The i500 Enterprise Directory Server is an X.500 and LDAP compliant directory for use with public key infrastructures. These instructions apply to the installation of general release 8A.2 for Windows NT Server.

The Entrust 5 is a software system that manages cryptographic keys for users.

Also, I would like to suggest to print out this document and check mark every step you have done. Especially all the command line stuff later in this document.

Prerequisites

Hardware (minimum required)

- Pentium 166 MHz
- Virtual Memory: 128 MB of swap space
- Installed Memory: 96MB (128 MB recommended - I've used 256 MB)

Software

- ❑ NT Server 4.0
- ❑ Service Pack 3 or higher for NT 4.0
- ❑ Internet Explorer 5.5
- ❑ ICL - i500 -8A
- ❑ I500 Patch Files, consists out of:
  - 8242ntbin.exe (5610kb)
  - 8242ntdsk.exe (190kb)
  - 8242ntsys32.exe (184kb)
  - ldap81162bin-nt.exe (687kb)
  - ldap81162lib-nt.exe (79kb)
- ❑ config8a2.i500
- ❑ config8a2.bat
- ❑ License String for ICL i500 Directory Server
  - Serial Number: _____
- ❑ License String for Entrust/Authority User Limit
  - Serial Number: _____
  - Enterprise User Limit _____
  - Enterprise Licensing Code _____

Preparation

Before you start with the actual i500 installation, make sure you have a brand new Windows NT 4.0 Server (without Microsoft Internet Information Server) on an **NTFS** partition installed. If you have FAT, you have to convert to NTFS !

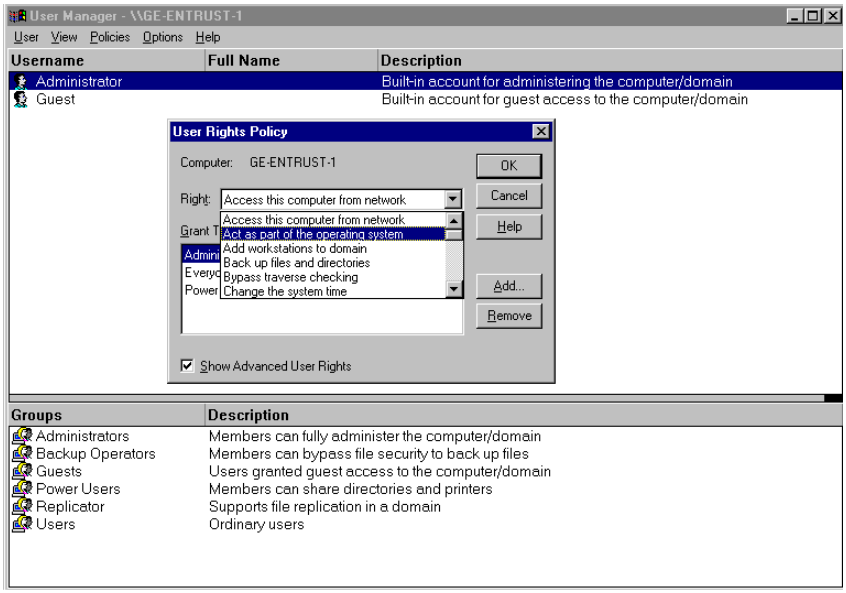
NT Server Configuration (mandatory)

1. Act as part of the operating system

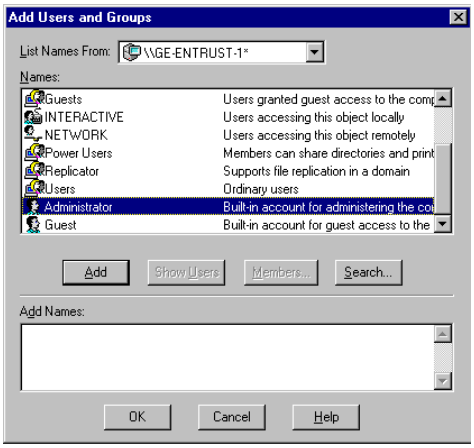
From the Start menu, select Programs, then Administrative Tools (Common), then User Manager for Domains.

From the policies menu, select User rights.

Select ☑ Show Advanced User Rights



Scroll down the “Rights” and find ***Act as part of the operating system***. Click on **Add**.



Click on ***Show Users*** -> ***Find Administrator*** and click on **Add**

2. Log on as service

Similar to Step 1, do the same procedure for another User Right. Find Log on as System and add the User: Administrator to it.

3. Have a permanent IP Address configured

When the PC is configured to obtain an IP Address out of DHCP, you have to change the IP Address to a permanent IP Address.

4. Edit Host File with the IP Address

The host file resides in WINNT\SYSTEM32\DRIVERS\ETC\hosts


```
# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

127.0.0.1               localhost
192.168.10.200          GE-ENTRUST-1            # this is the host name of your local workstation
```

5. Check availability of a frames based web browser, i.e Internet Explorer 5.x or equivalent

If you do not have a web browser installed, which supports frames, please install it, before you proceed with i500 Installation.

6. Administrator account should not have a password with a blank within

If your administrator password may have password, which also contains a blank like “san Francisco”, please change it to a non-blank password, to avoid problems with Informix at Entrust service.

7. NTFS partition is mandatory

Informix (part of Entrust) requires for security reason a NTFS partition. This could also be drive D:, but you have to remember, that Entrust needs to be installed on that drive, that is formatted with NTFS

8. Verify, that no i500 Directory Service is running

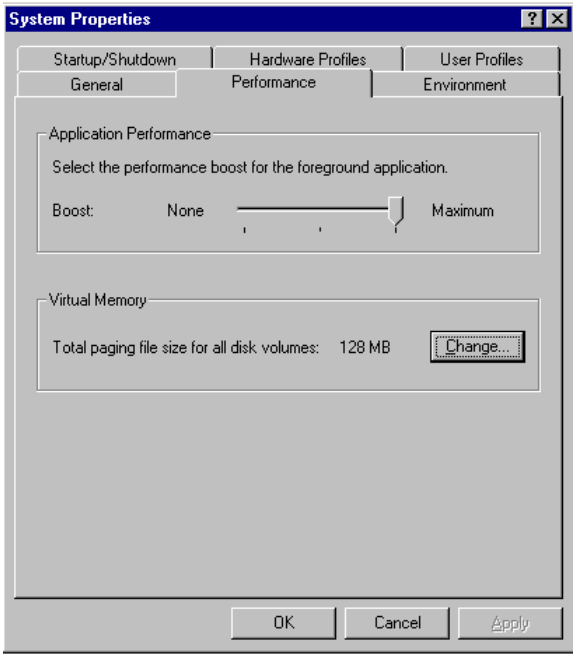
Open the Control Panel, search for Services and verify that no i500 Service is running. Usually, there should no such service be installed, as you are asked to do the installation on a brand new and unused NT Server.

9. Verify, that no SNMP Service is running

Open the Control Panel, search for Services and verify that no SNMP Service is running. If you see SNMP installed, but not running, this should be fine.

10. Check Virtual Memory, to have at least 128MB

Open the Control Panel, search for System, click on performance tab and there you can see, how much virtual memory you have available. With Change, you can modify the setting.

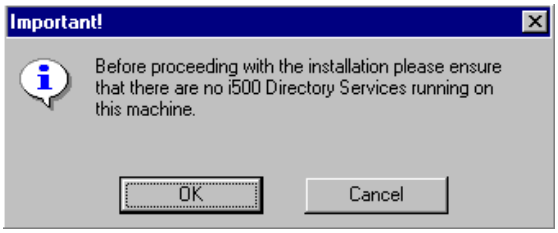


11. Once you run through all the Server configurations, including possible changes I highly recommend to do a reboot, before you proceed.

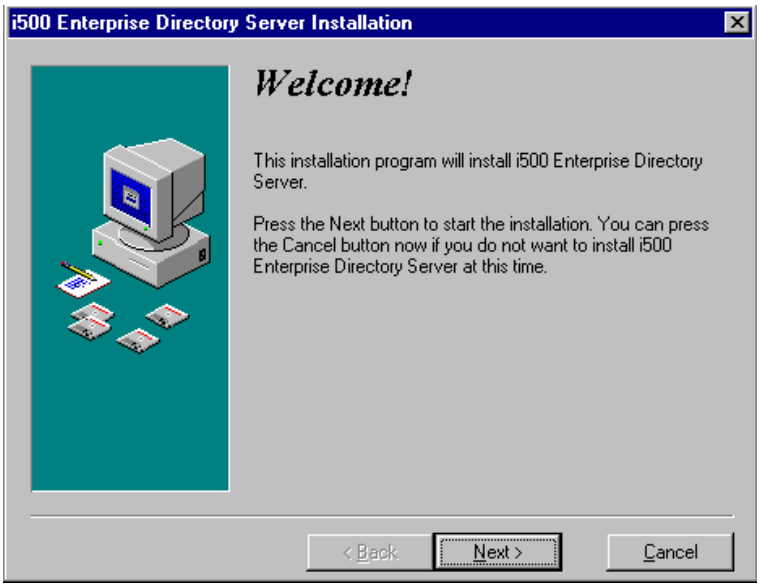
Running the Installation Program

Start the i500 setup Program (ICL-i500-8A\isetup.exe)

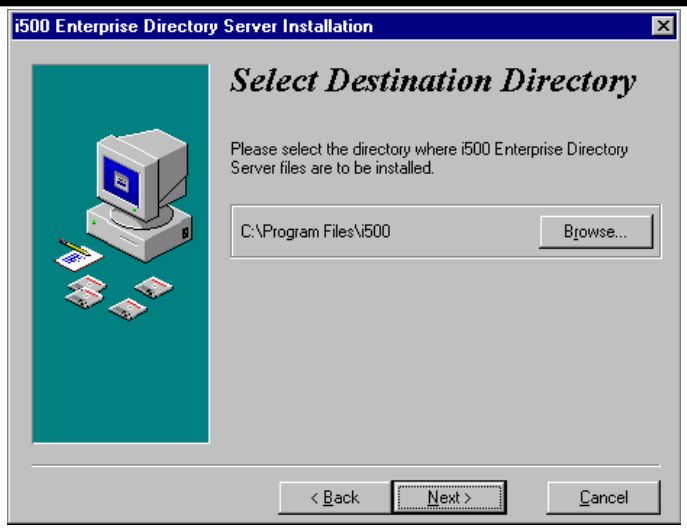
Click OK to confirm the information box



Click **NEXT** to accept the welcome screen.



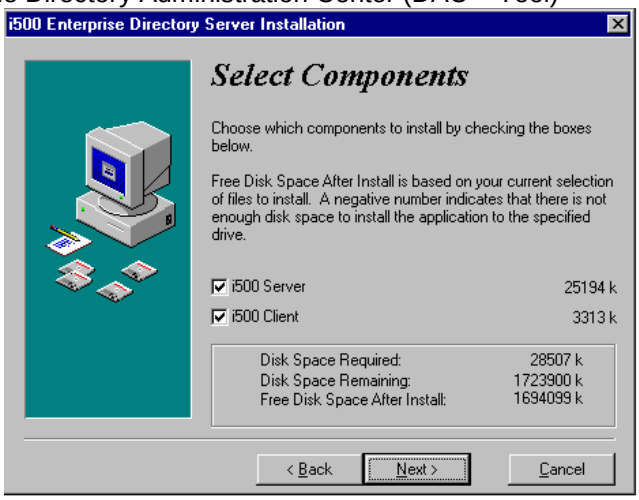
Click **NEXT** to accept the destination directory for the i500 files.



