

movianVPN™

Version 3.0

movianVPN User's Guide for Nokia Series 60 Mobile Phones

Nokia 3650/7650 phones.

PUB-0200-2001
May 29, 2003

© Certicom Corp. 2001-2003. All rights reserved.

Certicom(R), Certicom logos, movian (tm), movianVPN (tm) are trademarks of Certicom Corp. The movianVPN is covered by one or more of the following U.S. Patents: 6,078,667, 6,049,815, 5,999,626, 5,955,717, 5,933,504, 5,896,455, 5,889,865, 5,787,028, 5,761,305, 5,600,725, 4,745,568, 6,097,813, 6,122,736, 6,134,325, 6,141,420, 6,178,507, and 6,195,433.

Other applications and corresponding foreign protection pending.

Certicom Corp.
5520 Explorer Drive,
4th Floor,
Mississauga, Ontario,
Canada, L4W 5L1
905.507.4220



All information contained in this document is the sole property of the Certicom Corp and is licensed to you for your internal use only with movian products. Such document is provided "as is" without warranty or conditions of any kind, either express or implied, including, but not limited to, the implied warranties or conditions of merchantability, fitness for a particular purpose, or non-infringement. Certicom disclaims any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, procedure, method, apparatus, product, or process posted here. Neither Certicom, its employees, nor its associates assumes any responsibility for loss or damages resulting from the use of information contained in the documentation. Certicom assumes no responsibility for errors or omissions in this documentation. With respect to only limitation of direct damages, unless specifically stated otherwise in a license agreement executed between you and Certicom, you agree that any liability on the part of certicom for breach of the warranties contained herein or any of the other provisions of this agreement or any other breach giving rise to liability or in any other way arising out of or related to this agreement for any cause of action whatsoever and regardless of the form of action (including breach of contract, strict liability, tort including negligence or any other legal or equitable theory), shall be limited to your direct damages in an amount not to exceed one (\$1.00) us dollar you agree that in no event will Certicom be liable for damages in respect of incidental, ordinary, punitive, exemplary, indirect, special, or consequential damages even if Certicom has been advised of the possibility of such damages including, but not limited to, business interruption, lost business revenue, lost profits, failure to realize expected savings, economic loss, loss of data, loss of business opportunity or any claim against you by any other party. Because some jurisdictions do not allow the limitations on implied warranties or the exclusion or limitation of liability for consequential or incidental damages, the above limitations may not apply to you.

By using this documentation, you agree to be bound by the terms as stated herein. If you do not accept these terms and conditions, you must delete this document and not make any use of it. Additional terms and conditions may apply to you as per the software license agreement that you may have executed with Certicom.

Copyright Notice

© Certicom Corp. 2000, 2001, 2002,2003. All rights reserved. This documentation contains Certicom's proprietary information and any use and distribution are limited to authorized licensees of Certicom. Any unauthorized use, reproduction, and distribution of this documentation is strictly prohibited by law.

| | |
|--|----|
| Introduction | 1 |
| Overview: movianVPN | 1 |
| Using this document | 2 |
| VPNs | 3 |
| Gateway servers | 3 |
| IPSec | 4 |
| Handheld devices | 4 |
| movianVPN | 6 |
| Gateway access | 6 |
| Interoperability | 7 |
| Supported devices | 7 |
| VPN gateways currently supported | 7 |
| Connections | 7 |
| Installing movianVPN | 9 |
| System requirements | 9 |
| Checking the movianVPN version number | 10 |
| Licensing movianVPN | 11 |
| Licensing movianVPN | 11 |
| Checking the current license type | 11 |
| Getting updates for movianVPN | 11 |
| Uninstalling movianVPN | 12 |
| Getting Started | 13 |
| Overview: Getting Started | 13 |
| Providing a policy for your gateway | 14 |
| Information required for creating a policy | 14 |
| Creating a policy for a Cisco VPN Concentrator 3000 gateway | 15 |
| Creating a policy for a Nortel Contivity Series gateway | 18 |
| Creating a policy for Cisco Unity with a Cisco 3000 v3.0 gateway | 22 |
| Verifying your policy | 25 |
| Policy window checkboxes | 25 |
| Policy gateway access settings | 27 |
| Running movianVPN | 29 |
| Overview: Running movianVPN | 29 |
| Logging in to the gateway | 30 |
| Contacting the gateway | 30 |
| Authentication and Key Negotiation | 30 |
| Using movianVPN | 32 |
| Working with applications | 32 |
| Logging out of the gateway | 33 |
| Appendix A: | |
| Troubleshooting and using the Diagnostic Tools | 35 |
| Troubleshooting | 35 |

| | |
|---------------------------------------|----|
| Using the diagnostic tools | 36 |
| Ping | 36 |
| View IPSec Status. | 36 |
| View IPSec Policy | 37 |
| View IKE Log. | 38 |
| Connection (socket) options | 38 |

Appendix B:

| | |
|-----------------------------|----|
| Glossary of Terms | 39 |
|-----------------------------|----|

Appendix C:

| | |
|--------------------------------|----|
| Information worksheet. | 43 |
|--------------------------------|----|

| | |
|---|----|
| Information required for client configuration | 43 |
| Information required for creating a policy | 44 |

1

Introduction

Overview: movianVPN

For mobile professionals, owning a handheld personal computer such as a PDA or an advance cell phone means that downloading e-mail and accessing the Internet can occur anyplace, anytime. More difficult, however, is ensuring security when using a handheld device to remotely access confidential information on the corporate intranet.

movianVPN is a software application that allows mobile professionals to use their phones to connect securely to their corporate intranet, whether remotely or on-site at their company. The corporate intranet or VPN (Virtual Private Network) is accessed through a gateway server the user connects to by wireline dial-up or wireless access.

Once a user is logged in to the VPN gateway, information sent in each direction is encrypted and verified. The communicating parties are authenticated, ensuring confidentiality and integrity of the data. Authorized users have secure, real-time access to critical data and application servers behind the gateway, such as e-mail servers.

movianVPN can be downloaded from the **www.certicom.com** website and installed on your computer. The next time you synchronize your handheld device with the computer, the necessary files will be installed on the device.

The application is simple to use, with only a few steps to follow.

To use **movianVPN**, you will require:

- A phone or handheld device capable of connection to an Internet Service Provider or to a wireline or wireless LAN
- Information from your VPN administrator regarding the configuration required for your specific VPN gateway

Using this document

This User's Guide is intended for the **movianVPN** user with a Symbian/Nokia Series 60 mobile phone (Nokia models 3650 and 7650). It provides information on:

- VPNs and handheld devices
- Installing **movianVPN**
- Creating and verifying the policies used to connect to VPN gateways
- Accessing and using the gateway
- Diagnostic tools and troubleshooting

If your VPN administrator has already completed a particular chapter's procedures for installing and configuring **movianVPN** on your handheld device, you can move on to the next chapter.

VPNs

Virtual Private Networks (VPNs) are secure private networks operating either within a public network like the Internet or within an insecure private network.

A VPN links together particular computers within the wider network and provides authorized users with secure, confidential transmission of data. Security is maintained by encrypting communications and by creating secure "tunnels" to direct network traffic from one computer to another specific computer.

