

Enabling LDAPS on a Domain Controller

by Albert Lunde

December 14, 2006

Version: A

Enabling LDAPS on a Domain Controller

The Radiant Logic synchronization software communicates via LDAPS, so any domain controllers used with it will require an SSL certificate.

There is no specific option to turn on LDAPS. It just turns itself on if you've installed a trusted SSL key/certificate pair on your domain controller

The most likely ways to do this are either to get a certificate signed by our private "nuca" certificate authority or to run a Microsoft Certificate Authority integrated with Active Directory.

Microsoft talks about domain controller certificates in several articles.

One article gives a long, complex recipe for creating a domain controller certificate with an off-line Microsoft Certificate Authority. All the described X.509 attributes are apparently set up almost automatically if you run a Microsoft Certificate Authority integrated with Active Directory.

Another article gives a shorter cookbook for creating a certificate using a third party certificate authority. This is the basis of what we do if you want a certificate signed by our private "nuca" certificate authority.

The article giving the simplified approach is:

"How to enable LDAP over SSL with a third-party certification authority"

<<http://support.microsoft.com/default.aspx?scid=kb;en-us;321051>>

The Microsoft CA approaches are described in:

"Advanced Certificate Enrollment and Management"

<<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/advcert.msp>>

and a related page,

"Requirements for Domain Controller Certificates from a Third-Party CA"

<<http://support.microsoft.com/default.aspx?scid=kb;en-us;Q291010>>

Some forests at NU have used each approach.

There are significant features enabled by running a Microsoft Certificate Authority integrated with Active Directory. On the other side, it's more complex to set up and requires running an IIS web server with ASP enabled, on the certificate authority, which might be considered a security risk.

Using Our Private Certificate Authority

The steps involved are:

1. Create in input file for the certreq command.

2. Generate a key and certificate with "certreq":

```
certreq -new request.inf request.req
```

3. Send the file "request.req" to Xiaoxia Dong at x-dong@northwestern.edu

(She will sign it with our OpenSSL-based private Certificate Authority, and return the new certificate)

4. Accept the certificate with certreq:

```
certreq -accept filename
```

5. Set up your domain controller to trust our CA certificate, using "Certificates" MMC Snap-in. This is described in more detail in the following section.

The actual input to certreq for a test domain, "it.northwestern.edu", looked like this:

```
- - - cut here - - -
;----- request.inf -----

[Version]

Signature="$Windows NT$"

[NewRequest]

Subject = "CN=itdcl.it.northwestern.edu,OU=Domain
Controllers,DC=it,DC=northwestern,DC=edu,O=Northwestern
University,L=Evanston,S=Illinois,C=US"
;
KeySpec = 1
KeyLength = 1024
Exportable = TRUE
MachineKeySet = TRUE
SMIME = False
PrivateKeyArchive = FALSE
UserProtected = FALSE
UseExistingKeySet = FALSE
ProviderName = "Microsoft RSA SChannel Cryptographic Provider"
ProviderType = 12
RequestType = PKCS10
KeyUsage = 0xa0

[EnhancedKeyUsageExtension]

OID=1.3.6.1.5.5.7.3.1 ; this is for Server Authentication
;-----
- - - cut here - - -
```

Setting up trust for a certificate authority

The file cacert.cer is our local "nuca" CA certificate in pem/base64-encoded format with extra text before and after the certificate removed. Like thus:

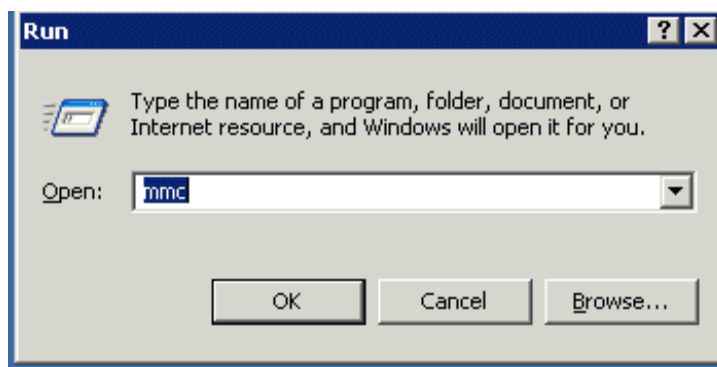
```
-----BEGIN CERTIFICATE-----
MIID4jCCA0ugAwIBAgIBADANBgkqhkiG9w0BAQQFADCBRTelMAkGA1UEBhMCVVMx
ETAPBgNVBAGTCe1sbG1ub21zMREwDwYDVQQHEWhFdmFuc3Rvb3JlEgMB4GA1UEChMx
Tm9ydGh3ZXN0ZXJlIFVuaXZlcnNpdHkxH3AdBgNVBAsTFkluZm9ybWF0aW9uIFRl
Y2hub2xvZ3kxDTALBgNVBAMTBG51Y2ExJjAkBgkqhkiG9w0BCQEF3gtZG9uZ0Bu
b3J0aHdlc3R1cm4uZWRLMB4XDTAzMDUyMzE1Mjg0NjEwXDEwMDEwMDEwMDEwMDEw
ga0xOzA0BjBGNVBAITAlVTMREwDwYDVQQIEWhJbGxpbm9pczERMA8GA1UEBxMIRXZh
bnN0b24xIDAeBgNVBAoTF05vcnRod2VzdGVybiBVbml2ZXJzaXR5MR8wHQYDVQQL
ExZJb250b24xIDAeBgNVBAMTb250b24xMjE1MjE1MjE1MjE1MjE1MjE1MjE1MjE1
hvcNAQkBFhd4LWRvbmdbAbm9ydGh3ZXN0ZXJlLmVkdTCBnzANBgkqhkiG9w0BAQEF
AAOBjQAwGykCgYEA7r410160lvUm/iU2K5wjAoSohBklxBUuo1R8wIHTQkfIM3Jh
K01L1TMs3EfoVukw/roonkagXCr/hosg+WNym1ggq26ivR6yAyg+acRLAH7aGolzk
2uEw50IxG2Ldk3KgHJsw9RfTcrQlbn0duRPlwVUE9FPp9L1U0VRAGRrgUCAwEA
AaOQAQ4wggEKMB0GA1UdDgQWBQw71T07aZuPUap6Ru64HhwD1G0yzCB2gYDVR0j
BIHSMIHGpBQw71T07aZuPUap6Ru64HhwD1G0y6GBs6SBSDCBRTelMAkGA1UEBhMC
VVMxETAPBgNVBAGTCe1sbG1ub21zMREwDwYDVQQHEWhFdmFuc3Rvb3JlEgMB4GA1UE
ChMxTm9ydGh3ZXN0ZXJlIFVuaXZlcnNpdHkxH3AdBgNVBAsTFkluZm9ybWF0aW9u
IFRlY2hub2xvZ3kxDTALBgNVBAMTBG51Y2ExJjAkBgkqhkiG9w0BCQEF3gtZG9u
Z0Bub3J0aHdlc3R1cm4uZWRL1ggEAMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEE
BQADgYEAsHu9hKKKOfz1jJMavYTB6nITDhdARsMs/oRcPjxibGFUDuI8bgBDVM3
Fy6ZmL6kREpB+fYj4v0UKXZ0bGD9G4eCD1D35uTBkTHvbbIzhdpDkaNZaEZOBf54
fta4gYPY/y4LhJBhMSE1v4KxzqoX1UsfbsNCmNbfwyo0edxIkCM=
-----END CERTIFICATE-----
```

