

NOKIA 9500

Communicator



9233513

Issue 1 EN

Nokia and Nokia Connecting People are registered trademarks of Nokia Corporation

VPN Client User's Guide

9233513

Issue 1

Copyright © 2004 Nokia. All rights reserved.

Reproduction, transfer, distribution or storage of part or all of the contents in this document in any form without the prior written permission of Nokia is prohibited.

Nokia is a registered trademark of Nokia Corporation. Other product and company names mentioned herein may be trademarks or tradenames of their respective owners.

This product includes software licensed from Symbian Software Ltd (c) 1998-2004. Symbian and Symbian OS are trademarks of Symbian Ltd.

SecurID is a registered trademark of RSA Security INC.

Nokia operates a policy of continuous development. Nokia reserves the right to make changes and improvements to any of the products described in this document without prior notice.

Under no circumstances shall Nokia be responsible for any loss of data or income or any special, incidental, consequential or indirect damages howsoever caused.

The contents of this document are provided 'as is'. Except as required by applicable law, no warranties of any kind, either express or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose, are made in relation to the accuracy, reliability or contents of this document. Nokia reserves the right to revise this document or withdraw it at any time without prior notice

The availability of particular products may vary by region. Please check with the Nokia dealer nearest to you.

Contents

Virtual private networking..... 4

Managing virtual private networking..... 4

Installing VPN client..... 5

System requirements 5

Managing VPN policies..... 5

Installing VPN policies from VPN policy servers... 5

Installing VPN policies from SIS files..... 6

Viewing VPN policies 7

Checking policy status 7

Checking certificate status 7

Updating VPN policies..... 8

Deleting VPN policies 8

Managing VPN policy servers..... 8

Connecting to VPN policy servers..... 8

Installing settings from SIS files 9

Adding VPN policy servers..... 9

Editing VPN policy servers..... 10

Synchronising VPN policy servers 11

Enrolling VPN certificates 11

Deleting VPN policy servers..... 11

Managing VPN access points..... 11

Viewing the VPN log..... 13

Key store passwords 13

Creating or changing a key store password..... 13

Entering key store passwords..... 13

Using VPN with applications 14

Authenticating to VPN gateways..... 14

Troubleshooting..... 14

Index..... 17

Virtual private networking

With **virtual private networking** (VPN), you can create encrypted connections to information you need while away from the office. You are in touch and in control with encrypted access to your enterprise network for email, database applications, and intranet.

Remote network traffic needs to be protected. Your company might use a VPN to tunnel network traffic and apply appropriate security policies. A VPN helps provide network transaction

ons with privacy and integrity and allows users to be authenticated and authorized for access to networks and network services.

To create a VPN, a gateway and the communicator authenticate each other and negotiate encryption and authentication algorithms to help protect the privacy and integrity of the information that you access.

Managing virtual private networking

To use VPN connections, you first create VPN access points, and then select VPN access points when you use applications to connect to the enterprise. A VPN connection is created to the enterprise network over another type of Internet access point connection. The

connection is created and encrypted according to a VPN policy that is loaded when you connect to a VPN access point.

To use virtual private networking

- 1 Install VPN client.

For more information, see "Installing VPN client" on page 5.

- 2 Specify a connection to a VPN policy server.

You can specify settings for a VPN policy server in [VPN management](#) or install the settings from a **Symbian installation system** (SIS) file.

For more information, see "Connecting to VPN policy servers" on page 8.



Note: If you install VPN policies from SIS files, you do not have to create connections to VPN policy servers.

- 3 Install VPN policies from the VPN policy server.

For more information, see "Installing VPN policies from VPN policy servers" on page 5.

- 4 Create VPN access points.

VPN access points specify an Internet access point and a VPN policy.



Note: VPN access points combine VPN policies with Internet access points. When you synchronise a VPN policy server for the first time, matching VPN access points are created

for each policy that you install on the communicator.

