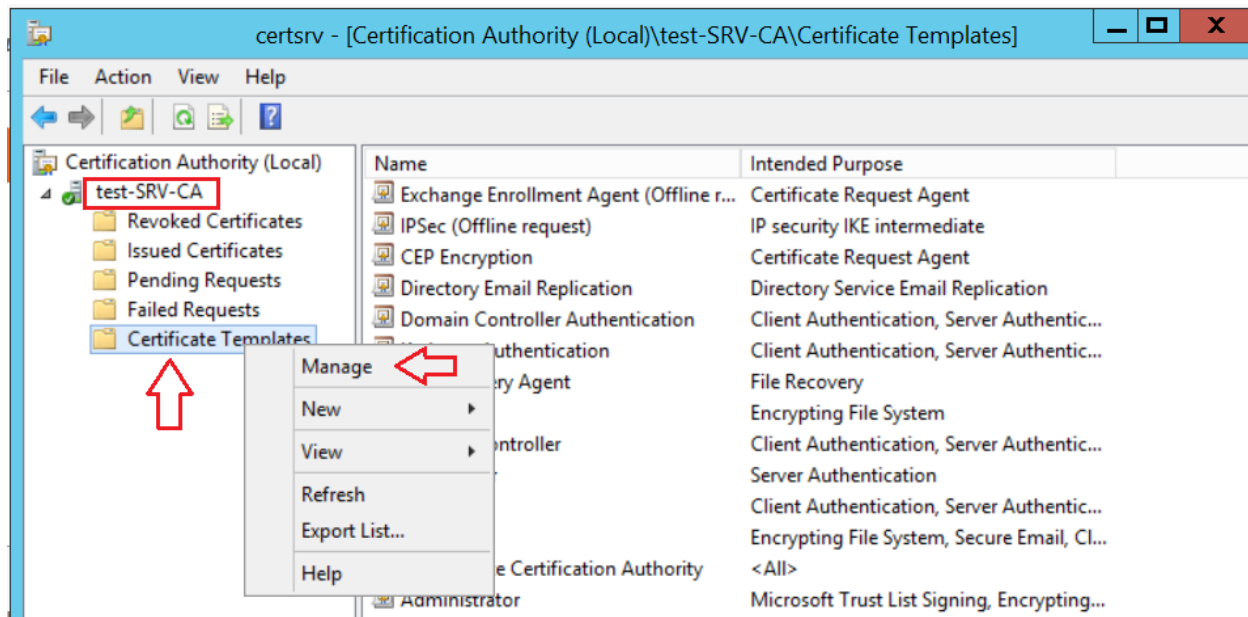


Create Computer Certificate Template:

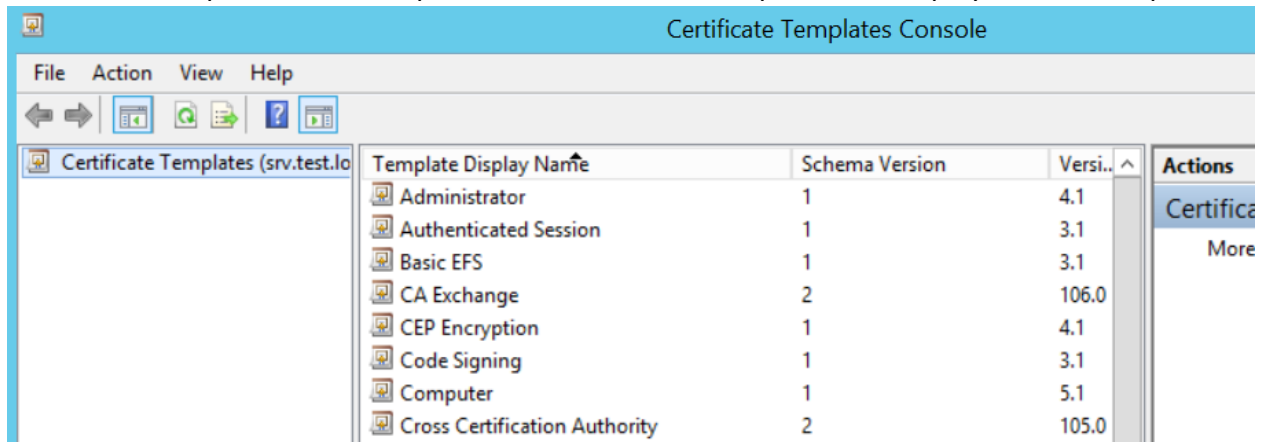
On CA, in **Server Manager**, click **Tools**, and then click **Certification Authority**. The Certification Authority Microsoft Management Console (MMC) opens.



