

COMODO
Creating Trust Online®



Comodo Certificate Manager

Software Version 4.5

Windows Auto Enrollment Setup Guide

Guide Version 4.5.052714

Comodo CA Limited
3rd Floor, 26 Office Village, Exchange Quay,
Trafford Road, Salford,
Greater Manchester M5 3EQ,
United Kingdom.

Table of Contents

1.Prerequisites.....	3
1.1.Server Requirement.....	3
1.2.Client Requirement.....	3
1.3.Modifications on Customer Side.....	3
2.Kerberos Configuration.....	3
2.1.Prepare Windows Server.....	3
2.2.Create/Modify login.conf in Certificate Manager.....	10
2.3.Configure Active Directory Properties in CCM Server.....	11
2.4.Synchronize Time between CCM Server and Domain Controller.....	13
2.5.Restart Comodo Certificate Manager.....	13
3.Deploy Script on Windows Server.....	13
3.1.VBScript Properties Configuration.....	13
3.2.Open Group Policy Editor.....	14
3.3.Edit Logon Script Properties.....	17
3.4.Distribute capicom.dll.....	20
3.5.Set Trusted Sites Policy.....	22
3.6.Deploy Trusted Root Certificates.....	24
3.7.Create User Accounts on Active Directory with Email Box.....	27
4.Client Configuration.....	29
4.1.Join Windows Server Domain.....	29
4.2.Logon as Domain User.....	29
5.Check Certificate.....	30
5.1.Check User Certificate.....	30
6.Multiple Customer Configuration.....	31
6.1.Configure Kerberos.....	31
6.2.Deploy VBScript.....	31
6.3.Restart CCM server.....	31
7.Known Issues.....	31
7.1.Don't Use CCM Server Machine as Client.....	31
7.2.Capicom Installation Fails.....	32
7.3.Cannot Set Password While Creating the User Keytab File.....	32
8.Troubleshooting.....	32
8.1.1.Errors in Script Log.....	32
About Comodo.....	35

1. Prerequisites

1.1. Server Requirement

- Windows Server 2003 or Windows Server 2008
- Exchange Server 2003 or Exchange Server 2007
- Certificate Manager Server running under JRE 1.6 or JDK 1.6

1.2. Client Requirement

- Windows XP SP2/SP3 or Windows Vista SP1
- Outlook 2003 or Outlook 2007

1.3. Modifications on Customer Side

- Active Directory changes:
 - Add one domain account (that will be used by CCM) and map 2 SPNs to the account
 - Modify Default Group Policy or create new Group Policy to deploy auto enrollment script and install special additional software
- Network changes:
 - When CCM is deployed outside customer's network: map port 88 and 389 of Active Directory on gateway server that will allow CCM to connect Active Directory
 - Add a host mapping in local DNS for domain users to access CCM by domain name
 - Following are IP addresses of cert-manager.comodo.com from where access to ports must be allowed.
 - 91.199.212.128/26
 - 87.127.204.128/26
 - 216.126.215.128/26

2. Kerberos Configuration

2.1. Prepare Windows Server

- Create a new user for Certificate Manager
Create a new domain account "ccm" or any name you like for Certificate Manager on Windows Server.
Open up Active Directory Users and Computers snap-in, right click on Users object on the left panel and select New->User from menu. See figure 2.1.
Fill in the necessary properties in User Object Editor. See figure 2.2.
IMPORTANT: Do not use the same name as any existing computer name in Active Directory!
Right click on the created user 'ccm' in Active Directory Users and Computers snap-in and click on Properties to open up Properties dialog. Check user's logon name, for now CCM's user logon name should be 'ccm'. See figure 2.3.

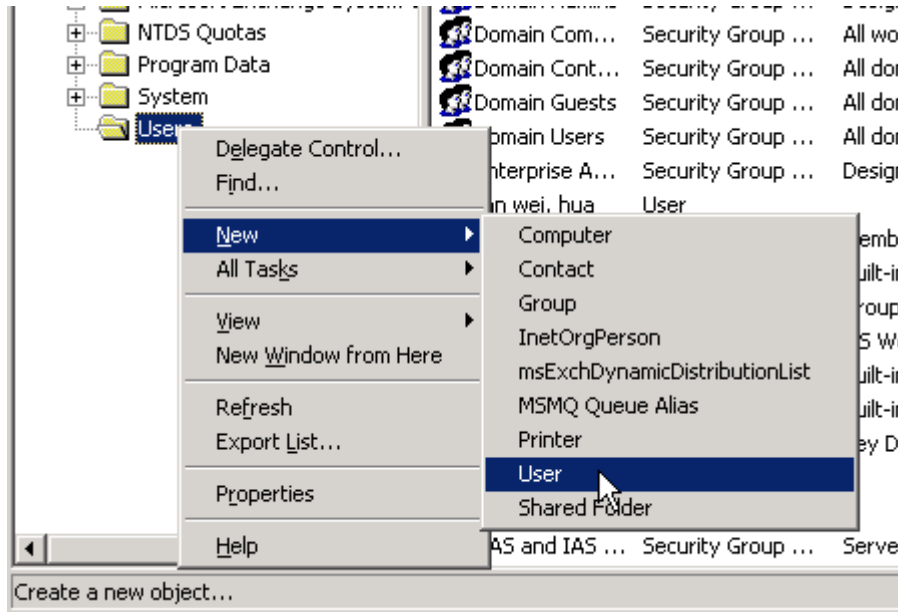


Figure 2.1 Open User Object Editor dialog

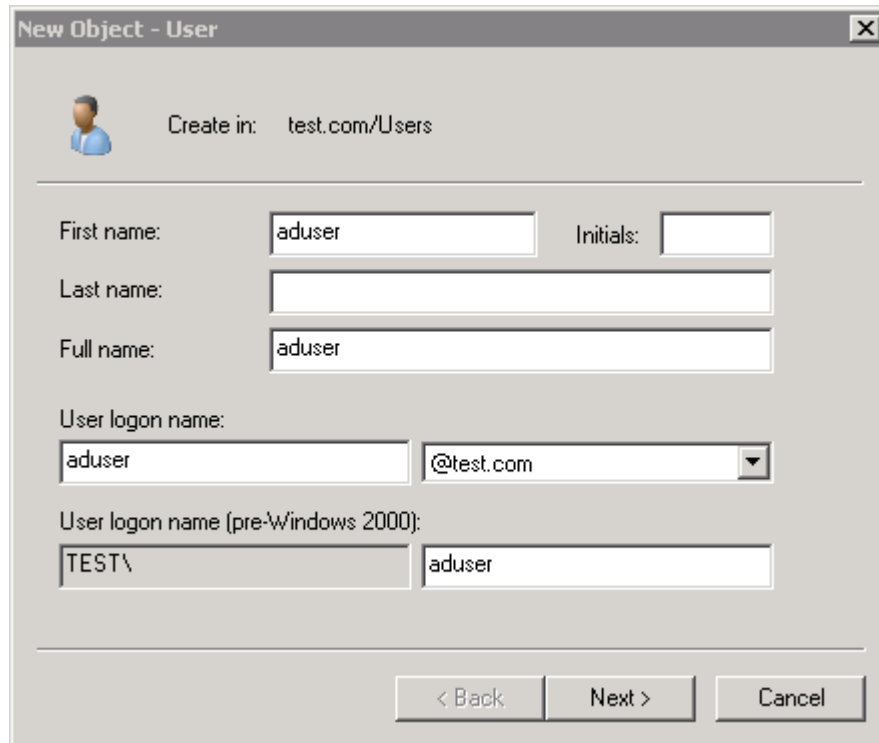


Figure 2.2 Create a new account in Users Object Editor

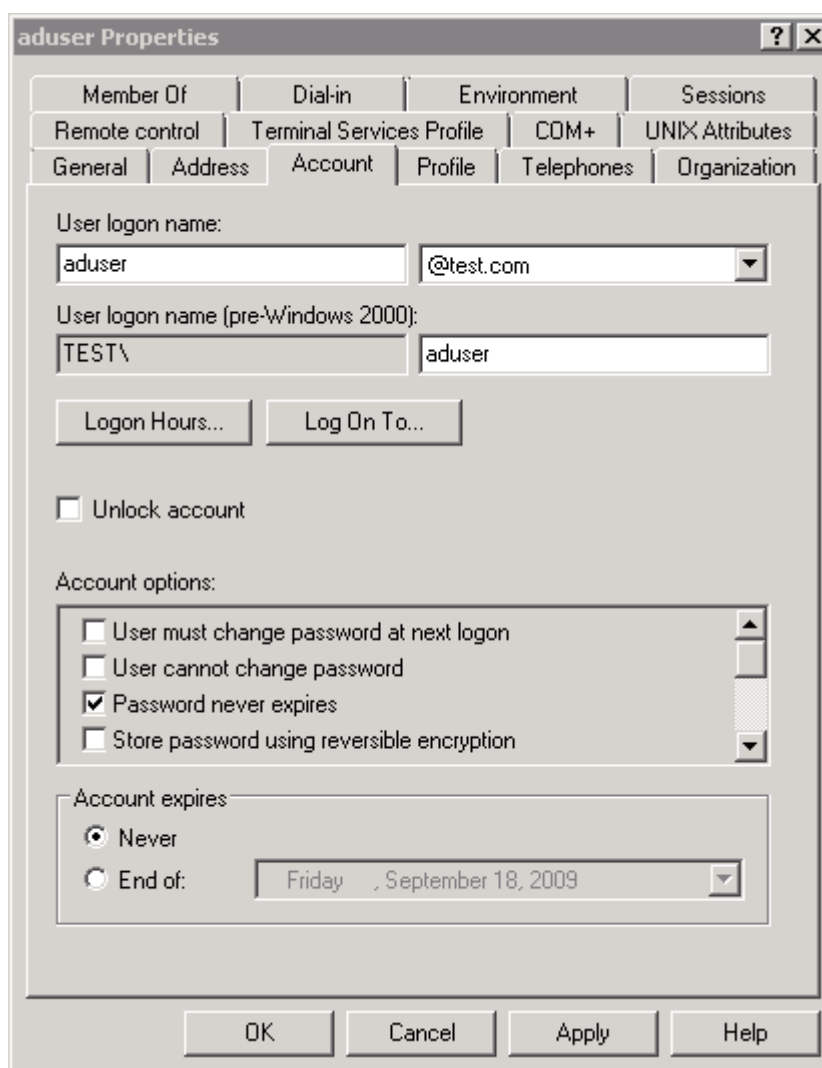


Figure 2.3 ccm Properties dialog

- **DNS Configuration**

Add CCM server into the Forward Lookup Zone.

Open DNS MMC, right click on your DNS in Forward Lookup Zones, select New Host. See figure 2.4.

Fill in Name and IP address in IP Host editor. See figure 2.5.

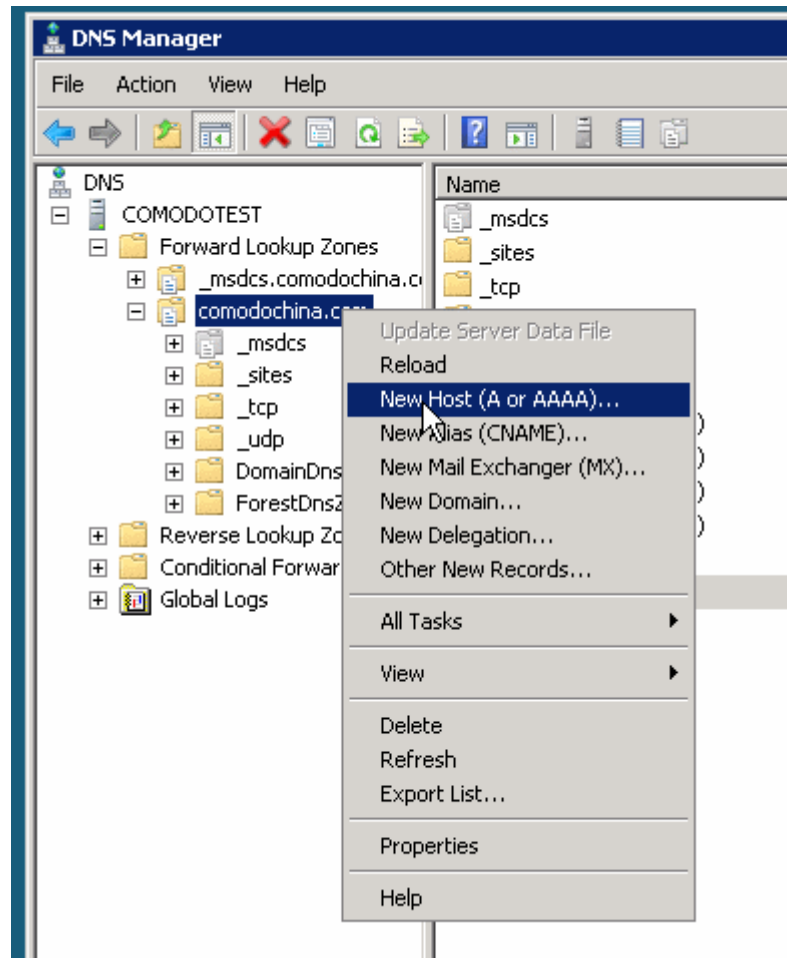


Figure 2.4 Create a new host

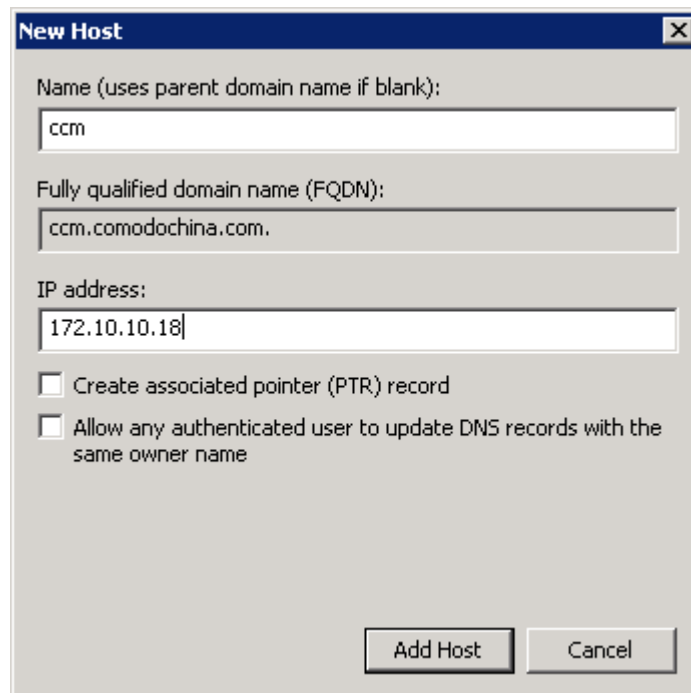


Figure 2.5 New Host Editor dialog

To ensure that your client can run auto enrollment script successfully, please set the Domain Controller's IP address (If DNS service is installed on the same server) as the Preferred DNS Server on the client computer. See figure 2.6.

