InCommon®

InCommon Certificate Manager

Windows Auto Enrollment Setup Guide

InCommon
c/o Internet2
1000 Oakbrook Drive, Suite 300
Ann Arbor MI, 48104

Table of Contents

1 Prerequisite

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 InCommon CM) 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 InCommon CM is deployed outside customer's network: map port 88 and 389 of Active Directory on gateway server that will allow InCommon CM to connect Active Directory
    - Add a host mapping in local DNS for domain users to access InCommon CM by domain name
    - Following are IP addresses of InCommon CM server, 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 “csm” or any name you like for the 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 'csm' in Active Directory Users and Computers snap-in and click on Properties to open up Properties dialog. Check user's logon name, for now InCommon CM's user logon name should be 'csm'. See figure 2.3.

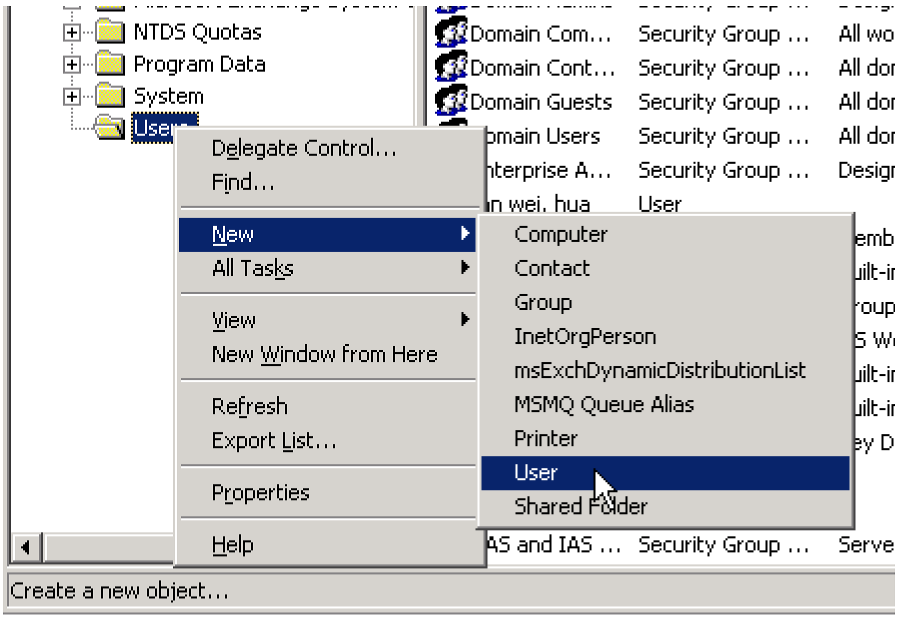
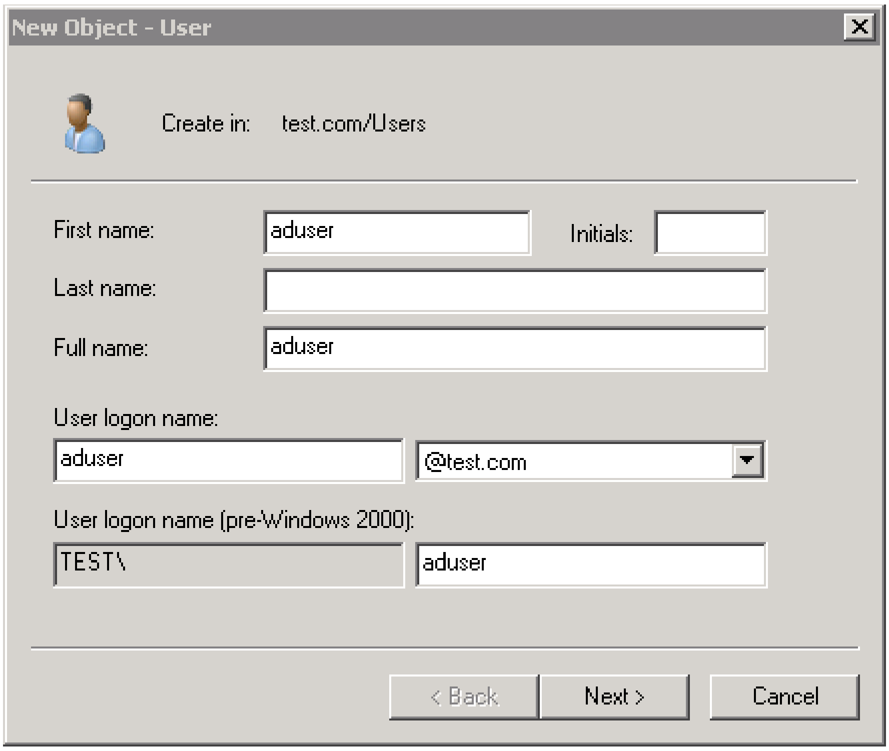

NTDS Quotas
Program Data
System
Users
Domain Com… Security Group … All wo
Domain Cont… Security Group … All dor
Domain Guests Security Group … All dor
Domain Users Security Group … All dor
Enterprise A… Security Group … Desigr
wei, hua User
Delegate Control…
Find…
New
All Tasks
View
New Window from Here
Refresh
Export List…
Properties
Help
Computer
Contact
Group
InetOrgPerson
msExchDynamicDistributionList
MSMQ Queue Alias
Printer
User
Shared Folder
RAS and IAS … Security Group … Serve
Create a new object…

Figure 2.1 Open User Object Editor dialog



Create in: test.com/Users

First name: aduser

Initials:

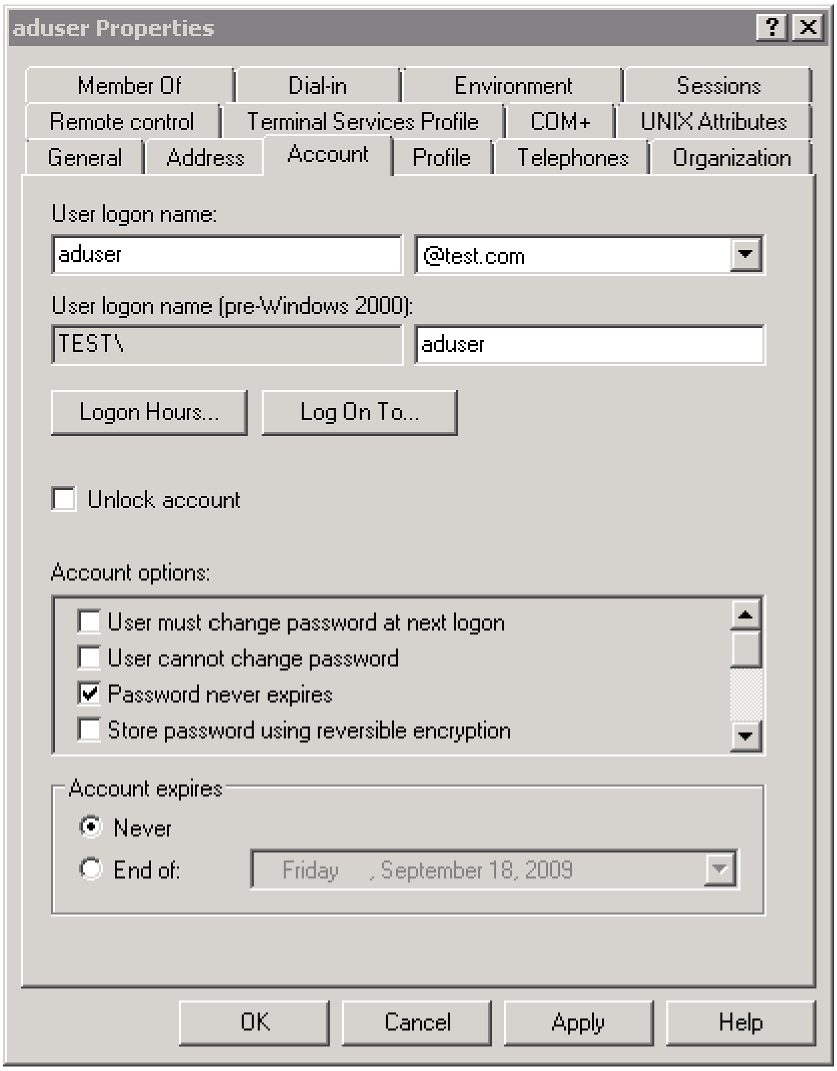
Last name:

Full name: aduser

User logon name: aduser @test.com

User logon name (pre-Windows 2000): TEST\ aduser

Figure 2.2 Create a new account in Users Object Editor



User logon name:

aduser @test.com

User logon name (pre-Windows 2000):

TEST\ aduser

□ Unlock account

Account options:

- □ User must change password at next logon
- □ User cannot change password
- ☑ Password never expires
- □ Store password using reversible encryption

Account expires

- ● Never
- ○ End of: Friday , September 18, 2009

Figure 2.3 csm Properties dialog

- DNS Configuration

Add InCommon CM 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.

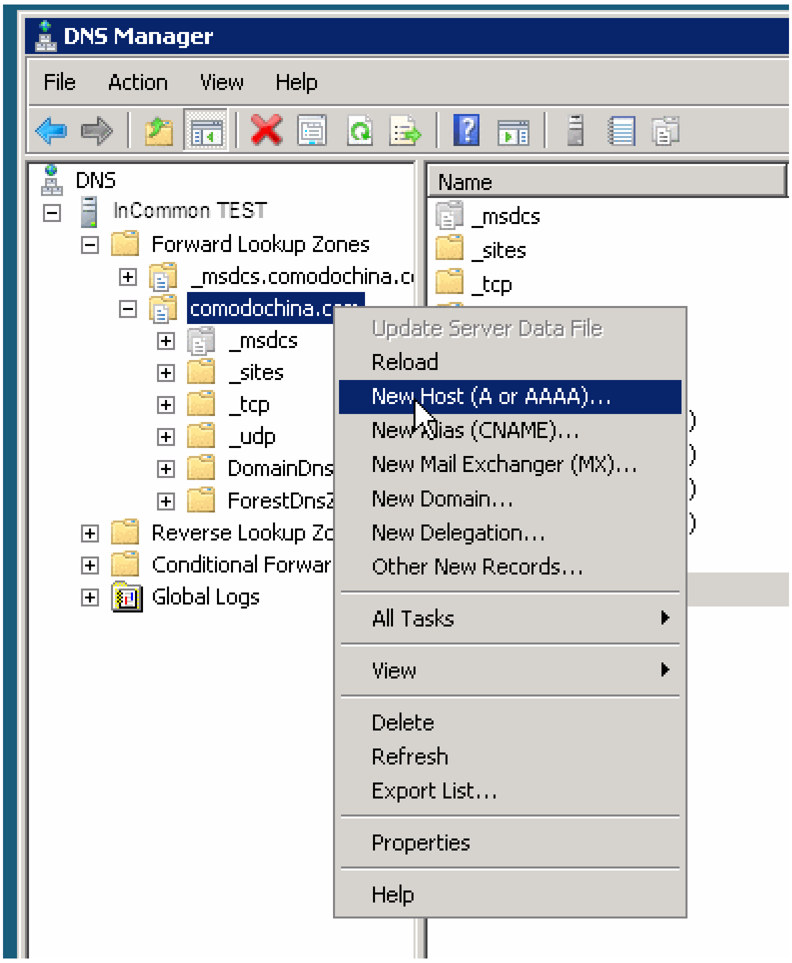
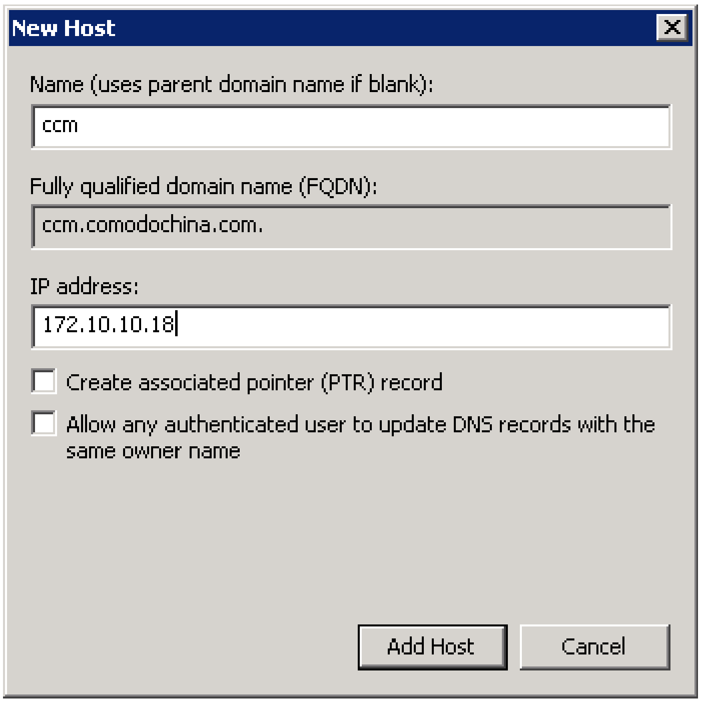


Figure 2.4 Create a new host


New Host

Name (uses parent domain name if blank):
ccm

Fully qualified domain name (FQDN):
ccm.comodochina.com.

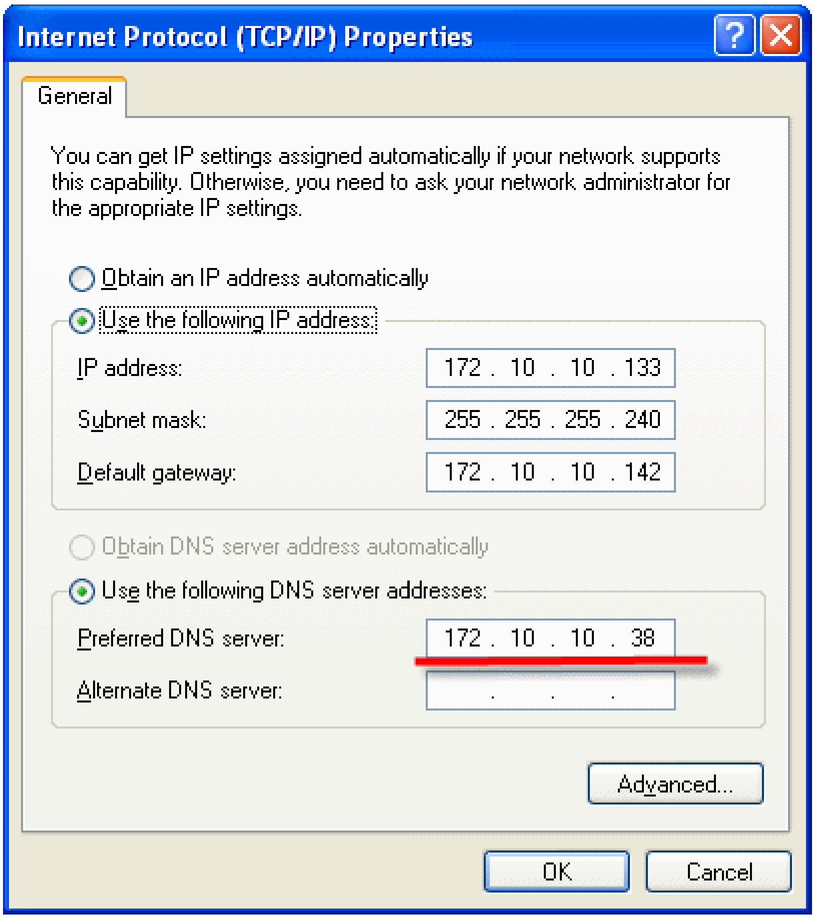
IP address:
172.10.10.18

□ Create associated pointer (PTR) record

□ Allow any authenticated user to update DNS records with the same owner name

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.