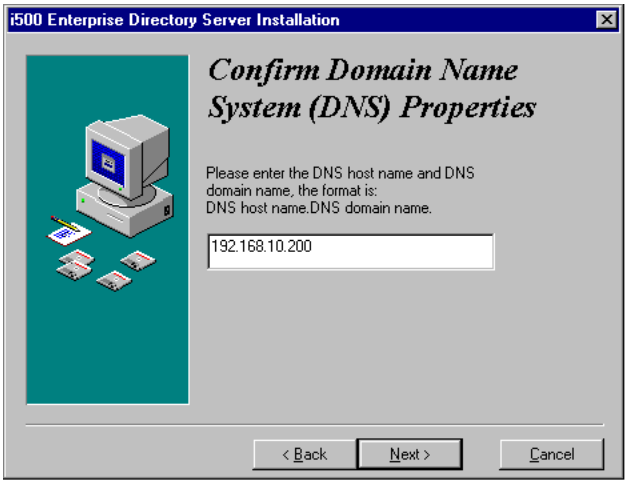
Click **NEXT** to accept the default choice of installing both components:

- ☑ Server
- ☑ Client

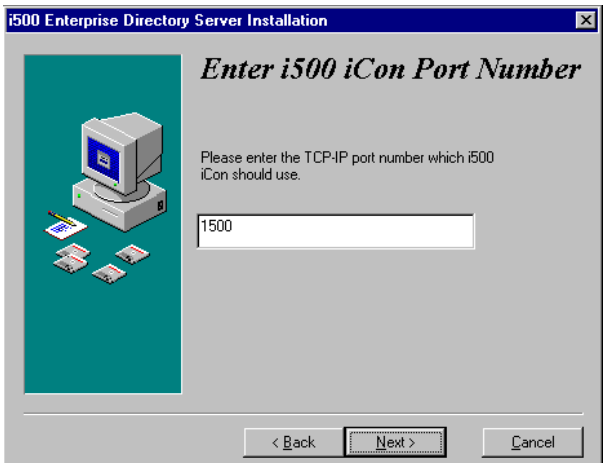
The Client component is the Directory Administration Center (DAC – Tool)



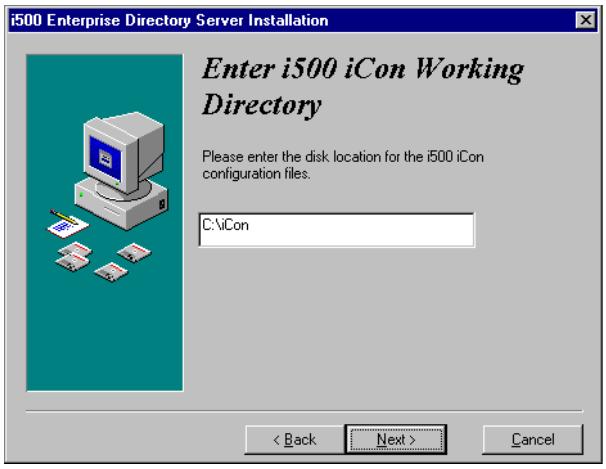
Replace the domain name with the IP Address of the host on which you are installing the i500 software and click **NEXT**



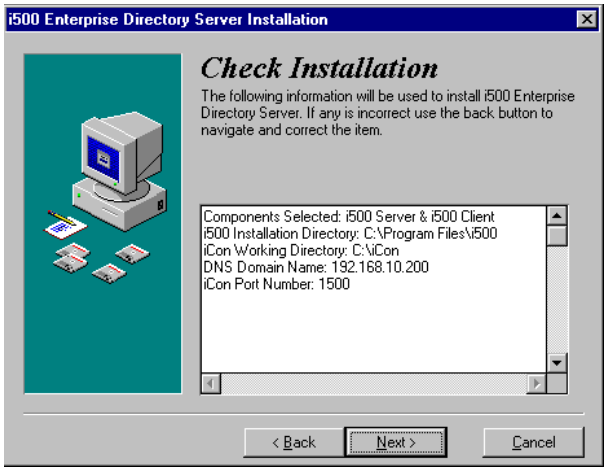
Click **NEXT** to accept the default port number (1500)



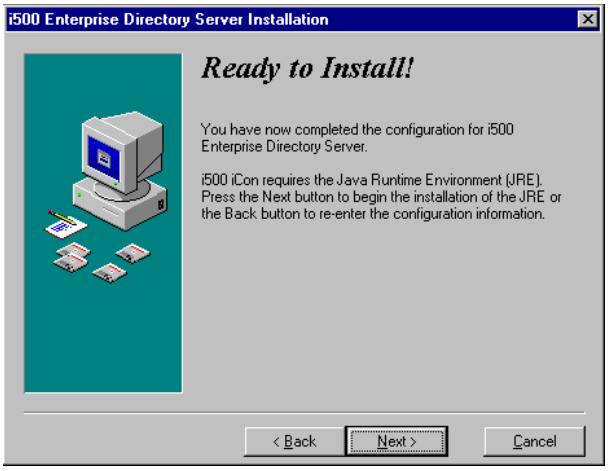
Click **NEXT** to accept the default i500 iCON working directory



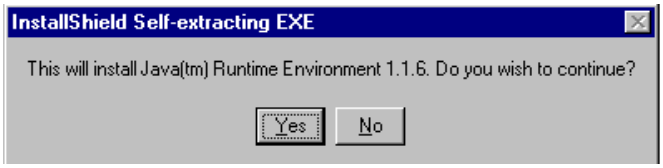
Click **NEXT** to accept the installation parameters selected so far



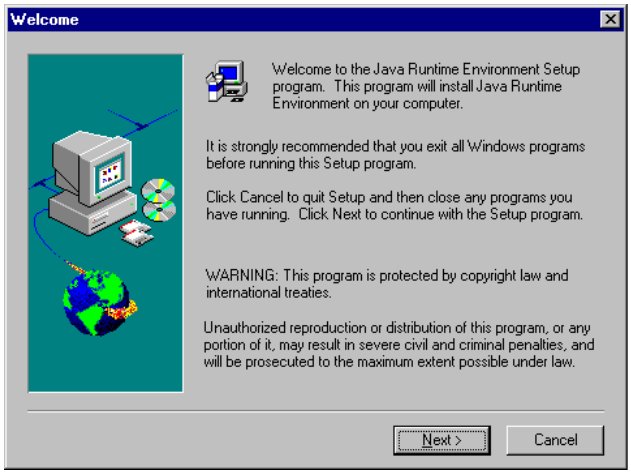
Click **NEXT** to accept the Ready to Install screen



Click **YES** to confirm installation of Java Runtime Environment
(A progress bar appears and then another install shield wizard loads)

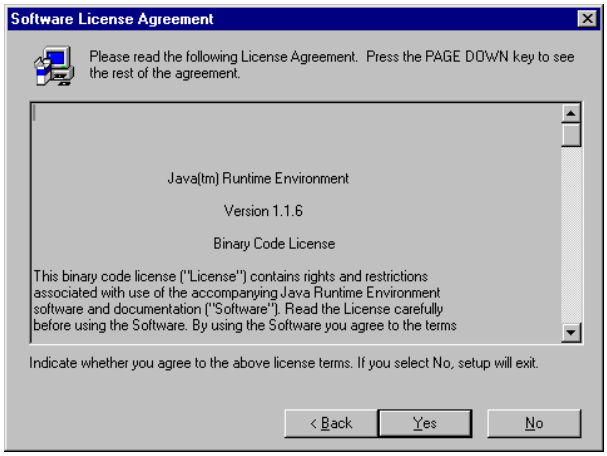


Click **NEXT** to accept the Java Runtime Environment Welcome Screen

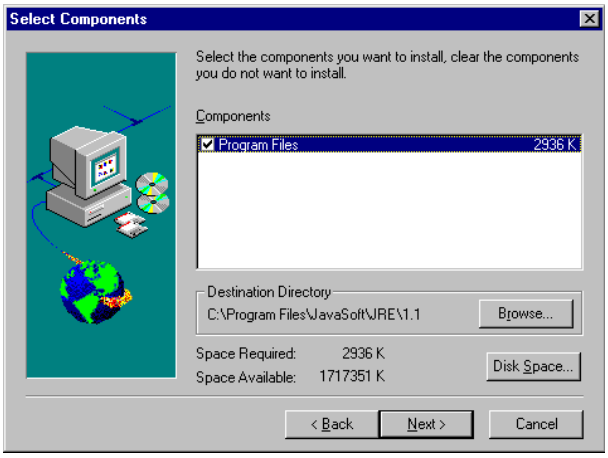


Click **YES** to accept the Software License Agreement

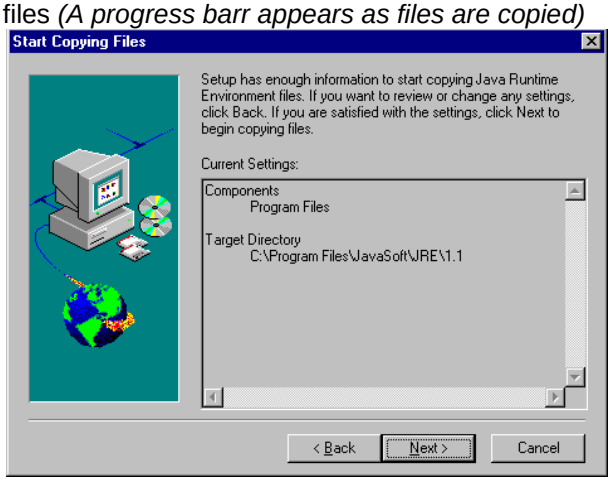
This technical document has been created and evaluated by myself with the purpose to help friends to get into new technology and installations. There is no financial interest, however, please respect the copyright.



Click **Next** to accept the default components



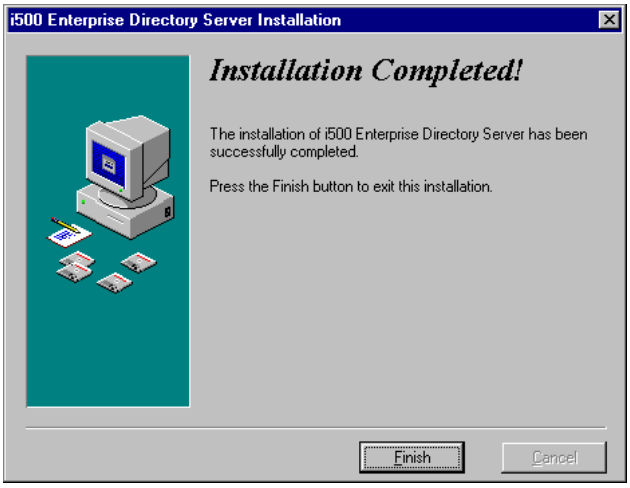
Click **NEXT** to start copying files *(A progress barr appears as files are copied)*



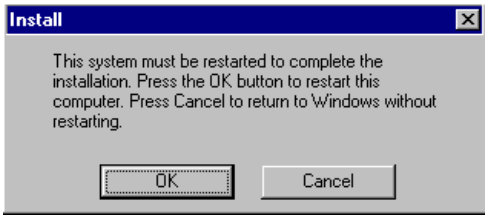
This technical document has been created and evaluated by myself with the purpose to help friends to get into new technology and installations. There is no financial interest, however, please respect the copyright.

