

movianVPN™

Version 3.0.5

© 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.

movianVPN Deployment Guide for Intel Netstructure VPN 3100 Series

PUB-0200-2000
May 14, 2003

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
Reaching movianVPN 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 security profile	12
Creating a tunnel	14
Adding a user	16
Creating a movianVPN policy for your gateway	19
Before you begin	19
Creating the policy	20
Creating a basic WinCE policy	21
Creating a Palm OS policy	24
Testing the policy	29
If the connection fails	29
Logging out of the gateway	30
Configuring features on movianVPN	31
IPSec	31
IPSec Crypto Suite	34
IKE Crypto Suite	34

Enhancing your movianVPN policy	37
Split Tunneling	37
Enabling split tunneling on the gateway	37
Enabling split tunneling on the movianVPN client	38
Perfect Forward Secrecy	39
Enabling perfect forward secrecy on the gateway	39
Enabling perfect forward secrecy on the movianVPN client	41
External Authentication	42
Setting up an external Radius authentication server	42
Enabling external authentication on the movianVPN client	43
DNS Support	45
Enabling DNS support	45
Enabling DNS on the movianVPN client	47
Deploying a pilot scheme	49
Choosing a range of IP addresses	49
Bandwidth Considerations	50
Appendix A: Using the Diagnostic Tools	51
Accessing diagnostic tools	51
Ping	52
Using Ping with a WinCE client	52
Using Ping with a Palm OS client	53
IPSec Status Log	54
Viewing IPSec Status for a WinCE client	54
Viewing IPSec Status for a Palm OS client	55
IP Packet Statistics Log	56
Viewing IP Packet Statistics for a WinCE client	56
Viewing IP Packet Statistics for a Palm OS client	57
Appendix B: Glossary of Terms	59
Appendix C:	
Client configuration worksheet	63
Information required for client configuration	63
Information required for creating a policy	64

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:

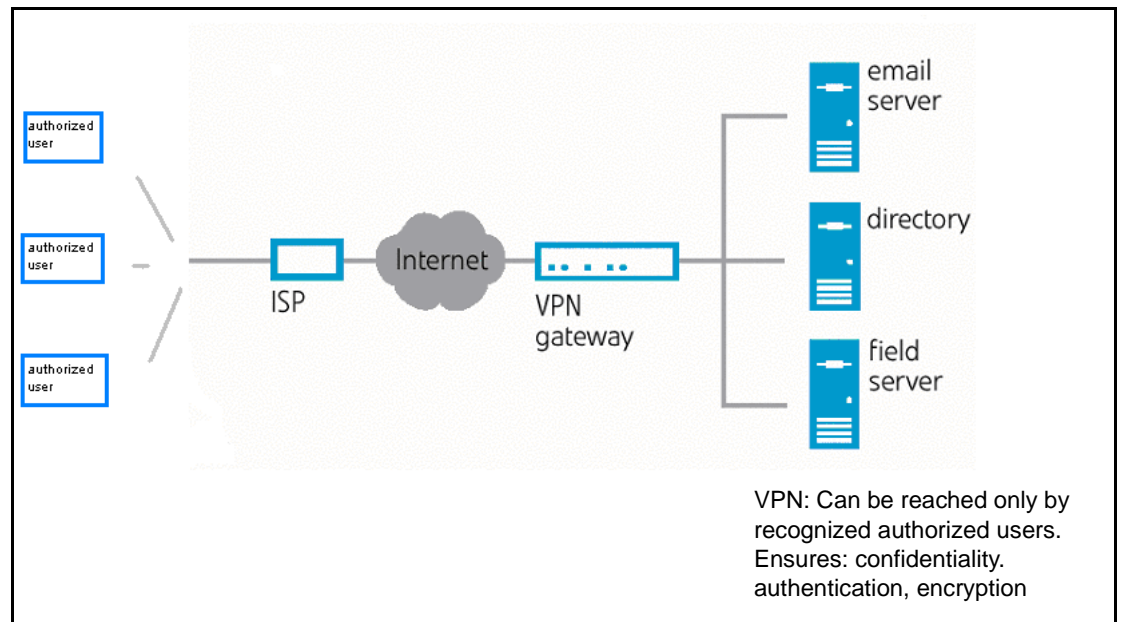
- **Intranet VPN:** Between a central corporate site and branch offices
- **Remote access VPN:** Between a central corporate site and individual remote users (the **movianVPN** model)
- **Extranet VPN:** Between an enterprise and its business partners, suppliers, and customers