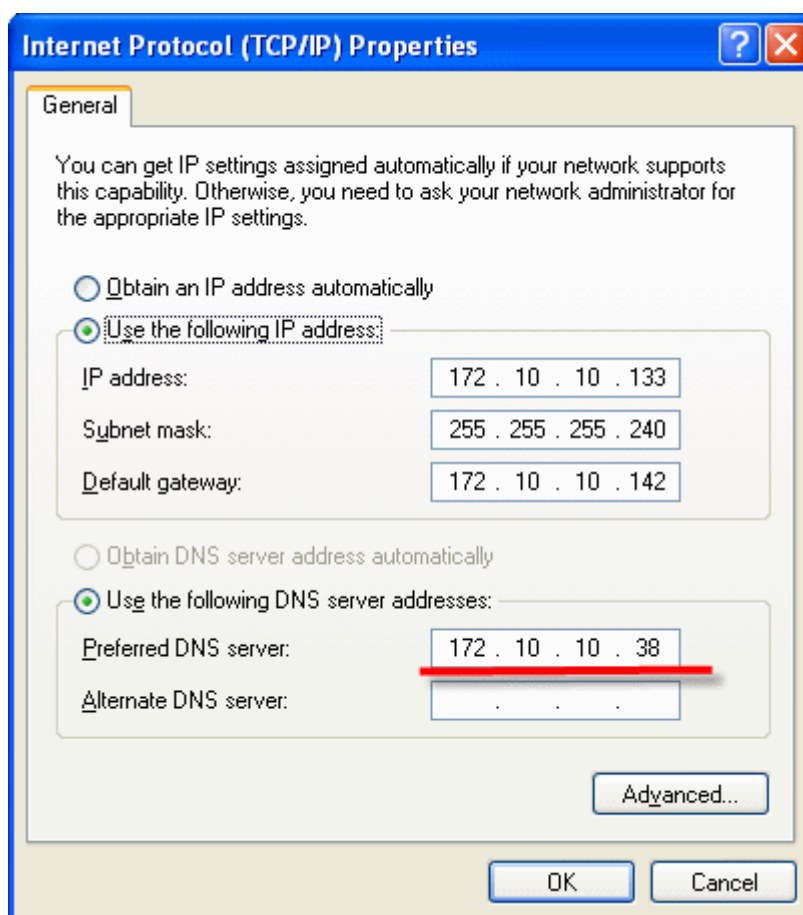


Figure 2.6 Setup Preferred DNS Server

If everything is OK, run "ping ccm" command from the client computer to validate. See figure 2.7.

```
C:\Users\zhoujian>ping ccm

Pinging ccm.comodocn.com [172.10.10.18] with 32 bytes of data:
Reply from 172.10.10.18: bytes=32 time=5ms TTL=63
Reply from 172.10.10.18: bytes=32 time=11ms TTL=63
Reply from 172.10.10.18: bytes=32 time=2ms TTL=64
Reply from 172.10.10.18: bytes=32 time=2ms TTL=64

Ping statistics for 172.10.10.18:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 11ms, Average = 5ms
```

Figure 2.7 Ping ccm server

- **Create keytab file and add new Service Principal Name**

In Windows Server 2003, ktpass command is not installed by default. You should install Windows Support Tools on the Domain Controller to get ktpass command.

Use ktpass command to create the user keytab file for the ccm server.

```
ktpass -princ HTTP/[CCM_DOMAIN_NAME]@[REALM_NAME] -mapuser [DOMAIN_USERNAME] -crypto DES-CBC-MD5 -ptype KRB5_NT_PRINCIPAL -mapop set +desonly -pass [PASSWORD] -out ccm.keytab
```

CCM_DOMAIN_NAME: host name in the DNS Forward Lookup Zone.

REALM_NAME: Windows Domain name.

DOMAIN_USERNAME: user name created for Certificate Manager server in chapter 2.1.

PASSWORD: password of the user created for Certificate Manager server in chapter 2.1.

For example:

```
ktpass -princ HTTP/ccm@TEST.COM -mapuser aduser -crypto DES-CBC-MD5 -ptype KRB5_NT_PRINCIPAL -mapop set +desonly -pass password -out ccm.keytab
```

Use setspn command to set Service Principal Name for the user 'aduser'

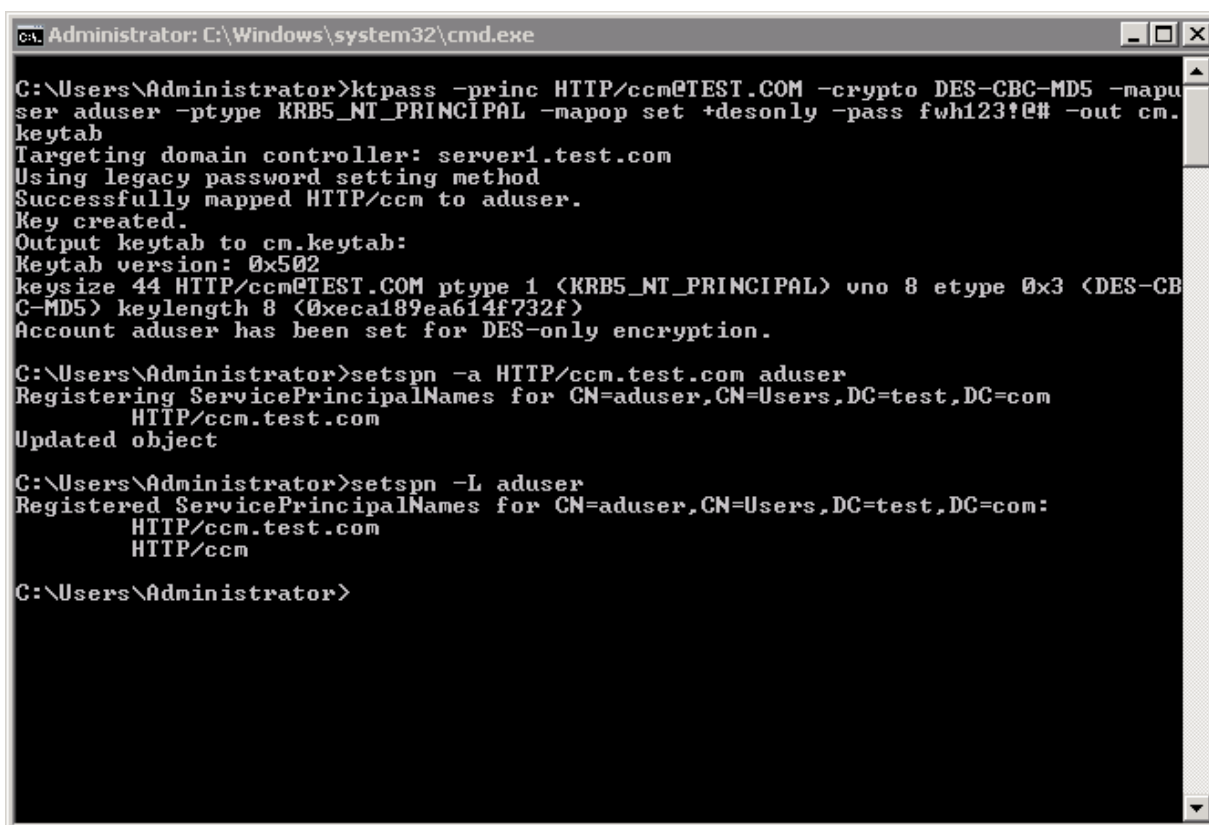
```
setspn -a HTTP/[FQDN] [DOMAIN ACCOUNT]
```

FQDN: Full Qualified Domain Name of CCM server in the DNS Forward Lookup Zone.

For example:

```
setspn -a HTTP/ccm.test.com aduser
```

Run 'setspn -l aduser' to check the Service Principal Names for user aduser.



```
Administrator: C:\Windows\system32\cmd.exe
C:\Users\Administrator>ktpass -princ HTTP/ccm@TEST.COM -crypto DES-CBC-MD5 -mapu
ser aduser -ptype KRB5_NT_PRINCIPAL -mapop set +desonly -pass fwh123!@# -out cm.
keytab
Targeting domain controller: server1.test.com
Using legacy password setting method
Successfully mapped HTTP/ccm to aduser.
Key created.
Output keytab to cm.keytab:
Keytab version: 0x502
keysize 44 HTTP/ccm@TEST.COM ptype 1 <KRB5_NT_PRINCIPAL> vno 8 etype 0x3 <DES-CB
C-MD5> keylength 8 <0xec189ea614f732f>
Account aduser has been set for DES-only encryption.

C:\Users\Administrator>setspn -a HTTP/ccm.test.com aduser
Registering ServicePrincipalNames for CN=aduser,CN=Users,DC=test,DC=com
HTTP/ccm.test.com
Updated object

C:\Users\Administrator>setspn -L aduser
Registered ServicePrincipalNames for CN=aduser,CN=Users,DC=test,DC=com:
HTTP/ccm.test.com
HTTP/ccm

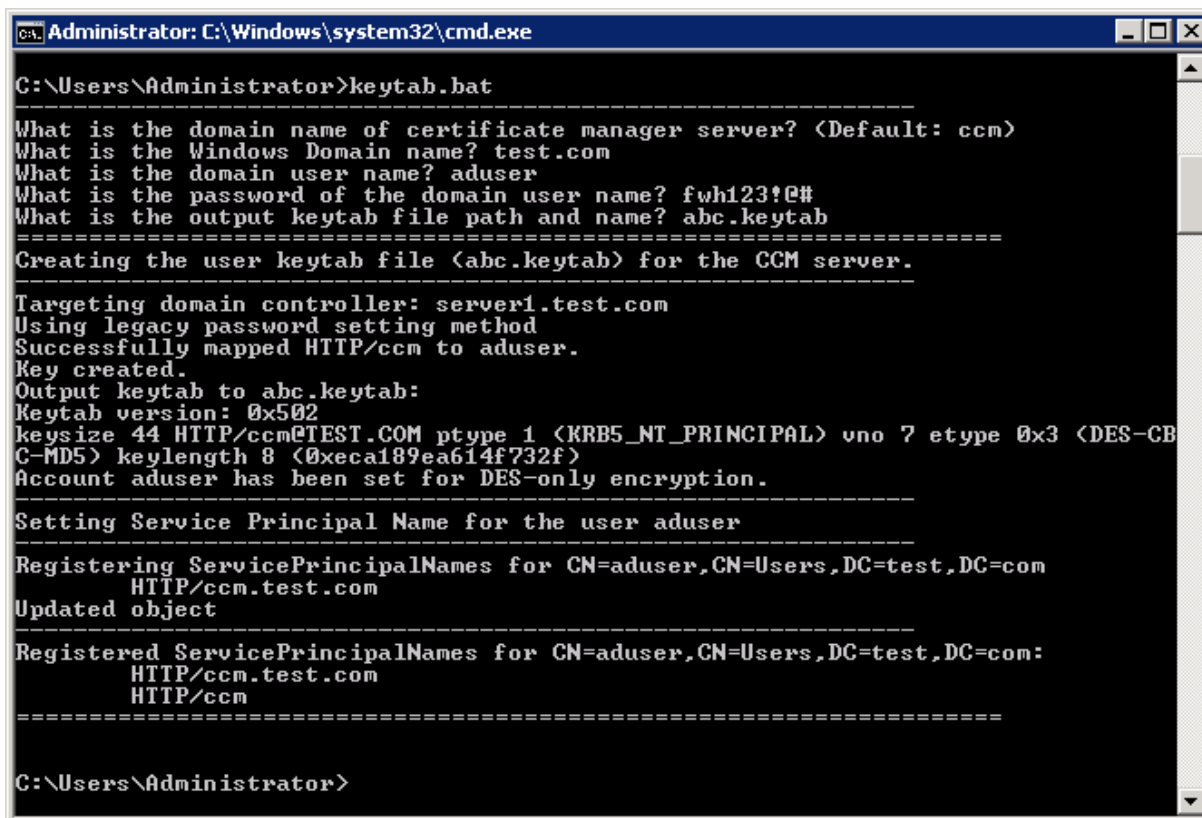
C:\Users\Administrator>
```

Figure 2.8 Create SPNs for CCM server

- **Use keytab.bat to create keytab file automatically**

Before running keytab.bat make sure you have ktpass command installed on server.

Open up Command Prompt window, navigate to the directory where keytab.bat resides in, run keytab.bat and following the questions as shown in Figure 2.9.



```
Administrator: C:\Windows\system32\cmd.exe
C:\Users\Administrator>keytab.bat
-----
What is the domain name of certificate manager server? (Default: ccm)
What is the Windows Domain name? test.com
What is the domain user name? aduser
What is the password of the domain user name? fwh123!@#
What is the output keytab file path and name? abc.keytab
-----
Creating the user keytab file (abc.keytab) for the CCM server.
-----
Targeting domain controller: server1.test.com
Using legacy password setting method
Successfully mapped HTTP/ccm to aduser.
Key created.
Output keytab to abc.keytab:
Keytab version: 0x502
keysize 44 HTTP/ccm@TEST.COM ptype 1 (KRB5_NT_PRINCIPAL) vno 7 etype 0x3 (DES-CB
C-MD5) keylength 8 (0xecal89ea614f732f)
Account aduser has been set for DES-only encryption.
-----
Setting Service Principal Name for the user aduser
-----
Registering ServicePrincipalNames for CN=aduser,CN=Users,DC=test,DC=com
HTTP/ccm.test.com
Updated object
-----
Registered ServicePrincipalNames for CN=aduser,CN=Users,DC=test,DC=com:
HTTP/ccm.test.com
HTTP/ccm
-----
C:\Users\Administrator>
```

Figure 2.9 Create keytab automatically

Copy the generated keytab file to the CCM server.

(for example : `/home/daniel/ccm.keytab` in Linux System)

After `ktpass` executes successfully, `aduser`'s properties will change to `HTTP/ccm`. See figure 2.10.

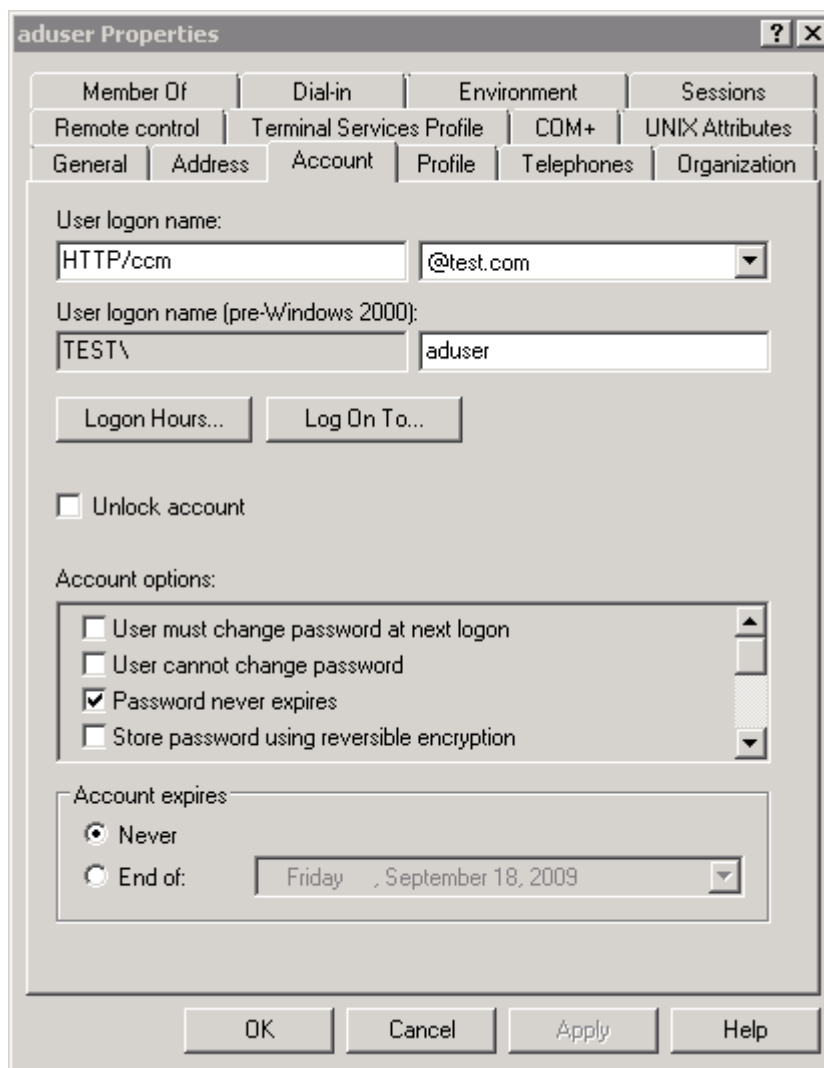


Figure 2.10 ccm's Properties dialog

2.2. Create/Modify login.conf in Certificate Manager

Access CCM SuperAdmin page, open Settings/Autoenrollment Tab.