Click **FINISH** to finalize the Java Runtime Environment installation (another progress bar appears)

Click **FINISH** to exit the installation program



Click **OK** to restart your system and complete this phase of the installation



After reboot, the Internet Connection Wizard will start, if you haven't been connected to the Internet before.

Select
◉ I want to set up my Internet connection manually, or I want to connect through a local area network (LAN)

Click **Next**

◉ I connect through a local area network (LAN)

Click **Next**

Do not use any of following Settings

☐ Automatic discovery of proxy server (recommended
☐ Use automatic configuration script
☐ Manual Proxy Server

Click **Next**

Do not setup your internet Mail Account this time. If you need to use it, configure Internet Mail, once you have finished i500 Directory Server Setup and Entrust 5 Setup.

O Yes
⊙ No

Click **Next**
Click **FINISH**
Once you see the i500 URL

http://192.168.10.200:1500 you have achieved the first main part. If you have problems to get this page, or anything else, do not continue further on, as the rest will fail !

Minimize Internet Explorer

Creating a DSA for Entrust 5.0

Before creating your DSA, you must create a directory for the DSA database.

Create a folder in the root of drive C to hold the Directory Service Agent

Open a command prompt box

```
C:\> mkdir i500Data\TimeStepDSA
```

Change to your c:\DSA directory. To create a new database to hold the Entrust Schema you have to execute following command line:

```
C:\> cd \i500Data\TimeStepDSA
C:\ i500Data\TimeStepDSA\odscreate -w permit -e "o=TimeStep,c=CA" -i
```

In response to the following prompts, type the responses indicated in bold and blue

```
Please enter the name of the DSA: cn=TimeStepDSA
Please enter the name of the DSA administrator: cn=diradmin
Please enter the administrator's password: diradmin
Please enter the t-selector for the DSA: 1002
Please enter the license key: 031b4d85cb92afe6c67042ba35880c81
```

(Note: the license key above is a demo key and will expire on November 1, 2001)

If you do have a permanent license key, of course you should use your own key.

When odscreate is done, a message appears indicating that the log file is du.000 – for example,

```
Initialising the DSA
Reading country codes from file iso3166
Admin>Reading country codes from file iso3166
Admin>Logfile was du.000
```

***Note**: Check the log file du.000 for errors before proceeding. If any errors are reported in the log file du.000, contact TimeStep Support for help **before continuing** with the configuration of your DSA for Entrust/PKI.*
You also can be sure to have errors, when seeing before the line "Logfile was du.000 messages like following example:

- There were 3 directory operation or scripting errors
- Failed to load the script

Configuring the LDAP schema files

1. Execute Batch File

Copy the file config8a2.bat into c:\i500DATA\TimeStepDSA and execute.

Note: Only run this batch file once !

Open a command prompt box and change to c:\i500DATA\TimeStepDSA

```
c:\>i500DATA\TimeStepDSA\config8a2
```

Note: When done, delete config8a2.bat out of this folder to avoid another unwanted execution.

There is a new folder with files been created by this batch file.
Navigate into \i500ldap

2. Configure the attributes.cfg file

2.1 Open the attributes.cfg file located in the i500ldap folder in c:\i500DATA\TimeStepDSA

2.2 Search for the ***attributeCertificate*** string

2.3 Comment out the definition of attributeCertificate defined with object indentifier '2.5.4.58' by placing '#' character at the beginning of each line. For example,

```
# (2.5.4.58 NAME 'attributeCertificate'
# (SYNTAX 1.3.6.1.4.4.1466.115.121.1.5)
```

3. Configure the oidtable.at file

3.1 Open the oidfile.at file located in c:\i500DATA\TimeStepDSA\i500ldap and search for the following:

```
userCertifcate:              attributeType.36  : Binary
cACertificate:               attributeType.37  : Binary
authorityRevocationList:     attributeType.38  :Binary
certificateRevocationList:   attributeType.39  :Binary
crossCertificatePair:        attributeTye.40   :Binary
deltaRevocationList:         attributeType.53  :Binary
```

3.2 Change the syntax of all entries from :**Binary** to :**unkown**

```
userCertifcate:              attributeType.36  : unknown
cACertificate:               attributeType.37  : unknown
authorityRevocationList:     attributeType.38  : unknown
certificateRevocationList:   attributeType.39  : unknown
crossCertificatePair:        attributeTye.40  : unknown
deltaRevocationList:         attributeType.53  : unknown
```

3.3 In the # Entrust 5.0 Schema section search for “entrustPolicyCertificate

```
entrustPolicyCertificate:secureNetworksAttributes.30: jpeg:file
entrustRoamFileEncInfo:secureNetworksAttributes.22: jpeg:file
entrustRoamingProfile:secureNetworksAttributes.23: jpeg:file
entrustRoamingPAB:secureNetworksAttributes.24: jpeg:file
entrustRoamingRecipList:secureNetworksAttributes.25: jpeg:file
entrustRoamingSLA:secureNetworksAttributes.26: jpeg:file
entrustRoamingPRV:secureNetworksAttributes.27: jpeg:file
entrustRoamingEOP:secureNetworksAttributes.28: jpeg:file
entrustRoamingCAPAB:roam.0: jpeg:file
```

3.2 Change the syntax of all entries from :**jpeg** to :**unkown**

```
entrustPolicyCertificate:secureNetworksAttributes.30: unknown:file
entrustRoamFileEncInfo:secureNetworksAttributes.22: unknown:file
entrustRoamingProfile:secureNetworksAttributes.23: unknown:file
entrustRoamingPAB:secureNetworksAttributes.24: unknown:file
entrustRoamingRecipList:secureNetworksAttributes.25: unknown:file
entrustRoamingSLA:secureNetworksAttributes.26: unknown:file
entrustRoamingPRV:secureNetworksAttributes.27: unknown:file
entrustRoamingEOP:secureNetworksAttributes.28: unknown:file
entrustRoamingCAPAB:roam.0: unknown:file
```

3.4 Search for the following lines and change the reading as marked in blue

```
cn,commonName:    attributeType.3   :CaseIgnoreString
commonName,cn:    attributeType.3   :CaseIgnoreString

mail,rfc822Mailbox:pilotAttributeType.3:CaseIgnoreIA5String
rfc822Mailbox,mail:pilotAttributeType.3:CaseIgnoreIA5String

sn,surname:       attributeType.4:  CaseIgnoreString
surname,sn:       attributeType.4:  CaseIgnoreString
```

3.5 Save and close the file

Upgrade i500 LDAP Server

Before you can use the Latin-1server, you have to upgrade to maintenance release 8.1.16.2.

1. Verify, that you have 8.1.16.2 version running by executing at the command prompt. If you don’t proceed with installing the patches outlined below.

```
c:\i500DATA\TimeStepDSA\odsldapv3 –v

odsldapv3 – ICL i500 Release 8.1.13.1
((Fri 22-Jan-99 9:59:4)
```

```
ldap@RDUBY:\users\ldap\work-ldap\v3wrkr\source
        i500 DSA build version is '8.2.1.1'
```

2. Use Control Panel Services to stop the i500iCon service

3. You will require the follwing self-extracting files

- 8242ntbin.exe
- 8242ntdsk.exe
- 8242ntsys32.exe
- ldap81162bin-nt.exe
- ldap81162lib-nt.exe

4. Create the following temporary directories

- C:\i500patches\bin
- C:\i500patches\sdk
- C:\i500patches\system32
- C:\i500patches\sdk\ldap\lib

5. Set view options in Windows Explorer to **Show all files**

6. Extract 8242ntbin.exe to c:\i500patches\bin
(114 files should have been extracted)

7. Extract 8242ntsdk.exe to c:\i500patches\sdk
(4 files should have been extracted)

This will create an mlog folder within the sdk folder and an examples, include and lib folder within the mlog folder

8. Extract 8242ntsys32.exe to c:\i500patches\system32
(5 files should have been extracted)

9. Extract ldap81162bin-nt.exe to c:\i500patches\bin
(6 files should have been extracted)

10. Extract ldap81162lib-nt.exe to c:\i500patches\sdk\ldap\lib
(2 files should have been extracted)

NOTE: You may have to stop icon Service in the Service panel, when having sharing violation during copy process.

11. Copy the contents of the c:\i500patches\bin to c:\program files\i500\bin
(120 files should have been copied)

12. Copy the contents of c:\i500patches\sdk\mlog\examples to c:\program files\i500\sdk\mlog\examples
(1 file should have been copied)

13. Copy the contents of c:\i500patches\sdk\mlog\include to c:\program files\i500\sdk\mlog\include
(1 file should have been copied)

14 Copy the contents of c:\i500patches\sdk\mlog\lib to c:\program files\i500\sdk\mlog\lib
(2 files should have been copied)

15. Copy the contents of c:\i500patches\system32 to c:\winnt\system32
(5 files should have been copied)

16. Reboot the PC to be sure everything has been initialized during startup

17. Now verify, that you are using version 8.1.16.2 by executing at the command prompt:

```
      c:\i500DATA\TimeStepDSA\odsldapv3 –v

odsldapv3 – ICL i500 Release 8.1.16.2
(Thu 8-Jul-99 16:3:8)
ldap@RDUBY:\users\ldap\work-ldap\v3wrkr\source
              i500 DSA build version is ‘8.2.4.2’
```

Start the Directory

Execute **c:\i500DATA\TimeStepDSA\odsmgmt**

From the menu presented, execute **s** to start the DSA
>**s**

```
odssched 241 started (the number 241 could be different)

-----------------------
ICL i500 DSA Management
-----------------------

Enter the letter for the management operation required:

      (x) Stop the directory
      (a) Add a process
      (r) Remove a process
      (v) View the current state of the processes
      (d) Take a diagnostic dump
      (w) Display directories running
      (l) Display odssched.log
      (m) Monitor odssched.log
      (e) Report any errors or warnings that have occurred
      (c) Clears any errors or warnings that have occurred
      (q) Quit

>
```

Press **v** to view the processes and confirm that all States are listed as OK and that the Fails column indicate no failure.

```
pid     inst      action              fails  stats    name         options
241     0         restart this        0      ok       odscomms           -P0
139     M         default             0      ok       odsmdsa      -d"C:\i500DATA\
TimeStepDSA"
248     0         restart this        0      ok       odssdsa
247     1         restart this        0      ok       odssdsa
240     0         restart this        0      ok       mtldapd
246     0         restart this        0      ok       odsldap
244     0         restart this        0      ok       odsldapv3
Press Return:
```

Configuring the DSA schema

The config8a2.i500 script adds the Entrust 5.0 schema to the DSA. Only run this script one (if it succeeds). Follow these instruction to run the script.