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

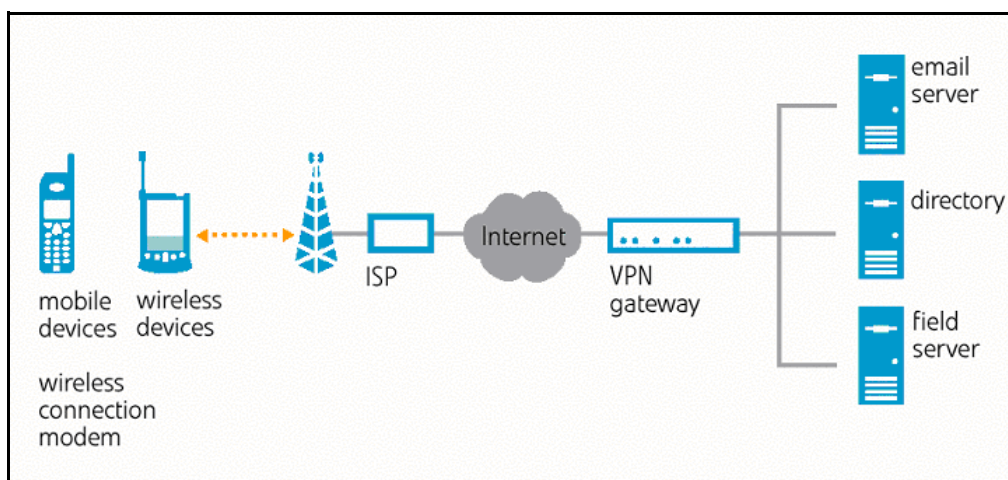
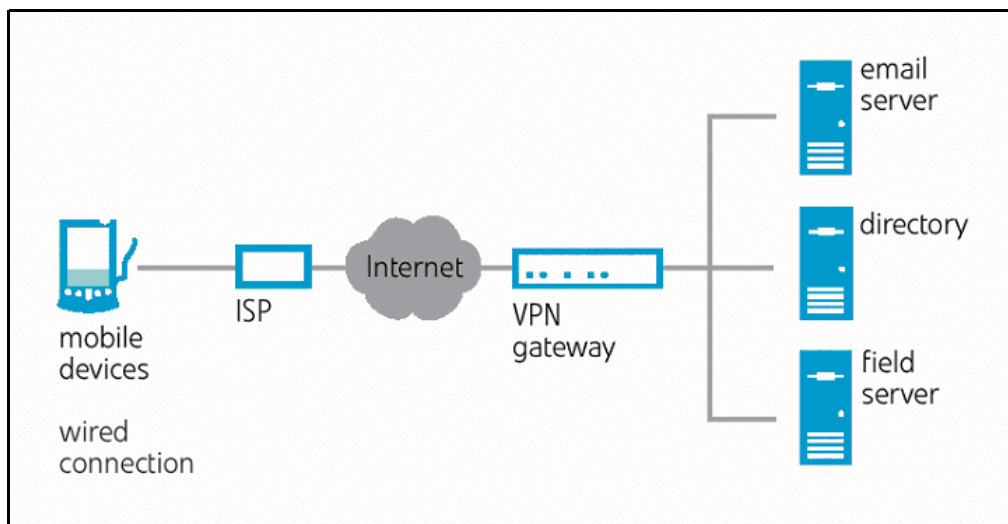
Using **movianVPN**, a traditional VPN can also have handheld devices added to the configuration without compromising network security.

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 Intel Netstructure VPN 3100 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
Intel	Netstructure VPN 3100 Series	6.9p4 and 7.0

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 37.

