

The F-Secure logo consists of the text "F-SECURE" in a bold, sans-serif font above a stylized shield icon. The shield is composed of three overlapping geometric shapes: a triangle pointing down, a square, and a triangle pointing up. The background of the logo is a circular, glowing effect with radiating lines.

F-Secure VPN+:

***PKI Integration with
Netscape Certificate
Management System***

F-Secure Corporation

Securing the Mobile Distributed Enterprise

**IMPLEMENTATION
GUIDE
OCTOBER 2000**

F-Secure VPN+: PKI Integration with Netscape Certificate Management System

Implementation Guide, October 2000

All product names referenced herein are trademarks or registered trademarks of their respective companies. F-Secure™ Corporation disclaims proprietary interest in the marks and names of others. Although F-Secure Corporation makes every effort to ensure that this information is accurate, F-Secure Corporation will not be liable for any errors or omission of facts contained herein. F-Secure Corporation reserves the right to modify specifications cited in this document without prior notice.

Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of F-Secure Corporation.

The purpose of this document is to help you identify the strengths of the integrated security solutions the F-Secure product line provides. It is not a comparative review of competitor's products but it may provide valuable information that will assist you see what makes our offering different from all the others.

<p>USA</p> <p>F-Secure Inc. 675 N. First Street, 5th floor San Jose, CA 95112, USA Tel (408) 938 6700 Fax (408) 938 6701 http://www.F-Secure.com/</p>	<p>Europe</p> <p>F-Secure Corporation PL 24 FIN-02231 Espoo, Finland Tel +358 9 859 900 Fax +358 9 8599 0599 http://www.F-Secure.com/</p>
---	--

Copyright © 1995-2000 F-Secure Corporation. All rights reserved.

Contents

1	<i>Executive Summary</i>	1
2	<i>Requirements</i>	1
3	<i>Assumptions</i>	1
4	<i>Installing PKI System</i>	2
4.1	<i>Install Netscape Certificate Management System 4.2</i>	2
4.2	<i>Run CMS Installation Wizard</i>	9
4.3	<i>Configure SCEP Enrolment</i>	26
5	<i>Integration with F-Secure VPN+</i>	31
5.1	<i>Add CA Certificate as Trusted Root</i>	31
5.1.1	Export CA Certificate	31
5.1.2	Import CA Certificate as Trusted Root.....	31
4.1	<i>Configure Certificate Handling</i>	32
4.1.1	Enable SCEP Enrollment.....	32
4.1.2	Enable CRL Retrieval	33
4.2	<i>Create Connection Template</i>	33
5.2	<i>Known Issues</i>	39

1 Executive Summary

F-Secure VPN+ is a software-based virtual private network that provides total end-to-end security by protecting every link in the corporate network chain including clients, servers, and gateways.

F-Secure VPN+ integrates with our world-class distributed firewall, anti-virus, and desktop encryption solutions under one policy management system, enabling you to deploy and manage your crucial security applications throughout the world from a single location and maintain complete transparency to the end-user.

F-Secure VPN+ supports SCEP and LDAP protocols for automated certificate enrollment, revocation, and updating, eliminating the need to manually download certificates and Certificate Revocation Lists (CRLs). F-Secure VPN+ has been tested and proven to interoperate with Netscape Certificate Management System. This implementation guide will detail the necessary steps to configure and use F-Secure VPN+ with Netscape Certificate Management System.

2 Requirements

Before you begin, you should have access to the following:

- ❑ NT Server with Service Pack 6a or later
- ❑ Netscape Certificate Management System 4.2 installation media
An evaluation version of this software can be downloaded from <http://www.iPlanet.com>.

3 Assumptions

The following assumptions have been made for the purposes of this document. If these assumptions are not correct for your individual installation, some of the information contained here may be inapplicable or incorrect.

- ❑ **All of the PKI components (LDAP Server and CA) will be residing on the same physical server.** Minor adjustments will need to be made to the installation procedures if some or all of these components are placed on separate servers.
- ❑ **None of components have been installed on the server yet.** It may only be necessary to make configuration changes instead of performing a complete installation of some components.
- ❑ **Server components (e.g. LDAP) will be used only for the PKI system.** If this is not the case, additional installation options may be required.

- ❑ **This PKI System is being set up for demonstration purposes only.** In the case of a production system additional steps must be taken to enhance security.

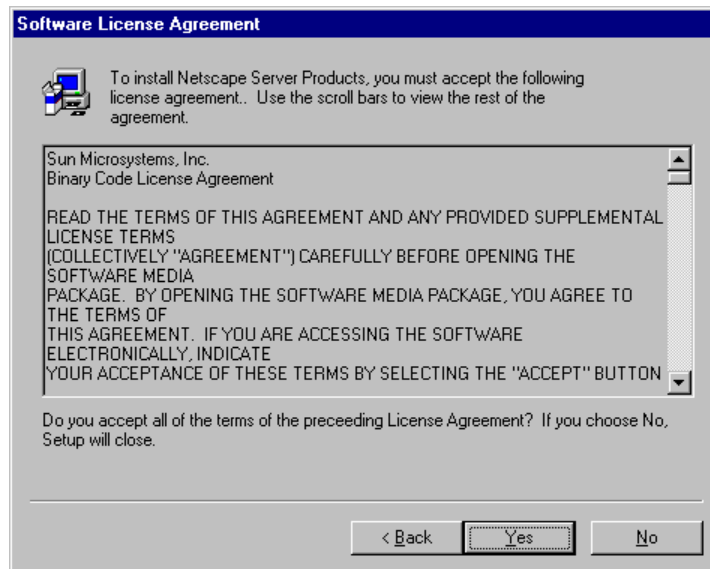
4 Installing PKI System

4.1 Install Netscape Certificate Management System 4.2

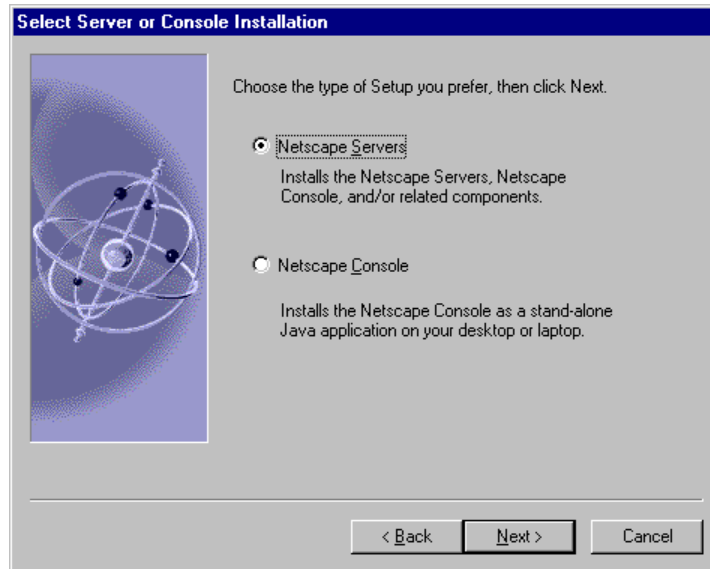
Run Setup.exe from Netscape Certificate Management System 4.2 installation media.



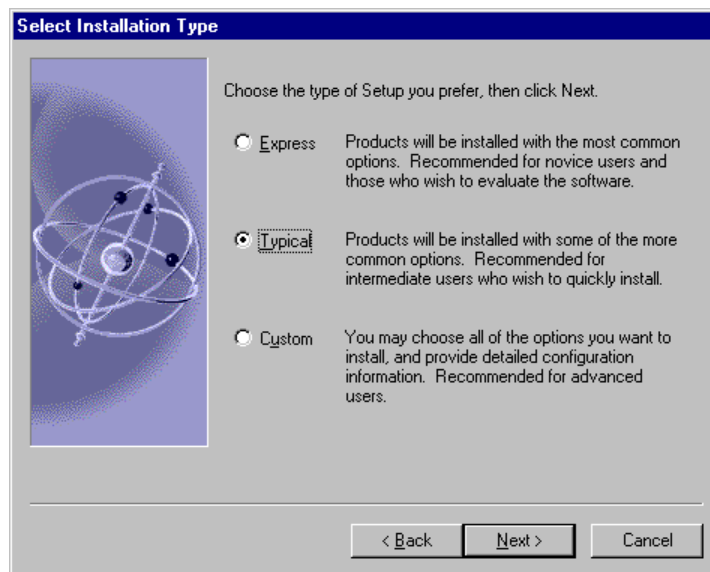
Click *Next* at the Welcome screen.



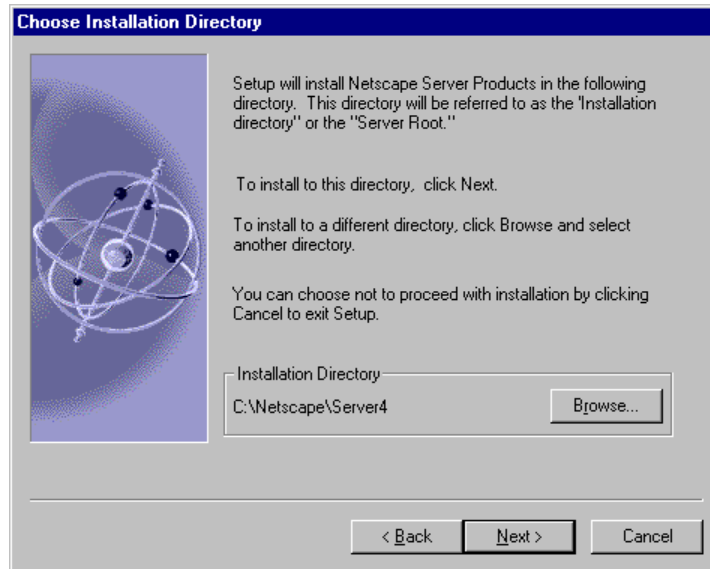
Click *Yes* to accept the License Agreement.



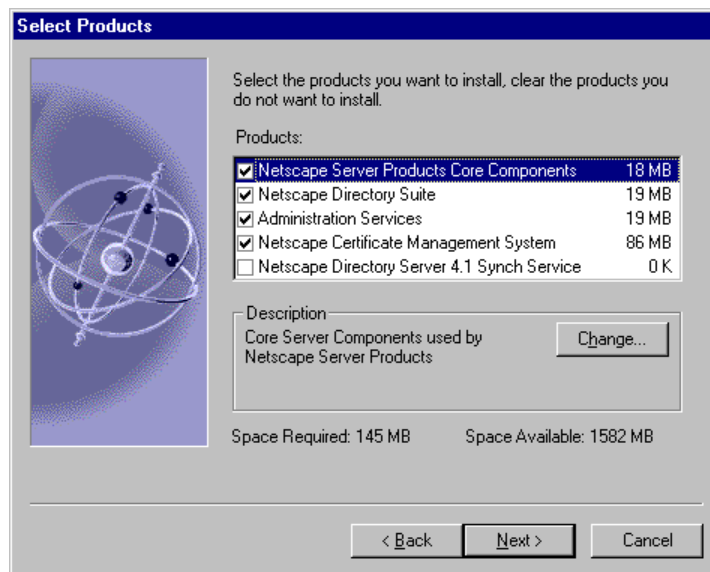
Select “Netscape Servers” as the type of setup and click *Next*.



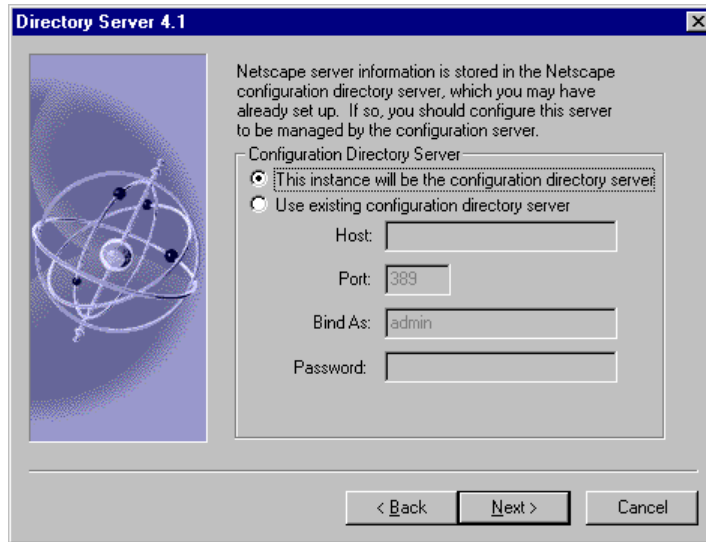
Select “Typical” setup type and click *Next*.



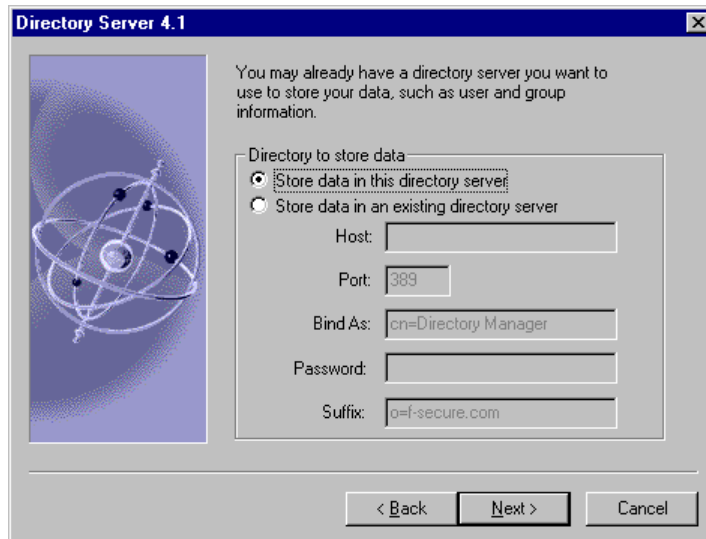
Click *Next* to accept the default directory of C:\Netscape\Server4.