Copy the file into c:\i500DATA\TimeStepDSA

Edit the file and replace two variable in the Bind statement at the beginning of the file.
Using a text editor, replace the following variables to look like that (based on this OmniTip)

```
OLD Line:       bind -n N(Rcn("ADMIN")) -p "PASSWORD"
NEW Line:       bind -n N(Rcn("diradmin")) -p "diradmin"
```

Save the changes and close the file

Run the script in odsadmin as follows

```
c:\>i500DATA\TimeStepDSA\odsadmin –fconfig8a2.i500
```

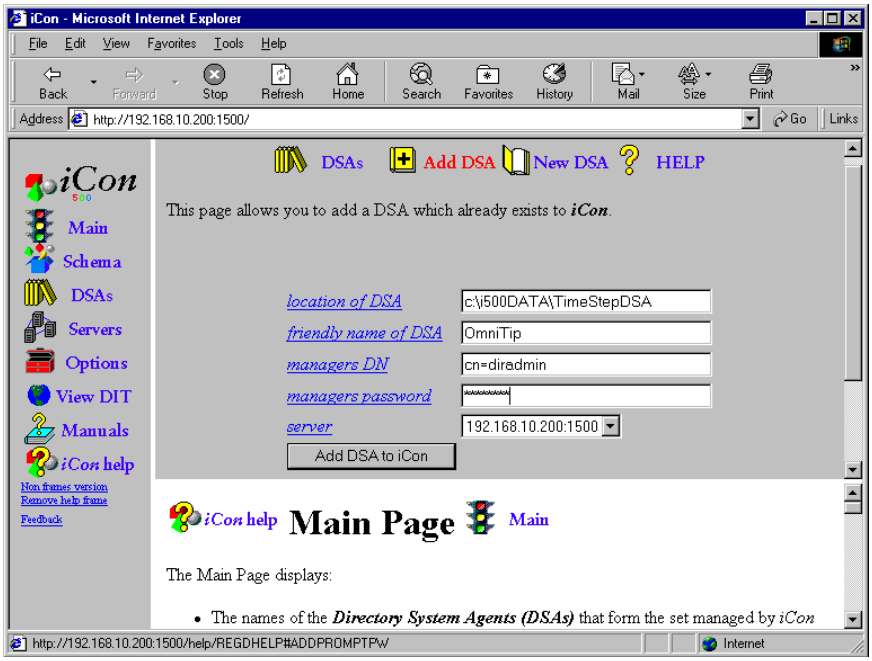
A new log file as been created named again du.000. Verify if you find any errors. If there is no error, you can proceed to the next main step. However, if you have found any error, please consult TimeStep support, before you continue further.

Configuring i500 Directory Server to Start automatically using icon

In order the have the i500 Directory start automatically when the server starts, it is necessary to have the icon service running. This requires a web browser that can handle frames.

Start the iCon clicking through Start -> Programs -> i500 -> icon

Click the **Add DSA** hyperlink in the top row

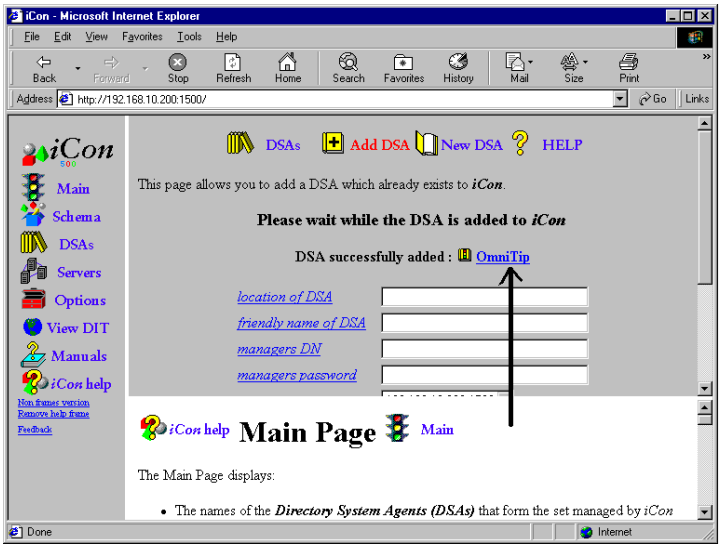


(please see next page)
Type the required information

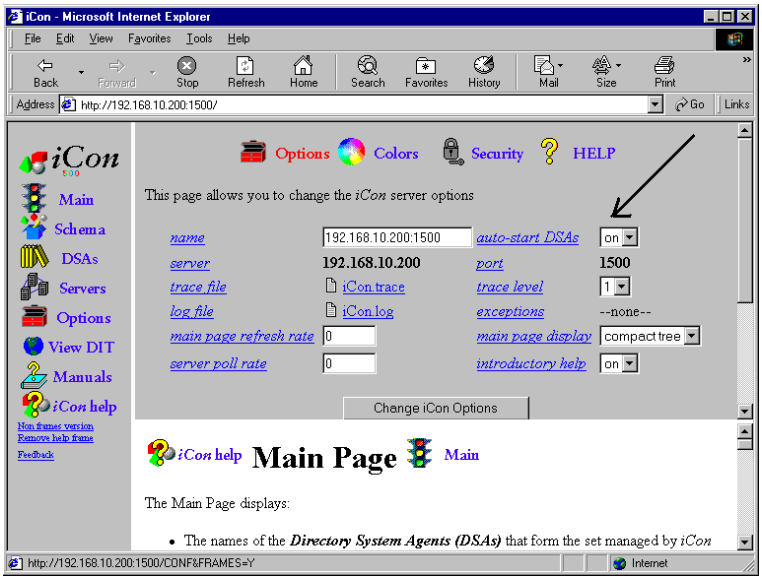
- Location of DSA -> **c:\i500DATA\TimeStepDSA**
- Friendly name of DSA -> **OmniTip**
- Managers DN -> **cn=diradmin**
- Manager's password -> **diradmin**

Click **Add DSA to icon**
Click **YES** if the Security Alert box appears. This procedure will take some time (depending on the PC).

Note that the DSA has been "successfully added" in iCon



Click the Options hyperlink on the left



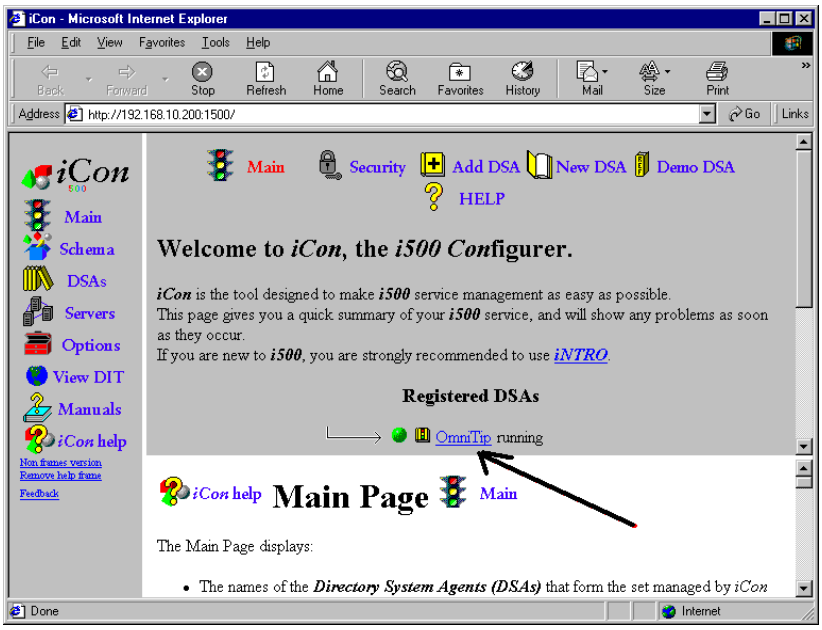
Note the **auto-start DSAs** in the right column of the main screen

By default, this setting is on. All registered DSAs start when the icon service start. By default, the icon Service is set to start automatically.

Close icon and perform final step for this part of installation.

Restart the PC, open the icon and verify, that newly registered DSA "OmniTip" is running. Once you have succeeded to this point you have achieved the second main step.

Start iCon



Installing Entrust 5

1. Verify, that Administrator rights a set properly

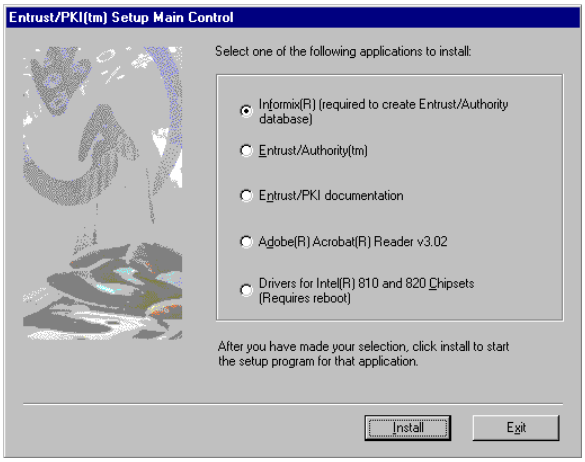
Log on as the Administrator to the Windows NT server that will host Informix, Entrust Manager and the Entrust/Mager database.

Remember step 1 and step 2 in the preparation section " ***NT Server Configuration***"

- Log on as system
- Act as part of the operating system

Run the installation program Setup.exe

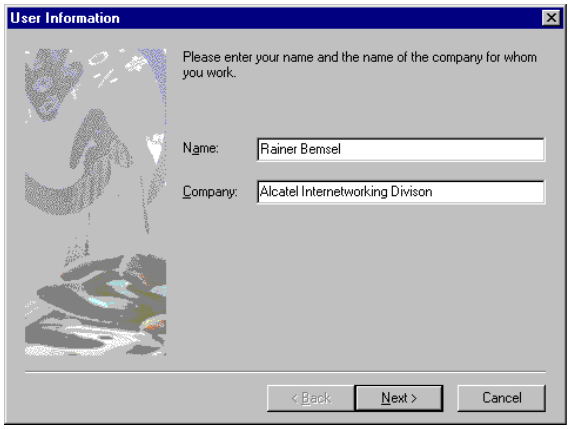
Ensure that Informix is selected and click **SETUP**



Once your PC do not have a powerful processor, you will get a question box.

