Nokia E61i

NOKIA
Eseries

Nokia E61i
Mobile VPN Client User's Guide

Mobile VPN Client User's Guide

Select *Menu* > *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 connection, a VPN gateway and the mobile device authenticate each other and negotiate encryption and authentication algorithms to help protect the privacy and integrity of the information you access.

Managing virtual private networking

To create VPN connections, you first connect to a VPN policy server to install VPN policies and VPN access points. Then you select a VPN access point whenever you use an application and want to connect to the enterprise network. The VPN connection to the enterprise network 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 need VPN policy server settings from your administrator.

To use virtual private networking

1 Connect to a VPN policy server.
See "Connecting to VPN policy servers" on page 7.

2 Install VPN policies from the VPN policy server.
See "Installing VPN policies" on page 4.
The VPN policy server automatically installs a VPN access point, specifying an Internet access point and a VPN policy to use with the access point.

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.

3 When using an application, select a VPN access point to connect to the enterprise network.
See "VPN and applications" on page 10.
A VPN connection is created on top of the Internet connection.

VPN policies

Select *Menu* > *Tools* > *Settings* > *Connection* > *VPN* > *VPN management* > *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. You install VPN policies from a VPN policy server. A VPN policy server is a Nokia Security Service Manager (Nokia SSM).

Installing VPN policies

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

To install VPN policies

1 Go to an empty *VPN policies* view, and press *Yes* when you are asked to install VPN policies.
2 Press *Yes* when you are asked to add VPN policy servers.
3 Specify the settings for connecting to a VPN policy server.
- *Policy server name*—enter a name for the VPN policy server. You can specify any name for the policy server, but it must be unique in the VPN policy servers view. If you leave this field empty, *Policy server addr.* appears in the field.
- *Policy server addr.*—enter the 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 get the policy server address from the administrator.
- *Internet access point*—associate the VPN policy server with an access point. The access point is used to connect to this VPN policy server.

  You get the access point information from the administrator.

4 Press *Back* to save the VPN policy server settings.
5 Press *Yes* when you are asked to **synchronise** the VPN policy server.

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

6 Create a **key store password**.

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

See "Creating or changing a key store password" on page 9.

You are connected to the VPN policy server.

7 Verify the identity of the VPN policy server. You receive a VPN policy server identity code from the administrator. Carefully compare the displayed VPN policy server identity code with the code that you have received from the administrator, enter the missing characters in the field, and press *OK*.

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

8 Enter your **user name** in *Policy server user name* and **password** in *Policy server password* to authenticate to the VPN policy server, and press *OK*.

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

You get the user name and password from the administrator.

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.

Note that you can also install VPN policies by adding a VPN policy server and then synchronising it. To do this, select *Menu* > *Tools* > *Settings* > *Connection* > *VPN* > *VPN management* > *VPN policy servers* > *Options* > *New server*.

Viewing VPN policies

The *VPN policies* view lists the VPN policies that you have installed 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 about the VPN policy. An administrator defined the description when the VPN policy was created.
- *Policy status*—indicates whether the VPN policy is ready to use or whether it is already in use.
- *Certificate status*—indicates whether or not valid user certificates are available on the mobile device.
- *Policy name*—the name an administrator gave to the VPN policy when the VPN policy was created.
- *Policy server*—the name of the VPN policy server from which you installed the VPN policy.
- *Updated*—the date when the VPN policy was last updated from the VPN policy server.

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 a 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 may 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 it with a VPN access point. In the *VPN policies* view, press *Options* and select *Define VPN ac. point*.

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.

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 the administrator has created a new version of the VPN policy, the new version is installed on the mobile device. If the administrator has 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 the administrator has deleted 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.

VPN policy servers

Select *Menu* > *Tools* > *Settings* > *Connection* > *VPN* > *VPN management* > *VPN policy servers*.

You 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 the VPN policy servers with the mobile device. For more information, see "Synchronising VPN policy servers" on page 7.

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.