(A certificate dump would show this is "Subject: C=US, ST=Illinois, L=Evanston, O=Northwestern University, OU=Information Technology, CN=nuca/emailAddress=x-dong@northwestern.edu")

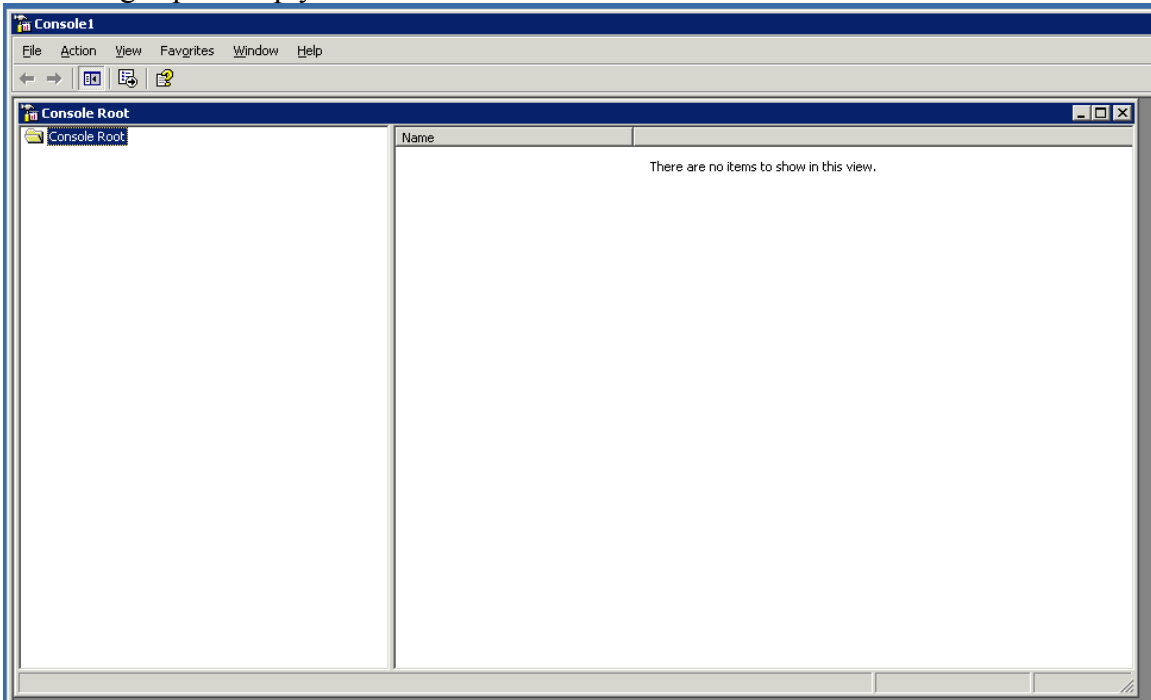
Transfer cacert.cer file to the domain controller. For example, transfer it via sftp to a trusted server, or by connecting via Remote Desktop with drive sharing enabled.)

Here is a step-by-step description of adding a trusted certificate authority on a domain controller with Windows 2003.

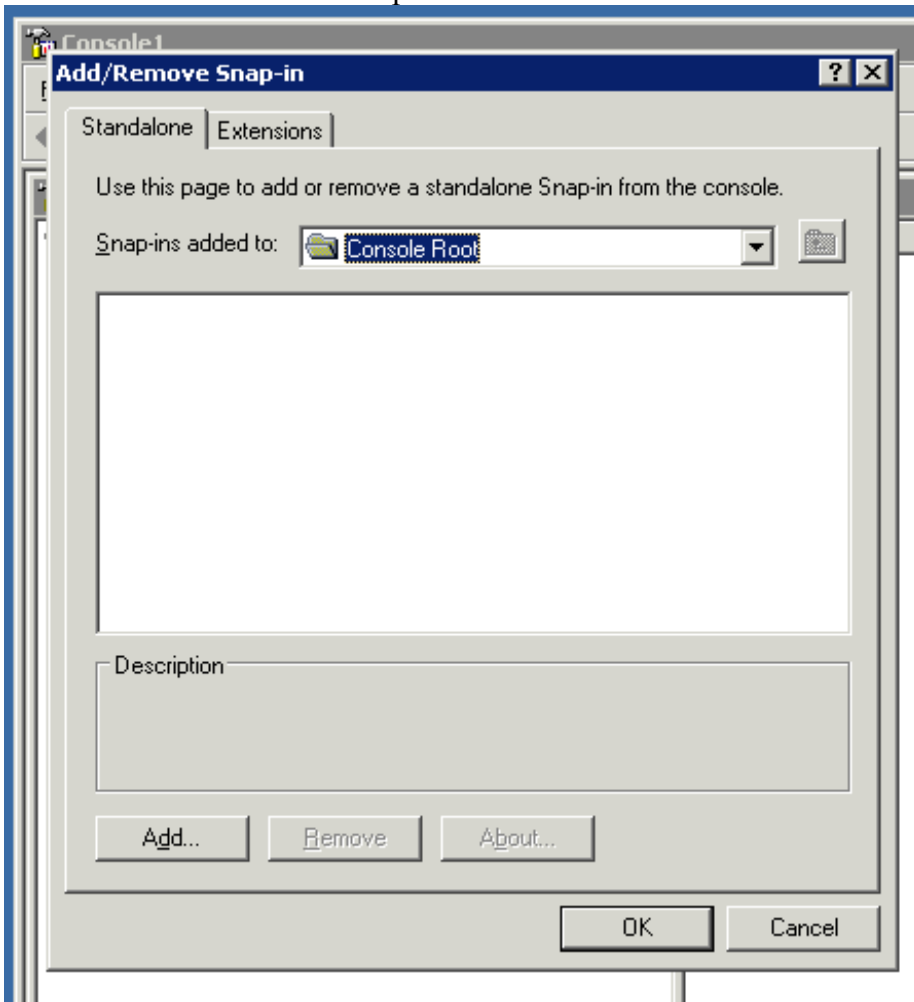
Pick "Start/Run...", enter "mmc":



