Installing a SSL Server Certificate on Client Access Server

Client Access Server mediates user access to mailboxes. Users interact with the Client Access Server through protocols such as Remote Procedure Call (RPC), IMAP, POP3,Outlook Anywhere, Active Sync or directly through Outlook Web Access (OWA). When we use SSL to secure a connection, third parties that might be intercepting your transmission are unable to access the content of that communication. This is especially important today when many clients are accessing sensitive organizational communication over insecure network. SSL or Secure Socket Layer certificates allow client to establish an encrypted connection to be established between a client and a Client Access Server. SSL certificates, also called *server Certificate* also have the added benefit of verifying the identity of the Client Access Server to the client.

When you install Exchange Server 2010, it install default self-signed certificate. As this certificate is not created or signed by a trusted certificate authorities (CA), this certificate will only trusted by other exchange servers in organization not by other clients in organization. The Exchange self-signed certificate will have Subject Alternate Name (SAN) that correspond to the name of exchange server, including server name and server fully qualified domain name. Since this type of self-signed exchange certificate will be not trusted by clients in organization, exchange administrators need to take an extra step to generate a certificate from internal trusted certificate authorities (CA).

In this article we will configure Active Directory Certificate Service to support the issuance of certificate that uses SAN. To demonstrate this in my lab environment I have used following server:

Domain *: abhi.local*

Domain Controller*: FQDN- DC01.abhi.local,* IP – *192.168.1.1*

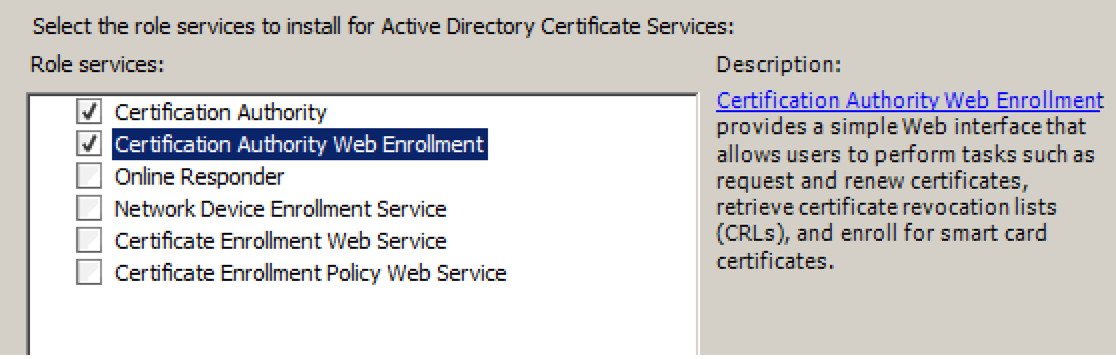
Client Access Server*:* FQDN – *EX02.abhi.local,* IP- *192.168.1.11*

So in this article we will configure our Client Access Server *EX02.abhi.local.* to request and install a server certificate that supports the multiple names the client access server uses.

First we will configure our domain controller *DC01.abhi.local* to issue certificates with multiple SANs and a Domain Name System (DNS) record for *mail.abhi.local.* To do so perform the following steps on domain controller .

- Open Server Manager Console on *DC01.abhi.local* to add the Active Directory Certificate Services role to server.

- Ensure that you add both the ***certification Authority*** and the ***Certification Authority Web Enrollment*** Role Services to the server. If prompted to add additional required role services,clisk add required role services.



Select the role services to install for Active Directory Certificate Services:

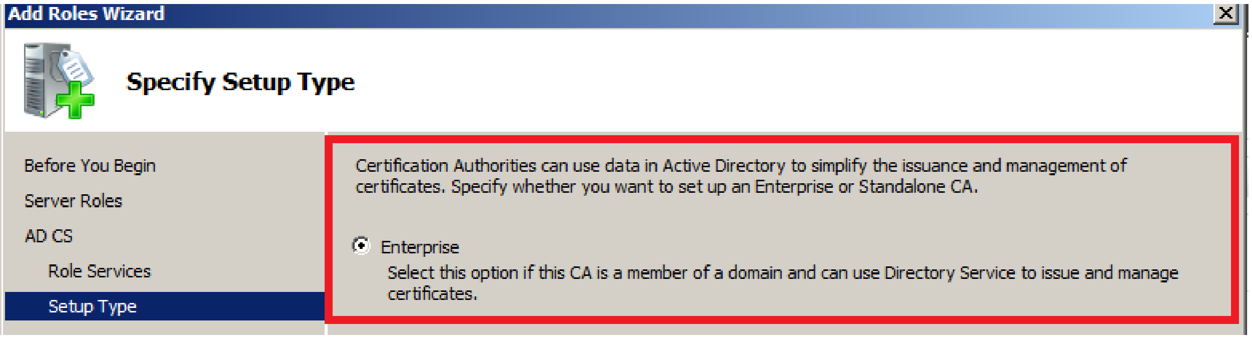
Role services:

☑ Certification Authority
☑ Certification Authority Web Enrollment
□ Online Responder
□ Network Device Enrollment Service
□ Certificate Enrollment Web Service
□ Certificate Enrollment Policy Web Service

Description:

Certification Authority Web Enrollment provides a simple Web interface that allows users to perform tasks such as request and renew certificates, retrieve certificate revocation lists (CRLs), and enroll for smart card certificates.

- Configure *DC01.abhi.local* as an **Enterprise Root CA**.



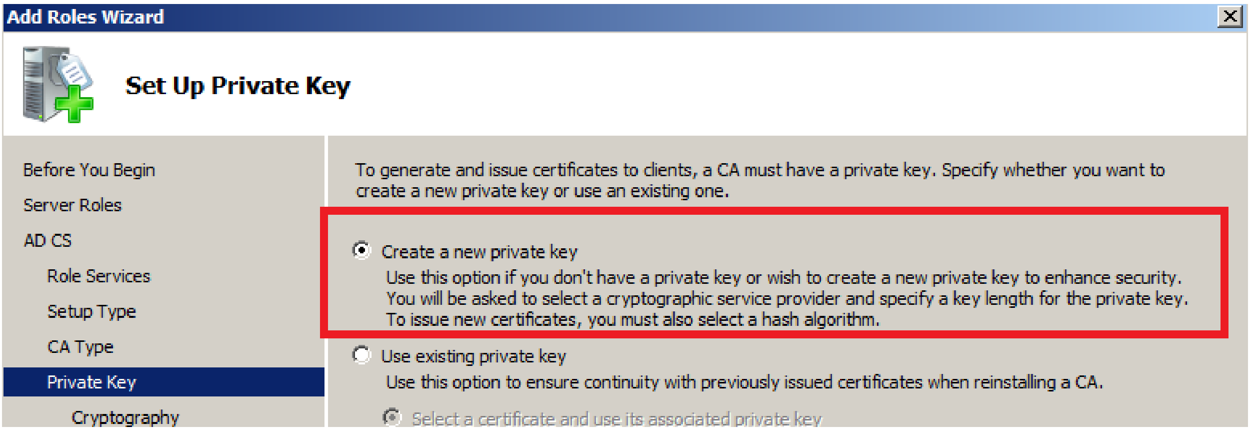
Add Roles Wizard

Specify Setup Type

Certification Authorities can use data in Active Directory to simplify the issuance and management of certificates. Specify whether you want to set up an Enterprise or Standalone CA.

● Enterprise
Select this option if this CA is a member of a domain and can use Directory Service to issue and manage certificates.

- Select the *Create A New Private Key* option.