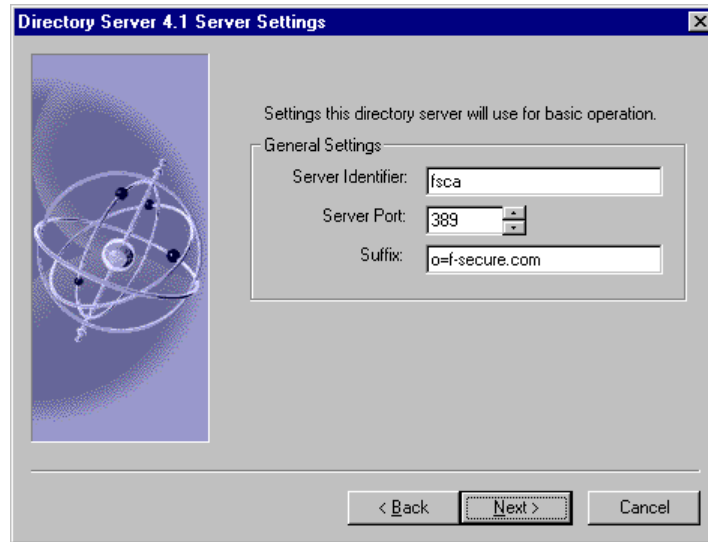
Select all components except the "Netscape Directory Server 4.1 Synch Service". Click *Next*.



Select the option to make this server the configuration directory server and click *Next*.



Select the option to store data in this directory server and click *Next*.

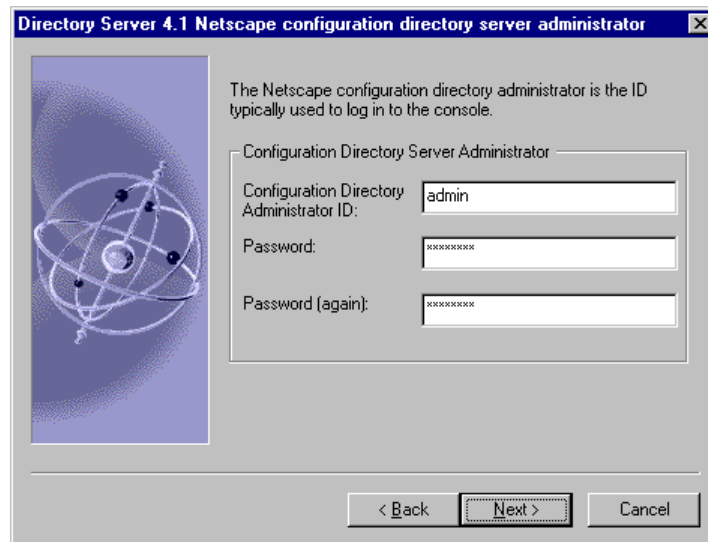


Enter the directory server settings and click *Next*.

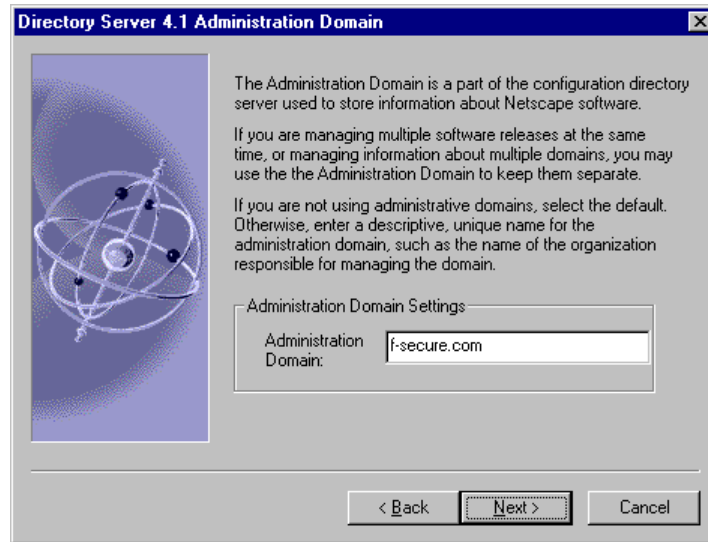
Server Identifier: host name of certificate server

Server Port: 389

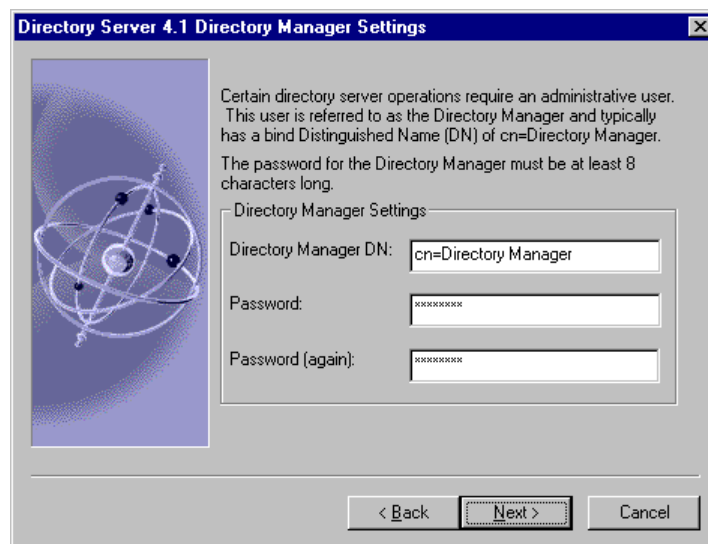
Suffix: o=<domain name>



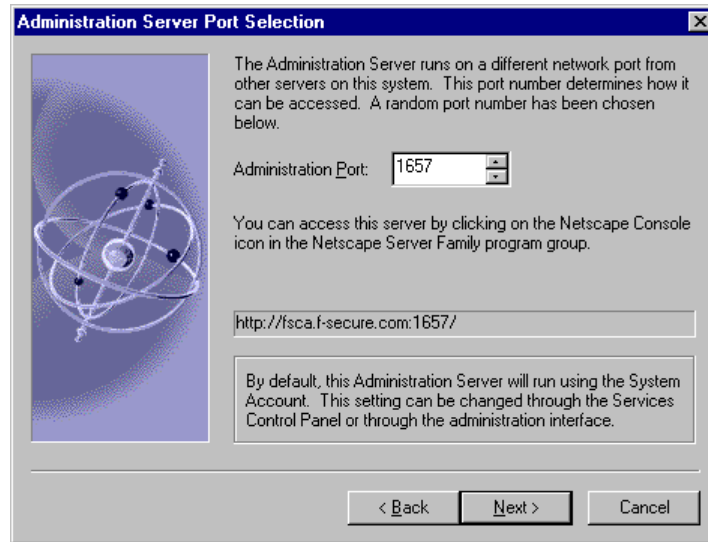
Enter the administrator ID and password and click *Next*.



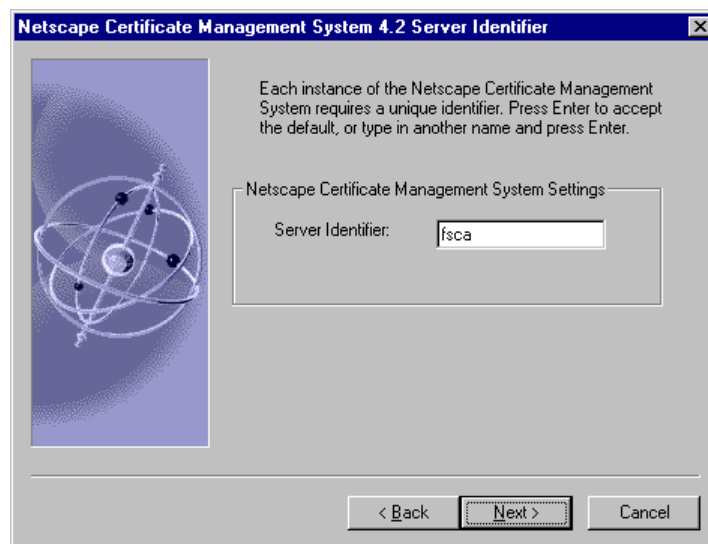
Enter the domain name or some other unique identifier as the “Administration Domain” and click *Next*.



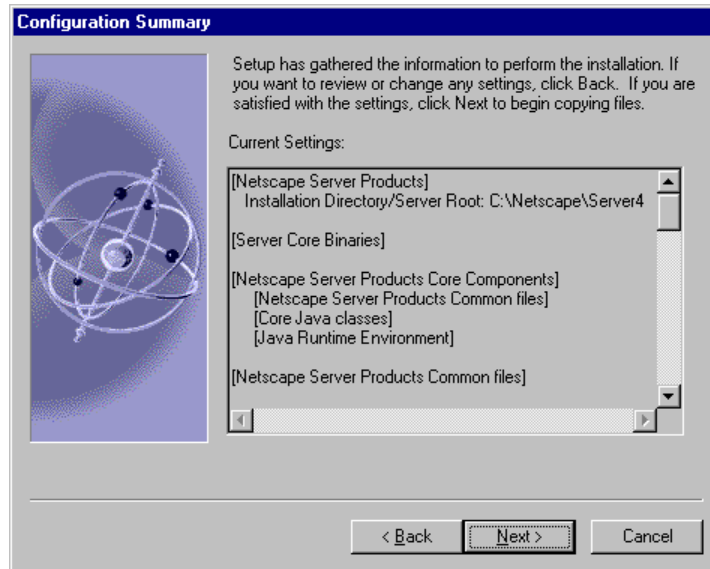
Enter the “Directory Manager DN” and password, then click *Next*.



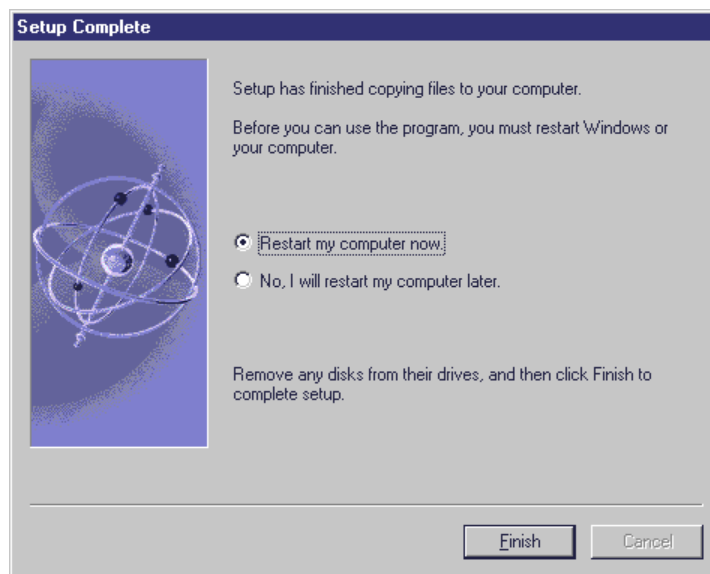
Accept the randomly generated administration port unless you require it to run on a specific port and click *Next*.



Click *Next* to accept the "Server Identifier" which is set to the server host name by default.



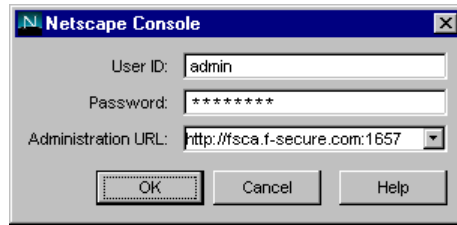
Click *Next* to begin copying files.