Click "Add"/ "Edit" button to add/edit KDC configuration to login.conf.

After making changes to properties here, click the "Save" button to apply. The login.conf file in CCM/conf will be created/updated. See figures 2.11 and 2.12.

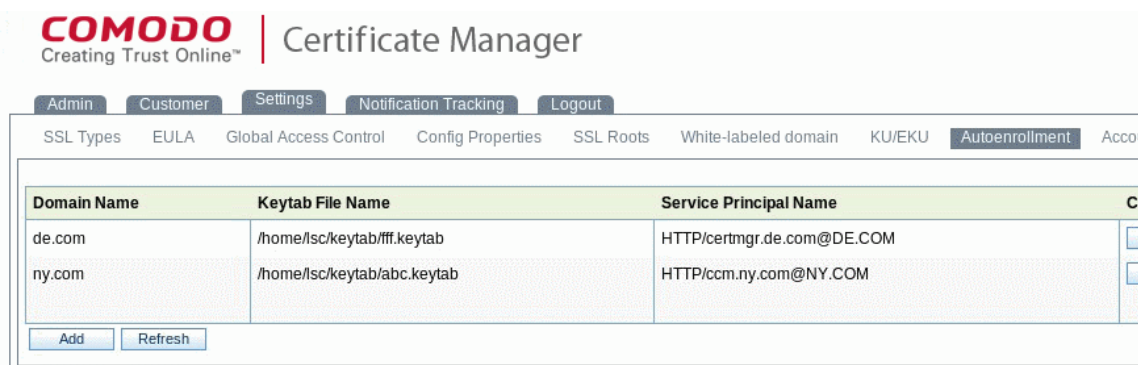


Figure 2.11 Autoenrollment view

Figure 2.12 Add/Edit Autoenrollment properties

Domain Name : Windows Server's Domain name.

Keytab File Name : Keytab file location and name.

Service Principal Name : principal should be the one defined in the above ktpass command.

IMPORTANT: If CCM will be deployed under Windows system, please change the file path form to Windows form. e.g. "C:/kerberos/ccm.keytab"

2.3. Configure Active Directory Properties in CCM Server

Certificate Manager server will use the user 'ccm' (that created above) to access Active Directory.

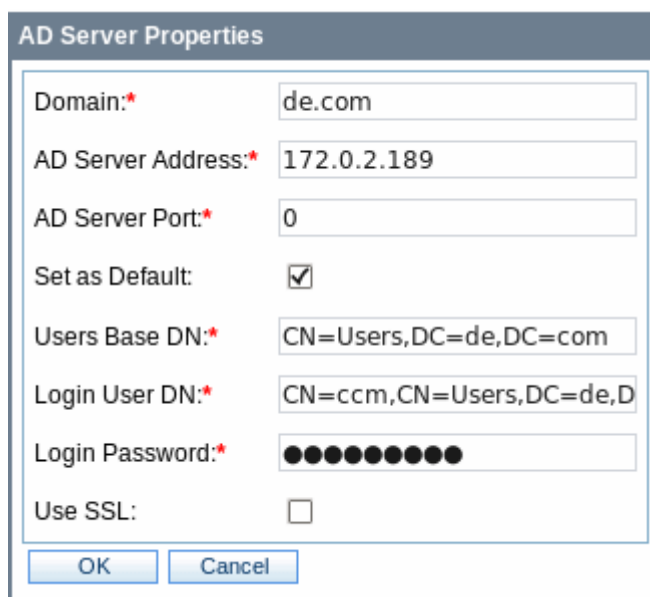
You can add/create Active Directory properties in Customer page under Settings/AD Server tab. See figures 2.13 and 2.14.

Domain	AD Server	Port	Use SSL	Organization/Department	Setup By Comodo
de.com (Default)	172.0.2.189	0	<input type="checkbox"/>	System	Yes
test.com	172.0.0.123	0	<input type="checkbox"/>		No

Figure 2.13 AD Server view

You can import your AD servers from CSV. Also you can click the 'Verify' button to verify if the AD server can be connected successfully or not.

Upon clicking 'Edit' button, you can enter all the properties in the pop up window:



Domain:*	de.com
AD Server Address:*	172.0.2.189
AD Server Port:*	0
Set as Default:	<input checked="" type="checkbox"/>
Users Base DN:*	CN=Users,DC=de,DC=com
Login User DN:*	CN=ccm,CN=Users,DC=de,D
Login Password:*	●●●●●●●●●●
Use SSL:	<input type="checkbox"/>

Figure 2.14 Setup AD server properties

Domain: the domain name use for auto enrollment

AD Server Address: Active Directory Server's IP address or DNS name

AD Server Port: Active Directory Server's LDAP port, default port 389 for non-SSL port and 636 for SSL port)

Set as Default: Mark current AD Server as Customer's default

Users Base DN: Distinguish Name of the user object in Active Directory

e.g. CN=Users, DC=comodo, DC=com

Login User DN: Distinguish Name of the user you just created in Active Directory

e.g. CN=ccm, CN=Users, DC=comodo, DC=com

Login Password: password of the user you've just created in AD for ccm server

Use SSL: check it if you want to use SSL to access Active Directory

(You have to enable SSL access for Active Directory first)

IMPORTANT: You must mark at least one AD Server as default. If CCM can't find ADServer that bind to your organization during auto enrollment, CCM will use the default one.

To bind AD Server to organization:

Access CCM Customer page, open Settings Tab and then Organizations Tab, press Edit button. See figure 2.15.

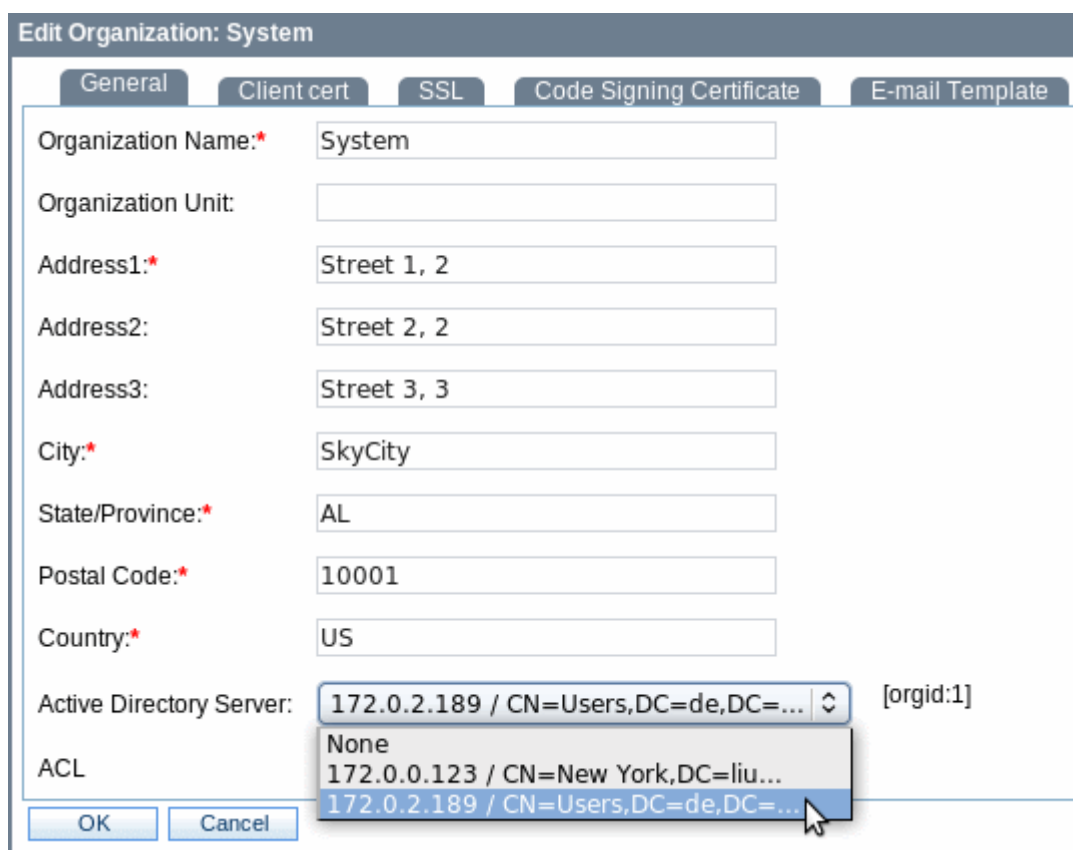


Figure 2.15 Bind AD Server

2.4. Synchronize Time between CCM Server and Domain Controller

If CCM server manages one Windows domain, just need CCM server to synchronize time with Domain Controller; If CCM server manages multiple domains we need all Domain Controllers and CCM server to synchronize time with one global NTP server.

2.5. Restart Comodo Certificate Manager

If everything is OK, Windows domain user can visit the auto enrollment service now.

IMPORTANT: Access from the outside to the Windows domain will get an error message:

“This request requires HTTP authentication ().”

3. Deploy Script on Windows Server

3.1. VBScript Properties Configuration

Edit *autoenroll.conf* in *vbscript* package:

requestpath : Certificate Manager auto enrollment service URL

issusername : issuer name in certificate which will be issued by Comodo CA

days(optional) : days left before certificate's expiration date

e.g. If the value is 20 and expiration date is 6/30/2008, then on 6/10/2008 vbscript will enroll new certificate and revoke the old one.

domainname: Windows Domain Name

customeruri : Customer's uri in CCM

orgid(optional): Organization id in CCM

3.2. Open Group Policy Editor

- In Windows Server 2003 EE

Open Active Directory Users and Computers Snap-In. See figure 3.1.

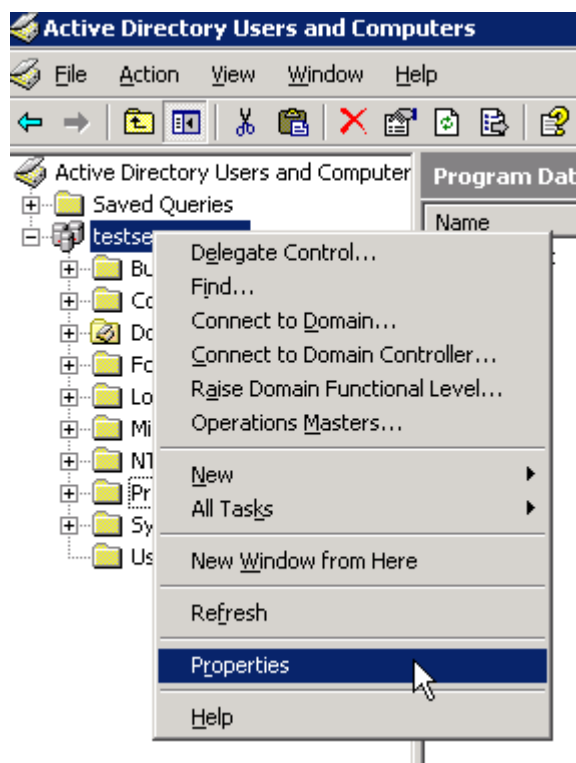


Figure 3.1 Open properties dialog of domain

Right click on the domain name->Properties

Properties dialog will pop up. See figure 3.2.

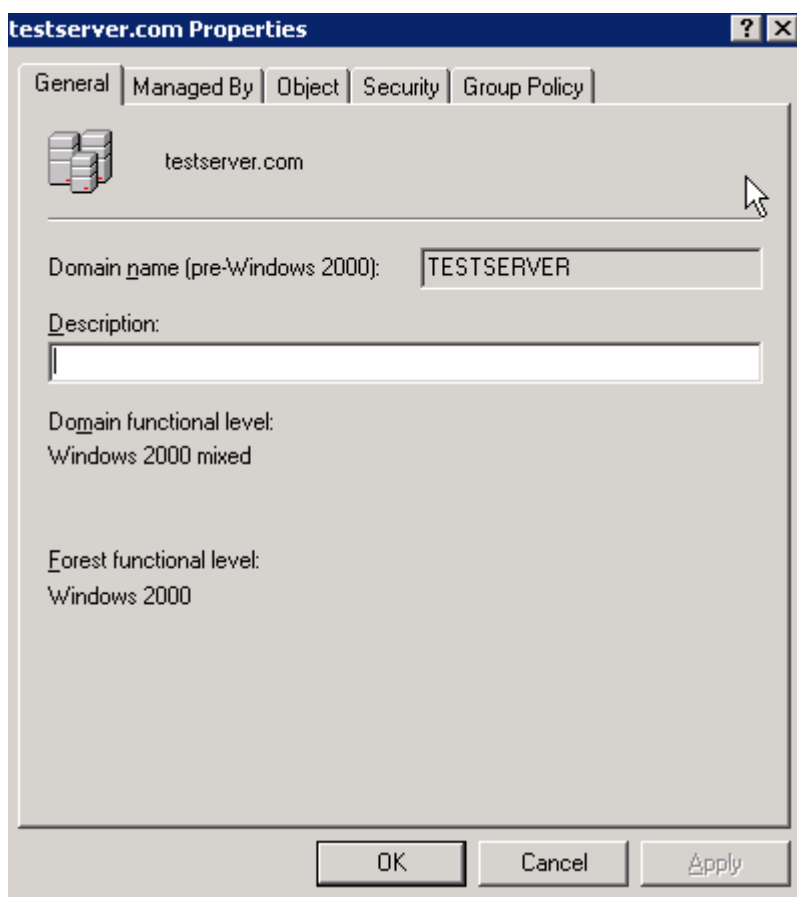


Figure 3.2 Domain properties

Select Group Policy tab then Choose Default Domain Policy and Click Edit See figure 3.3.

IMPORTANT: If modification of Default Domain Policy is not acceptable, you can create new Group Policy Object for this.

Group Policy Object Editor will pop up. See figure 3.4.

