

movianVPN™

Version 3.0.5

Deployment Guide for Nortel Contivity Series VPN Gateway

PUB-0200-2000
May 13, 2003

© Certicom Corp. 2000-2003. All rights reserved.

Certicom(R), Certicom logos, movian (tm), movianVPN (tm) are trademarks of Certicom Corp. All other trademarks or registered trademarks are property of their respective owners. This product 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. 2000-2003. 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.

Table of Contents

Introduction	1
Overview: movianVPN	1
Purpose of this document	2
Creating a basic policy and using advanced features	2
Using Appendix C: Client configuration worksheet	2
Licensing and Support for movianVPN	3
Installing movianVPN	3
Licensing movianVPN	3
Technical support	3
VPN infrastructures and handheld devices	4
VPNs	4
Gateway servers	4
IPSec	5
Handheld devices	6
movianVPN	7
movianVPN	7
ECC and movianVPN	7
Gateway access	7
Getting Started	9
Software Requirements	9
Gateway software	9
Connections	9
Supported devices	9
Configuring your gateway to support movianVPN	11
Before you begin	11
Gateway software	11
Creating a new group	12
Enabling ciphers	12
Adding a new group	13
Adding a user to the group	15
Creating a movianVPN policy for your gateway	17
Before you begin	17
Creating the policy	18
Creating a WinCE policy	19
Creating a Palm OS policy	22
Testing the policy	27
If the connection failed	27
Logging out of the gateway	28
Configuring features on movianVPN	29
IPSec	29
IPSec Crypto Suite	32
IKE Crypto Suite	32

Enhancing your movianVPN policy	35
Split Tunneling	36
Enabling split tunneling	36
Enabling split tunneling on movianVPN	38
Perfect Forward Secrecy	39
Enabling perfect forward secrecy on the gateway	39
Enabling perfect forward secrecy on the movianVPN client	40
DNS Support	41
Enabling DNS support on the gateway	41
Enabling DNS support on the movianVPN client	41
Authentication Using Certificates	43
Installing Certificates	43
Using Certificates	44
External Authentication	47
Setting up an external Radius authentication server	47
Enabling External Authentication on the movianVPN client	49
NAT Traversal	51
Enabling NAT traversal on the gateway	51
Banner Support and Password Save Feature	52
Enabling banner support and password save feature on the gateway	52
Deploying a pilot scheme	53
Choosing a range of IP addresses	53
Bandwidth Considerations	54
Appendix A: Using the Diagnostic Tools	55
Accessing diagnostic tools	55
Ping	56
Using Ping with a WinCE client	56
Using Ping with a Palm OS client	57
IPSec Status Log	58
Viewing IPSec Status for a WinCE client	58
Viewing IPSec Status for a Palm OS client	59
IP Packet Statistics Log	60
Viewing IP Packet Statistics for a WinCE client	60
Viewing IP Packet Statistics for a Palm OS client	61
Appendix B: Glossary of Terms	63
Appendix C:	
Client configuration worksheet	67
Information required for client configuration	67
Information required for creating a policy	68

1

Introduction

Overview: movianVPN

For mobile professionals, a handheld personal computer such as a Personal Digital Assistant (PDA) or Palm device 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 handheld devices 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.

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

Purpose of this document

This document contains the information necessary to configure **movianVPN** on your VPN gateway.

It is aimed at the administrators responsible for deploying, configuring and testing the **movianVPN** client software.

The chapters include information on:

- Licensing and support (this chapter)
- Getting Started
- Configuring your gateway to support movianVPN
- Creating a movianVPN policy for your gateway, and
- Enhancing your movianVPN policy.

The final chapter of this document contain a discussion of issues related to deploying a pilot system with a number of handheld devices. This may not be present if there are no additional issues related to your gateway.

Creating a basic policy and using advanced features

The creation of a policy as described in this document refers to a basic policy , intended for testing the handheld device's connection to the gateway. The basic policy does not include advanced features such as split tunneling or DNS support which may be supported on your gateway. Advanced features which may be enabled on the gateway and on users' handheld devices are described in the chapter on "Enhancing your **movianVPN** policy." For more information see also the *movianVPN User Guide for WinCE Pocket PC and Handheld PC* or *movianVPN User Guide for Palm OS*.

Using Appendix C: Client configuration worksheet

"Appendix C: Client configuration worksheet" contains a worksheet for the information required by users to configure their handheld devices for using **movianVPN** with your gateway. The sheet can be printed, the information entered as appropriate, and forwarded to users.

Some entries in the table may not be applicable for your gateway.

The *movianVPN User Guide for WinCE Pocket PC and Handheld PC* and the *movianVPN User Guide for Palm OS* include the same table, both as an appendix and as part of the chapter on creating a policy. In a limited deployment, printing and entering the information in individual user's guides may be appropriate.

Licensing and Support for movianVPN

Installing movianVPN

To find out how to install or upgrade movianVPN, please see the *movianVPN User Guide for WinCE Pocket PC and Handheld PC* or *movianVPN User Guide for Palm OS*.

Licensing movianVPN

The **movianVPN** evaluation license expires after a period of 30 days. In the final seven days of the evaluation period, you will be informed of the number of days remaining each time you start the application.

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

To find out which kind of license you have, open the movianVPN application and select the **About License** option.

Technical support

Please contact your reseller.

VPN infrastructures and handheld devices

This section contains a description of VPN gateways and IPSec protocols, and how handheld devices can be securely integrated into a VPN.

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:

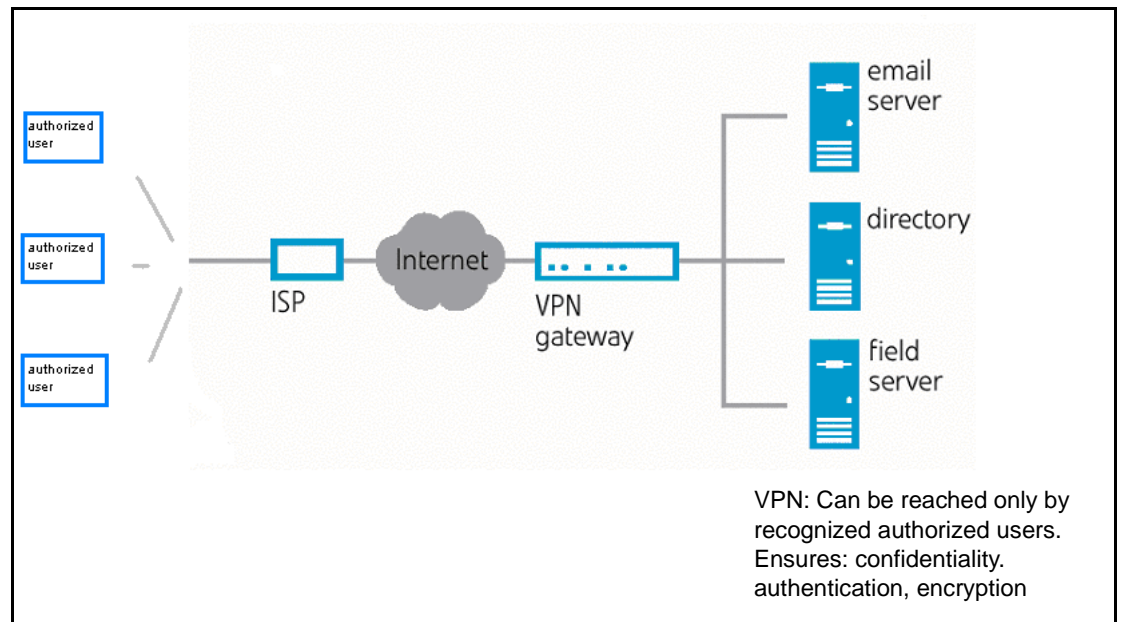
- **Intranet VPN:** Between a central corporate site and branch offices
- **Remote access VPN:** Between a central corporate site and individual remote users (the **movianVPN** model)
- **Extranet VPN:** Between an enterprise and its business partners, suppliers, and customers

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, 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: IPSec protocol makes this possible.

IPSec

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

Using IPSec therefore ensures that you know who the data came from; that it is securely encrypted; and that the communication has not been tampered with.

Handheld devices

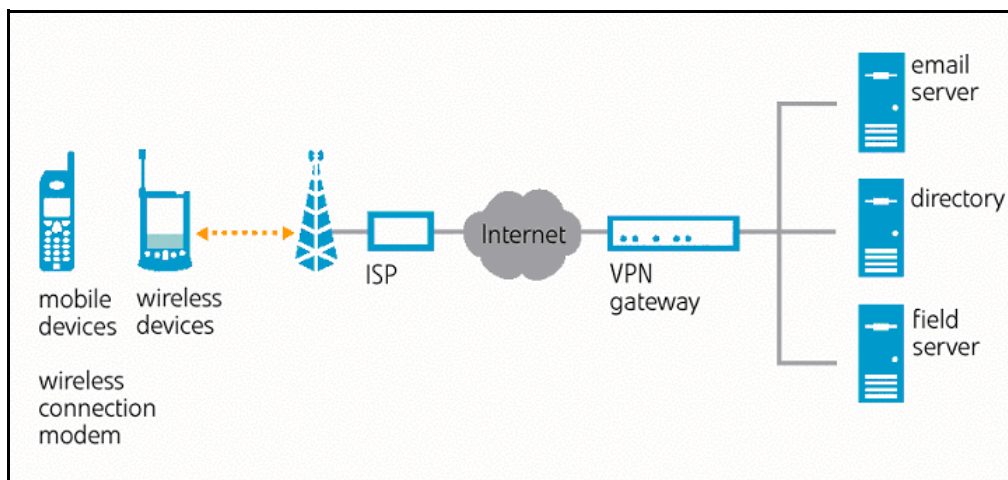
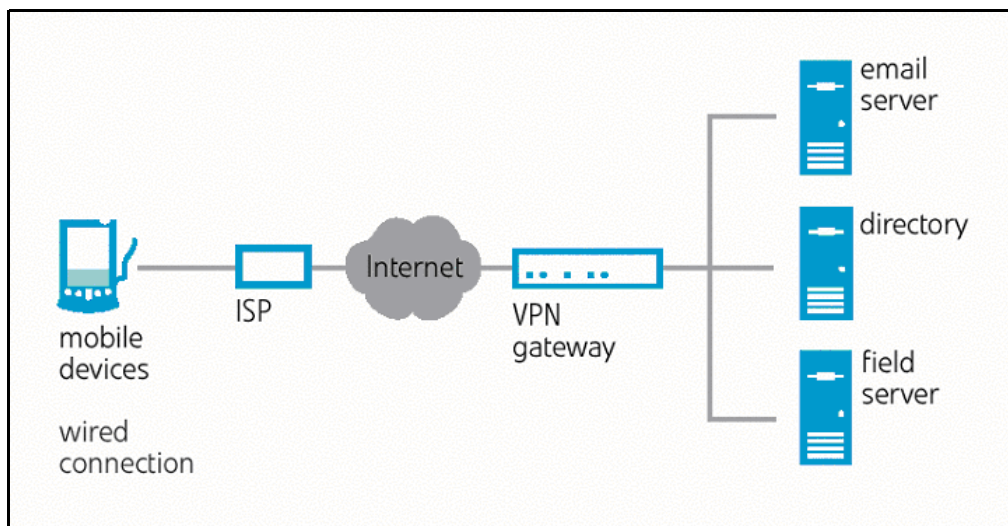
Using **movianVPN**, a traditional VPN can also have handheld devices added to the configuration without compromising network security.