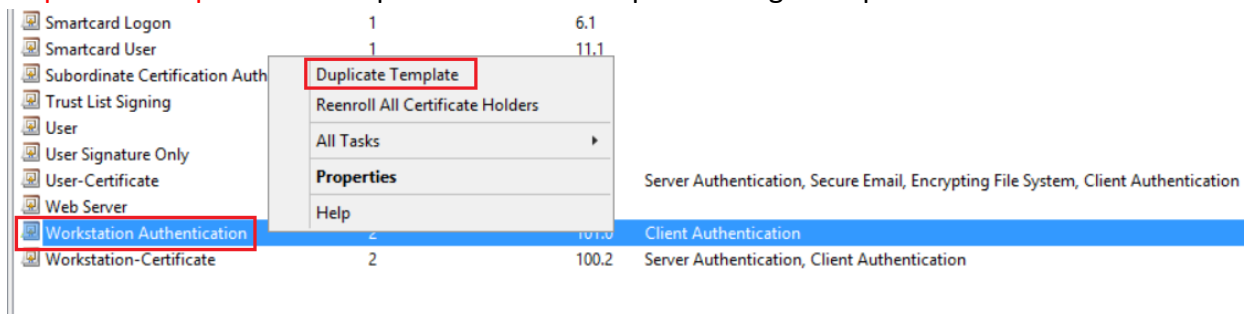
In the MMC, double-click the CA name, right-click Certificate Templates, and then click **Manage**.



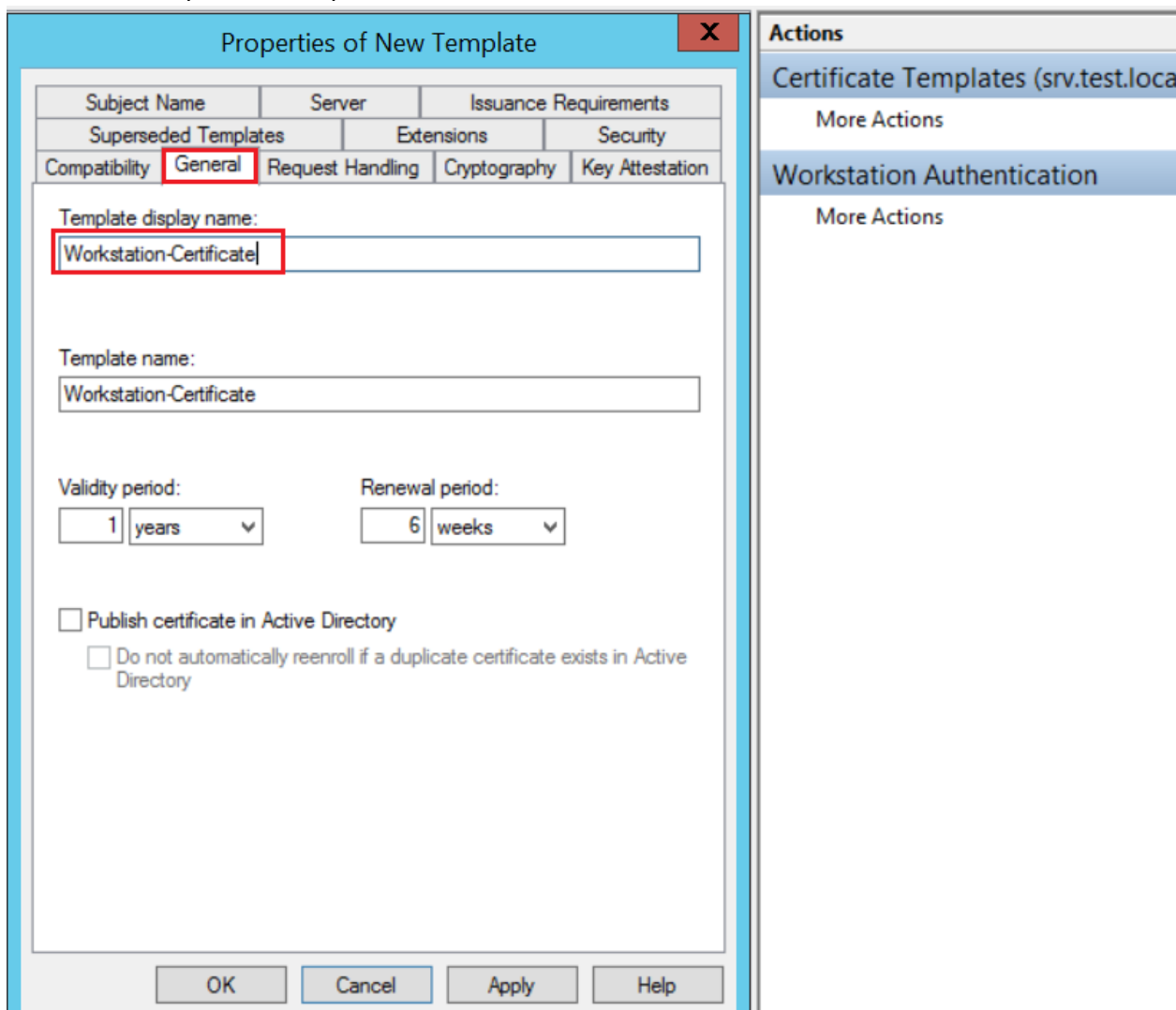
Certificate Templates console opens. All of certificate templates are displayed in details pane.