VPNs can create secure connections between an internal corporate network and external users in any combination of the following three forms:

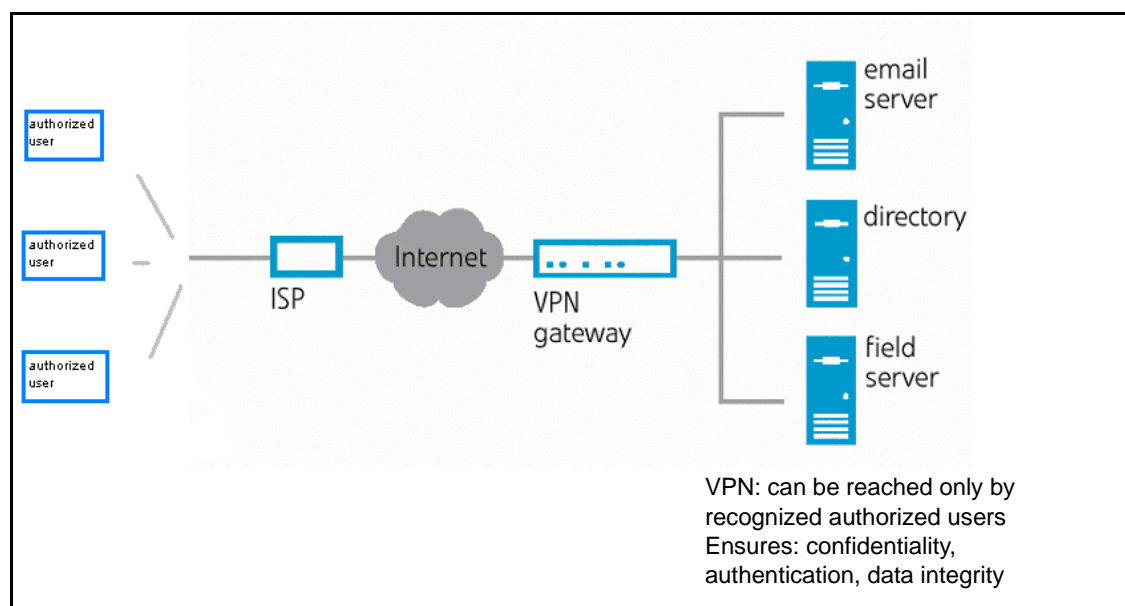
- **Intranet VPN:** Between a central corporate site and branch offices
- **Remote access VPN:** Between a central corporate site and individual remote users (the **movianVPN** model)
- **Extranet VPN:** Between an enterprise and its business partners, suppliers, and customers

VPNs provide a cost-effective means for secure e-mail access and functions such as sharing confidential information, updating databases for remote offices, and disseminating business applications.

Once you are logged in to a VPN, you can access the servers within the VPN, while other Internet or intranet users outside the VPN are unable to access the VPN and its subnets or enclosed networks.

Gateway servers

The VPN is accessed through a "VPN gateway server," a computer which recognizes authorized users and their passwords. The gateway server gives users access to the application servers for e-mail and other confidential information behind the gateway (that is, access to servers within the corporate intranet that have been designated as part of the VPN).



Secure access is provided through a combination of:

- Tunneling (directing encrypted communication and routing instructions from one computer to another specific computer using TCP/IP protocols)
- Encrypting data, and
- Using authentication technologies that verify the identity of the sender, the identity of the receiver, and the security of the information transmitted

A VPN must provide a reliable, secure communication between all hardware and software points of the VPN: the IPSec protocol makes this possible.

IPSec

The IPSec protocol is a framework of standards for network security, aimed at providing confidentiality, data integrity, and data source verification for any application using the network.

IPSec protocol ensures that:

- Communicating parties can authenticate both the source and the integrity of the data
- The data is encrypted for secure exchange
- The method of authentication and encryption can be negotiated by the communicating parties

Handheld devices

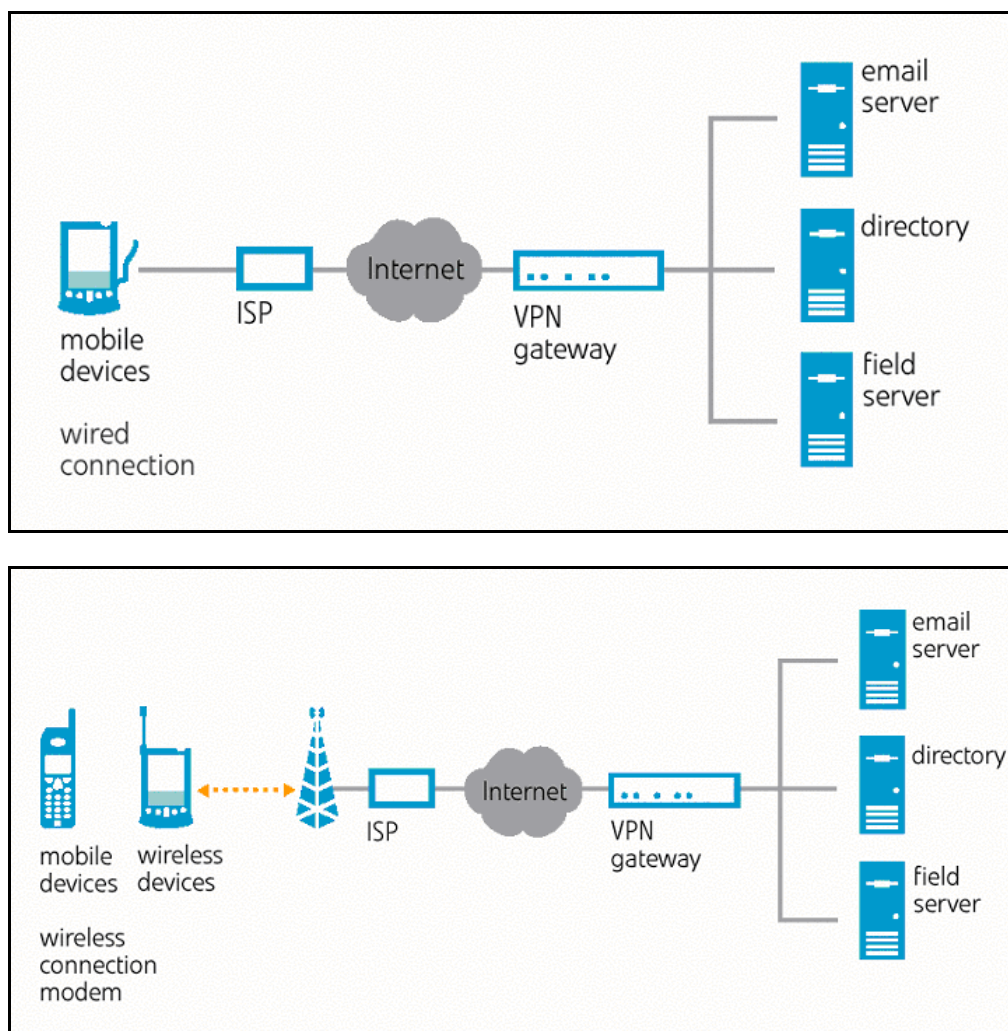
Using **movianVPN**, a traditional VPN can also have handheld devices added to the configuration.

Handheld devices can connect to the VPN by several options:

- Dedicated dial-up modem to access an ISP through the telephone network
- Wireless modem to access a Local Area Network or LAN
- Wireline (Ethernet) access to a LAN
- Modem with data-capable mobile phone to access the ISP

To access the VPN, the handheld device must support the standard IP or Internet Protocol, which addresses and sends information packets over the network.

Handheld devices can connect to the VPN by a wired connection or by a wireless connection, depending on the devices' hardware/software configuration.