To configure your gateway to support movianVPN, you will

- Create a security profile
- Create a tunnel
- Add a user

Gateway software

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

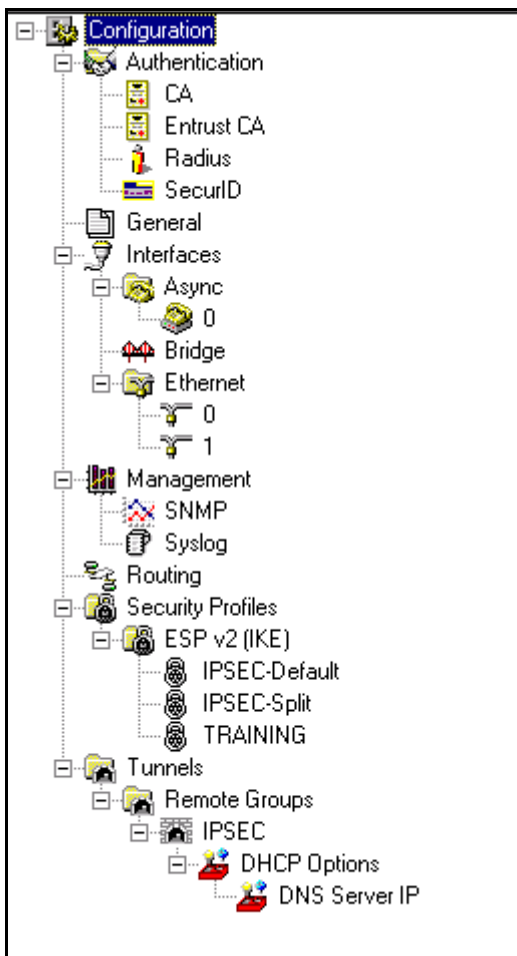
Note: If you have an older version of the software, you should upgrade. Please see the documentation for your gateway for the procedure.

Gateway	Product	Supported software versions
Intel	Netstructure VPN 3100 Series	6.9p4 and 7.0

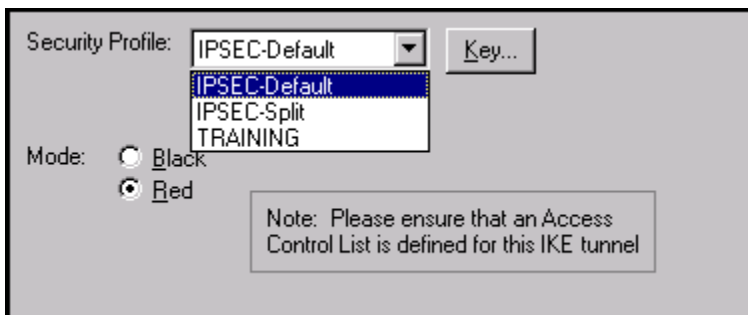
Creating a security profile

To create a security profile:

1. On the main menu, go to **Configure** then **Normal Configuration**.



2. In the new window (entitled **DevVPN - Normal Configuration**) menu, go to **Configuration**, then **Security Profiles** then **ESPv2 (IKE)**.
3. Select the default security profile (**IPSecDefault**).



Authentication:	<input type="text" value="Key"/>	Public Key (bits):	<input type="text"/>
IKE			
Algorithm:	<input type="text" value="3-DES (168-bit key)"/>		
Authentication:	<input type="text" value="HMAC MD5"/>		
Key Lifetime (time):	<input type="text" value="1"/>	<input type="text" value="hour(s)"/>	
<input type="checkbox"/> (Kbytes):	<input type="text" value="20,480"/>		
DH Group:	<input type="text" value="7 - ECC 1024 Bit"/>	<input checked="" type="checkbox"/> Aggressive Mode	
IPSec			
ESP Algorithm:	<input type="text" value="3DES (168-bit key)"/>		
ESP Authentication:	<input type="text" value="HMAC MD5"/>		
Authentication Header:	<input type="text" value="None"/>		
Key Lifetime (time):	<input type="text" value="1"/>	<input type="text" value="hour(s)"/>	
<input type="checkbox"/> (Kbytes):	<input type="text" value="20,480"/>		
Secondary Authentication:	<input type="text" value="None"/>	<input type="checkbox"/> Perfect Forward Secrecy	
		<input type="checkbox"/> Tunnel AH Mode	
		<input checked="" type="checkbox"/> Tunnel ESP Mode	
<input type="checkbox"/> Keepalive:	<input type="text" value="15"/>	<input type="text" value="second(s)"/>	
<input checked="" type="checkbox"/> Timeout:	<input type="text" value="1"/>	<input type="text" value="hour(s)"/>	
<input checked="" type="checkbox"/> Client Timeout:	<input type="text" value="1"/>	<input type="text" value="hour(s)"/>	
<input type="checkbox"/> Client Keepalive:	<input type="text" value="15"/>	<input type="text" value="second(s)"/>	
<input type="checkbox"/> UDP Encapsulation Port:	<input type="text" value="2233"/>	<input type="checkbox"/> Propose Higher Security	
		<input type="checkbox"/> Set Commit Bit	
		<input type="checkbox"/> Split Tunneling	
		<input checked="" type="checkbox"/> Preserve TOS Bits	