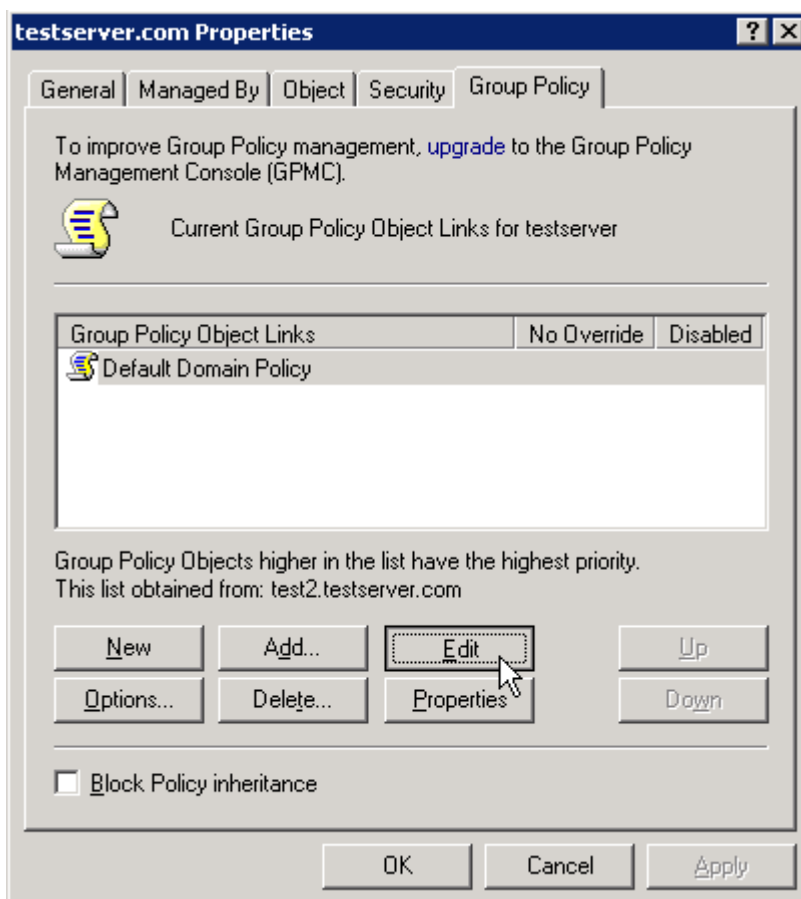


Figure 3.3 Open Default Domain Policy

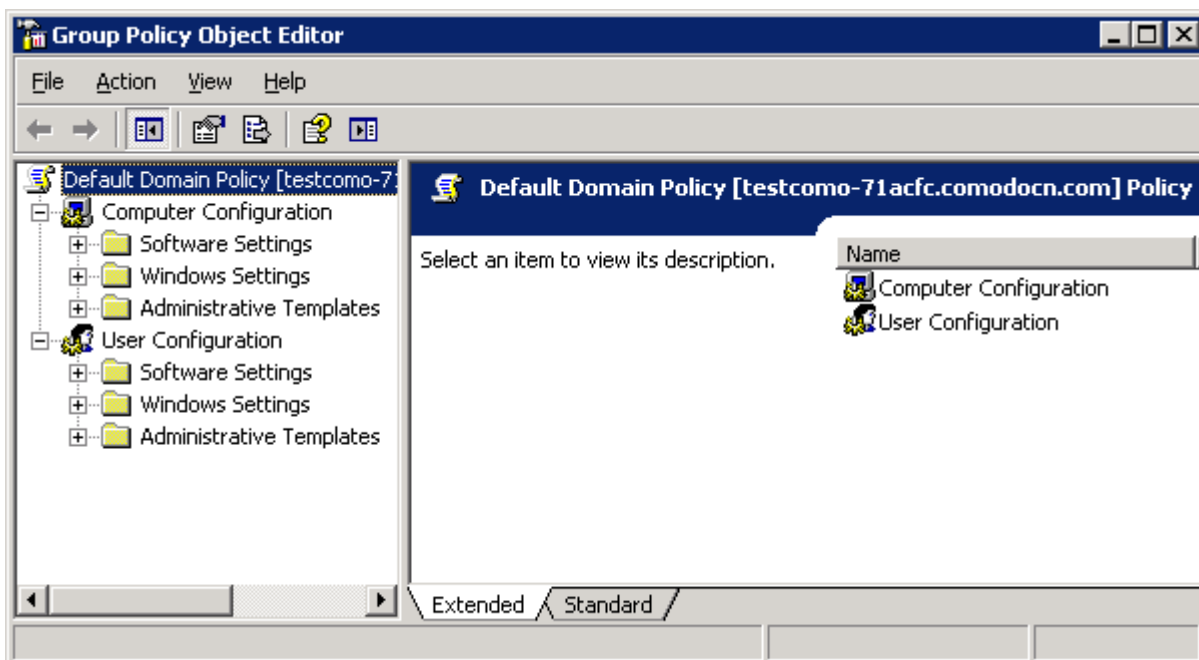


Figure 3.4 Group Policy Object Editor

- **In Windows Server 2008**

Open Group Policy Management, navigate to Forest->Domains->your domain->Group Policy Objects, right click on Default Domain Policy and click Edit. See figure 3.5.

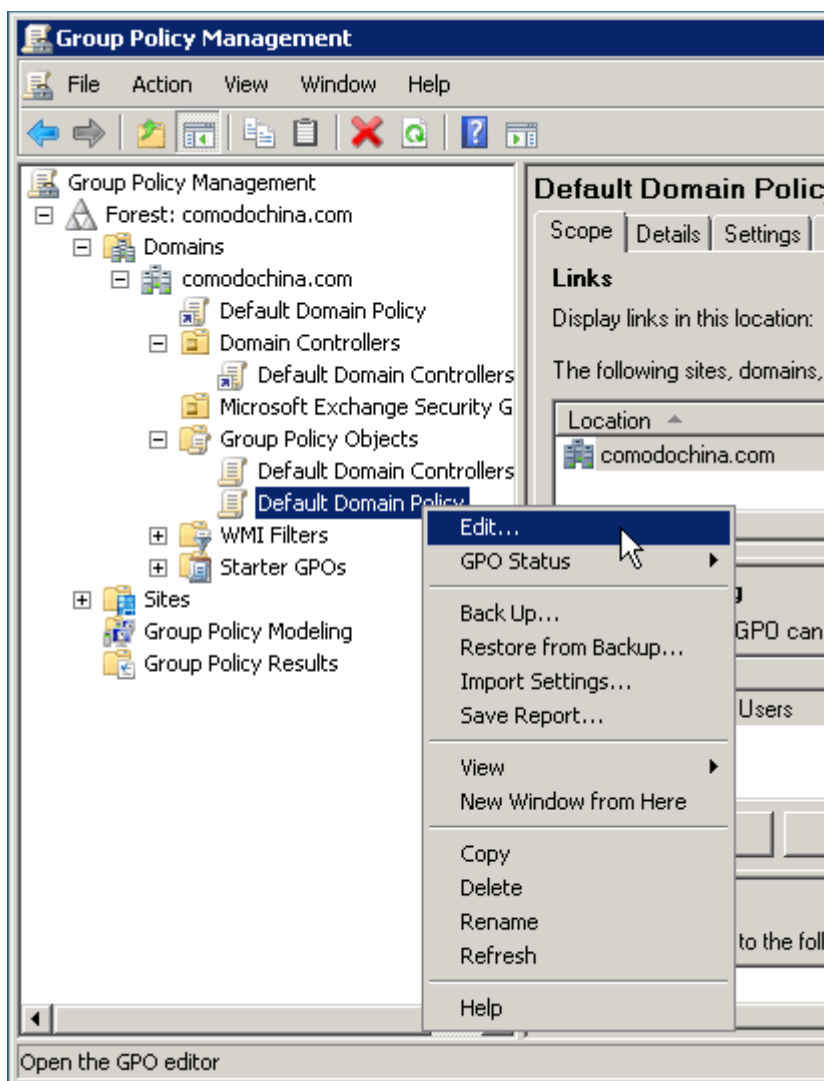


Figure 3.5 Group Policy Management

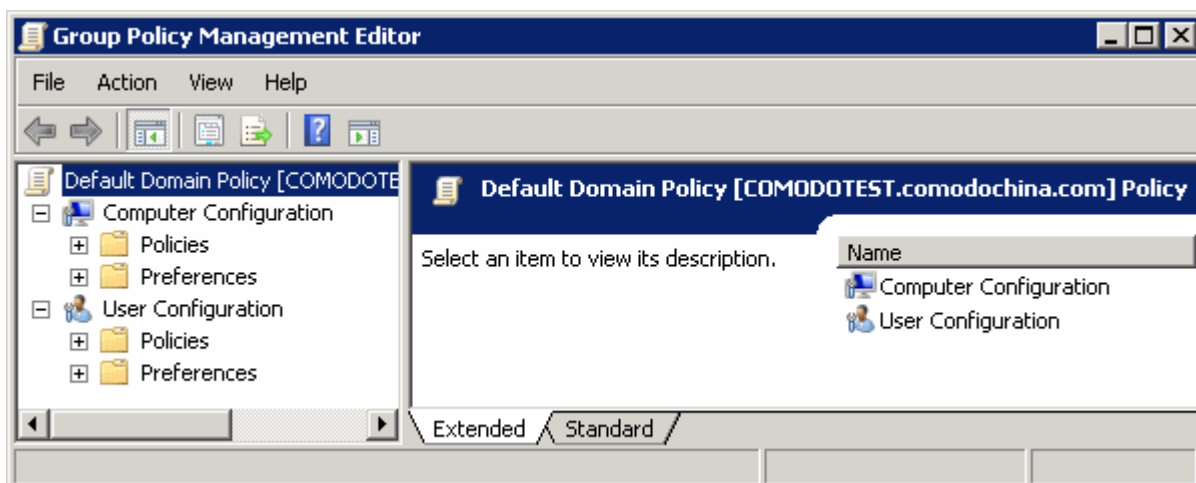


Figure 3.6 Group Policy Management Editor in Windows Server 2008

3.3. Edit Logon Script Properties

Open logon script properties, click User Configuration->Windows Settings->Scripts->Logon

In Windows Server 2008 click User Configuration->Policies->Windows Settings->Scripts->Logon

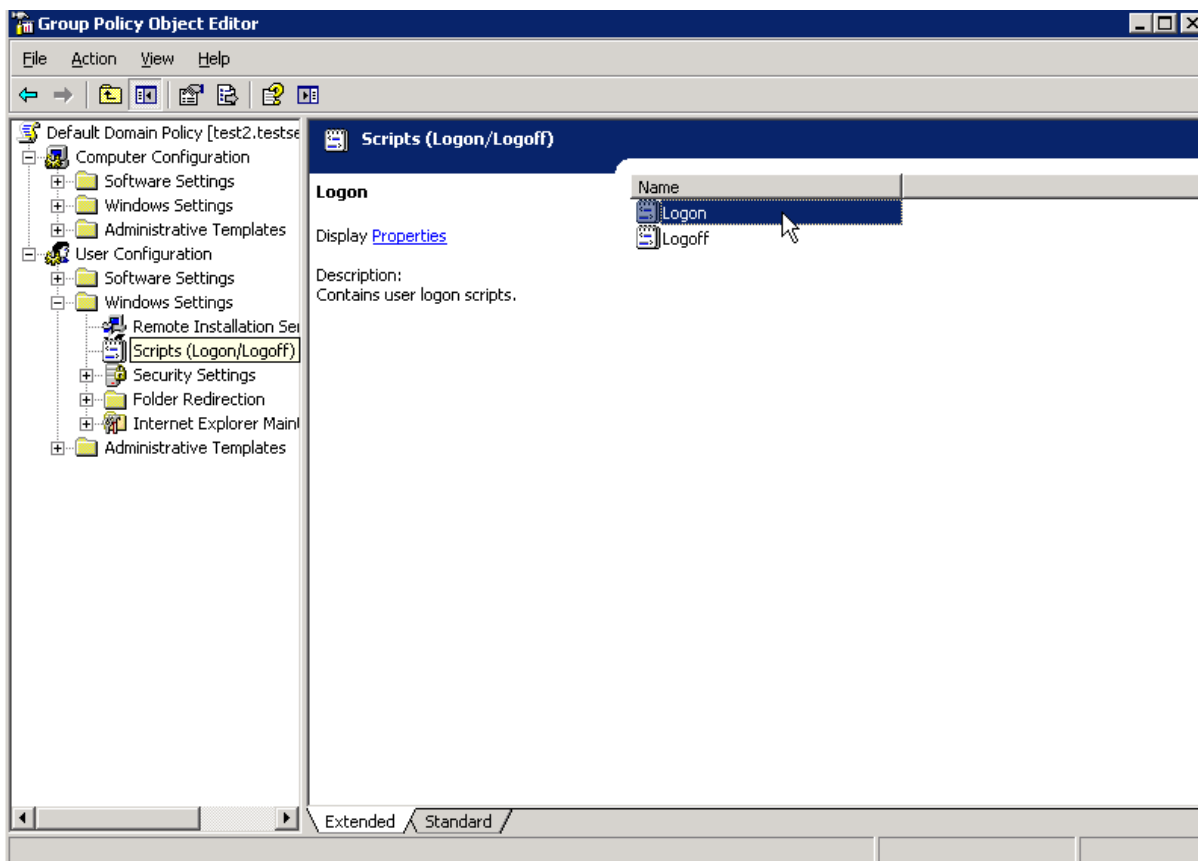


Figure 3.7 Open Logon Properties

Logon Properties dialog will pop up. See figure 3.8.

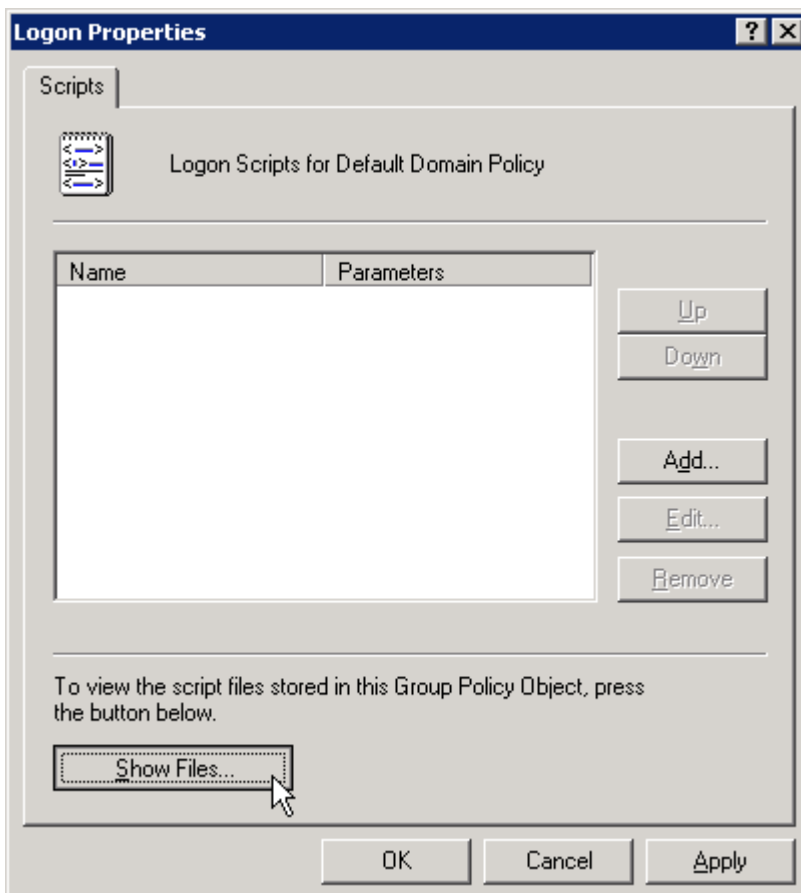


Figure 3.8 Logon Properties

In figure 3.8 click Show Files will open the default script directory, see figure 3.9.

Copy all script files into this directory.

Script File List:

autoenroll.conf

certadmin.dll

certcli.dll

certreq.exe

certutil.exe

ExchangeEnroll.vbs

IMPORTANT: Both autoenroll.conf and ExchangeEnroll.vbs should be updated to Windows Server when there is new version.