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 LAN
- Wireline access to a local 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 configurations.



For information on the handheld devices and operating systems that can use **movianVPN**, see the following chapter.

movianVPN

This section contains a description of the advantages of using movianVPN, particularly with ECC.

movianVPN

movianVPN allows mobile professionals to use their handheld devices to connect securely and easily to a corporate 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, tokens for two-factor authentication, and the use of digital signatures.
- 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.

ECC and movianVPN

movianVPN is specifically designed for the constrained environments of wireless and mobile devices. It uses ECC (Elliptic Curve Cryptography), which provides strong security with much smaller key sizes than legacy public-key encryption algorithms. In addition, ECC requires less processing power, which results in faster IKE (Internet Key Exchange) negotiation with ECDH (one of the algorithms in the ECC suite).

movianVPN also supports 768-bit and 1024-bit Diffie-Hellman algorithms for the case where the gateway does not support Certicom's patented ECC implementation.

Gateway access

Gateways are accessed using a "policy" set up 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.

2

Getting Started

Software Requirements

Gateway software

The following table details the Nortel Contivity VPN Switch Series gateway configuration software supported for movianVPN.

Note: If you have an older version of the software, you should upgrade. Please see the documentation for your gateway for the procedure.

Gateway	Product	Supported software versions
Nortel Network	Contivity VPN Switch Series	2.60.56 to 3.6.0/4.0

Connections

The following specific connections have been tested for interoperability:

- CDMA
- CDPD
- Ethernet
- GSM
- IDEN
- Richochet
- TDMA
- 802.11

Supported devices

The following devices are supported:.

Palm OS	Win CE OS
3.5 and up	Handheld PC 2000 Pocket PC v3.0 Pocket PC 2002

3

Configuring your gateway to support movianVPN

Before you begin

If you are setting up your gateway for the first time, please refer to your gateway configuration manual.

This chapter configures the gateway with only one user and tests the connection. Advanced features such as Extended Authentication and Split Tunneling are included in “Enhancing your movianVPN policy” on page 35.

Gateway software

The following table details the gateway configuration software supported for movianVPN.

Note: If you have an older version of the software, you should upgrade. Please see the documentation for your gateway for the procedure.

Gateway	Product	Supported software versions
Nortel Networks	Contivity VPN Switch series	2.60.56 to 3.6.0/4.0

Creating a new group

You must enable ciphers before creating a new group.

Enabling ciphers

To enable ciphers options:

- Using the navigation sidebar, select **Services**, then **IPSec**.



- Enable **ESP_Triple DES with SHA1 integrity** and **ESP_TripleDES with MD5 integrity, Triple DES with Group 7 (ECC 163-bit field)**.

Note: For a basic policy, disable NAT Traversal. This function is discussed in “NAT Traversal” on page 51.

Adding a new group

To add a new group:

1. In the navigation sidebar, select **Profiles**, then **Groups**.
2. Click on **Add**.

3. Enter the **group name**. Use the default setting for **parent group**.
4. Click **OK**.
5. Select the group and click **Edit**.

6. In the Profiles\Group window, click **Configure** under **Connectivity**.

Groups --> Edit --> Connectivity

Group Name: /Base/test1

Field	Value	Actions	Inherited From
Contact Information	(None)	Configure	/Base
Access Hours	Anytime	Configure	/Base
Call Admission Priority	Highest Prior	Configure	/Base
Forwarding Priority	Low Priority	Configure	/Base
Number of Logins	10	Configure	/Base
Password Management	Disabled	Configure	/Base
Maximum Password Age	30	Configure	/Base
Minimum Password Length	16	Configure	/Base
Alpha-Numeric Password Required	Disabled	Configure	/Base
Static Addresses	Enabled	Configure	/Base
Idle Timeout	00:15:00	Configure	/Base
Maximum number of login attempts to lock out an account.	0	Configure	/Base
Filters	permit all	Configure	/Base

7. Make sure the **Static Addresses** option is enabled. If necessary, click **Configure**, change the setting, and click **OK**.
8. In the Profiles|Group window, click **Configure** under **IPSec**.

Field	Value	Actions
Split Tunneling	Disabled	Configure
Split Tunnel Networks	(None)	Configure
Client Selection	Allowed Clients: Both Contivity and non-Contivity Clients Allow undefined networks for non-Contivity clients: Enabled	Configure
Authentication	Database Authentication (LDAP): - User Name and Password: Enabled * RADIUS Authentication: - User Name and Password: Disabled - Security Dynamics SecurID: Disabled Group ID: (None) LDAP Authentication: Group ID: (None)	Configure
Encryption	ESP - Triple DES with SHA1 Integrity Enabled ESP - Triple DES with MD5 Integrity Enabled ESP - 56-bit DES with SHA1 Integrity Enabled ESP - 56-bit DES with MD5 Integrity Enabled * ESP - 40-bit DES with SHA1 Integrity Disabled * ESP - 40-bit DES with MD5 Integrity Disabled ESP - NULL (Authentication Only) with SHA1 Integrity Enabled ESP - NULL (Authentication Only) with MD5 Integrity Enabled	Configure

9. Ensure that you allow both **Contivity** and **Non-Contivity** clients. If necessary, click **Configure**, change the setting, and click **OK**.

10. In the **Authentication** section, ensure that under **Database Authentication (LDAP)**, **username** and **password** are enabled. If necessary, click **Configure**, change the setting, and click **OK**.
11. In the **Encryption** section, enable **ESP_TripleDES with SHA1 integrity** and **ESP_TripleDES with MD5 integrity**, or if available, **Triple DES with Group 7 (ECC 163-bit field)**. If necessary, click **Configure**, change the setting, and click **OK**.
12. Scroll down if necessary, and ensure the **Compression** option is disabled.

* Allow Password Storage on Client	Disabled	<input type="button" value="Configure"/>	/Base
Compression	Disabled	<input type="button" value="Configure"/>	/Base
Rekey Timeout	08:00:00	<input type="button" value="Configure"/>	/Base

If necessary, click **Configure**, change the setting, and click **OK**.

13. Click **OK**.

Adding a user to the group

After creating the group, you can add a new user.

To add a user:

1. In the navigation bar, select **Profiles**, then **Users**.

The screenshot shows the 'User Management' interface. At the top, there is a 'Group' dropdown menu set to '/Base/test' and a 'Display' button. Below this is a 'User Search' section with a search input field and radio buttons for 'Last Name', 'User ID', 'Admin Rights', and 'LDAP'. To the right of the search options are 'Search Group' and 'Search All' buttons. Below the search section are 'Previous', 'Next', 'Add User', and 'More Reports' buttons. The main content area shows a table with columns 'Last', 'First', and 'Actions'. A message states: 'There are no users defined in this group. Press the Add User button to Add Users to this group.' At the bottom of the table area is an 'Add User' button.

2. Select the new **Group** (created above) from the drop-down list.
3. Click on **Add User**.

User Management --> Add User

[?](#) [X](#)
HELP LOGOFF

General

	First	Last
Name	<input type="text"/>	<input type="text"/>
Group	/Base/test ▼	

	Static IP Address	Static Subnet Mask
Remote User	<input type="text"/>	<input type="text"/>

Note: The static IP subnet mask is used for IPsec connections only

User Accounts

	User ID	Password	Confirm Password	Expires (Days)	status
IPsec	<input type="text"/>	<input type="text"/>	<input type="text"/>		
PPTP	<input type="text"/>	<input type="text"/>	<input type="text"/>		
L2TP	<input type="text"/>	<input type="text"/>	<input type="text"/>		
L2F	<input type="text"/>	<input type="text"/>	<input type="text"/>		

IPsec Certificate Credentials
(RSA Digital Signatures Disabled)

4. Enter the **first** and **last** name.
5. Enter the **static IP address** and **subnet mask**.
6. Under **User Account**, in the **IPSec** fields, enter the **User ID**, the **Password** and the **Confirm Password**.
7. Click **Add**.

4

Creating a movianVPN policy for your gateway

Before you begin

This chapter does not contain a complete description of the **movianVPN** client software. The policy described is a basic policy which does not make use of advanced features such as Perfect Forward Secrecy and DNS Support.

The procedures do assume that you have started **movianVPN** on a handheld device and have an active Internet connection.

***Note:** For more information on using **movianVPN** client software, please refer to the **movianVPN User Guide for WinCE Pocket PC and Handheld PC** or **movianVPN User Guide for Palm OS**.*

***Note:** **movianVPN** version 3.0 comes equipped with a **Deployment Tool**. This tool allows you to quickly create a security policy file that can be read by the client software. The **Deployment Tool** is useful if you are configuring a security policy for a large number of clients. For instructions on how to use the **Deployment Tool** please see the **movianVPN Deployment Tool User's Guide**.*

Creating the policy

The following information is required when creating a policy for the Nortel Contivity Series VPN gateway:

- 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

Note: Depending on the type of extended authentication selected, users are asked for a user password or user passcode when logging in to the gateway.

- DNS, IKE Suite and IPSec Suite settings
- SA life setting

When creating a policy to test the gateway, a basic policy is recommended. To simplify the connection, advanced features such as Perfect Forward Secrecy, Extended Authentication, and DNS support should not be used. These settings can be configured by users for general deployment (for more information see “Perfect Forward Secrecy” on page 39, “External Authentication” on page 47, and “DNS Support” on page 41.)

For more information on creating a policy with advanced features please refer to the *movianVPN User Guide for WinCE Pocket PC and Handheld PC* or *movianVPN User Guide for Palm OS*.

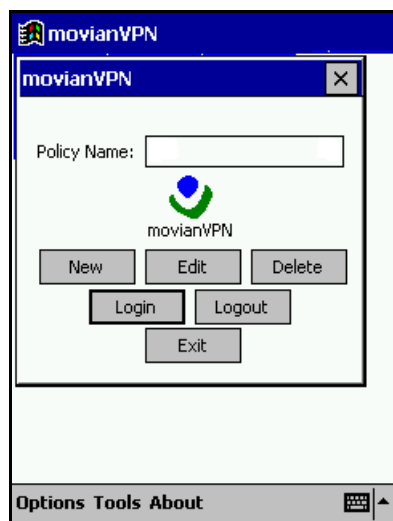
A worksheet is provided in “Appendix C: Client configuration worksheet” on page 67 that can be used to enter the required information and be given to users. The same table appears in the *User Guides*.

Creating a WinCE policy

To create a WinCE policy for a Nortel Contivity Series gateway:

1. To open the **movianVPN** application, either tap **Start** and select **movianVPN** from the list, or tap **Start**, select **Programs**, and tap the **movianVPN** icon.

The **movianVPN** application window appears.

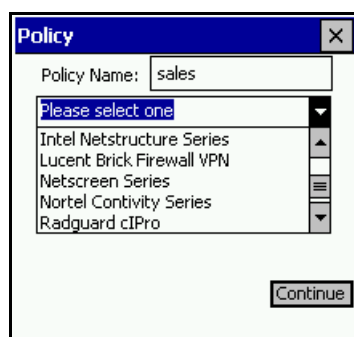


2. Tap **New**.

The **movianVPN** Policy window appears.