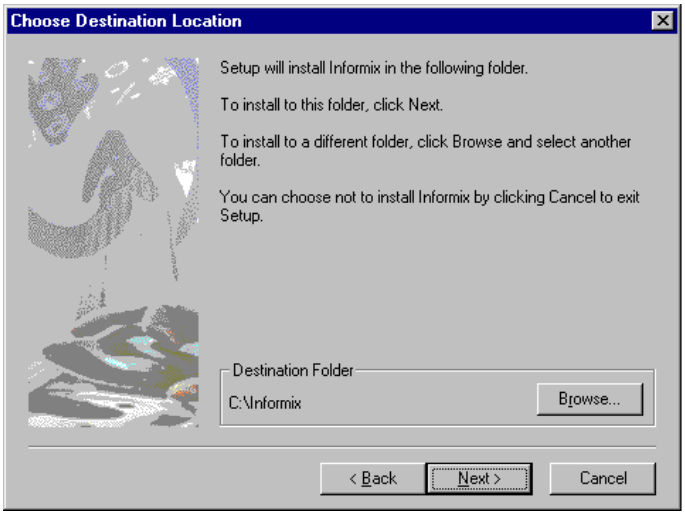
This does not say, that you cannot install Entrust, however, you may experience low performance.

Type in the User Information and click **NEXT**

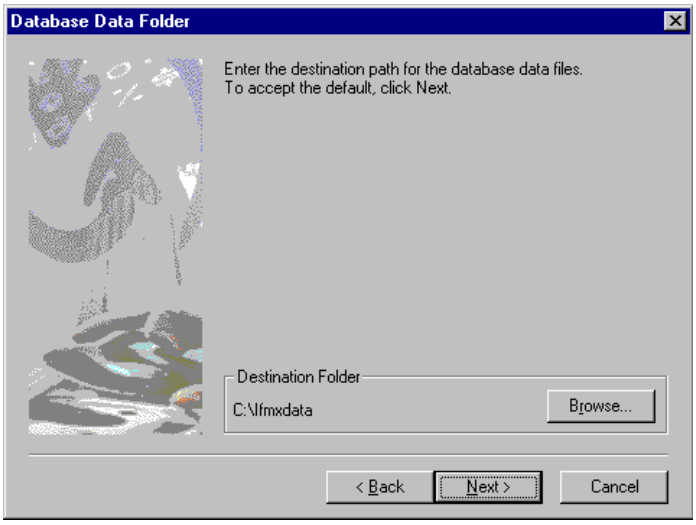


Click **NEXT** to accept the default entries

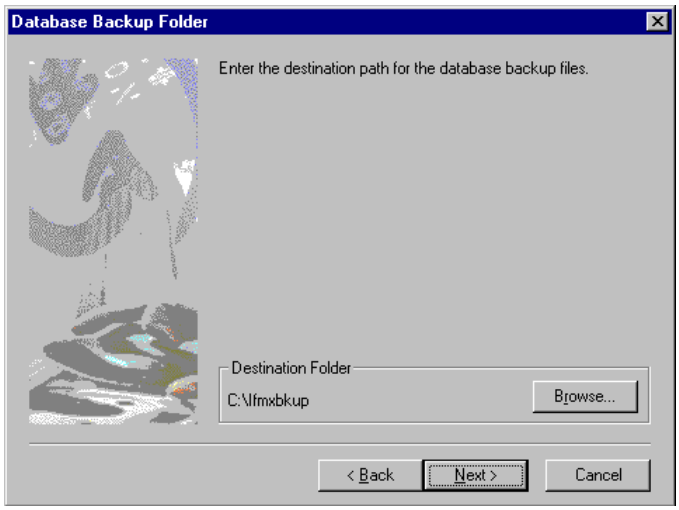
Click **NEXT** to accept the default location for ***INFORMIX***



Click **NEXT** to accept the default location forDatabase Folder -> ***Ifmxdata***



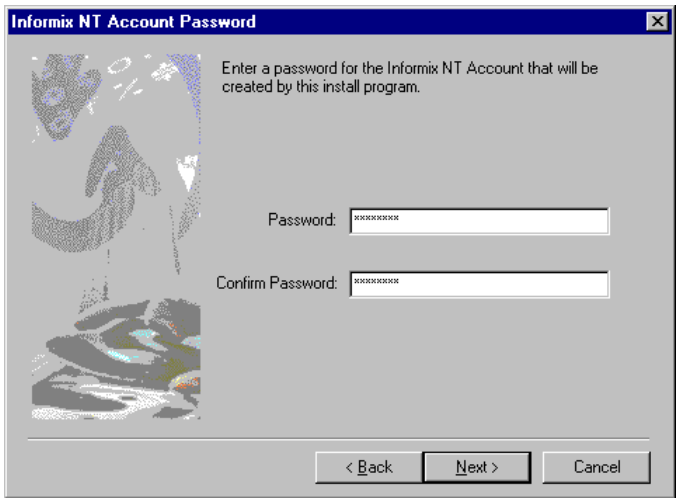
Click **NEXT** to accept the default location for ***lfmxbkup***



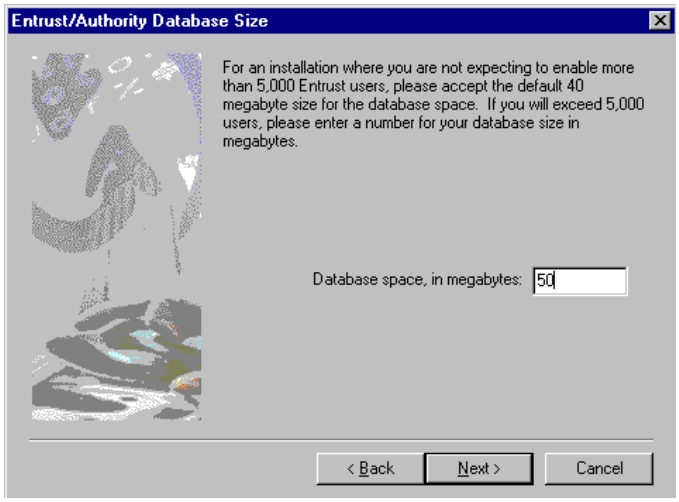
(A warning window pops up to ask if you want to have the backup folder on a different partition – if you have more than one partition on your harddisk)

Click NO to decline the opportunity to change selections

Type and confirm ***informix*** as the password and then click **NEXT**

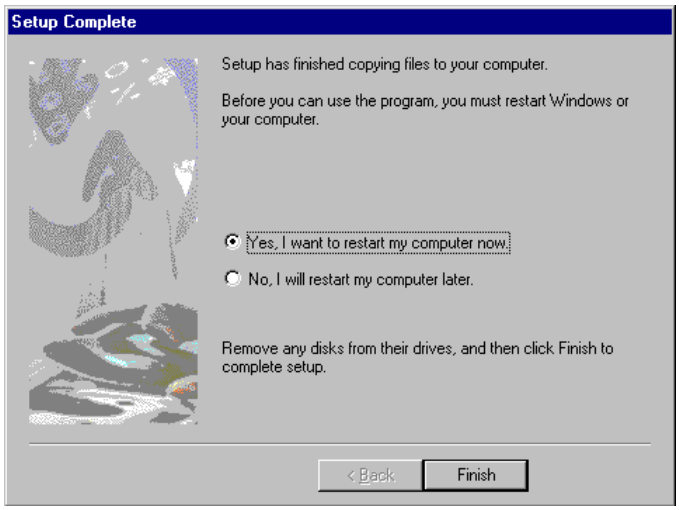


Click NEXT to accept the default database space (50MB)



An information box appears informing you that Informix Online Workgroup Server and ODBC clients components are being installed. This takes around 20 minutes or less (depending on the PC)

Ensure that the default option to restart your computer is selected and click FINISH



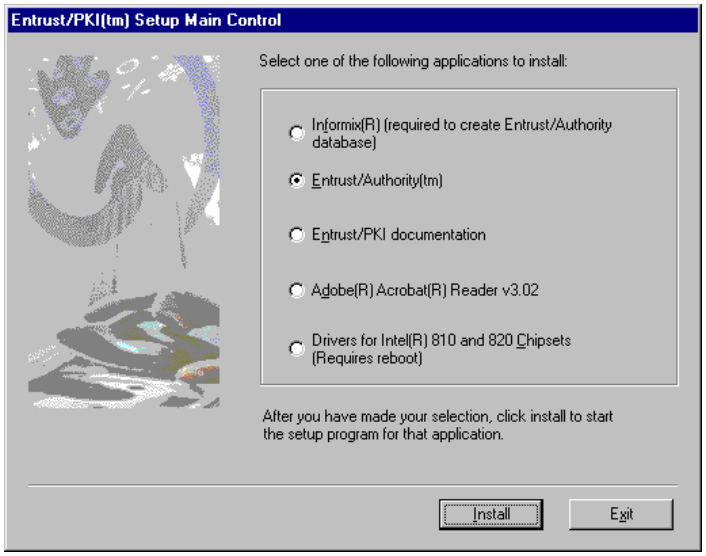
Allow your computer to reboot and then log back into NT

The Informix installation continues with a series of command prompt windows. No user input is required

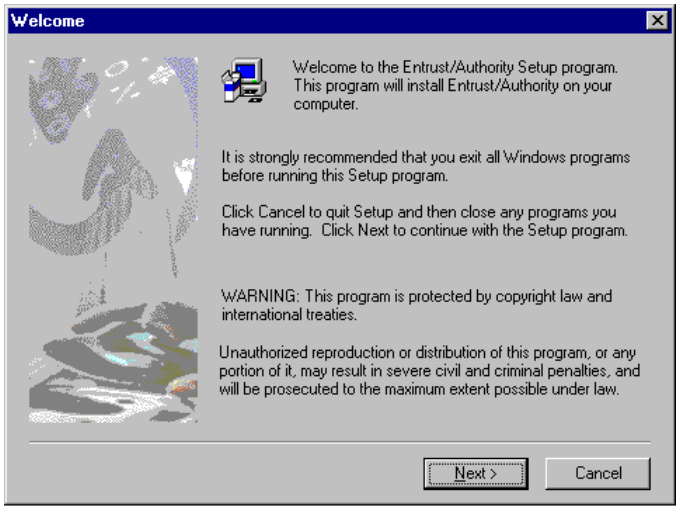
Installing Entrust/Authority

Restart the Entrust installation program (same setup.exe as before)

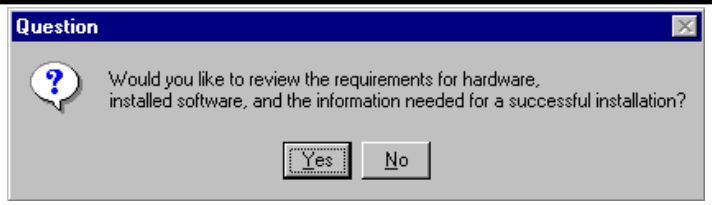
Ensure that Entrust/Authority is selected and click **SETUP**



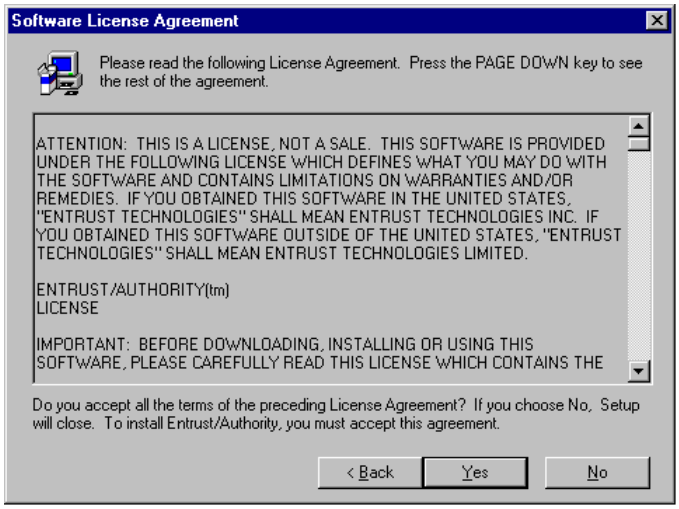
Click **NEXT** at the Welcome Window



(A Question box will ask you, if you want to review the requirements for hardware, installed software, and the information needed for a successful installation. It's up to you)

