VPN Client
User's Guide

9235966
Issue 2

Contents

1. Virtual Private Network

Go to *Menu* and select *Tools* > *Settings* > *Connection* > *VPN*.

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

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

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

Note: To use VPN, you must receive VPN policy server settings from administrators. Administrators can send the settings to you as a **Symbian installation system** (SIS) file.

To use virtual private networking

1 Install VPN Client.
For more information, see "Installation" on page 6.

2 Specify a connection to a VPN policy server.
You can specify settings for a VPN policy server or install the settings from a SIS file.
For more information, see "Connecting to VPN policy servers" on page 12.

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 7.

4 Create VPN access points.

VPN access points specify an Internet access point and a VPN policy.
For more information, see “Creating VPN access points” on page 17.

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 mobile device.

5 Select a VPN access point when you use applications to connect to the enterprise network.
For more information, see “VPN and applications” on page 21.
A VPN connection is created on top of the Internet connection.

2. Installation

You receive VPN client as a standard **Symbian installation system** (SIS) file.

You install VPN client on a compatible mobile device in the same way that you install other software. For more information about how to install software on the mobile device, see the documentation of the mobile device.

When the installation is complete, switch the mobile device off and on 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

You can install VPN client either on the phone memory or on a memory card. The installation of VPN client temporarily reserves phone memory twice the size of the installation package. Each VPN policy typically reserves from 1 K to 16 K of phone memory.

3. VPN policies

VPN policies define the method that a mobile device and a VPN gateway use to authenticate each other and the encryption algorithms that they use to encrypt the data. Administrators create VPN policies and store them on VPN policy servers or deliver them to you as **Symbian installation system** (SIS) files. You can install VPN policies from a VPN policy server or from SIS files.

Go to *Menu* and select *Tools* > *Settings* > *Connection* > *VPN* > *VPN management* > *VPN policies*.

Installing VPN policies from VPN policy servers

To install VPN policies

1. Press *Yes* when you go to an empty *VPN policies* view and you are prompted you to install VPN policies.
2. Press *Yes* when you are prompted to add VPN policy servers.
3. Specify settings for connecting to a VPN policy server.
   For more information, see "Connecting to VPN policy servers" on page 12.
4. Press *Yes* when you are prompted to synchronise the VPN policy server.
5. Create a **key store password**.
   For more information, see "Creating or changing a key store password" on page 20.
   You connect to the VPN policy server.
6. Verify the **VPN policy server identity code** to establish a trust relationship.
   You can skip this step if you install the settings for the VPN policy server from a SIS file.
   For more information, see "Adding VPN policy servers" on page 13.

Glossary: VPN policy servers are servers on the enterprise network that contain VPN policies.

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

Glossary: A VPN policy server identity code is the fingerprint of the VPN policy server certificate, which identifies the certificate.

Glossary: A key import password helps protect the private keys in a VPN policy file.

7 Key in authentication information to access the VPN policy server and press *OK*. The administrator of the VPN policy server provides you with this information.

VPN policies are installed on the mobile device.

Note: If you press *Cancel*, VPN policies are not installed. Press *Options* and select *Install policies* 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.

To install VPN policies from SIS files

1 Type the key import password in *Key import password* and press *OK*.
2 Type the key store password in *Key store password* and press *OK*.

Viewing VPN policies

The *VPN policies* view lists VPN policies that you install on the mobile device.

If *(no VPN policies)* is displayed, you must install VPN policies. Press *Options* and select *Install policies* to install VPN policies from a VPN policy server.

Select a VPN policy to view the following information:

- *Description*—additional information 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 whether it is already in use.

- *Certificate status*—indicates whether valid user certificates are available on the mobile device.
- *Policy name*—name administrators give to the VPN policy when they create the VPN policy.
- *Policy server*—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*—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.

Policy status

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

Policy status can have the following values:

- *In use*—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 taken to use.
- *Associated with 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 take the VPN policy to use.
- *Not associated with VPN access point*—you must associate the VPN policy with a VPN access point to take the VPN policy to use.