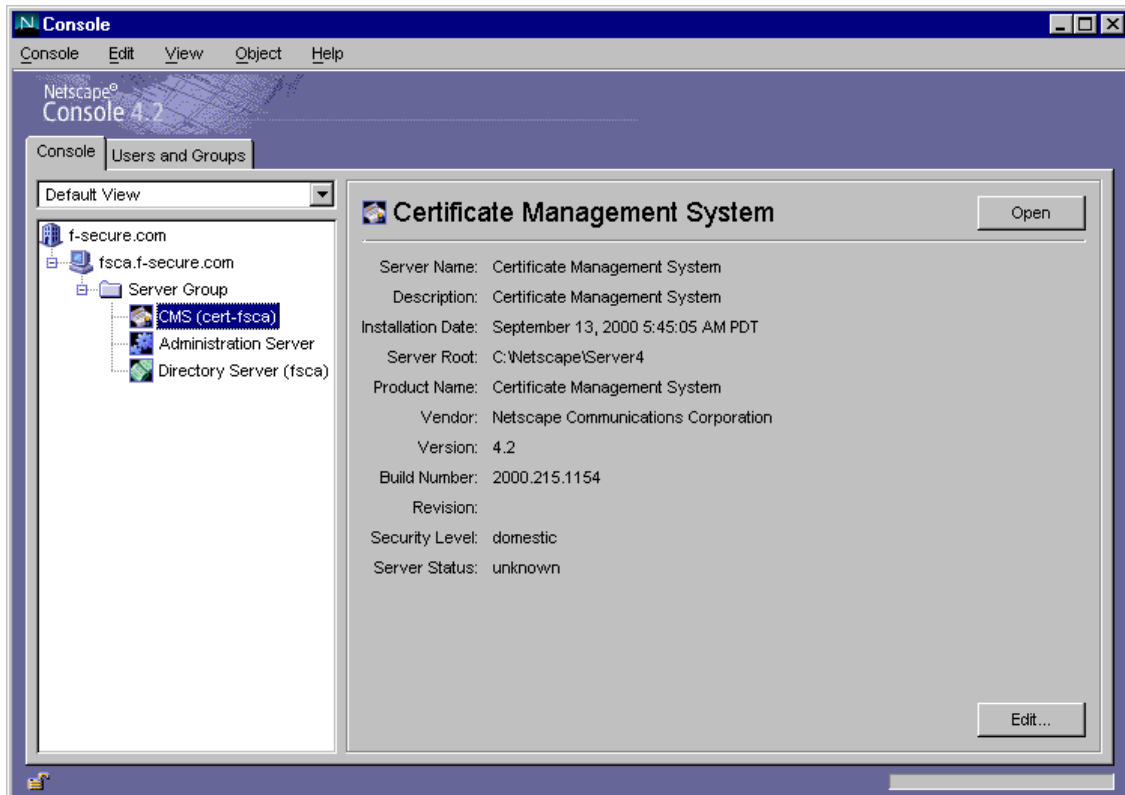
When the installation has finished, choose to “Restart my computer now” and click *Finish*.

4.2 Run CMS Installation Wizard

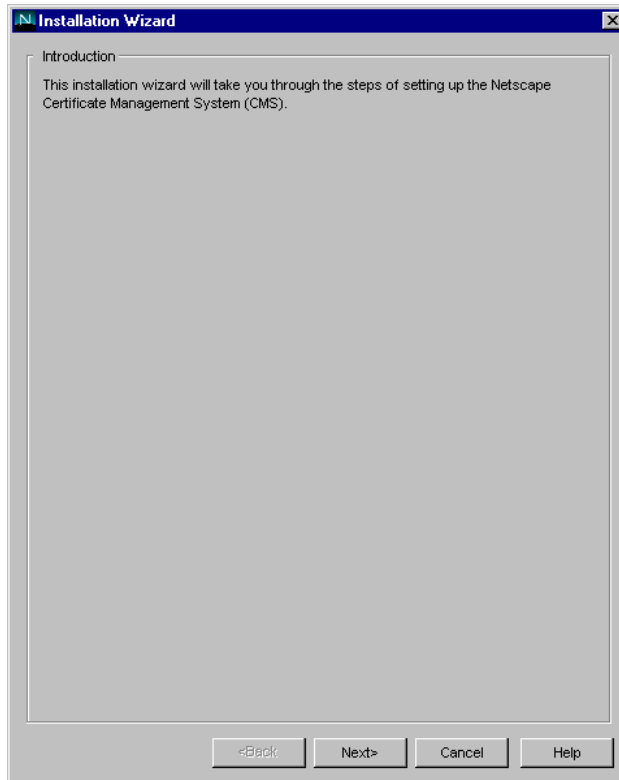
Start the Netscape Console from Start – Programs – Netscape Server Products – Netscape Console 4.2.



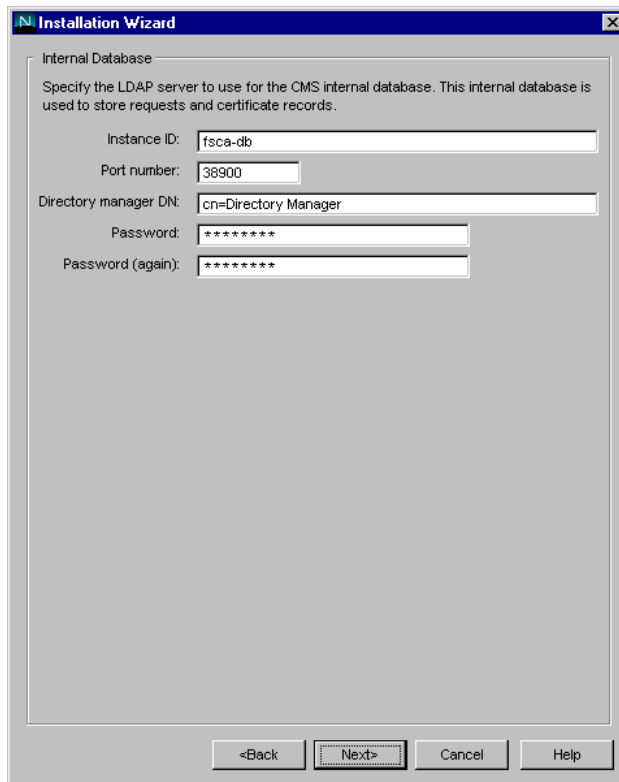
Log in as admin with the password you specified during the above installation.



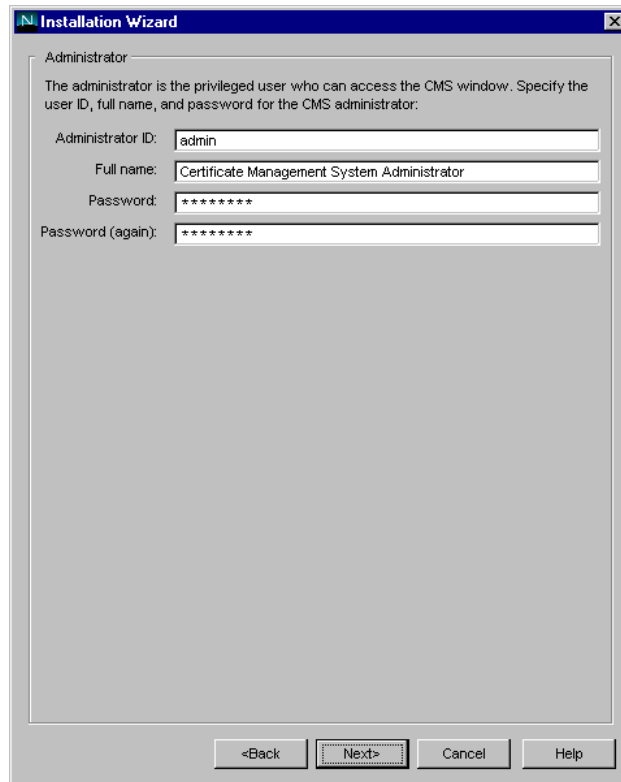
Browse to the instance of CMS in the console window and click the *Open* button. This will start the CMS Installation Wizard.



Click *Next* at the Introduction screen.

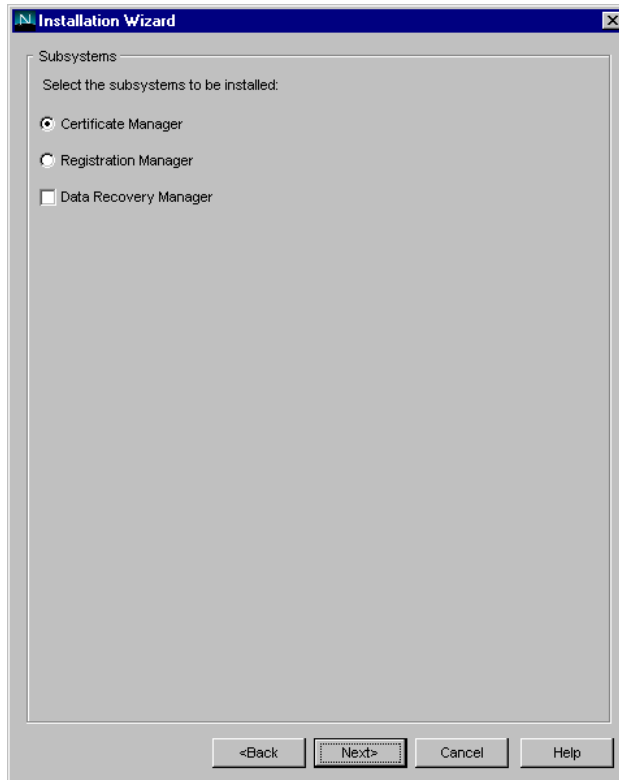


Enter the password for the cn=Directory Manager user and confirm it. Click *Next*.

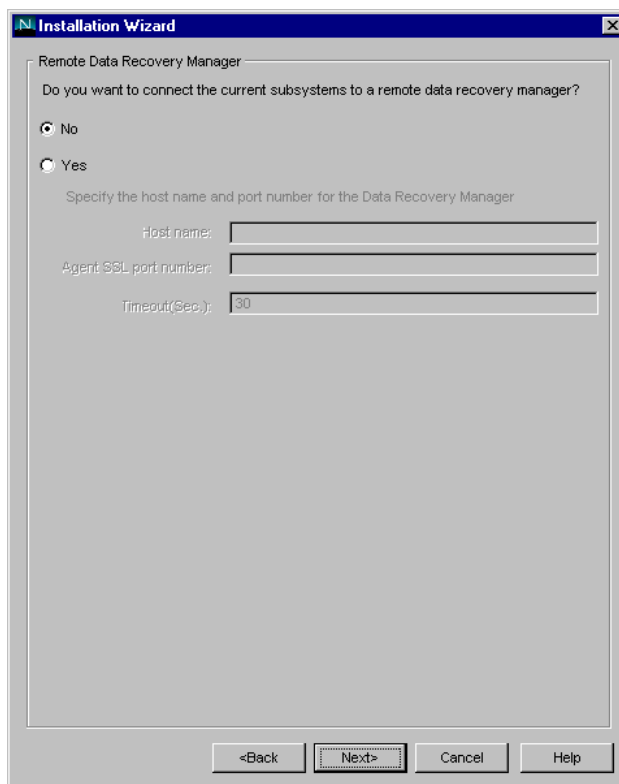


The image shows a Windows-style dialog box titled "Installation Wizard". It contains a section for configuring an administrator user. The text inside reads: "Administrator" followed by "The administrator is the privileged user who can access the CMS window. Specify the user ID, full name, and password for the CMS administrator:". Below this are four input fields: "Administrator ID:" with the value "admin", "Full name:" with the value "Certificate Management System Administrator", "Password:" with seven asterisks, and "Password (again):" with seven asterisks. At the bottom of the dialog are four buttons: "<Back", "Next>" (which is highlighted with a dotted border), "Cancel", and "Help".

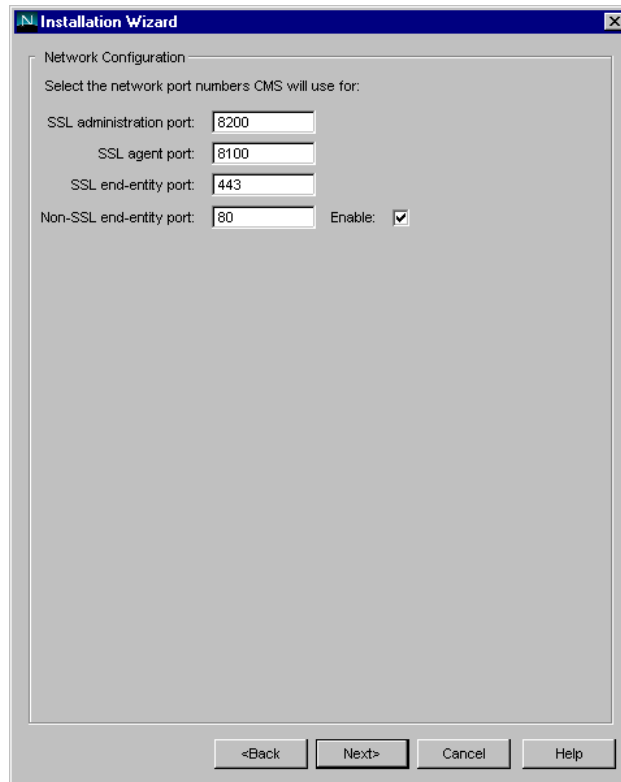
Enter a password for the CMS administrator user and click *Next*.



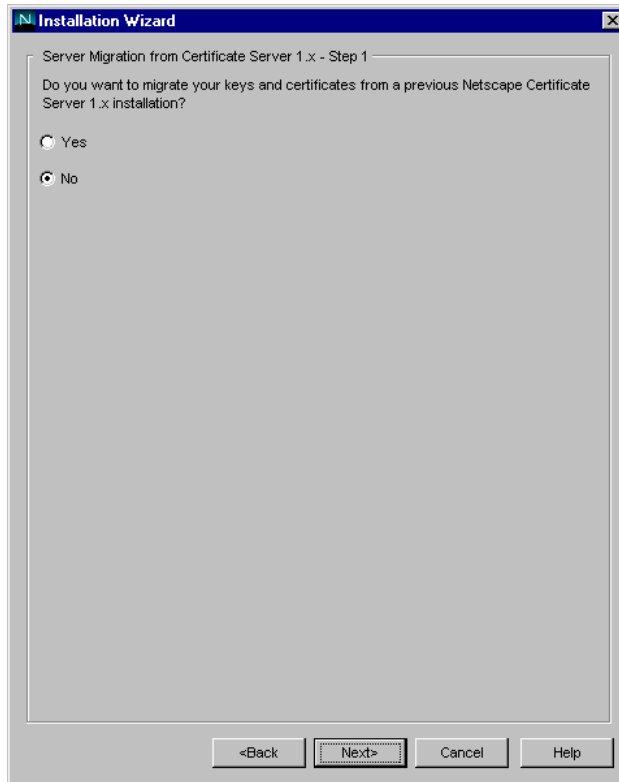
Select to install the “Certificate Manager” subsystem with no Data Recovery Manager and click *Next*.