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 172 . 10 . 10 . 133

Subnet mask: 255 . 255 . 255 . 240

Default gateway: 172 . 10 . 10 . 142

○ Obtain DNS server address automatically

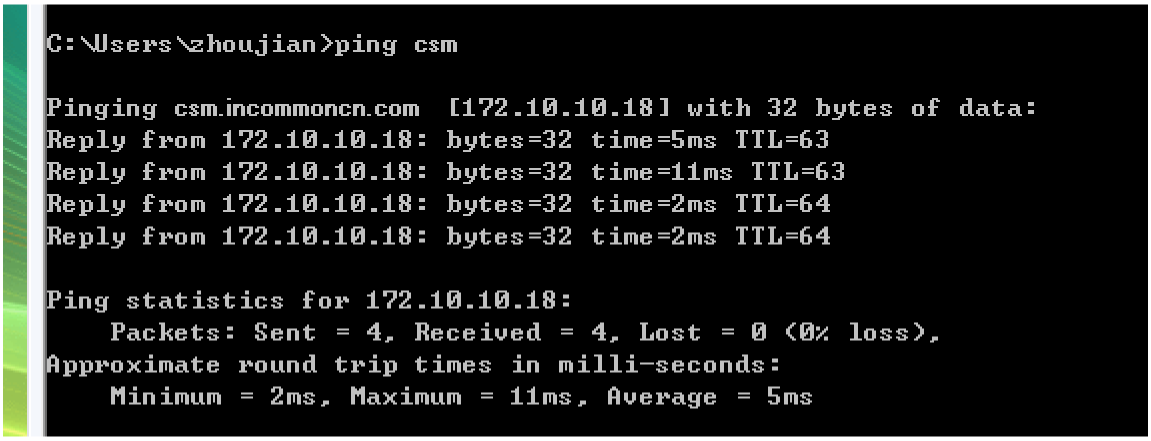
● Use the following DNS server addresses:

Preferred DNS server: 172 . 10 . 10 . 38

Alternate DNS server: . . .

Figure 2.6 Setup Preferred DNS Server

If everything is OK, run “ping csm” command from the client computer to validate. See figure 2.7.



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

Pinging csm.incommoncn.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 csm 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 csm server.

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

CSM_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/csm@TEST.COM -mapuser aduser -crypto DES-CBC-MD5-ptype KRB5_NT_PRINCIPAL -mapop set +desonly -pass password -out csm.keytab*

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

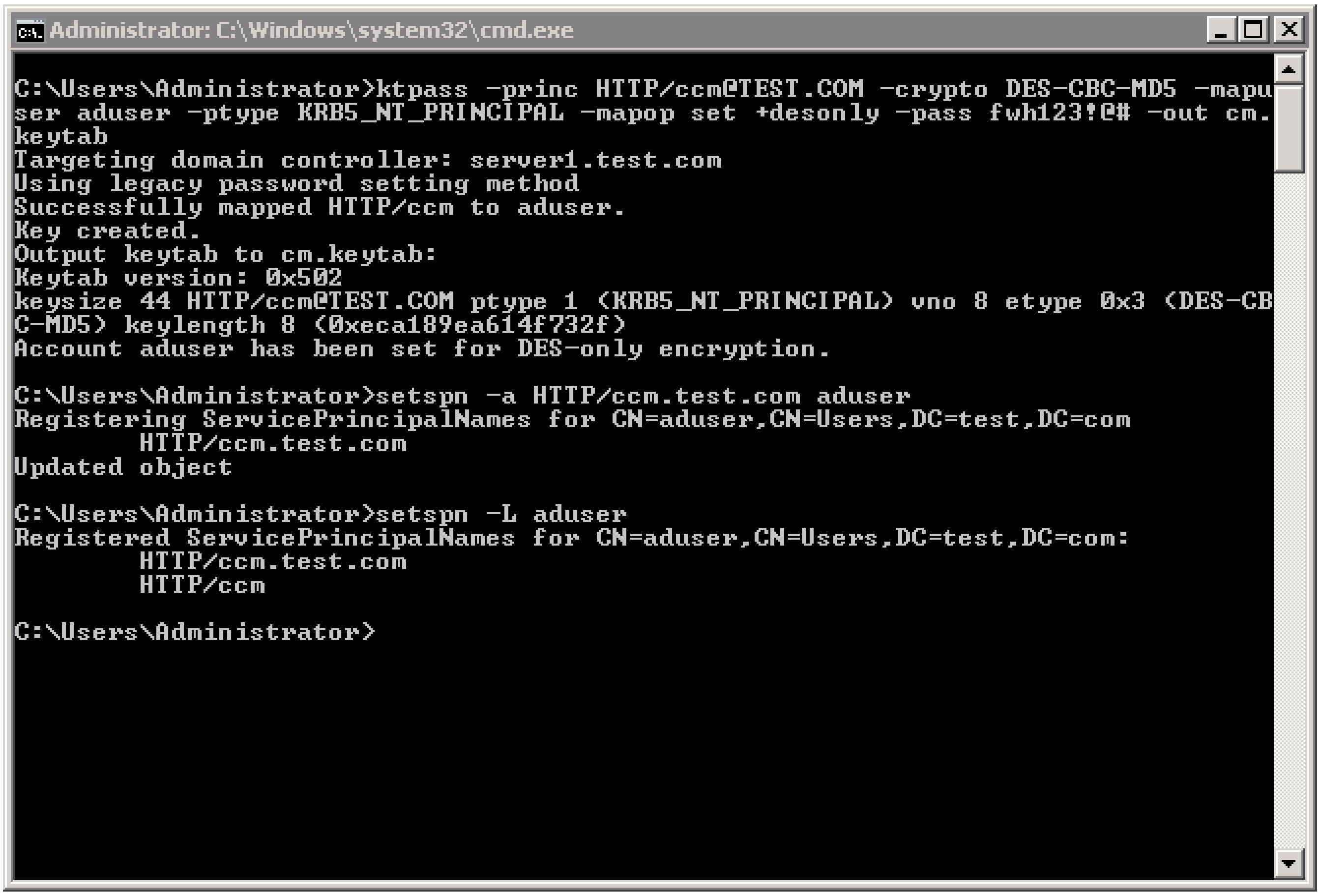
> *setspn -a HTTP/[FQDN] [DOMAIN ACCOUNT]*

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

For example:

setspn -a HTTP/csm .test.com aduser

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



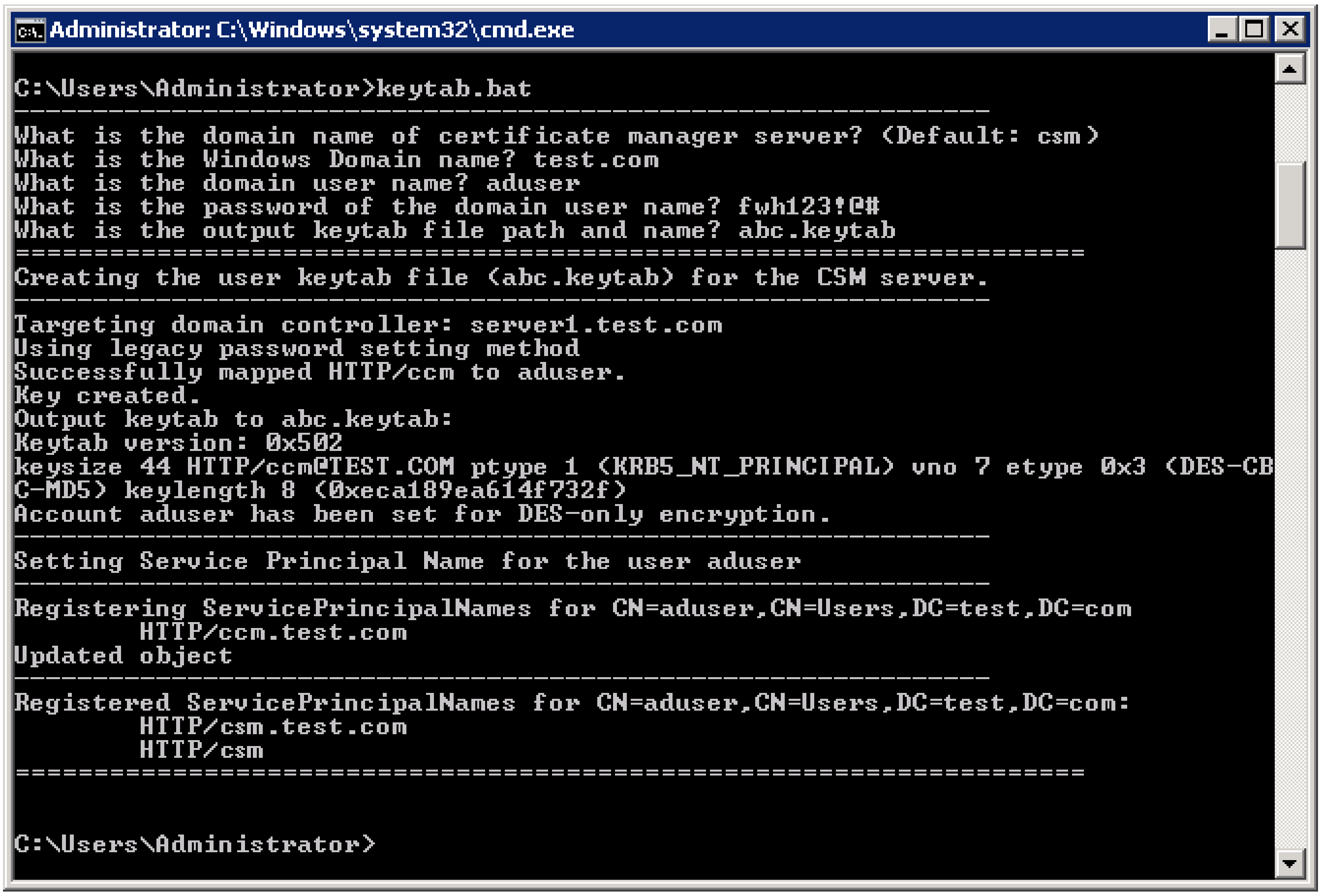
```
C:\Users\Administrator>ktpass -princ HTTP/ccm@TEST.COM -crypto DES-CBC-MD5 -mapu
ser aduser -ptype KRB5_NT_PRINCIPAL -mapop set +desonly -pass fwh123!@# -out cm.
keytab
Targeting domain controller: server1.test.com
Using legacy password setting method
Successfully mapped HTTP/ccm to aduser.
Key created.
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 (0xeca189ea614f732f)
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 CSM 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.



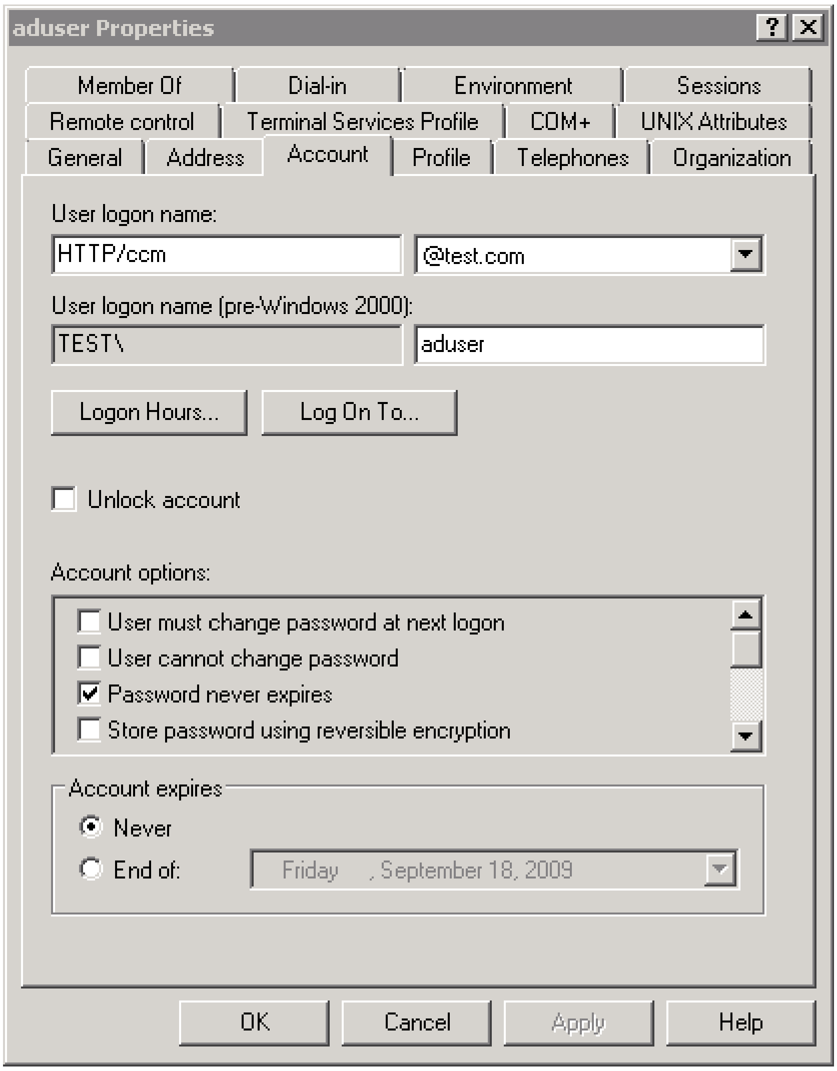
```
Administrator: C:\Windows\system32\cmd.exe

C:\Users\Administrator>keytab.bat
----------------------------------------------------------------
What is the domain name of certificate manager server? (Default: csm)
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 CSM 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 (0xeca189ea614f732f)
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/csm.test.com
        HTTP/csm
======================================================================