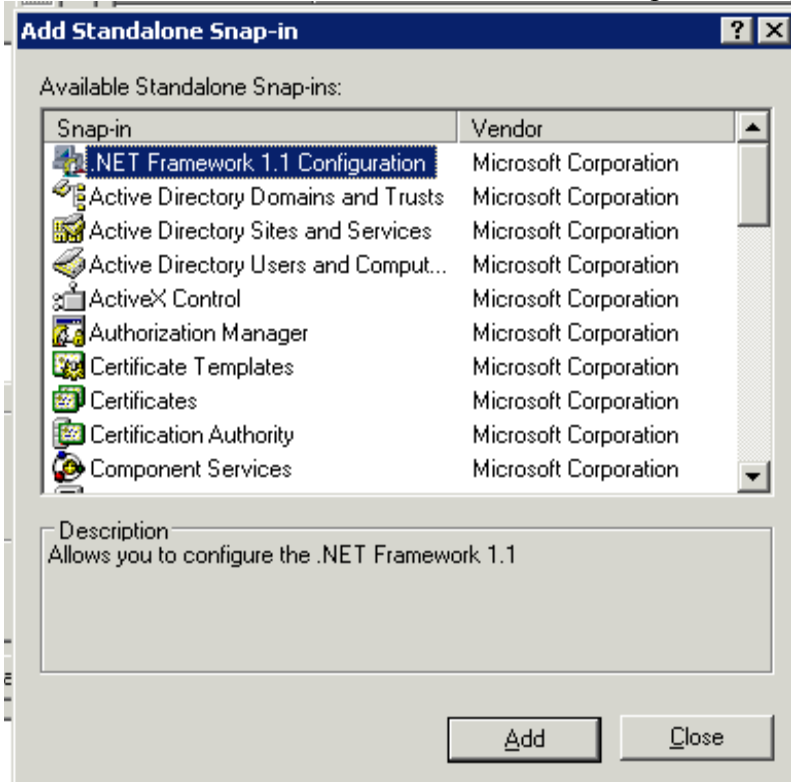
This brings up an empty MMC "Console" window:



Pick "File"/"Add Remove Snap-in..."



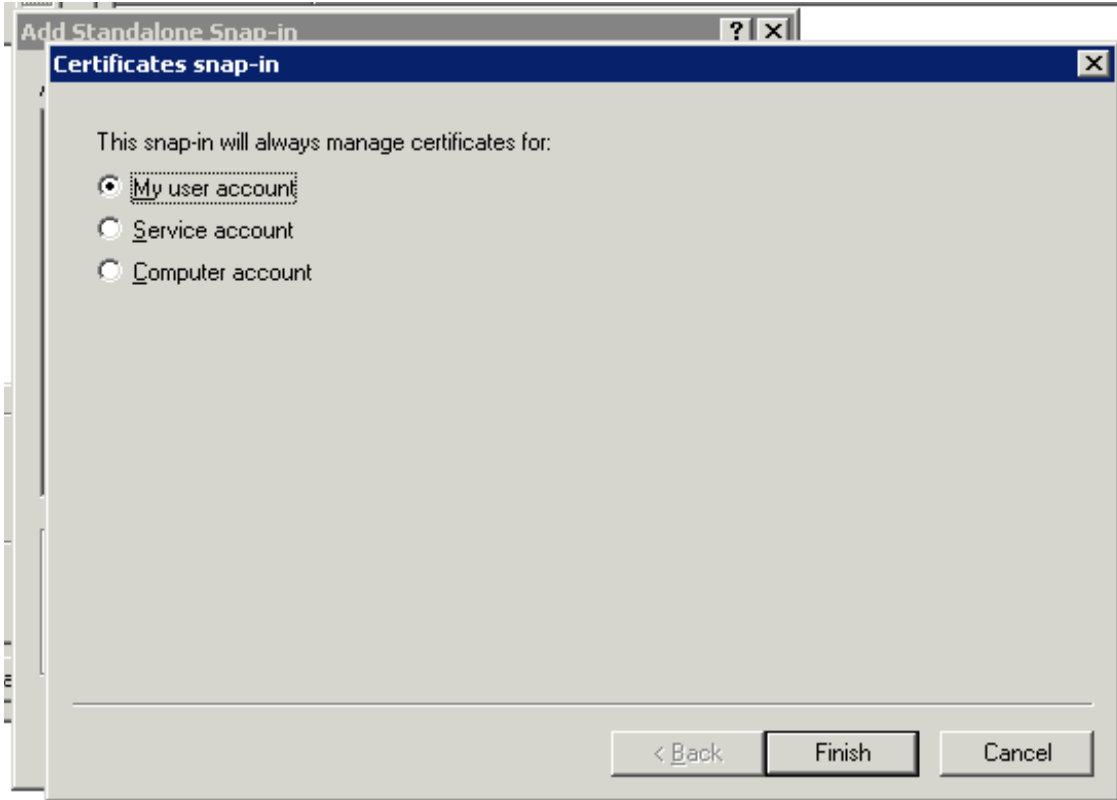
Click the "Add..." button in the "Add/Remove Snap-in" dialog box:



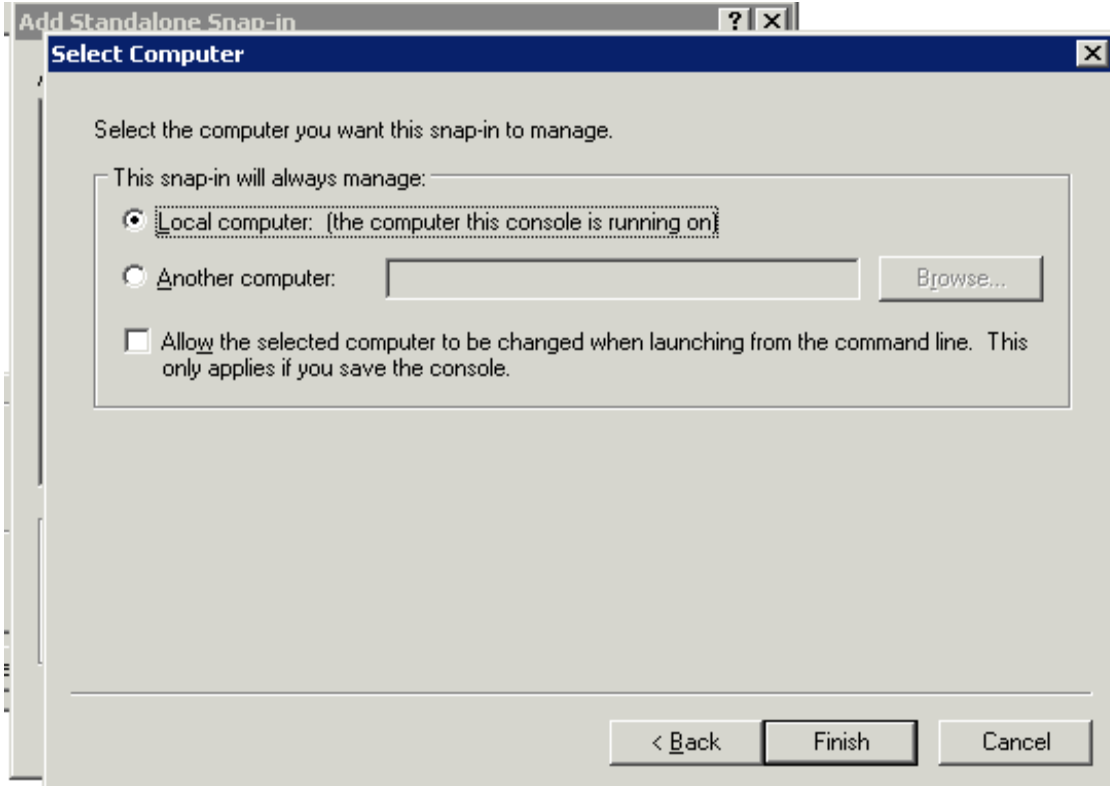
Pick "Certificates", in the list of "Available Standalone Snap-ins".

Click the "Add" button in the "Add Standalone Snap-in" dialog box, in the front.

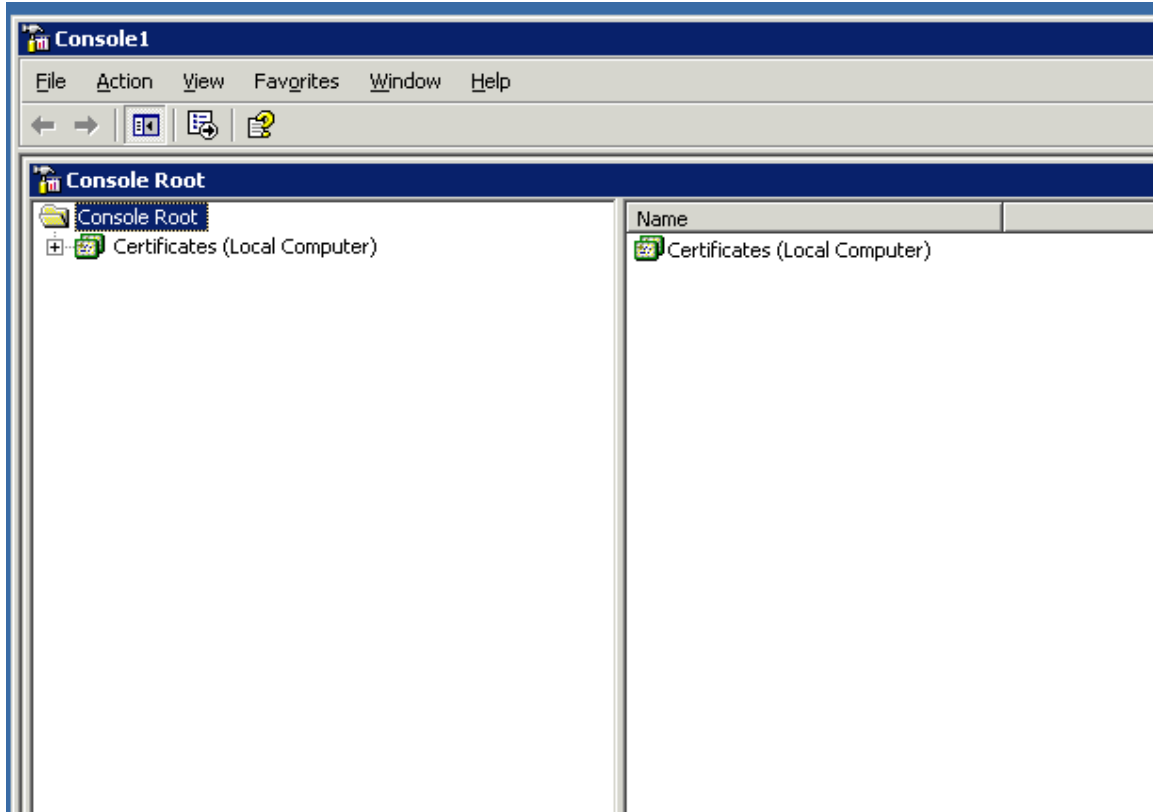
For "This snap-in will always manage certificates for", select "Computer account"; click "Next":