3. Enter a policy name in the **Policy Name** field.
4. Tap **Please select one** to access the pull-down menu.



5. Scroll down and tap **Nortel Contivity Series**.

The Nortel Contivity Series Gateway IP address field and the gateway policy option check boxes appear.

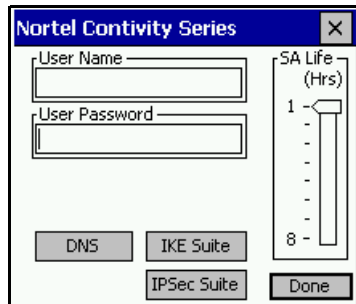


6. Enter the **Gateway IP Address**.

Note: When creating a policy to test the gateway, a basic policy is recommended. To simplify the connection, advanced features such as Perfect Forward Secrecy and Extended Authentication should not be used. These settings can be configured by users for general deployment.

Note: To use certificates imported with **movianCM**, activate the **Use Certificates (PKI)** checkbox. See the **movianVPN User Guide for WinCE Pocket PC and Handheld PC**.

7. Tap **Continue**.



Enter the **User Name** and **User Password** for the gateway.

Note: These entries should be as defined in “Creating a new group” on page 12 and “Adding a user to the group” on page 15.

Note: When creating a policy to test the gateway, a basic policy is recommended. To simplify the connection, advanced features such as DNS Support should not be used. These settings can be configured by users for general deployment.

8. Tap the **IKE Suite** button in the Nortel Contivity Series window.

The IKE Crypto Suite window appears. .

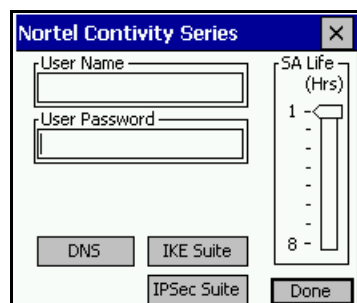


9. Select the appropriate settings from each of the pull-down lists for **Group**, **Cipher**, and **Hash** fields. The gateway allows you to choose one of a number of combinations of **group**, **cipher** and **hash** (see “Creating a new group” on page 12). We suggest you use **3DES with Group 7 (ECC 163-bit field)**.
10. Tap **Continue**.
11. Tap the **IPSec Suite** button in the Nortel Contivity Series window.

The IPSec Crypto Suite window appears.



12. Select the appropriate entry from the pull-down list in the **Suite** field. This should match one of the encryption options that you enabled in “Creating a new group” on page 12.
13. Tap **Continue**.
14. In the Nortel Contivity Series window, adjust the **SA Life** sidebar to time-out from the gateway as desired.



15. Tap **Done**.
The **movianVPN** application window appears.
16. To connect to the gateway, tap the **Login** button.

Creating a Palm OS policy

To create a Palm OS policy for a Nortel Contivity Series gateway:

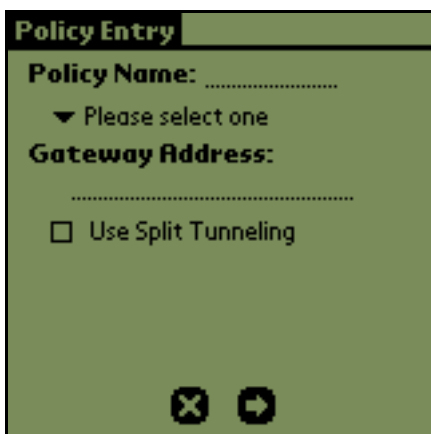
1. To open the **movianVPN** application, tap the arrow in the right corner of the top toolbar and select **movian** or **All**.
2. Tap the **movianVPN** icon.

The **movianVPN** application window appears.

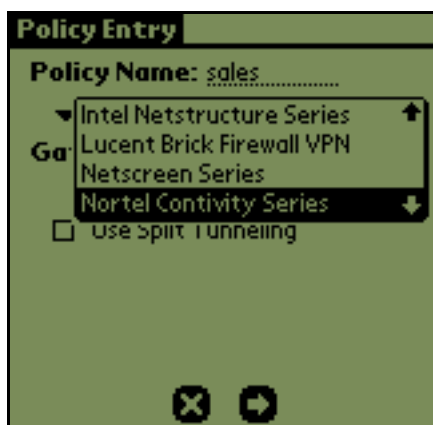


3. Tap **New**.

The **movianVPN** Policy window appears.

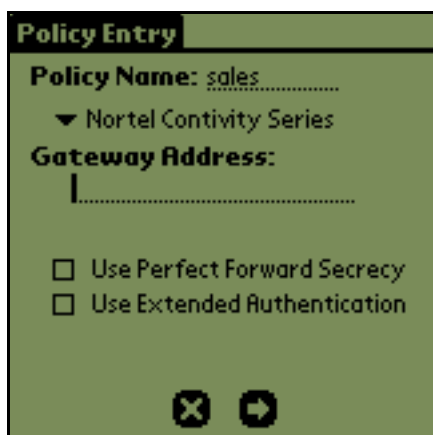


4. Enter a policy name in the **Policy Name** field.
5. Tap the pull-down menu at **Please select one**.



6. Scroll down to **Nortel Contivity Series** and tap the entry.

The Nortel Contivity Series Gateway Address field and the gateway policy option check boxes appear.



7. Enter the **Gateway Address**.

***Note:** When creating a policy to test the gateway, a basic policy is recommended. To simplify the connection, advanced features such as Perfect Forward Secrecy and Extended Authentication should not be used. These settings can be configured by users for general deployment.*

8. Tap the arrow icon.

The Nortel Contivity Series window appears. .



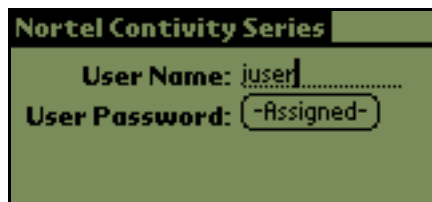
9. Enter the **User Name** for the gateway.
Note: These entries should be as defined in “Creating a new group” on page 12 and “Adding a user to the group” on page 15.
10. If you want a saved password, tap **Prompt** at the Group Password field **OR** at the User Password field.

The User password window appears.



11. Enter the password and tap **OK**.

In the Nortel Contivity Series window, the User Password now appears as **Assigned**. To delete or edit the password, tap **Assigned**, either leave the field blank to delete or enter a new password, and tap **OK**.



Note: If you do not enter the password at this time, you will be asked for it when you log in to the gateway.

12. Tap the **IKE...** button in the Nortel Contivity Series window.

The IKE Crypto Suite window appears. .



13. Select the appropriate settings from each of the pull-down lists for **Group**, **Cipher**, and **Hash** fields. The gateway allows you to choose one of a number of combinations of **group**, **cipher** and **hash** (see “Creating a new group” on page 12). We suggest you use **3DES with Group 7 (ECC 163-bit field)**.
14. Tap the checkmark icon.

Note: When creating a policy to test the gateway, a basic policy is recommended. To simplify the connection, advanced features such as DNS Support should not be used. These settings can be configured by users for general deployment.

15. Tap the **IPSec Suite** button in the Nortel Contivity Series window.

The IPSec Crypto Suite window appears.



16. Select the appropriate entry from the pull-down list in the **Suite** field. This should match one of the encryption options that you enabled in “Creating a new group” on page 12.
17. Tap the checkmark icon.
18. In the Nortel Contivity Series window, tap the **movianVPN tab** at the top of the window.

The Options pull-down list appears.



19. Tap **SA Lifetime**.

- Adjust the **SA Lifetime** setting using the arrows, to time-out of the gateway as desired.



- Tap the checkmark icon.
The Nortel Contivity Series window appears.
- Tap **Done**.
The **movianVPN** application window appears.
- To connect to the gateway, tap the **Login** button.

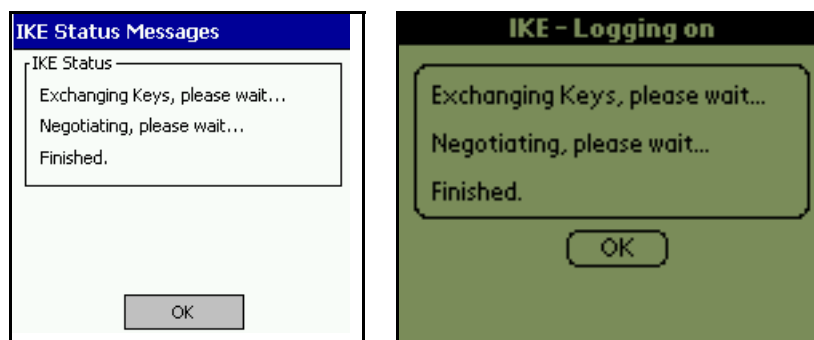
Testing the policy

For more information on verifying your policy, please refer to the *movianVPN User Guide for WinCE Pocket PC and Handheld PC* or *movianVPN User Guide for Palm OS*.

To test the policy:

1. In the **movianVPN** window, ensure the policy is selected.
2. Tap **Login**.

The IKE Messages display connection progress in generating and exchanging keys. If the connection is successful, the following screens will appear..



3. Tap **OK**.

If the connection failed

If the connection fails, complete the following:

- Check that the settings match on both the movianVPN client and the gateway
- Refer to the *movianVPN User Guide for WinCE Pocket PC and Handheld PC* or *movianVPN User Guide for Palm OS* for information on verifying your policy and troubleshooting logging in to the gateway

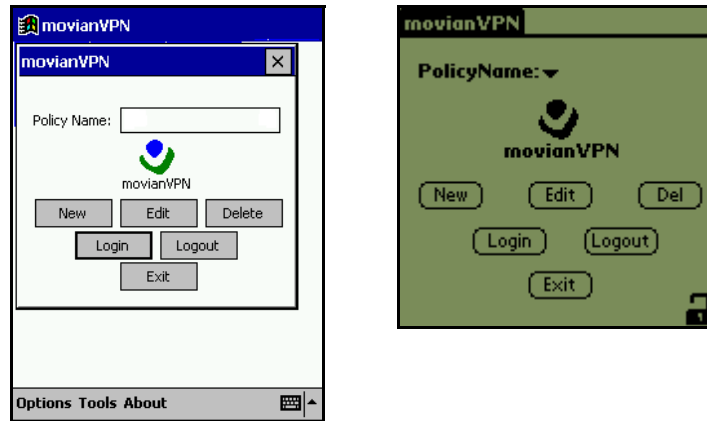
If the settings are correct and the connection is not successful:

- Refer to Appendix A for diagnostic tools
- Refer to the gateway configuration manual for information on how to view the connection log.