C:\Users\Administrator>
```

Figure 2.9 Create keytab automatically

Copy the generated keytab file to the InCommon CM server.

(for example : */home/daniel/csm.keytab* in Linux System)

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



User logon name: HTTP/ccm @test.com

User logon name (pre-Windows 2000): TEST\ aduser

□ Unlock account

Account options:

- □ User must change password at next logon
- □ User cannot change password
- ☑ Password never expires
- □ Store password using reversible encryption

Account expires

- ● Never
- ○ End of: Friday , September 18, 2009

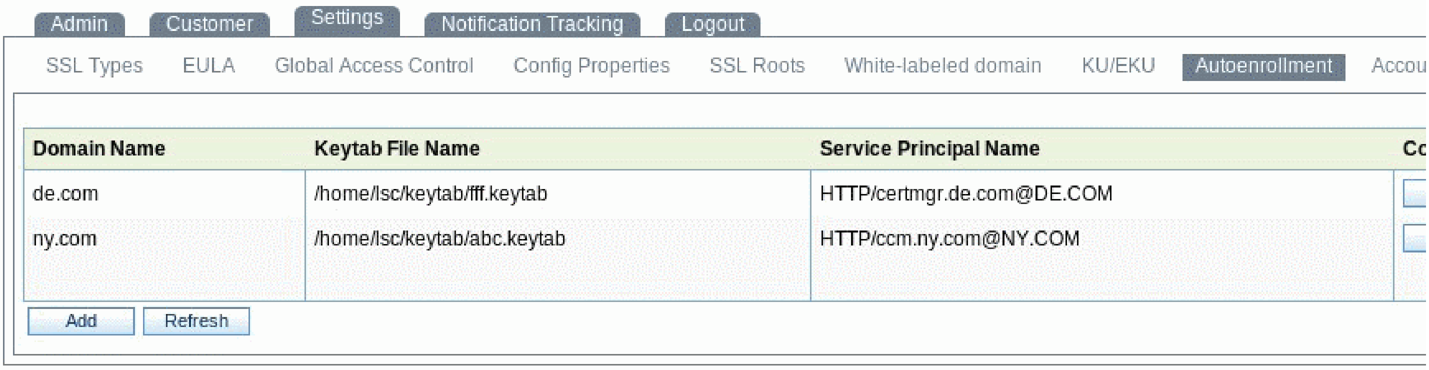
Figure 2.10 csm's Properties dialog

2.2 Create/Modify login.conf in Certificate Manager

Access InCommon CM SuperAdmin page, open Settings/Autoenrollment Tab.

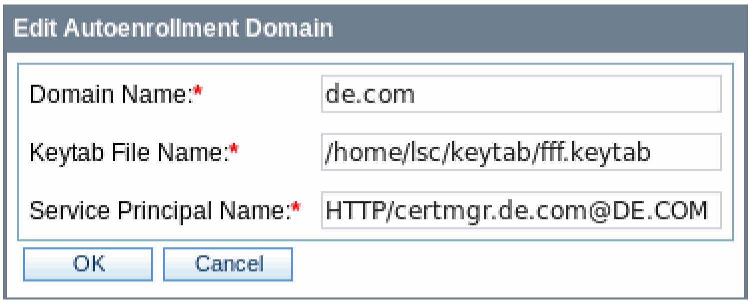
Click "Add"/ "Edit" button to add/edit KDC configuration to login.conf.

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



Domain Name	Keytab File Name	Service Principal Name	Co
de.com	/home/lsc/keytab/fff.keytab	HTTP/certmgr.de.com@DE.COM	
ny.com	/home/lsc/keytab/abc.keytab	HTTP/ccm.ny.com@NY.COM	

Figure 2.11 Autoenrollment view



Edit Autoenrollment Domain

Domain Name:*	de.com
Keytab File Name:*	/home/lsc/keytab/fff.keytab
Service Principal Name:*	HTTP/certmgr.de.com@DE.COM

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.

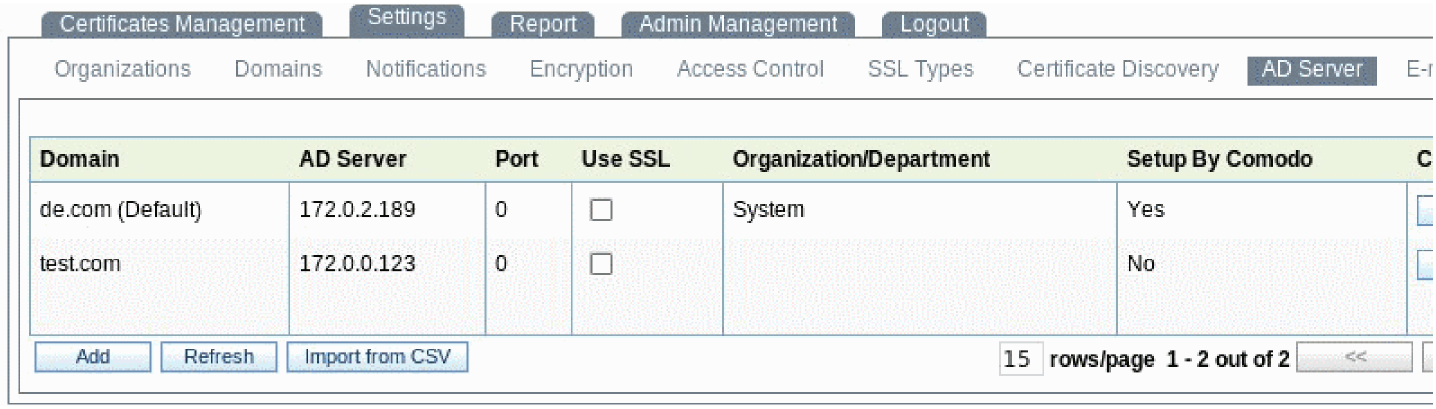
IMPORTANT: If CSM will be deployed under Windows system, please change the file path form to Windows form.

e.g. ”C:/kerberos/csm.keytab”

2.3 Configure Active Directory Properties in InCommon CM Server

The Certificate Manager server will use the user 'csm' (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.

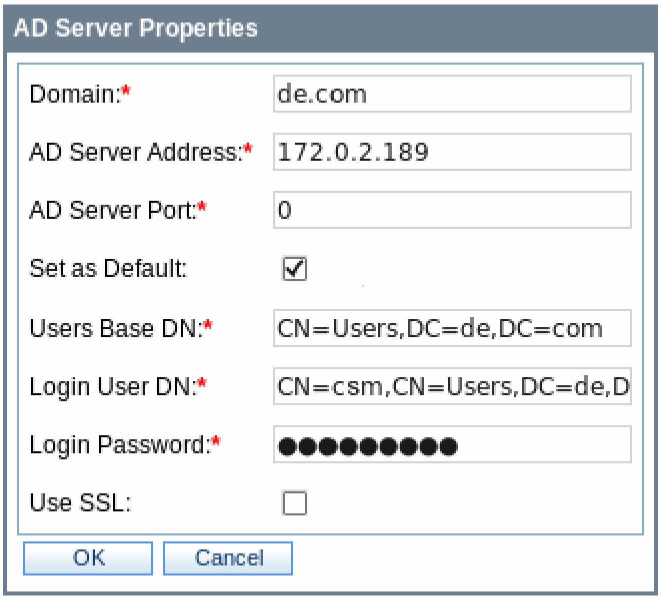


Domain	AD Server	Port	Use SSL	Organization/Department	Setup By Comodo	C
de.com (Default)	172.0.2.189	0	☐	System	Yes	
test.com	172.0.0.123	0	☐		No	

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:



AD Server Properties

Domain:*	de.com
AD Server Address:*	172.0.2.189
AD Server Port:*	0
Set as Default:	☑
Users Base DN:*	CN=Users,DC=de,DC=com
Login User DN:*	CN=csm,CN=Users,DC=de,D
Login Password:*	●●●●●●●●●
Use SSL:	☐

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=incommon, DC=com

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

e.g. CN=csm, CN=Users, DC=incommon, DC=com

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

