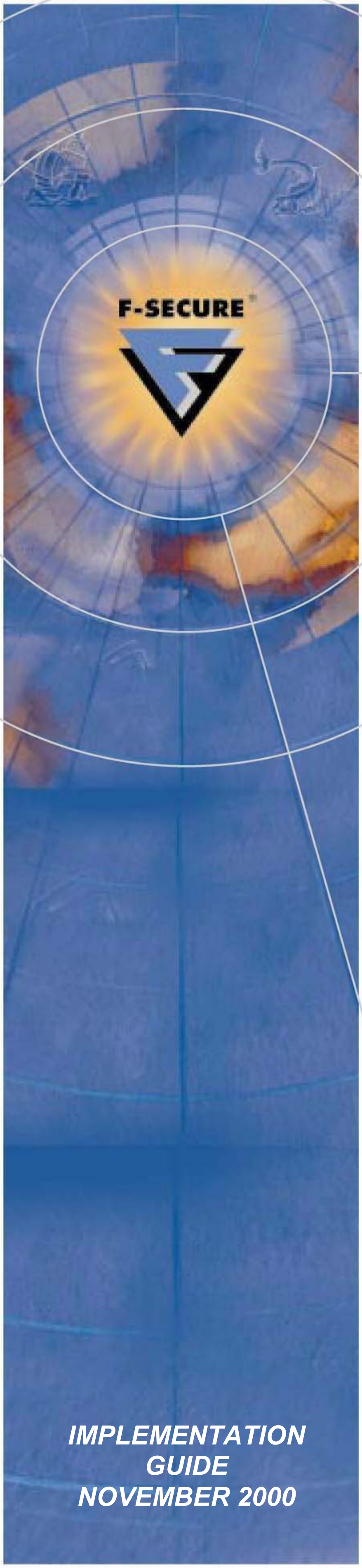


IMPLEMENTATION
GUIDE
NOVEMBER 2000

F-Secure VPN+:

PKI Integration with Windows 2000 Certificate Services

F-Secure Corporation

Securing the Mobile Distributed Enterprise

F-Secure VPN+: Integrating with Windows 2000 Certificate Services

Implementation Guide, November 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.

USA	***Europe***
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/	***F-Secure Corporation*** PL 24 FIN-02231 Espoo, Finland Tel +358 9 859 900 Fax +358 9 8599 0599 http://www.F-Secure.com/

Contents

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 fully with Microsoft Windows 2000 Certificate Services. This implementation guide will detail the necessary steps to configure and use F-Secure VPN+ with Microsoft Windows 2000 Certificate Services.

2 Requirements

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

- ❑ Microsoft Windows 2000 Server or Advanced Server
- ❑ Microsoft SCEP Add-in Module – from Windows 2000 Server Resource Kit
- ❑ Cryptographic Service Provider from smart card vendor (only required if using smart card support)

3 Assumptions

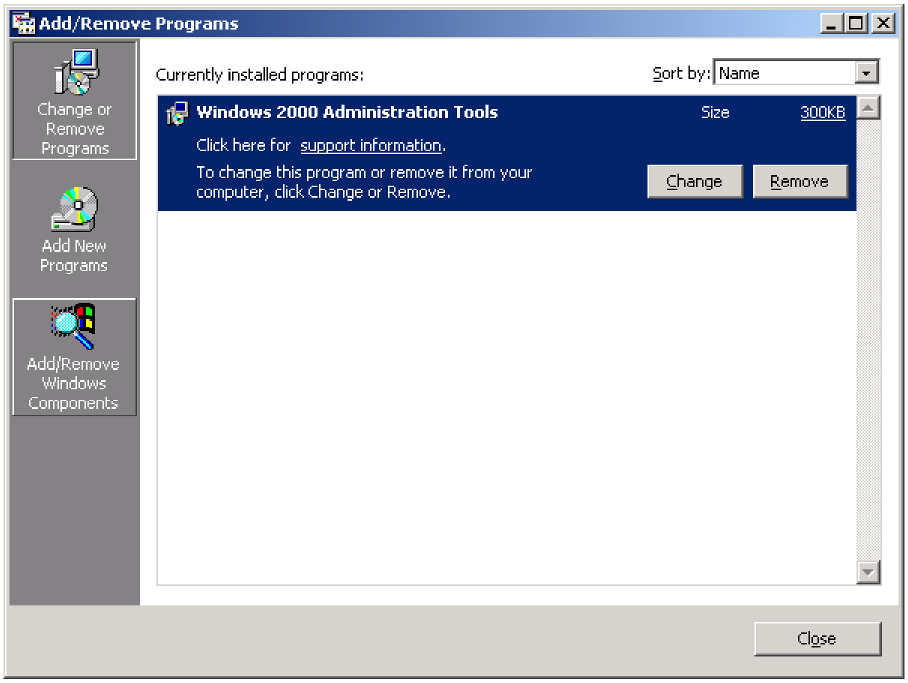
The following assumptions have been made for the purposes of this document. If these assumptions are not correct for your individual installation, some of the information contained in this document may be inapplicable or incorrect.

- ❑ **Windows 2000 Server has already been installed with Active Directory, Internet Information Server, and DNS Services configured.** These services need to be installed prior to installing Certificate Services.
- ❑ **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.
- ❑ **Certificate Services have not already been installed.**

4 Install the PKI System

4.1 Install Certificate Services

Start the Add/Remove Programs control panel (Start – Settings – Control Panel).



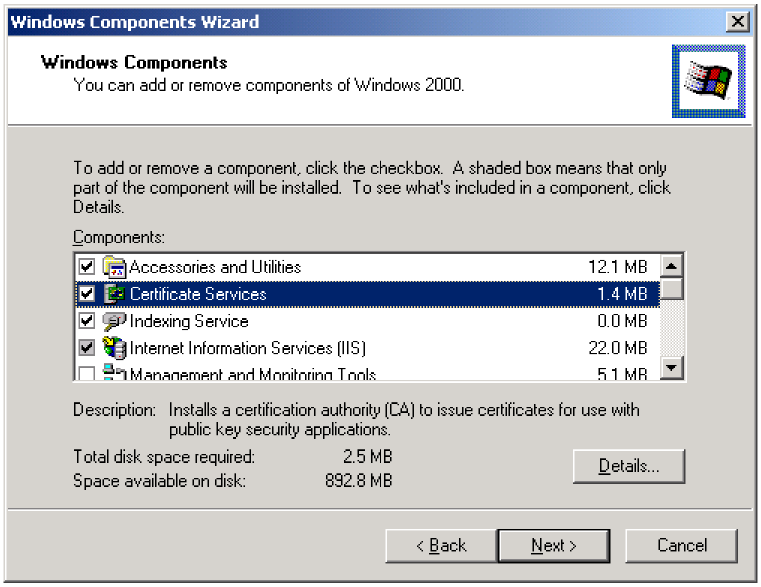
Currently installed programs:

Windows 2000 Administration Tools

Click here for support information.

To change this program or remove it from your computer, click Change or Remove.

Click on the “Add/Remove Windows Components” button.



Windows Components

You can add or remove components of Windows 2000.

To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Components:

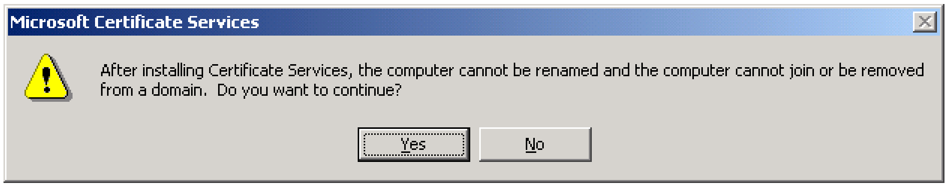
☑	Accessories and Utilities	12.1 MB
☑	Certificate Services	1.4 MB
☑	Indexing Service	0.0 MB
☑	Internet Information Services (IIS)	22.0 MB
□	Management and Monitoring Tools	5.1 MB

Description: Installs a certification authority (CA) to issue certificates for use with public key security applications.

Total disk space required: 2.5 MB

Space available on disk: 892.8 MB

Select the “Certificate Services” option.

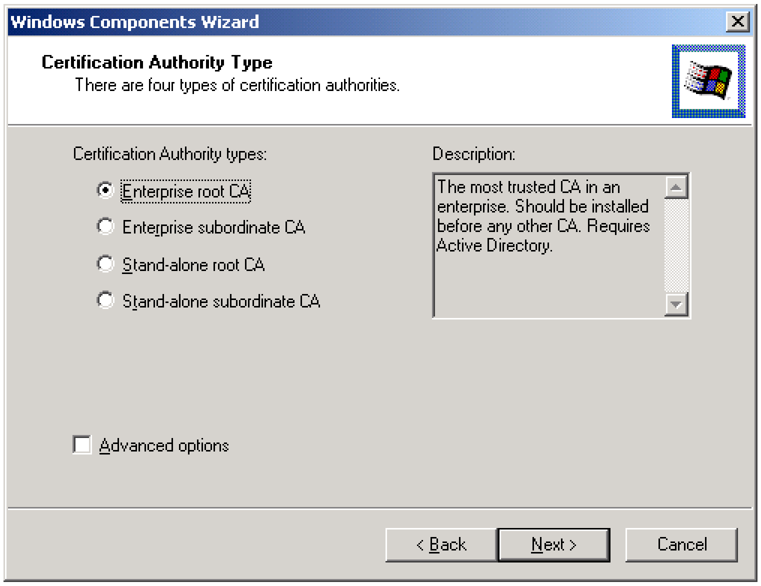


Microsoft Certificate Services

After installing Certificate Services, the computer cannot be renamed and the computer cannot join or be removed from a domain. Do you want to continue?

Click *Yes* to acknowledge that after installing Certificate Services the computer cannot be renamed or joined or removed from a domain.

Click *Next* to begin the installation of Certificate Services.



Windows Components Wizard

Certification Authority Type

There are four types of certification authorities.

Certification Authority types:

● Enterprise root CA

○ Enterprise subordinate CA

○ Stand-alone root CA

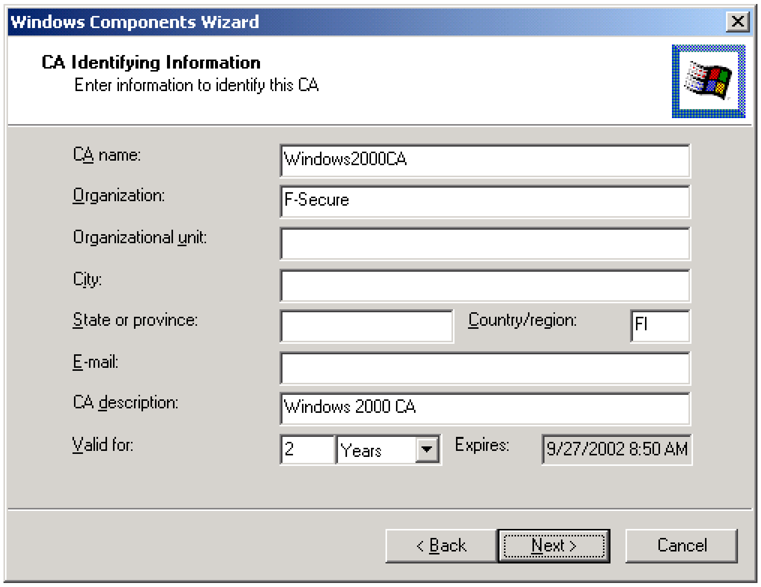
○ Stand-alone subordinate CA

Description:

The most trusted CA in an enterprise. Should be installed before any other CA. Requires Active Directory.

□ Advanced options

Select the type of Certificate Authority to install and click *Next*. In general, the "Enterprise root CA" should be used if the CA is being installed into a Windows 2000 domain environment and the issued smart cards will be used to authenticate users to Windows 2000 servers and workstations. In other cases a "Stand-alone root CA" will suffice.



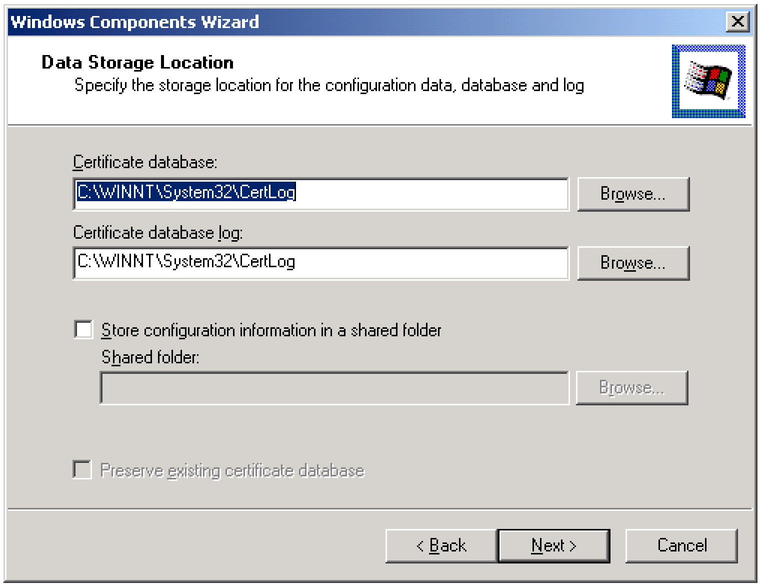
Windows Components Wizard

CA Identifying Information

Enter information to identify this CA

CA name:	Windows2000CA
Organization:	F-Secure
Organizational unit:	
City:	
State or province:	
Country/region:	FI
E-mail:	
CA description:	Windows 2000 CA
Valid for:	2 Years
Expires:	9/27/2002 8:50 AM

Enter the identifying information for the CA and click *Next*.