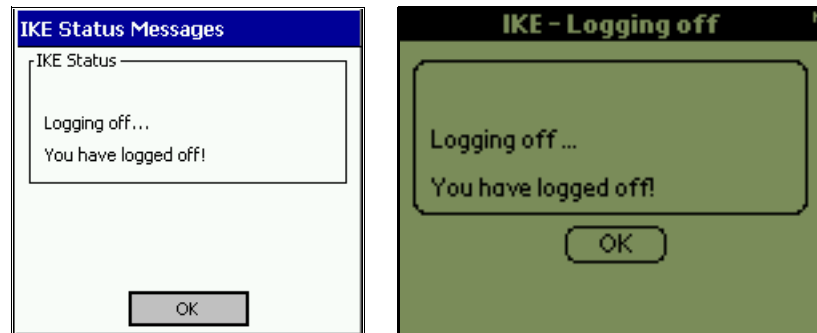
Logging out of the gateway

To close a session with the gateway server:

1. Access the **movianVPN** window,



1. Tap **Logout**.



2. Tap **OK**.
3. Tap **Exit** to close the **movianVPN** application.

Configuring features on movianVPN

Depending on the type of gateway, users can configure the following features on the client:

- “IPSec”
- “IPSec Crypto Suite”
- “IKE Crypto Suite”

For information on other features that can be selected on the client or are configured on the gateway, see also:

- “Split Tunneling” on page 36
- “Perfect Forward Secrecy” on page 39
- “DNS Support” on page 41
- “External Authentication” on page 47
- “NAT Traversal” on page 51
- “Banner Support and Password Save Feature” on page 52

IPSec

IPSec protocol allows **movianVPN** to negotiate methods of secure communication for authentication of identity, confirming data integrity, verifying data sources, and selecting encryption functions.

While using **movianVPN**, users can select and deselect IPSec during a session with the gateway. While IPSec is deselected, sent data will not be encrypted. This will allow users to access servers and websites outside the Virtual Private Network, on the Internet, but they will not be able to reach computers inside the VPN.

On gateways which permit it, **movianVPN** also supports Split Tunneling. When split tunneling is enabled, data will be either encrypted or unencrypted depending on whether it is being sent and received within the VPN or elsewhere on the Internet. Users can securely access your corporate intranet and freely access the Internet at the same time. For more information see “Split Tunneling” on page 36.

Warning: *While IPSec is deselected, the connection is not secure. Transmitted data is not encrypted.*

Enabling/Disabling IPSec in WinCE

To enable or disable IPSec in WinCE:

1. In the **movianVPN** window, while connected to the gateway, tap **Options**.



2. Select **IPSec** from the list.



3. Tap **OK**. When the checkmark is present, IPSec is enabled.

Warning: When IPSec is disabled your connection is not secure. Data is not encrypted.

Enabling/Disabling IPSec on Palm OS

To disable or enable IPSec on the Palm OS:

1. While you are connected to the VPN, in the **movianVPN** window, tap the **movianVPN** tab.

The Options pull-down list appears. When you are connected to the VPN, the IPsec entry appears on the list.

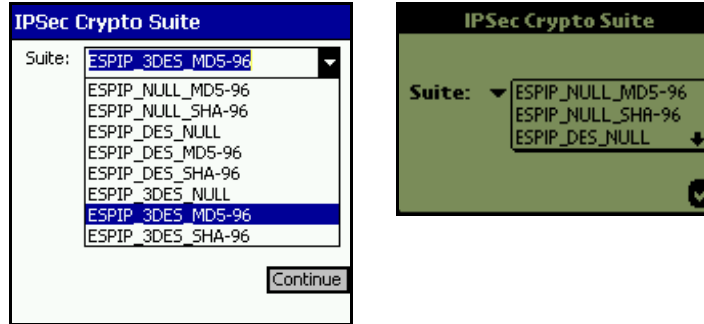
Note: While IPSec is enabled, a lock appears in the bottom right hand corner of the window.



2. Select **IPSec** from the list.
You will receive a warning that IPSec is about to be disabled.
3. Tap **OK**.

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.

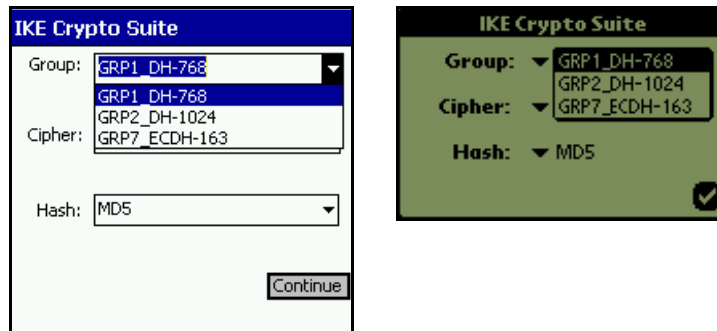
This should match one of the encryption options that you enabled in “Creating a new group” on page 12.



IKE Crypto Suite IKE (Internet Key Exchange) Crypto Suite configures the preferred protocols for exchanging keys. The gateway allows you to choose one of a number of combinations of **group**, **cipher** and **hash** (see “Creating a new group” on page 12). We suggest you use **3DES with Group 7 (ECC 163-bit field)**.

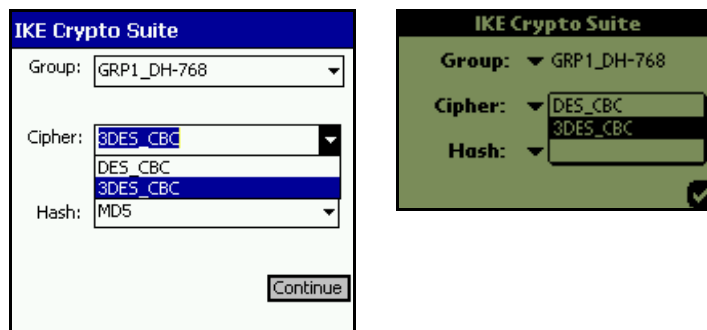
Group

Note: Group refers to the cryptographic algorithm that will be used and also the key size in the Diffie-Hellman key exchange.



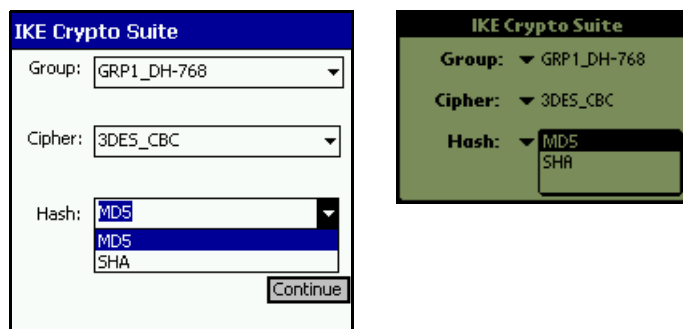
Cipher

Ciphers are used to encrypt the data using Digital Encryption Standard (DES) or 3DES, where the encryption is performed three times.



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..



5

Enhancing your movianVPN policy

Once your gateway has been configured for basic **movianVPN** functions and successfully tested, you can enhance your **movianVPN** policy with the following features:

- “Split Tunneling”
- “Perfect Forward Secrecy”
- “DNS Support”
- “External Authentication”
- "Authentication using certificates"
- “NAT Traversal”
- “Banner Support and Password Save Feature”

***Note:** If you have used the movianVPN Deployment tool to create a policy with enhanced features, you will not have to enable these features on the client software.*

Split Tunneling

Note: Your network configuration is more secure without split tunneling.

Split tunneling allows your users to use both the internet and the corporate intranet at the same time. Split tunneling is used by the VPN server to decide which traffic to send through an encrypted tunnel, depending on where the packets (the data being sent or received) originate or are directed.

When Split Tunneling is selected, all packets sent to or from the VPN and its identified subnets are encrypted; packets to outside the VPN are not encrypted, and go directly through the ISP to the internet.

When Split Tunneling is deselected, all packets are encrypted. If the packet is not to or from an identified address on the VPN, it is dropped from communication.

Users are not required to configure the client to enable split tunneling.

Enabling split tunneling

To enable split tunneling, you must enable the function, create an address list for split tunneling, and select the address list for the group.

Enabling split tunneling

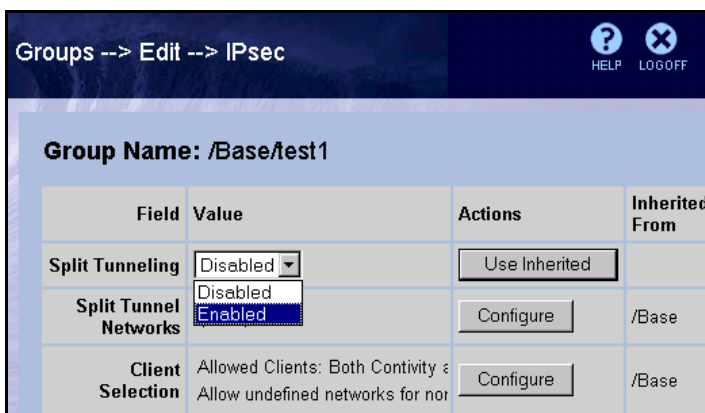
To enable split tunneling:

1. In the navigation sidebar, select **Profiles**, then **Groups**.
2. Select the group then click on **Edit**.



3. Scroll down and click **Configure** (under **IPSec**).

- Under **Split Tunneling**, click **Configure** and select **Enabled**.

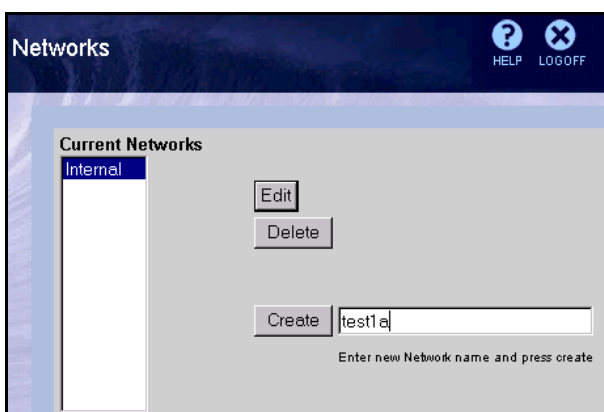


- Click **OK**.

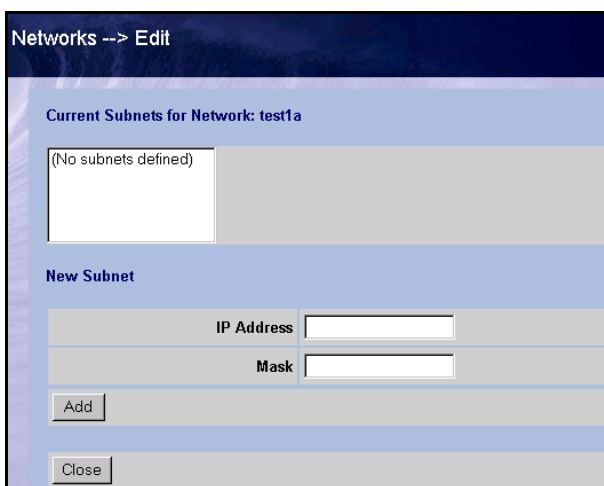
Creating and selecting an address list for split tunneling

To create an address list for split tunneling:

- In the navigation sidebar, select **Profiles**, then **Networks**.



- Enter a new **name** for the list, then click on **Create**.



3. Enter the **IP address** and the **subnet mask**.
4. Add additional subnets as required.
5. Click on **Add**.
6. In the navigation sidebar, select **Profiles**, then **Groups**.
7. Select the group and click **Edit**.
8. Click **Configure** (under **IPSec**).
9. Under **Split Tunnel Networks**, select the address list then click **OK**.

Field	Value	Actions	Inherited From
Split Tunneling	Disabled	<input type="button" value="Configure"/>	/Base
Split Tunnel Networks	(None selected) New Network	<input type="button" value="Use Inherited"/>	
Client Selection	(None selected) n Contivity and non-Contivity	<input type="button" value="Configure"/>	/Base

You should see a message saying split tunneling has been enabled.