For more information about creating and selecting VPN access points, see "Managing VPN access points" on page 11.

- 5 Select a VPN access point when you use applications to connect to the enterprise network.
For more information, see "Using VPN with applications" on page 14.
A VPN connection is created on top of the Internet access point connection.

Installing VPN client

You receive VPN client as a standard SIS file. You install VPN client on a communicator in the same way that you install other software. For more information about how to install software on a communicator, see the documentation of the communicator.

When the installation is complete, remove and re-insert the battery in the communicator for the changes to take effect.

You do not need the VPN client SIS file after the installation. Delete the SIS file to release memory.

System requirements

Nokia recommends that you install VPN client on a memory card, if you have a memory card, to save device

memory. The memory card must be in the communicator for VPN client to work.

During the installation of VPN client, you need at least 1.5 MB of memory in the communicator.

After the installation, VPN client reserves 900 K of memory on the communicator or on a memory card. Each VPN policy typically requires from 1 K to 16 K of memory on the communicator.

Managing VPN policies

VPN policies define the method that VPN client and a VPN gateway use to authenticate each other and the encryption algorithms that they use to help protect the confidentiality of the data. Administrators create VPN policies and store them on VPN policy servers or deliver them to you as SIS files. You install VPN policies from a VPN policy server in [VPN management](#).

Installing VPN policies from VPN policy servers

In [VPN management](#), you can install VPN policies from a VPN policy server.



Tip! VPN policy servers are servers on the enterprise network that contain VPN policies.

To install VPN policies

- 1 Go to [Tools](#) > [Control panel](#) > [Connections](#) > [VPN management](#).
 - 2 Press [Yes](#) when [VPN management](#) prompts you to install VPN policies.
 - 3 Press [Yes](#) again to add VPN policy servers.
 - 4 Specify settings for connecting to a VPN policy server and press [Done](#).
- For more information, see "Connecting to VPN policy servers" on page 8.
- 5 Press [Yes](#) to synchronise the VPN policy server.
 - 6 Create a key store password and press [OK](#).



Tip! A key store password helps protect private keys in VPN policies and VPN policy server connections from unauthorized use.

For more information, see "Creating or changing a key store password" on page 13.

The communicator connects to the VPN policy server.

- 7 Verify the identity code of the VPN policy server and key in the missing characters to establish trust between the communicator and the VPN policy server and press [OK](#).

You can skip this step if you install the settings for the VPN policy server from a SIS file.



Tip! A VPN policy server identity code is the fingerprint of the VPN policy server certificate, which identifies the certificate.

For more information, see "Adding VPN policy servers" on page 9.

- 8 Key in authentication information to access the VPN policy server and press [OK](#).
Administrators tell you what information to key in.

VPN policies are installed on the communicator.



Note: If you press Cancel, VPN policies are not installed. Select Install to install VPN policies from a VPN policy server.

Installing VPN policies from SIS files

Administrators can deliver VPN policies to you as SIS files. If you install VPN policies from SIS files, you do not have to define connections to VPN policy servers. After you install VPN policies, you can create VPN access points and associate them to applications.

If the VPN policies contain private keys and corresponding certificates, administrators define **key import passwords** to help protect the private keys. Administrators should use a secure method to deliver the key import password to you.



Tip! A key import password helps protect the private keys in a VPN policy file.

To install VPN policies from SIS files, type the key import password in [Password](#) and press [OK](#). Then type the key store password in [Password](#) and press [OK](#).

Viewing VPN policies

In *VPN management*, you can view, update, and delete the VPN policies that you install on a communicator.

To view VPN policy details, select a VPN policy and press *Open* to view more information.