For information on the handheld devices and operating systems that can use **movianVPN**, see “Interoperability” on page 7.

movianVPN

movianVPN allows mobile professionals to use their handheld devices to connect securely and easily to a corporate intranet's VPN gateway. The handheld can then be used to access the corporate intranet, providing you with secure, real-time access to confidential data and application servers behind the gateway, such as e-mail servers.

movianVPN uses IPSec standards to establish a secure end-to-end connection. The process for an IPSec-based communication works as follows:

- When your handheld device contacts the VPN gateway server to establish a connection, the "client" (that is, the part of the software resident on your handheld device) and the server identify themselves to each other.
There are several possible authentication methods, including passwords for the username you login with and tokens for two-factor authentication.
- Once the authentication is complete, the client generates a "key" and shares it with the VPN gateway server to use for the length of that session.
- When the client accesses data from the VPN, the gateway server encrypts the data, using the session key. The encrypted data travels securely across the Internet to the client, where it is decrypted with the same key.
Encryption is the process of converting a text or other communication into a coded format which cannot be read by other parties unless decrypted. Encryption and decryption relies on shared keys.

Gateway access

Gateways are accessed using a security "policy" configured within **movianVPN**. The policy contains the information required to connect to a specific gateway and to successfully negotiate the exchange of keys that will be used for encrypting the transmitted data, verifying identities, and confirming data integrity.

The network you use to access the VPN gateway server does not have to be secure. For example, you may use dial-up access to an Internet Service Provider to reach the gateway server, or access it through a wider corporate LAN.

Once you are recognized by the VPN gateway through providing your user name and password, **movianVPN** establishes a secure, encrypted "tunnel" for you to the VPN. While accessing the servers that comprise the VPN, you are provided with confidentiality, data integrity verification, and data source authentication for your communications.

A policy requires specific information from your VPN administrator regarding connection and encryption protocols, user names and passwords for authentication, and configuration modes for the particular type of gateway.

Interoperability

Supported devices The Nokia 3650 and Nokia 7650 devices are supported.

VPN gateways currently supported The following VPN gateways are currently supported:

| Company | Product | Software Version |
|----------------|----------------------------------|--------------------------------------|
| Cisco | VPN Concentrator 3000 Series | 3.0 to 3.5, limited 2.5.2E, 2.5, 2.1 |
| | Cisco Unity with Cisco 3000 v3.0 | |
| Nortel Network | Contivity VPN Switch series | 2.60.56 to 3.6.0 and 4.0 |

Connections The following specific connections have been tested for interoperability:

- GSM
- GPRS

Before you can use movianVPN on your phone, you need to create an Internet Access Point (IAP). You can do this through the **Tools** folder on the phone, using the **Settings** > **Connection** command. You can set up multiple IAPs, either GSM or GPRS. If you have more than one IAP, you will be prompted to choose an IAP when you log in though **movianVPN**.

2

Installing movianVPN

System requirements

To install and run **movianVPN**, you should have the following as a minimum:

- PC Suite for Nokia 3650/7650 software on your desktop or laptop computer
- Symbian OS for Nokia Series 60 on your Nokia 3650/7650 device

To connect to a VPN, you will also require:

- Account with an Internet Service Provider (ISP) and/or wireless data provider

movianVPN is contained in a zip file. To install **movianVPN**, follow the steps below.

- Extract the files to a designated folder.
- Double-click on the SIS file to run the PC Suite for Nokia 3650/7650 application.
- Follow the instructions on the screen to install **movianVPN** on the Nokia device.

Note that if you have a previous version of **movianVPN** on your device, it will be overwritten during the installation process. Your existing policies will be retained.

Checking the movianVPN version number

To resolve questions or issues more quickly when receiving technical support, you should be able to supply the **movianVPN** version number.

To check your **movianVPN** version number:

1. Open the **movianVPN** application. To open the **movianVPN** application, you may have to press the menu key and then select the **movianVPN** application using the scroll key. The **movianVPN** window will appear.



2. Select **Options** by pressing the left selection key, then select **About** on the menu toolbar using the scroll key.



3. Select **movianVPN** in the list.

The **About movianVPN** window appears.

Scroll down to display the **movianVPN** version and build number. You will need this information if you need to contact technical support.



Licensing movianVPN

The **movianVPN** evaluation license expires after a period of 30 days. In the final ten days of the evaluation period, you will see a message informing you that the license will expire soon.

To activate **movianVPN** for a longer period, you must license the application with Certicom.

Licensing movianVPN

To obtain a licensed version of **movianVPN**, visit our website at www.certicom.com/buymovian and contact one of our channel partners.

Once you purchase a license, you will receive a **.sis** file. When you run this file, it will install a license file on your handheld device. The license takes effect when you restart **movianVPN**.

Note: You must ensure that you install the license in the same directory as **movianVPN**.

Checking the current license type

To check on which type of license you currently have for **movianVPN** and when it expires:

1. Open the **movianVPN** application. The **movianVPN** window will appear.
2. Press the **Menu** key on the keyboard, then select **About** on the menu bar.
3. Select **License**. The **movianVPN License** window appears.

The **movianVPN License** window shows the current information on whether the installation is licensed or for evaluation, the number of licenses, and the days remaining. Select **Close** to close the window.



Getting updates for movianVPN

To download updates for **movianVPN**, visit our website at www.certicom.com and contact one of our channel partners.

Uninstalling movianVPN

To uninstall **movianVPN**, use the Install/Remove application on your handheld device.

1. Press the menu button on your device. Select the Tools folder.
2. Select the **Manager** application.
3. Select **movianVPN**.
4. Select **Remove** from the menu.

Note that if you install a new version of **movianVPN** using the PC Suite for Nokia Communicator application, the previous version of **movianVPN** is overwritten automatically. However, the old policies will only be deleted if you remove the old version of **movianVPN** first.

3 Getting Started

Overview: Getting Started

Getting started with **movianVPN** requires that you have the information necessary to complete both of the following:

- Set up your device to connect to the Internet
- Create the policy for your gateway

Your device documentation will explain what you need to do to connect your device to the Internet. This chapter explains how you create a policy for your gateway.

Note that your VPN administrator may already have configured your handheld device to connect to the Internet and created the policy. If this is the case, you can begin “Running movianVPN” on page 29.

Your administrator may have created a policy configuration file, with **movian Deployment Manager (movianDM)**, a Windows application. You must load the **.sis** policy file onto your device using PC Suite. The next time you run **movianVPN**, it will detect the new policy file and ask if you would like to install it. You may also need a password, if the policy file is encrypted. For more information, consult the **movianDM** documentation.

Providing a policy for your gateway

movianVPN supports access to the gateways listed in the table “VPN gateways currently supported” on page 7.

Note: To create a policy for your gateway, you will require specific information supplied by your VPN administrator. This information may be supplied to you in the table that follows or in a form such as that shown in “Appendix C: Information worksheet” on page 43.

Information required for creating a policy

The following information will be required as you create the policy for your gateway. The information must be entered in a field, selected from a pull-down list, or selected/deselected using checkboxes.