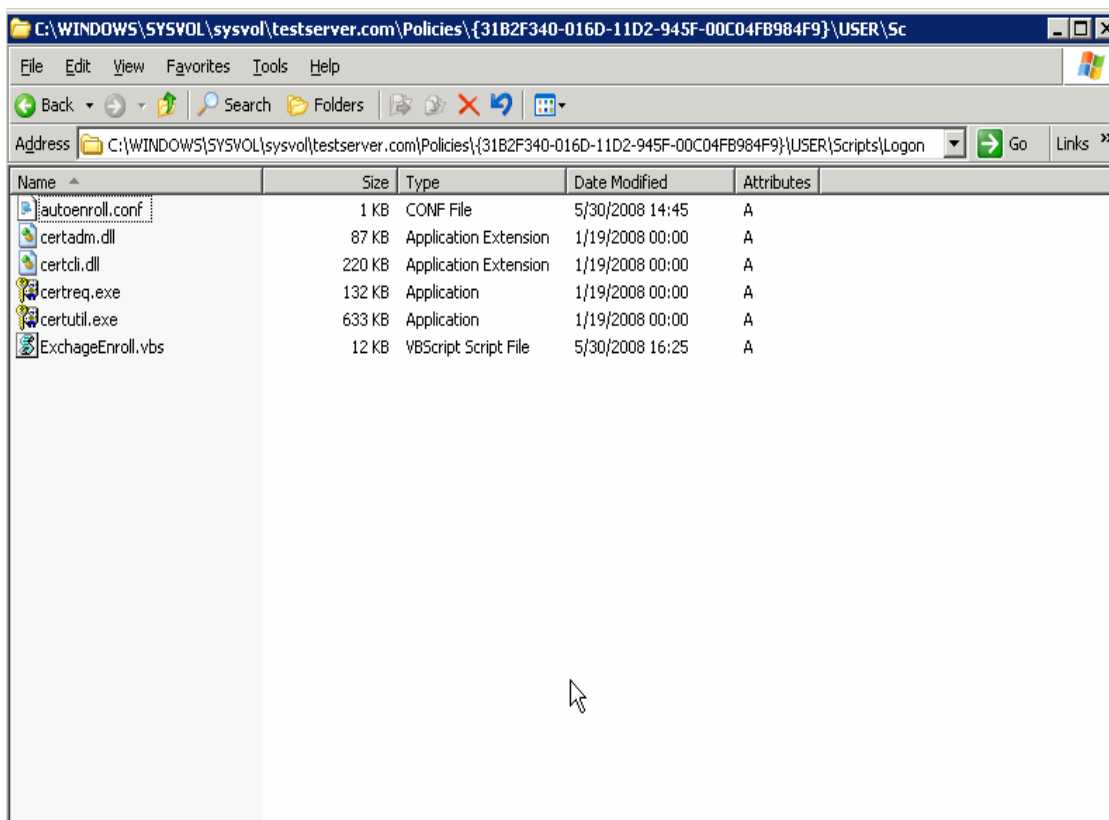


Figure 3.9 Logon script directory

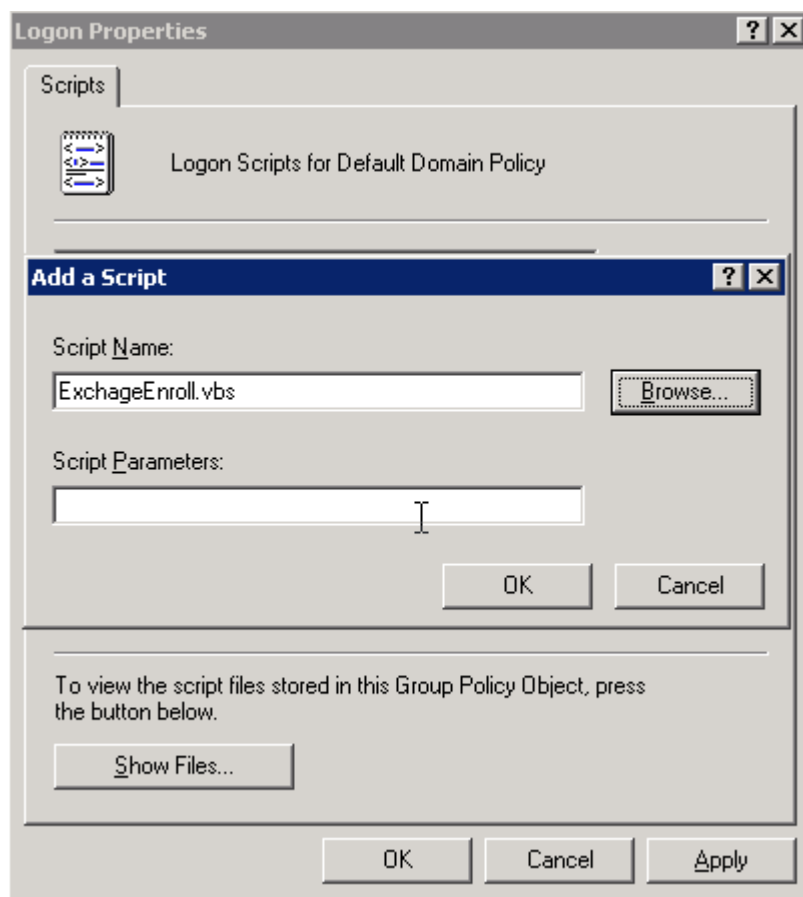


Figure 3.10 Add a Script to Logon process

Add ExchangeEnroll.vbs script to Logon Scripts for Default Domain Policy. See Figure 3.10.

3.4. Distribute capicom.dll

- Create a Distribution Point

To publish or assign a computer program, you must create a distribution point on the publishing server:

- Log on to the server computer as an administrator.
- Create a shared network folder in which to place the Microsoft Software Installer (MSI) package that you want to distribute. (For example : c:\dist\ copy capicom.msi to this directory)
- Set permissions on the share to allow access to the distribution package.
- Assign a Package
 - Click the Group Policy tab, select the group policy object that you want, and then click Edit. See figure 3.11.
 - Under **Computer Configuration**, expand **Software Settings**.
 - Right-click **Software installation**, point to New, and then click **Package**.
 - In the **Open** dialog box, type the full Universal Naming Convention (UNC) path to the shared folder that contains the MSI package that you want. See figure 3.12.
e.g. \\test2\dist\capicom.msi

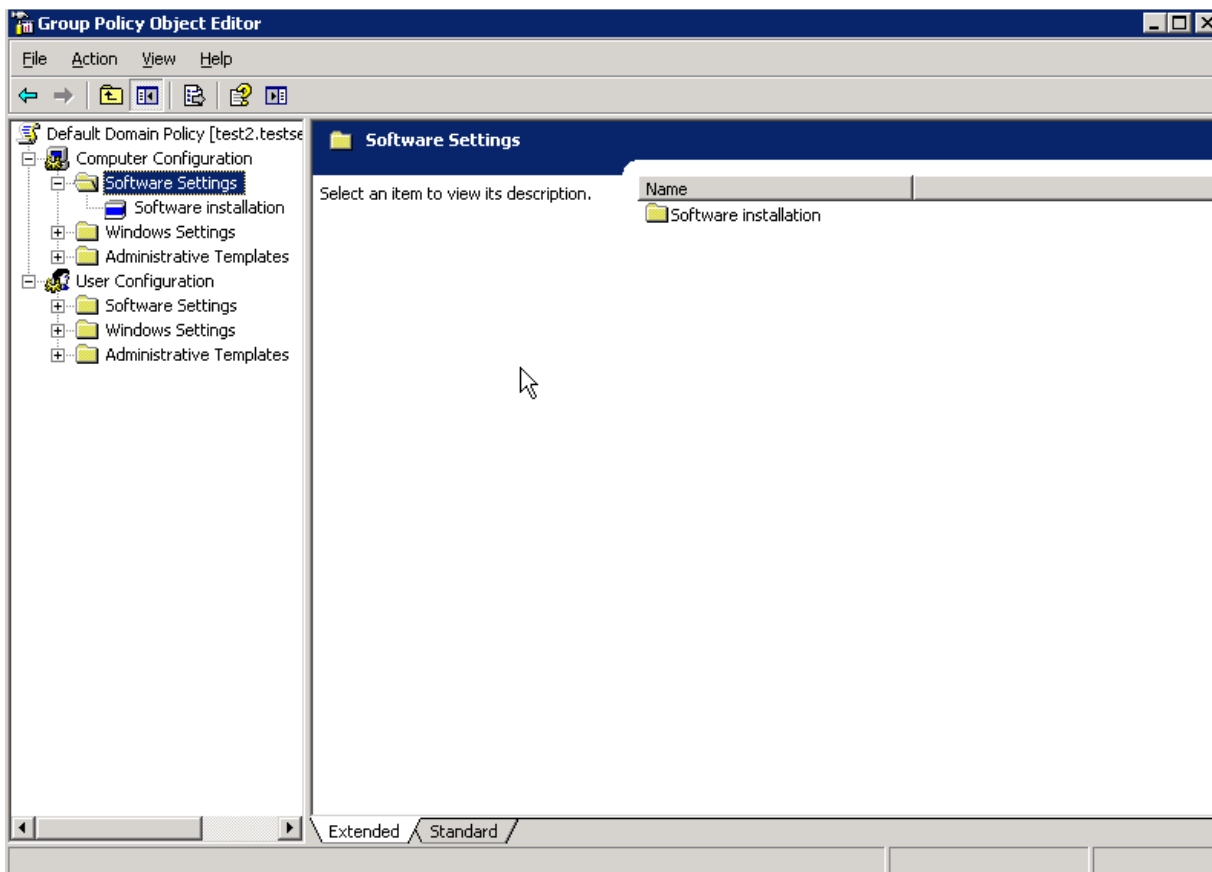


Figure 3.11 Open Software Installation

IMPORTANT: Do not browse to the location. Ensure that you use the UNC path to the shared folder. See figure 3.12.

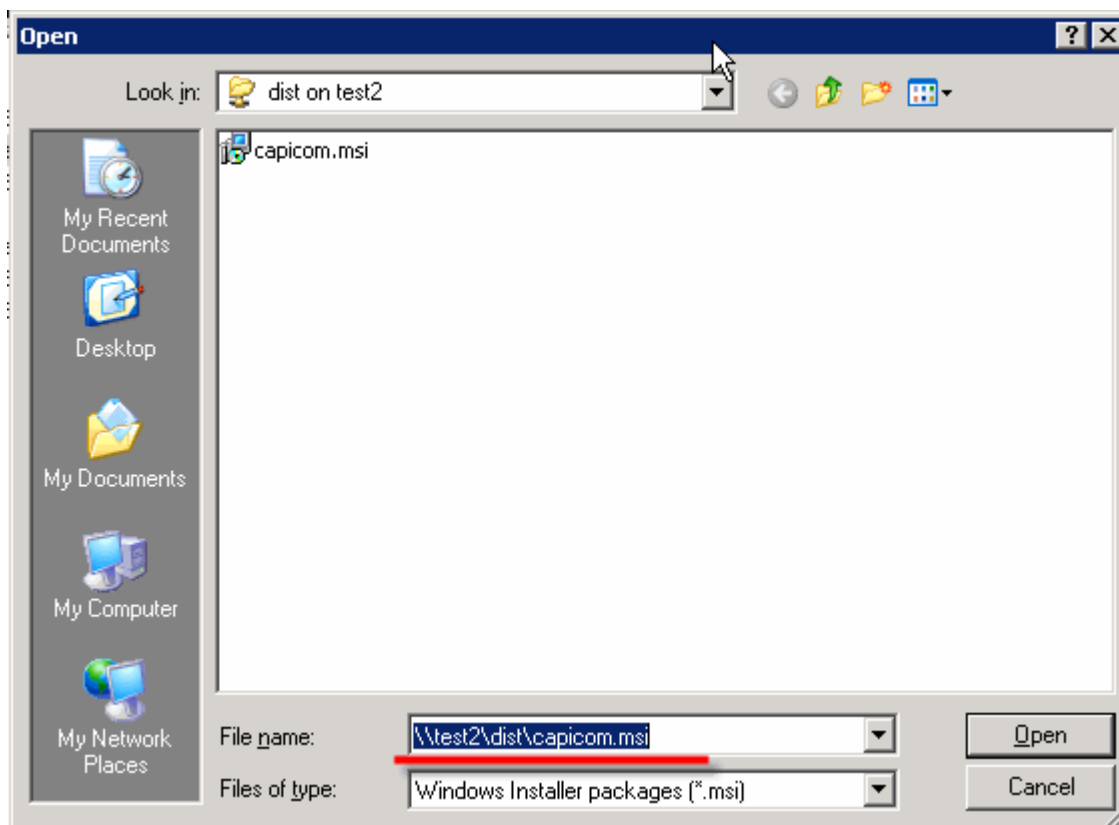


Figure 3.12 Select capicom.msi

- Click Open and Click Assigned, and then click OK. The package is listed in the right pane of the Group Policy window. See figure 3.13.

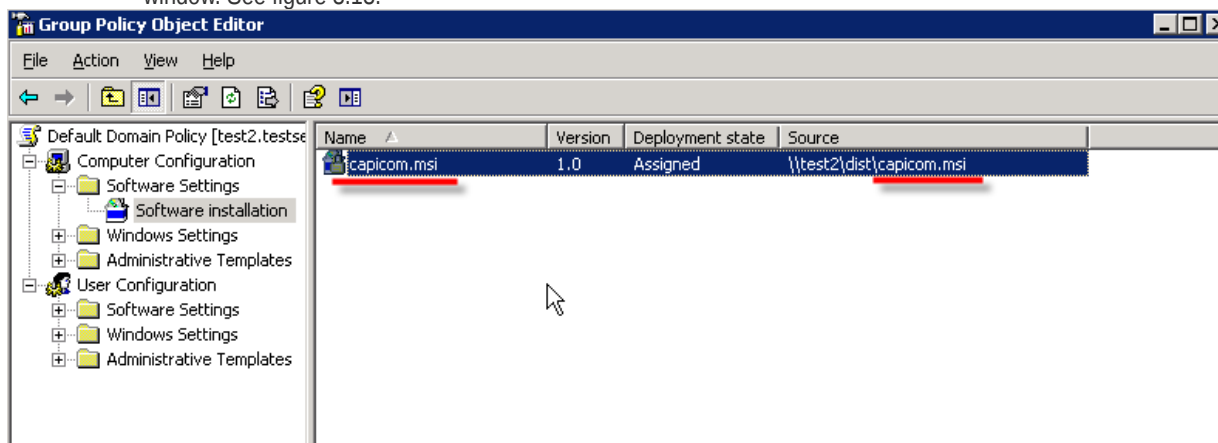


Figure 3.13 capicom.msi is added to Group Policy

- Close the Group Policy snap-in, click OK, and then quit the Active Directory Users and Computers snap-in. When the client computer starts, the managed software package is automatically installed to default install path C:\Program Files\Comodo\CapicomInstaller\

3.5. Set Trusted Sites Policy

Open Group Policy Object Editor, go to Computer Configuration->Administrative Templates->Windows Components->Internet Explorer->Internet Control Panel->Security Page

(In Windows Server 2008 navigate to Computer Configuration->Policies->Administrative Templates->Windows Components->Internet Explorer->Internet Control Panel->Security Page)