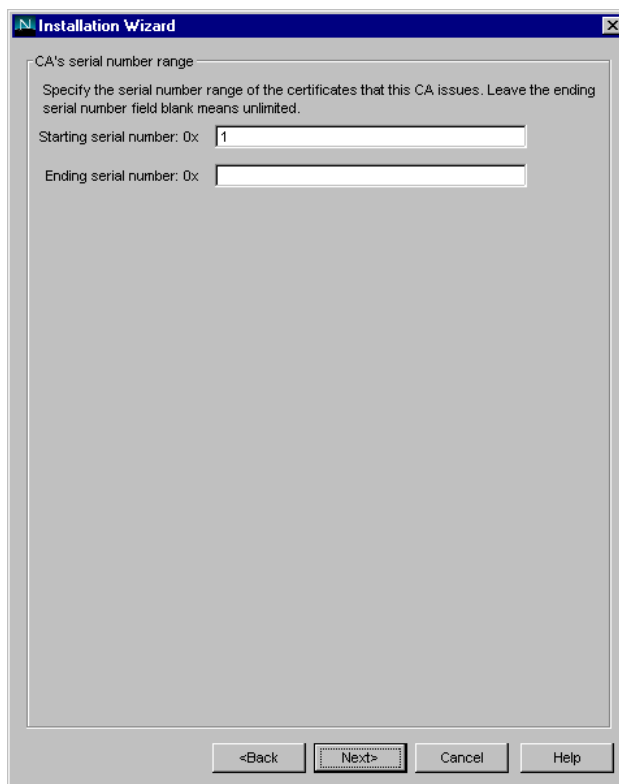
Select “No” to not connect to a remote Data Recovery Manager and click *Next*.



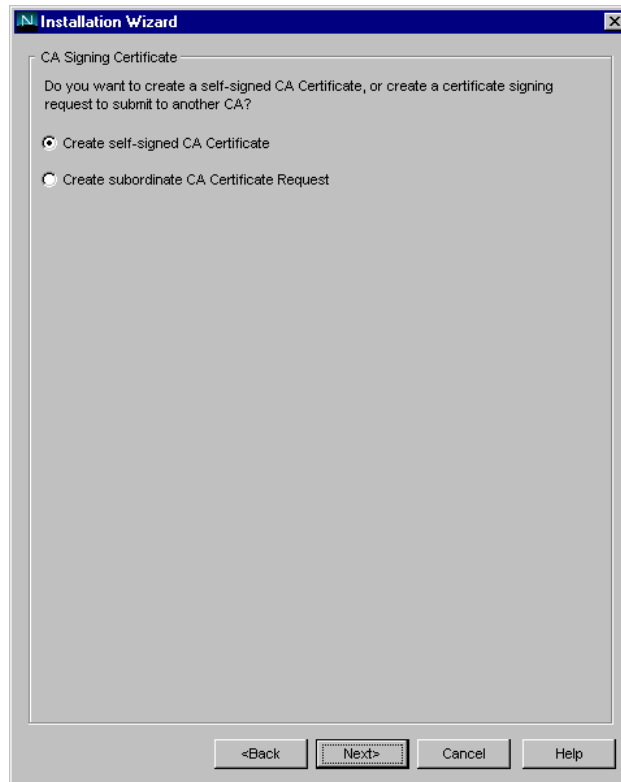
Check the “Enable” box to enable “Non-SSL end-entity port.” Click *Next* to continue.



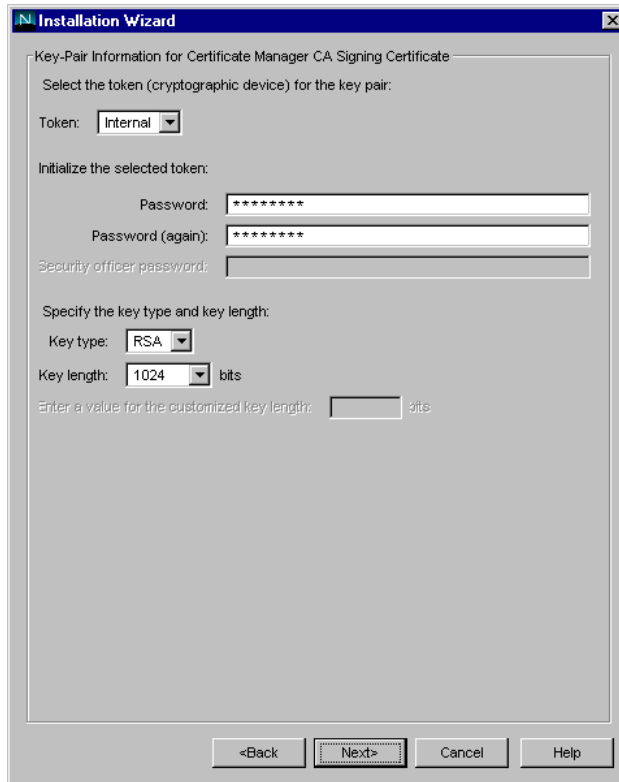
Select “No” to not migrate keys and certificates from a previous installation and click *Next*.



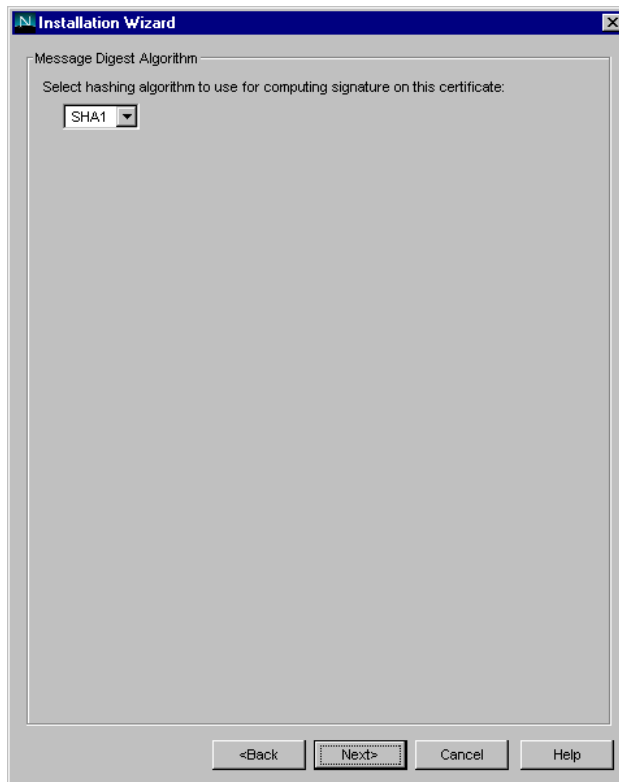
Enter a starting serial number of 1 and no ending serial number and click *Next*.



Select to “Create self-signed CA Certificate” and click *Next*.



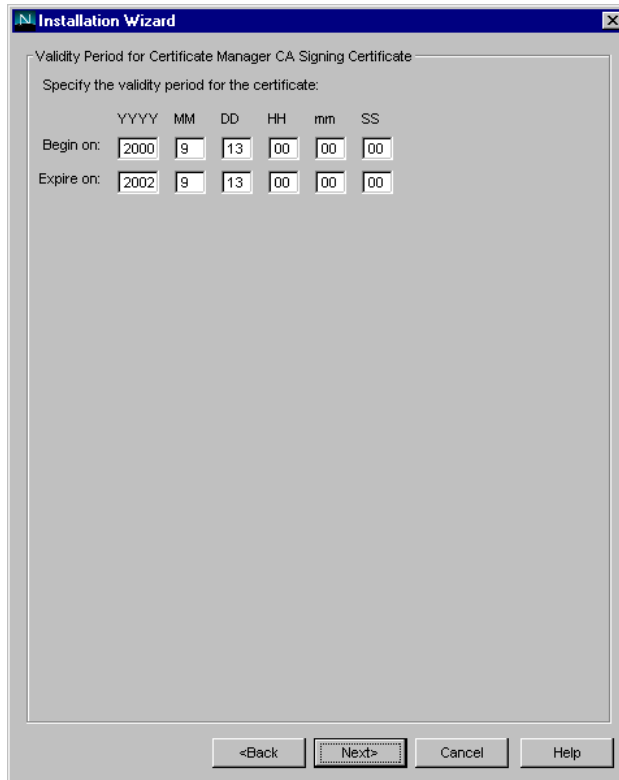
Enter a password for the CA key-pair and select a key length of 1024 bits. Click *Next*.



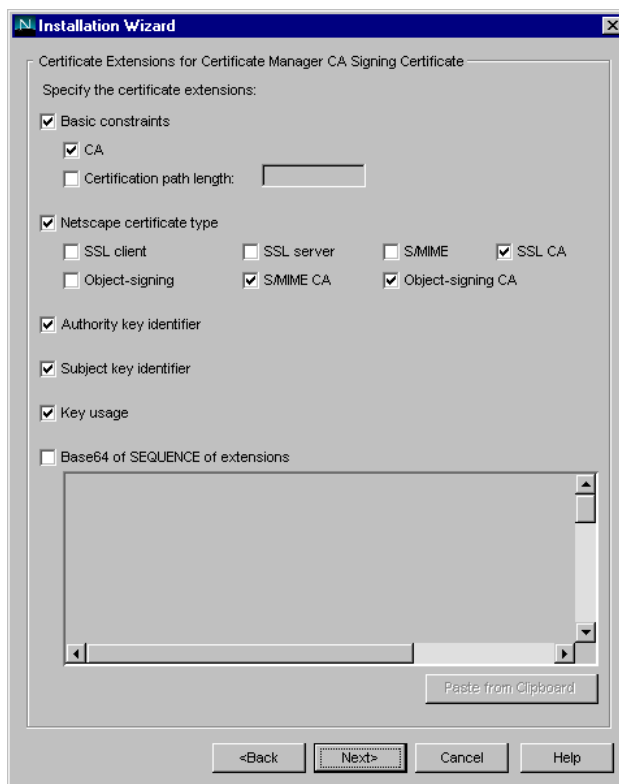
Select a hashing algorithm of SHA1 and click *Next*.

The screenshot shows a Windows-style dialog box titled "Installation Wizard". The main heading is "Subject Name for Certificate Manager CA Signing Certificate". Below this, it says "To modify the subject DN for the certificate:". There are two radio button options: "Enter the values for the subject DN components:" (which is selected) and "Enter the values for the subject DN string:". Under the selected option, there are several text input fields: "Common name (CN=):" with "Certificate Manager", "Organizational unit (OU=):" with "Test Lab", "Organization (O=):" with "FSecure", "Locality (L=):" (empty), "State (ST=):" (empty), and "Country (C=):" with "FI". Below these fields, it says "Selected DN: CN=Certificate Manager, OU=Test Lab, O=FSecure, C=FI". Under the unselected option, there is a single text input field containing "CN=Certificate Manager, C=US". At the bottom of the dialog, there are four buttons: "<Back", "Next>", "Cancel", and "Help". The "Next>" button is highlighted with a grey border.

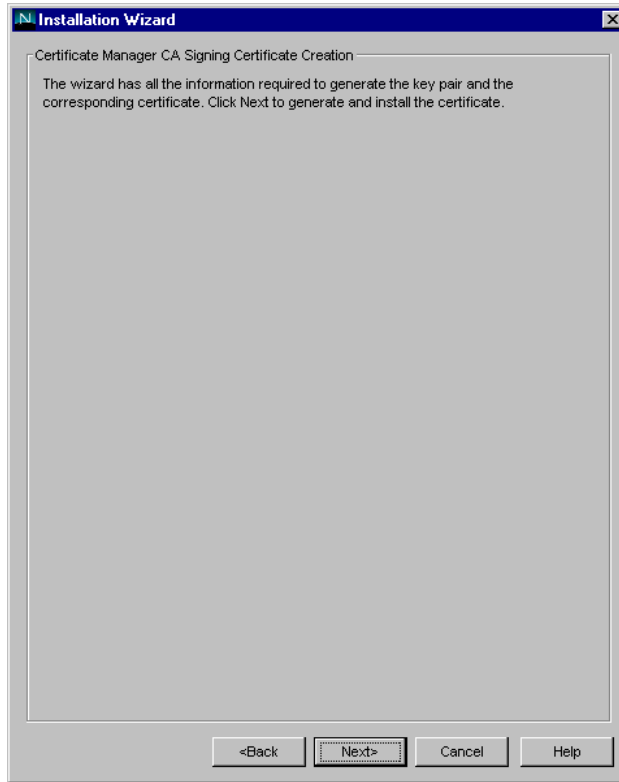
Enter the desired information for the CA Signing Certificate and click *Next*.