Note: Not all entries will be applicable for your gateway’s policy.

| Field, Checkbox or Button | Required | Information/Action |
|---|----------|--------------------|
| Policy Name | | |
| Gateway Type (Please select one) | | |
| Gateway IP Address | | |
| Perfect Forward Secrecy | | |
| Extended Authentication (Nortel gateway only) | | |
| IKE Suite | | Group: |
| | | Cipher: |
| | | Hash: |
| Group Name | | |
| Group Password | | |
| User Name | | |
| User Password | | |
| User Passcode (SecurID) | | |
| IPSec Suite | | |

Creating a policy for a Cisco VPN Concentrator 3000 gateway

To create a policy for a Cisco VPN Concentrator 3000 gateway you will require the following information from your VPN administrator:

- Gateway IP address
- Select/deselect Perfect Forward Secrecy
- Group name, group password, user name
- IKE Suite and IPSec Suite settings

1. To start the **movianVPN** application, press the menu button, select the **movianVPN** icon, and press the scroll button to open. The **movianVPN** application window appears.
2. Open the **Options** menu using the select key, and then select **Policy** using the scroll key. Select **New** to create a new policy.



3. The **New policy** window appears. Each piece of information appears as its own item in the **New policy** list. Scroll down using the scroll key to select and fill in each field.
4. Select the policy name using the scroll key and set the name by pressing down on the scroll key. Enter the name of the policy in the **Policy Name** field. The policy name must be no more than ten characters long.



5. Select **Gateway type** using the scroll key to display a list of all the available gateways. Select the **Cisco VPN Concentrator 3** gateway and press the **OK** button to return to the **New policy** screen.

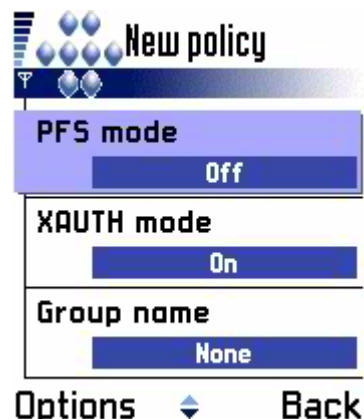


6. Select the **Gateway address** using the scroll key. Enter the IP address of the gateway in the **Gateway address** field. The IP address is supplied by your VPN administrator. When you have entered the IP address, press the **OK** button to return to the **New policy** screen.



7. Continue to scroll down to set the Perfect Forward Secrecy option if desired. Highlight the **PFS mode** item and toggle it from **Off** to **On**. For information on Perfect Forward Secrecy see “Perfect Forward Secrecy” on page 25.

*Note: The Extended Authentication **XAUTH Mode** option is selected by default and locked as required by the Cisco VPN Concentrator 3000 gateways. When you connect to the gateway, you will be asked for further authentication, supplied by your VPN administrator. For information on Extended Authentication, see “Extended Authentication” on page 25.*



8. Continue to scroll down to enter further information in the same manner. Enter the **Group Name**, **Group Password**, and **User Name** supplied by your VPN administrator.



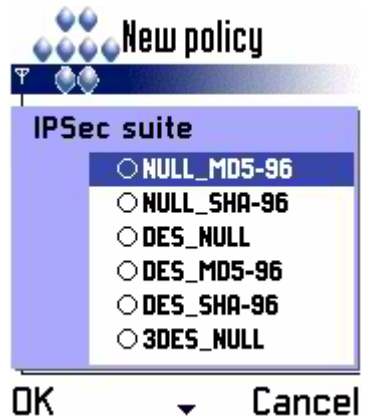
9. Next, scroll down to enter the IKE Options. Enter the **IKE group**, **IKE cipher** and **IKE hash** values (see “IKE Crypto Suite” on page 27 for more information on these settings).
10. Select **IKE Group** and set the Diffie-Hellman group. This information is supplied by your VPN administrator.
11. Select **IKE cipher** and set the cipher algorithm. This information is supplied by your VPN administrator.



12. Select **IKE hash** and set the hashing algorithm. This information is supplied by your VPN administrator.



13. Scroll down to **IPSec suite** and set the IPSec suite. This information is supplied by your VPN administrator (see “IPSec Crypto Suite” on page 28 for more information on this setting).



14. Scroll down to **SA Lifetime**. Set the lifetime of the security association. This information is supplied by your VPN administrator (see “SA (Security Association) Life” on page 28 for more information on this setting).



15. To complete the policy, select **Back**. Select **Yes** when prompted with **Save changes?** Your new policy is complete.



Creating a policy for a Nortel Contivity Series gateway

To create a policy for a Nortel Contivity Series VPN gateway you will require the following information from your VPN administrator:

- Gateway IP address
- Select/deselect Perfect Forward Secrecy
- Checkbox status and selected form of Extended Authentication
- A combination of group name, group password, user name and user password, depending on the authentication selected
- IKE Suite and IPSec Suite settings

1. To start the **movianVPN** application, press the menu button, select the **movianVPN** icon, and press the scroll button to open. The **movianVPN** application window appears.
2. Open the **Options** menu using the select key, and then select **Policy** using the scroll key. Select **New** to create a new policy.



3. The **New policy** window appears. Each piece of information appears as its own item in the **New policy** list. Scroll down using the scroll key to select and fill in each field.
4. Select the policy name using the scroll key and set the name by pressing down on the scroll key. Enter the name of the policy in the **Policy Name** field. The policy name must be no more than ten characters long.
5. Select **Gateway type** using the scroll key to display a list of all the available gateways. Select the **Nortel Contivity Series** gateway and press the **OK** button to return to the **New policy** screen.



6. Select the **Gateway address** using the scroll key. Enter the IP address of the gateway in the **Gateway address** field. The IP address is supplied by your VPN administrator. When you have entered the IP address, press the **OK** button to return to the **New policy** screen.

The screenshot shows a handheld device screen titled "New policy". At the top, there's a status bar with signal strength, a battery icon, and the number "123". Below the title, there's a section labeled "Gateway address" with a text input field containing "0.0.0.0". At the bottom of the screen are two buttons: "OK" and "Cancel".

7. Continue to scroll down to set the Perfect Forward Secrecy option if desired. Highlight the **PFS mode** item and toggle it from **Off** to **On**. For information on Perfect Forward Secrecy see “Perfect Forward Secrecy” on page 25.

The screenshot shows the "New policy" screen with three toggleable options. "PFS mode" is currently set to "Off". "XAUTH mode" is set to "On". "Group name" is set to "None". At the bottom, there are two buttons: "Options" with a small diamond icon and "Back".

8. Set the **Use Extended Authentication** option to On if the option is desired.

The screenshot shows the "New policy" screen with "PFS mode" set to "On" and "XAUTH mode" set to "On". The "XAUTH type" option is currently set to "Please select one". At the bottom, there are two buttons: "Options" with a small diamond icon and "Back".

9. Select the desired form of extended authentication, as directed by your VPN administrator.

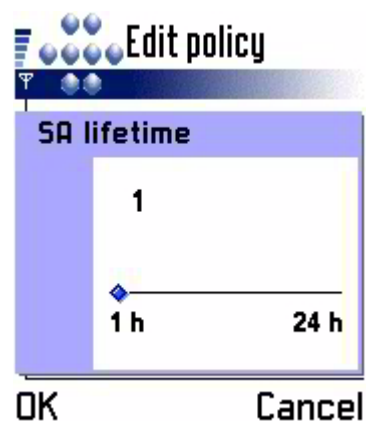
***Note:** When you log into the gateway, you will be asked to supply the selected form of extended authentication, supplied by your VPN administrator. For further information, see “Extended Authentication” on page 25.*

The screenshot shows the "New policy" screen with the "XAUTH type" section. There are two radio button options: "Username and P..." which is selected, and "SecurID". At the bottom, there are two buttons: "OK" and "Cancel".