Certificate status

Certificate status can have the following values:

- *OK*—at least one valid certificate is available in the mobile device or you do not use certificates to authenticate to VPN gateways.
- *Expired*—the validity of one or more certificates has ended.
  If you cannot create a VPN connection, try to update the VPN policy to enroll new certificates.

- *No certificate*—One or more of the required certificates cannot be found on the mobile device.
  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 mobile device are set in the past, time zones are not set correctly, or the daylight-saving setting is turned on.

Press the selection key to close the details and return to the *VPN policies* view.

Creating VPN access points with default values

To use the VPN policy, you must associate the VPN policy with a VPN access point. Press *Options* and select *Define VPN ac. point* in the *VPN policies* view.

Mobile VPN Client creates a VPN access point with default settings. You can create and modify VPN access points in the VPN access points view.

This option is not available if you installed the VPN policy from a SIS file.

Updating VPN policies

When you create a connection to a VPN access point, the status of the VPN policy is checked from the VPN policy server. If administrators created a new version of the VPN policy, the new version is installed on the mobile device. If administrators deleted the VPN policy from the VPN policy server, the VPN policy is removed from the mobile device.

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 the *VPN policies* view. To update a VPN policy, select a VPN policy, press *Options*, and select *Update policy*. The status of the VPN policy is checked from the VPN policy server.

Deleting VPN policies

VPN policies are deleted automatically when you synchronise a VPN policy server after administrators delete VPN policies from the VPN policy server. If you delete a VPN policy 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 the clear key.

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

4. VPN policy servers

Go to *Menu* and select *Tools* > *Settings* > *Connection* > *VPN* > *VPN management* > *VPN policy servers*.

You can install VPN policies from VPN policy servers. When you create a connection to a VPN access point, the VPN policy that is associated with the VPN access point is automatically updated from a VPN policy server. To update all VPN policies, synchronise VPN policy servers with the mobile device. For more information, see "Synchronising VPN policy servers" on page 15.

Connecting to VPN policy servers

When you install VPN policies from a VPN policy server, you create a trust relationship between the mobile device 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, a private key is generated and a corresponding certificate is enrolled. The certificate authenticates you to the VPN policy server. The private key and certificate are stored in a key store on the mobile device.

Tip! Administrators can deliver to you a SIS file that contains settings that specify a connection to a VPN policy server or you can specify settings for the VPN policy server.

Installing settings from SIS files

You can install VPN policy server settings to the VPN policy server from a SIS file. You install the settings on a mobile device 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 mobile device 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 are certain that the VPN policy server administrator created the SIS file and that the SIS file has not been modified.

Exit *VPN* before you install the settings from a SIS file, or installation fails.

Viewing VPN policy servers

The *VPN policy servers* view lists VPN policy servers that you create.

If *(no VPN policy servers)* is displayed, you must create VPN policy servers. To add a VPN policy server, press *Options* and select *New server*.

Adding VPN policy servers

If you do not install VPN policy server settings from a SIS file, specify settings for the VPN policy server.

When you connect to the VPN policy server address for the first time, you must authenticate the VPN policy server. You receive a VPN policy server identity code from administrators. Check and complete the VPN policy server identity code.

After successful authentication, a certificate is enrolled for subsequent authentication to the VPN policy server.

To add a VPN policy server

1. Press *Options* and select *New server* in the *VPN policy servers* view.
2. Select *Policy server name* to key in a name for the VPN policy server and press *OK*. You can choose any policy server name, but it must be unique in the VPN policy servers view.

If you leave this field empty, Policy server addr. appears 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.

3 Select *Policy server addr.*, key in the host name or IP address of the VPN policy server to install VPN policies from, and press *OK*.
You can also specify a port number, separated with a colon (:).
You receive the policy server address from administrators.

4 Select *Internet access point*, associate the VPN policy server with an access point, and press *OK*.
The access point is used to connect to this VPN policy server.
Administrators tell you which access point to select.

Glossary: Synchronising means that a VPN policy server is checked for new, updated, or removed VPN policies.

5 Press *Back* to save the VPN policy server settings.

6 Press *Yes* when you are prompted to **sychronise** the VPN policy server.
You are prompted to verify the identity of the VPN policy server.
You receive a VPN policy server identity code from administrators.