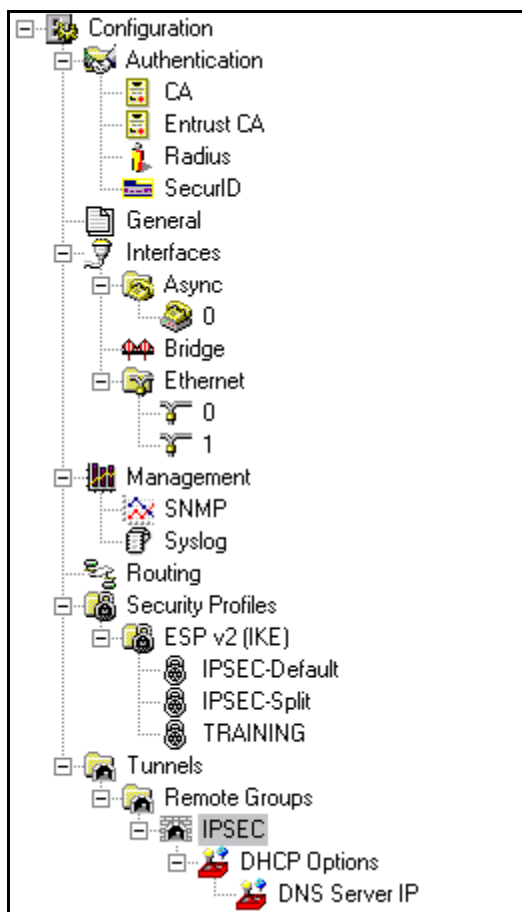
4. Make sure the **Authentication** field is set to **Key**. Click the field and select the setting from the pull-down list if necessary.
5. Use the default **IKE algorithms**.
6. Set the **DH group** according to your handheld device's operating system:
 - If running **movianVPN** on a Palm device, set **DH Group** to **7-ECC-1024 Bit**.
 - If running **movianVPN** on a WinCE device, set **DH Group** to either **1-768 Bit** or **2-1024 Bit**.

7. Enable **Aggressive Mode**.
8. Set **ESP algorithm** to **3DES (168-bit key)**.
9. Set **Authentication Header** to **None**.
10. Set **Secondary Authentication** to **None**.
11. Set **Perfect Forward Secrecy** to **Off**.
12. Make sure **tunnel ESP mode** checkbox is enabled.
13. Deselect **UDP encapsulation** checkbox.
14. Deselect **Propose Higher Security** checkbox.
15. Deselect **Set Commit bit** checkbox.
16. Deselect **Split Tunneling** checkbox.
17. Leave **Preserve TOS Bits** checkbox enabled.

Creating a tunnel

To create a tunnel:

1. Go to **Tunnels**, then **Remote Group**, then **IPSec**.



2. Select the default security profile (**IPSecDefault**).

Security Profile: **IPSEC-Default**

Mode: Black Red

Note: Please ensure that an Access Control List is defined for this IKE tunnel

Subnets

IP Address	Subnet Mask	Include/Exclude
10.5.1.0	255.255.255.0	Include

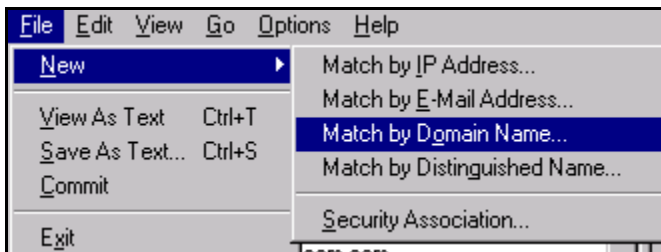
Client IPs

IP Address/DHCP	Count	DHCP Gateway
10.5.1.171	9	

3. Set **Security Profile** to **IPSecDefault** group.
4. Set **Mode** to **Red**.
5. Under **Subnets**, click **Add**.
6. Add the **Subnets** which are connected to the private side of the gateway.
7. On the main menu, go to **File**, then **Commit** to save the settings.

Adding a user

1. On the main menu, go to **Configure, Access Control List** then **Normal Image**.
2. In the new window menu, go to **File**, then **New**, then **Match by Domain Name...**