Viewing VPN policy servers

The *VPN policy servers* view lists VPN policy servers that you have defined.

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

Editing VPN policy servers

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

Select *Policy server name* to enter 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 have 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 have 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 the administrator has 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 may 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 may be used also as the user identity in VPN certificates. If this is not possible, you are asked to enter your user identity for a particular domain.

To create certification requests

1. Enter your certificate user identity for the specified domain in *User identity for*.
   You get this information from the administrator.
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 have installed from the VPN policy server.

VPN access points

Select *Menu* > *Tools* > *Settings* > *Connection* > *VPN* > *VPN access points*.

A VPN access point is a virtual access point that combines a VPN policy and an Internet access point. VPN access points are automatically created when you install VPN policies.

To create a VPN connection, select a VPN access point in the Internet access point list.

Viewing VPN access points

The *VPN access points* view lists VPN access points that you have created on the mobile device. The text *(no VPN access points)* means that you have not created any 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*—the name of the VPN policy that is associated with the VPN access point.
- *Internet access point*—the name of the access point over which the VPN connection is created.
- *Proxy serv. address*—the address of a proxy server in the enterprise network.
- *Proxy port number*—the port number to connect to the proxy server.

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.

VPN log

Select *Menu* > *Tools* > *Settings* > *Connection* > *VPN* > *VPN management* > *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.

Viewing the VPN log

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

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

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, with the 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 the administrator 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*.

Key store passwords

Select *Menu* > *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 unauthorised use.

Creating or changing a key store password

You create a key store password when you install the first VPN policy. If an attacker guesses or cracks a key store password, he can use the mobile device to access the enterprise network that the VPN helps to protect. Thus, you must create a key store password long enough so it cannot be cracked easily. Make sure to keep your password secret. Do not write the password down.

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

Entering key store passwords

You are asked 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 enter passwords, predictive text input is off. Enter the characters one by one. The characters are written in lower case by default.

VPN and applications

When you use an application and want to create a VPN connection, select a VPN access point instead of an Internet access point. The 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 must prove your identity when you log on to the enterprise network. The VPN policy determines the authentication method you need to use:

- Certificate-based authentication—You need a certificate signed by a trusted certification authority. You use online certificate enrollment to obtain the certificate.
- Legacy authentication—You need a user name and a passwords or passcode. The administrator creates the credentials or gives you SecurID tokens for generating the passcode.

If you are using certificates for authentication, enter the key store password.
If you are using legacy authentication, enter VPN authentication information when you are using an application that connects to a VPN access point, and the mobile device negotiates encrypted connections with the VPN gateway.

To authenticate to a VPN gateway

1 Enter your VPN user name in *VPN user name*.
2 Enter your VPN password or passcode:
   - Enter your password in *VPN password*.
   - Generate a SecurID passcode, enter the passcode in *VPN passcode*, and press *OK*.
3 If the SecurID token is not in sync with the clock of the ACE/Server, you are asked for the next passcode that the ACE/Server uses as a new reference for the time base of the token. Enter a new passcode in *Next passcode*.
   If this fails, contact the administrator.
4 Press *OK*.

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 enter an incorrect user name or password when you authenticate to a VPN policy server or log on to a VPN. • You enter the wrong passcode when you are asked for the Next passcode.	• Check your user name and password and try again. • Wait until the passcode in the SecurID token display changes, and enter the passcode.
Incorrect password.	You enter an incorrect key store password or key import password.	• Check the password and try again. • You receive the key import password from the administrator. You create the key store password yourself.
Incorrect server identity code.	You enter an incorrect string when you are asked to enter the VPN policy server identity code.	Check the VPN policy server identity code carefully against the code that you receive from administrators and enter 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.

Message	Cause	Action
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.
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.
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 the administrator revokes the certificate.	• Report this error to the administrator. He gives you a one-time password for logon. • Enter the user name and one-time password to authenticate to the VPN policy server. • A new certificate is enrolled for you.
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.

Message	Cause	Action
• *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.