Windows Components Wizard

Data Storage Location

Specify the storage location for the configuration data, database and log

Certificate database: C:\WINNT\System32\CertLog

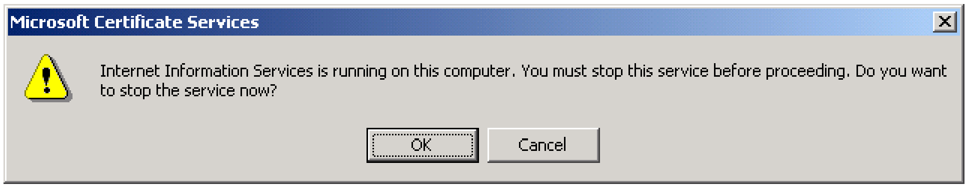
Certificate database log: C:\WINNT\System32\CertLog

□ Store configuration information in a shared folder

Shared folder:

□ Preserve existing certificate database

Accept the default data storage locations by clicking *Next*.

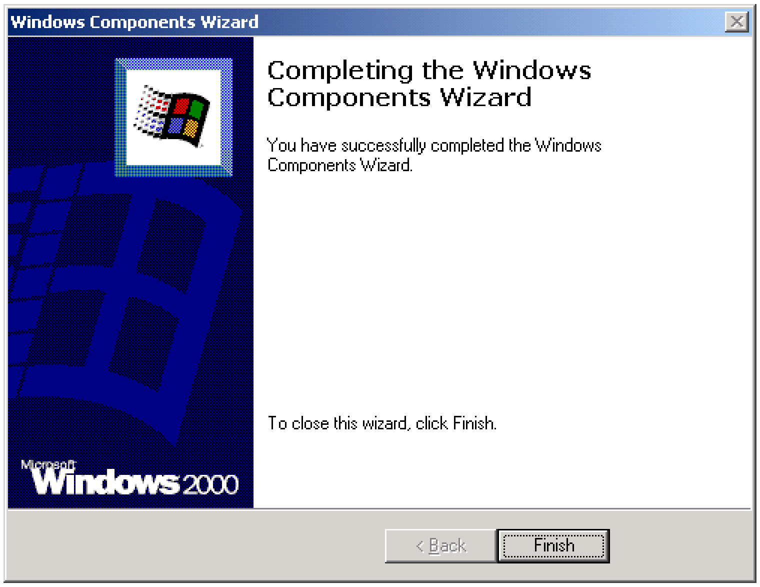


Microsoft Certificate Services

Internet Information Services is running on this computer. You must stop this service before proceeding. Do you want to stop the service now?

Click *Yes* to acknowledge that the Internet Information Services will be temporarily stopped during the installation.

Setup will now copy files and make the necessary configuration changes.



Completing the Windows Components Wizard

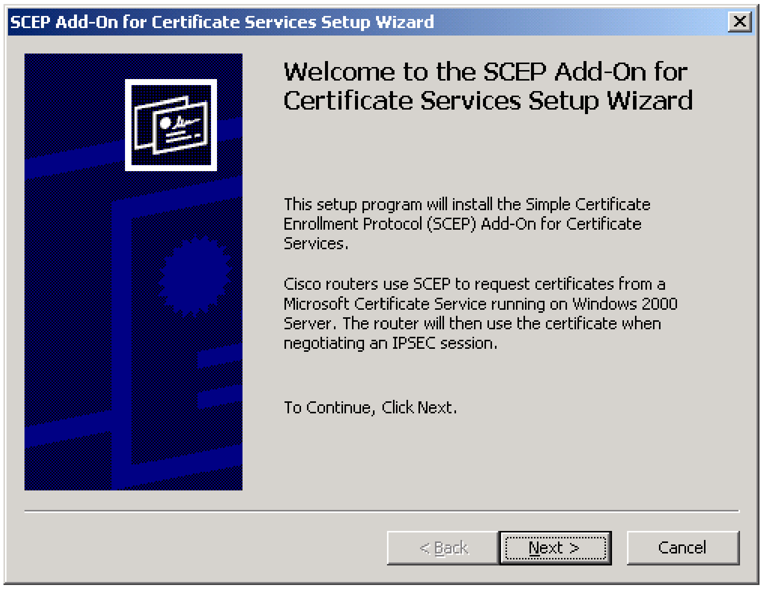
You have successfully completed the Windows Components Wizard.

To close this wizard, click Finish.

Click *Finish* to complete the installation.

4.2 Install SCEP Add-in Module

Run the cepsetup.exe application which is available from the Windows 2000 Server Resource Kit.



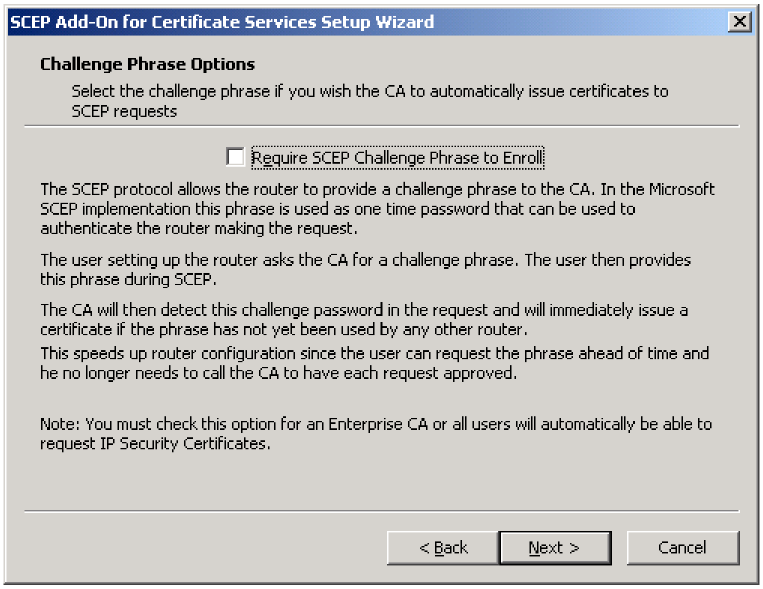
Welcome to the SCEP Add-On for Certificate Services Setup Wizard

This setup program will install the Simple Certificate Enrollment Protocol (SCEP) Add-On for Certificate Services.

Cisco routers use SCEP to request certificates from a Microsoft Certificate Service running on Windows 2000 Server. The router will then use the certificate when negotiating an IPSEC session.

To Continue, Click Next.

Click *Next* at the Welcome screen to begin the installation.



Challenge Phrase Options

Select the challenge phrase if you wish the CA to automatically issue certificates to SCEP requests

□ Require SCEP Challenge Phrase to Enroll

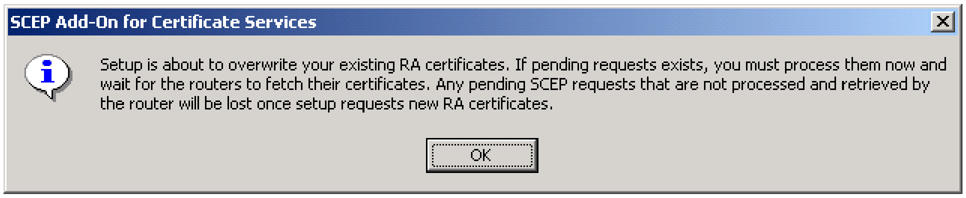
The SCEP protocol allows the router to provide a challenge phrase to the CA. In the Microsoft SCEP implementation this phrase is used as one time password that can be used to authenticate the router making the request.

The user setting up the router asks the CA for a challenge phrase. The user then provides this phrase during SCEP.

The CA will then detect this challenge password in the request and will immediately issue a certificate if the phrase has not yet been used by any other router.
This speeds up router configuration since the user can request the phrase ahead of time and he no longer needs to call the CA to have each request approved.

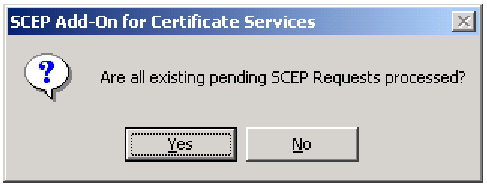
Note: You must check this option for an Enterprise CA or all users will automatically be able to request IP Security Certificates.

Deselect the checkbox to not “Require SCEP Challenge Phrase to Enroll” and click *Next*.



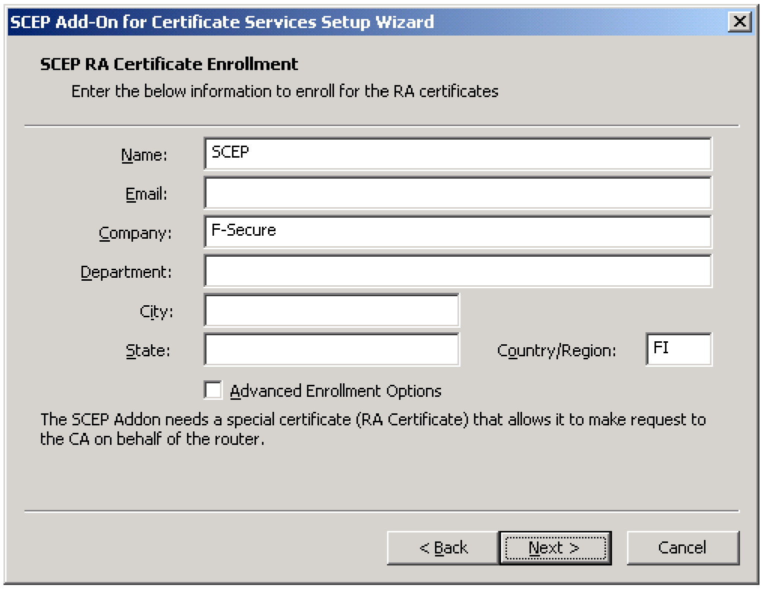
Setup is about to overwrite your existing RA certificates. If pending requests exists, you must process them now and wait for the routers to fetch their certificates. Any pending SCEP requests that are not processed and retrieved by the router will be lost once setup requests new RA certificates.

Click *OK* to acknowledge that existing RA certificates will be overwritten and pending requests will have to be resent.



Are all existing pending SCEP Requests processed?

Click *Yes* to confirm that all existing pending SCEP requests have been processed.



SCEP Add-On for Certificate Services Setup Wizard

SCEP RA Certificate Enrollment

Enter the below information to enroll for the RA certificates

Name: SCEP

Email:

Company: F-Secure

Department:

City:

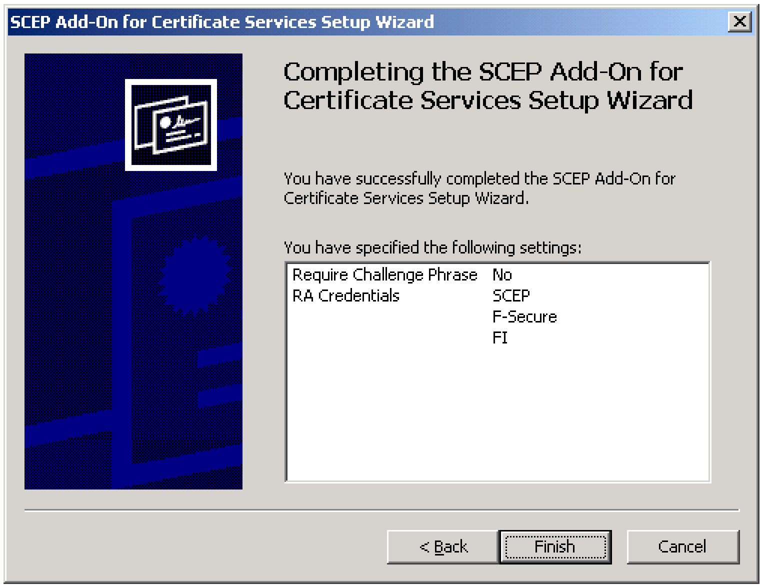
State:

Country/Region: FI

□ Advanced Enrollment Options

The SCEP Addon needs a special certificate (RA Certificate) that allows it to make request to the CA on behalf of the router.

Enter the desired identifying information for the SCEP RA certificate and click *Next*.



SCEP Add-On for Certificate Services Setup Wizard

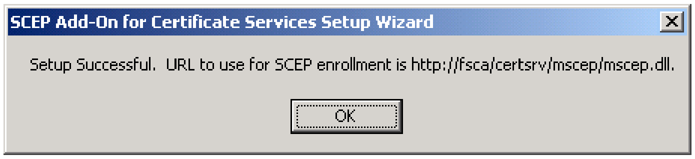
Completing the SCEP Add-On for Certificate Services Setup Wizard

You have successfully completed the SCEP Add-On for Certificate Services Setup Wizard.