Add Roles Wizard

Set Up Private Key

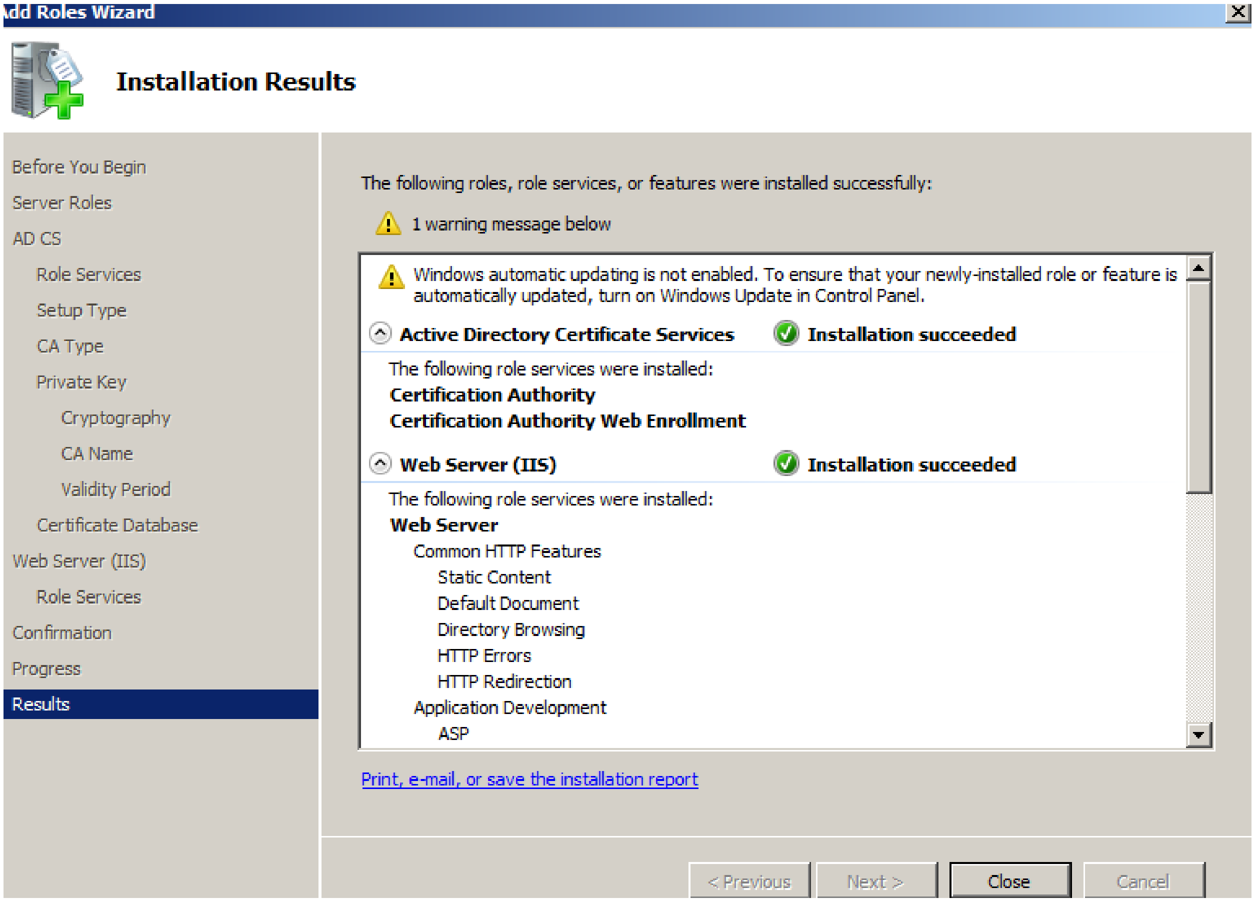
To generate and issue certificates to clients, a CA must have a private key. Specify whether you want to create a new private key or use an existing one.

● Create a new private key
Use this option if you don't have a private key or wish to create a new private key to enhance security. You will be asked to select a cryptographic service provider and specify a key length for the private key. To issue new certificates, you must also select a hash algorithm.

○ Use existing private key
Use this option to ensure continuity with previously issued certificates when reinstalling a CA.

● Select a certificate and use its associated private key

- Then Select the default options for *Cryptography, CA Name,Validity Period,* and *Certificate Database settings.* Continue clicking next until you have the option to install. Click Install and close when Active Directory Services is installed. (You can ignore the warning about windows update)



Installation Results

The following roles, role services, or features were installed successfully:

⚠ 1 warning message below

⚠ Windows automatic updating is not enabled. To ensure that your newly-installed role or feature is automatically updated, turn on Windows Update in Control Panel.

Active Directory Certificate Services ✓ **Installation succeeded**

The following role services were installed:
Certification Authority
Certification Authority Web Enrollment

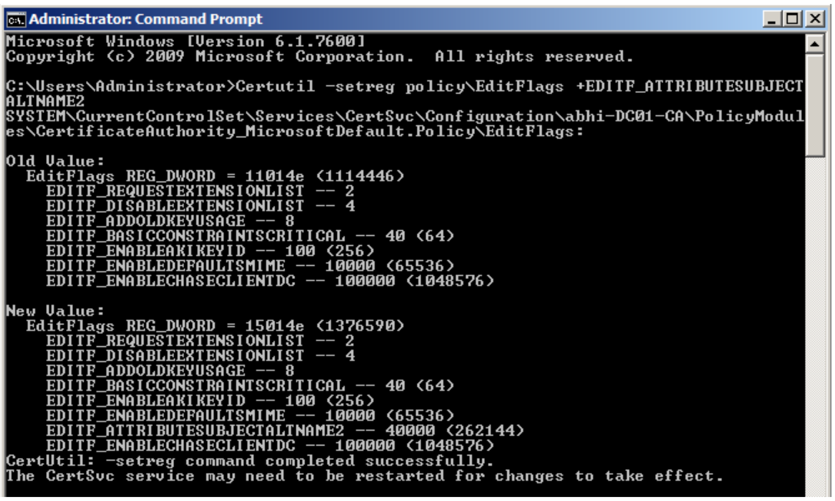
Web Server (IIS) ✓ **Installation succeeded**

The following role services were installed:
Web Server
Common HTTP Features
Static Content
Default Document
Directory Browsing
HTTP Errors
HTTP Redirection
Application Development
ASP

- Now Open an elevated command prompt and enter the following command:

Certutil –setreg policy\EditFlags +EDITF_ATTRIBUTESUBJECTALTNAME2

You will have output put like as below:



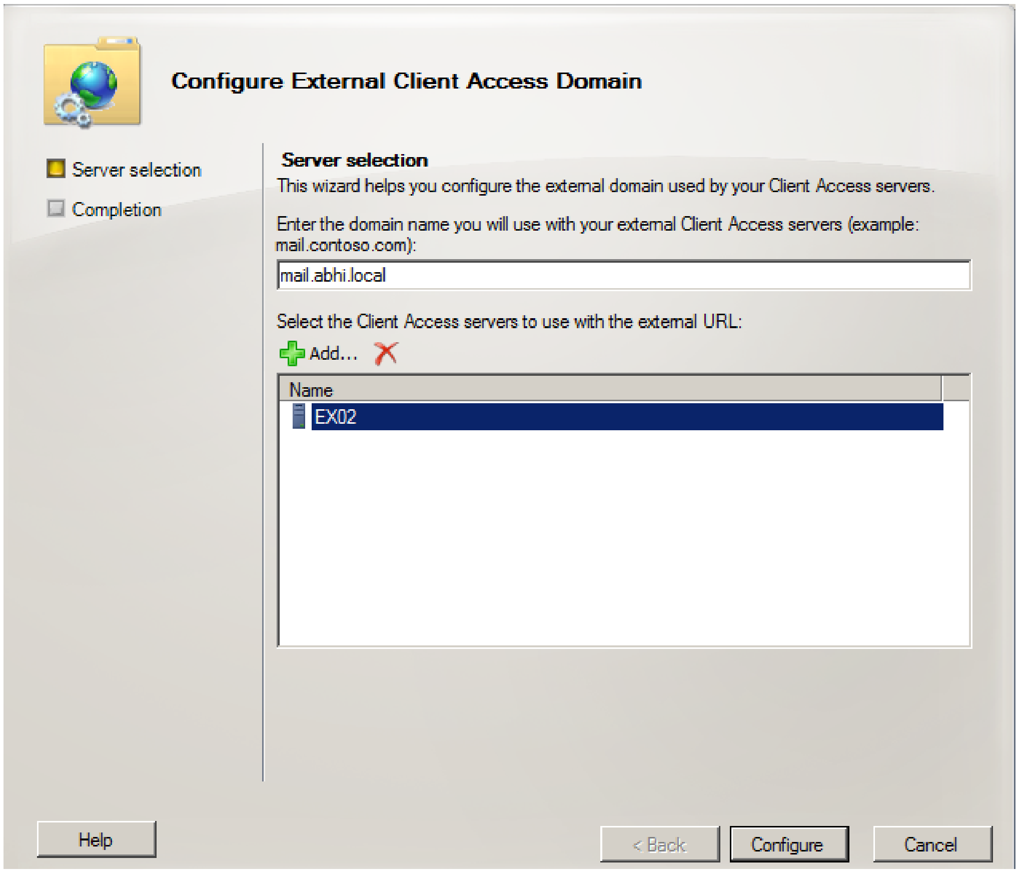
```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Administrator>Certutil -setreg policy\EditFlags +EDITF_ATTRIBUTESUBJECT
ALTNAME2
SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\abhi-DC01-CA\PolicyModul
es\CertificateAuthority_MicrosoftDefault.Policy\EditFlags:

Old Value:
  EditFlags REG_DWORD = 11014e (1114446)
    EDITF_REQUESTEXTENSIONLIST -- 2
    EDITF_DISABLEEXTENSIONLIST -- 4
    EDITF_ADDOLDKEYUSAGE -- 8
    EDITF_BASICCONSTRAINTSCRITICAL -- 40 (64)
    EDITF_ENABLEAKIKEYID -- 100 (256)
    EDITF_ENABLEDEFAULTSMIME -- 10000 (65536)
    EDITF_ENABLECHASECLIENTDC -- 100000 (1048576)

New Value:
  EditFlags REG_DWORD = 15014e (1376590)
    EDITF_REQUESTEXTENSIONLIST -- 2
    EDITF_DISABLEEXTENSIONLIST -- 4
    EDITF_ADDOLDKEYUSAGE -- 8
    EDITF_BASICCONSTRAINTSCRITICAL -- 40 (64)
    EDITF_ENABLEAKIKEYID -- 100 (256)
    EDITF_ENABLEDEFAULTSMIME -- 10000 (65536)
    EDITF_ATTRIBUTESUBJECTALTNAME2 -- 40000 (262144)
    EDITF_ENABLECHASECLIENTDC -- 100000 (1048576)
CertUtil: -setreg command completed successfully.
The CertSvc service may need to be restarted for changes to take effect.
```

- Restart the Active Directory Certificate Services using services console.

Now we have to create a host record for *mail.abhi.local* that maps to the IP address of Client Access Server 192.168.1.11. To do so create this record on domain controller dns console.

Once we have done with dns host record, we will configure external client access domain and request and assign a certificate to the client access server. To do so perform following steps:

- Open Exchange Management Console at server *EX02.abhi.local*
- Select the ***Server Configuration\Client Access*** node. In the Actions pane, click ***Configure External Client Access Domain.*** Enter the name ***mail.abhi.local.***



Configure External Client Access Domain

Server selection

This wizard helps you configure the external domain used by your Client Access servers.

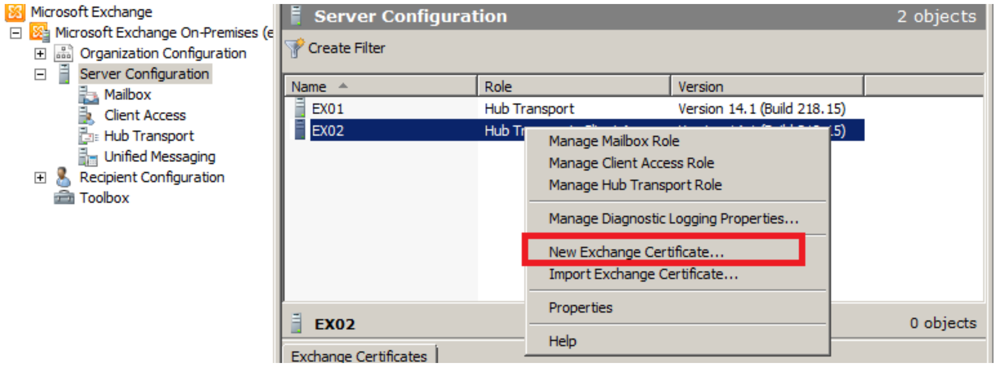
Enter the domain name you will use with your external Client Access servers (example: mail.contoso.com):

mail.abhi.local

Select the Client Access servers to use with the external URL:

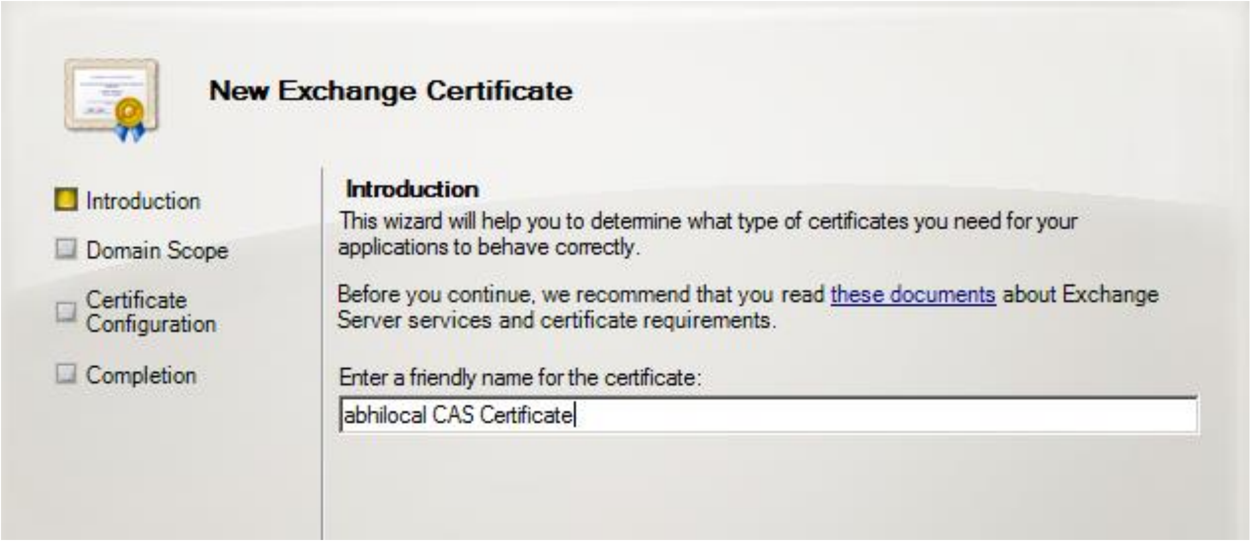
Name
EX02

- Click Configure. When the configuration change is complete, click finish.
- Click on the *Server Configuration* node, right click on *EX02* and then click ***New Exchange Certificate***



Name	Role	Version
EX01	Hub Transport	Version 14.1 (Build 218.15)
EX02	Hub Tr	5)

- On the introduction page, type the name of certificate, in this lab I type ***abhilocal CAS Certificate*** and then click next