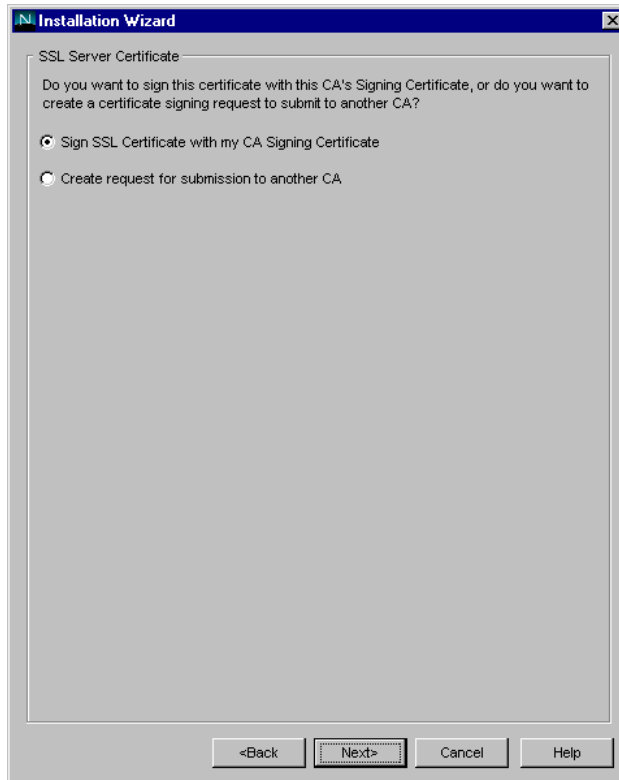
Select the validity period for the CA Signing Certificate. The default of 2 years should be sufficient. Click *Next*.



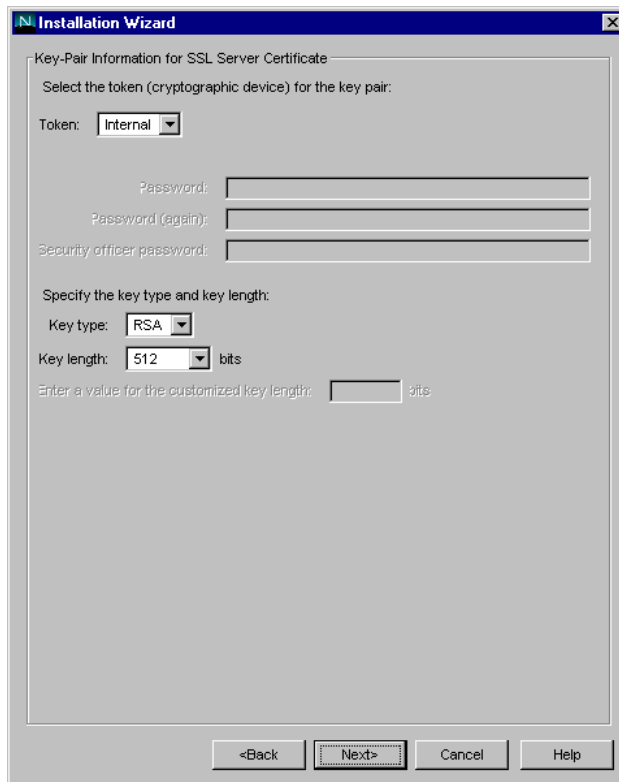
Accept the default certificate extensions by clicking *Next*.



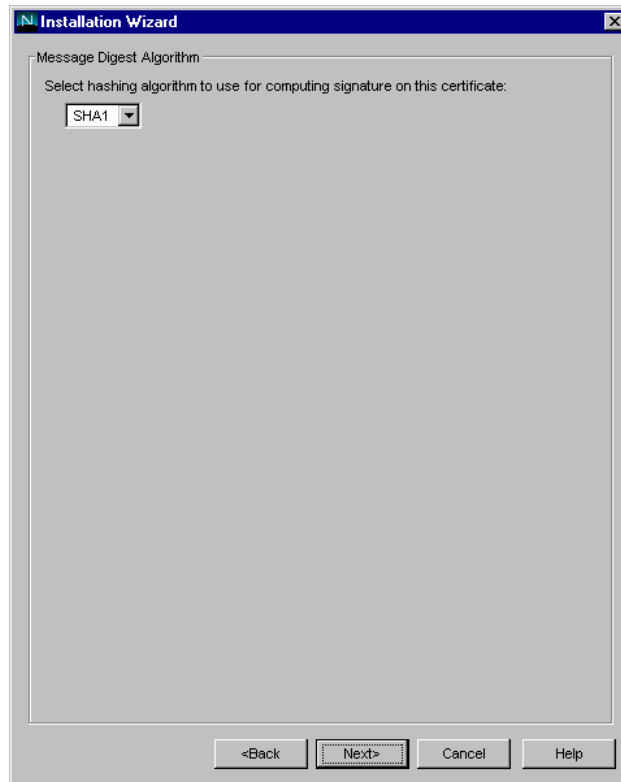
Click *Next* to generate and install the CA certificate.



Select to “Sign SSL Certificate with my CA Signing Certificate” and click *Next*.



Accept the default key-pair information for the SSL certificate by clicking *Next*.



Select the hashing algorithm of SHA1 for the certificate and click *Next*.

Installation Wizard

Subject Name for SSL Server Certificate

To modify the subject DN for the certificate:

Enter the values for the subject DN components:

*Common name (CN=):

Organizational unit (OU=):

Organization (O=):

Locality (L=):

State (ST=):

Country (C=):

Selected DN: CN=fsca.f-secure.com, OU=Test Lab, O=FSecure, C=FI

Enter the values for the subject DN string:

<Back Next> Cancel Help

Enter the desired information for the SSL Server Certificate. Note that the Common Name should be the fully qualified domain name of the server. Click *Next* to continue.

Installation Wizard

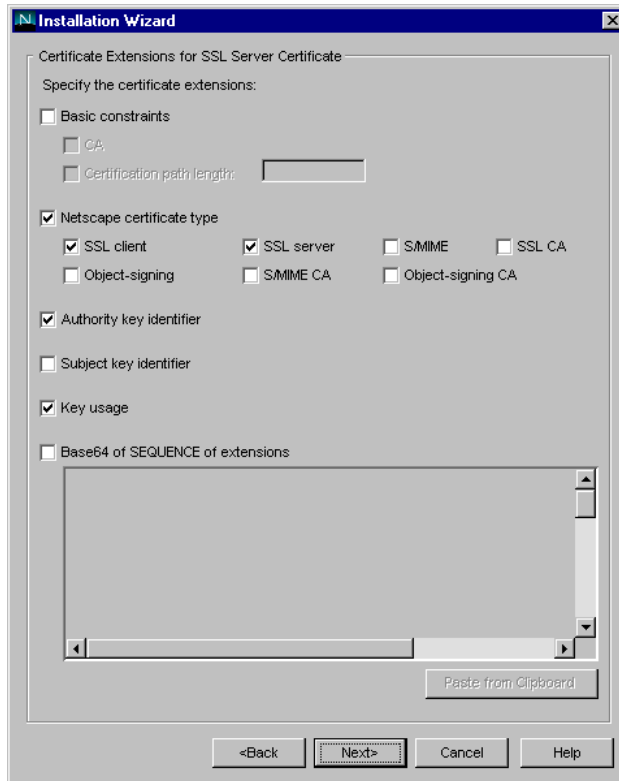
Validity Period for SSL Server Certificate

Specify the validity period for the certificate:

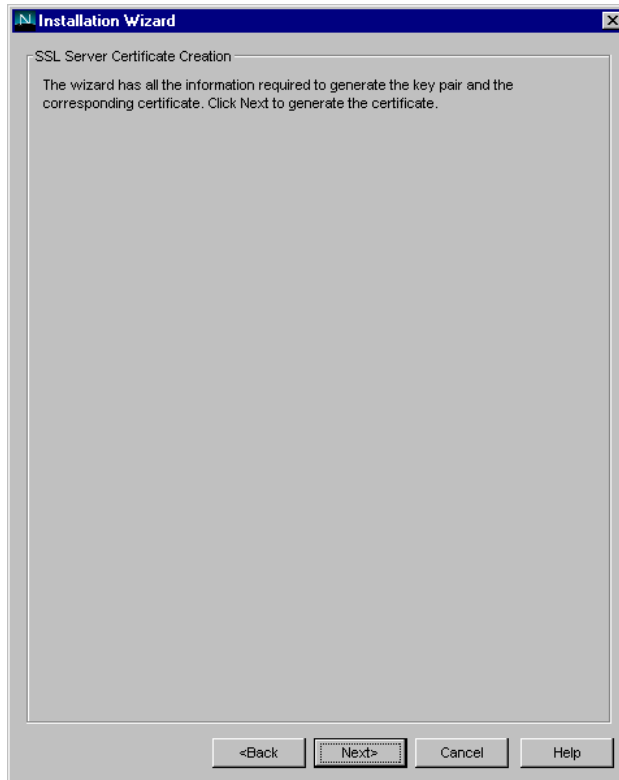
	YYYY	MM	DD	HH	mm	SS
Begin on:	2000	9	13	00	00	00
Expire on:	2001	9	13	00	00	00

<Back Next> Cancel Help

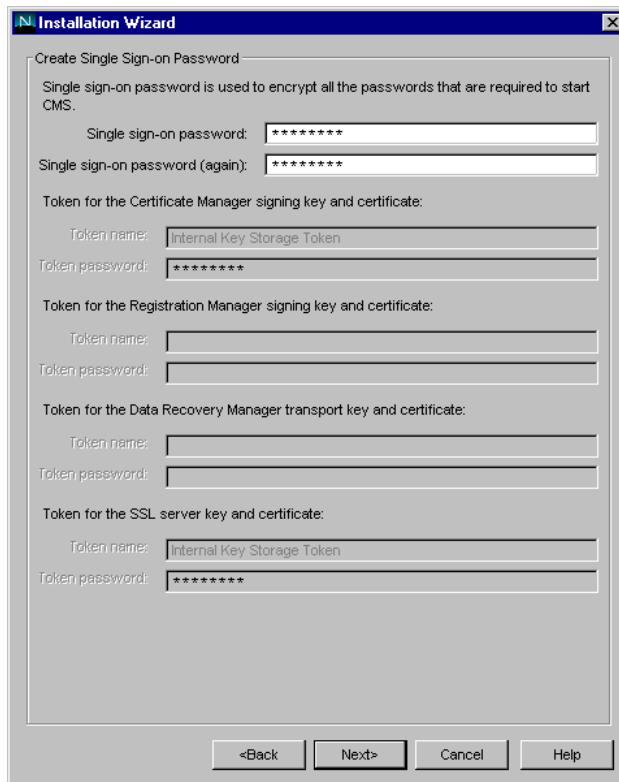
Enter the validity period for the SSL Server Certificate. Note that this must be less than the validity period for the CA Certificate. Select a one-year validity period and click *Next*.



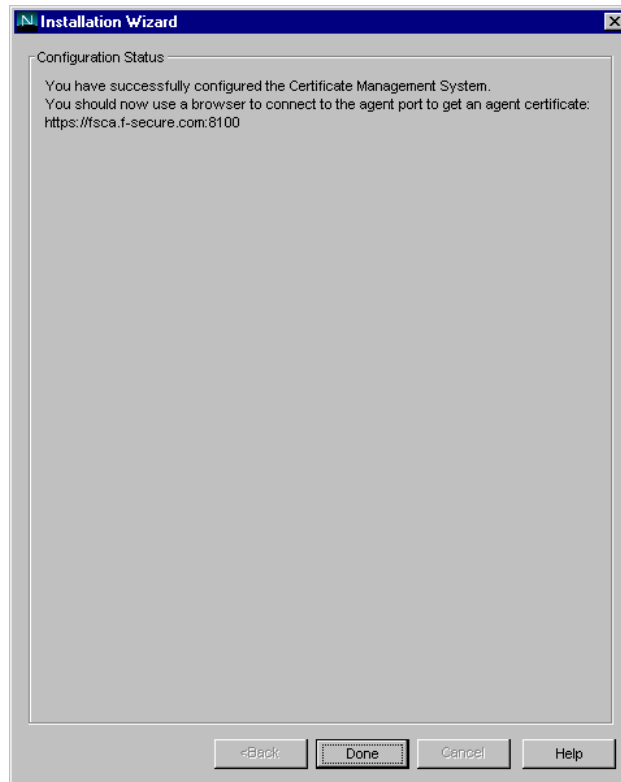
Accept the default certificate extensions by clicking *Next*.



Click *Next* to generate the SSL certificate.



Enter a password to be used as the single sign-on password for CMS and click *Next*.



Click *Done* to complete the Installation Wizard.

As the final screen says, you should now connect to <https://server:8100> and follow the instructions on the screen in order to get an agent certificate.

4.3 Configure SCEP Enrolment

Certificate Management System provides a menu-driven, interactive script to automate the configuration of the SCEP enrollment process. To use this script, follow the procedure below:

Create an SCEP Authorization file `cepauth.txt` in the `C:\Netscape\Server4` directory. This file should contain a single line: `"pwd: <password>"` where `<password>` can be any authorizing password to be sent with the CEP request. For a more secure environment this file can include additional fields that can be used to identify authorized requests before processing them. For more information regarding this file see the CMS documentation.