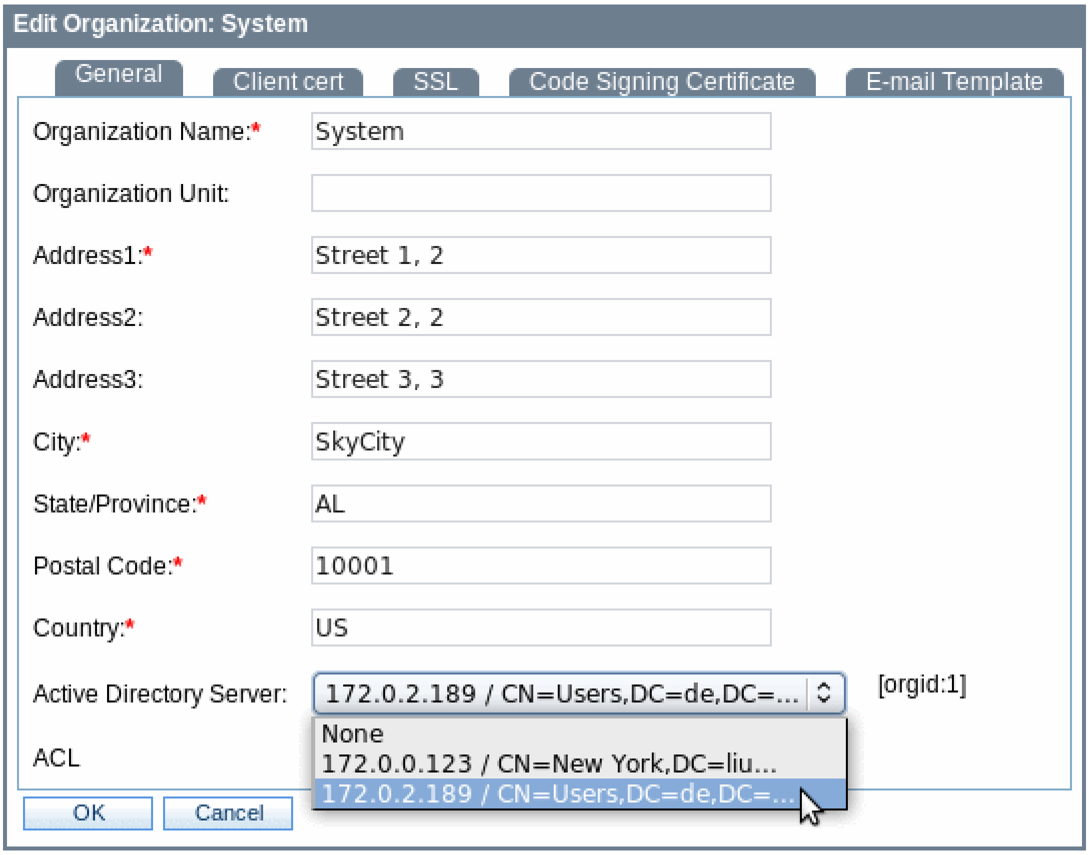
Use SSL: check it if you want to use SSL to access Active Directory

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

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

To bind AD Server to organization:

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



Edit Organization: System

Organization Name:*	System
Organization Unit:	
Address1:*	Street 1, 2
Address2:	Street 2, 2
Address3:	Street 3, 3
City:*	SkyCity
State/Province:*	AL
Postal Code:*	10001
Country:*	US
Active Directory Server:	172.0.2.189 / CN=Users,DC=de,DC=... [orgid:1]
ACL	

None
172.0.0.123 / CN=New York,DC=liu...
172.0.2.189 / CN=Users,DC=de,DC=...
OK
Cancel

Figure 2.15 Bind AD Server

2.4 Synchronize Time between InCommon CM Server and Domain Controller

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

2.5 Restart InCommon 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 : issuser name in certificate which will be issued by InCommon 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 InCommon CM

orgid(optional): Organization id in InCommon CM

3.2 Open Group Policy Editor

- In Windows Server 2003 EE

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

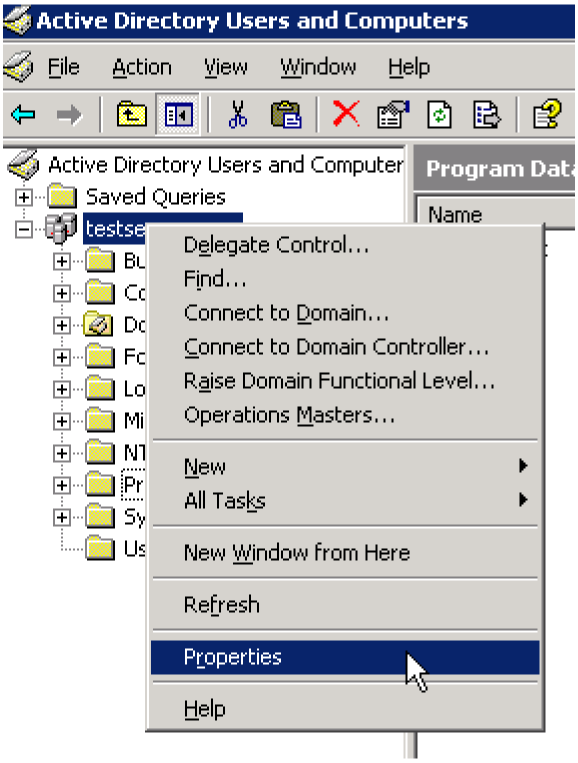
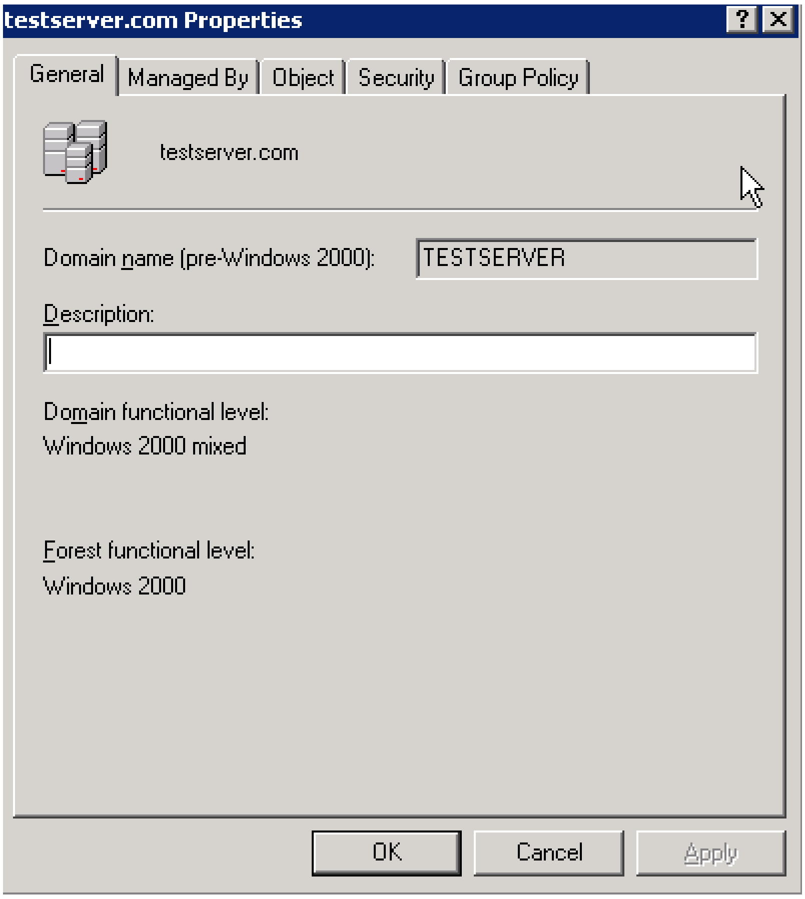


Figure 3.1 Open properties dialog of domain

Right click on the domain name->Properties

Properties dialog will pop up. See figure 3.2.



testserver.com Properties

Domain name (pre-Windows 2000): TESTSERVER

Description:

Domain functional level:
Windows 2000 mixed

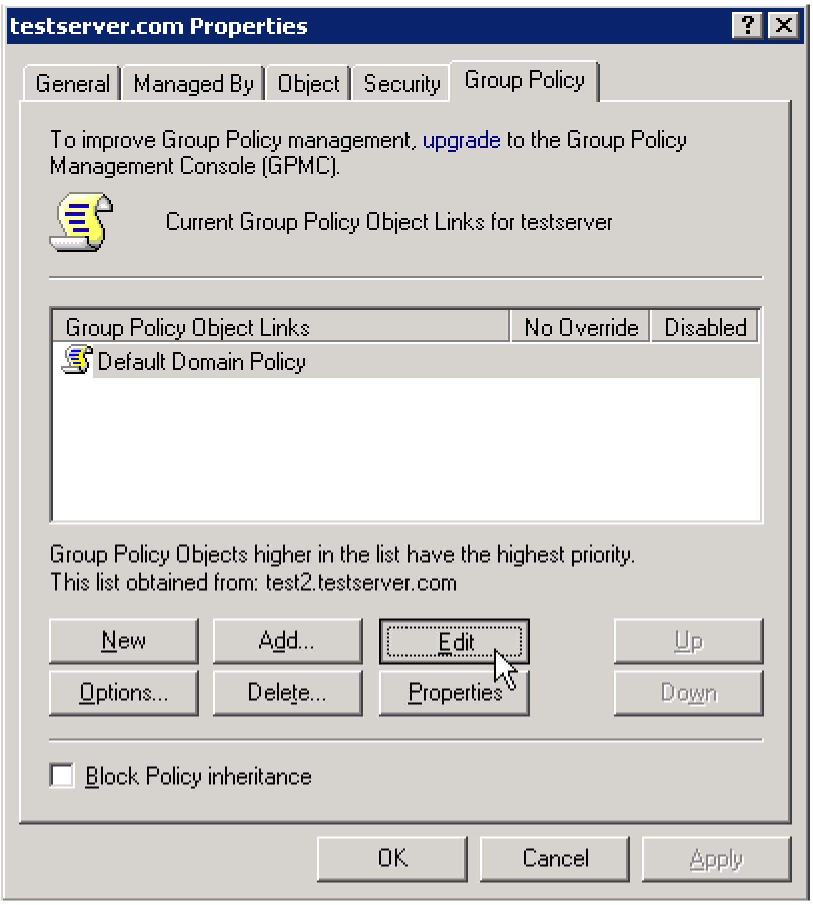
Forest functional level:
Windows 2000

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.



To improve Group Policy management, upgrade to the Group Policy Management Console (GPMC).

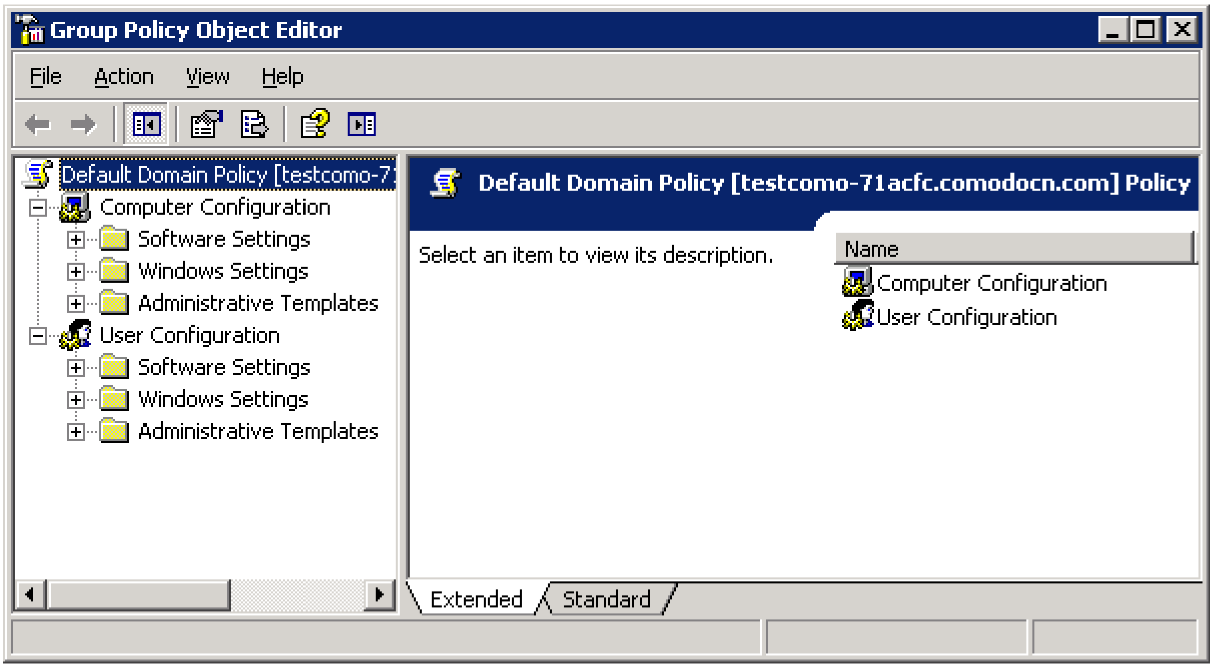
Current Group Policy Object Links for testserver

Group Policy Object Links	No Override	Disabled
Default Domain Policy		

Group Policy Objects higher in the list have the highest priority.
This list obtained from: test2.testserver.com

□ Block Policy inheritance

Figure 3.3 Open Default Domain Policy



Select an item to view its description.

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.

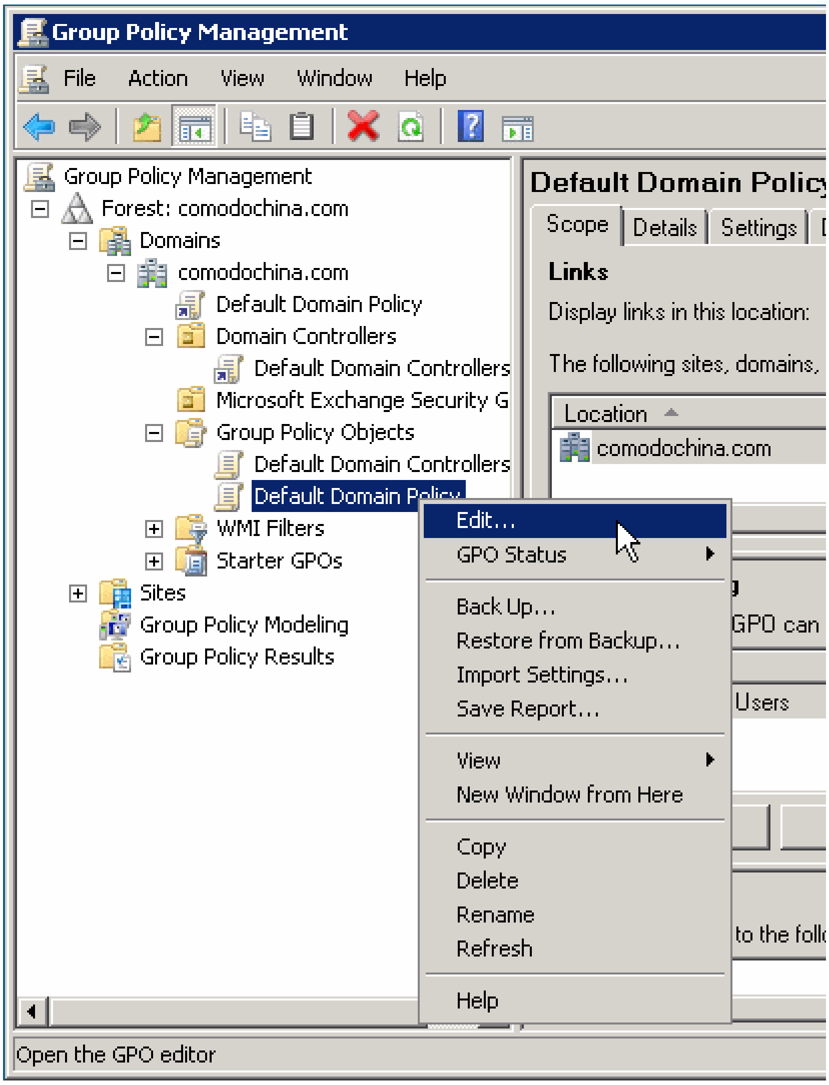


Figure 3.5 Group Policy Management

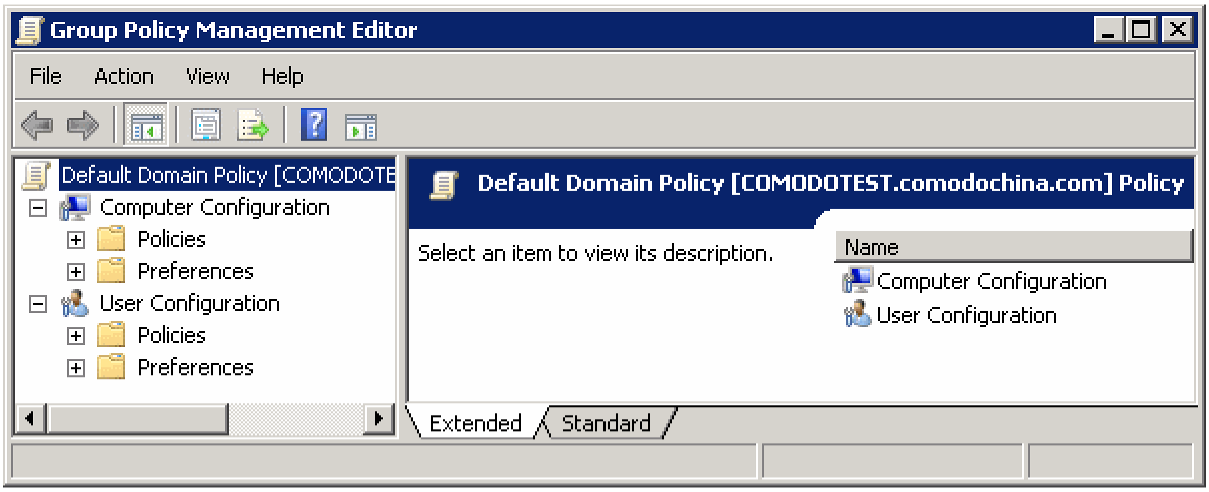