7 Carefully compare the VPN policy server identity code that is displayed with the code that you receive from administrators, key in the missing characters in the field, and press *OK*.

Glossary: A policy server user name and password help protect the VPN policy server from unauthorized access.

8 Key in your **user name** in *Policy server user name* and **password** in *Policy server password* to authenticate to the VPN policy server and press *OK*.
Administrators tell you the user name and password to key in.

A certificate is enrolled for subsequent authentication to the VPN policy server and VPN policies are installed on the mobile device.

You can now create VPN access points and associate them to applications. For more information, see "Creating VPN access points" on page 17.

Editing VPN policy servers

Select a VPN policy server in the *VPN policy servers* view to view or change the settings for the VPN policy server.

Select *Policy server name* to key in a new name for the policy server. The *VPN policy servers* view shows the new name.

You cannot change *Policy server addr.* after you install VPN policies from the VPN policy server, because the VPN policy server sends the address during the first connection.

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

Synchronising VPN policy servers

Select a VPN policy server in the *VPN policy servers* view, press *Options*, and select *Synchronise server* to install and update policies from the VPN policy server. The VPN policy server is checked for 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 to the mobile device. If administrators deleted VPN policies from the VPN policy server, the VPN policies are removed from the mobile device.

When you synchronise a VPN policy server for the first time, a matching VPN access point is created for each VPN policy that you install on the mobile device. You can create and edit VPN access points in the *VPN access points* view.

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

A certification request is created for each required certificate and sent to the VPN policy server. The VPN policy server enrolls each requested certificate from a **certification authority** (CA).

The certification request and the corresponding certificate contain your user identity. Depending on the VPN policy server configuration, the VPN policy server user identity might be used also as the user identity in VPN certificates. If this is not possible, you are asked for your user identity for a particular domain.

To create certification requests

1 Key in your certificate user identity for the specified domain in *User identity for*. Administrators tell you what information to key in.
2 Press *OK*.

Deleting VPN policy servers

To delete a VPN policy server, select the VPN policy server in the *VPN policy servers* view and press the clear key.

Confirm the deletion of the VPN policies that you installed from the VPN policy server.

5. 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.

Go to *Menu* and select *Tools* > *Settings* > *Connection* > *VPN* > *VPN access points*.

Viewing VPN access points

The *VPN access points* view lists VPN access points that you create on the mobile device. The text *(no VPN access points)* means that you have not created VPN access points. To create a new VPN access point, press *Options* and select *New access point*.

Select a VPN access point and then select *Options* > *Edit* to view and edit the following information:

- *Connection name*—identifies the VPN access point in access point lists.
- *VPN policy* —name of the VPN policy that is associated with the VPN access point.
- *Internet access point*—name of the access point over which the VPN connection is created.
- *Proxy serv. address*—address of a proxy server in the enterprise network.
- *Proxy port number*—port number to connect to the proxy server.

Creating VPN access points

The first time you open the *VPN access points* view, you are prompted to create VPN access points. Press *Yes*.

Tip! If you specify a proxy server in the VPN access point settings, you do not have to specify the proxy server in the Internet browser settings.

To create VPN access points

1 Press *Options* and select *New access point*.
2 Select *Connection name* to change the name of the connection. You can choose any connection name.
3 Select *VPN policy* to define how the connection is encrypted. If the list is empty, you must install VPN policies from SIS files or VPN policy servers.
4 Select *Internet access point* to select an access point to use for the VPN connection. If the list is empty, you must create access points.
5 Select *Proxy serv. address* to key in the address of a proxy server in the enterprise network.
6 Select *Proxy port number* to change the default port, 80.

Deleting VPN access points

To delete a VPN access point, select a VPN access point in the *VPN access points* view and press the clear key.

6. VPN log

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

Go to *Menu* and select *Tools* > *Settings* > *Connection* > *VPN* > *VPN management* > *VPN log*.

Icons: for errors, for warning, and for description.

Viewing the VPN log

The *VPN log* view shows the version number of VPN Client.

You can view the message type, the time of each message, and the beginning of the log message. Select a log message to view the complete log message.