Introduction

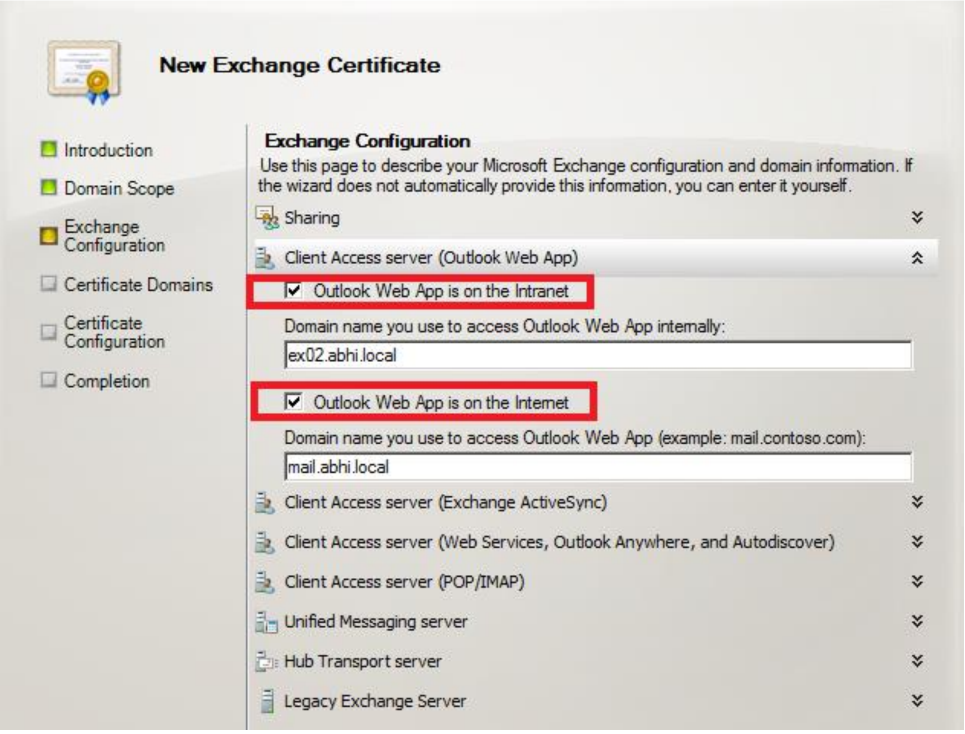
This wizard will help you to determine what type of certificates you need for your applications to behave correctly.

Before you continue, we recommend that you read these documents about Exchange Server services and certificate requirements.

Enter a friendly name for the certificate:

abhilocal CAS Certificate

- On the Exchange Configuration page, expand *Client Access Server (Outlook Web App)* and check the *Outlook Web App Is On The Intranet option* and *the Outlook Web App Is On The Internet* option. Verify your settings and then click next.



New Exchange Certificate

Exchange Configuration

Use this page to describe your Microsoft Exchange configuration and domain information. If the wizard does not automatically provide this information, you can enter it yourself.

☑ Outlook Web App is on the Intranet

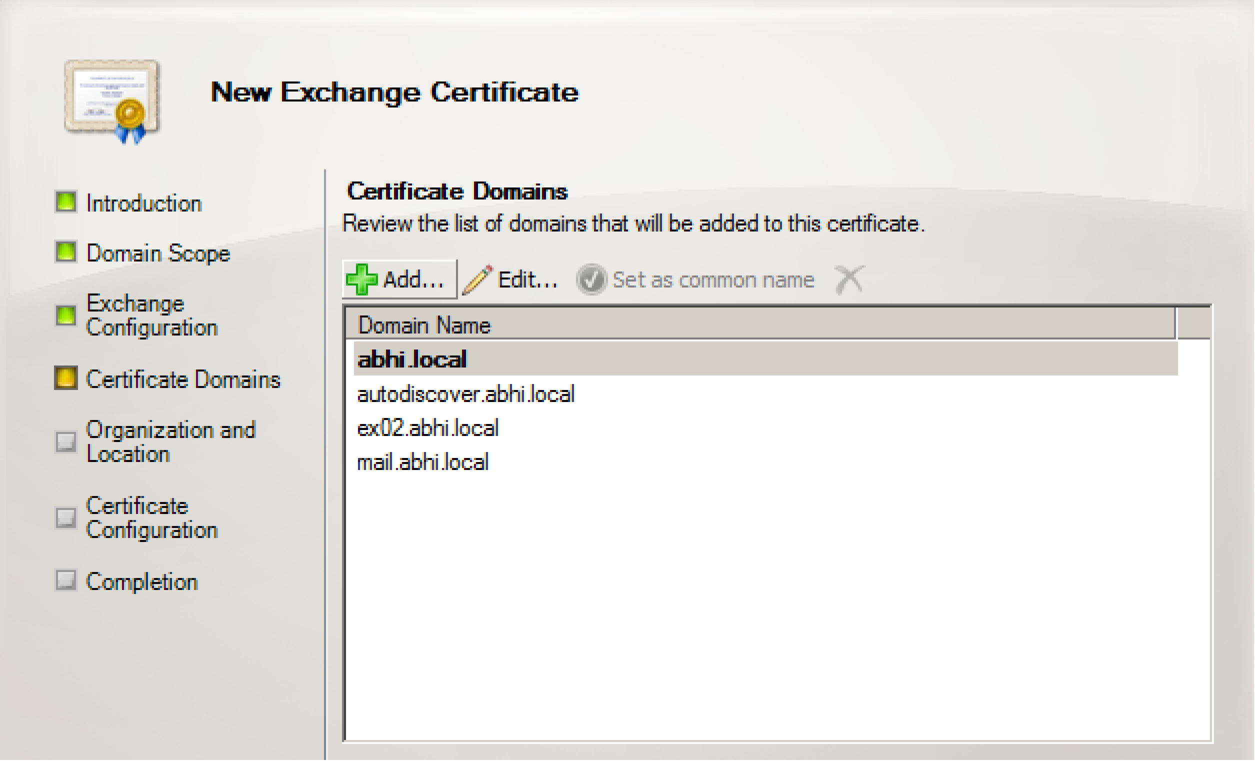
Domain name you use to access Outlook Web App internally: ex02.abhi.local

☑ Outlook Web App is on the Internet

Domain name you use to access Outlook Web App (example: mail.contoso.com): mail.abhi.local

Client Access server (Exchange ActiveSync)
Client Access server (Web Services, Outlook Anywhere, and Autodiscover)
Client Access server (POP/IMAP)
Unified Messaging server
Hub Transport server
Legacy Exchange Server

- Verify that your external client access domain name and local client access server name appear in the list of certificate domain and click next. In this lab it is *mail.abhi.local* and *EX02.abhi.local*