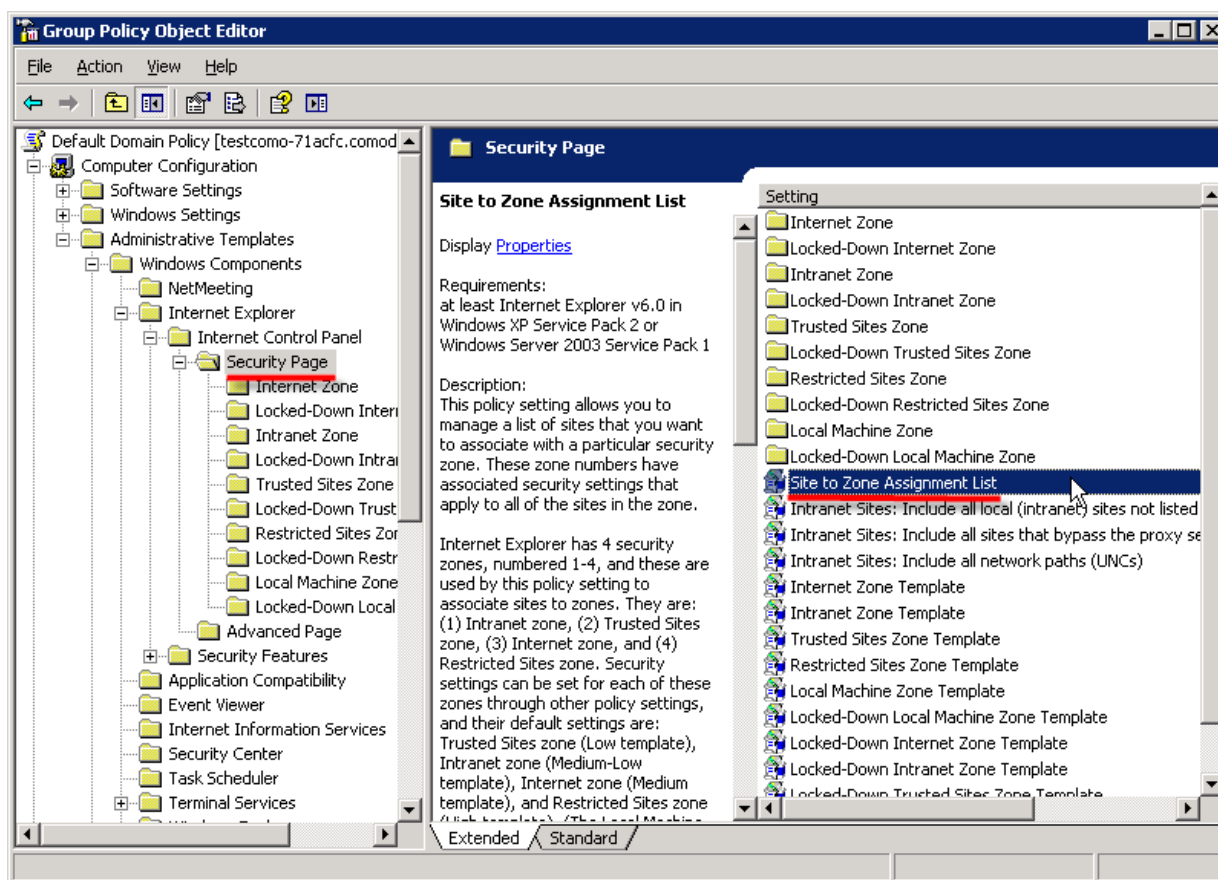


Figure 3.14 Open Site to Zone Assignment List

On the right panel, double click on Site to Zone Assignment List to open properties dialog. See figure 3.15.

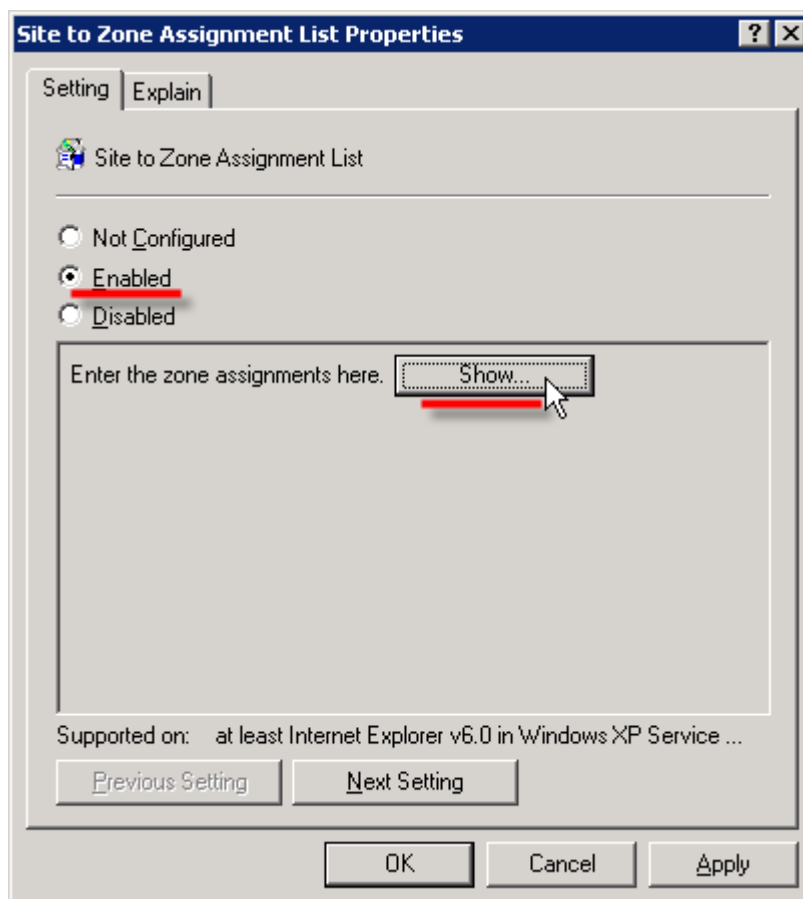


Figure 3.15 Site to Zone Assignment List Properties

On properties dialog check Enabled and press Show... button to open Show Contents dialog. See figure 3.16.

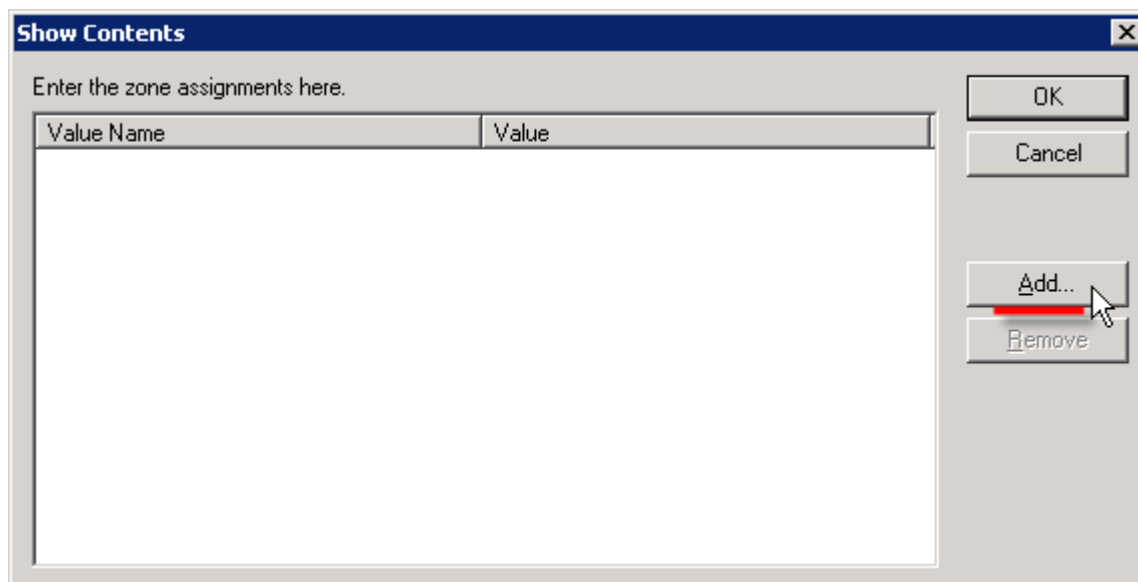


Figure 3.16 Add new zone assignment

Click Add.. to add new site to zone. See figure 3.17.

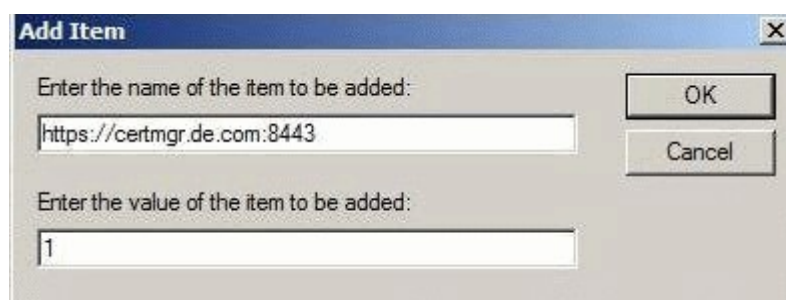


Figure 3.17 Add item

Enter Certificate Manager Server's URL in name field and put value 2 in value field, or value 1 for Windows Server 2008. Then press OK.

Add the same item in User Configuration->Administrative Templates->Windows Components->Internet Explorer->Internet Control Panel->Security Page

(In Windows Server 2008 navigate to User Configuration->Policies->Administrative Templates->Windows Components->Internet Explorer->Internet Control Panel->Security Page)

3.6. Deploy Trusted Root Certificates

Import Comodo CA's root certificate and CCM server's certificate to Group Policy.

Open Group Policy Object Editor, go to Computer Configuration->Windows Settings->Windows Security Settings->Public Key Policies->Trusted Root Certificate Authorities

(In Windows Server 2008 navigate to Computer Configuration->Policies->Windows Settings->Windows Security Settings->Public Key Policies->Trusted Root Certificate Authorities)