You have specified the following settings:

```
Require Challenge Phrase   No
RA Credentials             SCEP
                           F-Secure
                           FI
```

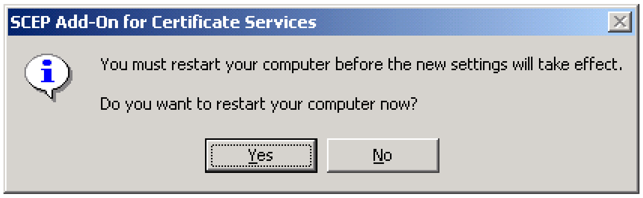
Click *Finish* to begin copying files and complete setup.



SCEP Add-On for Certificate Services Setup Wizard

Setup Successful. URL to use for SCEP enrollment is http://fsca/certsrv/mscep/mscep.dll.

Click *OK* to acknowledge that setup was successful.



You must restart your computer before the new settings will take effect.

Do you want to restart your computer now?

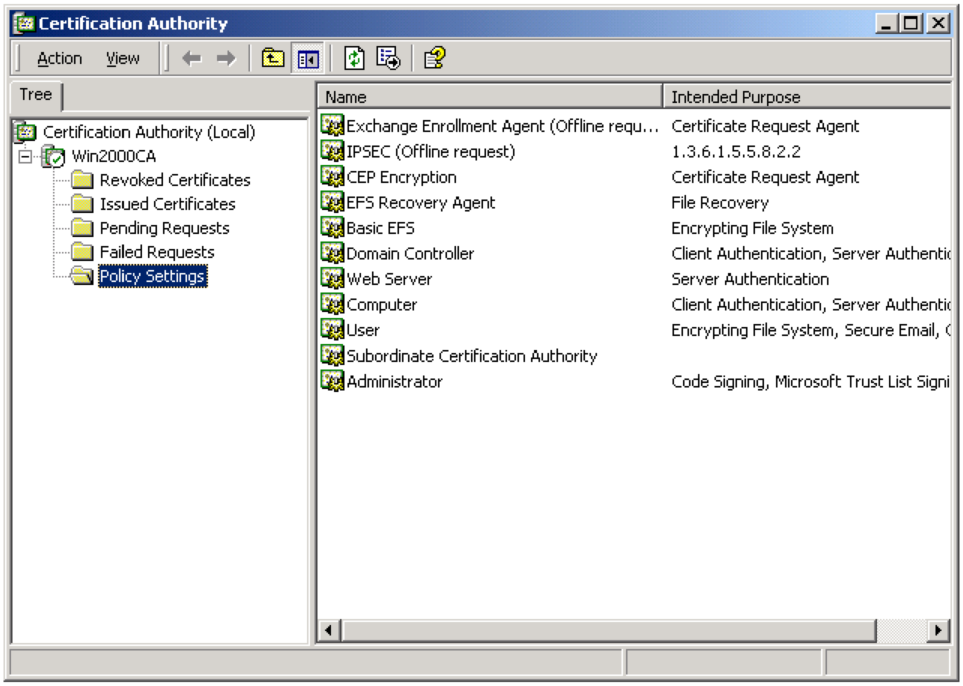
Click *Yes* to restart computer.

4.3 *Configure Smart Card Enrollment Settings (optional)*

Note: The steps in this section are only necessary if the issued smart cards are to be used for user logon to Windows 2000 computers. In order to support this, the CA must be installed as an Enterprise CA.

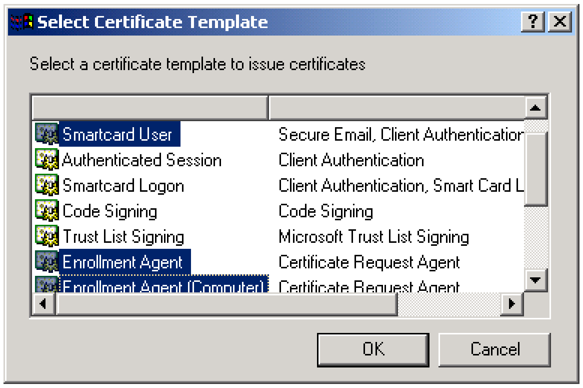
4.3.1 Configure Certificate Templates

Start the Certification Authority management console (Start – Programs – Administrative Tools.)



Name	Intended Purpose
Exchange Enrollment Agent (Offline requ…	Certificate Request Agent
IPSEC (Offline request)	1.3.6.1.5.5.8.2.2
CEP Encryption	Certificate Request Agent
EFS Recovery Agent	File Recovery
Basic EFS	Encrypting File System
Domain Controller	Client Authentication, Server Authentic
Web Server	Server Authentication
Computer	Client Authentication, Server Authentic
User	Encrypting File System, Secure Email, C
Subordinate Certification Authority	
Administrator	Code Signing, Microsoft Trust List Signi

Right-click on the “Policy Settings” folder and select New ▸ Certificate to Issue…



Select a certificate template to issue certificates

Smartcard User	Secure Email, Client Authenticatior
Authenticated Session	Client Authentication
Smartcard Logon	Client Authentication, Smart Card L
Code Signing	Code Signing
Trust List Signing	Microsoft Trust List Signing
Enrollment Agent	Certificate Request Agent
Enrollment Agent (Computer)	Certificate Request Agent

From the list of templates, click the following items (hold Ctrl key to select multiple items):

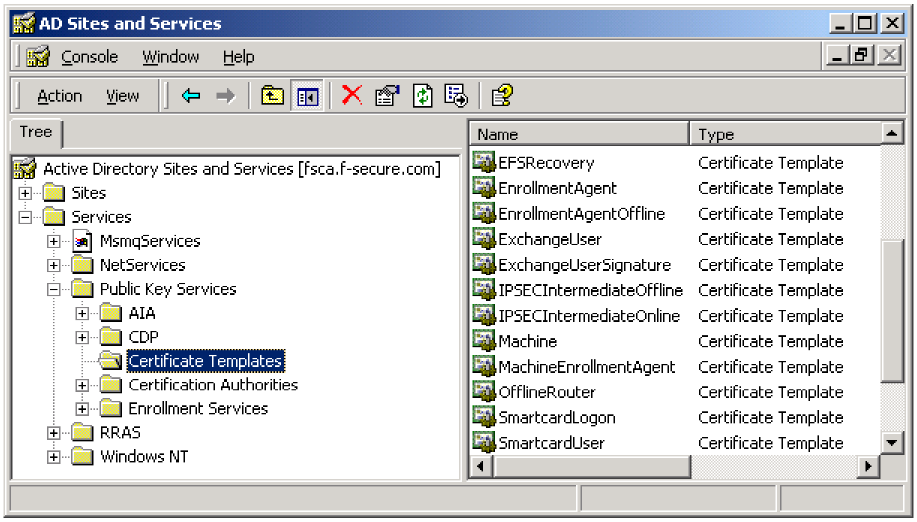
- Enrollment Agent (Computer)
- Enrollment Agent
- Smartcard User

Click *OK*. The CA has now been configured to issue certificates using the new templates.

4.3.2 Set Permissions on Certificate Templates

Certificates issued by the CA are based on certificate templates stored in the Active Directory. The Access Control Lists (ACLs) set on these templates dictate which user and machine accounts can request which certificates. To configure the ACLs on the templates added in the previous step, follow the instructions below:

Start the "Active Directory Sites and Services" management console (Start – Programs – Administrative Tools.)



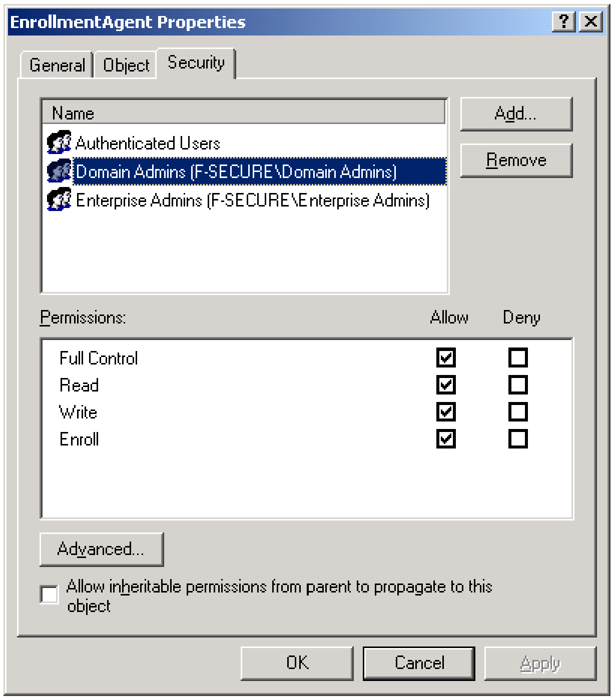
- Active Directory Sites and Services [fsca.f-secure.com]
  - Sites
  - Services
    - MsmqServices
    - NetServices
    - Public Key Services
      - AIA
      - CDP
      - Certificate Templates
      - Certification Authorities
      - Enrollment Services
    - RRAS
    - Windows NT

Name	Type
EFSRecovery	Certificate Template
EnrollmentAgent	Certificate Template
EnrollmentAgentOffline	Certificate Template
ExchangeUser	Certificate Template
ExchangeUserSignature	Certificate Template
IPSECIntermediateOffline	Certificate Template
IPSECIntermediateOnline	Certificate Template
Machine	Certificate Template
MachineEnrollmentAgent	Certificate Template
OfflineRouter	Certificate Template
SmartcardLogon	Certificate Template
SmartcardUser	Certificate Template

If the Services node is not visible, click “Show Services Node” on the View menu.

Expand the tree Services/Public Key Services/Certificate Templates.

Right-click the EnrollmentAgent template and select Properties.



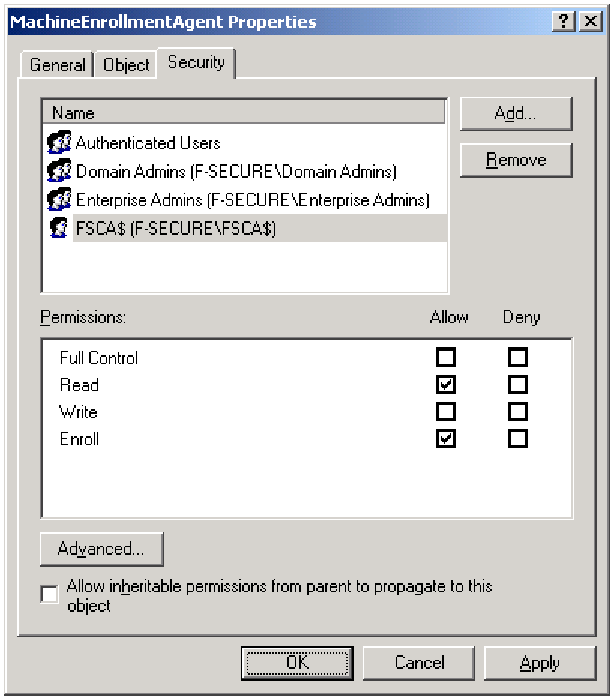
Name
- Authenticated Users
- Domain Admins (F-SECURE\Domain Admins)
- Enterprise Admins (F-SECURE\Enterprise Admins)

Permissions:	Allow	Deny
Full Control	☑	□
Read	☑	□
Write	☑	□
Enroll	☑	□

□ Allow inheritable permissions from parent to propagate to this object

On the Security tab make sure that the user or group of users who should be able to create the smart cards (enrolment agents) have Read and Enroll permissions then click *OK*.

Right-click the MachineEnrollmentAgent template and select Properties.



Name

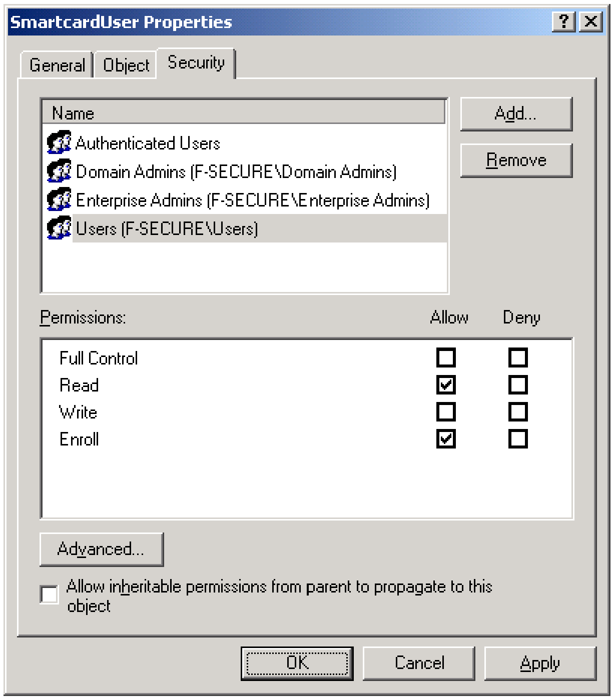
- Authenticated Users
- Domain Admins (F-SECURE\Domain Admins)
- Enterprise Admins (F-SECURE\Enterprise Admins)
- FSCA$ (F-SECURE\FSCA$)

Permissions:	Allow	Deny
Full Control	□	□
Read	☑	□
Write	□	□
Enroll	☑	□

□ Allow inheritable permissions from parent to propagate to this object

On the Security tab make sure that the computer from which the smart cards will be created (enrolment station) has Read and Enroll permissions then click *OK*.