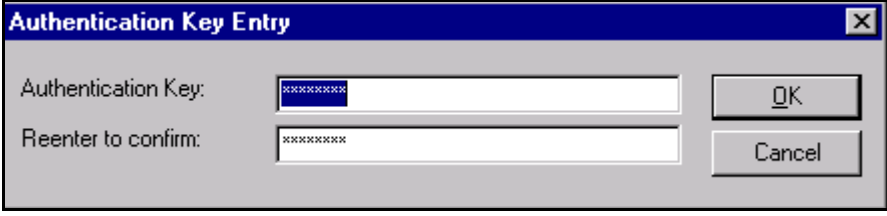


3. Enter the **user name**, then click **OK**.

 A screenshot of a configuration dialog box. The 'Authentication' checkbox is checked and set to 'Key'. The 'Negotiation Type' is set to 'Aggressive'. The 'IKE Algorithm' is set to 'DES (56-bit)'. The 'IKE Authentication' is set to 'HMAC MD5'. The 'IKE Key Lifetime (time)' is set to '720' minutes. The 'IKE Key Lifetime (Kbytes)' is set to '20,480'. There are also fields for 'Keepalive', 'Timeout', 'Client Timeout', and 'Client Keepalive'. The 'DH Group' is set to '7 - ECC 1024 Bit'. The 'Client IP' checkbox is checked and the field is empty. The 'Shared Secret' checkbox is checked and set to 'Set Secret...'. The 'Split Tunneling' is set to 'Off'. The 'Secondary Authentication' is set to 'None'. The 'Encapsulation' is set to 'IPSec'. The 'UDP Encapsulation Port' is set to '2233'. The 'Preserve Type Of Service' is set to 'Preserve TOS bits'. The 'PPP Authentication' is set to 'None'. A note on the right states: 'Note: Please ensure that this IP address is on a subnet permitted by an SA under this ACL match'.

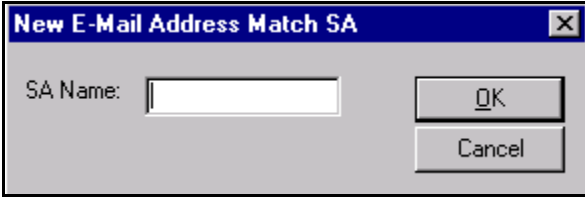
4. Select the **Client IP** checkbox and enter the IP address of the user.
5. Set **Authentication** to **Key**.

- Select the Shared Secret checkbox, click on **Set Secret...**



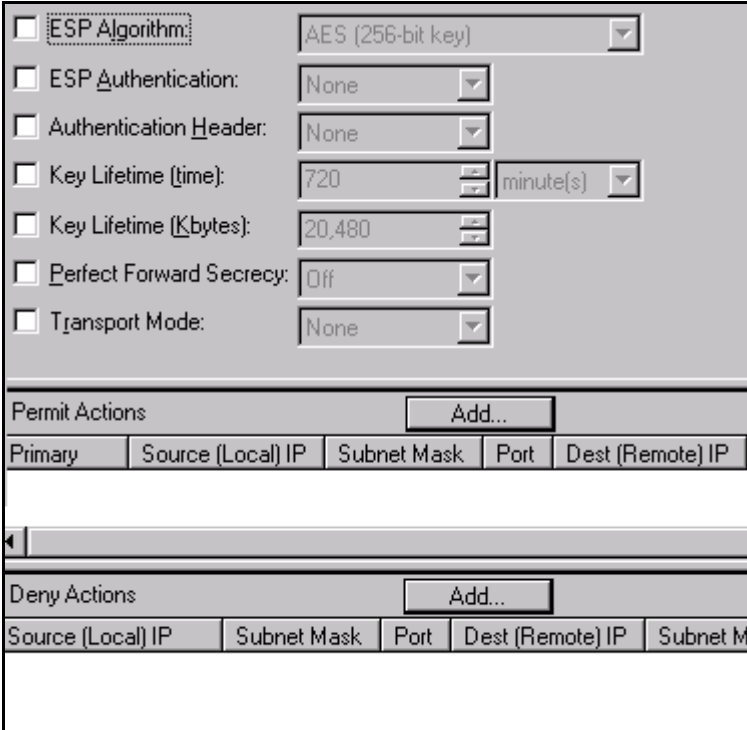
The dialog box titled "Authentication Key Entry" has a blue title bar with a close button. It contains two text input fields. The first field is labeled "Authentication Key:" and contains a masked password (represented by asterisks). The second field is labeled "Reenter to confirm:" and also contains a masked password. To the right of the first field is an "OK" button, and to the right of the second field is a "Cancel" button.

- Enter the **user password** and confirm it.
- Click **OK**.
- In the window menu, go to **File**, then **New**, then **Security Association**.
- Enter a **name** for the Security Association.



The dialog box titled "New E-Mail Address Match SA" has a blue title bar with a close button. It contains a single text input field labeled "SA Name:". To the right of the field are "OK" and "Cancel" buttons.