Figure 3.6 Group Policy Management Editor in Windows Server 2008

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

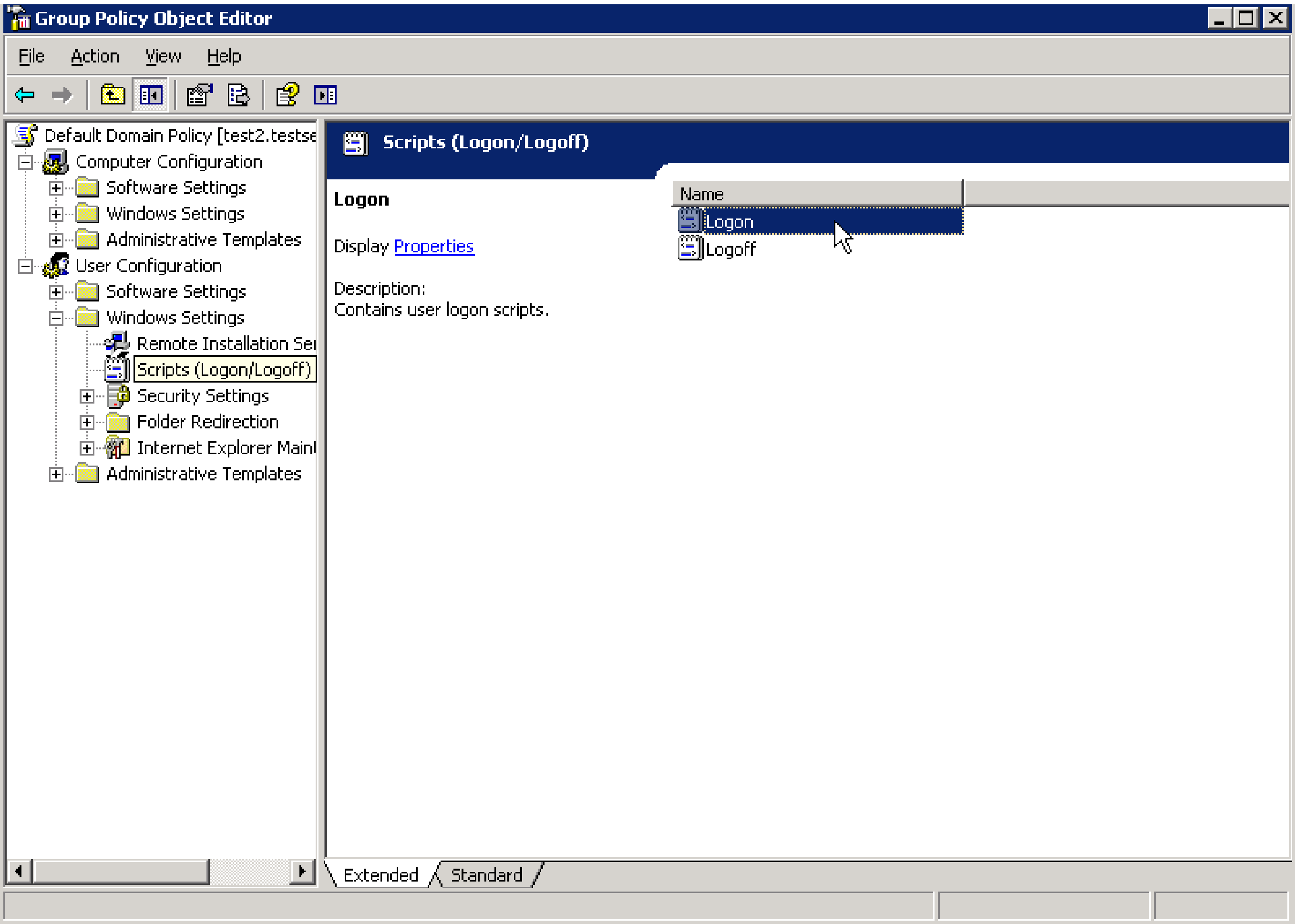


Figure 3.7 Open Logon Properties

Logon Properties dialog will pop up. See figure 3.8.

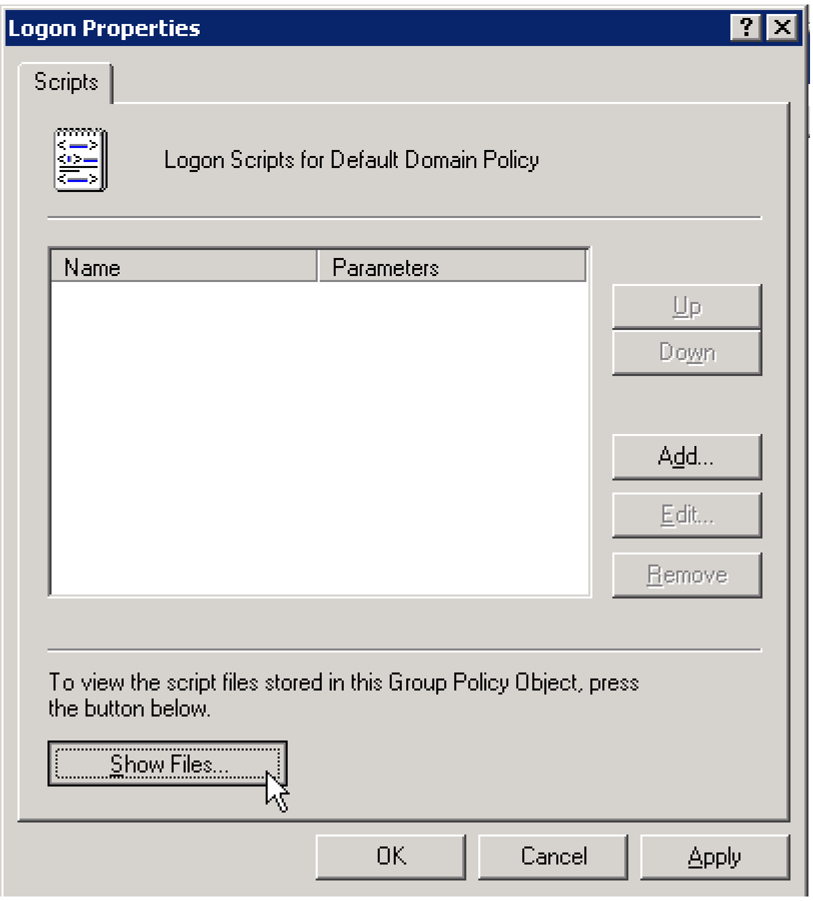

Logon Properties
Scripts
Logon Scripts for Default Domain Policy
Name
Parameters
Up
Down
Add...
Edit...
Remove
To view the script files stored in this Group Policy Object, press the button below.
Show Files...
OK
Cancel
Apply

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

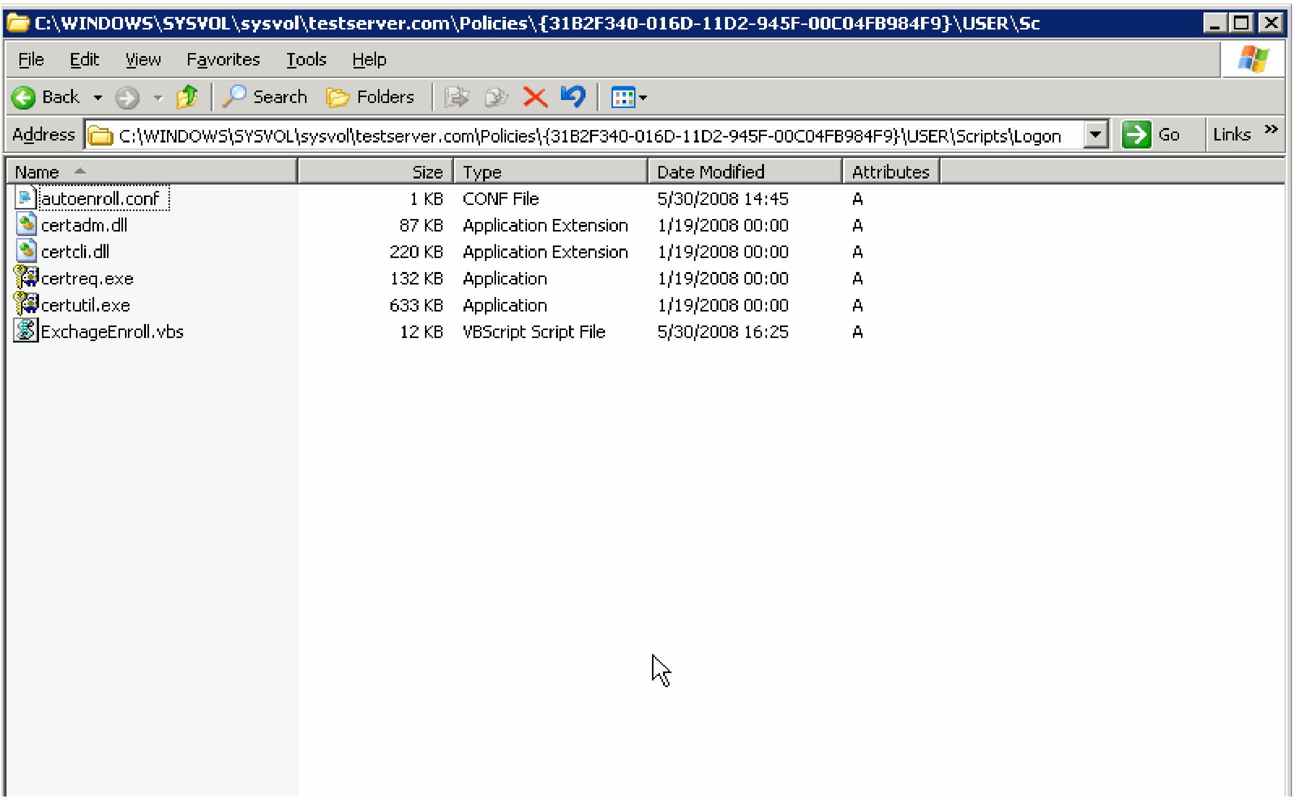
certcli.dll

certreq.exe

certutil.exe

ExchangeEnroll.vbs

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

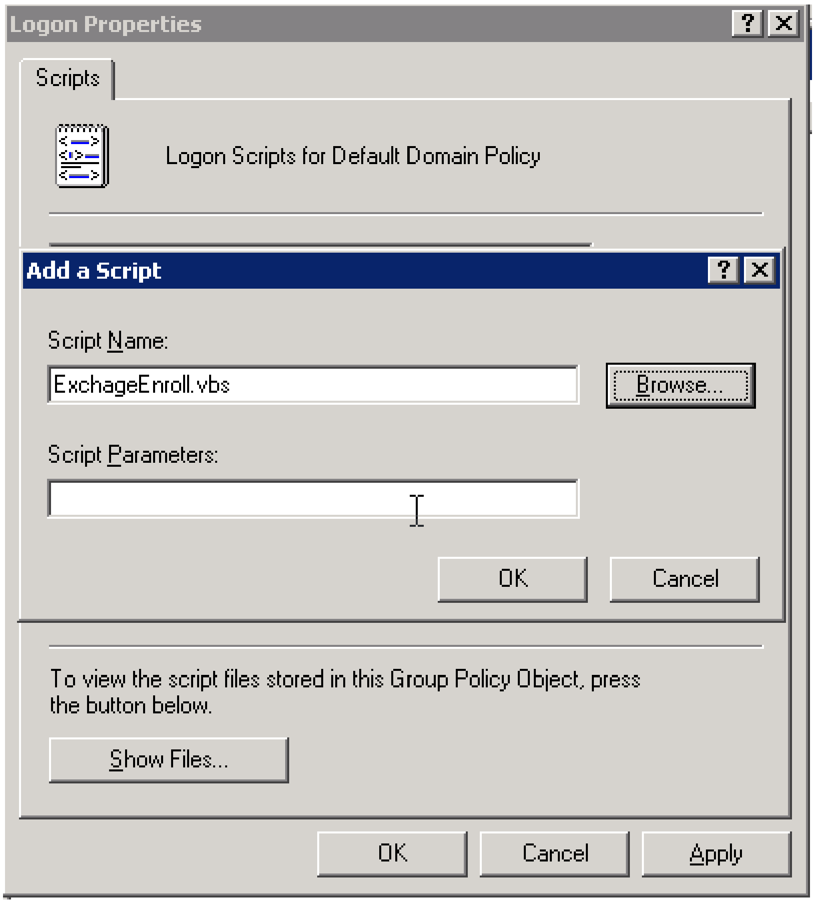


C:\WINDOWS\SYSVOL\sysvol\testserver.com\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\USER\Sc

Address C:\WINDOWS\SYSVOL\sysvol\testserver.com\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\USER\Scripts\Logon

Name	Size	Type	Date Modified	Attributes
autoenroll.conf	1 KB	CONF File	5/30/2008 14:45	A
certadm.dll	87 KB	Application Extension	1/19/2008 00:00	A
certcli.dll	220 KB	Application Extension	1/19/2008 00:00	A
certreq.exe	132 KB	Application	1/19/2008 00:00	A
certutil.exe	633 KB	Application	1/19/2008 00:00	A
ExchageEnroll.vbs	12 KB	VBScript Script File	5/30/2008 16:25	A

Figure 3.9 Logon script directory



Logon Properties

Logon Scripts for Default Domain Policy

Add a Script

Script Name: ExchageEnroll.vbs

Script Parameters:

To view the script files stored in this Group Policy Object, press the button below.

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*

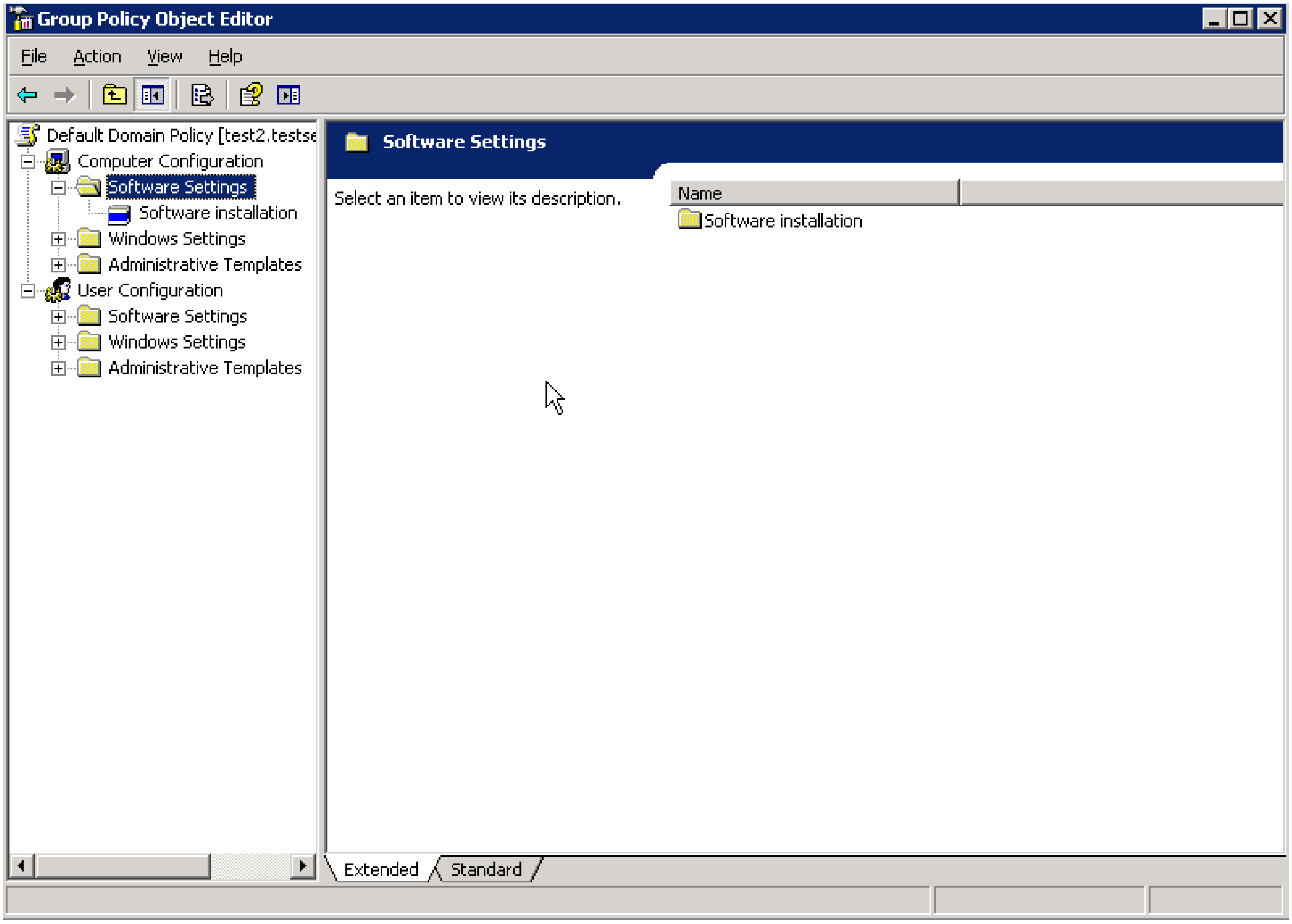
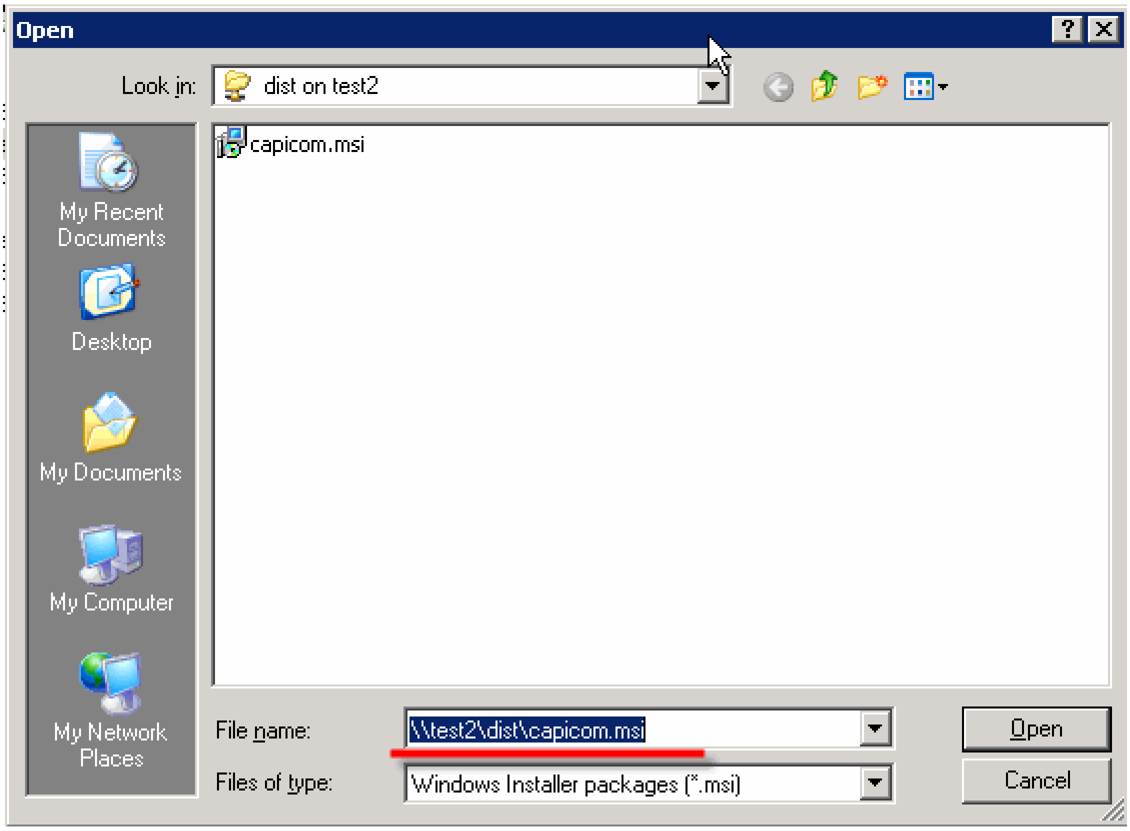


Figure 3.11 Open Software Installation

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



Look in: dist on test2

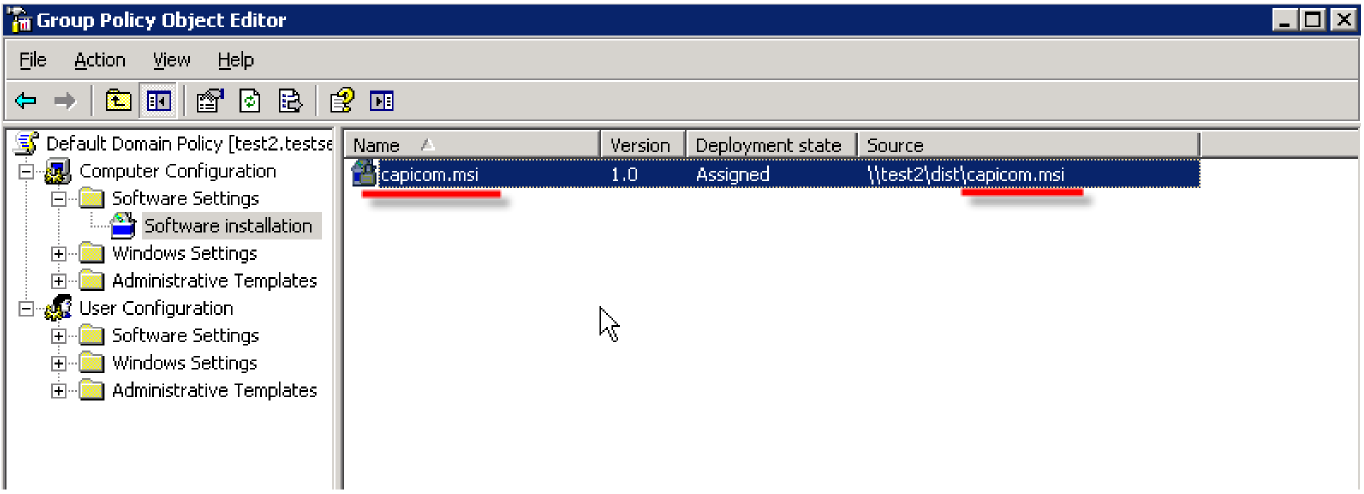
capicom.msi

File name: \\test2\dist\capicom.msi

Files of type: Windows Installer packages (*.msi)

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.



Name	Version	Deployment state	Source
capicom.msi	1.0	Assigned	\\test2\dist\capicom.msi

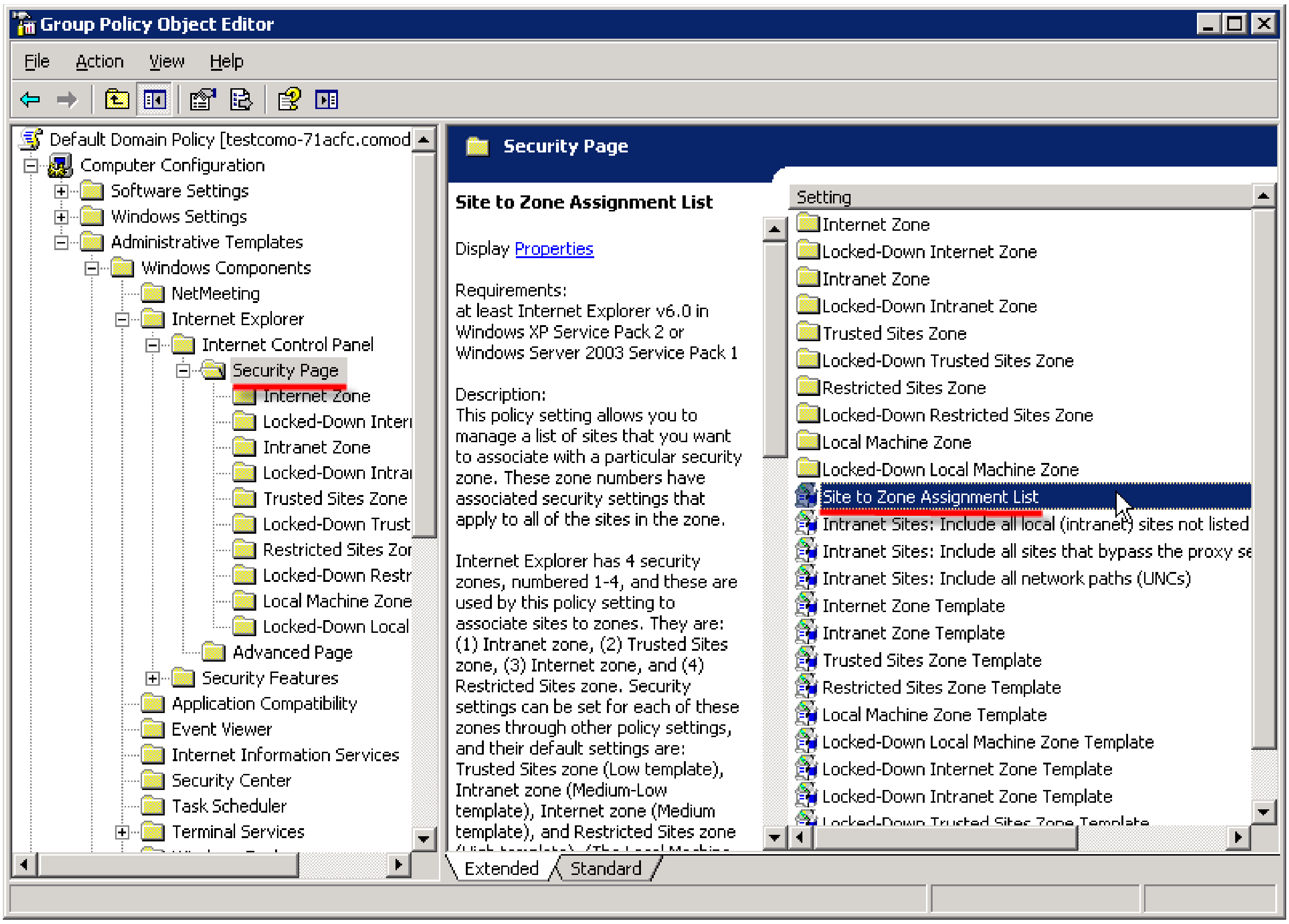
Figure 3.13 capicom.msi is added to Group Policy

- 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\InCommon\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)



Site to Zone Assignment List

Display Properties

Requirements:
at least Internet Explorer v6.0 in Windows XP Service Pack 2 or Windows Server 2003 Service Pack 1

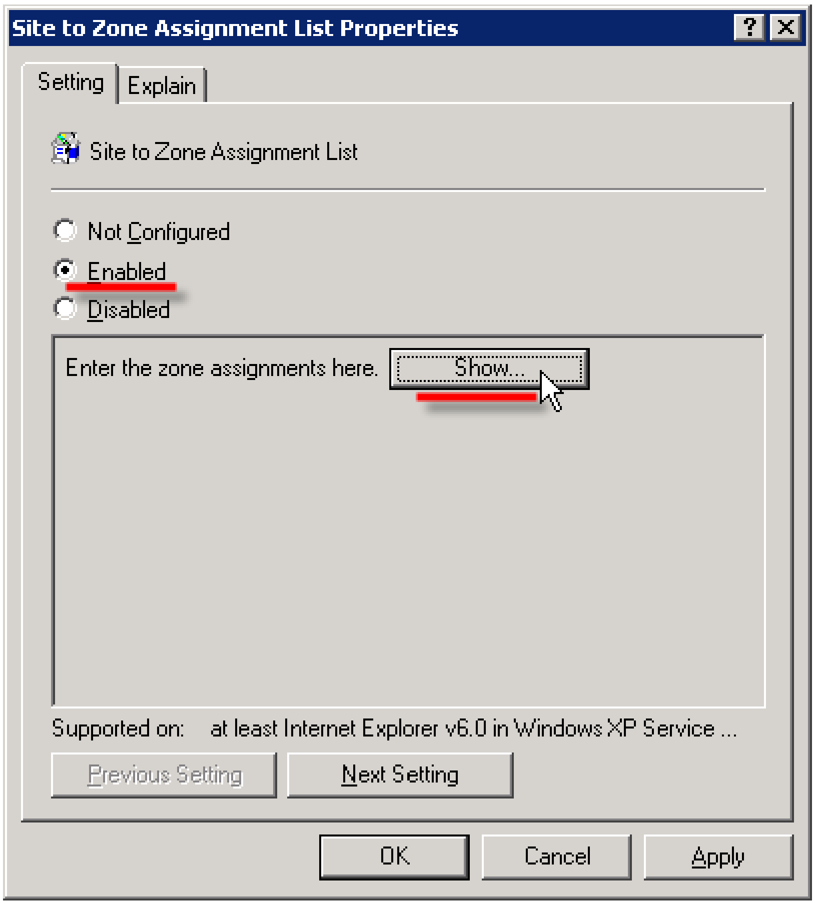
Description:
This policy setting allows you to manage a list of sites that you want to associate with a particular security zone. These zone numbers have associated security settings that apply to all of the sites in the zone.

Internet Explorer has 4 security zones, numbered 1-4, and these are used by this policy setting to associate sites to zones. They are: (1) Intranet zone, (2) Trusted Sites zone, (3) Internet zone, and (4) Restricted Sites zone. Security settings can be set for each of these zones through other policy settings, and their default settings are: Trusted Sites zone (Low template), Intranet zone (Medium-Low template), Internet zone (Medium template), and Restricted Sites zone

- Internet Zone
- Locked-Down Internet Zone
- Intranet Zone
- Locked-Down Intranet Zone
- Trusted Sites Zone
- Locked-Down Trusted Sites Zone
- Restricted Sites Zone
- Locked-Down Restricted Sites Zone
- Local Machine Zone
- Locked-Down Local Machine Zone
- Site to Zone Assignment List
- Intranet Sites: Include all local (intranet) sites not listed
- Intranet Sites: Include all sites that bypass the proxy se
- Intranet Sites: Include all network paths (UNCs)
- Internet Zone Template
- Intranet Zone Template
- Trusted Sites Zone Template
- Restricted Sites Zone Template
- Local Machine Zone Template
- Locked-Down Local Machine Zone Template
- Locked-Down Internet Zone Template
- Locked-Down Intranet Zone Template
- Locked-Down Trusted Sites Zone Template

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.


Site to Zone Assignment List Properties

Site to Zone Assignment List

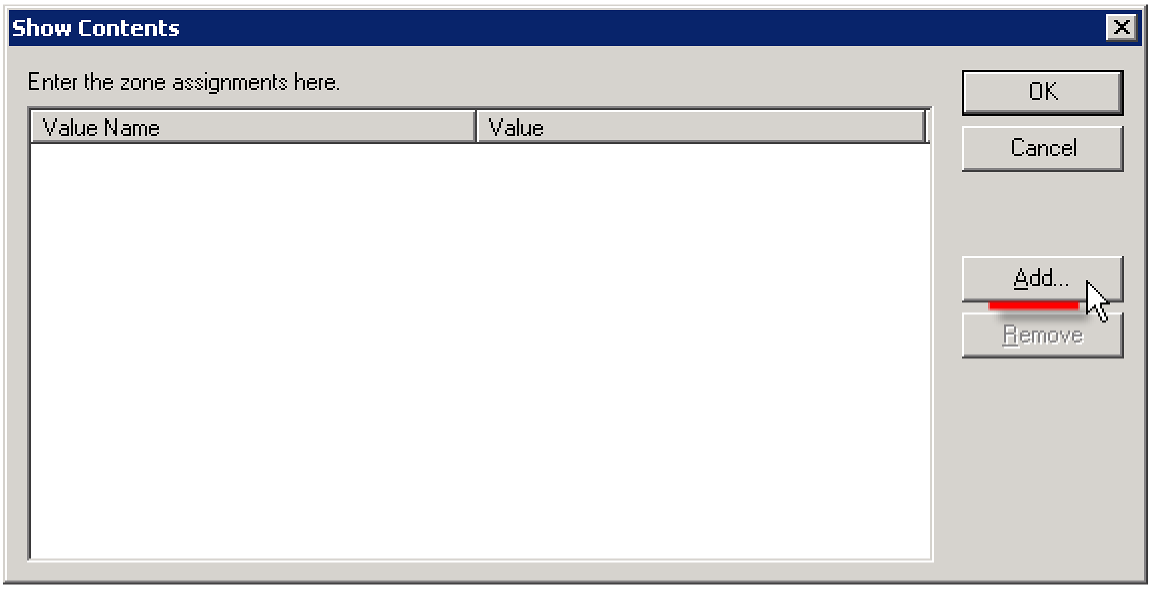
○ Not Configured
● Enabled
○ Disabled

Enter the zone assignments here. Show...

Supported on: at least Internet Explorer v6.0 in Windows XP Service ...

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.

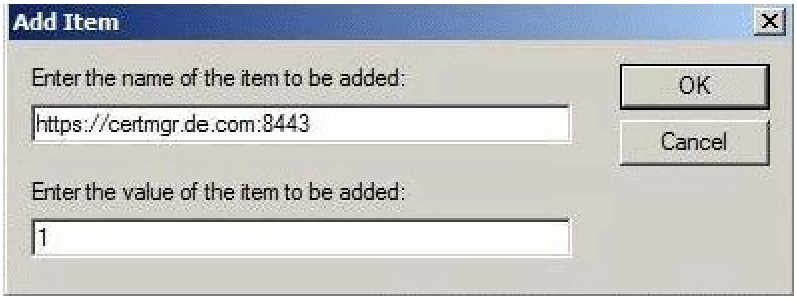

Show Contents

Enter the zone assignments here.

Value Name	Value

Figure 3.16 Add new zone assignment

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



Add Item

Enter the name of the item to be added:

https://certmgr.de.com:8443

Enter the value of the item to be added:

1

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 InCommon CA's root certificate and InCommon CM 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)