Enabling split tunneling on movianVPN

Users are not required to configure the client to support split tunneling; the gateway administrator determines whether this feature is enabled.

Perfect Forward Security

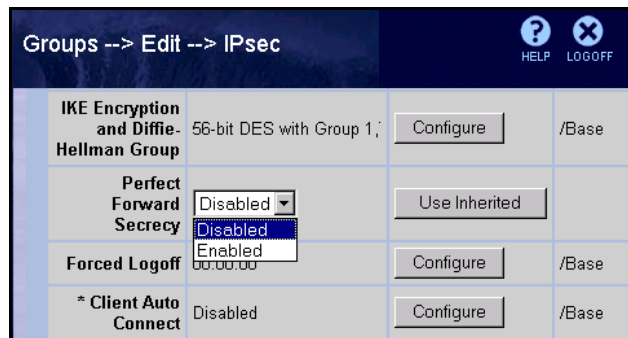
Perfect Forward Security is a cryptographic characteristic associated with a derived Shared Secret value. With Perfect Forward Security, if one key is compromised, previous and subsequent keys are not compromised, because subsequent keys are not derived from previous keys.

Perfect Forward Security 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. Thus, the previous key or the one following are not compromised even if the current one is.

Negotiation of the connection will take longer.

Enabling perfect forward security on the gateway

1. In the navigation sidebar, select **Profile**, then **Groups**.
2. Select the group, then click on **Edit**.
3. Click **Configure** (under **IPSec**).
4. Scroll down if necessary to Perfect Forward Security and click **Configure**.



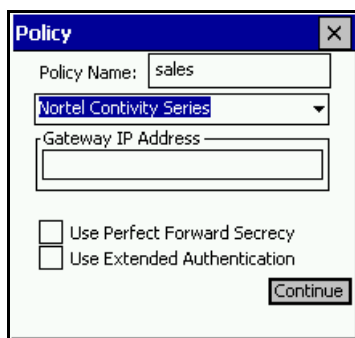
5. Enable **Perfect Forward Security**.
6. Click **OK**.

Enabling perfect forward security on the movianVPN client

Once the gateway will support Perfect Forward Security, users can enable the function on their clients.

To enable split tunneling on the **movianVPN** client:

1. In the **movianVPN** window, select the policy.
2. Tap **Edit**.
3. Select the **Use Perfect Forward Security** checkbox.



4. Tap **Continue** in WinCE OS or the the arrow/check icon in Palm OS until editing changes to the policy are complete and the **movianVPN** window appears.
5. Tap **Login**. Perfect Forward Security will be enabled for the policy.

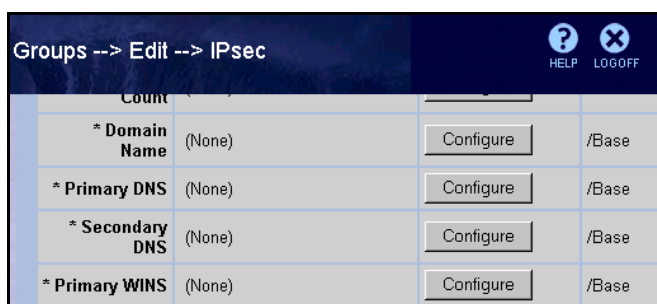
DNS Support

The Domain Name System (DNS) is used to identify particular computers or parts of the network. Some gateways supply this information to the handheld device during key negotiation.

If Query DNS is checked, the handheld device will download the DNS information from the gateway server. If you supply the DNS information, your handheld device's settings will override other information provided by the gateway.

Enabling DNS support on the gateway

1. In the navigation sidebar, select **Profile**, then **Groups**.
2. Click **Configure** under **IPSec**.



3. Under **domain name**, select **Configure** and enter the domain name.
4. Under **Primary DNS**, select **Configure** and enter the address.
5. Under **Secondary DNS**, select **Configure** and enter the address.
6. Click **OK**.

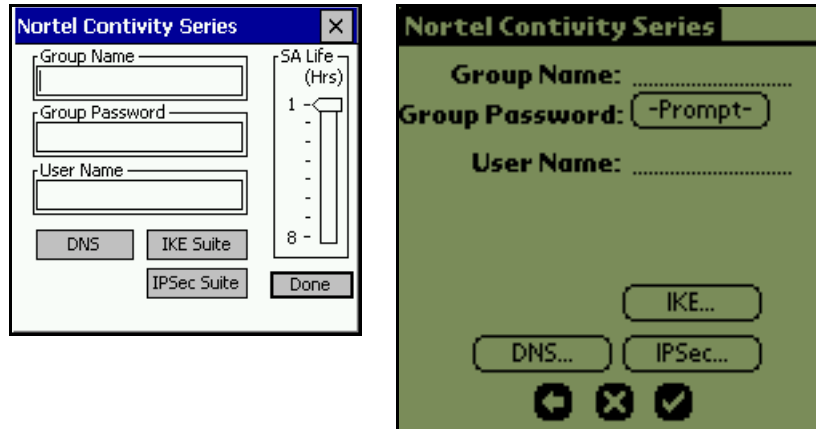
Enabling DNS support on the movianVPN client

If the client is supplying DNS settings, they must be set on the client software.

To enable and set DNS support:

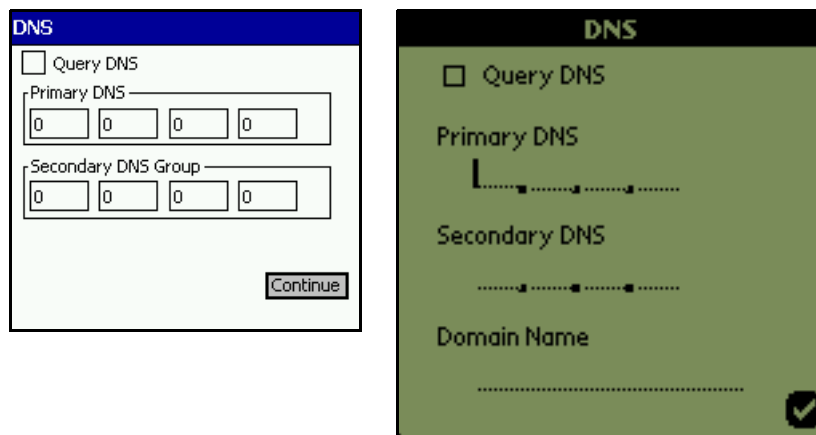
1. On the **movianVPN** client, enter or select the Policy Name.
2. Tap **Edit**.
3. Tap **Continue** for WinCE OS or tap the arrow icon for Palm OS.

- The gateway window will appear..



Note: If extended authentication has not been selected as an option, the windows will appear with User Name and User Password.

- Select **DNS ...**
- Uncheck the **Query DNS** box. The DNS entry fields appear.



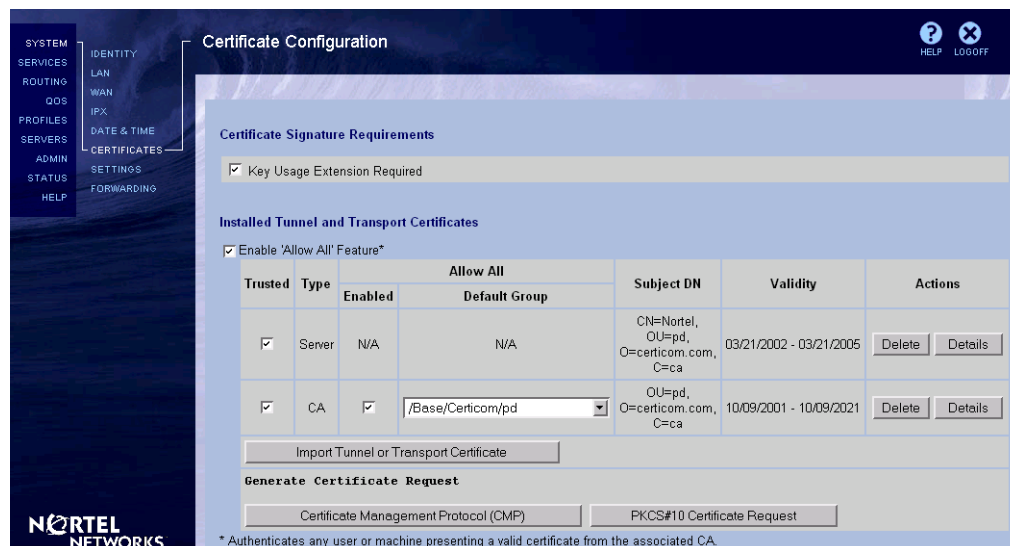
- Enter the **Primary** and **Secondary DNS** addresses. In Palm OS, enter the **Domain Name**.
- Tap **Continue** in WinCE OS or tap the checkmark icon in Palm OS.
- Tap **Done**.

Authentication Using Certificates

The **movianVPN** client supports certificate-based authentication with the Nortel Contivity Series gateway.

Installing Certificates

You must install a certificate on the VPN gateway to allow clients to authenticate. In the navigation sidebar, select **System**, then **Certificates**. This displays a list of installed certificates.



Certificate Configuration

Certificate Signature Requirements

Key Usage Extension Required

Installed Tunnel and Transport Certificates

Enable 'Allow All' Feature*

Trusted	Type	Enabled	Allow All		Subject DN	Validity	Actions
			Default Group				
<input checked="" type="checkbox"/>	Server	N/A	N/A		CN=Nortel, OU=pd, O=certicom.com, C=ca	03/21/2002 - 03/21/2005	Delete Details
<input checked="" type="checkbox"/>	CA	<input checked="" type="checkbox"/>	/Base/Certicom/pd		OU=pd, O=certicom.com, C=ca	10/09/2001 - 10/09/2021	Delete Details

Import Tunnel or Transport Certificate

Generate Certificate Request

Certificate Management Protocol (CMP) PKCS#10 Certificate Request

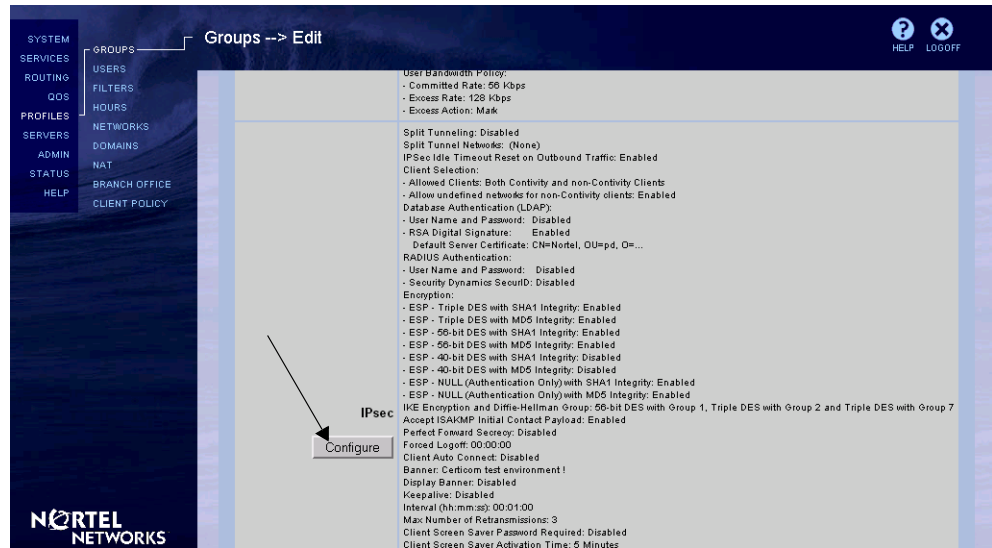
* Authenticates any user or machine presenting a valid certificate from the associated CA.