10. Continue to scroll down to enter further information in the same manner. Enter the **Group Name**, **Group Password**, and **User Name** supplied by your VPN administrator.
11. Next, scroll down to enter the IKE Options. Enter the **IKE group**, **IKE cipher** and **IKE hash** values (see “IKE Crypto Suite” on page 27 for more information on these settings).
12. Select **IKE Group** and set the Diffie-Hellman group. This information is supplied by your VPN administrator.
13. Select **IKE cipher** and set the cipher algorithm. This information is supplied by your VPN administrator.
14. Select **IKE hash** and set the hashing algorithm. This information is supplied by your VPN administrator.
15. Scroll down to **IPSec suite** and set the IPSec suite. This information is supplied by your VPN administrator (see “IPSec Crypto Suite” on page 28 for more information on this setting).



16. Scroll down to **SA Lifetime**. Set the lifetime of the security association. This information is supplied by your VPN administrator (see “SA (Security Association) Life” on page 28 for more information on this setting).



17. To complete the policy, select **Back**. Select **Yes** when prompted with **Save changes?** Your new policy is complete.



Creating a policy for Cisco Unity with a Cisco 3000 v3.0 gateway

To create a policy for Cisco Unity with the Cisco 3000 v3.0 gateway, you will require the following information from your VPN administrator:

- Gateway IP address
- Select/deselect Perfect Forward Secrecy
- Group name, group password and user name
- IKE Suite, and IPSec Suite settings

1. To start the **movianVPN** application, press the menu button, select the **movianVPN** icon, and press the scroll button to open. The **movianVPN** application window appears.

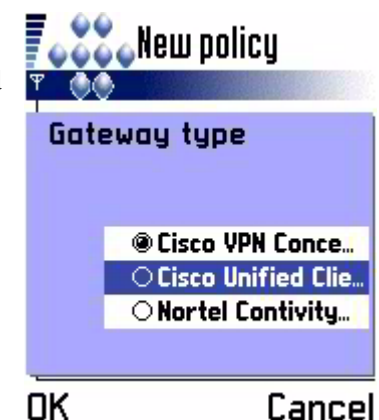
2. Open the **Options** menu using the select key, and then select **Policy** using the scroll key. Select **New** to create a new policy.

3. The **New policy** window appears. Each piece of information appears as its own item in the **New policy** list. Scroll down using the scroll key to select and fill in each field.

4. Select the policy name using the scroll key and set the name by pressing down on the scroll key. Enter the name of the policy in the **Policy Name** field. The policy name must be no more than ten characters long.

5. Select **Gateway type** using the scroll key to display a list of all the available gateways. Select the **Cisco Unified Client** gateway and press the **OK** button to return to the **New policy** screen.

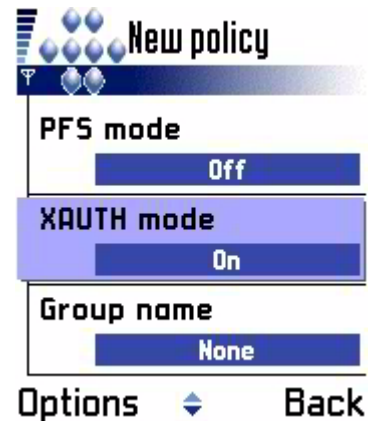
6. Select the **Gateway address** using the scroll key. Enter the IP address of the gateway in the **Gateway address** field. The IP address is supplied by your VPN administrator. When you have entered the IP address, press the **OK** button to return to the **New policy** screen.



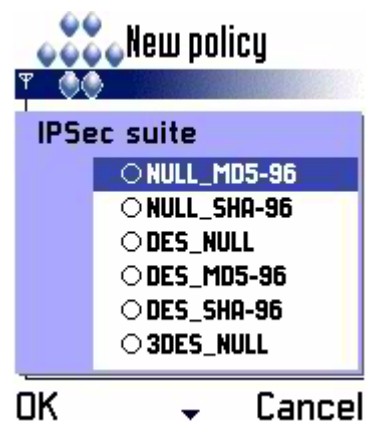
7. Continue to scroll down to set the Perfect Forward Secrecy option if desired. Highlight the **PFS mode** item and toggle it from **Off** to **On**. For information on Perfect Forward Secrecy see “Perfect Forward Secrecy” on page 25.

*Note: The Extended Authentication **XAUTH Mode** option is selected by default and locked as required by Cisco Unified Client gateways. When you connect to the gateway, you will be asked for further authentication, supplied by your VPN administrator. For information on Extended Authentication, see “Extended Authentication” on page 25.*

8. Continue to scroll down to enter further information in the same manner. Enter the **Group Name**, **Group Password**, and **User Name** supplied by your VPN administrator.
9. Next, scroll down to enter the IKE Options. Enter the **IKE group**, **IKE cipher** and **IKE hash** values (see “IKE Crypto Suite” on page 27 for more information on these settings).
10. Select **IKE Group** and set the Diffie-Hellman group. This information is supplied by your VPN administrator.
11. Select **IKE cipher** and set the cipher algorithm. This information is supplied by your VPN administrator.
12. Select **IKE hash** and set the hashing algorithm. This information is supplied by your VPN administrator.



13. Scroll down to **IPSec suite** and set the IPSec suite. This information is supplied by your VPN administrator (see “IPSec Crypto Suite” on page 28 for more information on this setting).



14. Scroll down to **SA Lifetime**. Set the lifetime of the security association. This information is supplied by your VPN administrator (see “SA (Security Association) Life” on page 28 for more information on this setting).



15. To complete the policy, select **Back**. Select **Yes** when prompted with **Save changes?** Your new policy is complete.



Verifying your policy

Once your policy is in place, you may need to review the settings and options.

Policy window checkboxes

When you start the movianVPN application, the policy you used in your last session is loaded by default. To switch to another policy, simply select the policy and with the scroll button.

To edit the policy, press the **Options** button on the keyboard and select **Policy** then **Edit** on the menu bar.

When you edit a policy, the **Edit policy** window will show you all the same options that you set when creating the policy.

You will be able to set or change most of these options. However, depending on your gateway, some options may be permanently set and locked. These options include the following:

- Perfect Forward Secrecy
- Extended Authentication

Not all settings or modes are available for each type of gateway; if your gateway does not support an option, the option will not be available.

Perfect Forward Secrecy

Perfect Forward Secrecy is a cryptographic characteristic associated with a derived Shared Secret value. With Perfect Forward Secrecy, if one key is compromised, previous and subsequent keys are not compromised, because subsequent keys are not derived from previous keys.

Perfect Forward Secrecy performs the key exchange twice as your handheld device negotiates with the gateway, using the same key material. A new key is created for each step of the Internet Key Exchange (IKE), and each new key is not derived from the previous key. The previous key or the one following are not compromised even if the current one is.

To set Perfect Forward Secrecy in your policy, set the PFS option to **On** in the movianVPN policy window.

Note that if Perfect Forward Secrecy is enabled, negotiation of the connection will take longer.

Extended Authentication

Extended Authentication requires the user to supply an additional password or another form of additional authentication when you log onto the gateway. Extended Authentication can be used to require an additional password or a



passcode associated with a token card, depending on the type of gateway. Extended Authentication is always required for some gateways. In those instances, Extended Authentication is selected and the option is disabled.

Other extended authentication methods

movianVPN also supports Safeword.



Policy gateway access settings

Each gateway may require specific settings to access the server. These settings are configured for each policy, depending on the gateway. Not all settings or modes are available to configure for each specific gateway.

The following may be configured on the client software, depending on your gateway:

- IKE Crypto Suite
- IPSec Crypto Suite
- SA Life

Note: Gateway settings should be set or changed as directed by your VPN administrator.