Right-click the SmartcardUser template and select Properties.



Name

- Authenticated Users
- Domain Admins (F-SECURE\Domain Admins)
- Enterprise Admins (F-SECURE\Enterprise Admins)
- Users (F-SECURE\Users)

Permissions:	Allow	Deny
Full Control	□	□
Read	☑	□
Write	□	□
Enroll	☑	□

□ Allow inheritable permissions from parent to propagate to this object

On the Security tab make sure that the user or group of users who should be able to use smart cards to log onto Windows 2000 computers have Read and Enroll permissions on the template then click *OK*.

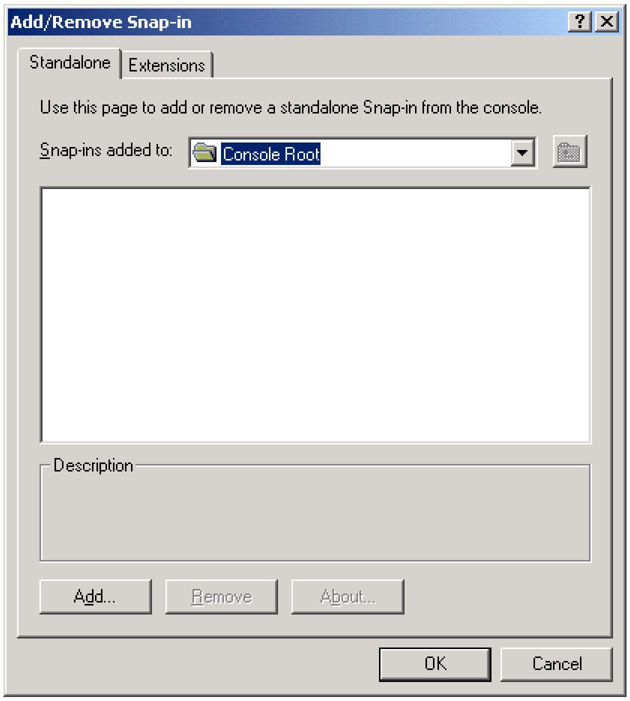
The access permissions for the new templates are now set correctly for smart card enrollment.

4.3.3 Configure Enrollment Station Account

have an enrollment station certificate. The following steps describe how to obtain this certificate:

Log onto the enrollment station as with administrative rights.

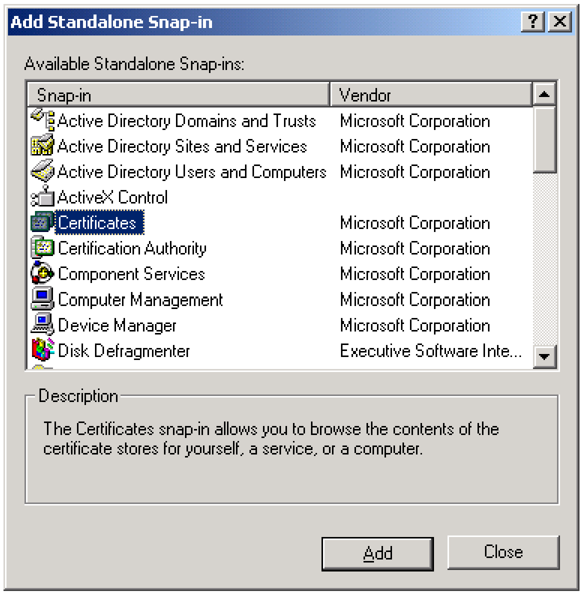
Start the Microsoft Management Console (Start – Run… mmc.exe).



Use this page to add or remove a standalone Snap-in from the console.

Snap-ins added to: Console Root

Select "Add/Remove Snap-in" from the Console menu and then click the *Add* button.


Add Standalone Snap-in

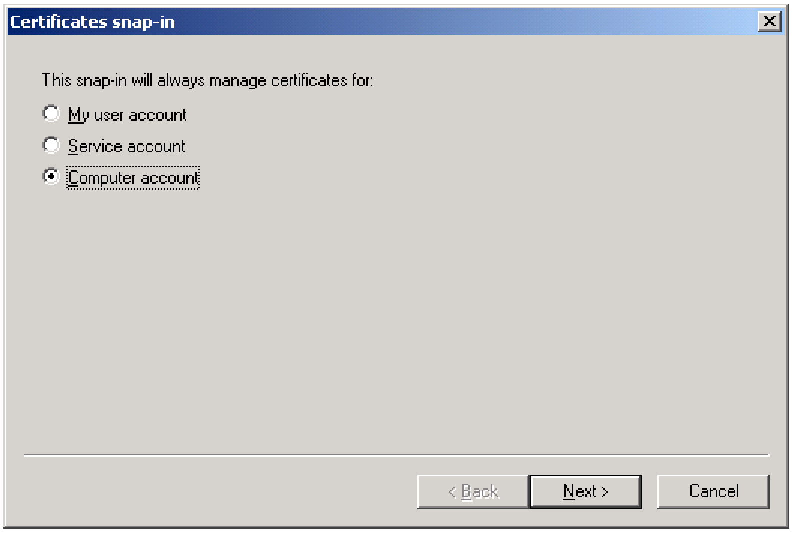
Available Standalone Snap-ins:

Snap-in	Vendor
Active Directory Domains and Trusts	Microsoft Corporation
Active Directory Sites and Services	Microsoft Corporation
Active Directory Users and Computers	Microsoft Corporation
ActiveX Control	
Certificates	Microsoft Corporation
Certification Authority	Microsoft Corporation
Component Services	Microsoft Corporation
Computer Management	Microsoft Corporation
Device Manager	Microsoft Corporation
Disk Defragmenter	Executive Software Inte...

Description

The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

From the list of available snap-ins select “Certificates” and click *Add*.


Certificates snap-in

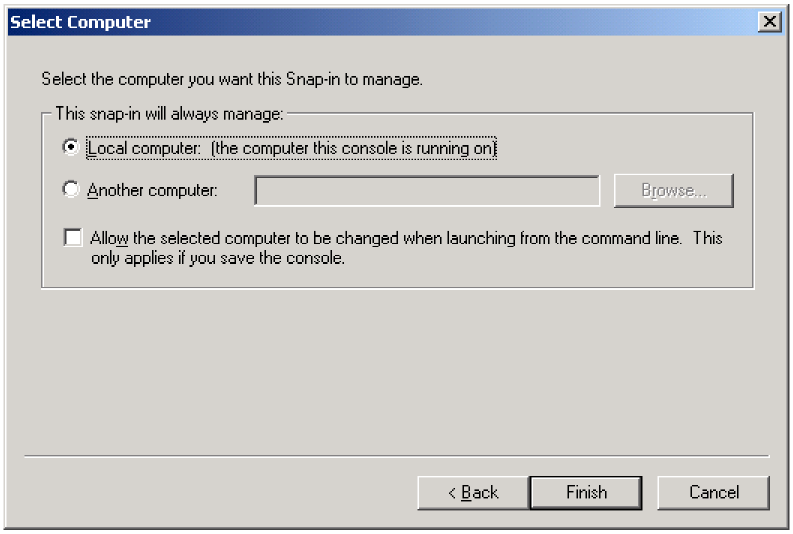
This snap-in will always manage certificates for:

○ My user account

○ Service account

● Computer account

Select the option to manage certificates for the “Computer Account” and click *Next*.



Select Computer

Select the computer you want this Snap-in to manage.

This snap-in will always manage:

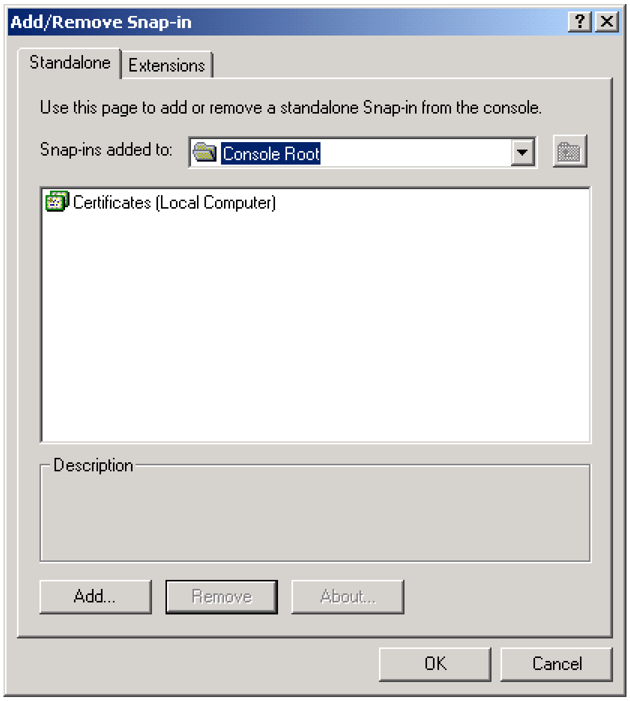
● Local computer: (the computer this console is running on)

○ Another computer:

□ Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.

Select the option to manage the local computer and click *Finish*.

Click *Close* from the list of available snap-ins.



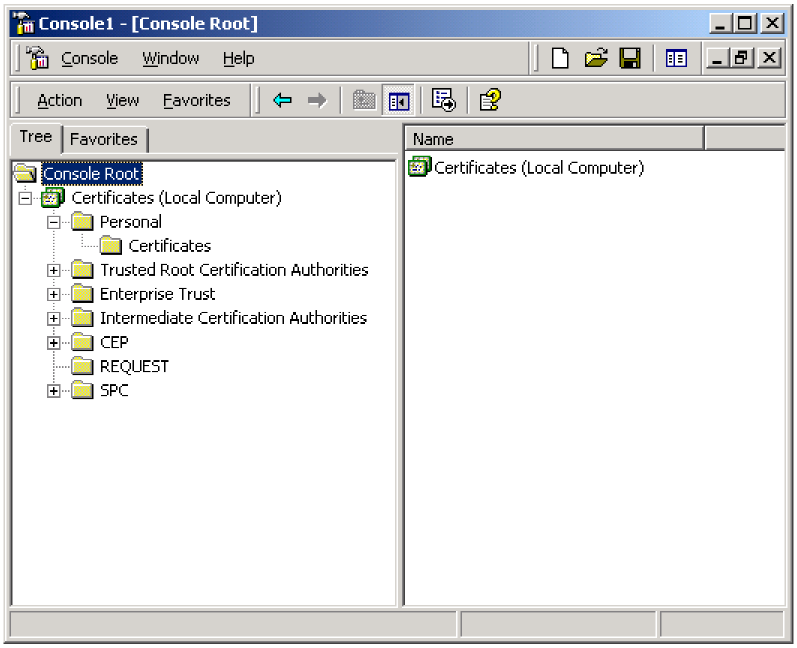
Add/Remove Snap-in

Use this page to add or remove a standalone Snap-in from the console.

Snap-ins added to: Console Root

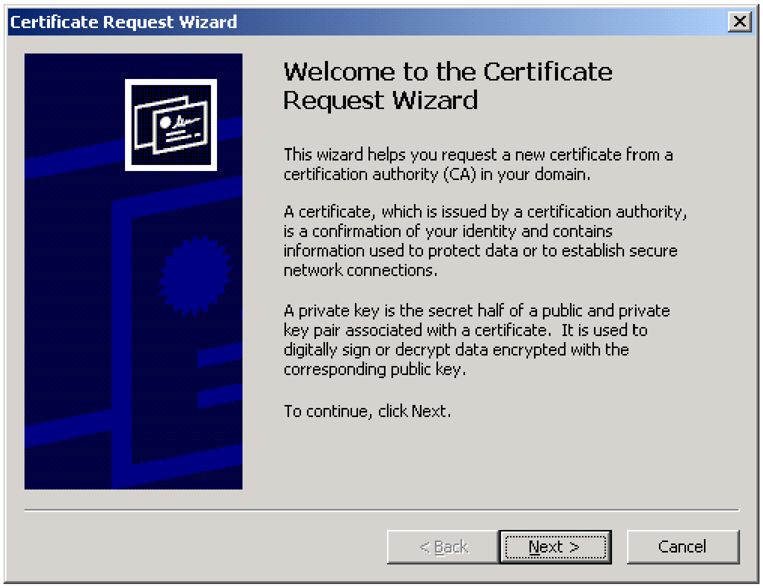
Certificates (Local Computer)

Click *OK* from the “Add/Remove Snap-in” window.


Console1 - [Console Root]
Console
Window
Help
Action
View
Favorites
Tree
Favorites
Name
Console Root
Certificates (Local Computer)
Personal
Certificates
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
CEP
REQUEST
SPC
Certificates (Local Computer)

Expand the tree Console Root/Certificates (Local Computer)/Personal/Certificates.