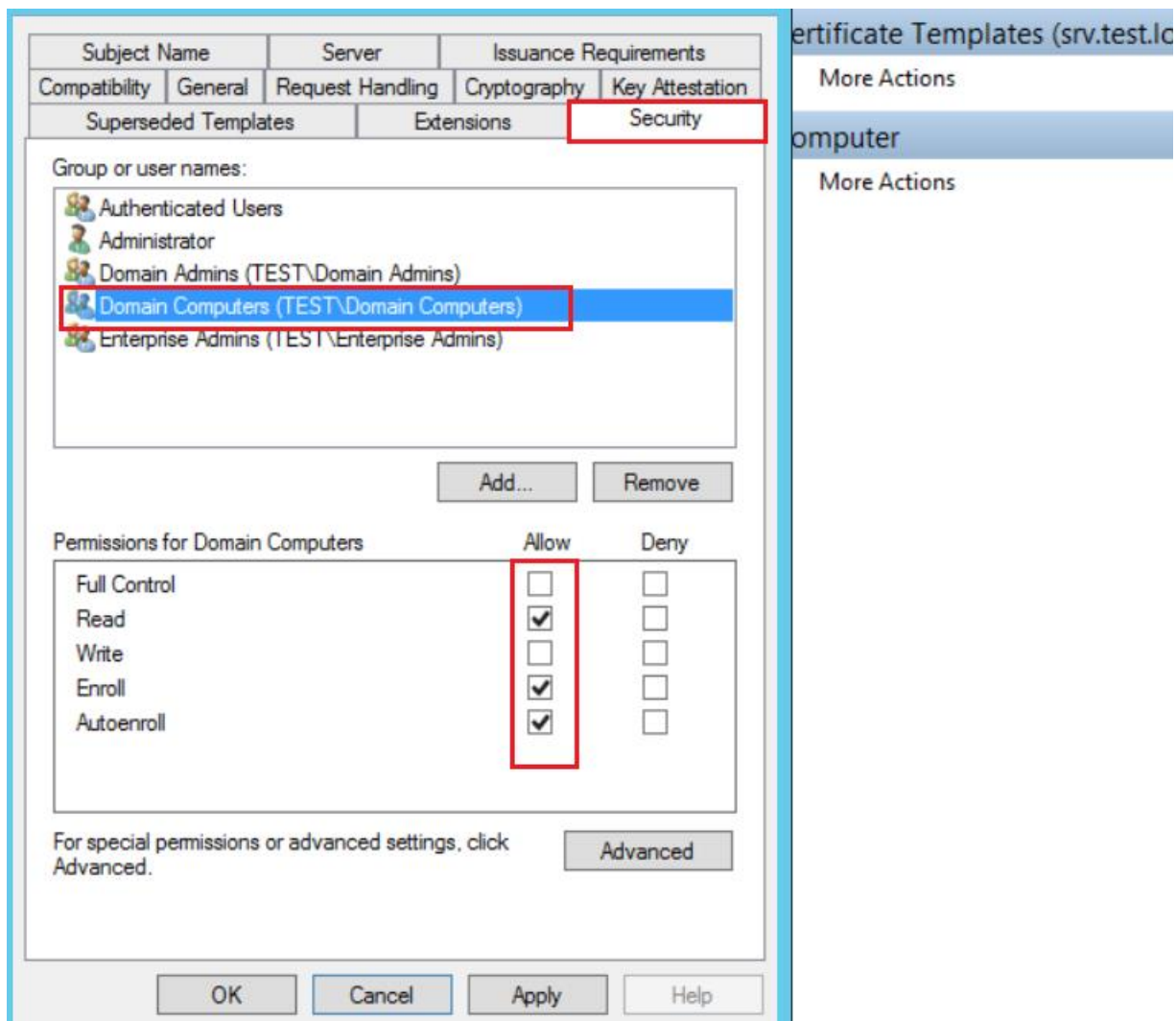
In the details pane, click the **Workstation Authentication** template. On the Action menu, click **Duplicate Template**. The Properties of New Template dialog box opens.