- Click **OK**.
- Leave the remaining settings at their default values:



The Security Association configuration dialog box is divided into several sections. The top section contains several options, each with a checkbox and a dropdown menu or spinner:

- ESP Algorithm: AES (256-bit key)
- ESP Authentication: None
- Authentication Header: None
- Key Lifetime (time): 720 minute(s)
- Key Lifetime (Kbytes): 20,480
- Perfect Forward Secrecy: Off
- Transport Mode: None

 Below this is a "Permit Actions" section with an "Add..." button and a table with columns: Primary, Source (Local) IP, Subnet Mask, Port, and Dest (Remote) IP. The table is currently empty. Below that is a "Deny Actions" section with an "Add..." button and a table with columns: Source (Local) IP, Subnet Mask, Port, Dest (Remote) IP, and Subnet M. This table is also empty.

- Under **Permit Actions**, click **Add**.

The screenshot shows a dialog box titled "New Domain Permit Action". It has a close button in the top right corner. The dialog contains the following fields and controls:

- Source (Local):** Three input fields for "IP Address", "Subnet Mask", and "Port". The "Port" field is a dropdown menu currently set to "ALL".
- Dest (Remote):** Three input fields for "IP Address", "Subnet Mask", and "Port". The "Port" field is a dropdown menu currently set to "ALL".
- Dynamic:** A checkbox that is currently unchecked.
- Protocol:** A dropdown menu currently set to "ALL".
- Primary:** A checkbox that is currently checked.
- Buttons:** "OK" and "Cancel" buttons are located on the right side of the dialog.

- In the **Source (Local)** fields, enter the **IP Address** and **Subnet Mask** of the private side of the gateway.
- Under **Dest (Remote)**, select the **Dynamic** checkbox.
- Leave **Source (Local) Port** field and **Protocol** field set to **ALL**.
- Click **OK**.
- On the main menu go to **File**, then **Commit** to save the settings.

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.

For more information on creating a policy 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 Intel Netstructure VPN gateway:

- Gateway IP address
- Select/deselect Split Tunneling, Perfect Forward Secrecy, and Extended Authentication
- A combination of group name, group password, user name and user password, depending on the authentication selected

Note: If extended authentication is selected, you will be asked for an additional password 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 Split Tunneling, 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 “Split Tunneling” on page 37, “Perfect Forward Secrecy” on page 39, “External Authentication” on page 42, and “DNS Support” on page 45).

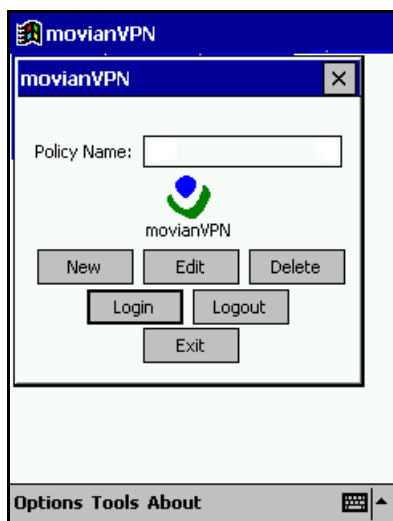
A worksheet is provided in “Appendix C: Client configuration worksheet” on page 55 that can be used to enter the required information and be given to users. The same table appears in the *User Guides*.

Creating a basic WinCE policy

To create a basic WinCE policy for an Intel Netstructure 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.

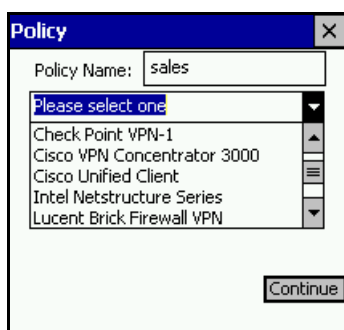


2. Tap **New**.

The **movianVPN** Policy window appears.

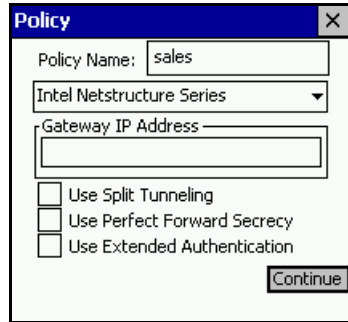


3. Enter a policy name in the **Policy Name** field.
4. Tap **Please select one** to access the pull-down menu.



5. Scroll down and tap **Intel Netstructure Series**.

The Intel Netstructure Series IP address field and the gateway policy security option check boxes appear.