Right-click on the "Certificates" folder and select All Tasks ▶ Request New Certificate…



Welcome to the Certificate Request Wizard

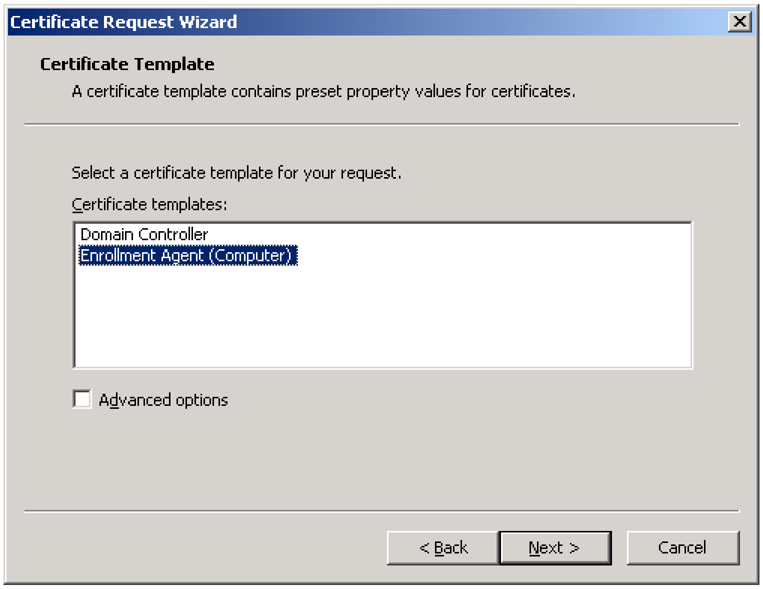
This wizard helps you request a new certificate from a certification authority (CA) in your domain.

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 private key is the secret half of a public and private key pair associated with a certificate. It is used to digitally sign or decrypt data encrypted with the corresponding public key.

To continue, click Next.

The Certificate Request Wizard will start. Click *Next* at the Welcome screen.


Certificate Request Wizard

Certificate Template

A certificate template contains preset property values for certificates.

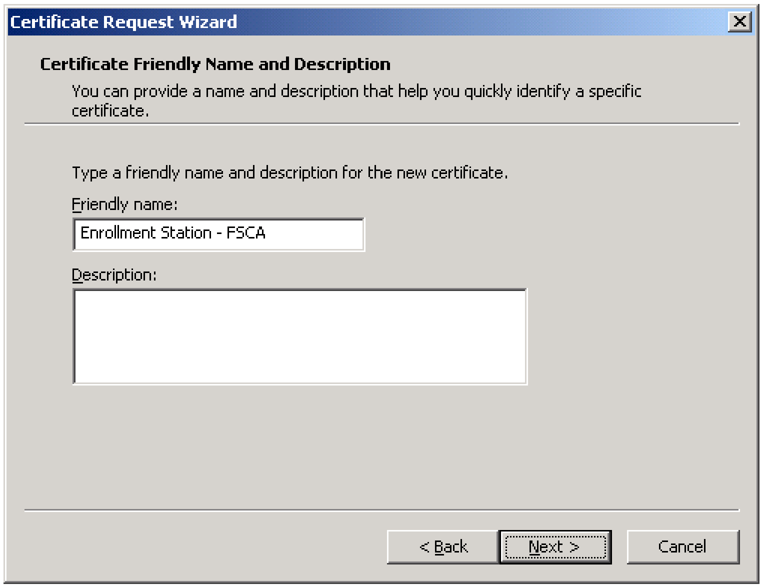
Select a certificate template for your request.

Certificate templates:

Domain Controller
Enrollment Agent (Computer)

□ Advanced options

Select the “Enrollment Agent (Computer)” certificate template and click *Next*.


Certificate Request Wizard

Certificate Friendly Name and Description

You can provide a name and description that help you quickly identify a specific certificate.

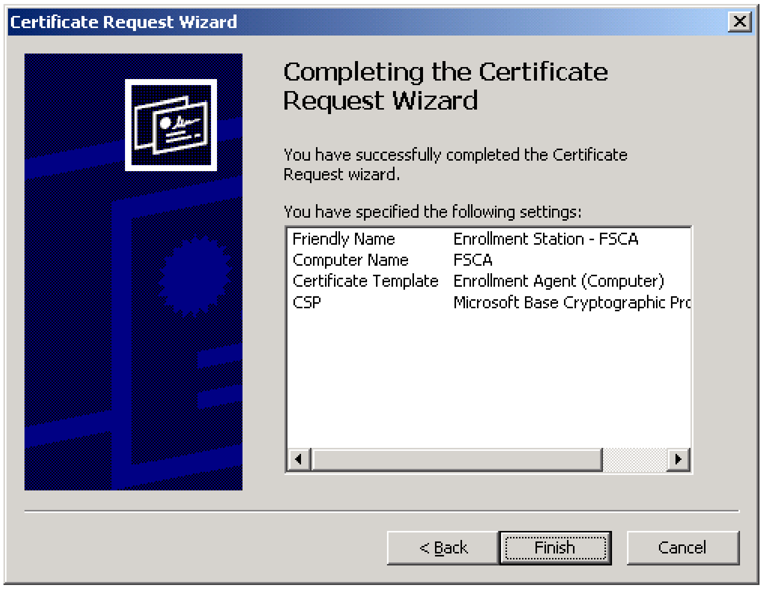
Type a friendly name and description for the new certificate.

Friendly name:

Enrollment Station - FSCA

Description:

Enter a “Friendly Name” to identify the certificate and click *Next*.



Certificate Request Wizard

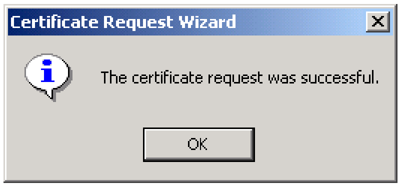
Completing the Certificate Request Wizard

You have successfully completed the Certificate Request wizard.

You have specified the following settings:

Friendly Name	Enrollment Station - FSCA
Computer Name	FSCA
Certificate Template	Enrollment Agent (Computer)
CSP	Microsoft Base Cryptographic Prc

Click *Finish* to generate the certificate.



Certificate Request Wizard

The certificate request was successful.

Click *OK* to acknowledge that the certificate request was successful.

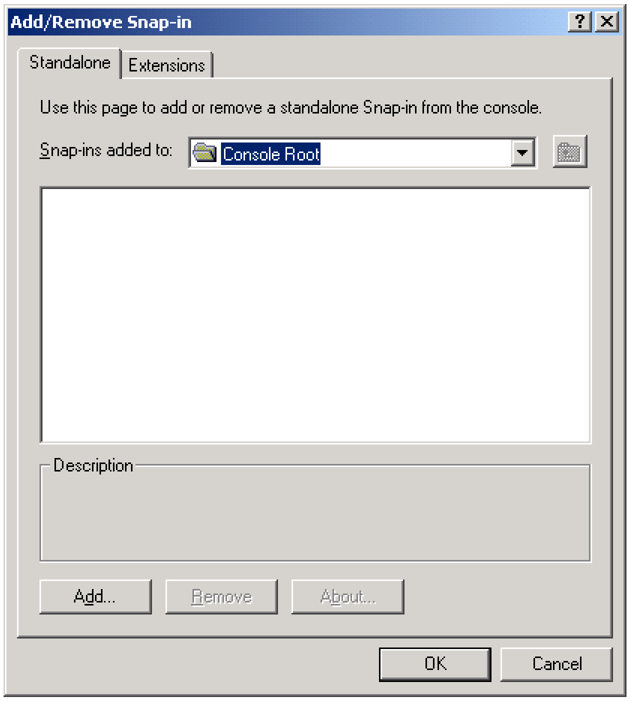
The enrollment station is now certified to enroll for smart card certificates.

4.3.4 Configure Enrollment Agent Account

In order to issue certificates to a smart card the user performing the enrollment must have an enrollment agent certificate. The following steps describe how to obtain this certificate:

Log onto the enrollment station as the user who will be enrolling the smart cards.

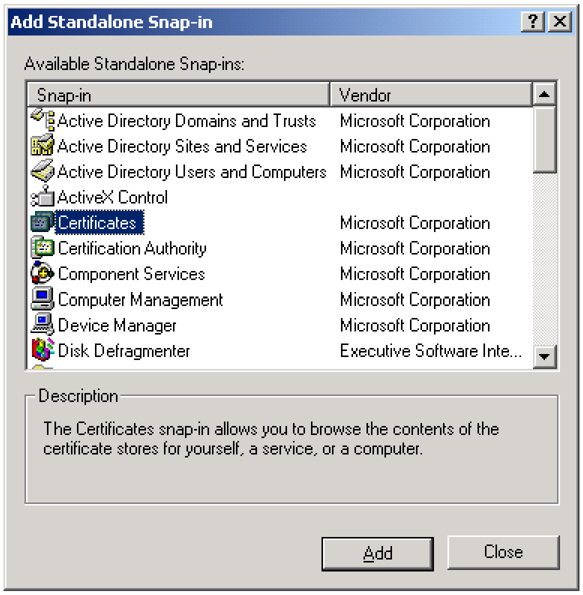
Start the Microsoft Management Console (Start – Run… mmc.exe).



Use this page to add or remove a standalone Snap-in from the console.

Snap-ins added to: Console Root

Select “Add/Remove Snap-in” from the Console menu and then click the *Add* button.

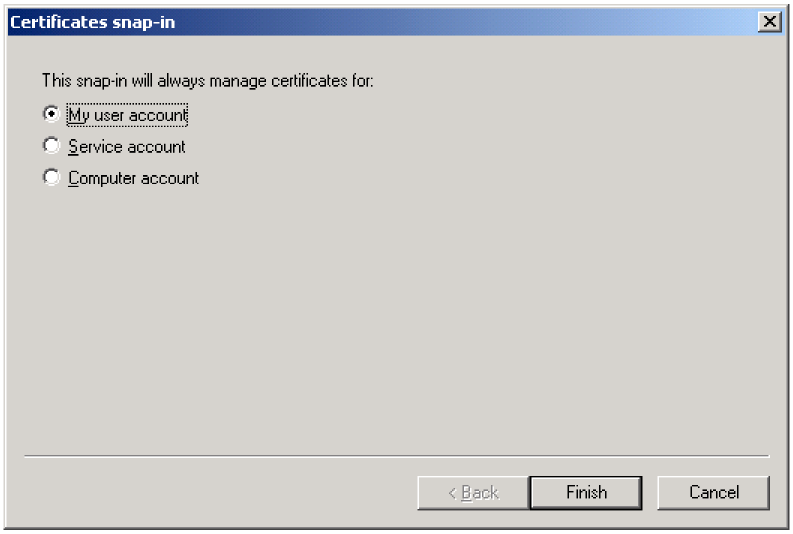


Available Standalone Snap-ins:

Snap-in	Vendor
Active Directory Domains and Trusts	Microsoft Corporation
Active Directory Sites and Services	Microsoft Corporation
Active Directory Users and Computers	Microsoft Corporation
ActiveX Control	
Certificates	Microsoft Corporation
Certification Authority	Microsoft Corporation
Component Services	Microsoft Corporation
Computer Management	Microsoft Corporation
Device Manager	Microsoft Corporation
Disk Defragmenter	Executive Software Inte...

The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

From the list of available snap-ins select “Certificates” and click *Add*.

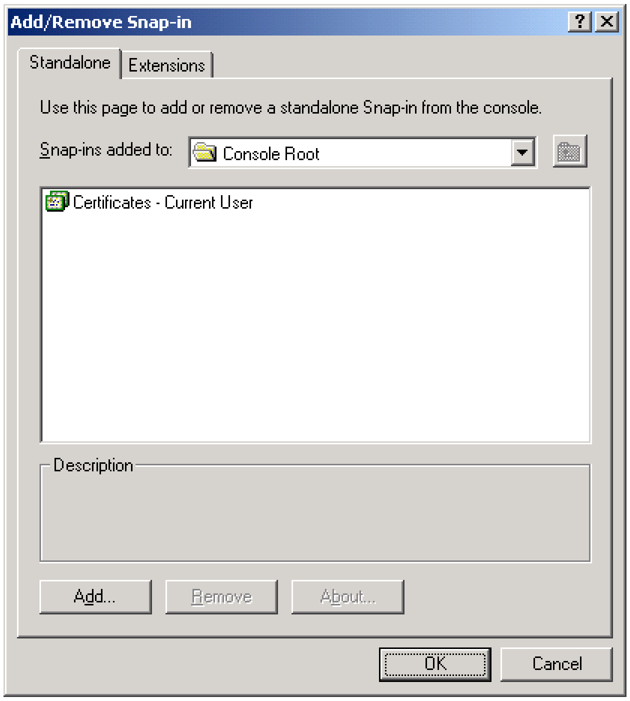


This snap-in will always manage certificates for:

● My user account
○ Service account
○ Computer account

Select the option to manage certificates for “My user account” and click *Finish*.

Click *Close* from the list of available snap-ins.