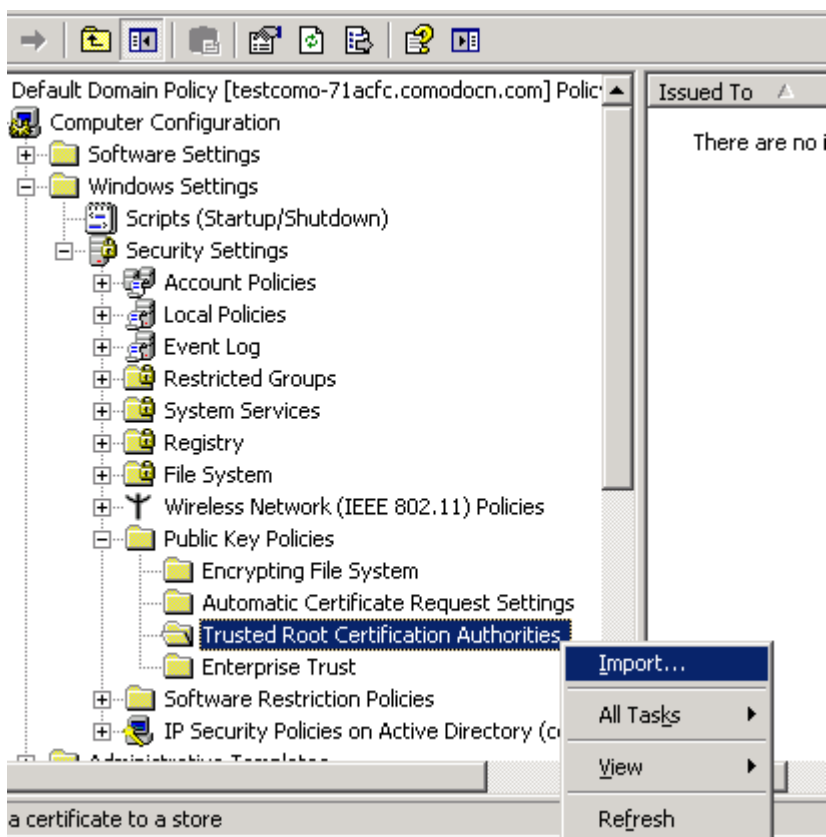


Figure 3.18 Navigate to Trusted Root Certificate Authorities

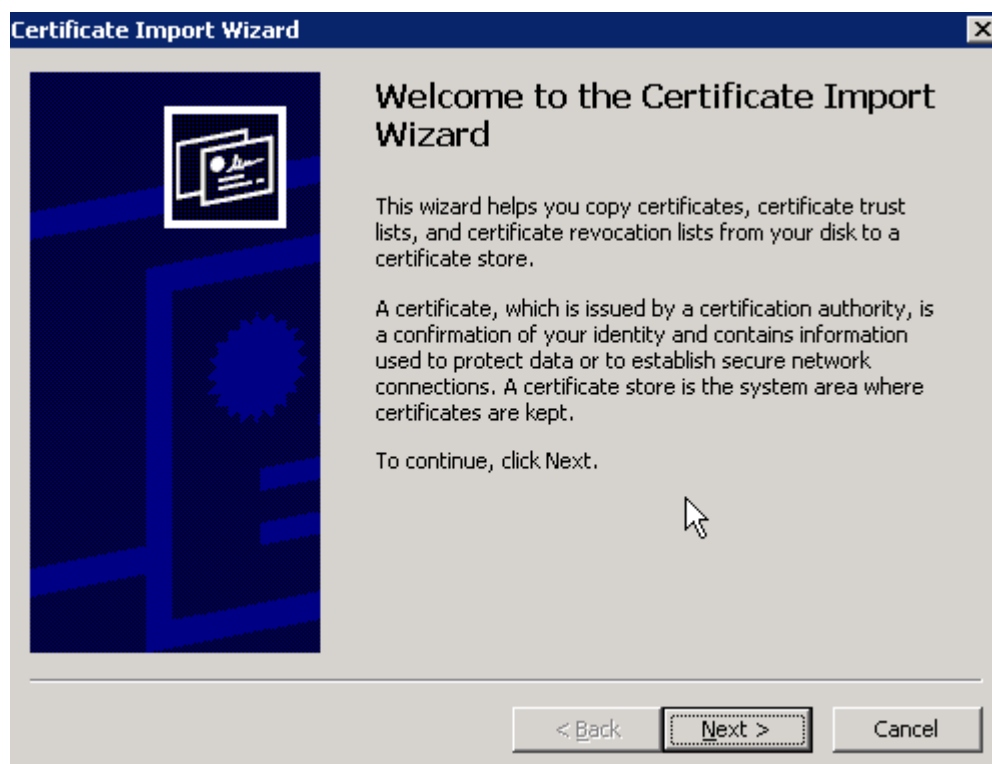


Figure 3.19 Certificate Import Wizard

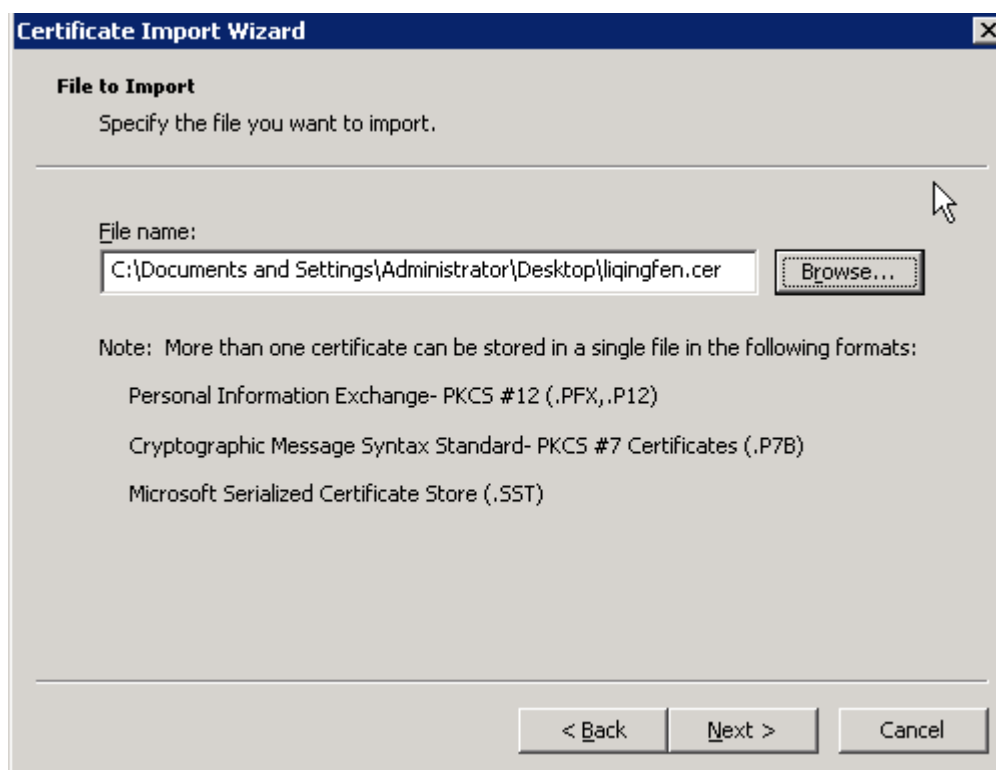


Figure 3.20 Select certificate file to import

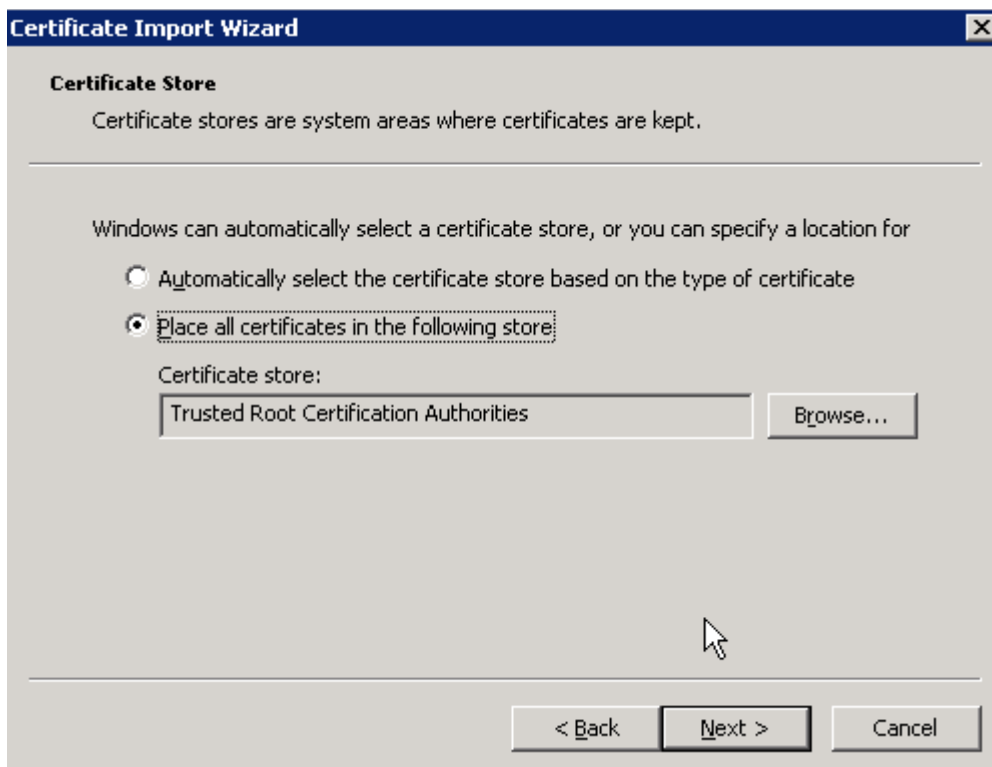


Figure 3.21 Select certificate store

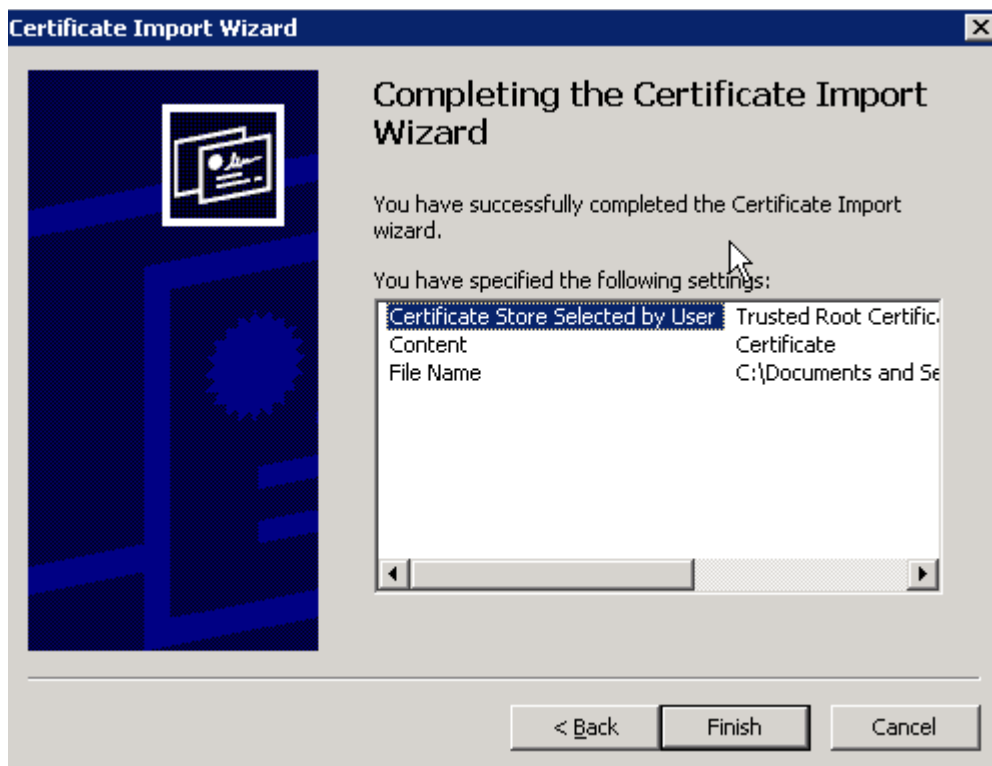


Figure 3.22 Completing the Certificate Import Wizard

After importing 2 certificates, you should see the 2 certificates in Group Policy. See figure 3.23.

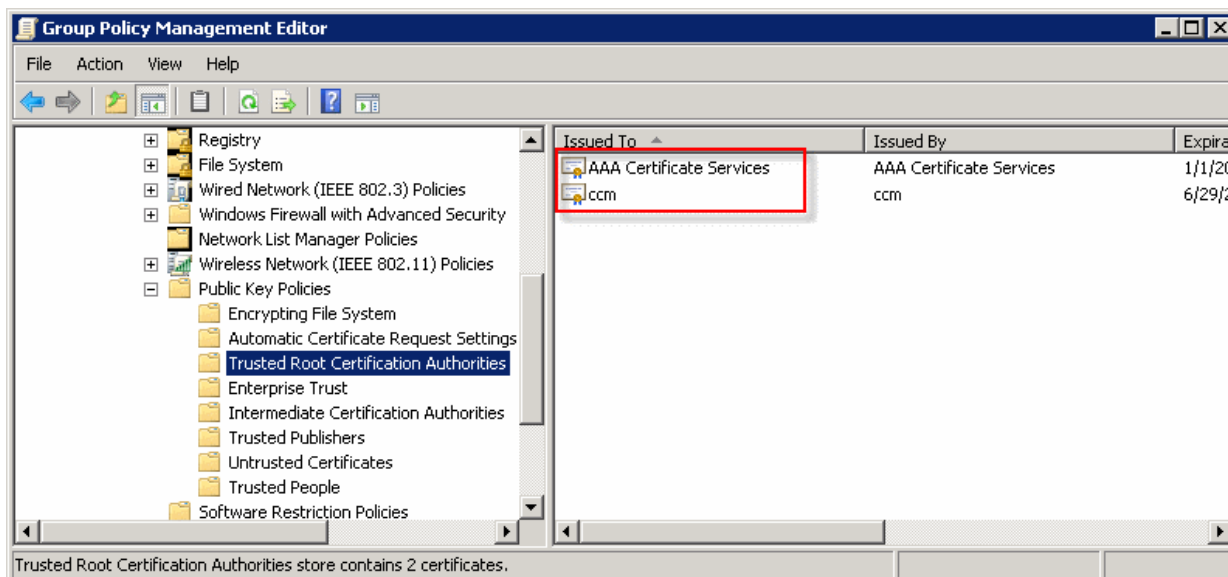


Figure 3.23 Imported 2 certificates in Group Policy

3.7. Create User Accounts on Active Directory with Email Box

user1 user1@yourcompany.com

user2 user2@yourcompany.com

- **In Exchange Server 2003**

Open Active Directory Users and Computers snap-in, you will get a new step after installing Exchange Server 2003, as shown in figure 3.24, here you can click 'Next' to set the mailbox.

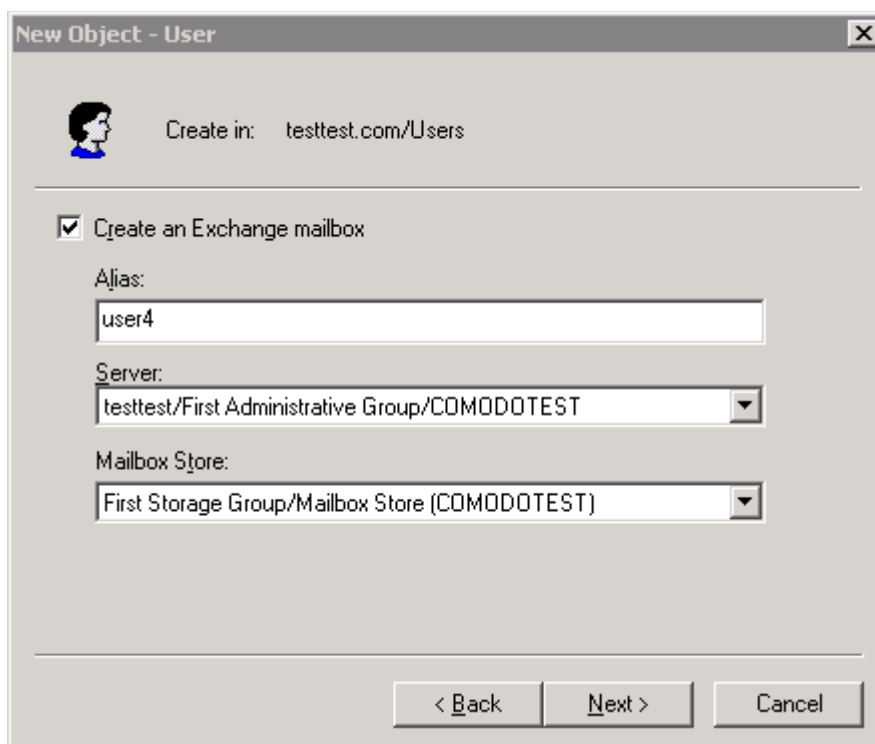


Figure 3.24 setup Mailbox

- **In Exchange Server 2007**

Open Exchange Management Console > Recipient Configuration > Mailbox, right click on Mailbox and click New Mailbox..., as shown in figure 3.25.

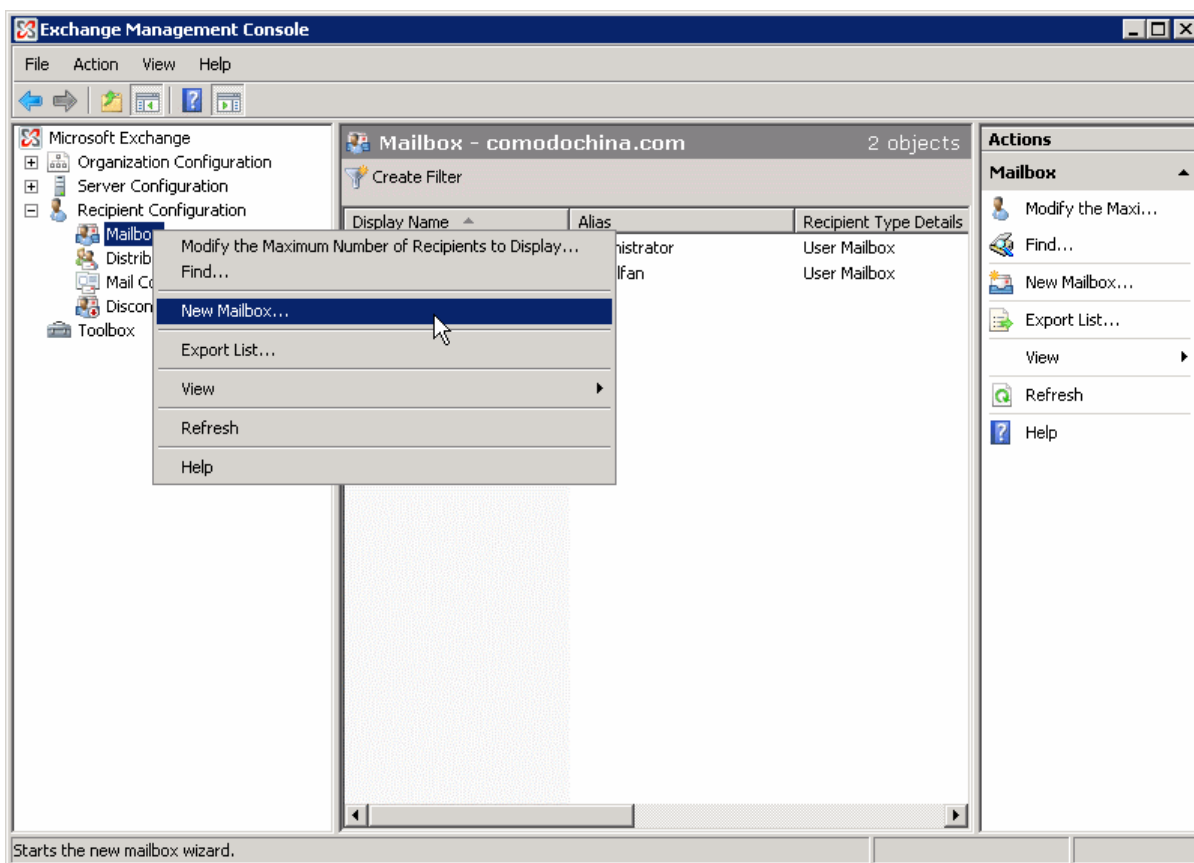


Figure 3.25 Open New Mailbox Window

In New Mailbox window, select User Mailbox, as shown in figure 3.26, here you can click 'Next' to set the mailbox.