Scroll to view the following information about each VPN policy:

- *Description* shows additional information about the VPN policy. The description is read from the VPN policy. Administrators define the description when they create the VPN policy.
- *Policy status* indicates whether the VPN policy is ready to use or not or whether it is already in use.
- *Certificate status* indicates whether valid user certificates are available in the communicator.
- *Policy name* shows the name of the VPN policy. Administrators define the name when they create the VPN policy.
- *Policy server name* shows the name of the VPN policy server from where you installed the VPN policy. You give names to VPN policy servers when you define connections to VPN policy servers. This field is hidden if you installed the VPN policy from a SIS file.
- *Updated* shows the date when the VPN policy was last updated from the VPN policy server. This field is hidden if you installed the VPN policy from a SIS file.

Checking policy status

Policy status can have the following values:

Active — you created a connection to a VPN access point that is associated with the VPN policy. When you create a connection, the VPN policy is activated.

Associated with a VPN access point — you associated the VPN policy with one or several VPN access points. You can select any of the VPN access points to activate the VPN policy.

Not associated with a VPN access point — you must associate the VPN policy with a VPN access point to activate the VPN policy.



Note: The VPN policy details view is not refreshed if the policy status changes while the view is open.

Checking certificate status

Certificate status can have the following values:

OK — at least one valid certificate is available in the communicator or you do not use certificates to authenticate to VPN gateways.

Expired — lifetime of one or more certificates has ended. If you cannot create a VPN connection, update the VPN policy to enroll new certificates.

Missing — One or more of the required certificates cannot be found on the communicator. If you cannot create a VPN connection, try to update the VPN policy to enroll new certificates.

Not yet valid — one or more certificates are for future use. This value might also mean that the date and time on the

communicator are set in the past, time zones are not set correctly, or the daylight-saving setting is turned on.

To delete the VPN policy, press [Delete](#).

To close the VPN policy details, press [Close](#).

Updating VPN policies

When you create a connection to a VPN access point, VPN client checks the status of the VPN policy that is associated with the VPN access point from the VPN policy server. If administrators created a new version of the VPN policy, the new version is installed on the communicator. If administrators deleted the VPN policy from the VPN policy server, the VPN policy is removed from the communicator.

Changes become effective the next time you create a connection to the VPN access point, so they do not affect the current VPN connection.

You can also update a VPN policy in [VPN management](#).

To update a VPN policy, select a VPN policy and press [Update](#). VPN client checks the status of the VPN policy from the VPN policy server.

Deleting VPN policies

VPN policies are deleted automatically after administrators delete them from the VPN policy server when you update a VPN policy or synchronise the VPN policy server.

If you delete a VPN policy in [VPN management](#) that still exists on the VPN policy server, the VPN policy is installed again when you synchronise VPN policies from the VPN policy server.

To delete a VPN policy, select the VPN policy, and press Ctrl + [D](#).

You cannot use a VPN access point if you delete the VPN policy that is associated with it.

Managing VPN policy servers

In [Policy servers](#), you can install VPN policies from VPN policy servers. When you create a connection to a VPN access point, the communicator connects to the VPN policy server to automatically update the VPN policy that is associated with the VPN access point. To update all VPN policies, synchronise VPN policy servers with the communicator.

Connecting to VPN policy servers

When you install VPN policies from a VPN policy server, you create a trust relationship between the communicator and the VPN policy server. To create the trust relationship, you must authenticate the VPN policy server and the VPN policy server must authenticate you.

After the VPN policy server authenticates you, VPN client generates a private key and enrolls a corresponding certificate for you. The private key and certificate are

stored in a key store on the communicator. The certificate authenticates you to the VPN policy server.



Tip! Administrators can deliver to you a SIS file that contains settings that specify a connection to a VPN policy server or you can add the VPN policy server in [VPN management](#).

Installing settings from SIS files

You can install VPN policy server settings on the VPN policy server from a SIS file. You install the settings on a communicator in the same way that you install other software.

The settings consist of the address and server certificate of the VPN policy server. The server certificate makes the communicator trust the VPN policy server, so you only need to present a user name and password to prove your identity.

The SIS file does not contain settings for the Internet access point to connect to the VPN policy server. To specify the Internet access point, edit VPN policy server settings. You can also select the Internet access point when you connect to the VPN policy server.