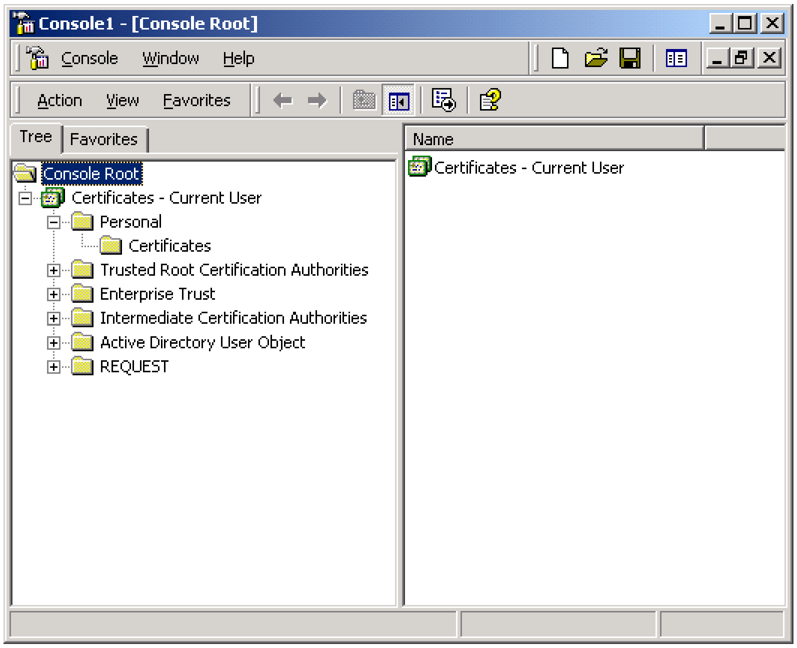


Use this page to add or remove a standalone Snap-in from the console.

Snap-ins added to: Console Root

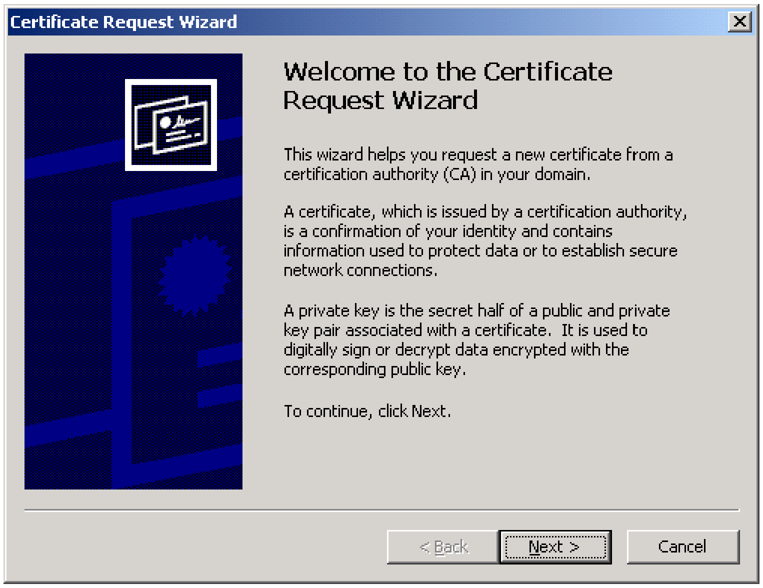
Certificates - Current User

Click *OK* from the “Add/Remove Snap-in” window.


Console1 - [Console Root]
Console
Window
Help
Action
View
Favorites
Tree
Favorites
Console Root
Certificates - Current User
Personal
Certificates
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Active Directory User Object
REQUEST
Name
Certificates - Current User

Expand the tree Console Root/Certificates – Current User/Personal/Certificates.

Right-click on the “Certificates” folder and select All Tasks ▶ Request New Certificate…



Welcome to the Certificate Request Wizard

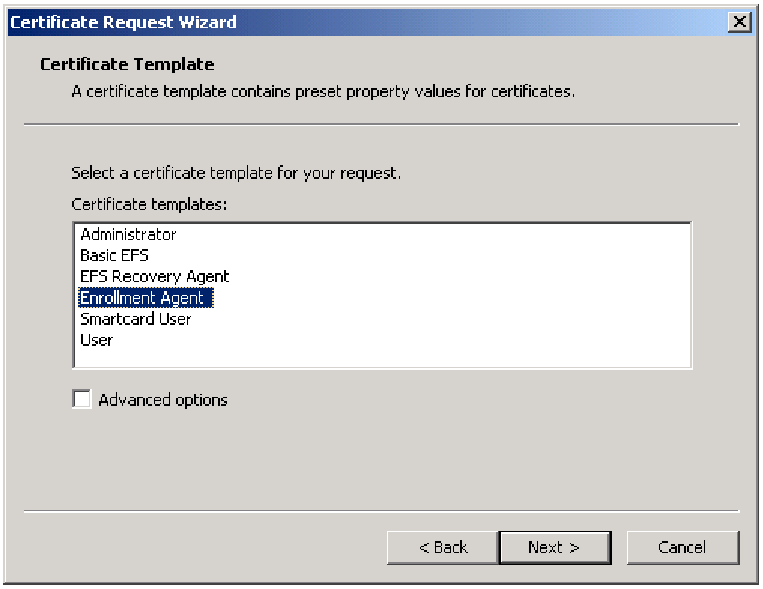
This wizard helps you request a new certificate from a certification authority (CA) in your domain.

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 private key is the secret half of a public and private key pair associated with a certificate. It is used to digitally sign or decrypt data encrypted with the corresponding public key.

To continue, click Next.

The Certificate Request Wizard will start. Click *Next* at the Welcome screen.



Certificate Template

A certificate template contains preset property values for certificates.

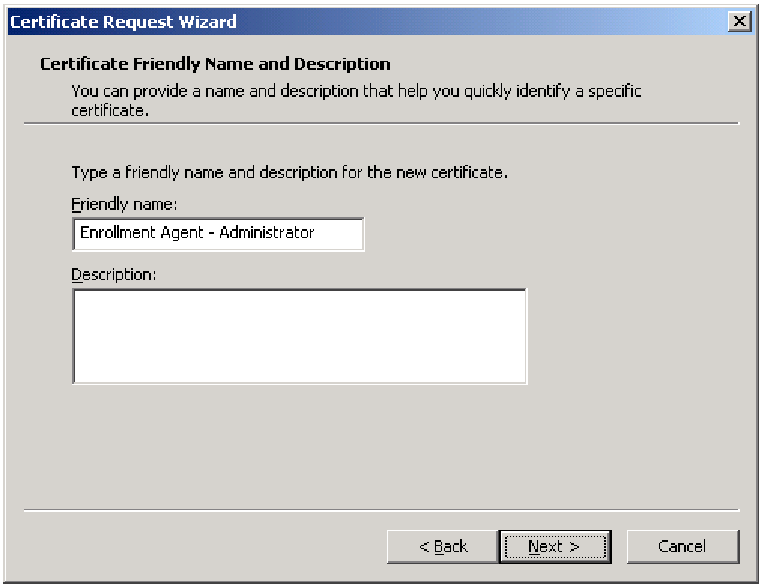
Select a certificate template for your request.

Certificate templates:

- Administrator
- Basic EFS
- EFS Recovery Agent
- Enrollment Agent
- Smartcard User
- User

□ Advanced options

Select the "Enrollment Agent" certificate template and click *Next*.



Certificate Friendly Name and Description

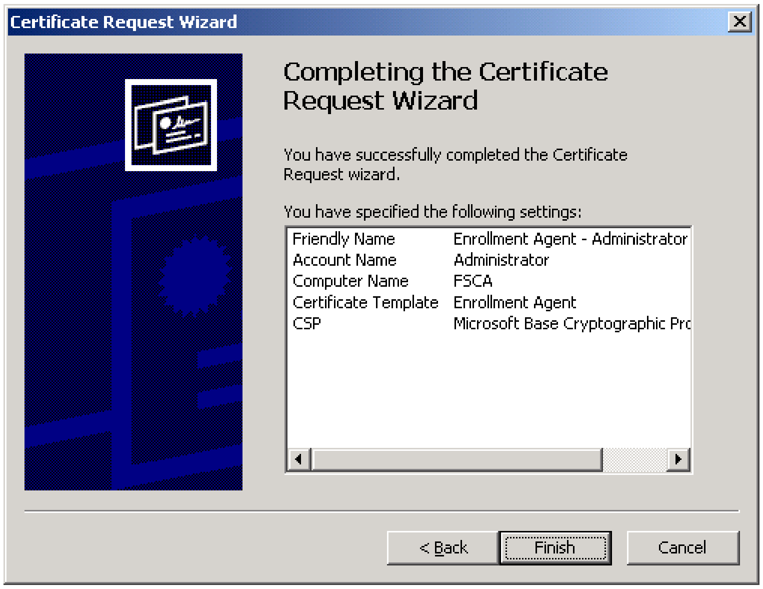
You can provide a name and description that help you quickly identify a specific certificate.

Type a friendly name and description for the new certificate.

Friendly name: Enrollment Agent - Administrator

Description:

Enter a "Friendly name" to identify the certificate and click *Next*.



Certificate Request Wizard

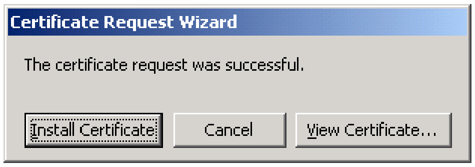
Completing the Certificate Request Wizard

You have successfully completed the Certificate Request wizard.

You have specified the following settings:

Friendly Name	Enrollment Agent - Administrator
Account Name	Administrator
Computer Name	FSCA
Certificate Template	Enrollment Agent
CSP	Microsoft Base Cryptographic Prc

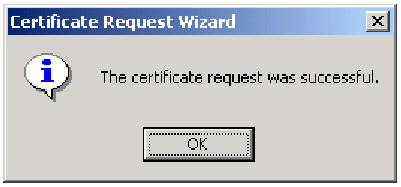
Click *Finish* to generate the certificate.



Certificate Request Wizard

The certificate request was successful.

When prompted, click *Install Certificate*.



Certificate Request Wizard

The certificate request was successful.

Click *OK* to acknowledge that the certificate request was successful.

The user account is now certified to enroll for smart card certificates on behalf of other users.

5 Enroll for Smart Card Certificate

5.1 Pre-personalize Smart Card

In order to issue certificates to a smart card with Windows 2000 Certificate Services the cards must be pre-personalized. This process involves creating the file structure on the card. The process for doing this will vary from card to card so it is not discussed in detail here.

If Schlumberger Cryptoflex for Windows 2000 or GemPlus GemSAFE cards are being used, no pre-personalization of the cards is required.

5.2 Enroll for Certificate

Note: Enrolling for a smart card certificate must be done from a Windows 2000 Professional or Server computer.

5.2.1 Stand-Alone CA

Launch a web browser and browse to "http://<ca server>/certsrv."

Select "Request a certificate" and click the *Next* button.

Select the "Advanced request" option and click the *Next* button.

Select "Submit a certificate request to this CA using a form" and click *Next*.

Fill in the certificate request form with the appropriate user information.

Select an "Intended Purpose" of "Client Authentication Certificate."

Select the correct "CSP" for the type of smart card to be issued (this will vary from vendor to vendor).

Check the "Enable strong private key protection" checkbox.

Click *Enroll*.

Enter the PIN for the smart card when prompted.

The certificate request has now been sent to the Certificate Authority. To issue the certificate, log onto the CA server (if you aren't already) and start the Certification Authority administrative tool (Start – Programs – Administrative Tools – Certification Authority) .

Expand the Certification Authority console tree and click on the Pending Requests folder.

In the details pane find the request that you just submitted. Right-click on it and select "All Tasks ▸ Issue."

Return to the web browser that you used to send the request and browse to http://<certificate server>/certsrv.

Select "Check on a pending certificate" and click *Next*.

Select the certificate you requested and click *Next*.

On the Certificate Issued page, click the “Install this certificate” link.

If prompted for a PIN code, enter it and click *OK*.

The smart card will now be personalized with a public/private key-pair and a user certificate and is ready for use with F-Secure VPN+.

5.2.2 Enterprise CA

Logon to the “Enrollment Station” as the “Enrollment Agent” (as configured in steps above.)

Launch a web browser and browse to “http://<ca server>/certsrv.”

Select “Request a certificate” and click the *Next* button.

Select the “Advanced request” option and click the *Next* button.

Select the “Request a certificate for a smart card on behalf of another user using the Smart Card Enrollment Station” option and click the *Next* button.

Fill out the enrollment form using a “Certificate Template” of “Smartcard User” and click *Enroll*.

Enter the PIN for the smart card when prompted.

The smart card will now be personalized with a public/private key-pair and a user certificate and is ready for use with F-Secure VPN+.

6 Integration with F-Secure VPN+

6.1 Add CA Certificate as Trusted Root

In order for VPN+ clients to know which certificates are to be trusted when remote computers attempt to establish an IPSec connection, it is necessary to configure a list of trusted root (issuer) certificates. These certificates need to be manually exported from the third-party CA and imported to the VPN+ hosts either manually or using centrally managed policies (recommended). The sections below describe the process of establishing trust with the Windows 2000 CA.

6.1.1 Export CA Certificate

Launch a web browser and go to http://<certificate server>/certsrv

Select the “Retrieve the CA certificate or certificate revocation list” task and click *Next*.