In Properties of New Template, on the **General** tab, in Display Name, type a new name for the certificate template or keep the default name. In this case **Workstation-Certificate**



Click the **Security** tab. In **Group or user names**, click **Domain Computers**. In Permissions for Domain Computers, under Allow, ensure that **Enroll** is selected, and then select the **Read** and **Autoenroll** check boxes.



Click the **Subject Name** Tab. Ensure that **Build from this Active Directory information** is selected. Also ensure that Subject name format has the value of **Fully distinguished name**. In Include this information in alternate subject name, ensure that **User principal name (UPN)** is selected. ensure that **Include e-mail name in subject name** is not selected.

Compatibility General Request Handling Cryptography Key Attestation
Superseded Templates Extensions Security
Subject Name Server Issuance Requirements

☐ Supply in the request
☐ Use subject information from existing certificates for autoenrollment renewal requests (*)

☒ Build from this Active Directory information
Select this option to enforce consistency among subject names and to simplify certificate administration.

Subject name format:
None

☐ Include e-mail name in subject name

Include this information in alternate subject name:
☐ E-mail name
☒ DNS name
☒ User principal name (UPN)
☐ Service principal name (SPN)

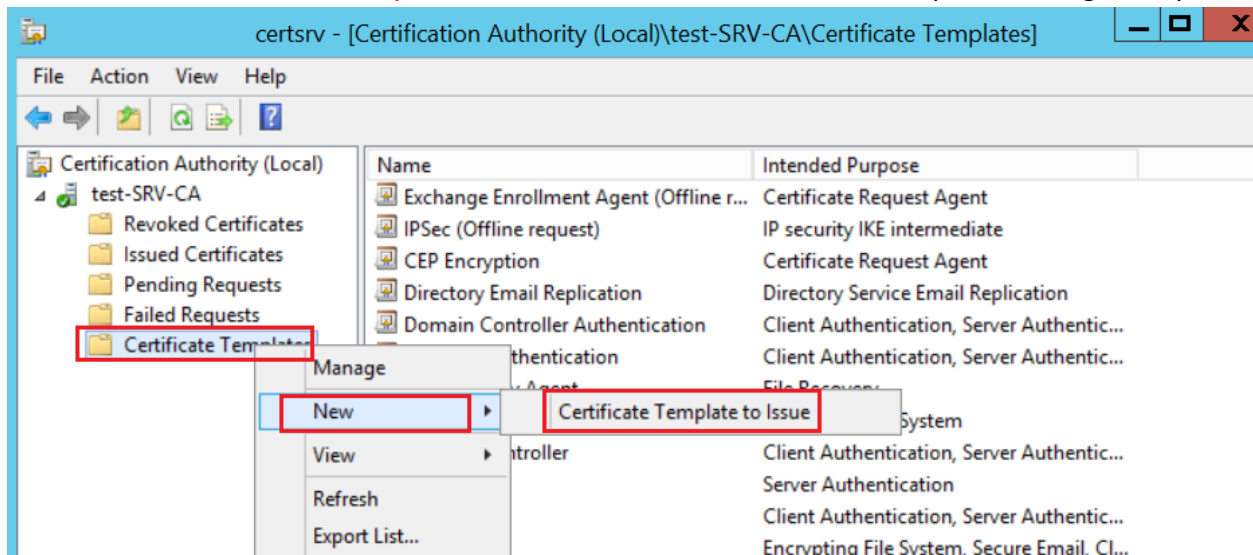
* Control is disabled due to [compatibility settings](#).

OK Cancel Apply Help

Click **OK**, and close the Certificate Templates MMC.

Template Display Name	Schema Version	Version	Actions
Administrator	1	4.1	Certificate More
Authenticated Session	1	3.1	
Basic EFS	1	3.1	
CA Exchange	2	106.0	
CEP Encryption	1	4.1	
Code Signing	1	3.1	
Computer	1	5.1	
Cross Certification Authority	2	105.0	

In Certification Authority MMC, click **Certificate Templates**. On the Action menu, point to **New**, and then click **Certificate Template to Issue**. The Enable Certificate Templates dialog box opens.



Click the name of the certificate template you just configured, and then click **OK**.