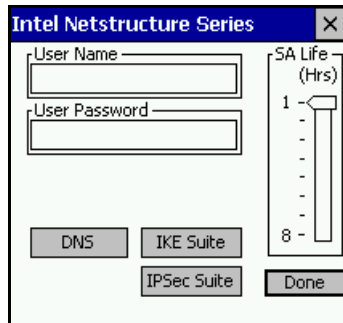


6. Enter the **Gateway IP Address**.

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

7. Tap **Continue**.

The Intel Netstructure Series window appears..



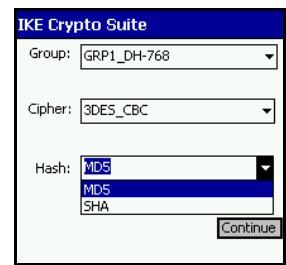
8. Enter the **User Name** and **User Password** for the gateway.

Note: The username should be match the setting in the step “Enter the user name, then click OK.” on page 16 and the password should match the setting in the step “Select the Shared Secret checkbox, click on Set Secret....” on page 17.

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.

9. Tap the **IKE Suite** button in the Intel Netstructure Series window.

The IKE Crypto Suite window appears..

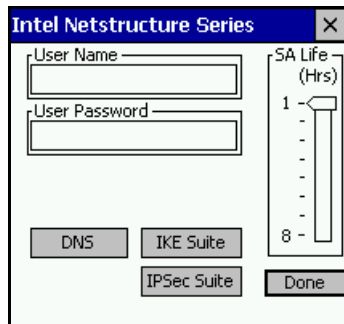


10. Select the appropriate settings from each of the pull-down lists for **Group**, **Cipher**, and **Hash** fields. These should match the settings from “Creating a security profile” on page 12.
11. Tap **Continue**.
12. Tap the **IPSec Suite** button in the Intel Netstructure Series window.

The IPSec Crypto Suite window appears.



13. Select the appropriate entry from the pull-down list in the **Suite** field. These should match the settings from “Creating a security profile” on page 12.
14. Tap **Continue**.
15. In the Intel Netstructure Series window, adjust the **SA Life** slide bar to time-out from the gateway as desired. .



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

Creating a Palm OS policy

To create a basic Palm OS policy for an Intel Netstructure Series gateway:

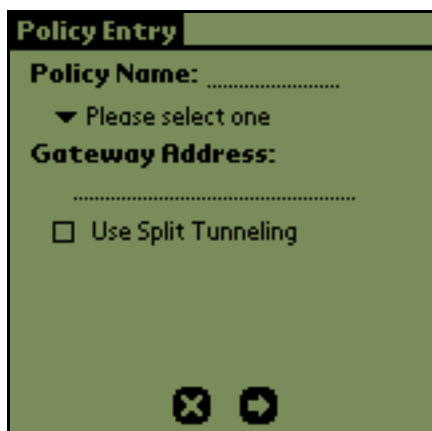
1. To open the **movianVPN** application, tap the arrow in the right corner of the top toolbar and select **movian** or **All**.
2. Tap the **movianVPN** icon.

The **movianVPN** application window appears.

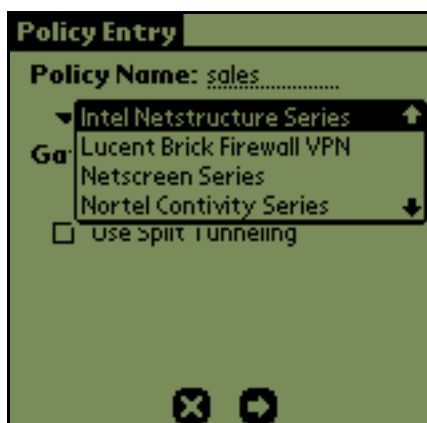


3. Tap **New**.

The **movianVPN** Policy window appears.

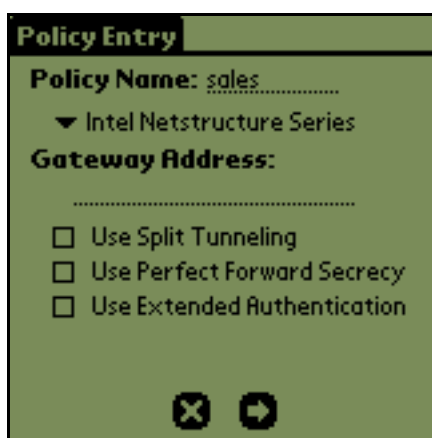


4. Enter a policy name in the **Policy Name** field.
5. Tap the pull-down menu at **Please select one**.



6. Scroll down to **Intel Netstructure Series** and tap the entry.

The Intel Netstructure Series Gateway Address field and the gateway policy security 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 Split Tunneling, 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 Intel Netstructure Series window appears...