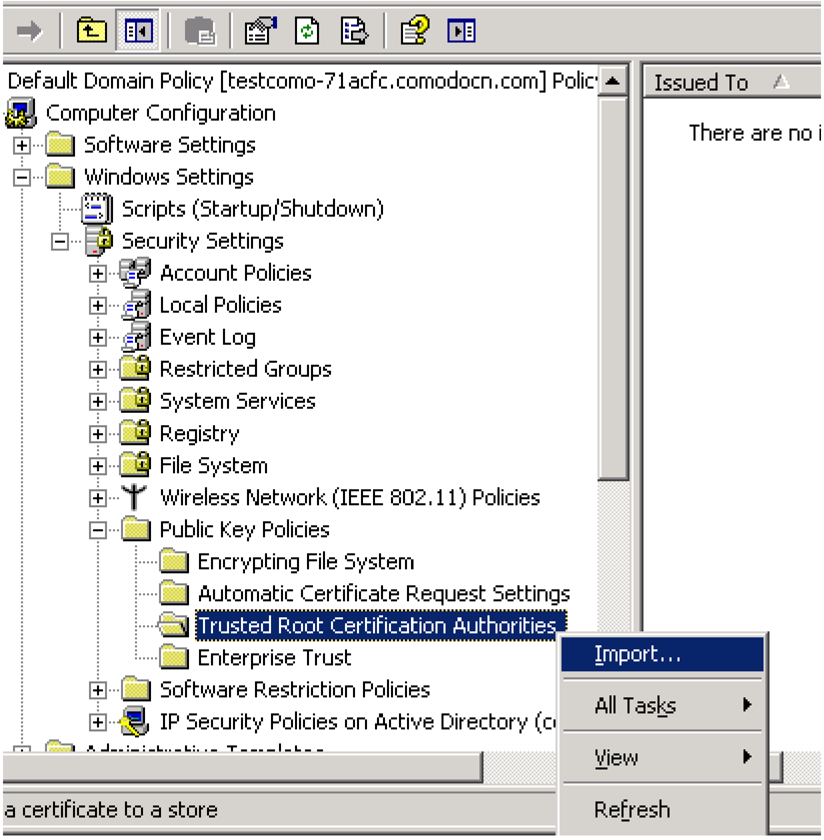
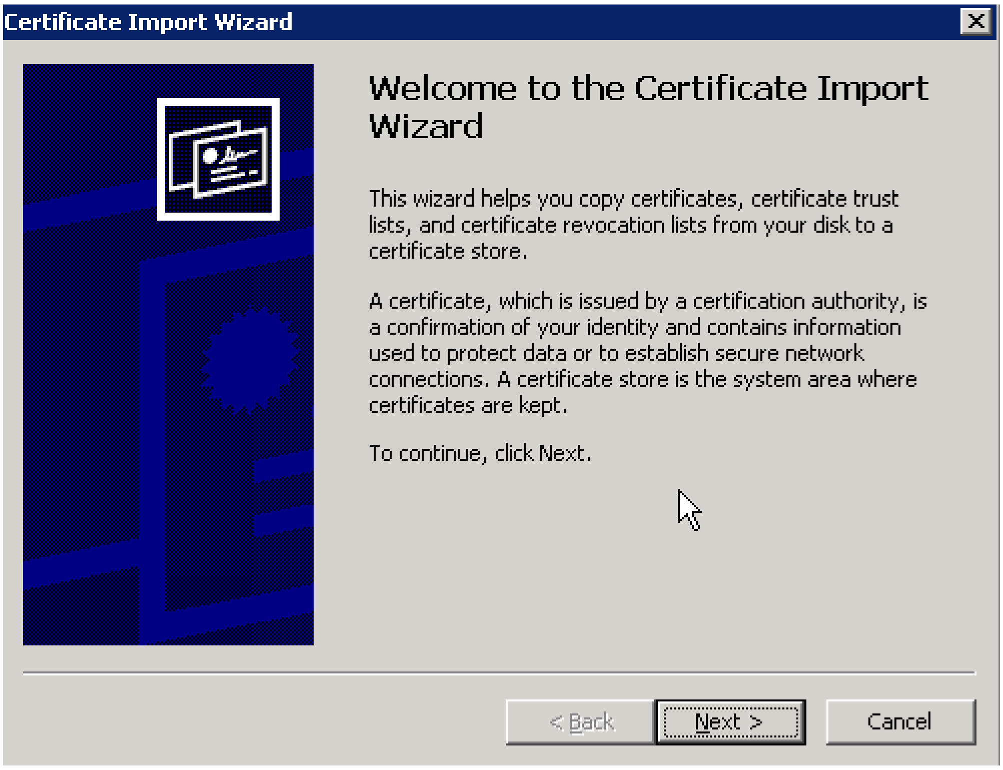


Figure 3.18 Navigate to Trusted Root Certificate Authorities



Certificate Import Wizard

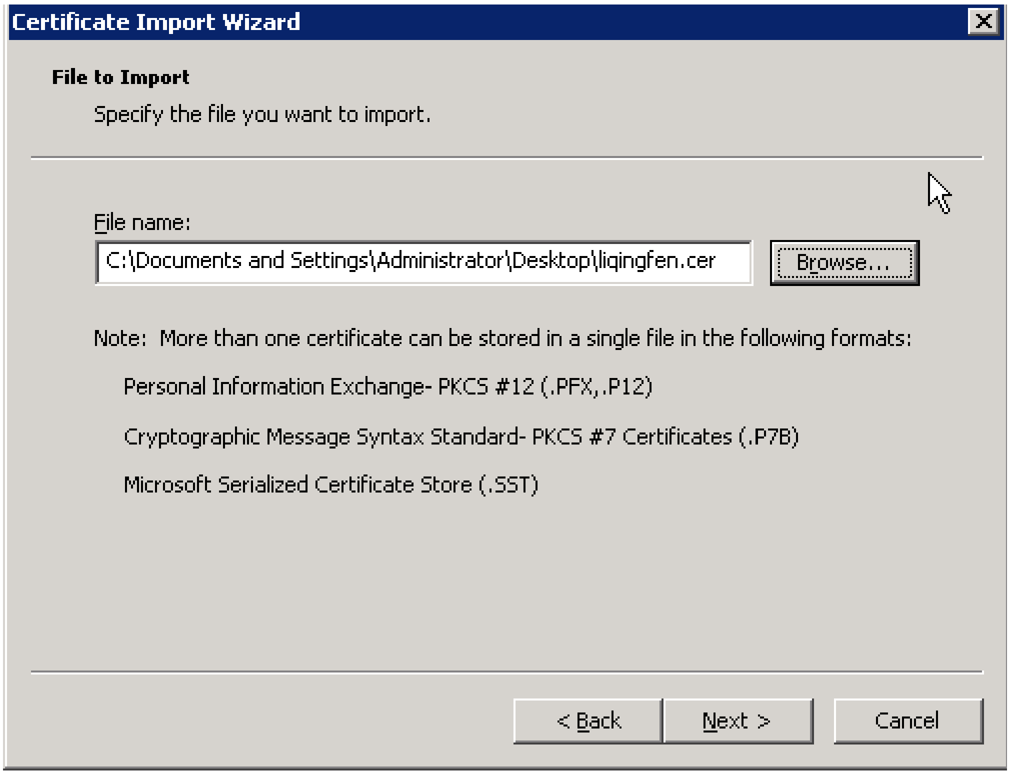
Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

Figure 3.19 Certificate Import Wizard



Certificate Import Wizard

File to Import

Specify the file you want to import.

File name: C:\Documents and Settings\Administrator\Desktop\liqingfen.cer

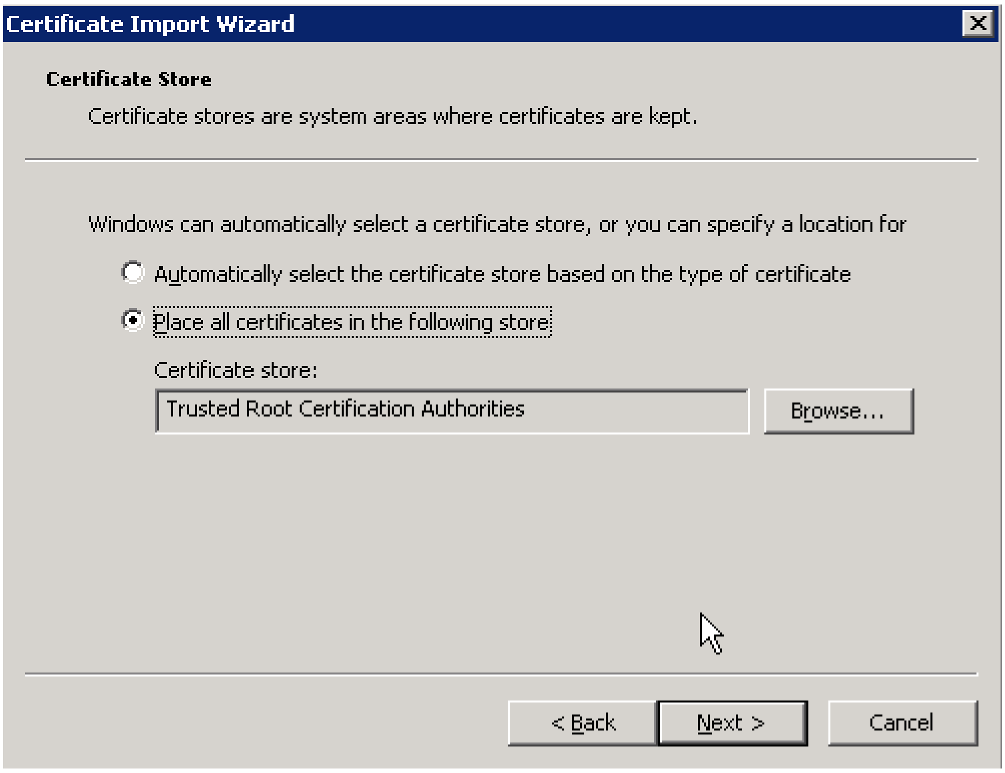
Note: More than one certificate can be stored in a single file in the following formats:

Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

Figure 3.20 Select certificate file to import



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for

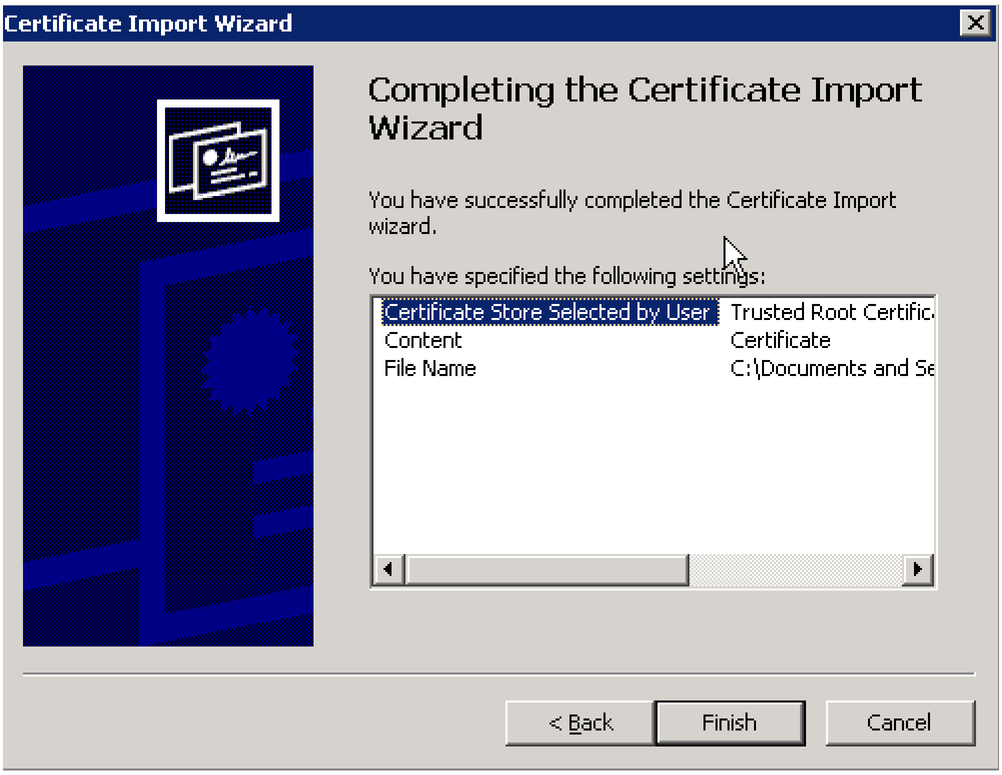
○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store:

Trusted Root Certification Authorities

Figure 3.21 Select certificate store



Certificate Import Wizard

Completing the Certificate Import Wizard

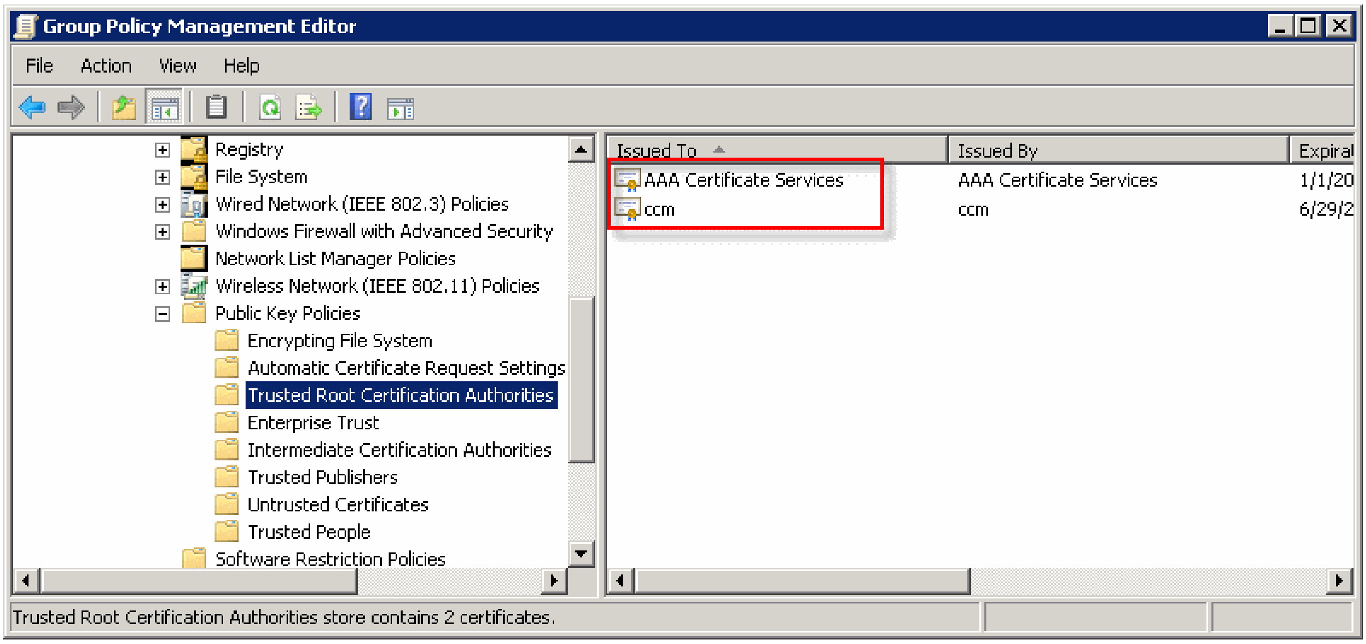
You have successfully completed the Certificate Import wizard.

You have specified the following settings:

Certificate Store Selected by User	Trusted Root Certific
Content	Certificate
File Name	C:\Documents and Se

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.



Group Policy Management Editor

Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Firewall with Advanced Security
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Encrypting File System
Automatic Certificate Request Settings
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates
Trusted People
Software Restriction Policies

Issued To	Issued By	Expiral
AAA Certificate Services	AAA Certificate Services	1/1/20
ccm	ccm	6/29/2

Trusted Root Certification Authorities store contains 2 certificates.

Figure 3.23 Imported 2 certificates in Group Policy

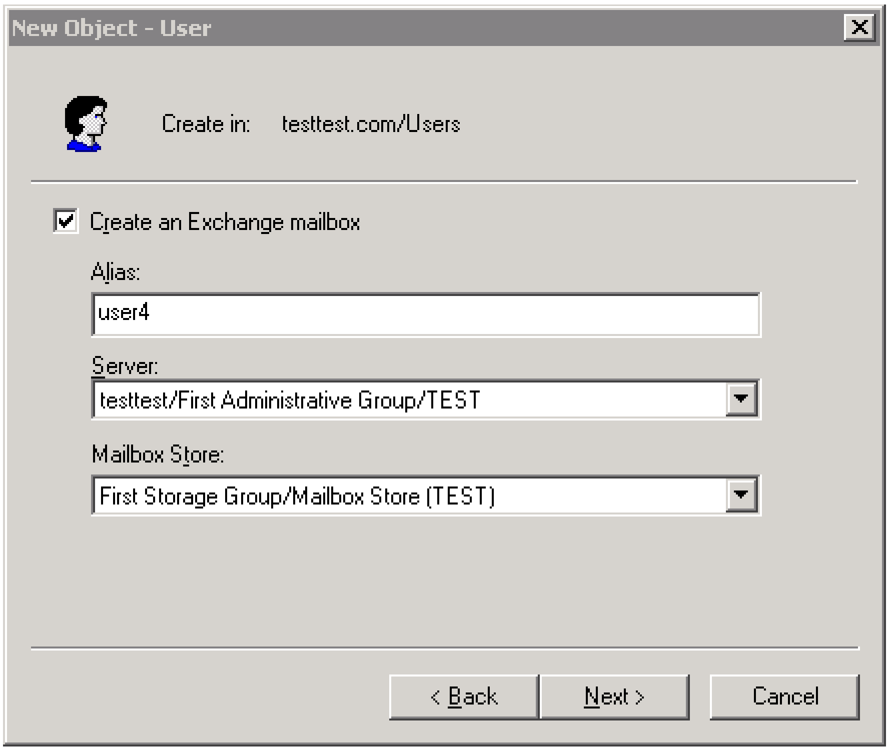
3.7 Create User Accounts on Active Directory with Email Box

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.



New Object - User

Create in: testtest.com/Users

☑ Create an Exchange mailbox

Alias: user4

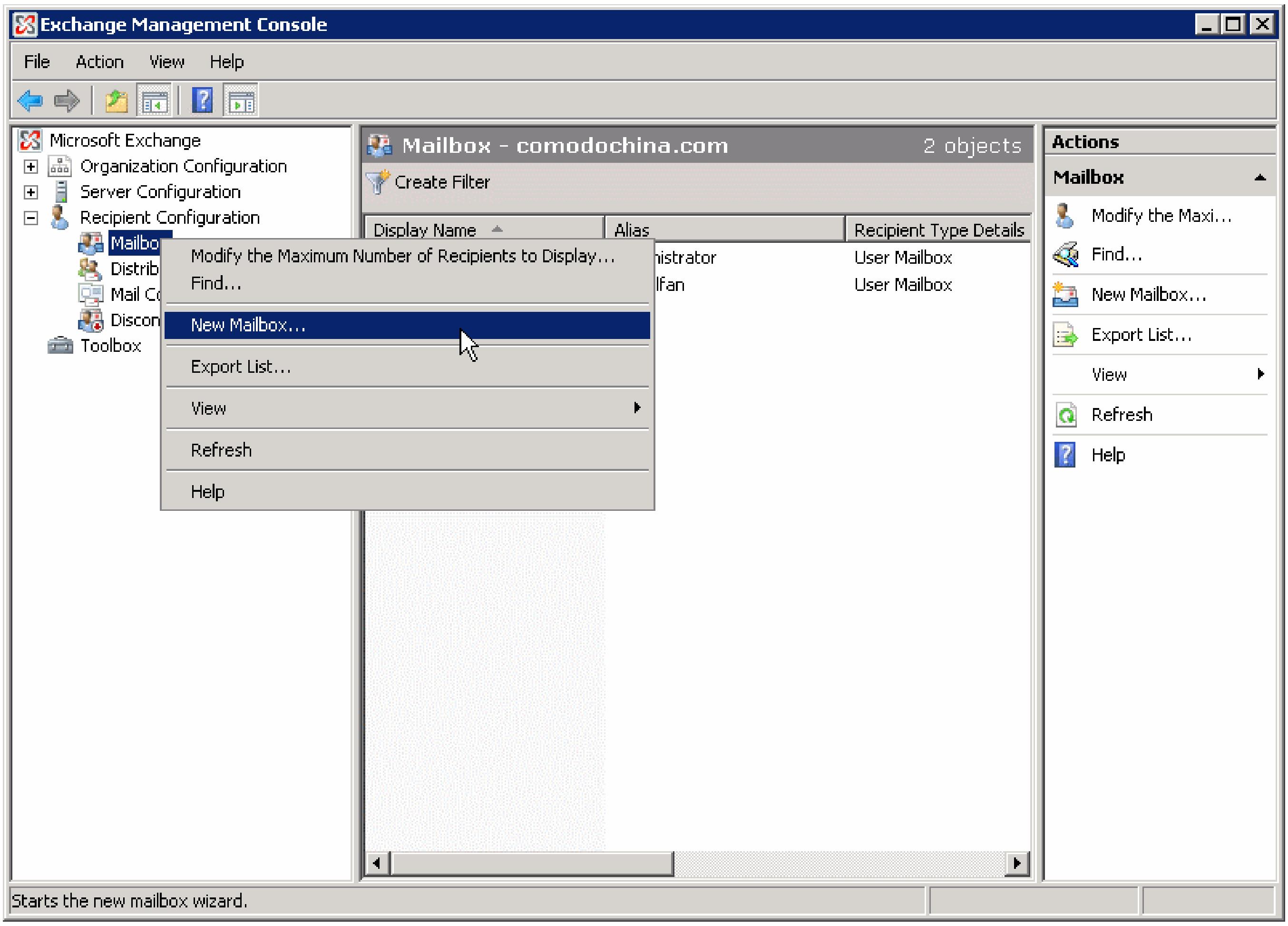
Server: testtest/First Administrative Group/TEST

Mailbox Store: First Storage Group/Mailbox Store (TEST)

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.