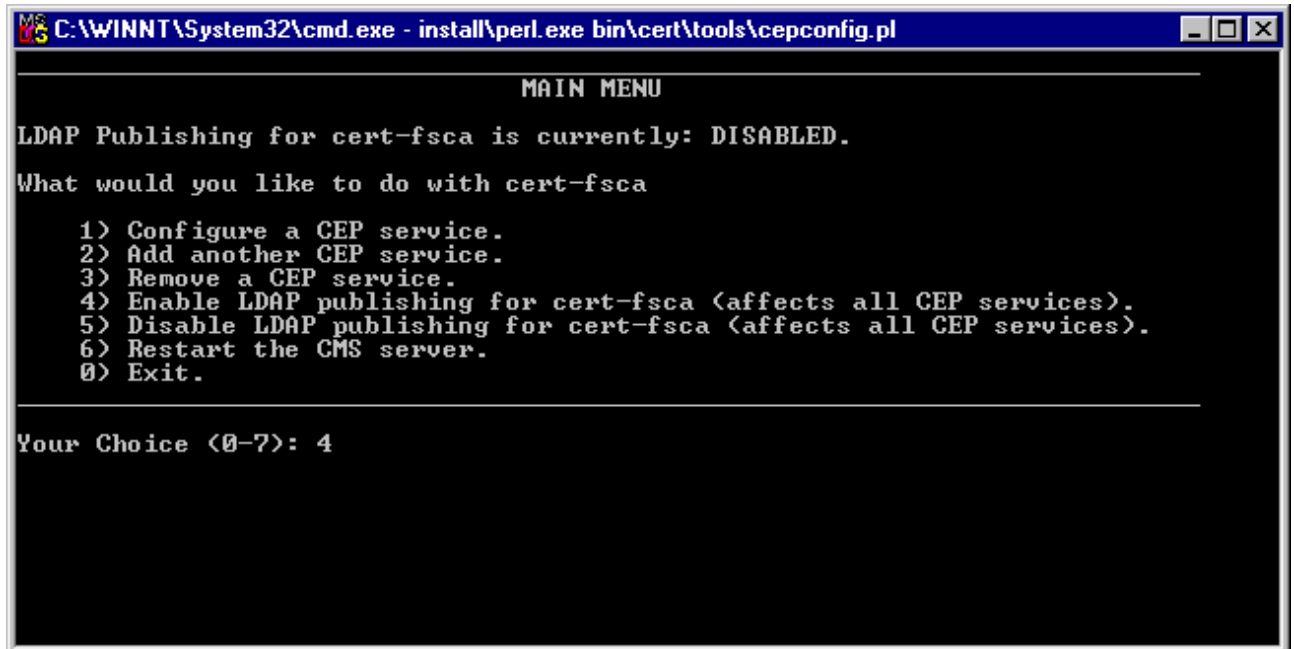
Open a command prompt window on the CMS host system.

Change to the `<root server>` directory. (e.g. `cd \netscape\server4`)

Enter the following at the command prompt and press Enter:

```
install\perl.exe bin\cert\tools\cepconfig.pl
```

Press Enter a few times to get to the “Main Menu” screen.



```
C:\WINNT\System32\cmd.exe - install\perl.exe bin\cert\tools\cepconfig.pl

MAIN MENU

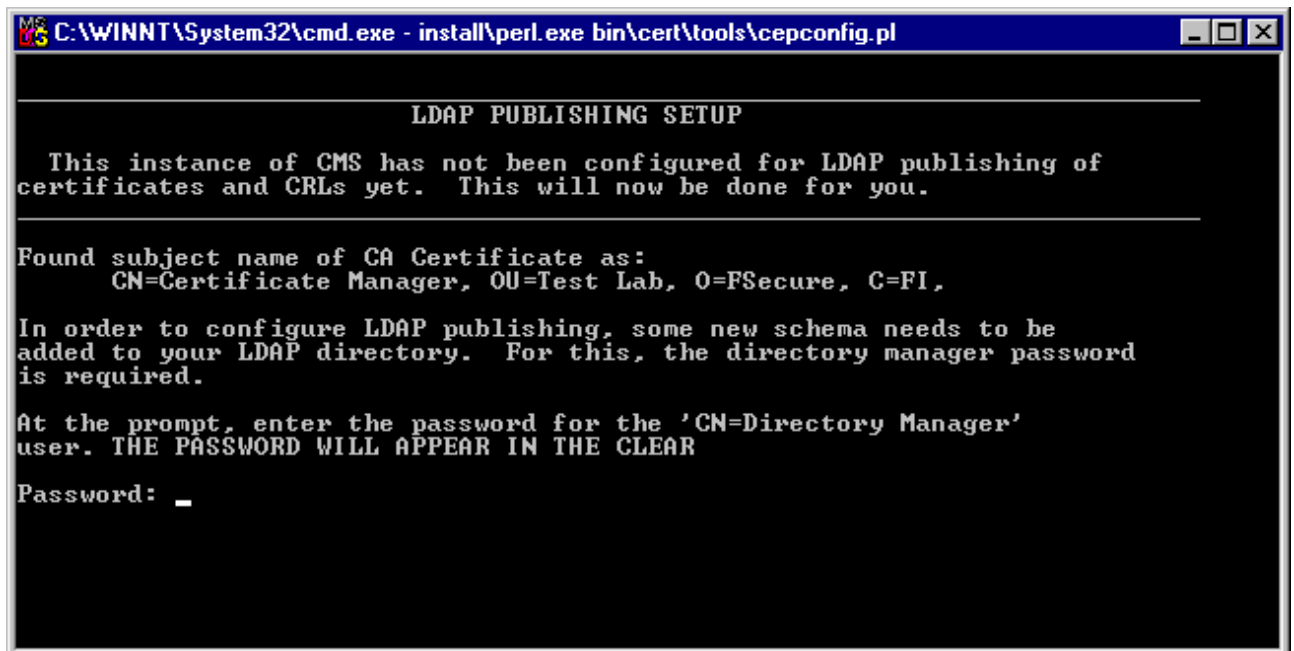
LDAP Publishing for cert-fsca is currently: DISABLED.

What would you like to do with cert-fsca

1) Configure a CEP service.
2) Add another CEP service.
3) Remove a CEP service.
4) Enable LDAP publishing for cert-fsca (affects all CEP services).
5) Disable LDAP publishing for cert-fsca (affects all CEP services).
6) Restart the CMS server.
0) Exit.

Your Choice <0-7>: 4
```

The first task is to enable LDAP publishing for the server. Enter “4”.



```
C:\WINNT\System32\cmd.exe - install\perl.exe bin\cert\tools\cepconfig.pl

LDAP PUBLISHING SETUP

This instance of CMS has not been configured for LDAP publishing of
certificates and CRLs yet. This will now be done for you.

Found subject name of CA Certificate as:
  CN=Certificate Manager, OU=Test Lab, O=FSecure, C=FI,

In order to configure LDAP publishing, some new schema needs to be
added to your LDAP directory. For this, the directory manager password
is required.

At the prompt, enter the password for the 'CN=Directory Manager'
user. THE PASSWORD WILL APPEAR IN THE CLEAR

Password: _
```

When prompted enter the Directory Manager password and press Enter.

```
C:\WINNT\System32\cmd.exe - install\perl.exe bin\cert\tools\cepconfig.pl

add objectclass:
    top
    person
add cn:
    Certificate Manager
add sn:
    CA Certificate
adding new entry cn=Certificate Manager,0=FSecure
modify complete

Enabling LDAP publishing.

Enter the CMS single-signon password: password

LDAP publishing of certificates and CRLs is now ENABLED for cert-fsca.
This means that each CEP service may now be configured for LDAP Publishing.
If you want to enable LDAP Publishing for a CEP service, you must
configure that service explicitly and enable LDAP Publishing for that
service.

You have made changes that will not become effective until the
CMS server has been restarted. Do you want to restart the server now?
Restart (y/n)? n_
```

When prompted enter the CMS single sing-on password and press Enter.

Enter “n” to not restart the server at this time. This will be done once the configuration is complete.

You should now be back to the Main Menu. Enter “1” to configure a CEP service.

```
C:\WINNT\System32\cmd.exe - install\perl.exe bin\cert\tools\cepconfig.pl

Listing of CEP services currently installed:

-----
Service 1:
Service Name.....Default CEP Service
Service URL...../cgi-bin/pkiclient.exe
LDAP publishing.....Disabled.
Autoenrollment.....Disabled.

Please select the CEP service you want to configure. (<Specify 0 to cancel>)
Your Choice (0-1): 1_
```

Enter “1” to configure the default CEP service.

```
C:\WINNT\System32\cmd.exe - install\perl.exe bin\cert\tools\cepconfig.pl
CONFIGURE CEP SERVICE

Current Configuration:

Service Name.....Default CEP Service
Service URL...../cgi-bin/pkiclient.exe
LDAP publishing.....Disabled.
Autoenrollment.....Disabled.

What would you like to do with 'Default CEP Service'?

1) Rename this CEP service.      5) Enable autoenrollment.
2) Change the service URL.       6) Disable autoenrollment.
3) Enable LDAP publishing.       7) Configure autoenrollment
4) Disable LDAP publishing.      8) Return to main menu.

Your Choice <0-8>: 3
LDAP publishing of certificates and CRLs is now enabled for Default CEP Service.

You have made changes that will not become effective until the
CMS server has been restarted. Do you want to restart the server now?
Restart <y/n>? n
```

Enter “3” to enable LDAP publishing for the CEP service.

When prompted, enter “n” to not restart the CMS server.

Back at the Configure CEP Service menu enter “5” to enable autoenrollment.

```
C:\WINNT\System32\cmd.exe - install\perl.exe bin\cert\tools\cepconfig.pl
Service Name.....Default CEP Service
Service URL...../cgi-bin/pkiclient.exe
LDAP publishing.....Disabled.
Autoenrollment.....Enabled.
  Authentication file....<not configured>
  Key Attributes.....IPAddress
  Auth Attributes.....pwd
  Defer on failure.....false

To enable automated enrollment, your users identifying criteria must
be stored in a password-file.

Include in this file whatever items you want to authenticate with.
More information is in the Administrator's guide, - look for
'CEP', and 'Flatfile' in the index

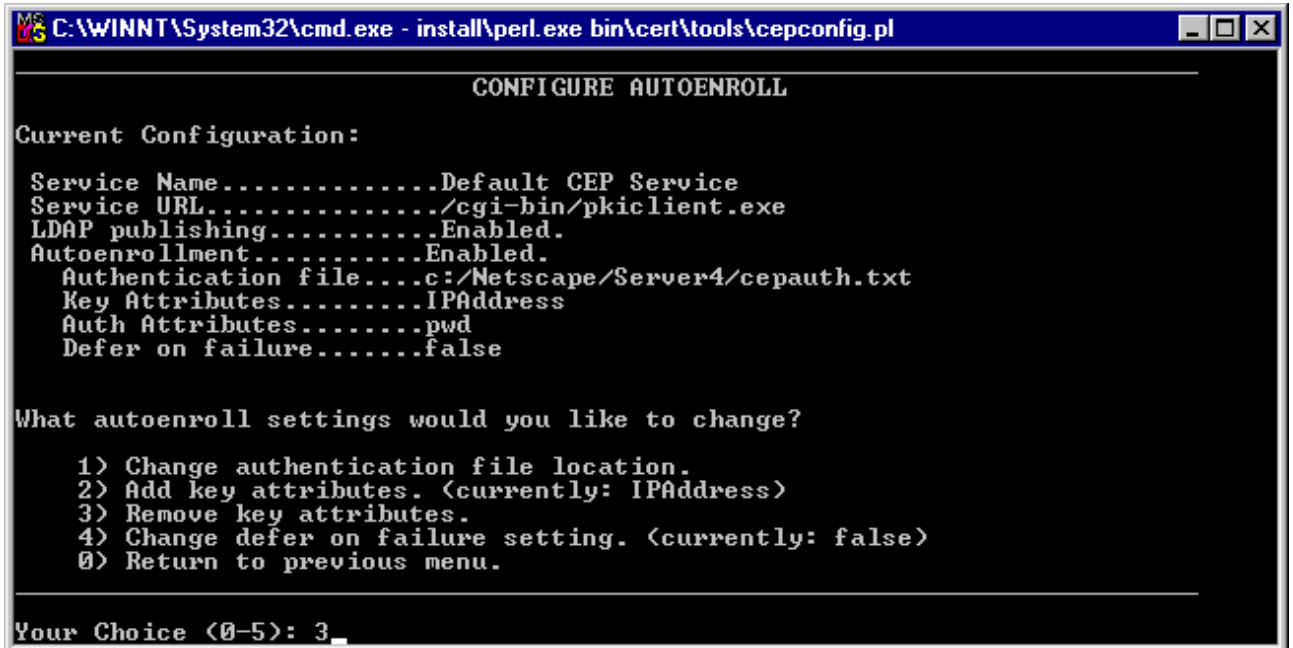
Please specify the full pathname of the password file:
File: c:\netscape\server4\cepauth.txt

You have made changes that will not become effective until the
CMS server has been restarted. Do you want to restart the server now?
Restart <y/n>? n
Press enter to continue...
```

Enter the path to the password file that you created earlier (e.g. c:\netscape\server4\cepauth.txt) and press Enter.

Again, enter “n” to not restart the CMS server and press Enter to return to the Configure CEP Service menu.