If administrators do not sign the SIS file, a security warning is displayed when you install the SIS file. You can ignore the warning if you can be sure that you received the SIS file from administrators.

You must exit [VPN management](#) before you install the settings from a SIS file or installation fails.

Adding VPN policy servers

In [Policy servers](#), you can specify settings for a VPN policy server if you do not install the settings from a SIS file.

When you connect to the VPN policy server address for the first time, the communicator does not trust the VPN policy server, so you must authenticate the VPN policy server. You receive a VPN policy server identity code from administrators. You check and complete the VPN policy server identity code and VPN client verifies it.

After successful authentication, VPN client enrolls a certificate from the VPN policy server for subsequent authentication to the VPN policy server.

To add a VPN policy server, press [New](#). Key in the following settings:

- [Policy server name](#) — you can choose any name, but it must be unique in [VPN policy servers](#).
If you leave this field empty, [Policy server address](#) is inserted in this field.
The policy server name appears in the VPN policy server list and on the title bar of the VPN policy server settings dialog.
- [Policy server address](#) — host name or IP address of the VPN policy server to install VPN policies from. You can also specify a port number, separated with a colon (:). You receive the policy server address from administrators.
- [Internet access point](#) — Internet access point used to connect to this VPN policy server.

Administrators tell you which access point to select.

To install VPN policies from the VPN policy server, press **Yes** when **VPN management** prompts you to synchronise the VPN policy server.



Tip! Synchronising means that VPN client connects to a VPN policy server to check for new, updated, or removed VPN policies and installs the VPN policies on the communicator.

When you connect to the VPN policy server address for the first time, the VPN policy server is not trusted, so you must authenticate the VPN policy server. You receive a VPN policy server identity code from administrators.

To verify the identity of the VPN policy server, carefully compare the VPN policy server identity code in the **VPN policy server identity code** dialog with the code that you receive from administrators, key in the missing characters in **Missing characters**, and press **OK**.



Note: If you install VPN policy server settings from a SIS file, you do not have to verify VPN server identity and this view never appears.

To authenticate to the VPN policy server, key in your user name in **Policy server user name** and password in **Policy server password** and press **OK** in the **VPN policy server authentication** dialog.

Administrators tell you the user name and password to key in.



Tip! A policy server user name and password help protect the VPN policy server from unauthorized access.

VPN client enrolls a certificate for subsequent authentication to the VPN policy server and installs VPN policies on the communicator.



Tip! Enrolling a certificate means sending a certification request to a certification authority and receiving a certificate.

You can now create VPN access points and associate them with applications.

Editing VPN policy servers

In **Policy servers**, you can view, edit, synchronise, and delete VPN policy servers.

To view or change the settings for a VPN policy server, select the VPN policy server and press **Edit** to change:

- **Policy server name** — name for the policy server. **Policy servers** shows the new name.
- **Internet access point** — Internet access point used to connect to this VPN policy server.

If you deleted the access point that is associated with the VPN policy server, **Internet access point** shows the text **(not selected)**. If you deleted all access points, **VPN management** cannot save the settings.

You cannot change **Policy server address** after you install VPN policies from the VPN policy server, because the VPN

policy server sends the address to [VPN management](#) during the first connection.

To delete the VPN policy server, press [Delete](#).

To save the settings, press [Done](#).



Tip! To close the view without saving your changes, press Esc.

Synchronising VPN policy servers

To install and update policies from the VPN policy server, select a VPN policy server and press [Synchronise](#). VPN client connects to the VPN policy server to check whether administrators added, updated, or deleted VPN policies.

If the VPN policy server contains new VPN policies or new versions of VPN policies, the VPN policies are installed on the communicator. If administrators deleted VPN policies from the VPN policy server, the VPN policies are removed from the communicator.