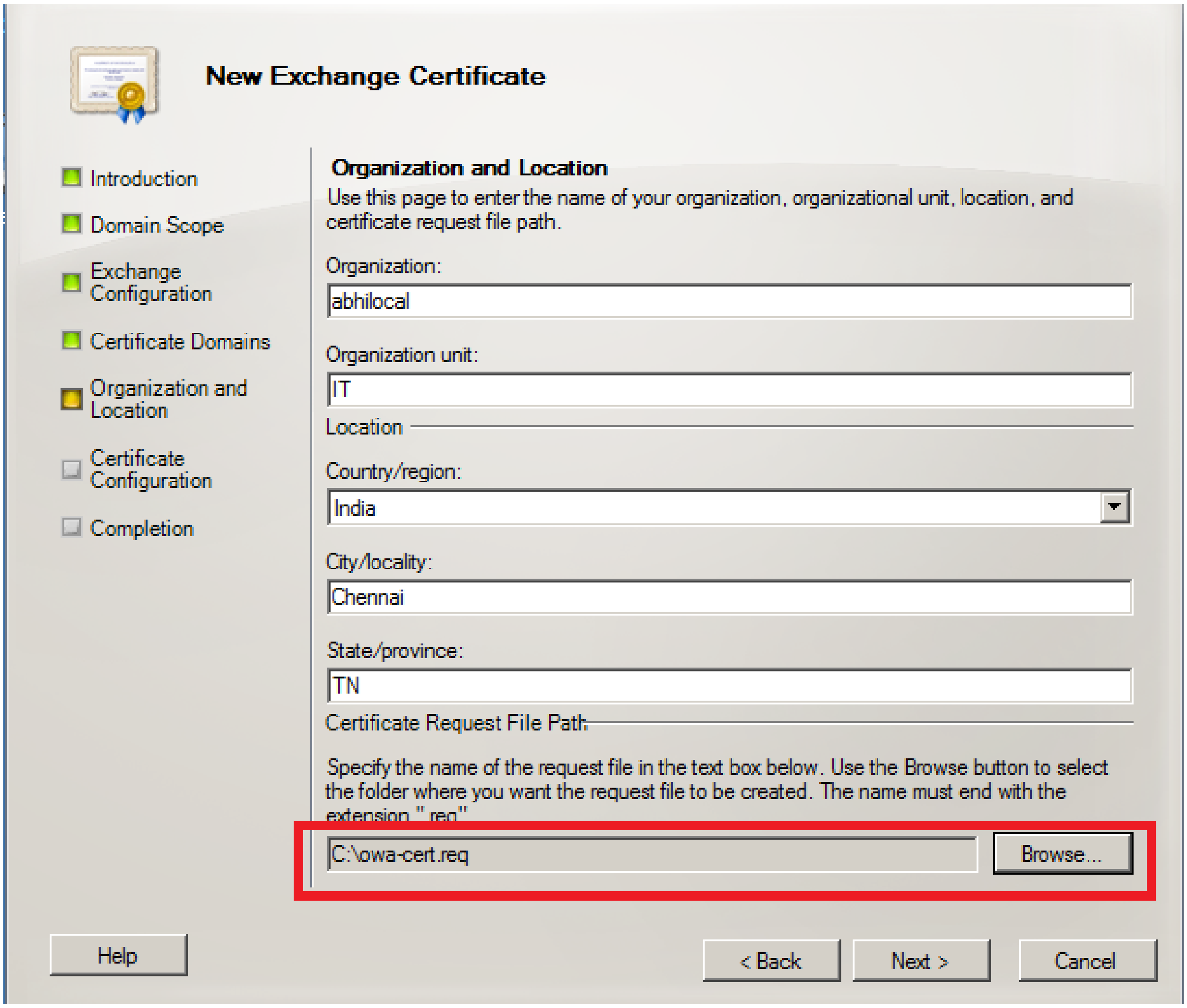
New Exchange Certificate

Certificate Domains

Review the list of domains that will be added to this certificate.

Domain Name
abhi.local
autodiscover.abhi.local
ex02.abhi.local
mail.abhi.local

- On the Organization and Location page, enter the value which most suites your environment. In this lab I have entered following :



New Exchange Certificate

Organization and Location

Use this page to enter the name of your organization, organizational unit, location, and certificate request file path.

Organization: abhilocal

Organization unit: IT

Location

Country/region: India

City/locality: Chennai

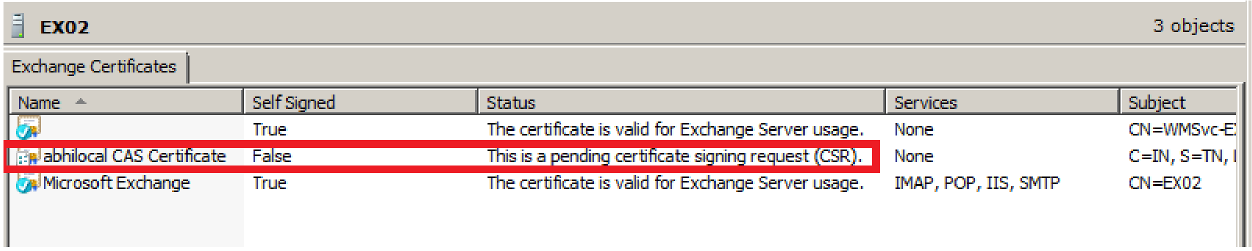
State/province: TN

Certificate Request File Path

Specify the name of the request file in the text box below. Use the Browse button to select the folder where you want the request file to be created. The name must end with the extension ".req"

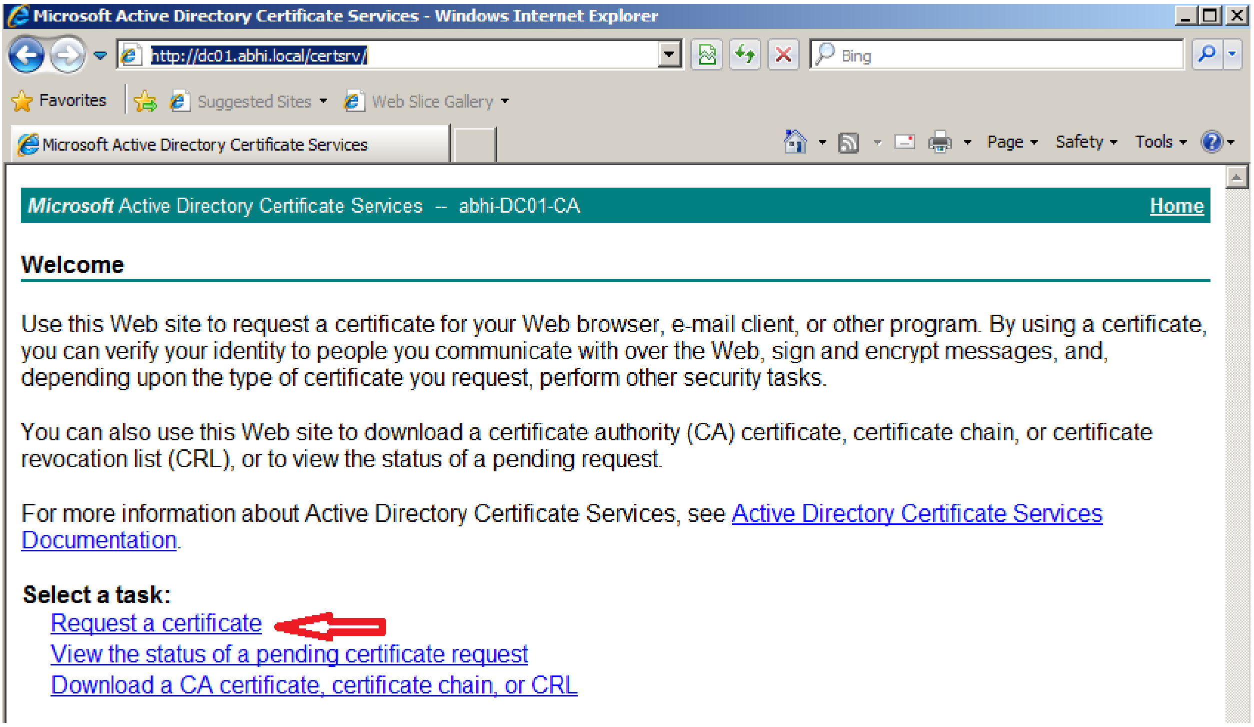
C:\owa-cert.req

- Click next , Click New and then Click Finish.
- You will see the status of this certificate in Exchange management console is in pending status. It need to get signed and trusted by our local certificate authoritative server



Name	Self Signed	Status	Services	Subject
	True	The certificate is valid for Exchange Server usage.	None	CN=WMSvc-E
abhilocal CAS Certificate	False	This is a pending certificate signing request (CSR).	None	C=IN, S=TN, I
Microsoft Exchange	True	The certificate is valid for Exchange Server usage.	IMAP, POP, IIS, SMTP	CN=EX02

- Now once this done, Open the file ***owa-cert.req*** using notepad and copy all the text on clipboard. Disable ***Internet Explorer Enhanced Security Configuration.*** Open command prompt and type – ***gpupdate /force.***
- Open IE and type ***http://dc01.abhi.local/certsrv.*** On the Microsoft Active Directory Certificate Services Welcome page, Click ***Request A Certificate*** and then click ***Advanced Certificate Request.***


Microsoft Active Directory Certificate Services - Windows Internet Explorer
http://dc01.abhi.local/certsrv/
Bing
Favorites
Suggested Sites
Web Slice Gallery
Microsoft Active Directory Certificate Services
Page
Safety
Tools

Microsoft Active Directory Certificate Services -- abhi-DC01-CA Home

Welcome

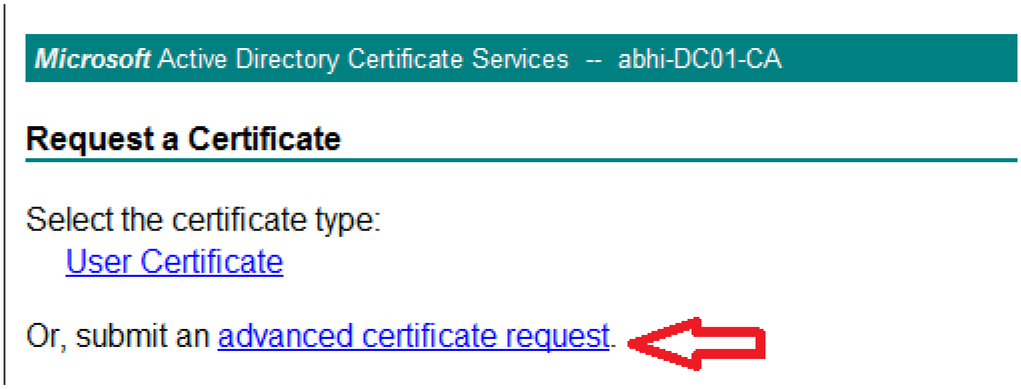
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see Active Directory Certificate Services Documentation.