IKE Crypto Suite

IKE (Internet Key Exchange) Crypto Suite configures the preferred protocols for exchanging keys.

Note: If they must be set or changed, use the settings provided to you by your VPN administrator.

Group

Group refers to the strength of the key encryption negotiation.



Cipher

Ciphers are used to encrypt the data using Digital Encryption Standard (DES), 3DES, or the Advanced Encryption Algorithm (AES).



Hash

Hash numbers confirm that communicated data has not been changed during transmission. A hash number is generated for a particular set of data's characteristics, and sent along with the communication. When the communication is received, the hash number is generated again in the same way, and compared to the first.



IPSec Crypto Suite

IPSec settings are used to encrypt the data. The various settings represent the strengths of security, 3DES being the strongest while Null represents no encryption.

Note: If they must be changed, these settings will be provided to you by your VPN administrator.

SA (Security Association) Life

A security association describes the security policy negotiated between two communicating devices (in this case the client device and a gateway). This can include things such as the session keys and the encryption algorithms.

The security association has a limited lifetime. When a security association expires, the client device is logged out of the gateway. You must then attempt to log on to the gateway again to negotiate a new security policy.

You can set the security association lifetime in the policy settings. Note, however, that if the gateway has a set a shorter lifetime then this takes precedence over the setting on the client device.



4

Running movianVPN

Overview: Running movianVPN

Running movianVPN is a simple process of:

- Logging in to the VPN gateway
- While the **movianVPN** connection is established, using applications such as e-mail or the web browser as you normally would
- Logging out of the VPN gateway

Logging in to the gateway

When you attempt to login to the VPN gateway, the following actions occur:

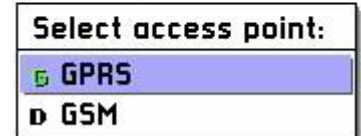
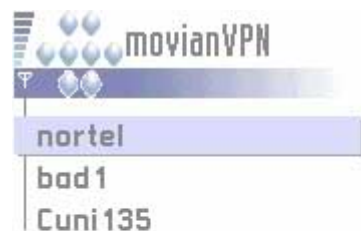
- **movianVPN** contacts the gateway
- The gateway prompts you for further authentication (if extended authentication is enabled)
- Keys are negotiated and accepted
- You are logged in to the gateway

Contacting the gateway

1. To start the **movianVPN** application, press the menu button, select the **movianVPN** icon, and press **Options**, and select the **Open** item from the list. The **movianVPN** application window appears. The last policy you created will be selected by default. To switch to another policy, simply scroll down to the desired policy using the scroll button.
2. Press the **Options** button, and from the list select **Login**. If you have multiple internet access points (IAPs) set up, you may be asked to choose between them. The example at right shows two IAPs, one called GPRS and one called GSM. **movianVPN** displays status messages as it attempts to connect to the gateway.



Select Cancel



Select Cancel



OK Cancel

Authentication and Key Negotiation

After **movianVPN** has contacted the gateway, depending on the gateway you may be asked for further authentication. The type of authentication requested depends on the gateway and the policy settings.

If requested, enter the password or SecurID passcode supplied to you by your VPN administrator.

When the connection to the gateway has been made, a message appears indicating that the IPSec tunnel has been established. At this point all the data between the mobile device and the gateway is encrypted.

If you experience difficulty while logging into the gateway, review your policy and connection type settings. Settings should be as directed by your VPN administrator. If after checking policy and connection type settings you are still unable to log in, contact your gateway administrator or support

team. You may wish to consult “Appendix A: Troubleshooting and using the Diagnostic Tools” on page 35.

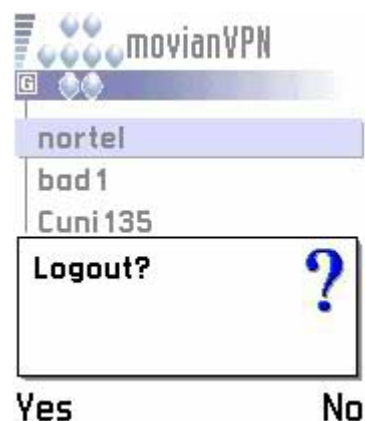
Using movianVPN

Once you have logged in to the gateway, you can leave movianVPN running in the background by pressing the **Exit** button. The application menu will appear, and you can start your email client or your web browser. All data to and from your email client, web browser and VPN servers will be securely encrypted until you log out again.

Working with applications

To access the web browser, press the **menu** key and select the **Browser** icon. Open the browser by pressing the **Options** button and then selecting **Open**.

To access the email client, press the menu key and select the **Messaging** icon. Open email by pressing the **Options** button and then selecting **Open**.



Logging out of the gateway

To log out of the gateway:

1. Bring the **movianVPN** window to the foreground.
2. Select the active policy (it will have a checkmark next to it) and press the **Options** button, and then select the **Logout** item. When the connection has ended, a message appears indicating that the tunnel has been removed.
3. To close **movianVPN** press **Options** and then select **Exit**.

If you exit you may not be able to login again because your previous session will still be active. Contact your gateway administrator if this is the case.

A

Appendix A: Troubleshooting and using the Diagnostic Tools

Troubleshooting

While logging into the gateway, you may see a login failure message. If you experience login failure, the most likely cause is an incorrect policy setting. Review your policy and connection settings again. The settings should be as specified by your VPN administrator.

You should also bear the following in mind:

- If **movianVPN** cannot negotiate a connection to the gateway although the settings appear correct, check that the group name, group password and user name do not have a trailing space after the entry.
- If your dial-up connection is normally made from a particular location, such as home or from the office, you may or may not be required to include a 9 or make other changes in the dialing number. See your Nokia device documentation to find out how to change your Internet settings.
- Poor cellular coverage could also have an effect on your connection.
- If your settings are correct but you cannot connect to your gateway, the gateway may be down or inaccessible for some reason. Contact your gateway administrator.

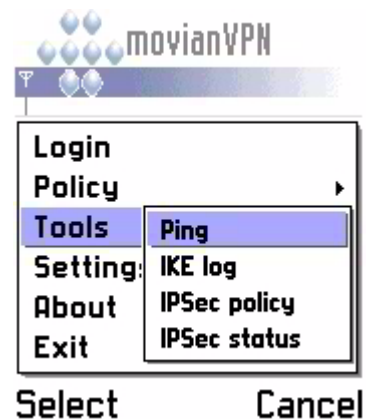
Using the diagnostic tools

If you are having trouble with your VPN connection, you can try running the movianVPN diagnostic tools.

Ping

You can use the Ping utility to test your network connection.

1. To use the Ping utility, select **Tools** on the menu bar, then **Ping**.

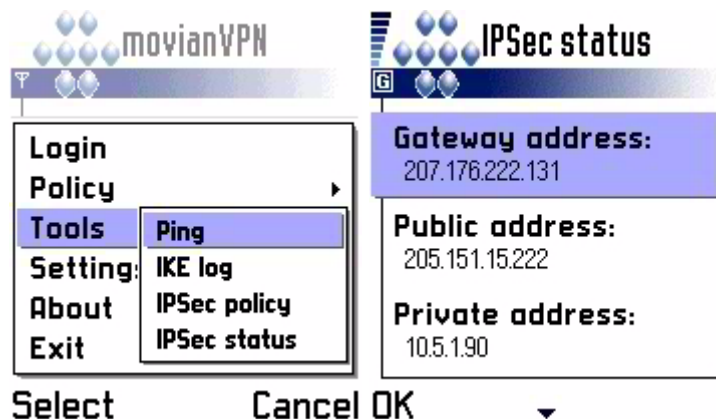


2. Enter the IP address of the computer you wish to contact. movianVPN will attempt to verify the accessibility of that machine and report on the results.