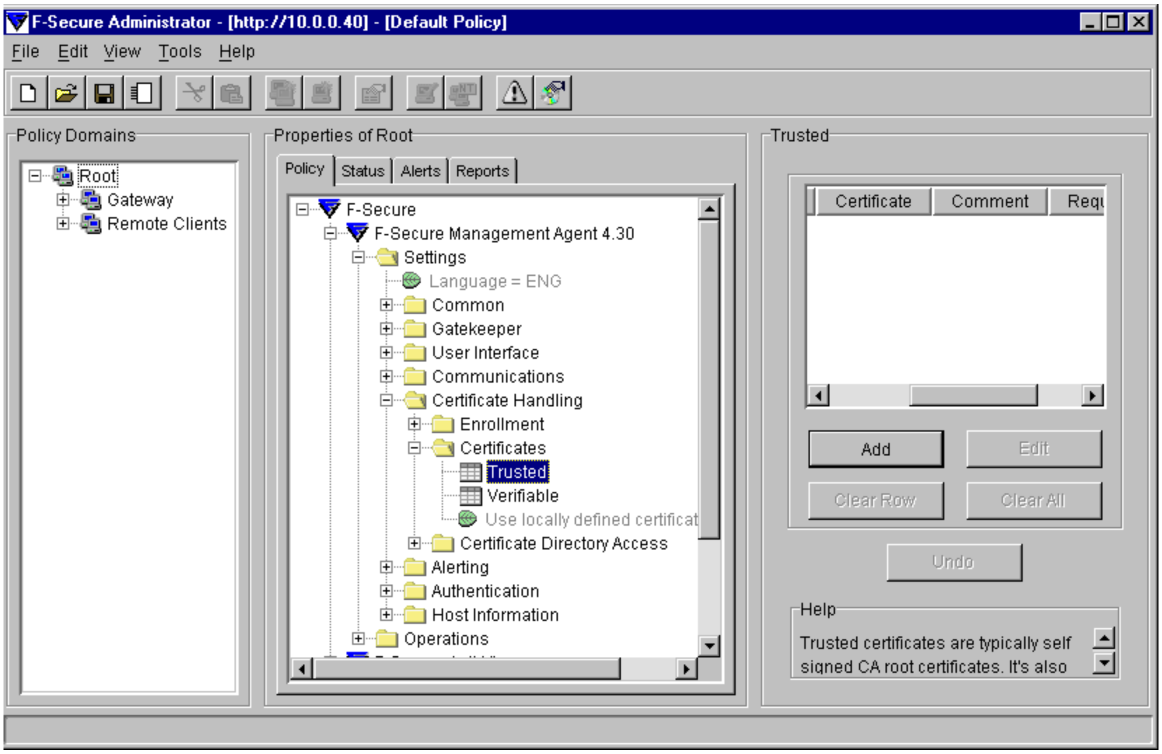
Choose the current CA certificate from the list, select the “Base 64 encoded” option and click on the “Download CA certificate” link.

Choose to “Save this file to disk” and click *OK*.

Select a temporary location to store the certificate file, name the file “win2k_ca.cer”, and click *Save*.

6.1.2 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.)



Trusted certificates are typically self signed CA root certificates. It's also

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. Windows 2000 CA).

6.2 Configure Smart Card Support on VPN+ Client

NOTE: The configuration described here is only necessary if you are using smart cards for authenticating VPN+ connections.