Consult your gateway documentation for detailed certificate installation instructions.

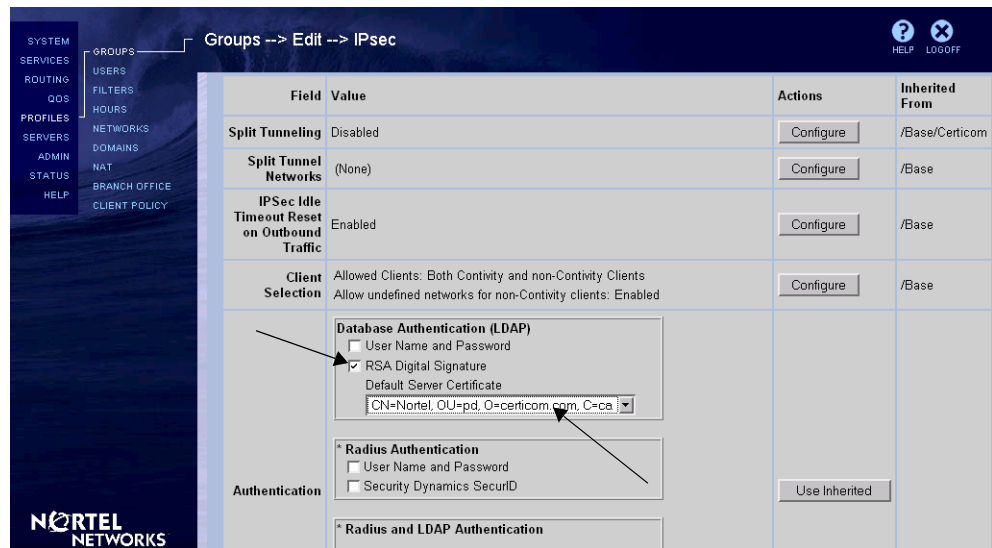
Using Certificates

Once a certificate of the correct type has been installed, you can configure the VPN gateway so that users can use certificates for authentication.

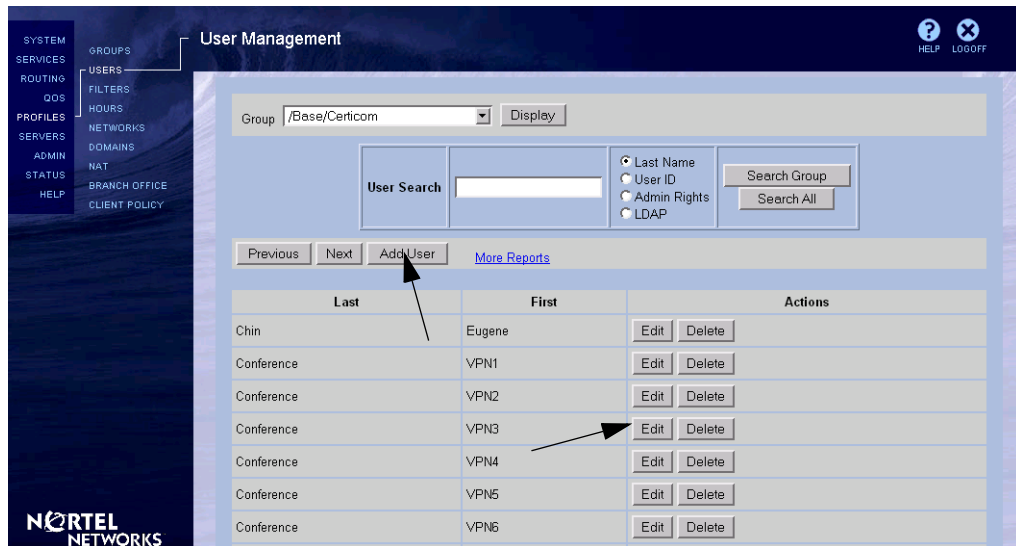
1. In the navigation sidebar, select **Profile**, then **Groups**. Then click **Configure** to edit the **IPSec** settings.



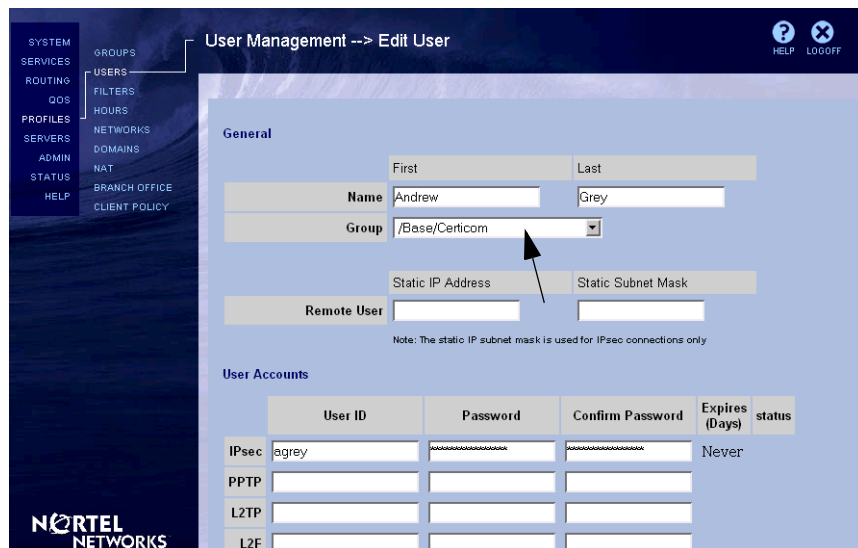
2. Activate the **RSA Digital Signature** checkbox in the **Database Authentication (LDAP)** configuration section. Select the appropriate entry from the **Default Server Certificate** drop-down list.



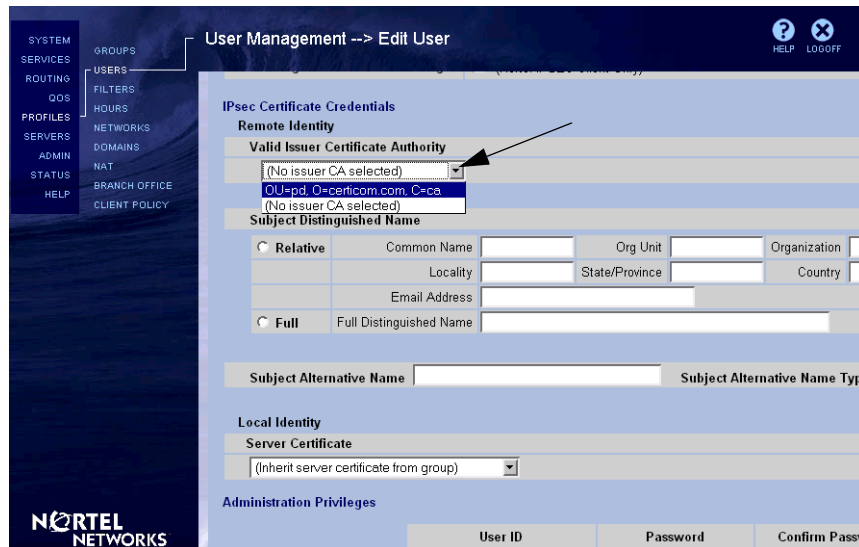
- In the navigation sidebar, select **Profile**, then **Users**. Create a new user by clicking **Add User** or modify an existing user's configuration by clicking **Edit** beside a user's name.



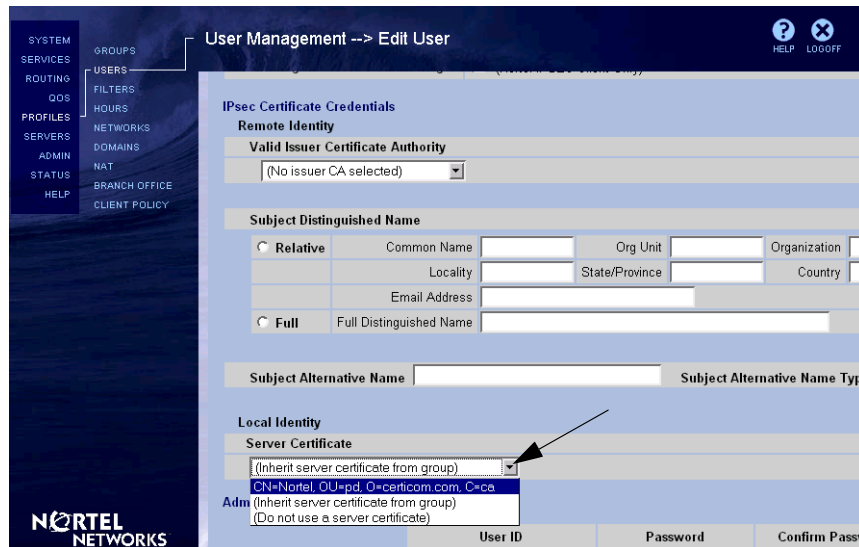
- Select the group you have configured to use digital certificates for authentication from the **Group** drop-down list.



5. Select the correct **Certificate Authority** from the drop-down list.



6. Select the correct **Server Certificate** from the drop-down list.



External Authentication

Extended Authentication requires the user to supply an additional authentication when logging in to the gateway. Depending on the form of authentication required, users can be asked to supply a User Password or a passcode associated with a token card.

movianVPN client must be configured to support external authentication.

Setting up an external Radius authentication server

To set up a Radius authentication server, you must select the authentication method and then enable the server.

To set up a Radius authentication server:

1. In the navigation sidebar, select **Profiles**, then **Groups**.
2. Select the group, then click **Edit**.
3. Click on **Configure** (under **IPsec**).
4. In the Profiles|Groups|IPSec window, under **Authentication**, click on **Configure**.

The screenshot shows the configuration interface for a group's IPsec settings. The breadcrumb path is 'Groups --> Edit --> IPsec'. The 'Authentication' section is expanded, revealing three options:

- Database Authentication (LDAP)**: Includes a checked checkbox for 'User Name and Password'.
- * Radius Authentication**: Includes unchecked checkboxes for 'User Name and Password' and 'Security Dynamics SecurID'.
- * Radius and LDAP Authentication**: Includes a sub-section 'Group ID and Password' with a note: 'Note: Required for all groups using RADIUS or LDAP authentication.' Below this are three input fields: 'Group ID', 'Group Password', and 'Group Confirm Password'.

A 'Use Inherited' button is located to the right of the authentication options.

5. Under **Radius authentication**, select the **username and password** box. If the user has a physical token, then select the **Security Dynamics SecurID** box.
6. Enter the **group ID**, the **password**, and the **confirmation**.