View IPSec Status

The IPSec status can be used to confirm that a tunnel is working and provide information about it. It also provides information on the handheld device and the gateway. The IPSec Status is only available while the VPN tunnel is up.



1. To view the IPSec status, select **Tools** on the menu bar, then **View IPSec Status**.

The fields provide the following information:

| Field | Information |
|------------|-------------------------------|
| Gateway IP | VPN gateway server IP address |

| Field | Information |
|----------------|--|
| Our Public IP | IP address supplied by ISP |
| Our Private IP | IP address within the VPN |
| NAT Port | States if NAT (Network Address Translation) is enabled |
| Split Tunnel | States if split tunneling is enabled |

Split Tunneling

Split tunneling allows you to use both the internet and the corporate internet at the same time. When split tunneling is enabled, all packets sent to or from the VPN and its identified subnets are encrypted; packets directed outside the VPN are not encrypted, and go directly through the ISP to the internet.

When split tunneling is disabled, all packets are encrypted. If the packet is not to or from an identified address on the VPN, it is dropped from communication.

Network Address Translation

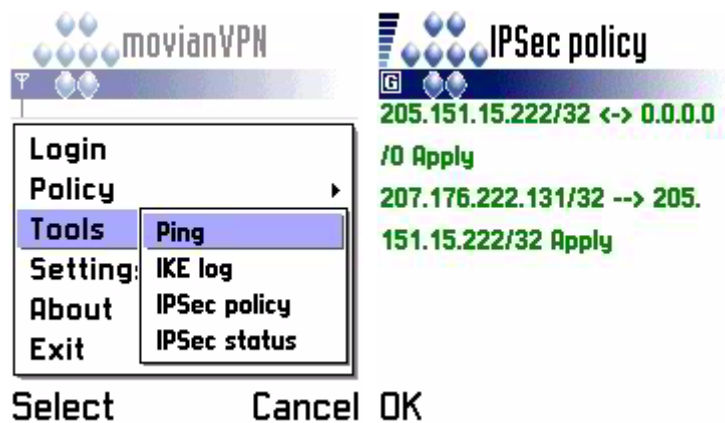
NAT (Network Address Translation) is a gateway technology that allows IP packets to be transmitted between two networks which use different addressing schemes. NAT allows the two networks (or subnetworks) to communicate with each other without any conflicts by resolving the destination address of an incoming IP packet. This involves modifying the header of the IP packet. However, since it modifies the packet header, it cannot be used with IPSec because the latter encrypts all the traffic.

View IPSec Policy

The IPSec policy shows where the data has been encrypted (between which IP addresses).

1. In the movianVPN menu bar, select **Tools**, then **View IPSec Policy**.

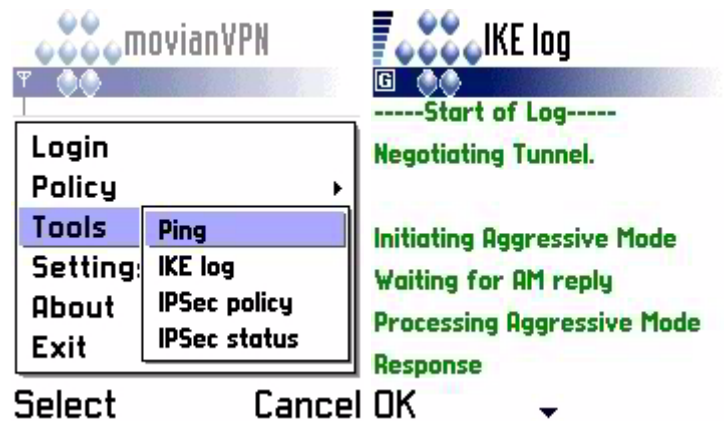
2. The IPSec policy window shows where the data was encrypted: **Apply** indicates that the data was encrypted between the two addresses; **Bypass** indicates that it was not encrypted.



View IKE Log

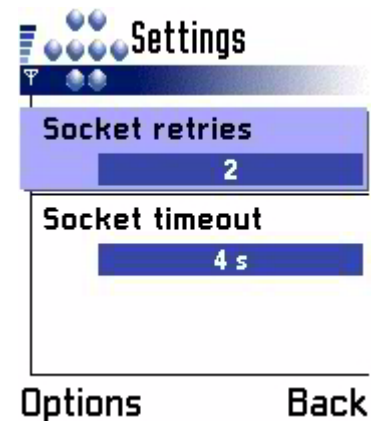
The IKE log displays the negotiations that occurred between the movianVPN client and the VPN gateway.

1. To view the IKE log, select **Tools** on the menu bar, then **View IKE Log**.
2. The IKE log displays status messages about the connection with the gateway. To close the window, press **OK**.

Connection
(socket) options

If you are having trouble getting a reply from your VPN gateway or ISP mobile connection, you could try adjusting the socket settings.

1. In the **movianVPN** menu bar, select your policy, then press **Options**, then select the **Settings** item.
2. The **Settings** window appears. It contains the **Socket retries** and **Socket timeout** items.
 - **Socket retries** option sets the number of times **movianVPN** will attempt to connect.
 - **Socket timeout** option sets the time the system will allow before considering each attempt to be a failure.
3. Change the **Socket retries** and **Socket timeout** values as appropriate.
4. Select **Close** to close the **Settings** window.



B

Appendix B: Glossary of Terms

| | |
|------------------------------|---|
| Authentication | Authentication refers to the verification of the identity of communicating parties. |
| Cipher | Ciphers are algorithms or mathematical functions used to encrypt data. movianVPN uses Digital Encryption Standard (DES) or 3DES, where the encryption is performed three times. |
| Client software | Client software is the software installed on your handheld device. It communicates with the software installed on your gateway server. |
| Confidentiality | Confidentiality is the need to restrict access to information to people with the appropriate authorization. This need is typically addressed by encryption, which restricts access to information to people possessing the correct key. |
| Digital signatures | Digital signatures provide a form of authentication, confirming the identity of communicating parties and acting as a legally binding signature. |
| DNS Domain Name System | Domain Name System (DNS) settings are used to identify particular computers or parts of the network. |
| Encryption | Encryption is the process of converting a text or other communication into a coded format which cannot be read by other parties unless decrypted. Encryption and decryption relies on shared keys. |

Extended Authentication

Extended Authentication (XAUTH) inserts a new level of security in the middle of the IKE (Internet Key Exchange), after the device authentication. A prompt asking for the User Name and Password or another form of additional authentication appears when you log onto the gateway.

If you answer the prompt correctly, the second security set-up phase continues. Extended Authentication can be used to require an additional password or code, depending on the type of gateway.

Gateway

A gateway is the server which recognizes and authenticates a user attempting to access a VPN.

Hash Numbers

Hash numbers confirm that communicated data has not been changed during transmission. A hash number is generated for a particular set of data's characteristics, and sent along with the communication. When the communication is received, the hash number is generated again in the same way, and the results compared to the original hash number.

**IKE
Internet Key
Exchange protocol**

Part of the IPSec protocol, allows communicating parties to negotiate methods of secure communication—such as how the parties will authenticate themselves initially, which hash functions will be used to confirm data integrity, or which forms of encryption will be used.