Note: When you synchronise a VPN policy server for the first time, matching VPN access points are created for each policy that you install on the communicator. VPN access points combine VPN policies with Internet access points.

When you connect to a VPN policy server to install or update VPN policies, you might need to enroll VPN certificates from the VPN policy server.

Enrolling VPN certificates

VPN client creates a certification request for each required certificate and sends the request to the VPN policy server. The VPN policy server enrolls each requested certificate from a **certification authority** and returns it to VPN client.

The certification request and the corresponding certificate contain the identity of the user. Depending on the VPN policy server configuration, the VPN policy server user identity might be used as the user identity in VPN certificates. If this is not possible, [VPN management](#) asks the user identity from you for a particular domain. Administrators tell you what information to key in.

To create certification requests, in the [VPN user identity](#) dialog, key in your certificate user identity for the specified domain in [User identity](#) and press [OK](#).

Deleting VPN policy servers

To delete a VPN policy server, select the VPN policy server and press Ctrl + [D](#).

[VPN management](#) asks you to confirm the deletion of the VPN policies that you installed from the VPN policy server.

Managing VPN access points

A VPN access point is a virtual access point that combines a VPN policy and an Internet access point. Select a VPN

access point in Internet access point lists to create a VPN connection.

In *VPN access points*, you can view, create, and delete VPN access points on the communicator. Go to *Tools > Control panel > Connections > VPN access points*. An icon indicates the type of the Internet connection over which the VPN connection is created.

To create VPN access points, press *New*. In *General settings*, key in the following settings:

- *VPN access point name* — identifies the VPN access point in Internet access point lists.
- *Internet access point* — name of the Internet connection over which the VPN connection is created.
- *VPN policy* — name of the VPN policy that is associated with the VPN access point.
- *Network* — identifies the VPN network.

You must select a different network than the network for the Internet access point.



Note: If you create VPN connections to several VPN gateways, create separate networks for connecting to each VPN gateway.

To select a network, go to *Network* and press *Change*:

- Select a network and press *OK*.
- **To add a network**, press *Add network*, key in a name for the network in *Network name*, and press *OK*.
- **To rename a network**, press *Rename network*, change the network name in *Network name*, and press *OK*.

To specify settings for a proxy server in the enterprise network, go to *Proxy settings* and key in the following settings:



Note: A proxy server is an intermediate server that acts as a security barrier between an intranet and the Internet. Administrators tell you the appropriate settings.

- *Proxy protocol* — protocol that the proxy server uses.
- *Use proxy server* — select *Yes* to specify settings for a proxy server in the enterprise network.
- *Proxy server* — address of a proxy server in the enterprise network.
- *Port number* — port number to connect to the proxy server.
- *No proxy for* — Internet addresses to bypass the proxy server for particular sites.

To view and edit VPN access point settings, select a VPN access point and press *Edit*.

To delete a VPN access point, select a VPN access point and press *Ctrl + D*.

To save the settings, press *Done*.






Tip! To close the view without saving your changes, press *Esc*.

Viewing the VPN log

The VPN log contains log messages that are recorded when you update and synchronise VPN policies and use VPN access points to create VPN connections to VPN gateways.

In [Log](#), you can view and clear log messages. You can view the message type, the time when each message is recorded, and the beginning of the log message.

 indicates error,  warning, and  information.

To view the complete log message, press [Open](#).

[Log](#) sorts log messages by the time and date when they are recorded, most recent messages first. You can view messages up to the time when you opened [Log](#).

To view the most recent log messages, press [Refresh](#).

Log messages can contain error, status, and reason codes. Report the codes to administrators when you report errors.

To delete all log messages from the log, press [Clear log](#).

Log messages are recorded to a circular buffer. When the log size reaches 20 kilobytes, new log messages are written on top of the oldest log messages.

Key store passwords

In [Password](#), you can create or change a key store password. A key store password helps protect private keys in the communicator and VPN policy server connections from unauthorized use.