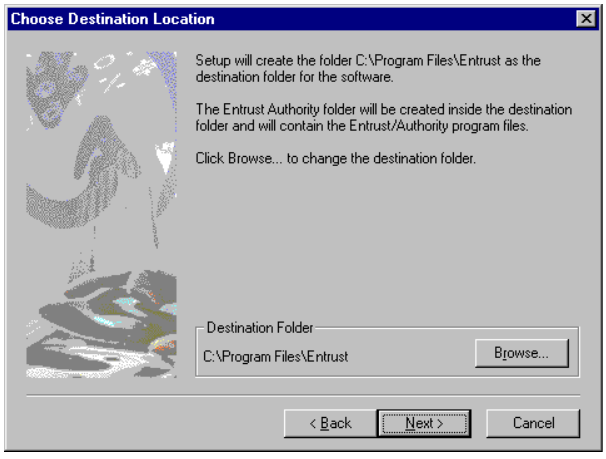


Accept the Software License Agreement by clicking on **YES**



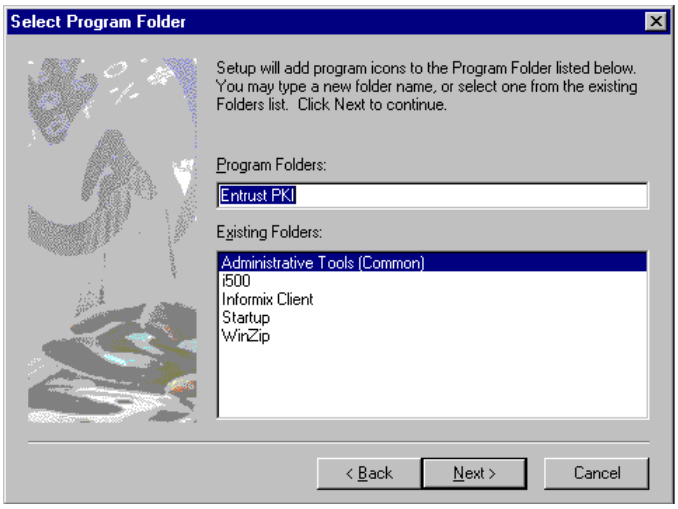
Click **NEXT** to accept the default Destination Folder.If not already set to your NTFS partition, change the Destination Drive to the proper partition

Do not change to c:, if C drive is formatted as FAT or FAT32)

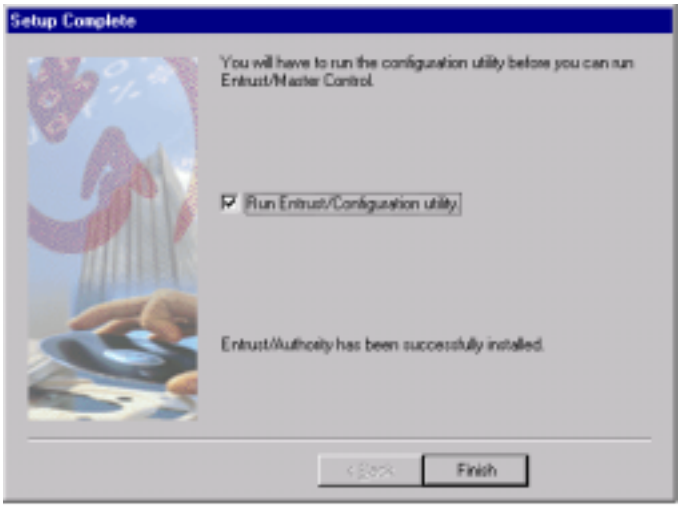


This technical document has been created and evaluated by myself with the purpose to help friends to get into new technology and installations. There is no financial interest, however, please respect the copyright.

Click **NEXT** to accept the Program Folder (Entrust PKI)
(A progress bar appears)



Once this part is finished, and the Setup Complete Window appears, make sure the Entrust Configuration Utility is marked. You may want to wish to do a reboot here, but this is only necessary, when having a slow performance PC



When you have decided to reboot, log on as Administrator after reboot and start Entrust Configuration Utility

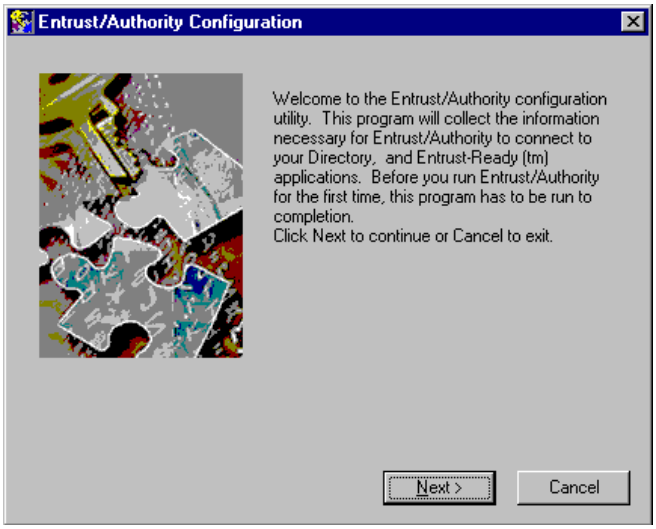
Open Entrust Configuration Utility

START - Programs – Entrust PKI – Entrust Configuration Utility

When Setup is complete make sure that

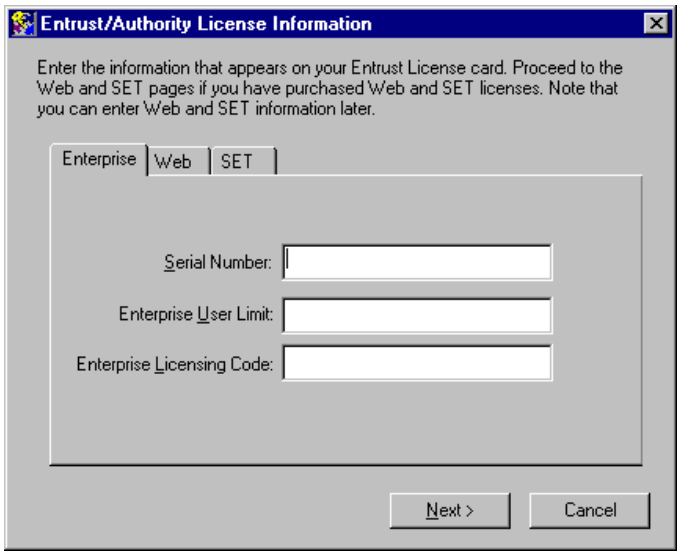
☑ Run Entrust/Configuration utility

Is selected and click on **FINISH**



Click on **NEXT**

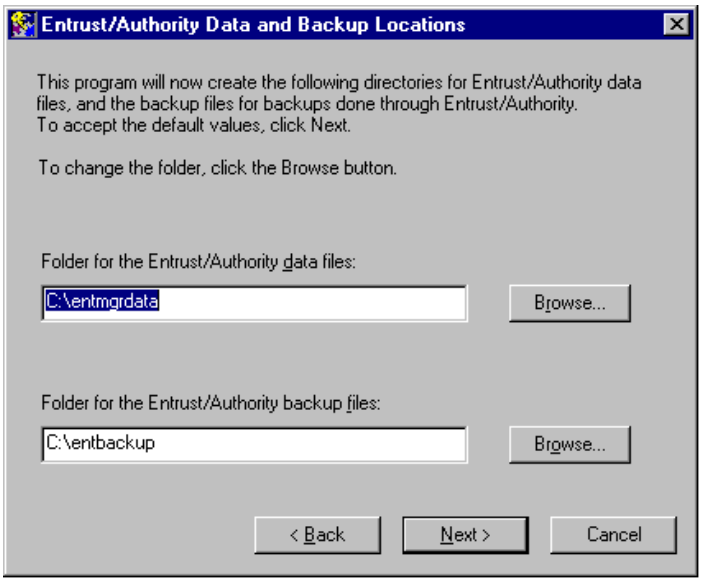
The license Information Window appears and here you need to set the license information



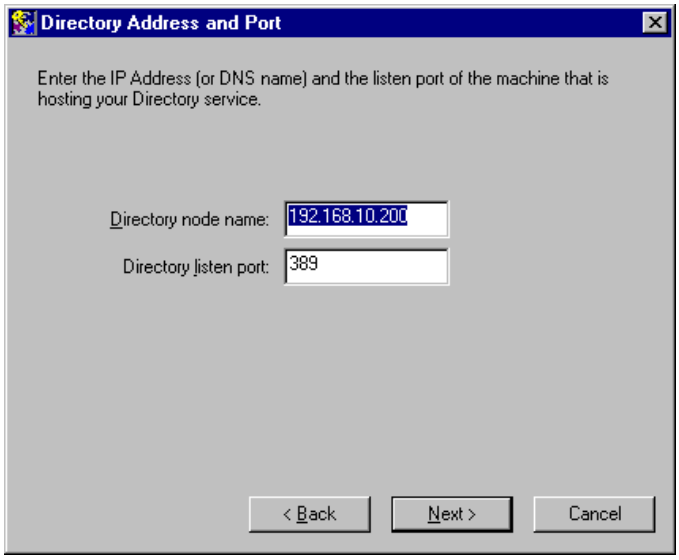
- Serial Number: _____
- Enterprise User Limit _____
- Enterprise Licensing Code: _____

Note that you can enter Web and SET license information later, if you have purchased them as well.