Select a task:

Request a certificate
View the status of a pending certificate request
Download a CA certificate, certificate chain, or CRL



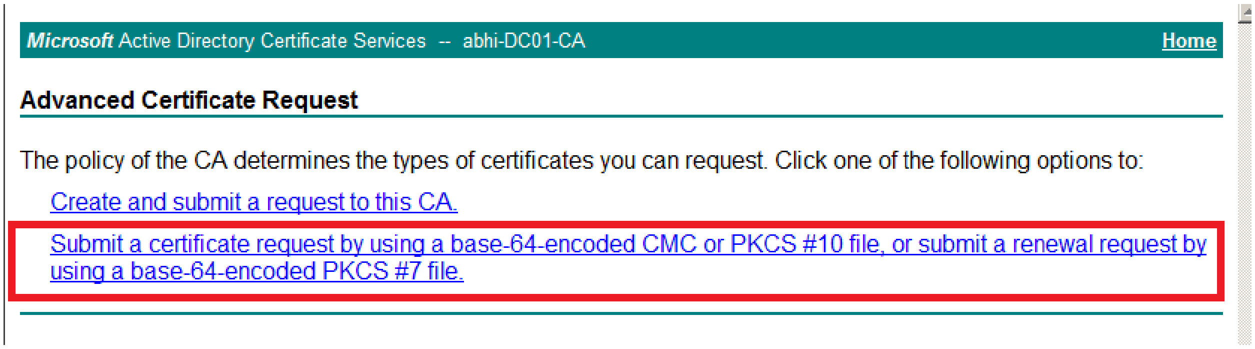
Microsoft Active Directory Certificate Services -- abhi-DC01-CA

Request a Certificate

Select the certificate type:
User Certificate

Or, submit an advanced certificate request.

- On the Advanced certificate request page, Click ***Submit A certificate Request By using A Base-64 Encoded CMC or PKCS#10 File,*** Or ***Submit A renewal Request By Using A Base-64 Encoded CMC Or PKCS#7 File.***



Microsoft Active Directory Certificate Services -- abhi-DC01-CA

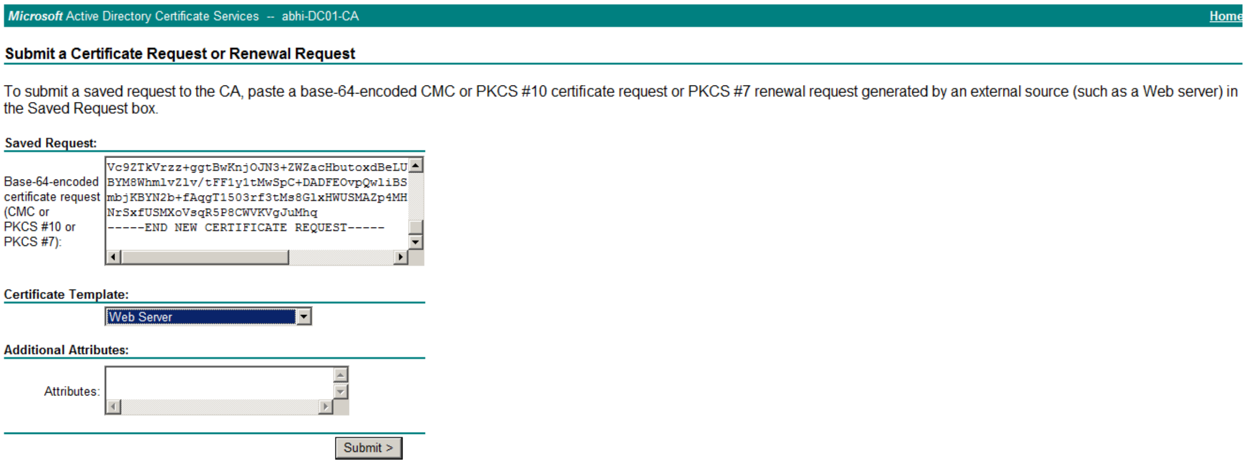
Advanced Certificate Request

The policy of the CA determines the types of certificates you can request. Click one of the following options to:

Create and submit a request to this CA.

Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.

- On the following page, Click on the ***Saved Request text*** box and copy all the text from the file ***C:\owa-cert.req.*** (*This file is created when we configure exchange certificate request).* Verify that the Certificate Template drop-down is set to ***Web Server*** and then click Submit