By default F-Secure Authentication Agent loads the iD2 pkcs#11 cryptographic provider (id2cbox.dll) which is installed with iD2 Personal. This provider does not recognize smart cards created by Windows 2000 Certificate Services because the profile that is created is not supported. In order to use these cards you can set the following registry entry to point to the pkcs provider dll provided by the card manufacturer:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Data Fellows\F-Secure\Authentication
Agent\DefaultProvider\PKCS#11="<pkcs#11 dll>"
```

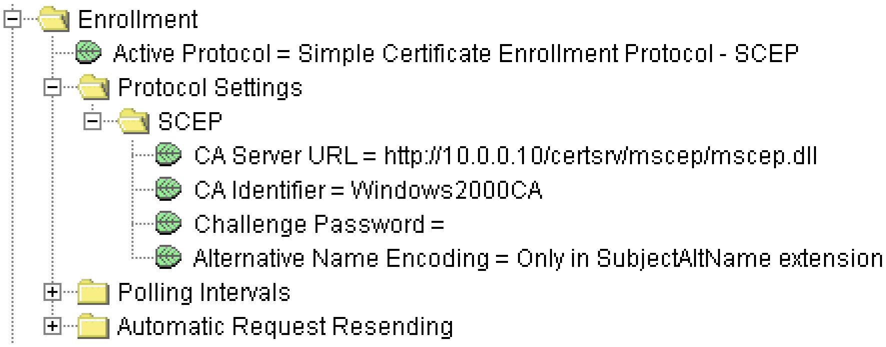
To date, the following smart cards and providers have been tested and work:

Schlumberger Cryptoflex 8K – slbck.dll

6.3 Configure Certificate Handling

6.3.1 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.



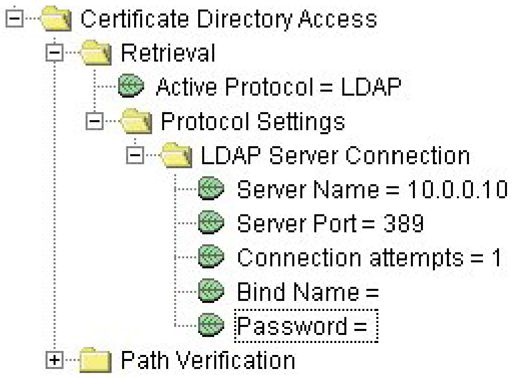
```
Enrollment
    Active Protocol = Simple Certificate Enrollment Protocol - SCEP
    Protocol Settings
        SCEP
            CA Server URL = http://10.0.0.10/certsrv/mscep/mscep.dll
            CA Identifier = Windows2000CA
            Challenge Password =
            Alternative Name Encoding = Only in SubjectAltName extension
    Polling Intervals
    Automatic Request Resending
```

6.3.2 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-compliant Windows 2000 Active 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.



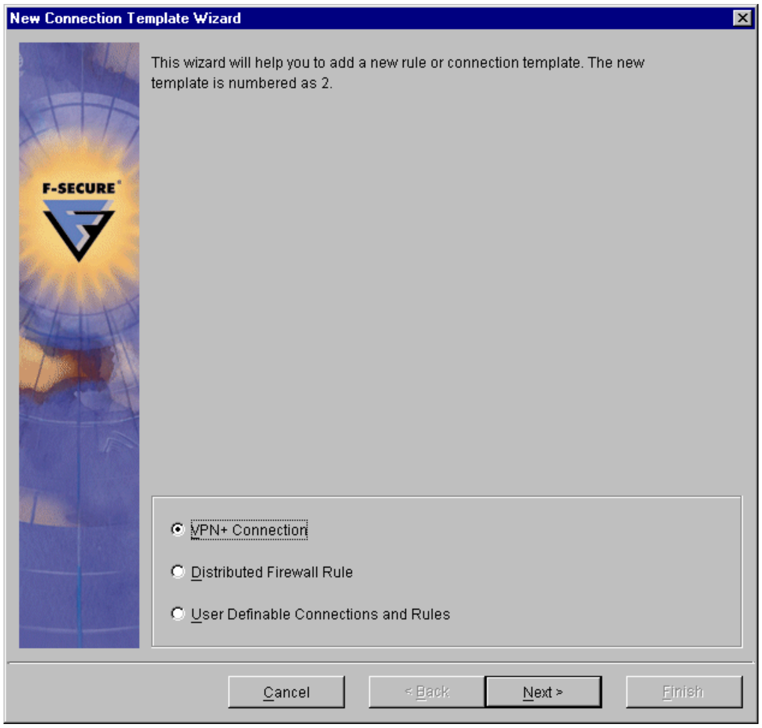
```
⊟ Certificate Directory Access
   ⊟ Retrieval
      Active Protocol = LDAP
      ⊟ Protocol Settings
         ⊟ LDAP Server Connection
            Server Name = 10.0.0.10
            Server Port = 389
            Connection attempts = 1
            Bind Name =
            Password =
   ⊞ Path Verification
```

6.4 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.



New Connection Template Wizard

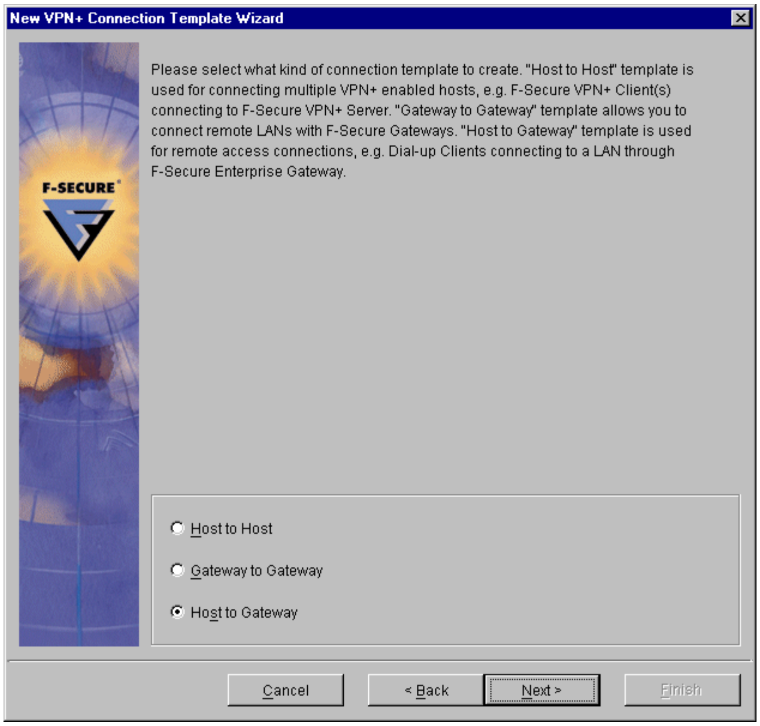
This wizard will help you to add a new rule or connection template. The new template is numbered as 2.

● VPN+ Connection

○ Distributed Firewall Rule

○ User Definable Connections and Rules

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



New VPN+ Connection Template Wizard

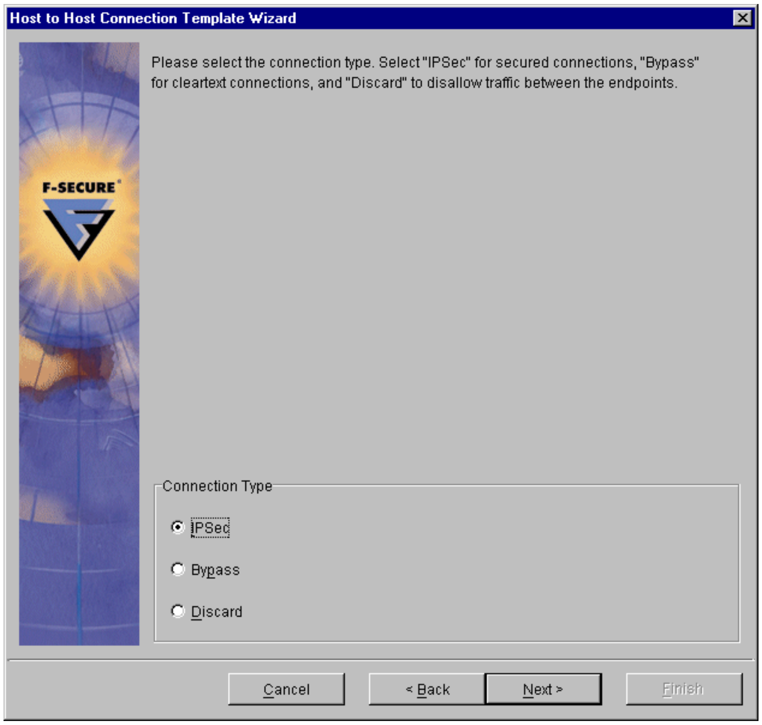
Please select what kind of connection template to create. "Host to Host" template is used for connecting multiple VPN+ enabled hosts, e.g. F-Secure VPN+ Client(s) connecting to F-Secure VPN+ Server. "Gateway to Gateway" template allows you to connect remote LANs with F-Secure Gateways. "Host to Gateway" template is used for remote access connections, e.g. Dial-up Clients connecting to a LAN through F-Secure Enterprise Gateway.

○ Host to Host

○ Gateway to Gateway

● Host to Gateway

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



Host to Host Connection Template Wizard

Please select the connection type. Select "IPSec" for secured connections, "Bypass" for cleartext connections, and "Discard" to disallow traffic between the endpoints.

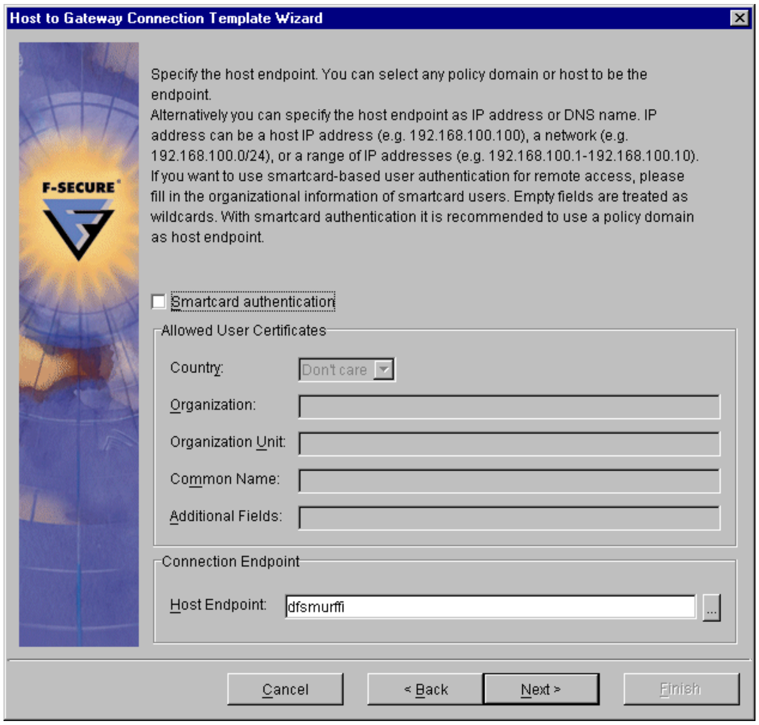
Connection Type

● IPSec

○ Bypass

○ Discard

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



Host to Gateway Connection Template Wizard

Specify the host endpoint. You can select any policy domain or host to be the endpoint.
Alternatively you can specify the host endpoint as IP address or DNS name. IP address can be a host IP address (e.g. 192.168.100.100), a network (e.g. 192.168.100.0/24), or a range of IP addresses (e.g. 192.168.100.1-192.168.100.10).
If you want to use smartcard-based user authentication for remote access, please fill in the organizational information of smartcard users. Empty fields are treated as wildcards. With smartcard authentication it is recommended to use a policy domain as host endpoint.

□ Smartcard authentication

Allowed User Certificates

Country: Don't care

Organization:

Organization Unit:

Common Name:

Additional Fields:

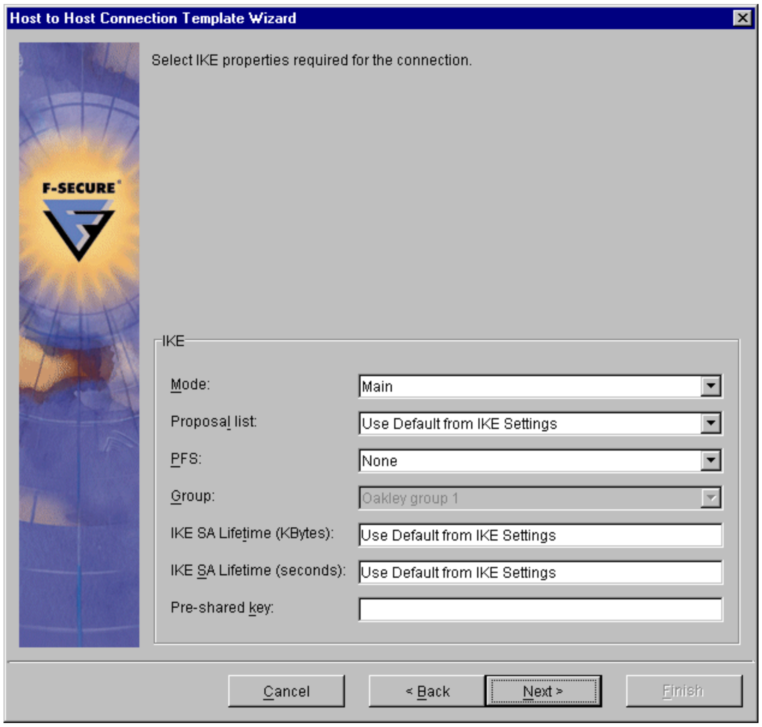
Connection Endpoint

Host Endpoint: dfsmurffi

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.


Host to Host Connection Template Wizard

Select IKE properties required for the connection.

IKE

Mode: Main

Proposal list: Use Default from IKE Settings

PFS: None

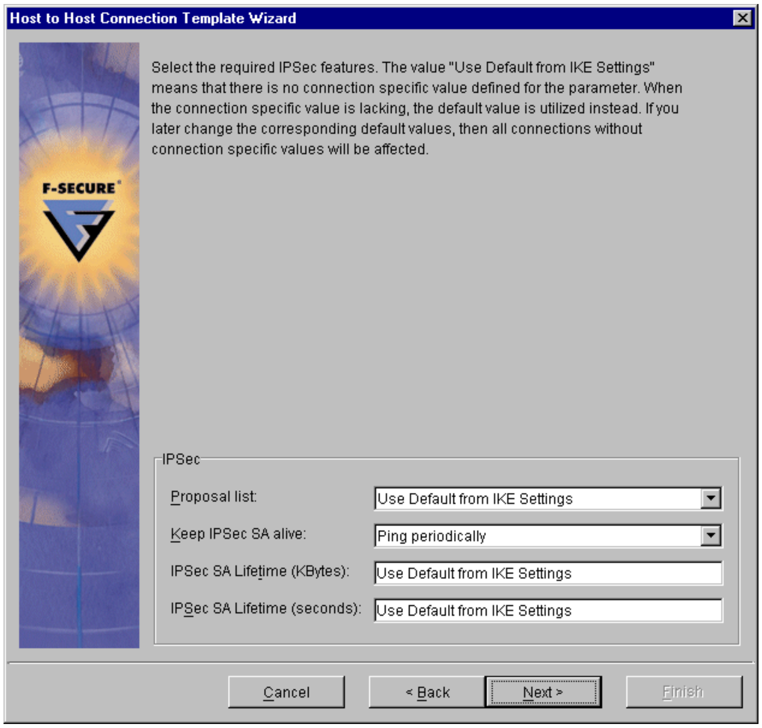
Group: Oakley group 1

IKE SA Lifetime (KBytes): Use Default from IKE Settings

IKE SA Lifetime (seconds): Use Default from IKE Settings

Pre-shared key:

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



Host to Host Connection Template Wizard

Select the required IPSec features. The value "Use Default from IKE Settings" means that there is no connection specific value defined for the parameter. When the connection specific value is lacking, the default value is utilized instead. If you later change the corresponding default values, then all connections without connection specific values will be affected.

IPSec

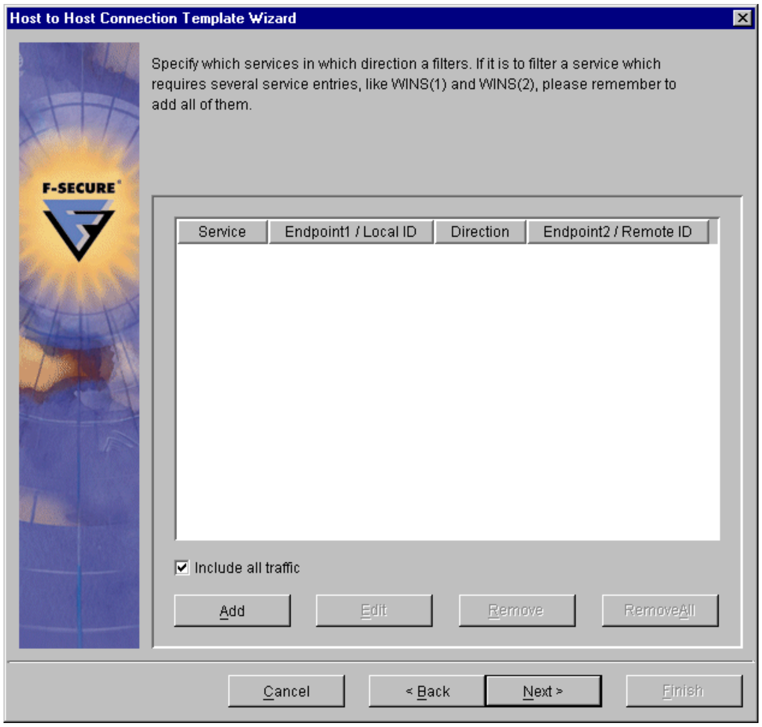
Proposal list: Use Default from IKE Settings

Keep IPSec SA alive: Ping periodically

IPSec SA Lifetime (KBytes): Use Default from IKE Settings

IPSec SA Lifetime (seconds): Use Default from IKE Settings

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



Host to Host Connection Template Wizard

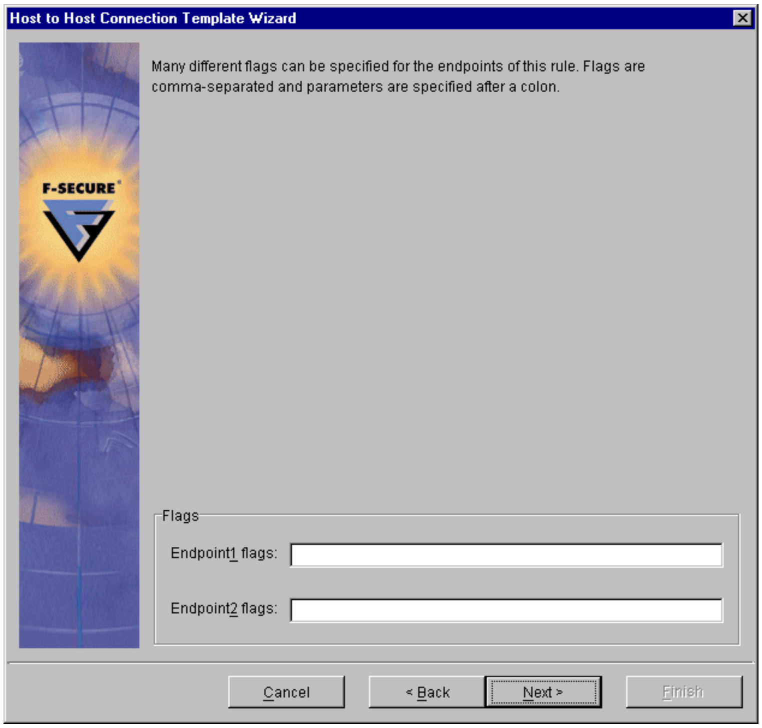
Specify which services in which direction a filters. If it is to filter a service which requires several service entries, like WINS(1) and WINS(2), please remember to add all of them.

Service	Endpoint1 / Local ID	Direction	Endpoint2 / Remote ID

☑ Include all traffic

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.



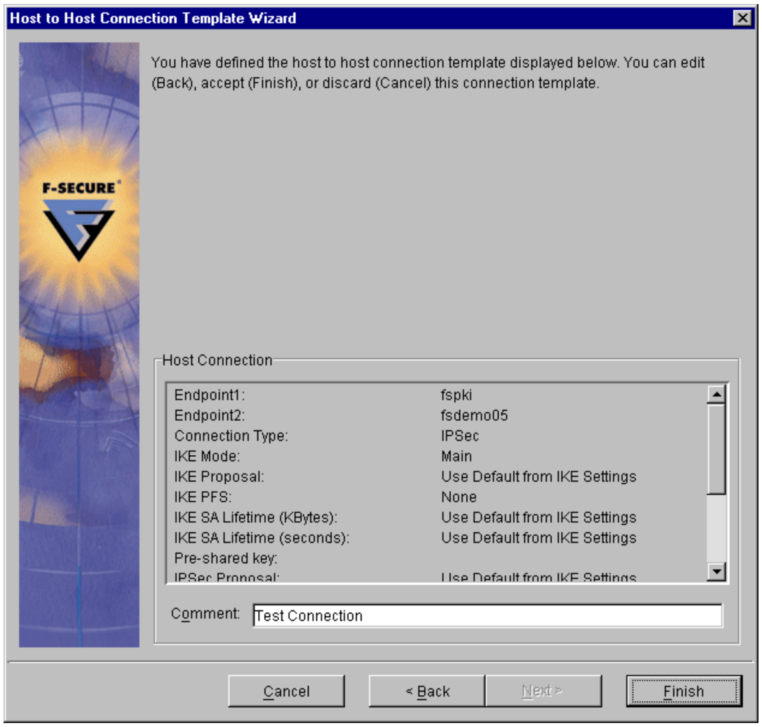
Many different flags can be specified for the endpoints of this rule. Flags are comma-separated and parameters are specified after a colon.

Flags

Endpoint1 flags:

Endpoint2 flags:

Leave the endpoint flags empty and click *Next*.



You have defined the host to host connection template displayed below. You can edit (Back), accept (Finish), or discard (Cancel) this connection template.

Host Connection

Endpoint1:	fspki
Endpoint2:	fsdemo05
Connection Type:	IPSec
IKE Mode:	Main
IKE Proposal:	Use Default from IKE Settings
IKE PFS:	None
IKE SA Lifetime (KBytes):	Use Default from IKE Settings
IKE SA Lifetime (seconds):	Use Default from IKE Settings
Pre-shared key:	
IPSec Proposal:	Use Default from IKE Settings

Comment: Test Connection

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.

6.5 Known Issues

SCEP Add-in may return “Bad Message Check” during SCEP enrollment. The cause of this error is unknown at this time but in order fix the problem it is necessary to restart the IIS Administration service (and all dependent services) on the server.