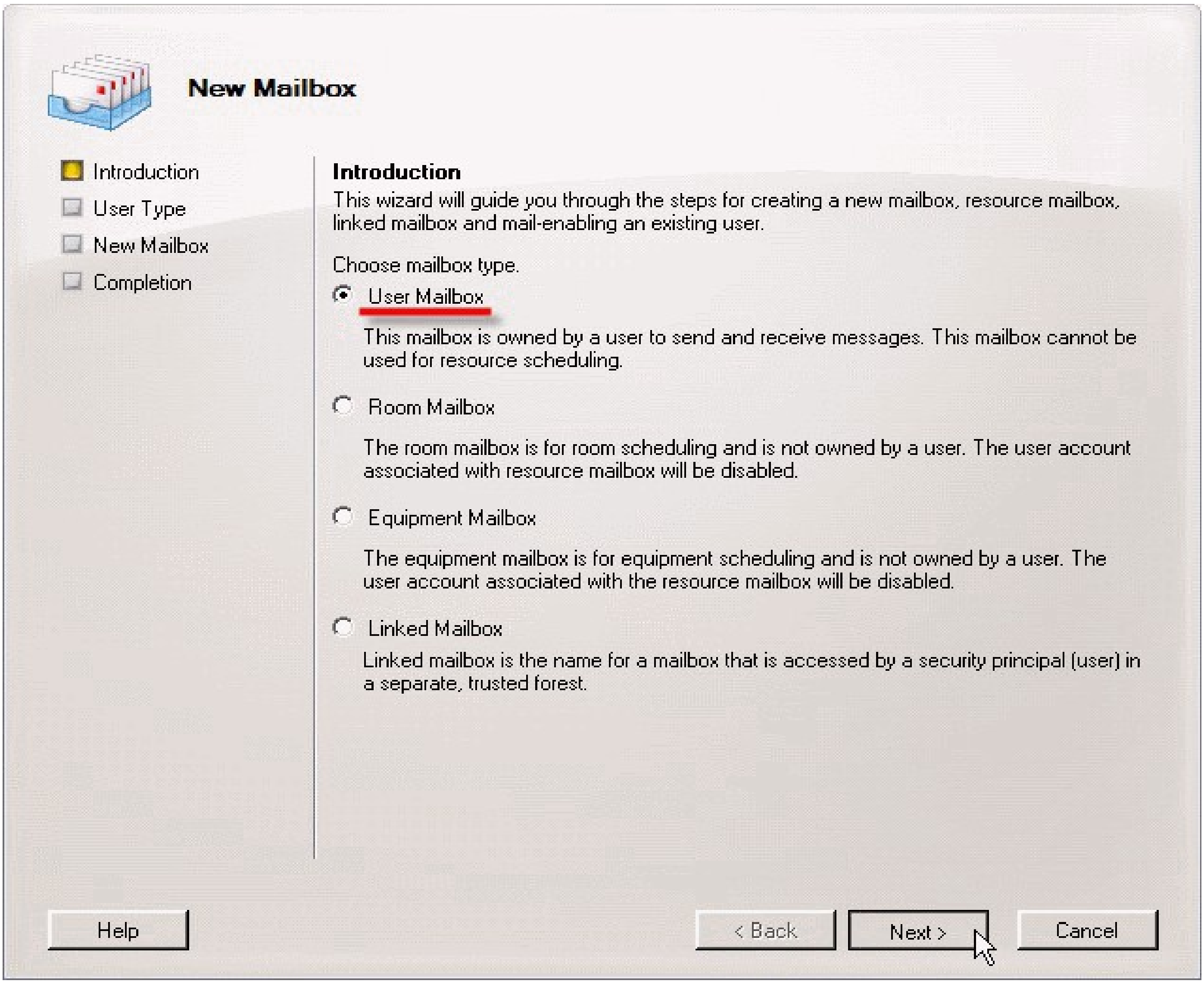


Display Name	Alias	Recipient Type Details
	istrator	User Mailbox
	lfan	User Mailbox

Starts the new mailbox wizard.

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.



Introduction

This wizard will guide you through the steps for creating a new mailbox, resource mailbox, linked mailbox and mail-enabling an existing user.

Choose mailbox type.

● User Mailbox

This mailbox is owned by a user to send and receive messages. This mailbox cannot be used for resource scheduling.

○ Room Mailbox

The room mailbox is for room scheduling and is not owned by a user. The user account associated with resource mailbox will be disabled.

○ Equipment Mailbox

The equipment mailbox is for equipment scheduling and is not owned by a user. The user account associated with the resource mailbox will be disabled.

○ Linked Mailbox

Linked mailbox is the name for a mailbox that is accessed by a security principal (user) in a separate, trusted forest.

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.

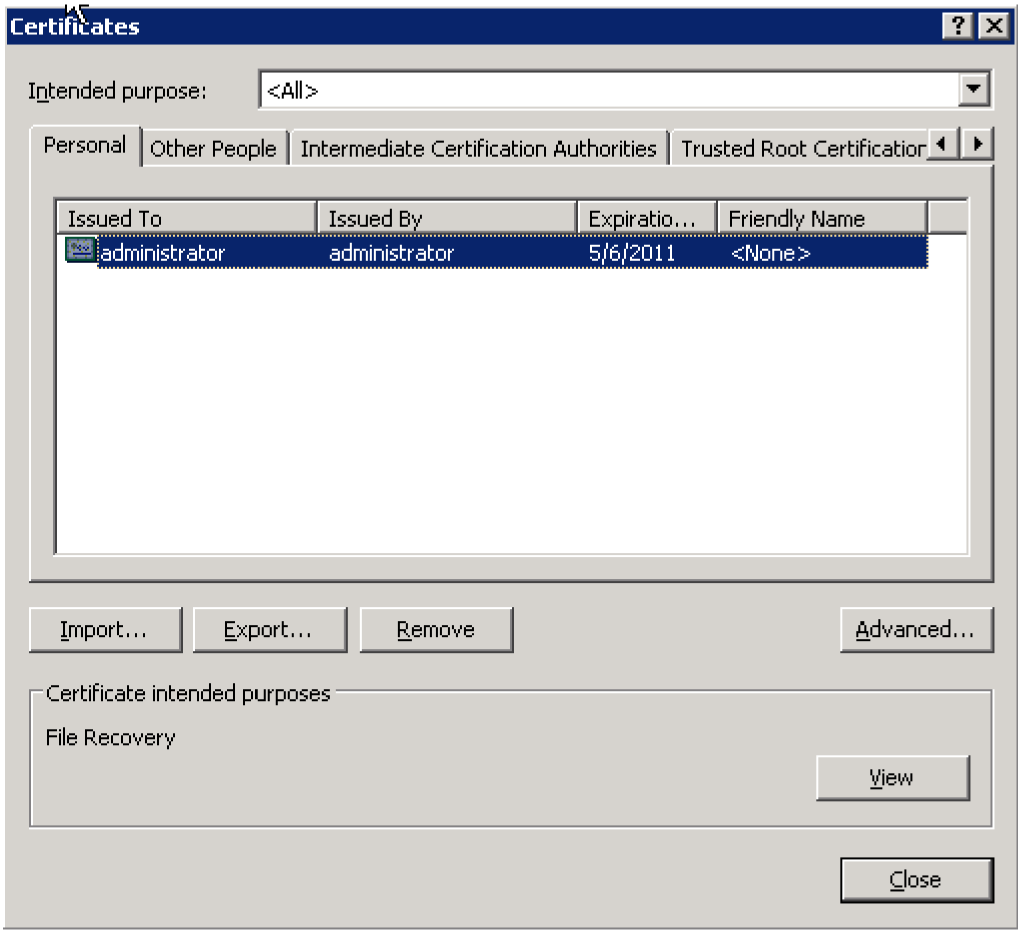
Restart the client PC and logon domain as domain user.

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



Certificates

Intended purpose: <All>

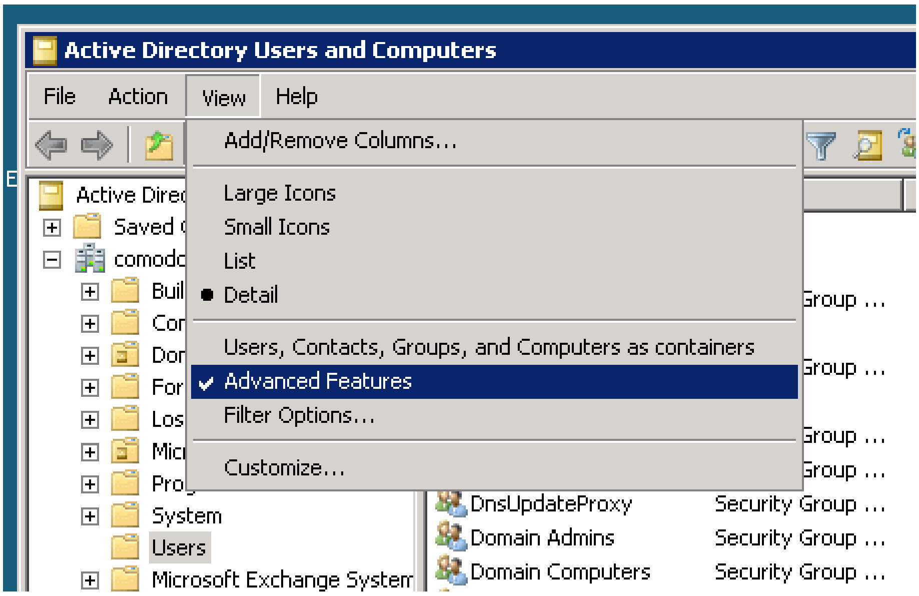
Issued To	Issued By	Expiratio...	Friendly Name
administrator	administrator	5/6/2011	<None>

Certificate intended purposes

File Recovery

Personal
Other People
Intermediate Certification Authorities
Trusted Root Certification
Import...
Export...
Remove
Advanced...
View
Close

Figure 5.1 Check personal certificate



Active Directory Users and Computers

View menu: Add/Remove Columns..., Large Icons, Small Icons, List, ● Detail, Users, Contacts, Groups, and Computers as containers, ✓ Advanced Features, Filter Options..., Customize...

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/csm.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 InCommon CM server

7 Known Issues

7.1 Don't Use InCommon CM Server Machine as Client

If use csm 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 InCommon 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

download and install the hotfix.

8 Troubleshootings

8.1 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 services 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 installed the InCommon CM 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.