Creating or changing a key store password

You create a key store password when you install the first VPN policy. Create key store passwords that are long and difficult enough to help protect the information in the communicator. If the key store password is broken, the enterprise network might be exposed to unauthorised access.



Tip! A key store password must be at least six characters long and can contain letters, numbers, and special characters.

To change the key store password, press [Change password](#).

Key in a password that is easy for you to remember but difficult for anyone else to guess in [Password](#). To avoid typing errors, key in the password again in [Confirm](#) and press [OK](#).

Entering key store passwords

You must enter the key store password when you:

- Install new or updated VPN policies from VPN policy servers.
- Use applications to connect to VPN access points that require certificate authentication.

Using VPN with applications

When you use an application to create a connection to a VPN access point, the communicator:

- Connects to the Internet access point that is associated with the VPN access point.
- Loads the VPN policy that is associated with the VPN access point.
- Connects to a VPN gateway to create a VPN connection.

Authenticating to VPN gateways

You need to prove your identity when you log on to the enterprise VPN. The VPN policy determines the authentication method that you use:

- Certificate-based authentication — you must have a certificate that a trusted certification authority signs. You use online certificate enrollment to obtain the certificate or you install certificates when you install the VPN policy from a SIS file.
- Legacy authentication — you use user names and passwords or passcodes to authenticate. Administrators create the user names and passwords or give you SecurID tokens to generate the passcodes.

If you use certificates for authentication, enter the key store password.

If you use legacy authentication, key in VPN authentication information when you use applications to

connect to VPN access points and the communicator negotiates encrypted connections with the VPN gateway.

To use usernames and passwords to authenticate to a VPN gateway, key in your VPN user name in *VPN user name* and VPN password in *VPN password*. Press *OK*.

To use usernames and passcodes to authenticate to a VPN gateway, key in your VPN user name in *VPN user name*. Generate a SecurID passcode and key in it in *VPN passcode*. Press *OK*.

If the SecurID token has become out of synchronisation with the time clock of the ACE/Server, you are prompted for the next passcode that the ACE/Server uses as a new reference for the time base of the token. Key in your VPN user name in *VPN user name*. Generate and key in a new passcode in *Next passcode* and press *OK*. If this fails, contact administrators.

Troubleshooting

This section lists error messages in alphabetical order, describes the possible causes of the errors, and suggests actions to recover from the errors.

Authentication failed.

- You key in an incorrect user name or password when you authenticate to a VPN policy server or log on to a VPN.
- You key in the wrong passcode when you are prompted for the Next passcode.

Try the following solutions:

- Check your user name and password and try again.
- Generate and key in a passcode.

Automatic policy server logon failed. Enter policy server user name and password to continue.

The certificate that authenticates you to the VPN policy server expires or administrators revoke the certificate.

Report this error to administrators, who give you a one-time password for logon. Key in the user name and one-time password to authenticate to the VPN policy server. VPN client enrolls a new certificate for you.

Automatic policy server logon failed. See VPN log for details.

The validity period of the certificate that authenticates you to the VPN policy server has not begun yet.

Check the date and time settings or wait until the validity period of the certificate begins.

Crypto library is too weak.

If the cryptographic library that is installed on the communicator is too weak, you cannot use VPN connections.

Contact administrators.

Incorrect password.

You key in an incorrect key store password or key import password.

Check the password and try again.

You receive the key import password from administrators. You create the key store password yourself.

Policy server is currently in use. Unable to delete.

You cannot delete a VPN policy server while you update VPN policies from the server. If you use an application that creates a connection to a VPN access point, VPN policies are automatically updated.

Wait until VPN policy update finishes and try again.

Policy server logon failed. Delete and re-create the server definition.

The server certificate of the VPN policy server expires.

To delete the VPN policy server, select the VPN policy server in [Policy servers](#) and press Ctrl + **D**.

To add the VPN policy server again, press **New**, or ask the administrator for a SIS file that contains new settings for the VPN policy server.