Enter “7” to configure autoenrollment.



```
C:\WINNT\System32\cmd.exe - install\perl.exe bin\cert\tools\cepconfig.pl

CONFIGURE AUTOENROLL

Current Configuration:

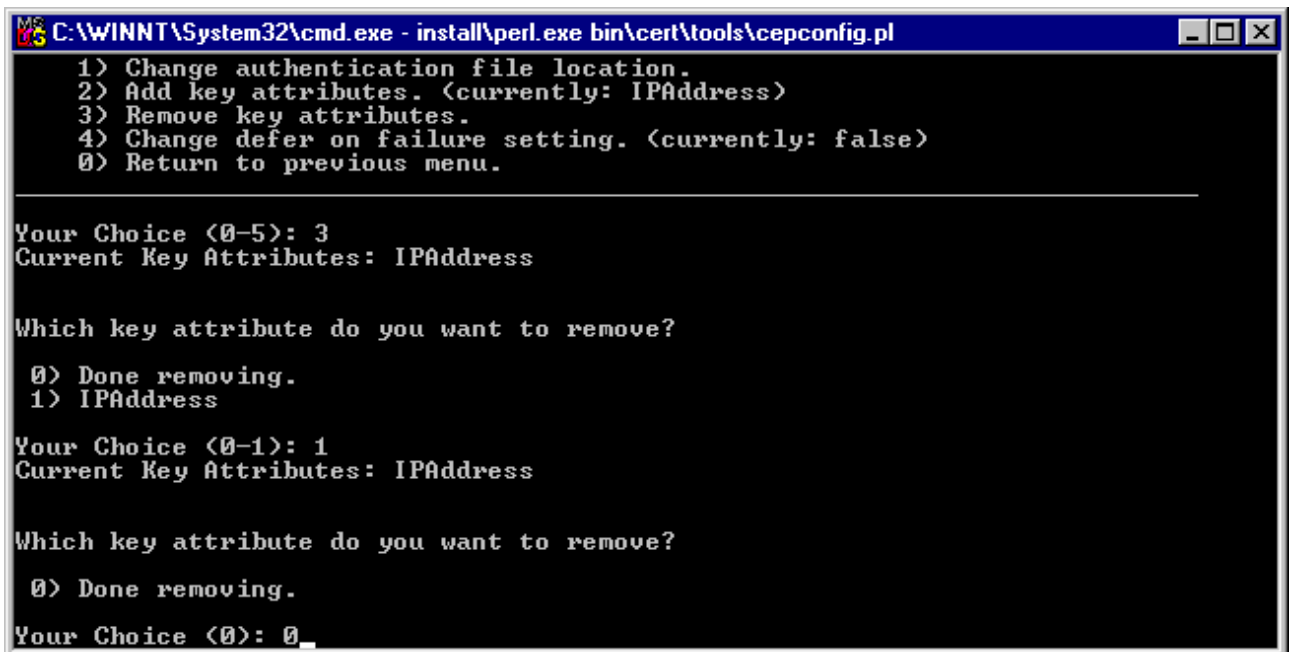
Service Name.....Default CEP Service
Service URL...../cgi-bin/pkiclient.exe
LDAP publishing.....Enabled.
Autoenrollment.....Enabled.
  Authentication file....c:/Netscape/Server4/cepauth.txt
  Key Attributes.....IPAddress
  Auth Attributes.....pwd
  Defer on failure.....false

What autoenroll settings would you like to change?

1) Change authentication file location.
2) Add key attributes. (currently: IPAddress)
3) Remove key attributes.
4) Change defer on failure setting. (currently: false)
0) Return to previous menu.

Your Choice <0-5>: 3_
```

Enter “3” to remove key attributes.



```
C:\WINNT\System32\cmd.exe - install\perl.exe bin\cert\tools\cepconfig.pl

1) Change authentication file location.
2) Add key attributes. (currently: IPAddress)
3) Remove key attributes.
4) Change defer on failure setting. (currently: false)
0) Return to previous menu.

Your Choice <0-5>: 3
Current Key Attributes: IPAddress

Which key attribute do you want to remove?

0) Done removing.
1) IPAddress

Your Choice <0-1>: 1
Current Key Attributes: IPAddress

Which key attribute do you want to remove?

0) Done removing.

Your Choice <0>: 0_
```

Enter “1” to remove the IPAddress attribute.

Enter “0” to return to the Configure CEP Service Menu.

Enter “0” to return to the Main Menu.

Enter “6” to restart the CMS Server.



Enter the CMS Single Sign-On password and click *OK*.

Enter “0” to exit the script.

5 Integration with F-Secure VPN+

5.1 Add CA Certificate as Trusted Root

5.1.1 Export CA Certificate

Launch a web browser and go to <https://<cms server>:8100>.

Click on the “Certificate Manager Agent Services” link.

Click on the “List Certificates” link.

Click the *Find* button.

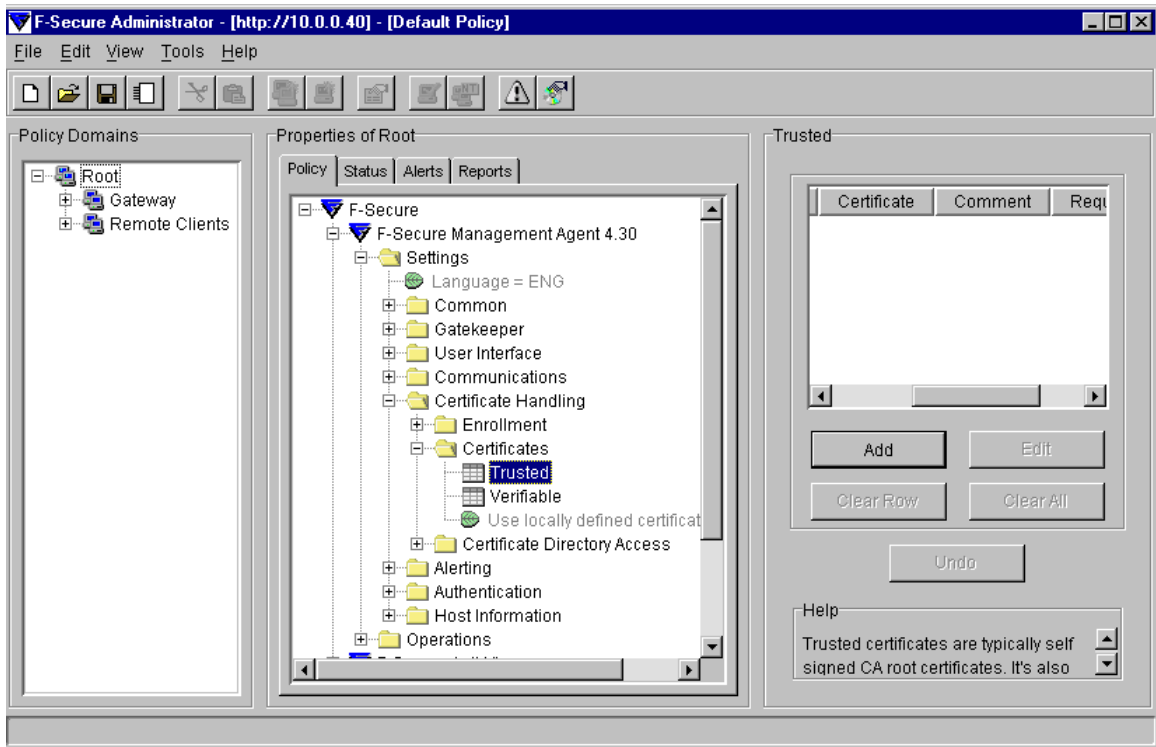
Click on the *Details* button of the certificate with serial number 0x00000001

Scroll down and copy the Base 64 encoded certificate details to an empty text file including the BEGIN CERTIFICATE and END CERTIFICATE lines.

Save the text file to a temporary location as cms_ca.pem (e.g. c:\temp\cms_ca.pem)

5.1.2 Import CA Certificate as Trusted Root

On the F-Secure Policy Manager Console computer, start F-Secure Administrator (Start – Programs – F-Secure Policy Manager Console.)



In the F-Secure Administrator (FSA) select the policy domain or host that you wish to enroll via SCEP.

Browse to F-Secure/F-Secure Management Agent/Settings/Certificate Handling/Certificates/Trusted item in the Properties pane.

Click on the *Add* button and browse to find the CA root certificate file that you created when exporting the CA certificate in the section above. Click *Open*.

Enter a descriptive comment (e.g. Netscape CA).

4.1 Configure Certificate Handling

4.1.1 Enable SCEP Enrollment

F-Secure VPN+ hosts can enroll for host certificates using the Simple Certificate Enrollment Protocol (SCEP.) An example of the policy settings that need to be configured is shown in the image below. The image is a snapshot of the settings under the F-Secure/F-Secure Management Agent/Settings/Certificate Handling section of the policy.

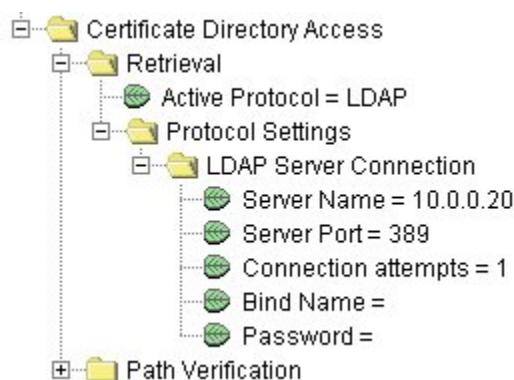


4.1.2 Enable CRL Retrieval

F-Secure VPN+ supports Certificate Revocation List (CRL) retrieval. If certificates are revoked from the CA, the serial numbers of the revoked certificates are stored in a CRL in the LDAP directory.

As IPSec connections are established between hosts, the host will check the CRL of the issuing CA to ensure that the certificate has not been revoked. This CRL is cached locally on the host for future use. A new CRL is fetched from the LDAP directory when the old CRL expires. The CRL Trust Time policy setting in FSA can be used to define how often to try to fetch a new CRL even if the host has a valid CRL available. Normally a CA system issues CRLs periodically, but they may also issue a new CRL right after a certificate has been revoked. This CRL Trust Time setting can be used to assure that the revocation information is transferred to the host faster than the normal CRL update time.

An example of the policy settings that need to be configured to enable CRL retrieval is shown in the image below. The image is a snapshot of the settings under the F-Secure/F-Secure Management Agent/Settings/Certificate Handling section of the policy.



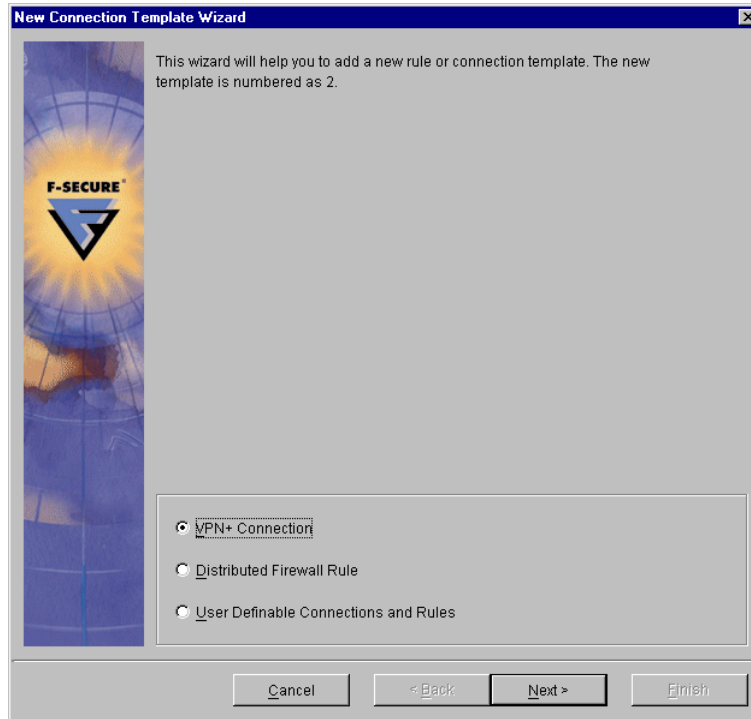
4.2 Create Connection Template

Once the certificates have been installed on the required hosts and/or gateways according to the steps above, you are ready to create an IPSec connection. Again, these can either be centrally managed using F-Secure Administrator (recommended) or set up manually

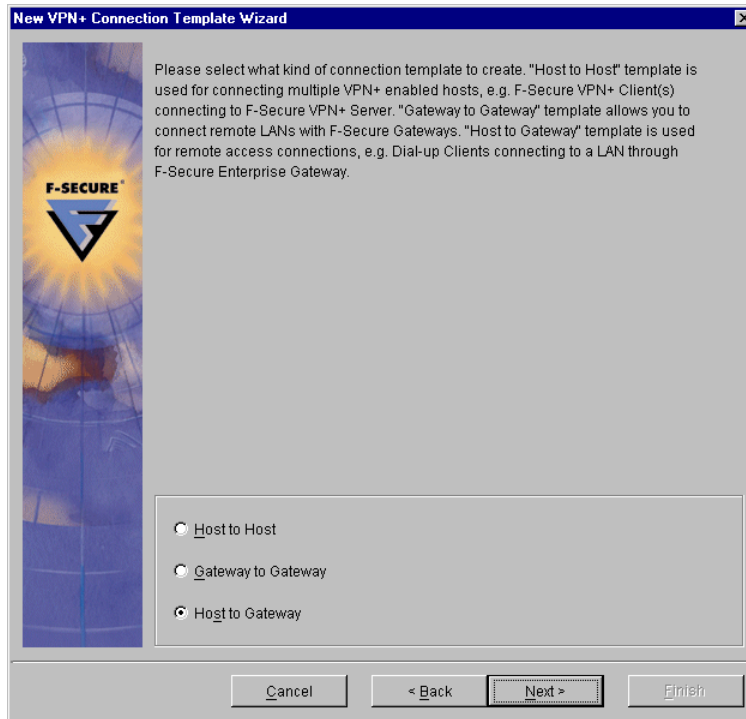
on each client. For the purposes of this document, the creation of a simple host-to-gateway IPSec connection will be demonstrated below.