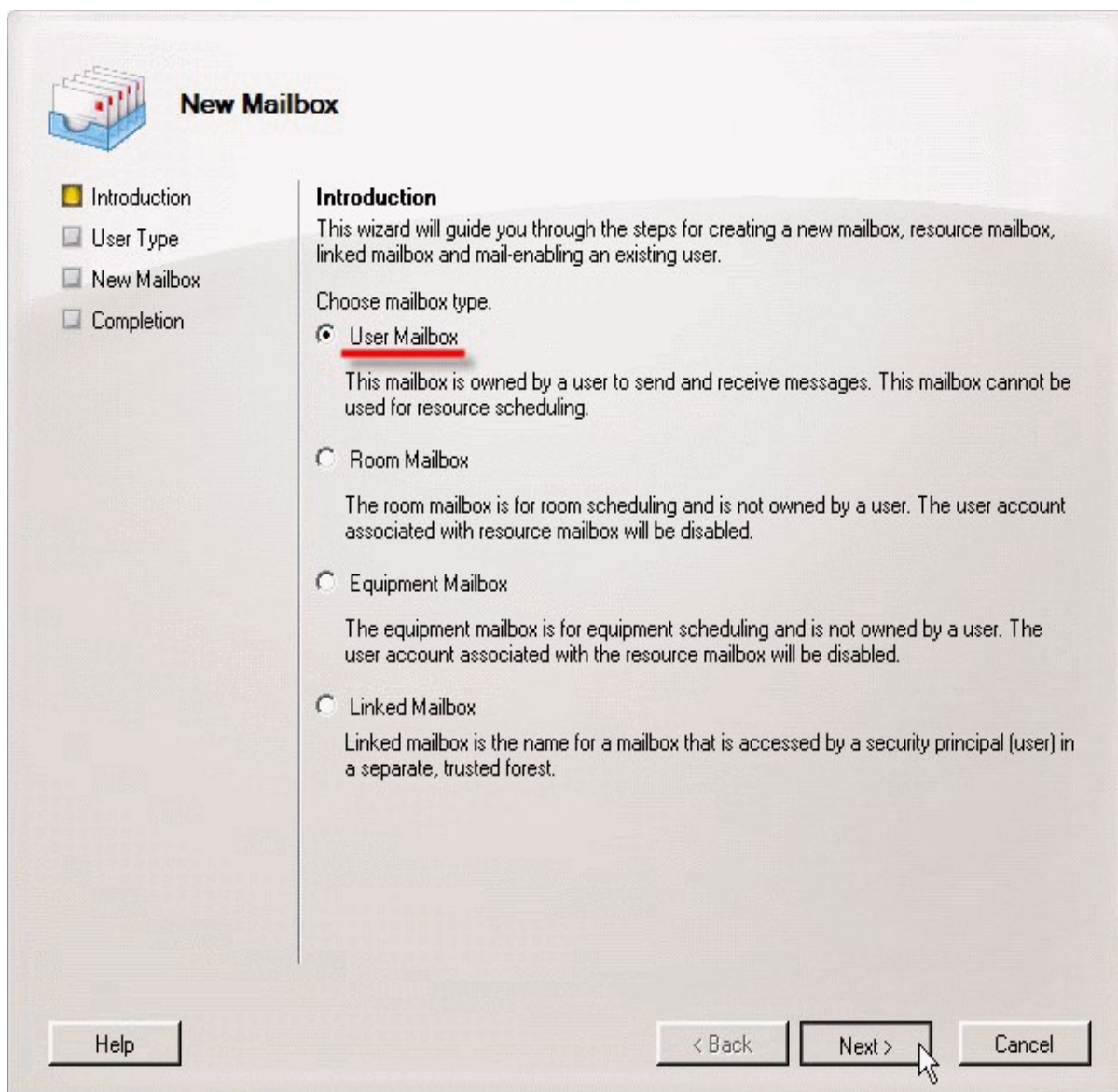


Figure 3.26 Setup New Mailbox

4. Client Configuration

4.1. Join Windows Server Domain

On the client machine from computer's properties dialog click Change button to change the computer's domain.

4.2. Logon as Domain User

After joining to Windows Domain Windows will ask you to restart computer.

Restart the client PC and logon domain as domain user.

IMPORTANT: after joining to Windows Domain, you have to restart computer to make sure that all Group Policies for computer work properly.

5. Check Certificate

5.1. Check User Certificate

IE->Tools->Internet Options->Content->Certificates->Personal

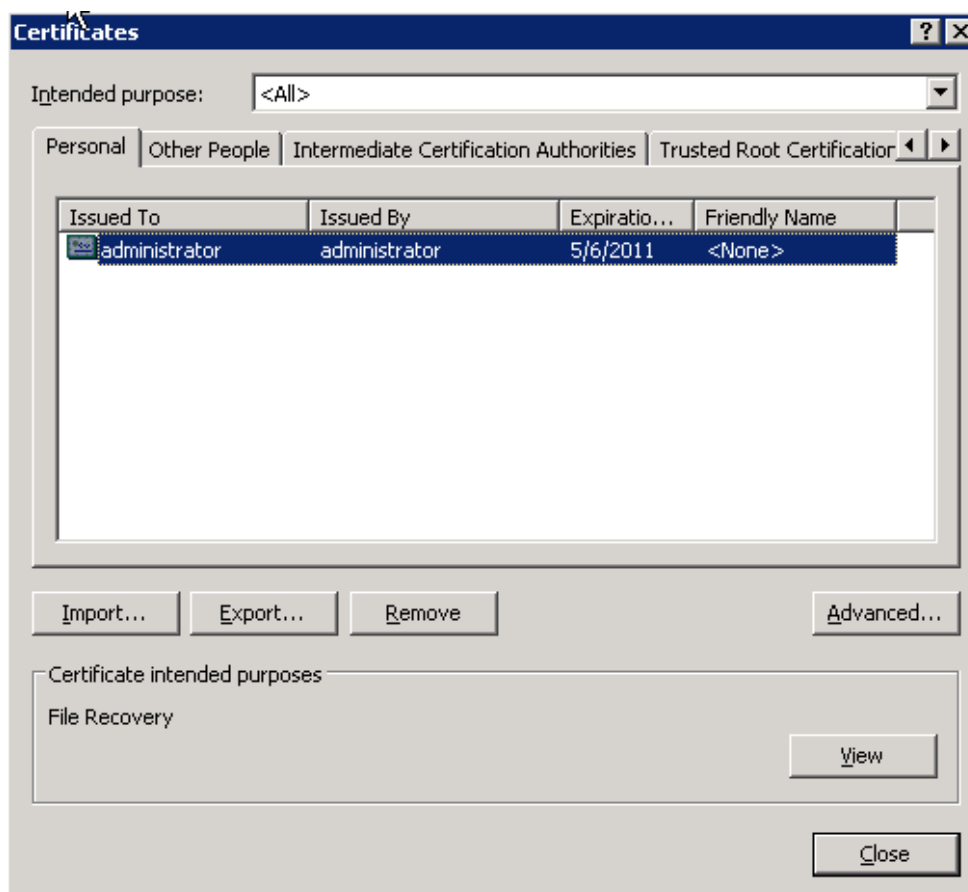


Figure 5.1 Check personal certificate

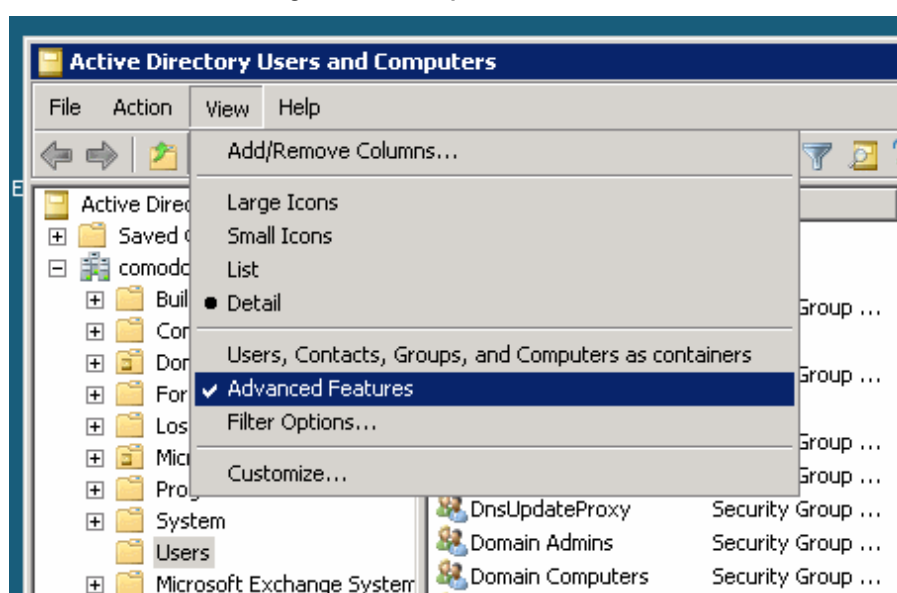


Figure 5.2 Check Advanced Features

6. Multiple Customer Configuration

6.1. Configure Kerberos

Do kerberos configuration for a new customer following instructions of chapter 2. And copy the generated keytab file to certificate manager server. Then

Modify login.conf:

```
de.com {  
    com.sun.security.auth.module.Krb5LoginModule required  
    storeKey=true  
    useKeyTab=true  
    refreshKrb5Config=true  
    isInitiator=false  
    keyTab="/home/lsc/keytab/fff.keytab"  
    principal="HTTP/certmgr.de.com@DE.COM";  
};  
ny.com {  
    com.sun.security.auth.module.Krb5LoginModule required  
    storeKey=true  
    useKeyTab=true  
    refreshKrb5Config=true  
    isInitiator=false  
    keyTab="/home/lsc/keytab/abc.keytab"  
    principal="HTTP/ccm.ny.com@NY.COM";  
};
```

to set the login configuration for a new customer. The parameters to be changed are same as those in section 2.2.
Please don't forget to add Active Directory Properties for a new customer.

6.2. Deploy VBScript

Deploy script for a new customer following chapter 3.

6.3. Restart CCM server

7. Known Issues

7.1. Don't Use CCM Server Machine as Client

If use ccm server as a client, IE can't get proper service principal name from Domain Controller.

7.2. Capicom Installation Fails

If Group Policy fails to install capicom automatically, please install it manually. To make this, launch capicom.msi installation package on a domain client PC where capicom was not installed. Contact COMODO if such situation occurs.

7.3. Cannot Set Password While Creating the User Keytab File

In Windows Server 2008, when using ktpass command to create the user keytab file as the part I in section 2.1, if the password is not set as expected, please refer to <http://support.microsoft.com/kb/960830> and download and install the hotfix.

8. Troubleshooting

8.1.1. Errors in Script Log

In Windows XP you can locate the script log in \Documents and Settings\

[ACCOUNT_NAME]\Local Settings\Temp\autoenroll.log

In Windows Vista you can locate the script log in \Users\

[ACCOUNT_NAME]\AppData\Local\Temp\autoenroll.log

Error 1: "No customer URI supplied.."

- potential reason : "customeruri" was not provided in autoenroll.conf.

Error 2: "Customer invalid.."

- potential reason : The provided "customeruri" is invalid.

Error 3: "Customer disabled.."

- potential reason : The customer has been disabled.

Error 4: "No matched domain.."

- potential reason : The domain from user's email is invalid.

Error 5: "Domain unauthorized.."

- potential reason : The domain is unauthorized for this customer.

Error 6: "Supplied orgid invalid.."

- potential reason : The provided "orgid" is invalid. (not a number)

Error 7: "No organization found.."

- potential reason : Can't find match organization in certificate manager or the id is invalid

Error 8: "No matched organization.."

- potential reason : The found organization is not managed by the customer or has been deleted or does not match with domain from the user's email.

Error 9: "Failed to find the AD Server.."

- potential reason : The organization or the customer didn't bind with any Active Directory Server in certificate manager.

Error 10: "Windows domain mismatch.."

- potential reason: The domain from bound Active Directory Server in certificate manager doesn't match the one from windows server.

Error 11: "No suitable organization.."

- potential reason : There is no proper organization bind to the Active Directory Server.

Error 12: "No matched ADServer.."

- potential reason : Can't find matched Active Directory Server in certificate manager.

Error 13: "Failed to get adserver or attributes.."

- potential reason : certificate manager can't connect with Active Directory. Check the Active Directory properties defined in certificate manager.

Error 14: "Failed to sync person.."

- potential reason : certificate manager internal error.

Error 15: "Invalid CSR.."

- potential reason : autoenrollment script generate invalid CSR, make sure you use the latest autoenroll.conf and ExchangeEnroll.vbs.

Error 16: "No valid Email in AD.."

- potential reason 1: User with this email does not exist or has been deleted.

- potential reason 2: The request may be sent by an impostor.

Error 17: "No valid User Name in AD.."

- potential reason 1: User does not exist or has been deleted.

- potential reason 2: The request may be sent by an impostor.

Error 18: "Email in AD mismatch.."

- potential reason 1: email from autoenroll request does not match with email on AD server.

- potential reason 2: The request may be sent by an impostor.

Error 19: "User Name in AD mismatch.."

- potential reason 1: CN from autoenroll request does not match with user's CN on AD server.

- potential reason 2: The request may be sent by an impostor.

Error 20: "Person mismatch.."

- potential reason : User is not from the customer specified by "customeruri".

Error 21: "Invalid status supplied.."

- potential reason 1: The autoenrollment script maybe out-of-date.

- potential reason 2: The request may be sent by an impostor.

Error 22: "Unknown person for processStatus.."

- potential reason 1: The user in certificate manager may already be deleted.

- potential reason 2: The request may be sent by an impostor.

Error 23: "Failed to process status.."

- potential reason 1: certificate manager internal error.

- potential reason 2: The request may be sent by an impostor.

Error 24: "Invalid serial number supplied.."

- potential reason 1: The serial number sent by autoenrollment script is invalid. Update script.

- potential reason 2: There are more than 1 valid certificates from the same issuer in user's MY store.

- potential reason 3: The certificate matched the serial number may not be in valid state.

Error 25: "Failed to get cert.."

- potential reason 1: The CA server is down.

- potential reason 2: certificate manager internal error.

Error 26: "No email supplied.."

- potential reason 1: can't get email from autoenroll request, script maybe out-of-date..

- potential reason 2: The request may be sent by an impostor.

Error 27: "Invalid remote user.."

- potential reason 1: can't get user credential from autoenroll request, script maybe out-of-date.

- potential reason 2: The request may be sent by an impostor.

Error 28: "No synchronized person .."

- potential reason : certificate internal error.

Error 29: "No request supplied.."

- potential reason 1: can't get CSR from autoenroll request, script maybe out-of-date..

- potential reason 2: The request may be sent by an impostor.

Error 30: "Failed to enroll certificate.."

- potential reason : certificate manager internal error.

Error 31: "Open local certificate store error."

- potential reason : Capicom.dll may not be distributed successfully.

Error 32: "User has no email address in AD."

- potential reason : User has no exchange mailbox or no mail address is set in user's account.

Error 33: "Create certificate request error."

- potential reason : script may not be configured correctly on Group Policy.

Error 34: "Certificate response timeout."

- potential reason : certificate manager didn't issued certificate in 2 minutes.

Error 35: "Connect to certificate manager error."

- potential reason : certificate manager can not be reached at this time.

Error 36: "Certificate manager internal error."

- potential reason : certificate manager internal error.

Error 37: "Authentication error."

- potential reason : certificate manager does not authorized the autoenroll request. Check kerberos configuration.

Error 38: "Request certificate error."

- potential reason : certificate manager internal error.

Error 39: "Install certificate error."

- potential reason : script may not be configured correctly on Group Policy.

Error 40: "Wait sync response timeout."

- potential reason : certificate manager didn't response in 40 seconds.

Error 41: "Not yet install the CCM security certificate."

- potential reason 1: certificate manager SSL certificate is not properly installed.

- potential reason 2: certificate manager SSL certificate is not in Group Policy 's trusted store.

About Comodo

The Comodo companies are leading global providers of Security, Identity and Trust Assurance services on the Internet. Comodo CA offers a comprehensive array of PKI Digital Certificates and Management Services, Identity and Content Authentication (Two-Factor - Multi-Factor) software, and Network Vulnerability Scanning and PCI compliance solutions. In addition, with over 10,000,000 installations of its threat prevention products, Comodo Security Solutions maintains an extensive suite of endpoint security software and services for businesses and consumers.

Continual innovation, a core competence in PKI and a commitment to reversing the growth of Internet-crime distinguish the Comodo companies as vital players in the Internet's ongoing development. Comodo, with offices in the US, UK, China, India, Romania and the Ukraine, secures and authenticates the online transactions and communications for over 200,000 business customers and millions of consumers, providing the intelligent security, authentication and assurance services necessary for trust in on-line transactions.

Comodo CA Limited

3rd Floor, 26 Office Village, Exchange Quay, Trafford Road,
Salford, Greater Manchester M5 3EQ,

United Kingdom.

Tel : +44 (0) 161 874 7070

Fax : +44 (0) 161 877 1767

Email: EnterpriseSolutions@Comodo.com

Comodo Security Solutions, Inc.

1255 Broad Street

Clifton,

NJ 07013

United States

Tel: +1.877.712.1309

Tel: +1.888.256.2608

For additional information on Comodo - visit <http://www.comodo.com>.