Enabling the server address

To enable the server address:

1. In the navigation sidebar, select **Servers**, then **Radius authentication**.

RADIUS Authentication

Enable Access to RADIUS Authentication

Remove Suffix from User ID (e.g. jsmith@nortelnetworks.com)
 Delimiter Value=@

RADIUS Users Obtain Default Settings from the Group /Base/Radius

Server-Supported Authentication Options

Enabled	Type	Description
<input type="checkbox"/>	CHALLENGE	Challenge/Response Token Cards
<input checked="" type="checkbox"/>	RESPONSE	Response Only Token Cards
<input type="checkbox"/>	MS-CHAP	MSCHAP - Microsoft encrypted CHAP. <input type="checkbox"/> RFC-2548 (Microsoft Vendor-specific RADIUS Attributes) compliant
<input type="checkbox"/>	CHAP	CHAP - Challenge Handshake Authentication Protocol.
<input checked="" type="checkbox"/>	PAP	PAP - Password Authentication Protocol.

RADIUS Servers

2. Check the **Enable Access to RADIUS Authentication** box.
3. Select appropriate options under **Server-supported authentication options**.
4. In the **Radius server** section, enable **IP address** and **interface**.

RADIUS Servers

Enabled	Server	Host Name or IP Address	Interface	Status	Port	Secret	Confirm Secret
<input type="checkbox"/>	Primary	10.5.1.100	Private (10.5.1.2) Public 207.176.222.68	Not Configured	1645	XXXXXXXXXX	XXXXXXXXXX
<input checked="" type="checkbox"/>	Alternate 1	10.5.1.101	Private (10.5.1.2) Public 207.176.222.68	Operational	1812	XXXXXXXXXX	XXXXXXXXXX
<input type="checkbox"/>	Alternate 2		Private (10.5.1.2) Public 207.176.222.68	Not Configured	1645		

Response Timeout Interval 10 (seconds)

Maximum Transmit Attempts 3

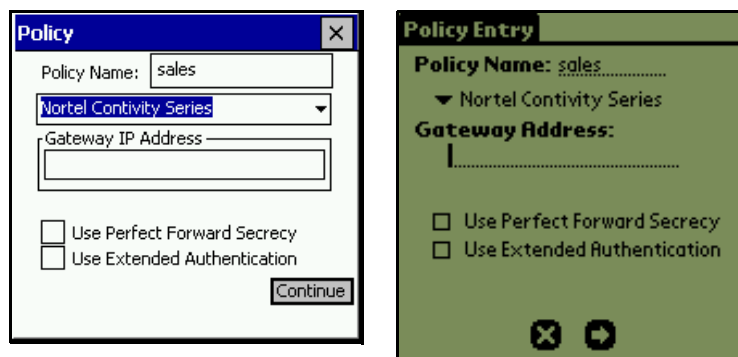
5. Enter the **port number** and **secret**.
6. Enter the **confirmation**.
7. Click **OK**.

Enabling External Authentication on the movianVPN client

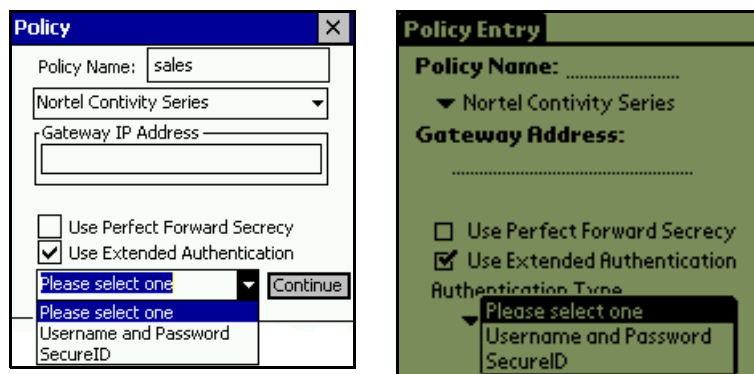
Once the gateway will support extended authentication, users can enable the function on their clients.

To enable Extended Authentication on the **movianVPN** client:

1. In the **movianVPN** window, select the policy.
2. Tap **Edit**.
3. Select the Use Extended Authentication checkbox in the policy window

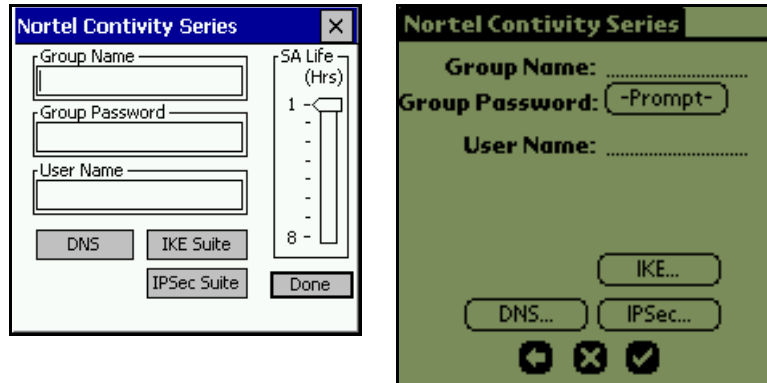


4. A pull-down list appears..



5. Select which type of Extended Authentication to use.

6. Tap **Continue** in WinCE OS or the the arrow icon in Palm OS..



7. Enter the Group Name, Group Password, and User Name as created in “Configuring your gateway to support movianVPN” on page 11.
8. Tap **Continue** in WinCE OS or the the arrow icon in Palm OS until editing changes to the policy are complete and the **movianVPN** window appears.
9. Tap **Login**. Extended Authentication will be enabled for the policy.
When logging in to the gateway, the user will be asked for an additional password or passcode.

NAT Traversal

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.

The Nortel gateway and the movianVPN client can overcome this limitation by adding a UDP header to each packet. The NAT gateway can then carry out its address translation as normal by modifying this header.

The section below shows you how to set 'NAT traversal' on the Nortel gateway.

Note: NAT traversal is only available in version 4.x of the configuration software.

Enabling NAT traversal on the gateway

1. In the navigation sidebar, select **Profile**, then **Groups**.
2. Select the group, then click on **Edit**.
3. Click **Configure** under **IPsec**.
4. Scroll down if necessary, to **NAT Traversal** and click **Configure**.

The screenshot shows the configuration page for an IPsec profile. The breadcrumb navigation at the top reads "Groups --> Edit --> IPsec". There are "HELP" and "LOGOFF" icons in the top right corner. The main configuration area is a table with the following rows:

IPsec Transport Mode Connections	Disabled	Configure	/Base
* NAT Traversal	<input type="text" value="Auto-Detect NAT"/> <ul style="list-style-type: none"> Auto-Detect NAT Not Allowed Auto-Detect NAT Auto-Detect IPsec capable NAT 	Use Inherited	
	All Fields	Configure	Use Inherited

5. Set **NAT traversal** to **auto-detect NAT**.
6. Leave **Nat keep-alive** at its default value.
7. Click **OK**.

Banner Support and Password Save Feature

You can configure the Nortel gateway so that a welcome screen or banner appears on the client screen whenever the user logs on to the gateway.

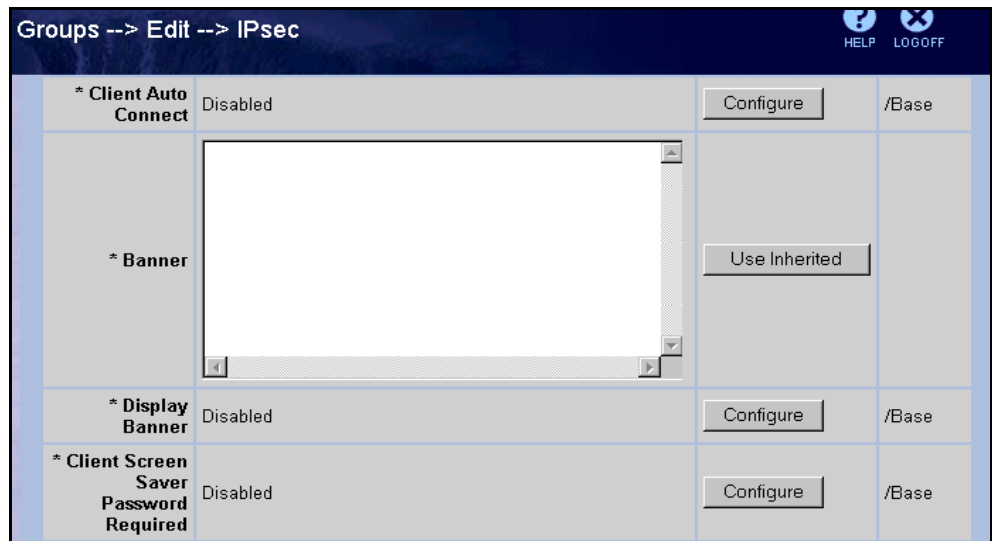
As a security feature, you can also prevent the user from saving their password on their handheld device.

The following section shows you how you can modify the settings for the banner support and password save features.

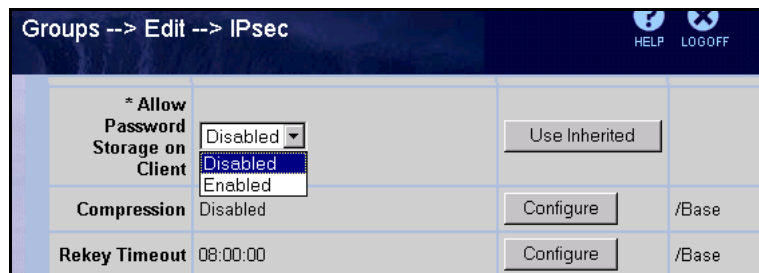
Enabling banner support and password save feature on the gateway

To enable banner support and password save:

1. In the navigation sidebar, select **Profiles**, then **Groups**.
2. Select the group then click on **Edit**.
3. Scroll down if necessary, to **Display Banner** and click **Configure**.



4. Enable **Display Banner**.
5. Enter the banner message in the window.
6. Scroll if necessary, to **Allow Password Storage on Client** and click **Configure**.



7. Enable **Allow Password Storage On Client**.
8. Click **OK**.

6

Deploying a pilot scheme

If you plan on setting up a pilot scheme with movianVPN, you should consider setting an IP address range to include all your users.

Choosing a range of IP addresses

To choose a range of IP addresses:

1. Go to **Servers**, then **user IP address**.

The screenshot shows the 'Remote User IP Address Pool' configuration window. It includes fields for 'Secondary' and 'Tertiary' IP addresses, both set to '0.0.0.0' and marked as '*Optional'. Below these are fields for 'DHCP Cache Size' (set to 5), 'Immediate Address Release' (checked), 'DHCP Blackout Interval*' (set to 300 seconds), and 'Override Blackout Interval when no addresses are available' (checked). A table titled 'Address Pool' shows a single entry: 'default' with start '10.5.1.61', end '10.5.1.90', subnet mask '255.255.0.0', total '30', and in use '0'. An 'Add' button is visible below the table, and another 'Address Pool Blackout Interval*' field is at the bottom.

Secondary	Optional	Not Configured
0.0.0.0	*Optional	Not Configured
Tertiary	Optional	Not Configured
0.0.0.0	*Optional	Not Configured

DHCP Cache Size: 5

Immediate Address Release:

DHCP Blackout Interval*: 300 (seconds) *Amount of time before an address is available for reissue.

Override Blackout Interval when no addresses are available:

Address Pool						
Pools	Start	End	Subnet Mask	Total	In Use	Action
default	10.5.1.61	10.5.1.90	255.255.0.0	30	0	Edit Delete

Add

Address Pool Blackout Interval*: 0 (seconds) *Amount of time before an address is available for reissue.