Microsoft Active Directory Certificate Services -- abhi-DC01-CA

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
Vc9ZTkVrzz+ggtBwKnjOJN3+ZWZacHbutoxdBeLU
BYM8WhmlvZlv/tFF1y1tMwSpC+DADFEOvpQwliBS
mbjKBYN2b+fAqgT1503rf3tMs8GlxHWUSMAZp4MH
NrSxfUSMXoVsqR5P8CWVKVgJuMhq
-----END NEW CERTIFICATE REQUEST-----
```

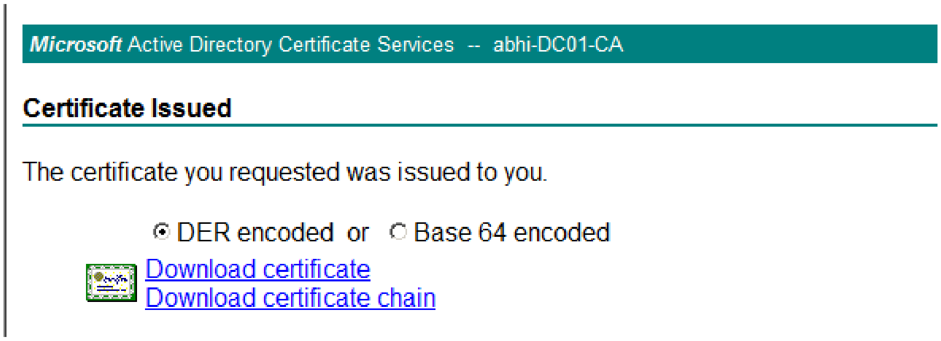
Certificate Template:

Web Server

Additional Attributes:

Attributes:

- On the certificate issued page, Click ***Download Certificate.*** Save the Certificate on the desktop as ***certnew.cer***



Microsoft Active Directory Certificate Services -- abhi-DC01-CA

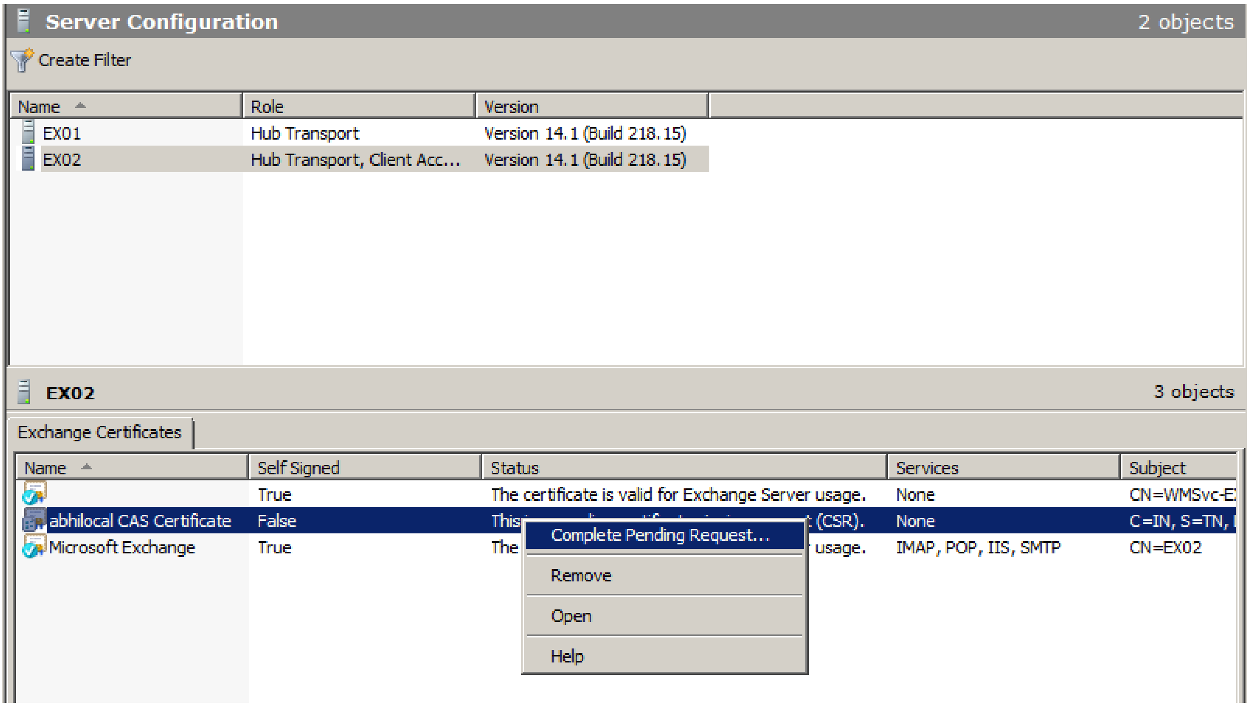
Certificate Issued

The certificate you requested was issued to you.

● DER encoded or ○ Base 64 encoded

Download certificate
Download certificate chain

- Once this done, Open EMC, Click *Server Configuration,* Click *EX02,* and in the bottom pane click *abhilocal CAS Certificate.* In the action pane, click ***Complete Pending Request*** and browse to locate the file ***certnew.cer*** and then click Complete. Click Finish to close the dialog box.

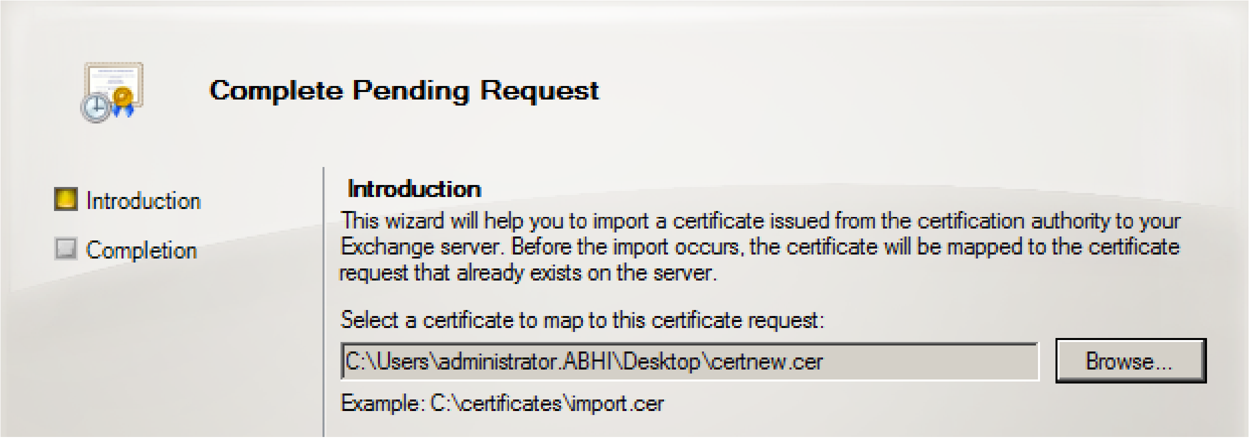


Server Configuration — 2 objects

Name	Role	Version
EX01	Hub Transport	Version 14.1 (Build 218.15)
EX02	Hub Transport, Client Acc...	Version 14.1 (Build 218.15)

EX02 — 3 objects

Name	Self Signed	Status	Services	Subject
	True	The certificate is valid for Exchange Server usage.	None	CN=WMSvc-E
abhilocal CAS Certificate	False	This [illegible] (CSR).	None	C=IN, S=TN,
Microsoft Exchange	True	The [illegible] usage.	IMAP, POP, IIS, SMTP	CN=EX02



Complete Pending Request

Introduction

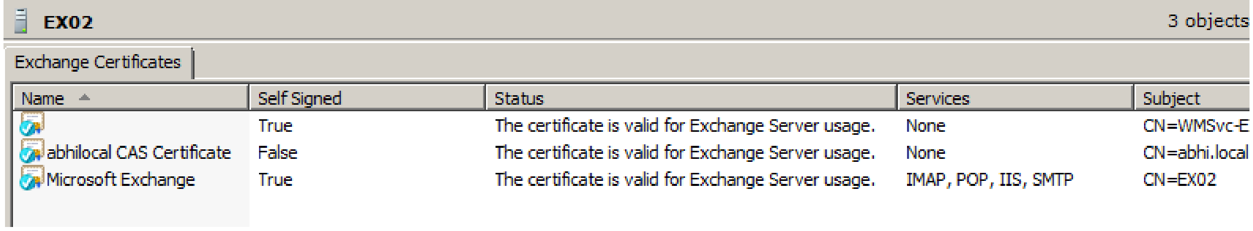
This wizard will help you to import a certificate issued from the certification authority to your Exchange server. Before the import occurs, the certificate will be mapped to the certificate request that already exists on the server.

Select a certificate to map to this certificate request:

C:\Users\administrator.ABHI\Desktop\certnew.cer

Example: C:\certificates\import.cer

Now you will see the status of Exchange certificate is changed to as valid certificate.

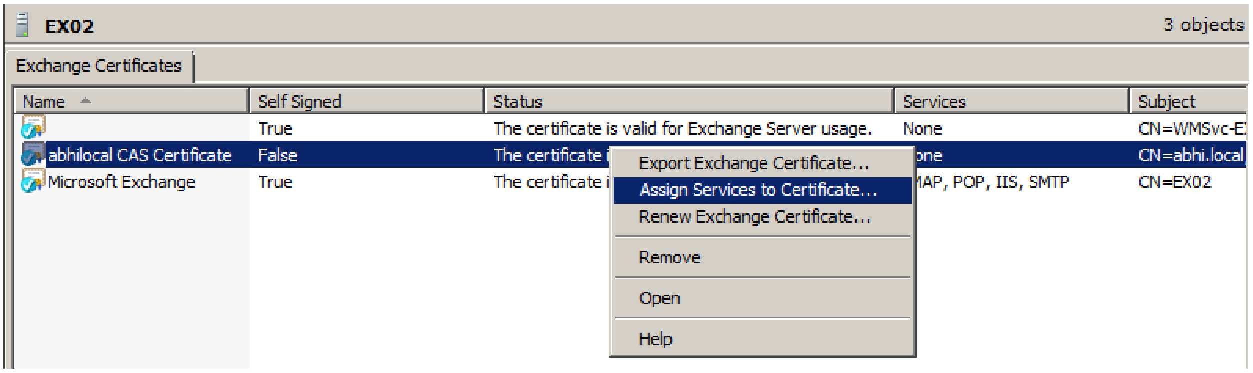


EX02 — 3 objects

Name	Self Signed	Status	Services	Subject
	True	The certificate is valid for Exchange Server usage.	None	CN=WMSvc-E
abhilocal CAS Certificate	False	The certificate is valid for Exchange Server usage.	None	CN=abhi.local
Microsoft Exchange	True	The certificate is valid for Exchange Server usage.	IMAP, POP, IIS, SMTP	CN=EX02

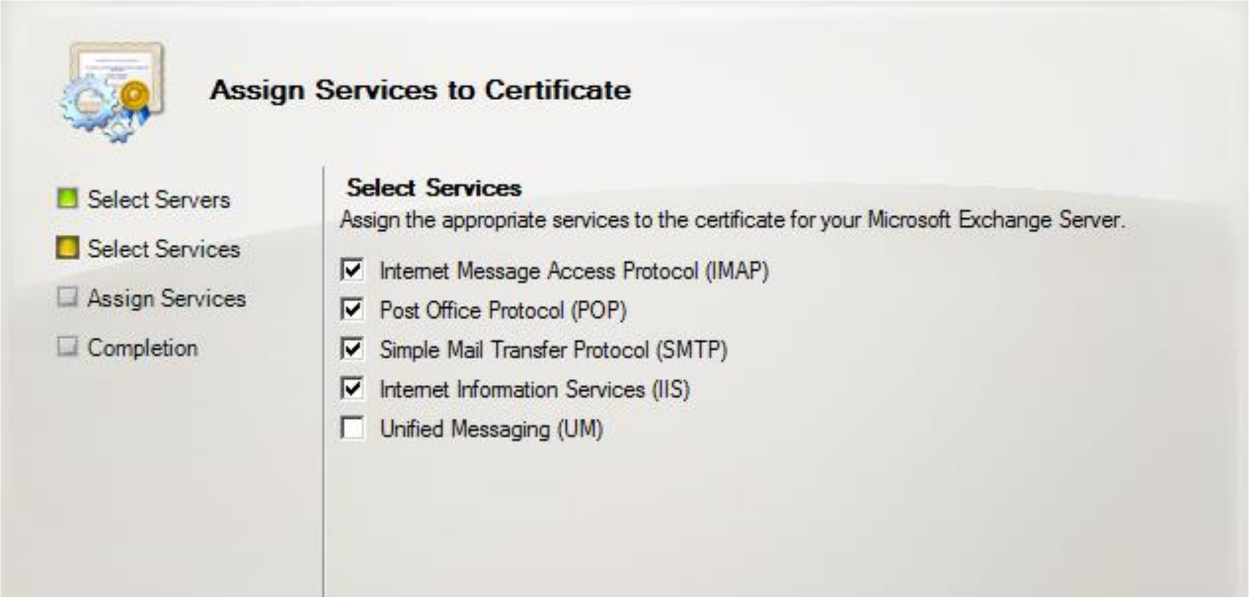
So now our certificate has a valid status for exchange server usage, bit it haven't configure for any services so we need to assign services to our Exchange CAS certificate. To do so, perform following:

- Right click *abhilocal CAS Certificate* **and** then click ***Assign Services To Certificate.*** Ensure that your CAS server is selected. In this lab it is EX02. Click Next.


EX02
3 objects
Exchange Certificates
Export Exchange Certificate...
Assign Services to Certificate...
Renew Exchange Certificate...
Remove
Open
Help

Name	Self Signed	Status	Services	Subject
	True	The certificate is valid for Exchange Server usage.	None	CN=WMSvc-E
abhilocal CAS Certificate	False	The certificate i	one	CN=abhi.local
Microsoft Exchange	True	The certificate i	MAP, POP, IIS, SMTP	CN=EX02

- On following dialog page, select the Services which you want to assign to the certificaste for your Exchange Server, and then click next. If asked to replace any existing assignments click yes. Click Assign and then click Finish.

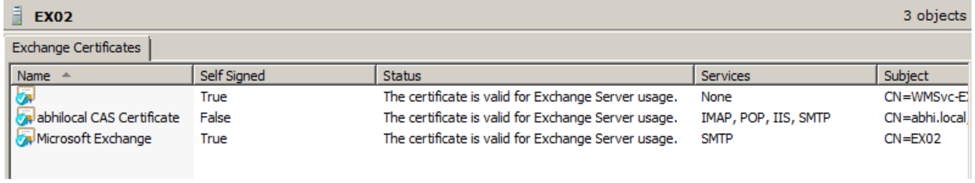


Select Services

Assign the appropriate services to the certificate for your Microsoft Exchange Server.

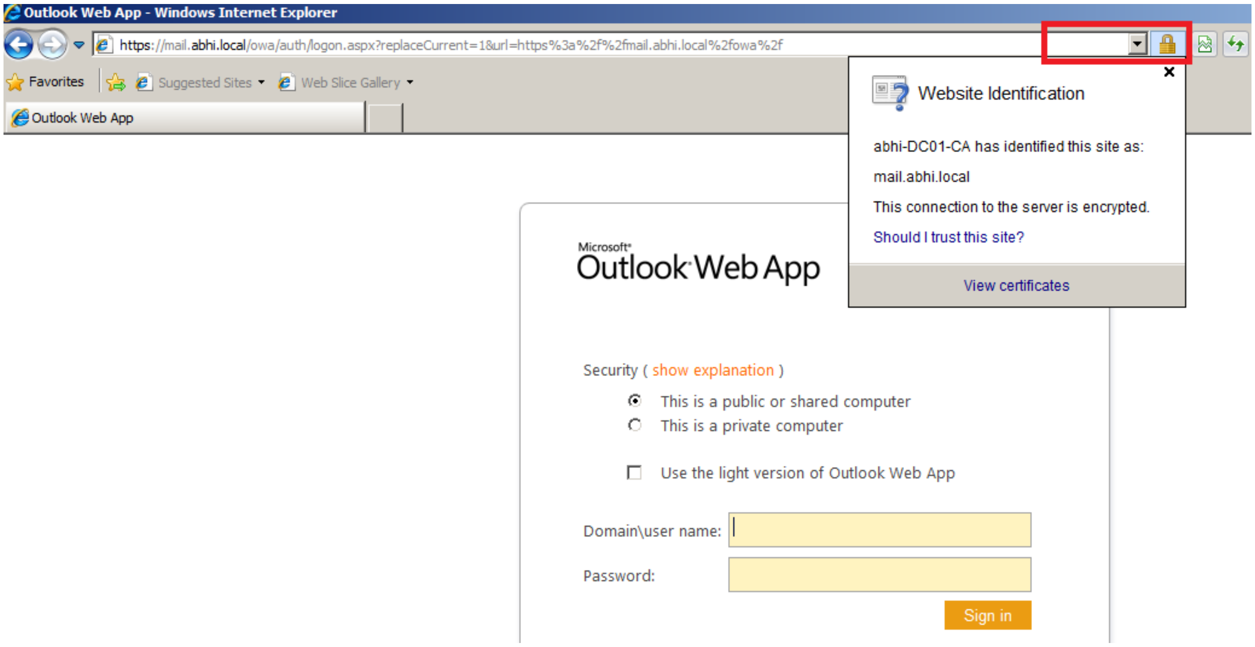
☑ Internet Message Access Protocol (IMAP)
☑ Post Office Protocol (POP)
☑ Simple Mail Transfer Protocol (SMTP)
☑ Internet Information Services (IIS)
□ Unified Messaging (UM)

Now the services have been assigned to our CAS certificate.



Name	Self Signed	Status	Services	Subject
	True	The certificate is valid for Exchange Server usage.	None	CN=WMSvc-E
abhilocal CAS Certificate	False	The certificate is valid for Exchange Server usage.	IMAP, POP, IIS, SMTP	CN=abhi.local
Microsoft Exchange	True	The certificate is valid for Exchange Server usage.	SMTP	CN=EX02

- Verify that the certificate is correctly assigned by browsing to ***https://mail.abhi.local/owa*** and viewing the security report by clicking the lock icon on IE address bar.


Outlook Web App - Windows Internet Explorer
https://mail.abhi.local/owa/auth/logon.aspx?replaceCurrent=1&url=https%3a%2f%2fmail.abhi.local%2fowa%2f
Favorites
Suggested Sites
Web Slice Gallery
Outlook Web App
Website Identification
Should I trust this site?
View certificates
Microsoft® Outlook Web App
Security (show explanation)
Sign in

Website Identification

abhi-DC01-CA has identified this site as:

mail.abhi.local

This connection to the server is encrypted.

Security (show explanation)

● This is a public or shared computer

○ This is a private computer

□ Use the light version of Outlook Web App

Domain\user name:

Password:

So we verified that connection to the client access server is encrypted. Now our exchange server will use the certificate for identification and secure communication. SSL certificates are usually signed by an internal or trusted third-party CA. Obtaining a certificate from an internal CA has no associated charge, but clients outside your organization are unlikely to trust the certificate. Therefore please note that you should obtain a certificate from a third-party CA using same procedure and steps when you need to support users from outside your organization.