In FSA, browse to the F-Secure/F-Secure VPN+/Settings/Connections item.

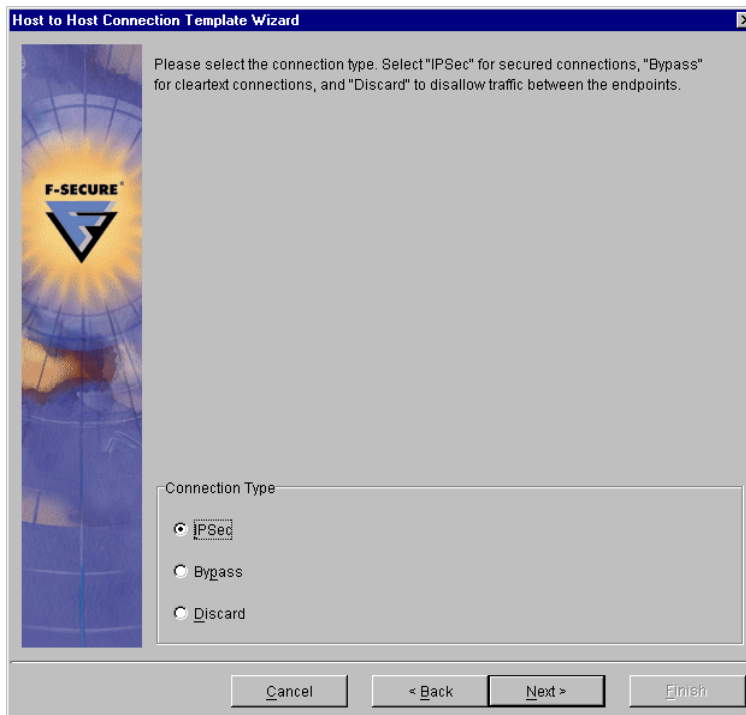
Click on the *Add* button to add a new connection.



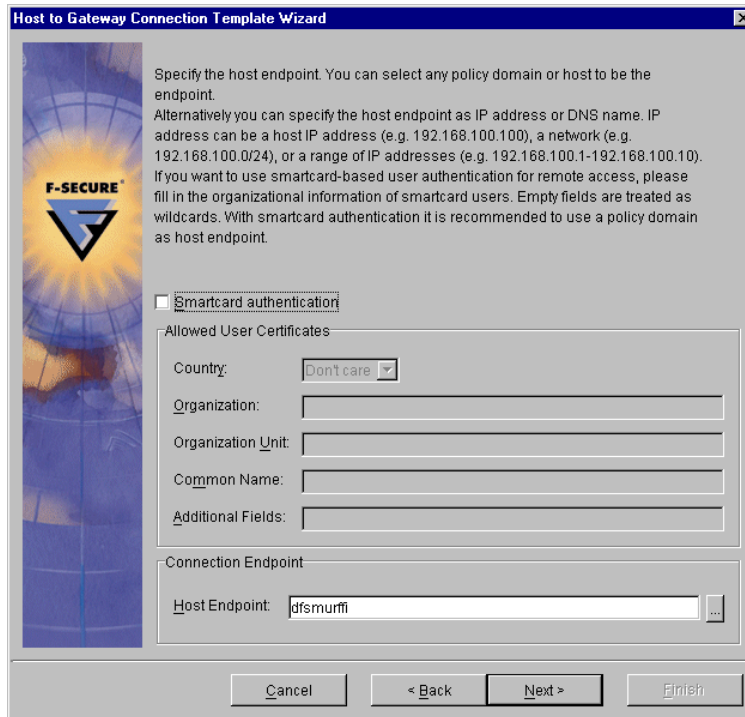
Select “VPN+ Connection” and click *Next*.



Select “Host to Gateway” and click *Next*.

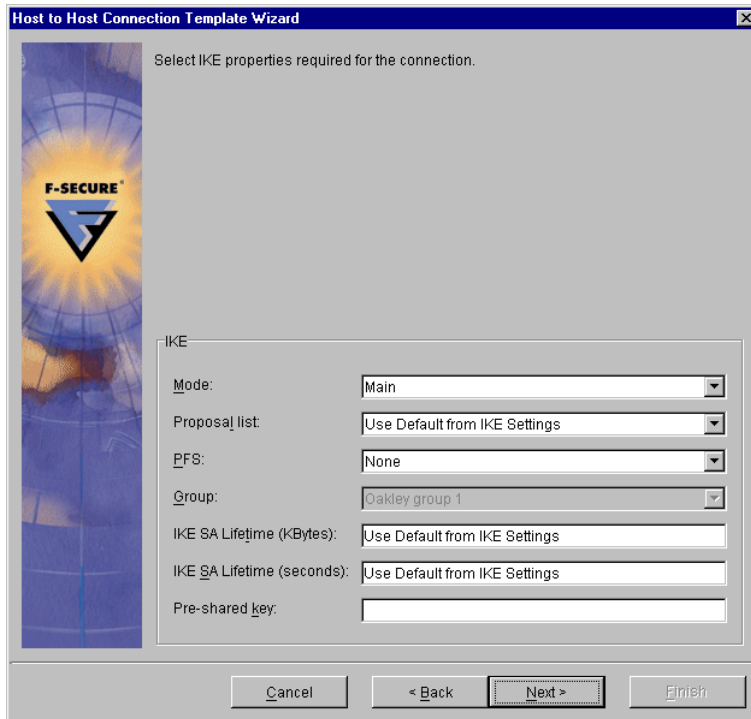


Select a connection type of “IPSec” and click *Next*.

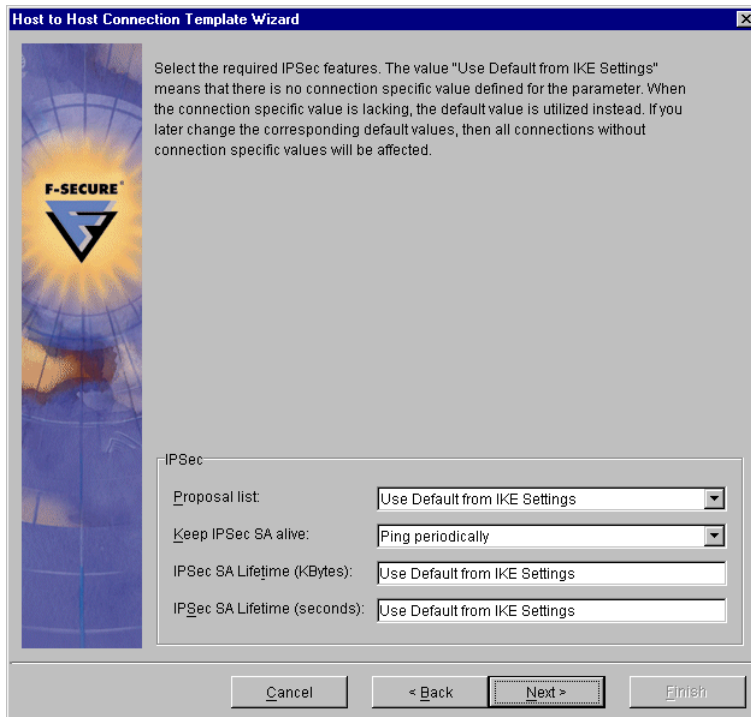


Select the desired host endpoint for the host-to-gateway connection. This endpoint can be a single host or a security domain (group of hosts.) On this screen it is also possible to configure the connection to use smart card authentication. If this is desired, check the “Smartcard authentication” checkbox and fill in the identifying fields for the allowed smart cards. When all required settings are filled, click *Next*.

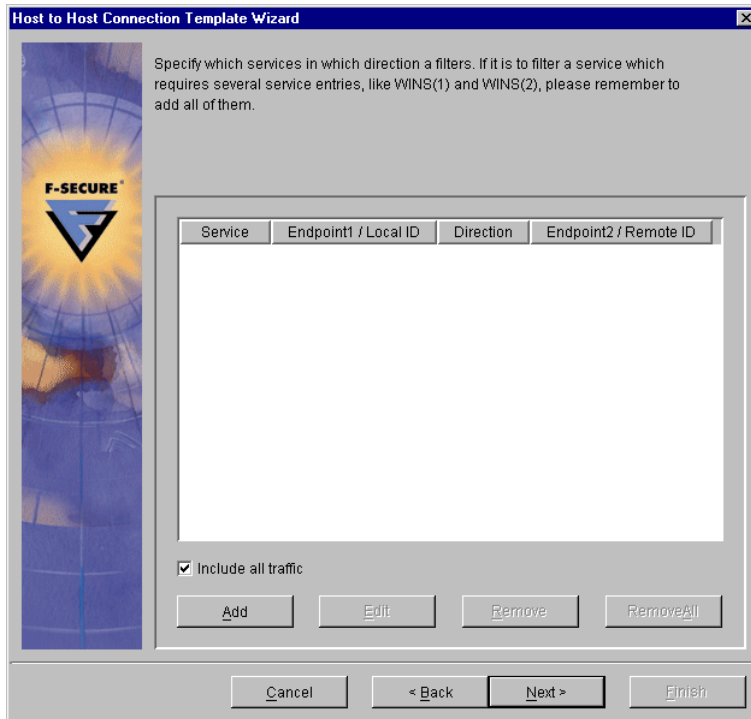
Note: If “Smartcard authentication” is checked but no fields are filled, you must enter `sc[]` in the “Additional Fields” box for the connection to work.



Leave the IKE settings at the default values and click *Next*.

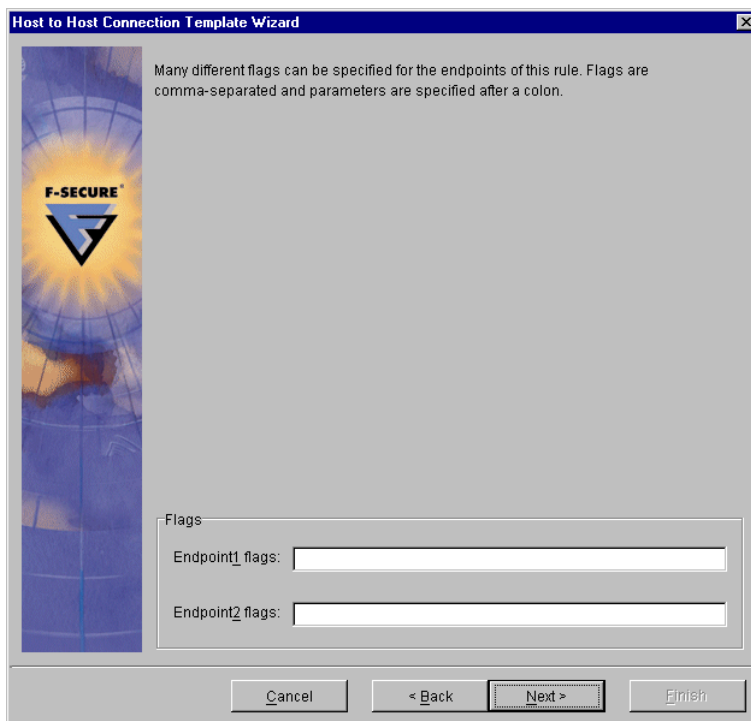


Leave the IPsec settings at the default values and click *Next*.

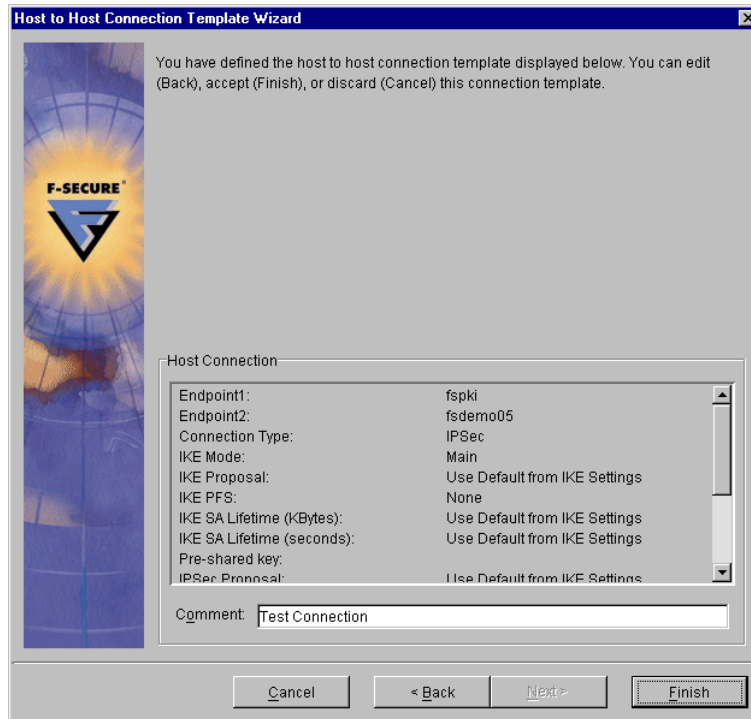


Leave the traffic filtering settings at the default of “Include all traffic” and click *Next*.

Note: Configured traffic filters are only used if F-Secure Distributed Firewall is also installed on the client computers.



Leave the endpoint flags empty and click *Next*.



Add a descriptive comment if desired and click *Finish*.

Distribute the updated policy by selecting *Distribute* from the *File* menu.

Once the VPN+ hosts have received the updated policy, test the connection you just created by “pinging” from the VPN+ client to a host on the other side of the gateway.

5.2 *Known Issues*

No known issues at this time.