2. Enter a **name** for the address range.
3. Click **Add**.

4. Enter **IP address range** and the **subnet mask**. Click **OK**.
5. In the navigation sidebar, select **Group**, then **Connectivity**.
6. Under **Address Pool Name**, click on **Configure**.

RSVP: Token Bucket Depth	3000 Bytes	Configure	/Base
RSVP: Token Bucket Rate	28 Kbps	Configure	/Base
Address Pool Name	(None defined on this switch) New Address Pool	Use Inherited	
User Bandwidth Policy	Excess Rate: 128 Kbps Excess Action: Mark	Configure	/Base

7. Select the **Name**.
8. Click **OK**.

Bandwidth Considerations

Your Internet Service provider must have sufficient bandwidth to support all your **movianVPN** users.

A

Appendix A: Using the Diagnostic Tools

The following diagnostic tools are available for **movianVPN** clients:

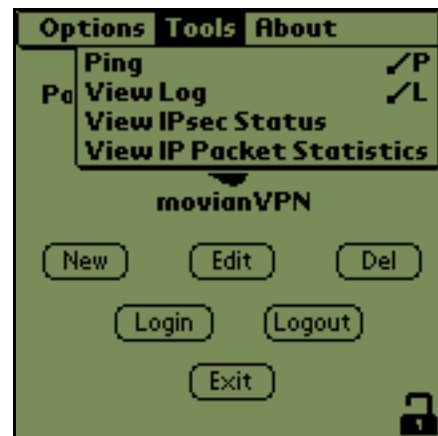
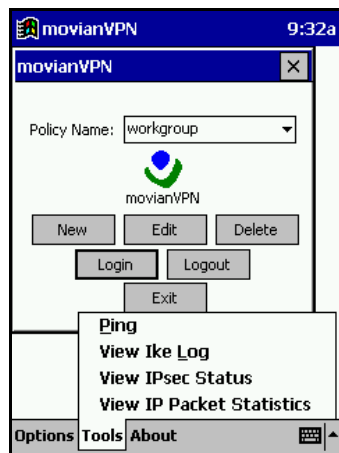
- Ping
- View IPsec Status
- View IP Packet Status

Note: For further diagnostic procedures, refer to the gateway configuration manual for information on how to view the connection log.

Accessing diagnostic tools

To access the diagnostic tools:

1. In the **movianVPN** window
 - For WinCE, tap **Tools** in the lower tool bar
 - For Palm OS tap the **movianVPN** tab in the top of the window and tap **Tools**.



2. Tap the diagnostic tool you want to open

Ping

Use Ping to determine whether you have established a connection with or have access to a particular server.

Note: If the first attempt fails, ping the server twice.

Using Ping with a WinCE client

To ping a server with a WinCE device:

1. Tap **Tools** and select **Ping** from the list.

The Ping window appears.



2. Enter the IP address of the server you wish to ping.

3. Tap **Ping**.

The Ping window will display the results.



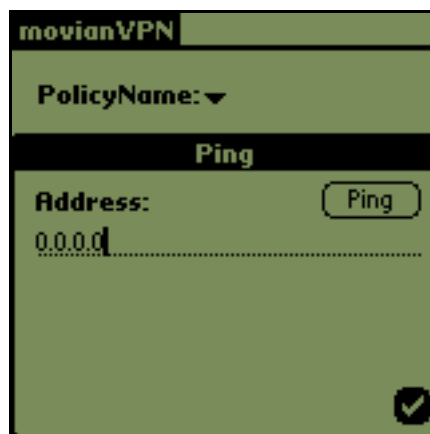
4. To close the window, tap **OK** or the **X** in the top right corner of the Ping window.

Using Ping with a Palm OS client

To ping a server using a Palm OS device:

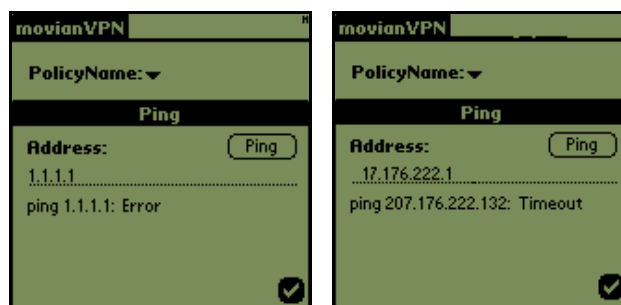
1. Tap the **movianVPN tab**.
2. Tap **Tools** and select **Ping** from the list.

The Ping window appears.



3. Enter the IP address of the server you wish to ping.
4. Tap **Ping**.

The Ping window will display the results.



5. Tap the checkmark icon when finished.

IPSec Status Log

IPSec Status can be used to confirm that a tunnel is working and provide information about it.

Note: View IPSec Status is only available while the VPN tunnel is up.

Viewing IPSec Status for a WinCE client

To view IPsec status with a WinCE device:

1. Tap **Tools** and select **View IPSec Status** from the list.

The IPsec Status window appears.



The fields provide status information on the handheld device and gateway.

2. Tap **OK** when finished.

The fields provide the following information:

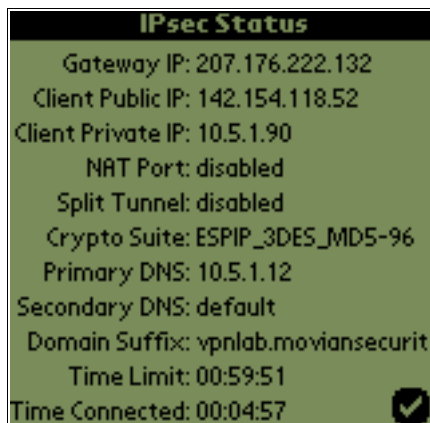
Field	Information
Gateway IP	VPN gateway server IP address
Client Public IP	IP address supplied by ISP
Client Private IP	IP address within the VPN
NAT Port	If NAT is enabled
Split Tunnel	If Split Tunnel is enabled
Crypto Suite	Crypto Suite setting
Primary DNS	DNS setting from VPN gateway or supplied by client
Secondary DNS	DNS setting from VPN gateway or supplied by client
Domain Suffix	In Palm OS, setting from VPN gateway or supplied by client
Time Limit	SA proposal
Time Connected	Since tunnel established

Viewing IPSec Status for a Palm OS client

To view IPSec status with a Palm OS device:

1. Tap the **movian VPN tab**.
2. Tap **Tools** and select **View IPSec Status** from the list.

The IPSec Status window appears.



The fields provide status information on the handheld device and gateway.

3. Tap the checkmark icon when finished.

The fields provide the following information:

Field	Information
Gateway IP	VPN gateway server IP address
Client Public IP	IP address supplied by ISP
Client Private IP	IP address within the VPN
NAT Port	If NAT is enabled
Split Tunnel	If Split Tunnel is enabled
Crypto Suite	Crypto Suite setting
Primary DNS	DNS setting from VPN gateway or supplied by client
Secondary DNS	DNS setting from VPN gateway or supplied by client
Domain Suffix	In Palm OS, setting from VPN gateway or supplied by client
Time Limit	SA proposal
Time Connected	Since tunnel established

IP Packet Statistics Log

IP Packet Statistics are used primarily for diagnostic purposes. The window provides information on the amount of traffic passing through the tunnel, and its reliability. Your VPN administrator may ask you to clear the statistics while debugging; this will clear the statistics from previous communications, for example from a previous VPN session or if you have been using the Internet before starting the VPN tunnel.

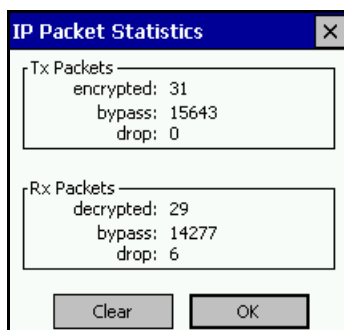
Note: View IP Packet Statistics is only available while the VPN tunnel is up.

Viewing IP Packet Statistics for a WinCE client

To view IP Packet Statistics with a WinCE device:

1. Tap **Tools** and select **View IP Packet Statistics** from the list.

The IP Packet Statistics window appears.



2. Tap **Clear** to clear information, if desired.
3. Tap **OK** when finished.

The fields indicate the following information:

Field	Information
Tx Packets	Transmitted encrypted packets
Rx Packets	Received packets

Packets may be:

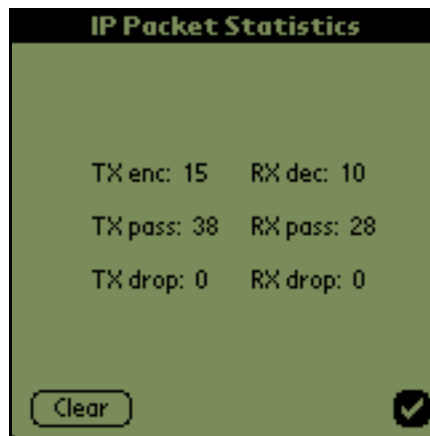
- Encrypted/decrypted
- Bypass: Sent without encryption
- Drop: Dropped from communication

Viewing IP Packet Statistics for a Palm OS client

To view IP Packet Statistics with a Palm OS device:

1. In the **movianVPN** window, tap the **movianVPN tab**.
2. Tap **Tools** and select **View IP Packet Statistics** from the list.

The IP Packet Statistics window appears.



3. Tap **Clear** to clear information, if desired.
4. Tap the checkmark icon when finished.

The fields indicate the following information on transmitted encrypted packets:

- Encrypted/decrypted
- Bypass: Sent without encryption
- Drop: Dropped from communication

B

Appendix B: Glossary of Terms

Authentication Authentication refers to the verification of the identity of communicating parties.

**AH
Authentication
Header** Part of the IPSec protocol, the Authentication Header allows communicating parties to verify both the source and integrity of the data.

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 Server** Domain Name Server (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.

**ESP
Encapsulation
Security Payload**

Part of the IPSec protocol, provides encryption for data exchange security.

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.

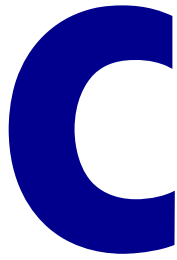
When you select Split Tunneling, packets of data headed to inside the VPN will still be encrypted and forwarded. Packets that are not directed to inside the VPN will not be encrypted, nor is the reply.

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: Client configuration worksheet

Information required for client configuration

The following information will be required by your users to create a 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 the configuration you have selected for your gateway and for the users of the gateway.

Information required for creating a policy

Field, Checkbox or Button	Required	Information/Action
Policy Name		
Gateway Type (Please select one)		
Gateway IP Address		
Split Tunnelling		
Perfect Forward Secrecy		
Extended Authentication		
DNS checkbox		Primary DNS:
		Secondary DNS Group:
IKE Suite		Group:
		Cipher:
		Hash:
Group Name		
Group Password		
User Name		
User Password		
User Passcode (SecurID)		
Network Properties		Primary Subnet IP Address:
		Primary Subnet Subnet Mask:
		Secondary Subnet IP Addresses:
		Secondary Subnet Subnet Masks:
IPSec Suite		
SA Lifetime		
Options > Connection Type		
Options > Dial-up RAS entry		