The *VPN log* view sorts log messages by time and date, most recent messages first. You can view messages up to the time when you opened the *VPN log* view. Press *Options* and select *Refresh log* to view the most recent log messages.

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

Clearing the VPN log

Log messages are recorded to a circular buffer. When the log size reaches 20 kilobytes, new log messages replace the oldest log messages.

To delete all log messages from the log and to clear the *VPN log* view, press *Options* and select *Clear log*.

7. Key store passwords

Go to *Menu* and select *Tools* > *Settings* > *Connection* > *VPN* > *VPN management* > *Key store password*.

A key store password helps protect private keys in the mobile device 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. If attackers guess or crack a key store password, they can use the mobile device to access the enterprise network that the VPN helps protect. Thus, you must create key store passwords that are long enough to be difficult to crack. Make sure to keep your password secret. Do not write down passwords.

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

To create or change the key store password:

1. In *New key store password*, key in a password that is easy for you to remember but difficult for anyone else to guess.
2. Select *Verify password* and key in the password again to omit typing errors.
3. Press *OK* to create the password.

Entering key store passwords

You are prompted to 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.

Note: When you key in passwords, predictive text input is off. Key in the characters one by one. The characters are written in lower case by default.

8. VPN and applications

When you use an application to create a VPN connection, VPN client performs the following tasks:

- 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 network. 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 mobile device negotiates encrypted connections with the VPN gateway.

To authenticate to a VPN gateway

1 Key in your VPN user name in *VPN user name*.

2 Key in your VPN password or passcode:
   - Key in your password in *VPN password*.
   - Generate a SecurID passcode, key in the passcode in *VPN passcode*, and press *OK*.

3 If the SecurID token becomes 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.
Generate and key in a new passcode in *Next passcode*.
If this fails, contact administrators.

4 Press *OK*.

9. Troubleshooting

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

Message	Cause	Action
Authentication failed. Check user name and password.	• 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.	• Check your user name and password and try again. • Wait until the passcode in the SecurID token display changes, and key in the passcode.
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.

Message	Cause	Action
Incorrect server identity code.	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.
Policy server is currently in use. Unable to delete.	You cannot delete a VPN policy server while you update VPN policies from the server. When you use an application to create a VPN connection, VPN policies are automatically updated.	Wait until VPN policies are updated and try again.
Unable to activate VPN connection. Update VPN policy first.	• Legacy authentication failed. • The certificate that you use to authenticate to the VPN gateway is missing, expired, or its validity period has not begun yet.	• Check your user name and password and try again. • Select a VPN policy in the in the *VPN policies* view, press *Options*, and select *Update policy* to update the VPN policy. • Check the date and time settings on the mobile device.

Message	Cause	Action
Unable to log on to policy server. Delete server and redefine details.	The server certificate of the VPN policy server expires.	In the *VPN policy servers* view: **1** Press *Options* and select *Delete server* to delete the VPN policy server. **2** Press *Options* and select *New server* to add the VPN policy server again, or ask the administrator for a SIS file that contains new settings for the VPN policy server.
Unable to log on to policy server. Enter policy server user name and password.	The certificate that authenticates you to the VPN policy server expires or administrators revoke the certificate.	• Report this error to administrators. They give you a one-time password for logon. • Key in the user name and one-time password to authenticate to the VPN policy server. • A new certificate is enrolled for you.

Message	Cause	Action
Unable to log on to policy server. 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.
• *Unable to update policy. See VPN log for details.* • *Unable to synchronise. See VPN log for details.*	An error occurs while VPN policies download from the VPN policy server or installed on the mobile device.	• In the *VPN policies* view, select a VPN policy, press *Options*, and select *Update policy* to update a VPN policy. • In the *VPN policy servers* view, select a VPN policy server, press *Options*, and select *Synchronise server* to install policies from the VPN policy server.
VPN policy deleted. Try redefining VPN access point.	The VPN policy that was associated with the VPN access point was deleted because the VPN policy was obsolete.	In the *VPN access points* view, select a VPN access point, press *Options*, and select *Edit* to associate another VPN policy with the VPN access point

Index