Click **NEXT** by accepting default locations for ***Entrust/Authority Data and Backup Locations***



Click **NEXT** when Directory Node Name (IP: 192.168.10.200) and Directory Listen Port (389) is set



Validate or type the proper IP Address and click OK

Hint: To verify the IP Address, open a command prompt box and type c:\ipconfig

```
C:\>ipconfig
Windows NT IP Configuration
```

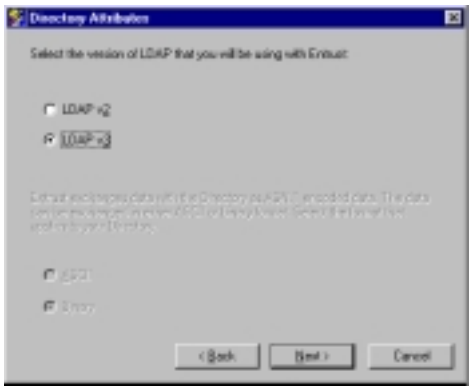
```
Ethernet adapter xyz:
      IP Address . . . . . . . . . . . 192.168.10.200
      Subnet Mask  . . . . . . . . . . 255.255.255.0
      Default Gateway. . . . . . . . . 192.168.10.1

C:\>
```

Click **NEXT** to accept LDAPv3 and ASN.1 Encoding with ASCII

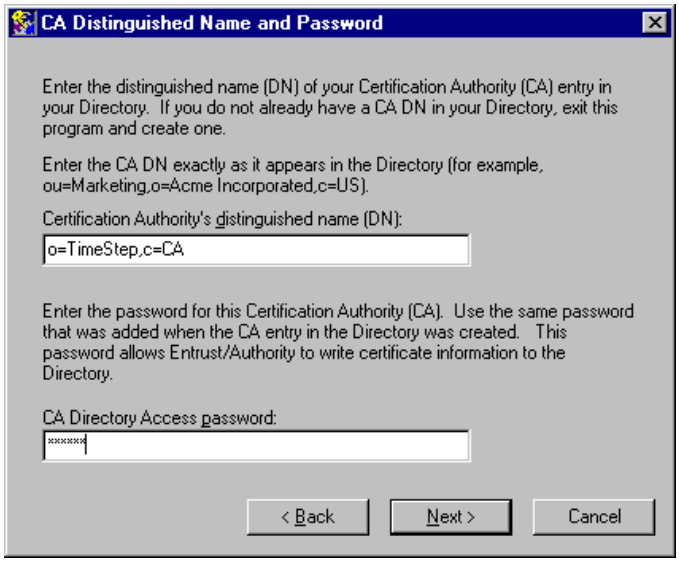
- O LDAP v2
- ⊙ LDAP v3

- O ASCII format
- ⊙ binary format



Fill in the value for ***Certification Authority's distinguished name*** (DN)

Fill in the value for ***CA Directory Access password***



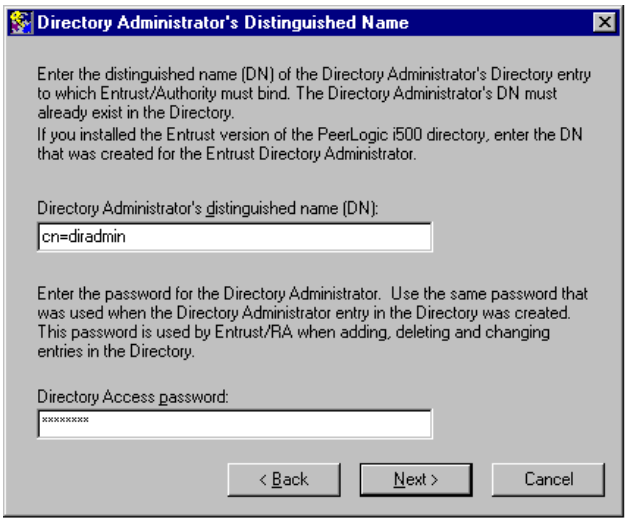
- Certification Authority's distinguished name -> **o=TimeStep,c=CA**

- CA Directory Access password -> **permit**

Click **NEXT**

Fill in the value for ***Directory Administrator's distinguished name*** (DN)

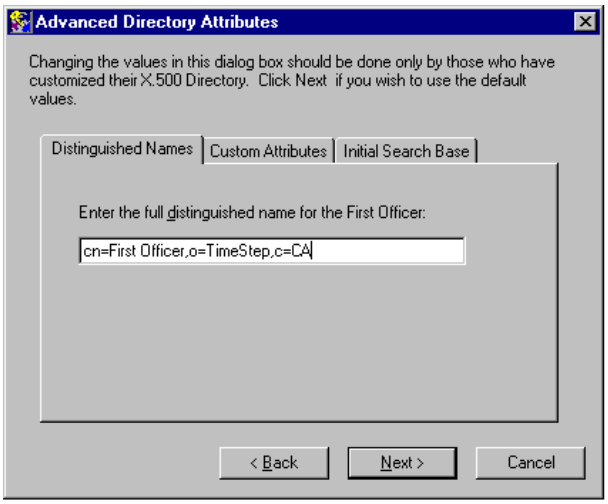
Fill in the value for ***Directory Access password***



- Certification Authority's distinguished name -> **cn=diradmin**
- CA Directory Access password -> **diradmin**

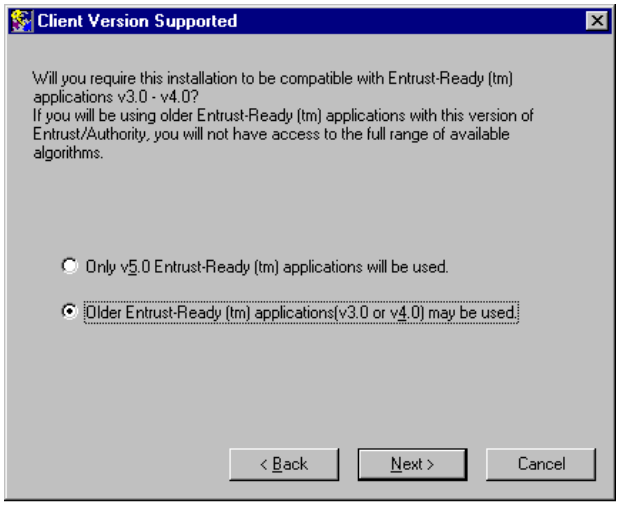
Click **NEXT**

Accept the default value in ***Advanced Directory Attributes*** for the First Officer



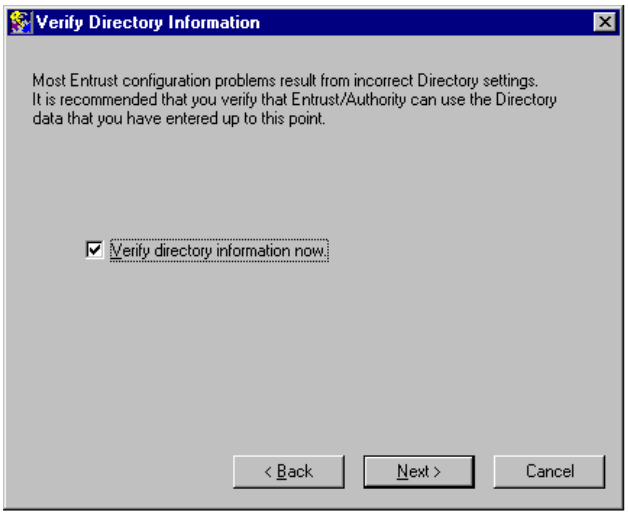
- Distinguished Name :**cn=First Officer,o=TimeStep,c=CA**
- Custom Attributes :**mail**
- Initial Search Base :**o=TimeStep,c=CA**

Verify setting on Client Version Supported



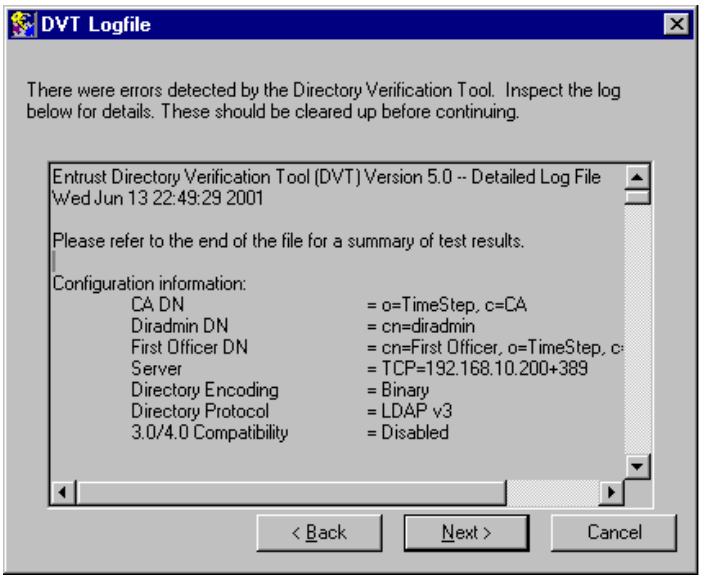
○ Only v5.0 Entrust-Ready ™ applications will be used
⊙ Older Entrust-Ready ™ applications (v3.0 or v4.0) may be used

Click on **NEXT**
☑ Verify Directory Information



In the case of found errors:

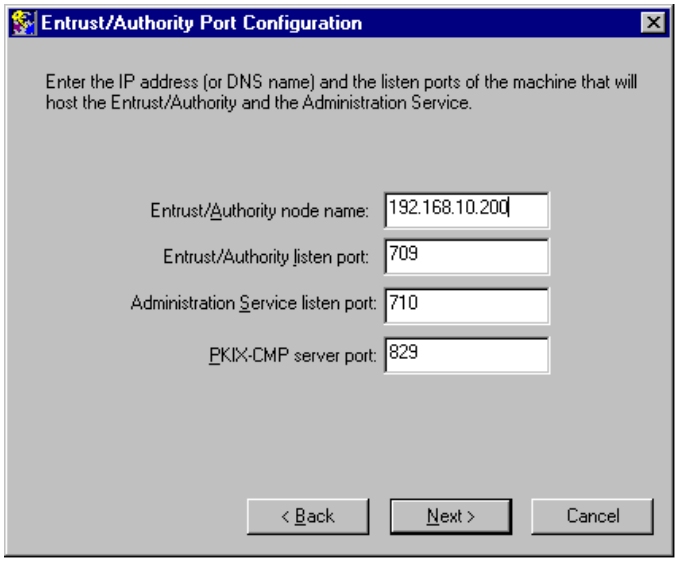
There were errors detected by the Directory Verification Tool. Inspect the log below for details. These should be cleared up before continuing.