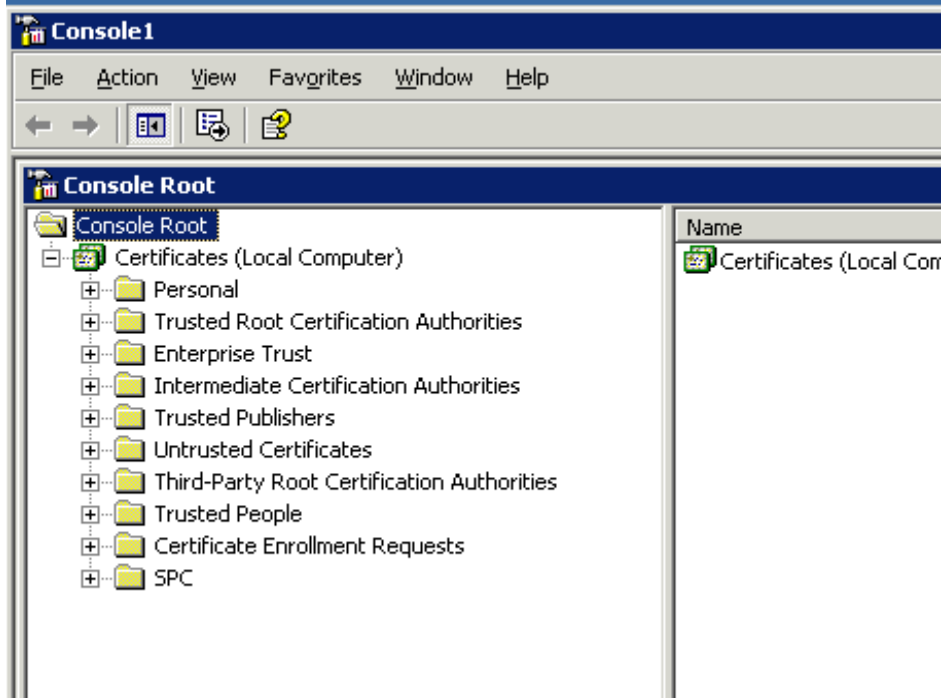
For "Select the computer you want this snap-in to manage", select "Local computer"; click "Finish":



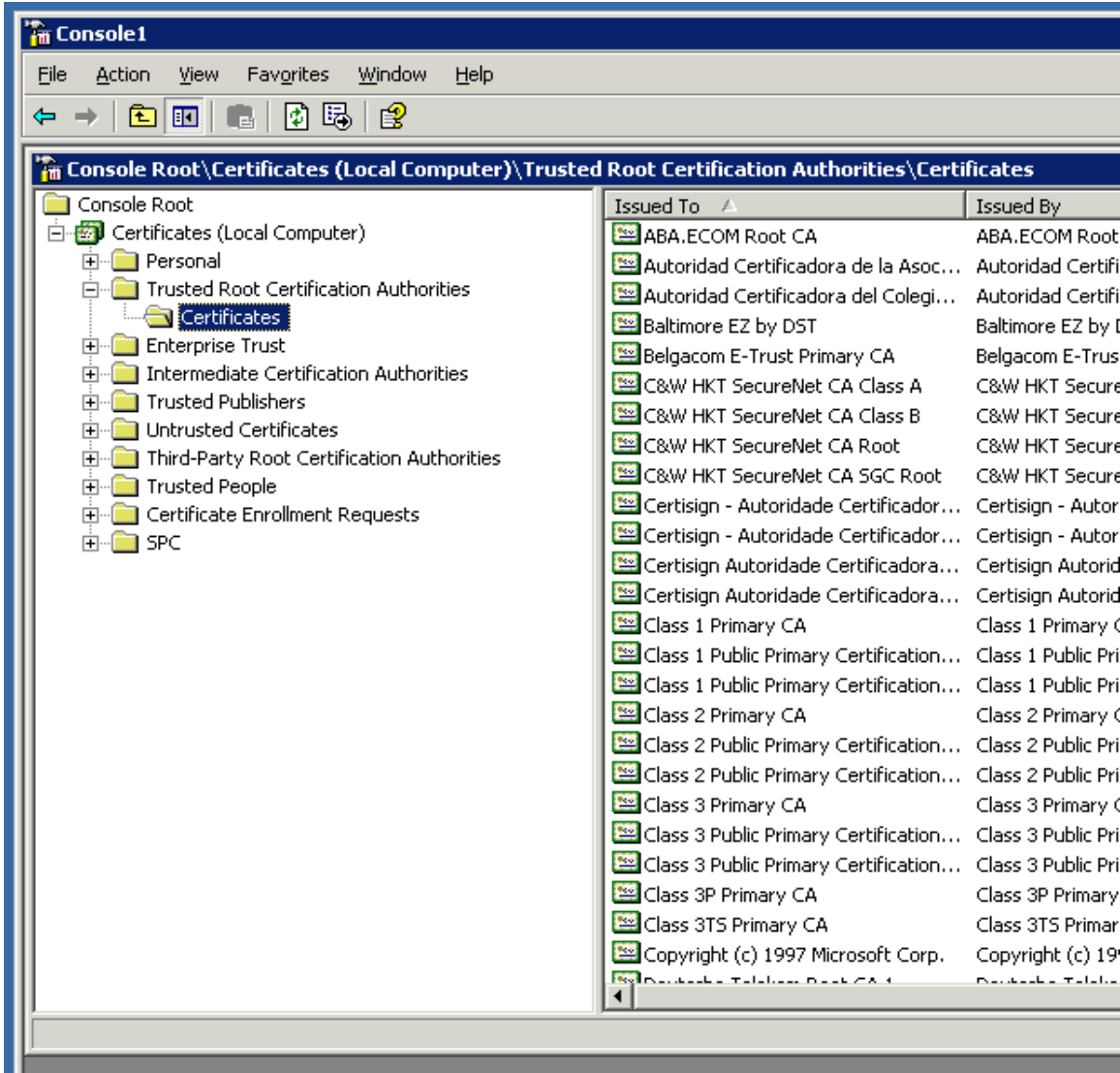
Click the "Close" button; click the "OK" button. Then you will see the Certificates console for the domain controller:



Click the "+" next to "Certificates (Local Computer)" to expand the tree:

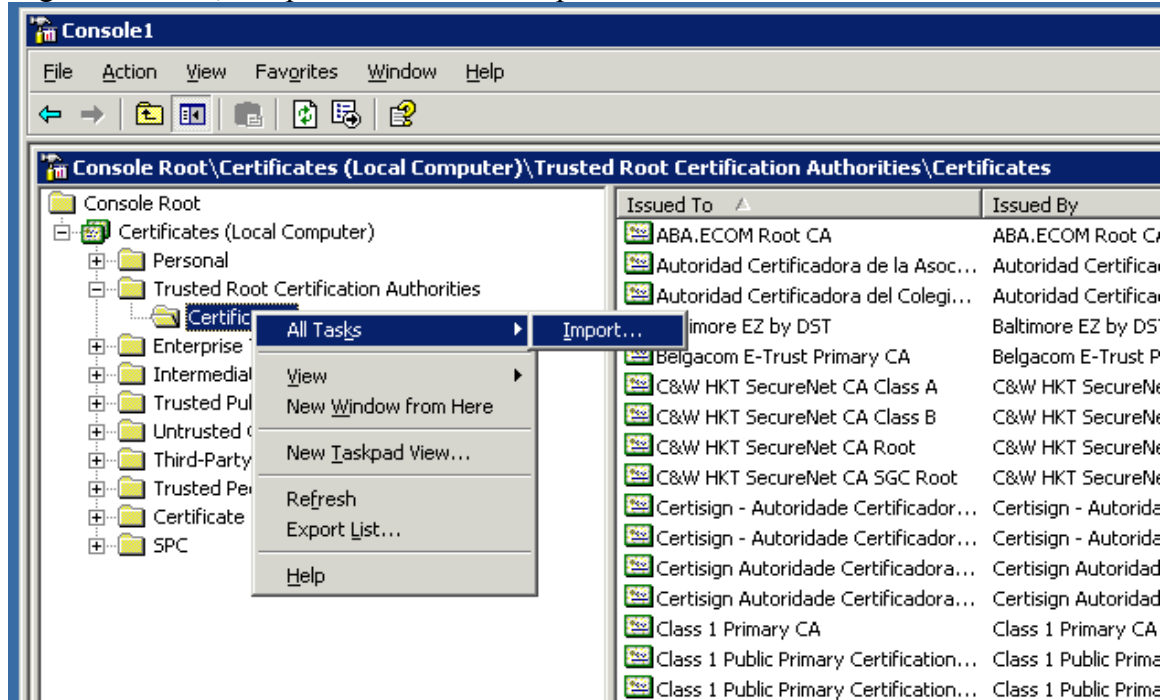


Click the "+" next to "Trusted Root Certification Authorities", exposing "Certificates" under it:



Select "Certificates"

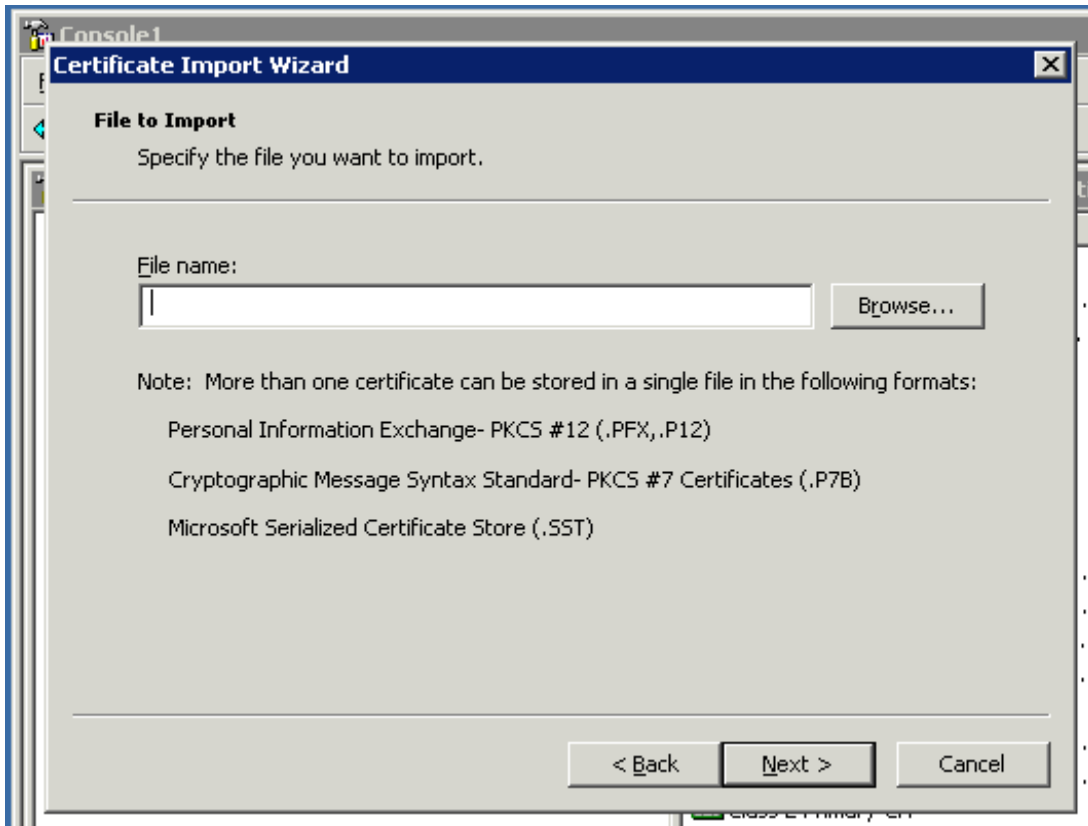
Right click on it, and pick "All Tasks"/"Import..."