Policy update failed. See VPN log for details.

Policy server synchronisation failed. See VPN log for details.

An error occurs while VPN policies are downloaded from the VPN policy server or installed on the communicator.

To update a VPN policy, select a VPN policy in [Policies](#) and press **Update**.

To install policies from the VPN policy server, select a VPN policy server in [Policy servers](#) and press **Synchronise**.

Server identity code is incorrect.

You key in an incorrect string when you are prompted to key in the VPN policy server identity code.

Check the VPN policy server identity code carefully against the code that you receive from administrators and key in the missing characters again.

VPN connection activation failed. See VPN log for details.

Legacy authentication failed or the certificate that you use to authenticate to the VPN gateway is missing, expired, or its validity period has not begun yet.

Check the date and time settings on the communicator.

To update a VPN policy, select a VPN policy in *Policies* and press *Update*.

VPN policy in use has been deleted. Try reconfiguring the internet access point.

The VPN policy that was associated with the VPN access point became obsolete and was deleted automatically.

To associate another VPN policy with the VPN access point, in *VPN access points*, select the VPN access point, and press *Edit*.

Index

A

Add network button 12
adding networks 12
Authentication failed 14
Automatic policy server logon failed 15

C

Certificate status field 7
certificate-based authentication 14
certificates

- authenticating to VPN policy servers 8
- enrolling 11
- status 7
- user identity 11

Change password button 13

Clear log button 13

Confirm field 13

Connectivity Client

- installing 5
- introducing 4
- system requirements 5

creating VPN access points 12

D

Delete button 8, 11

deleting 8

- VPN access points 12

VPN policies 8

VPN policy servers 11

Description field 7

E

Edit button 12

editing VPN access points 12

enrolling certificates 11

error messages 14

expired certificates 7

F

fields

Certificate status 7

Confirm 13

Description 7

Internet access point 9, 12

Network 12

Next passcode 14

No proxy for 12

Password 13

Policy name 7

Policy server address 9

Policy server name 7, 9

Policy server password 10

Policy server user name 10

Policy status 7

Port number 12

Proxy protocol 12

Proxy server 12

Updated 7

Use proxy server 12

User identity 11

VPN access point name 12

VPN passcode 14

VPN password 14

VPN policy 12

VPN user name 14

I

Incorrect password 15

installing

- Connectivity Client 5

- VPN policies 5, 11

- VPN policy server settings from SIS files 9

Internet access point field 9, 12

K

Key store password view 13

key store passwords

- about 13

- creating 13

- entering 13

L

legacy authentication 14

M

memory requirements 5

missing certificates 7

N

Network field 12

networks

- adding 12

- renaming 12

- selecting 12

Next passcode field 14

No proxy for field 12

not yet valid certificates 7

P

Password field 13

Policy name field 7

Policy server address field 9

Policy server is currently in use 15

Policy server logon failed 15

Policy server name field 7, 9

Policy server password field 10

Policy server user name field 10

Policy status field 7

Policy update failed 15

Port number field 12

Proxy protocol field 12

Proxy server field 12

Proxy settings view 12

R

Refresh button 13

Rename network button 12

S

SecurID passcode 14

Select network view 12

selecting networks 12

Server identity code is incorrect 15

system requirements 5

U

Updated field 7

Use proxy server field 12

User identity field 11

V

VPN

- about 4

- authenticating to 14

- using with applications 14

VPN access point name field 12

VPN access points

- deleting 12

- editing 12

- managing 11

- view 12

VPN connection activation failed 16

VPN log

- clearing 13

- view 13

VPN passcode field 14

VPN password field 14

VPN policies 8

- about 5

- deleting 8

- details 7

- installing 5

- managing 5

- status 7

- updating 8

VPN policy field 12

VPN policy in use has been deleted 16

VPN policy servers

- adding 9

- connecting 8

- deleting 11

- installing settings from SIS files 9

- managing 8

VPN user name field 14