IPSec

Developed by the Internet Engineering Task Force (IETF), IPSec protocol is a framework of open standards that provides flexible network security, providing confidentiality, data integrity, and data source verification for any application using the network. A protocol is a series of clearly-defined, agreed upon steps that are followed by all parties in an interaction.

**ISP
Internet Service
Provider**

A company providing dial-up connections to access the Internet.

Key

A key is used to encrypt and decrypt a communication so that it cannot be read by any parties except the sender and intended receiver.

**Perfect Forward
Secrecy**

Perfect Forward Secrecy is designed to keep previous traffic locked in the past. This is accomplished by executing the key exchange twice, using the same key material. Using Perfect Forward Secrecy prevents the compromise of the secret keys.

Perfect Forward Secrecy creates new keys for each step of the Internet Key Exchange (IKE). Negotiation of the connection will take longer.

**PDA
Personal Digital
Assistant**

Personal Digital Assistants (PDAs) are handheld personal computing devices.

Policy

A policy contains the settings used by **movianVPN** to contact and negotiate access to a VPN. The policy includes information on making a connection; negotiating authentication and key exchange; and encryption protocols.

**SA
Security
Association**

A limited-lifetime statement of the negotiated security policies between the communicating devices, such as session keys and agreed encryption algorithms. SA Lifetime provides an automatic time-out from a session with a gateway.

Split Tunnelling

Split tunneling is a method used by the VPN server to decide which traffic to send through an encrypted tunnel. Traffic sent to or from the VPN is encrypted, while other traffic goes directly through the ISP to or from the internet. Split tunneling secures sensitive VPN traffic, while allowing less sensitive material to flow normally.

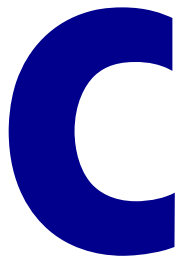
When you select Split Tunneling, packets of data headed to inside the VPN will still be encrypted and forwarded. Packets that are not directed to inside the VPN will not be encrypted, nor is the reply.

Tunnel

A tunnel is created to securely send encrypted information directly from one computer to another.

**VPN
Virtual Private
Network**

A Virtual Private Network or VPN is used to provide secure, encrypted communication between specific computers on a wider network.



Appendix C: Information worksheet

Information required for client configuration

The following information will be required as you create the policy for the gateway. The information must be entered in a field, selected from a pull-down list, or selected/deselected using checkboxes.

Not all fields will apply for your specific gateway.

Information required for creating a policy

| Field, Checkbox or Button | Required | Information/Action |
|---|----------|--------------------|
| Policy Name | | |
| Gateway Type (Please select one) | | |
| Gateway IP Address | | |
| Perfect Forward Secrecy | | |
| Extended Authentication (Nortel gateway only) | | |
| IKE Suite | | Group: |
| | | Cipher: |
| | | Hash: |
| Group Name | | |
| Group Password | | |
| User Name | | |
| User Password | | |
| User Passcode (SecurID) | | |
| IPSec Suite | | |

Index

A

- authentication, 4
 - key, 6
 - logging in, 30

C

- Cipher (IKE Crypto Suite), 27
- Cisco Unity with Cisco 3000 v3.0 gateway, 22
- Cisco VPN Concentrator 3000 gateway
 - policy, 15
 - Unity policy, 22
- connection options
 - socket retries, 38
 - socket timeout, 38
- connections
 - supported, 7

D

- devices
 - handheld and wireless, 4
 - supported, 7
- diagnostic tools
 - accessing, 36

E

- encryption, 4, 6
 - key, 6
- evaluation licenses, 11
 - expiration, 11
- Extended Authentication, 25
- extranet VPN, 3

G

- gateway
 - access, 6
 - authentication and key negotiation, 30
 - contacting, 30
 - Extended Authentication, 25
 - logging in, 30, 35
 - authentication, 30
 - key negotiation, 30
 - troubleshooting, 35
 - logging out, 33
 - Perfect Forward Secrecy, 25
 - policy
 - creating, 14
 - verifying, 25
 - policy information required, 14
 - settings
 - DNS, 27
 - Extended Authentication, 25
 - IKE Crypto Suite, 27
 - IPSec Crypto Suite, 27, 28
 - Network Properties, 27
 - Perfect Forward Secrecy, 25
 - troubleshooting log in, 35
- gateway access settings, 27
- gateway server
 - access, 6
- gateway servers, 3
- gateways
 - Cisco Unity with the Cisco 3000 v3.0, 22
 - Cisco VPN Concentrator 3000, 15, 22
 - Nortel Contivity Series, 18
 - supported by movianVPN, 7
 - using, 32
- getting started, 13
- Group (IKE Crypto Suite), 27

H

handheld devices

- connecting to VPN, 4

Hash (IKE Crypto Suite), 27

Hash numbers, 27

hash numbers, 27

I

IKE Crypto Suite, 27

- Cipher, 27

- Group, 27

- Hash, 27

installation

- overview, 9

- uninstalling, 12

interoperability, 7

intranet VPN, 3

IPSec, 4

- communication process, 6

IPSec Crypto Suite, 28

K

keys

- authentication, 6

- encryption, 6

- exchange protocols, 27

- IKE Crypto Suite, 27

- negotiation when logging in, 30

L

licensing movianVPN, 11

- checking license type, 11

- evaluation versions, 11

logging in

- authentication, 30

- contacting the gateway, 30

- key negotiation, 30

- troubleshooting, 35

logging out, 33

M

minimizing the movianVPN window, 32

moivanVPN

- system requirements, 9

movianVPN, 6

- accessing VPN servers, 32

- client software, 6

- creating policies, 14

- diagnostic tools, 36

- installing, 9

- interoperability, 7

- licensing, 11

- logging in to gateway, 30

- logging out, 33

- overview, 1

- policies, 6, 14

- running, 29

- system requirements, 9

- technical support, 10

- uninstalling, 12

- updates, 11

- using the gateway, 32

- version number, 10

- window

 - minimizing, 32

N

Nortel Contivity Series gateway, 18

- policy, 18

O

overview

- getting started, 13

- installation, 9
- movianVPN, 1
- running movianVPN, 29

P

- Perfect Forward Secrecy, 25
 - key, 25
- policies, 6
 - creating, 14
 - Cisco Unity with Cisco 3000 v3.0, 22
 - Cisco VPN Concentrator 3000, 15, 22
 - Nortel Contivity Series, 18
 - editing
 - access settings, 27
 - Extended Authentication, 25
 - information required, 14
 - reviewing, 25
 - settings, 27
 - Extended Authentication, 25
 - IKE Crypto Suite, 27
 - IPSec Crypto Suite, 28
 - Perfect Forward Secrecy, 25
 - verifying, 25

R

- remote access VPN, 3

S

- servers
 - accessing VPN, 32
 - gateway, 3, 6
- Socket Retries, 38
- Socket Timeout, 38
- system requirements, 9

T

- troubleshooting
 - logging in to gateway, 35
 - using diagnostic tools, 36
- tunneling, 3, 4

U

- uninstalling movianVPN, 12
- updating movianVPN, 11

V

- version number, 10
- Virtual Private Network. *see* VPN
- VPN, 3
 - gateway access, 6
 - gateway servers, 3
 - intranet, 3
 - logging in, 30
 - overview, 3
 - tunneling, 3, 4
 - using, 3
 - wireless and handheld devices, 4
- VPN servers
 - accessing, 32
- VPNs
 - accessing, 6
 - extranet, 3
 - forms, 3
 - gateway servers, 6
 - remote access, 3

W

- wireless devices
 - connecting to VPN, 4