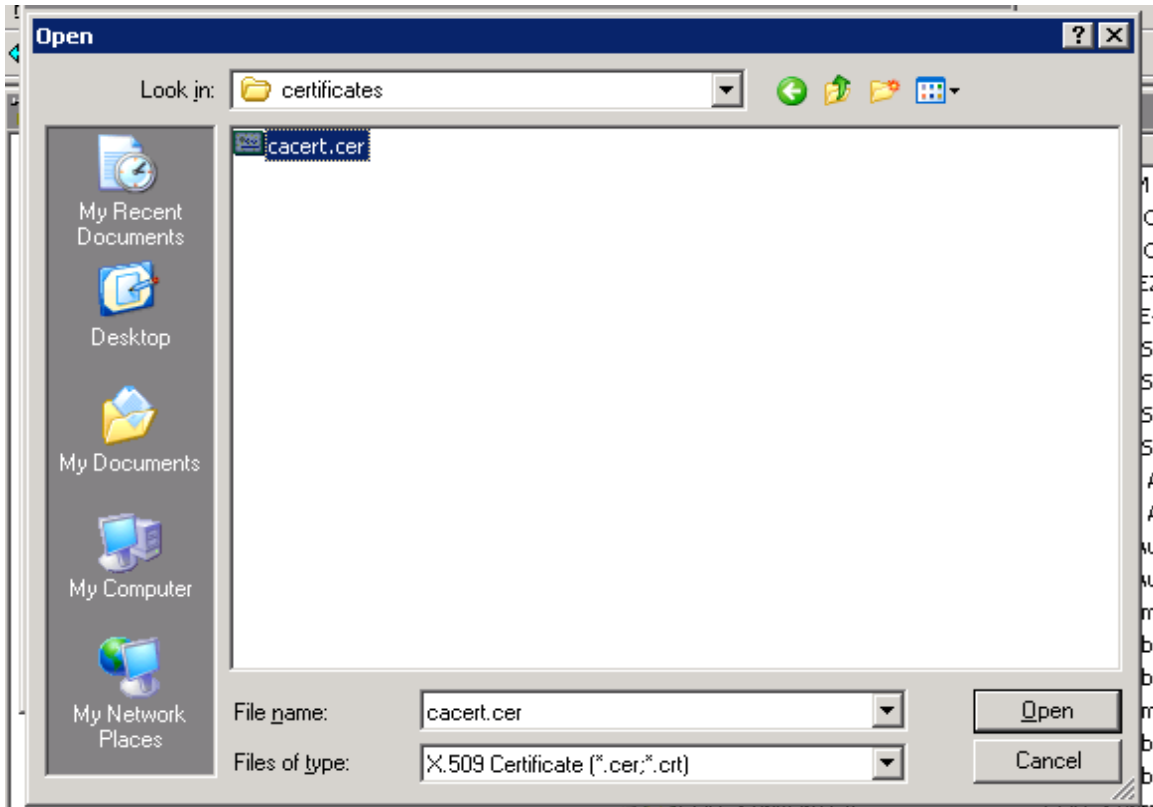
This should bring up the "Certificate Import Wizard":



Click the "Next" button:

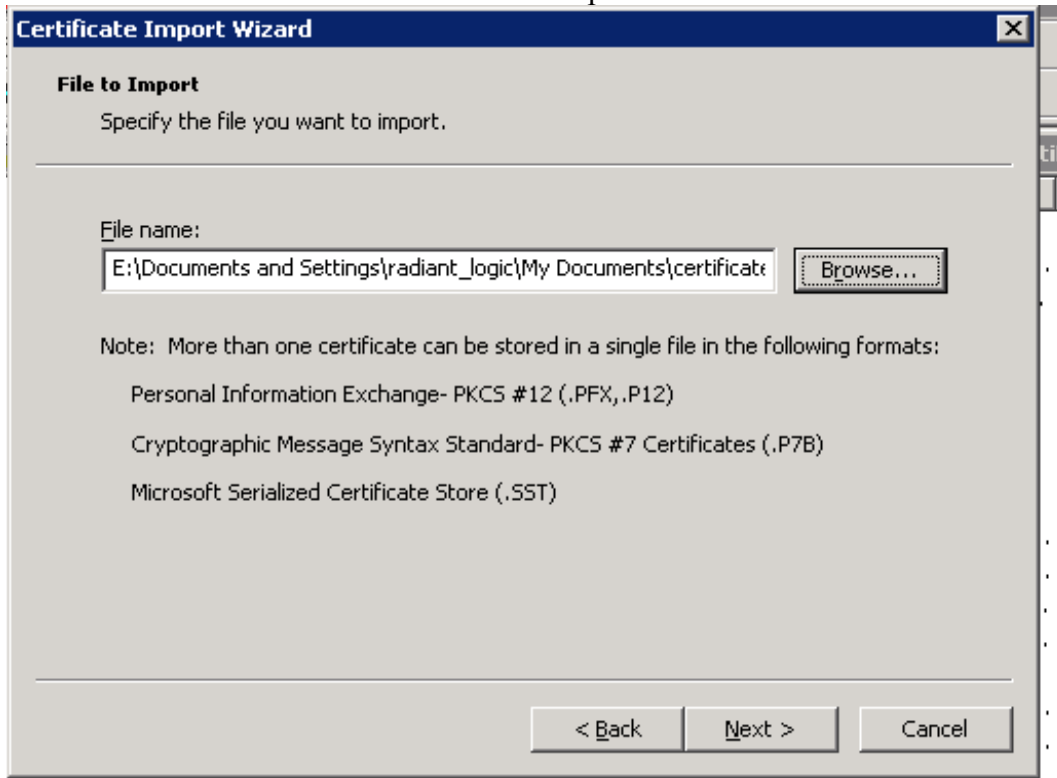


Click the "Browse..." button and locate and select the "cacert.cer" file:

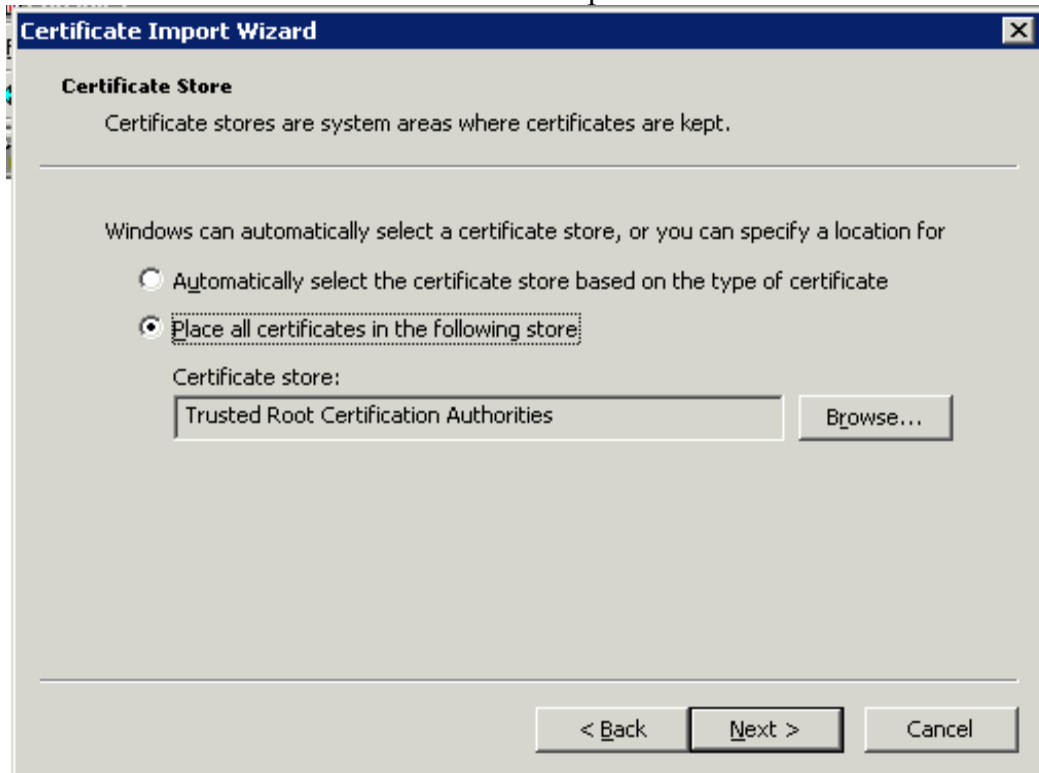


Click "Open" in the file dialog.

Click the "Next" button in the "Certificate Import Wizard":



Click the "Next" button in the "Certificate Import Wizard":



Click the "Finish" button in the "Certificate Import Wizard":

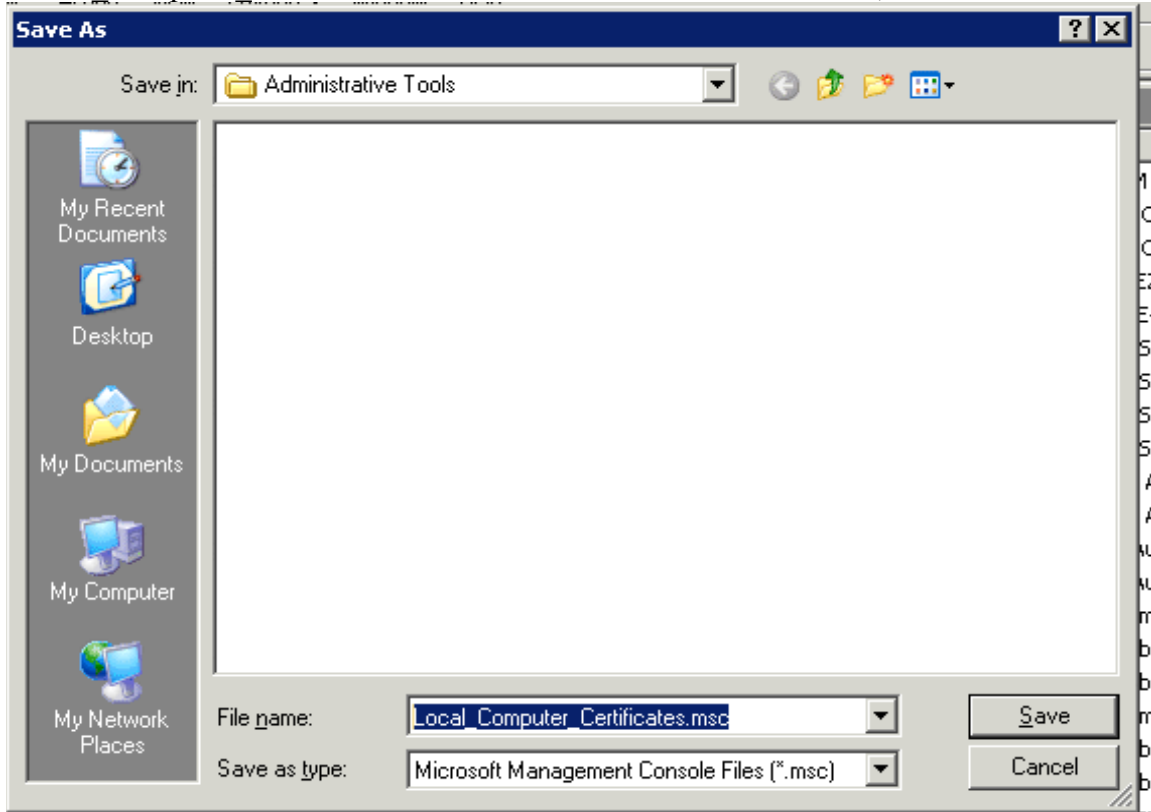


You should get a message "The import was successful"
Click "OK" to close it:



At this point LDAPS should be enabled on the Domain Controller.

Optionally, you can go to "File"/"Save As..." and save the console set-up, say, as "Local Computer Certificates.msc" with in "Administrative Tools";



This adds it to "Start"/"All Programs"/"Administrative Tools":