Here's an extract out the DVT Logfile on the error, which was found.

```
Searching for user entry with an e-mail address as part of RDN.
Received the following LDAP message:
Invalid DN syntax <ILW3_SHf_ldap2HS>
ERROR: Searching for this entry as CA failed.
Possible reasons for failure: The search DN is invalid, or CA does not have permission
to search the Directory.
Searching for user entry with a serial number as part of RDN.
Entry not found in the Directory.
```

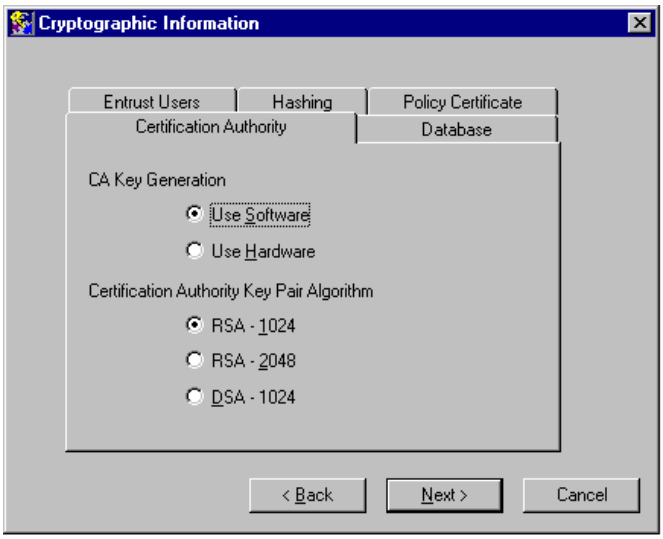
Change Entrust/Authority node name with the proper IP Address and leave the rest with their default values



- Entrust/Authority node name -> **192.168.10.200**
- Entrust/Authority listen port -> **709**
- Administration Service listen port -> **710**
- PKIX-CMP server port -> **829**

Click **NEXT**

Accept or change values on ***Cryptographic Information***



Certificate Authority - TAB

CA Key Generation
- ⊙ Use Software
- O Use Hardware

Certification Authority Key Pair Algorithm
- ⊙ RSA – 1024
- O RSA – 2048
- O DSA – 1024

Database – TAB

Database Encryption Algorithm
- CAST-128
- Triple DES

Policy Certificate Lifetime – TAB

Number of days: **30**

Click **NEXT**

Hashing – TAB

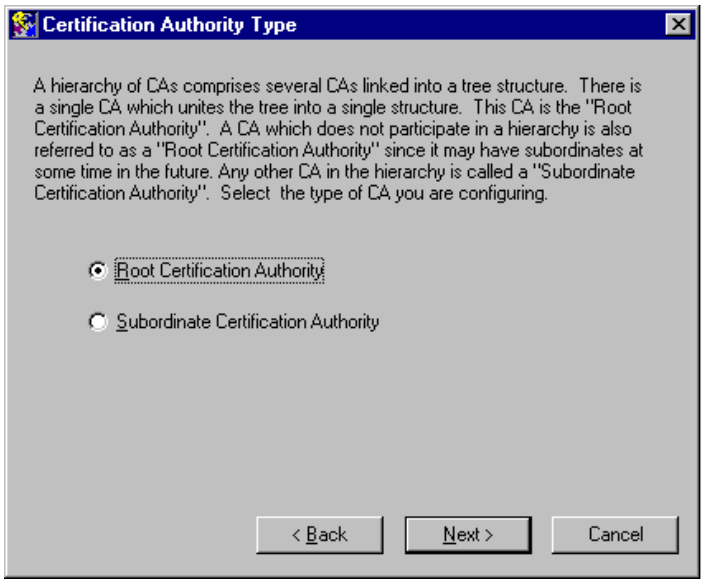
Signing Certificate Hashing algorithm
- ⊙ SHA-1
- O MD5

Entrust Users – TAB

Signature Algorithm
- ⊙ RSA-1024
- O DSA-1024

Encryption Algorithm
- ⊙ RSA-1024
- O RSA-2048

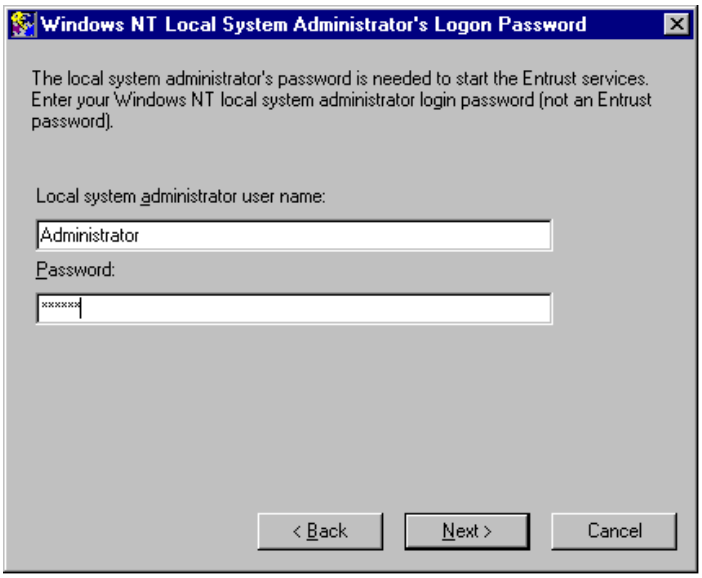
Accept Certification Authority Type



- ⊙ Root Certification Authority
- O Subordinate Certification Authority

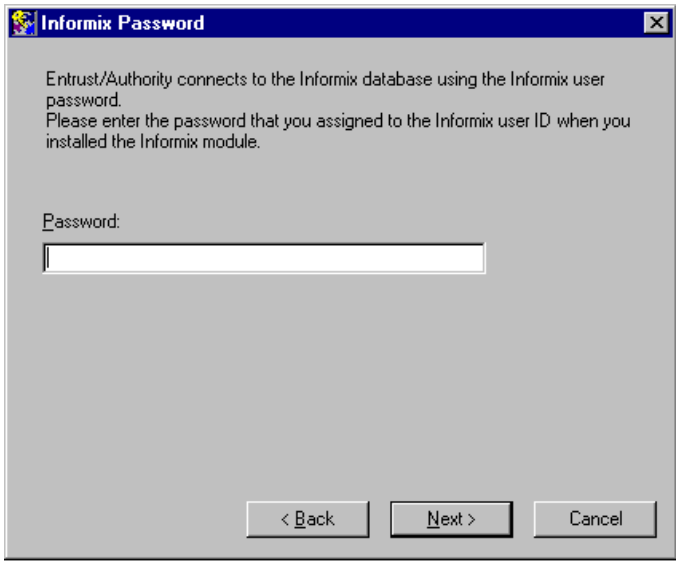
and click **NEXT**

Type and confirm switch as the Administrator's Logon Password
*(Note: **switch** is the password I've used for my NT Administrator. If you've used a different password, than use yours)*



Click **NEXT**

Type the Informix password which is ***informix***

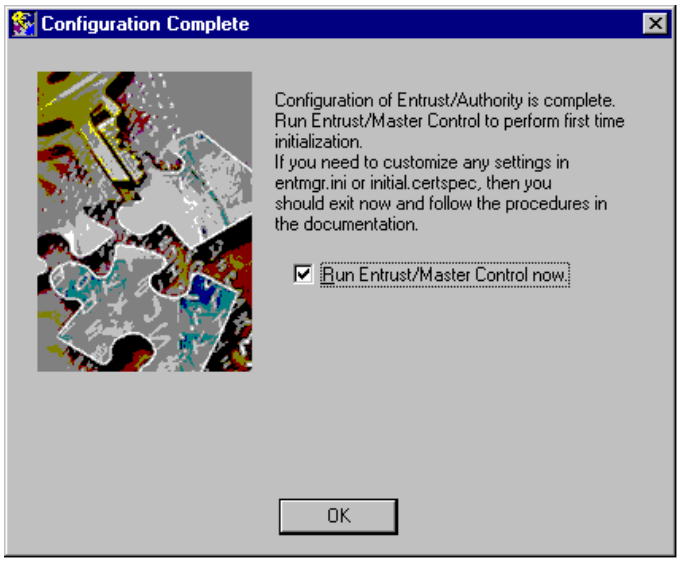


And click **NEXT**

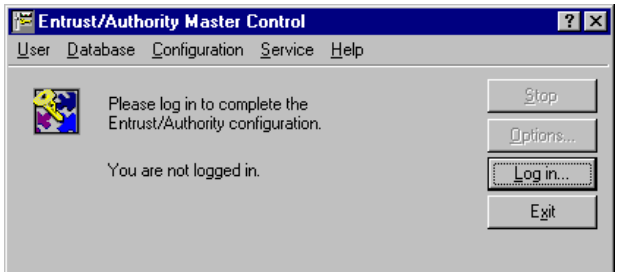
A couple of SQL statement occurs and run ……

Have Run Entrust/Master Control checked and click on OK

☑ Run Entrust/Master Control now



Log into the Entrust/Authority Master Control. When clickin on Log in… the first time, it will take some seconds for the initialization



Set the initial Passwords

Entrust Password Requirements:

- Minimum 8 characters
- At least on upper case letter
- At least one digit
- At least one lower case letter
- Must not be part of the home directory path
- Must not be a person's name (Entrust maintains a list)

- Must not be a dictionary word (Entrust maintains a dictionary
- Must not contain many occurrences of the same letter
- Must not be the same as your Entrust profile username
- Must not contain a long substring of your Entrust profile username

Entrust shows you when you've typed something wrong in a Verify box by displaying x's instead of asterisks Type and confirm the passwords in the table below. Note that an error in the verify box turns the entry from asterisks to x's

Click **OK** and wait for the following screen

(Please see matrix on next page)

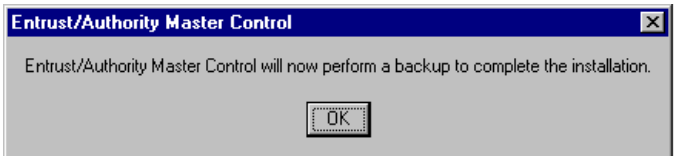
Master1	TimeStepM1
Master2	TimeStepM2
Master3	TimeStepM3
First Officer	TimeStepF1

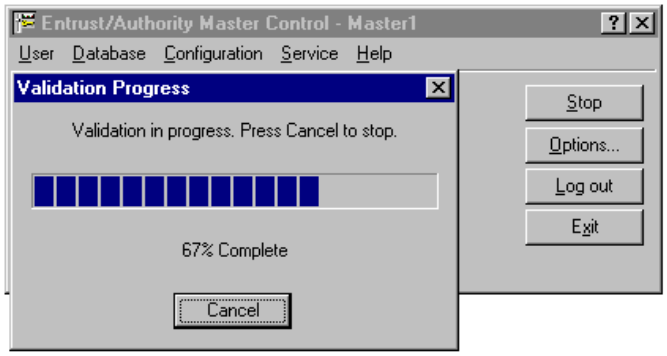
When done, click **NEXT**

Ensure that the box on the screen tells you…

- The Entrust infrastruture has been initialized successfully
- Three Master Users have been defined: “Master1”, “Master2” and “Master3”
- The Administration Service profile has been created
- An Entrust Security Office identity “cn=First Officer,o=TimeStep,c=CA” has been created in “C:/Program Files/Entrust/entmgrdata/manager/epf/First Officer.epf”.
- You are now logged in as Master User ‘Master1’.

An automatic Backup will be performed to complete the installation. Click **OK**





A command prompt box appears as backup is running

Finally, you should get a “Backup Completed Successfully”

This was the last main step for the installation. When you see this window you are done!

Conclusion:

If you are new to i500 and / or Entrust, take quite some time to perform this installation. Every small, single failure you make will force you to re-install from scratch. (just the experience I made)

☺

APPENDIX A:

Pre-Installation Checklist

License Summary

Platform	License Key	Notes
I500 v8a.2		
Entrust User Limit		

Password Summary

Platform	Account	Password
Windows NT	Administrator	Switch
Directory Administrator	diradmin	diradmin
Directory Administrator's Distinguished Name	cn=diradmin	diradmin
Entrust NT Database	---	informix
Informix		informix
Entrust/Master Control	Master1	TimeStepM1
Entrust/Master Control	Master2	TimeStepM2
Entrust/Master Control	Master3	TimeStepM3
Entrust/Master Control	First Officer	TimeStepF1
CA Distinguished Name	o=TimeStep,c=CA	permit