9. Enter the **User Name** for the gateway.
Note: The username should be match the setting in the step “Enter the user name, then click OK.” on page 16 and the password should match the setting in the step “Select the Shared Secret checkbox, click on Set Secret....” on page 17.
10. Tap **Prompt** at the User Password field.
The User password window appears.



11. To save a password, enter the password and tap **OK**.
In the Intel Netstructure 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 Intel Netstructure 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. These should match the settings from “Creating a security profile” on page 12.
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...** button in the Intel Netstructure Series window.

The IPSec Crypto Suite window appears.



16. Select the appropriate entry from the pull-down list in the **Suite** field. These should match the settings from “Creating a security profile” on page 12.
17. Tap the checkmark icon.
18. In the Intel Netstructure Series window, tap the **movianVPN tab** at the top of the window.

The Options pull-down list appears.



19. Tap **SA Lifetime** in the pull-down.
20. Adjust the **SA Lifetime** setting using the arrows, to time-out of the gateway as desired.



21. Tap the checkmark icon.
The Intel Netstructure Series window appears.
22. Tap **Done**.
The **movianVPN** application window appears.
23. To connect to the gateway, tap the **Login** button.

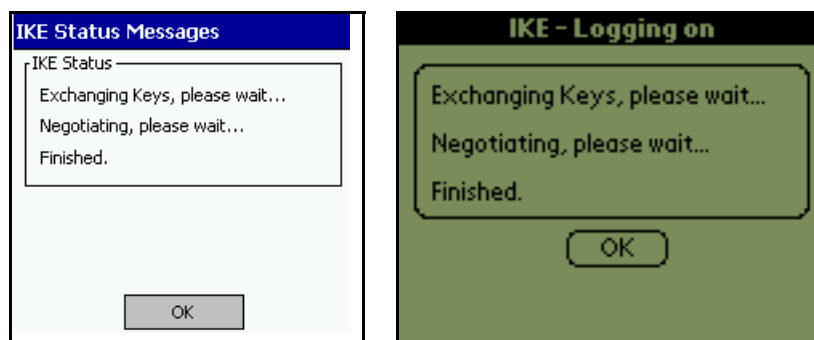
Testing the policy

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 fails

If the connection fails, complete the following:

- Check that the settings match on 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

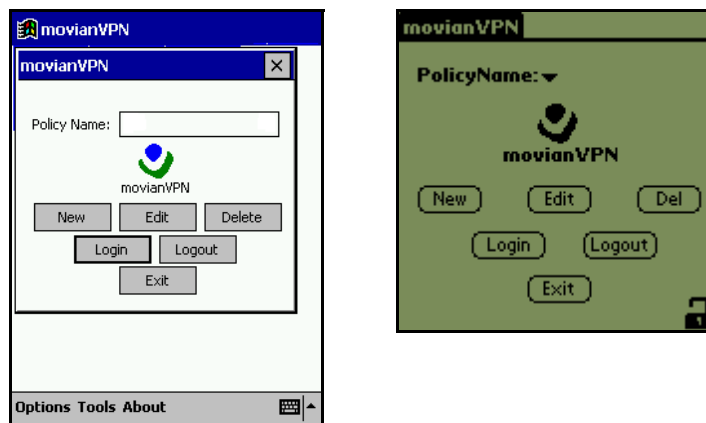
If the settings are correct and the connection is not successful:

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

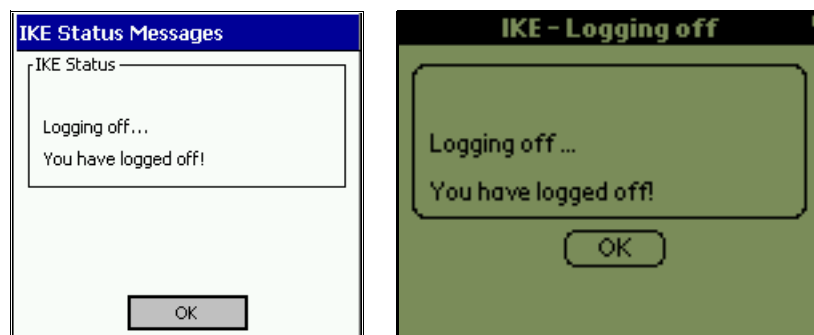
Logging out of the gateway

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 37
- “Perfect Forward Secrecy” on page 39
- “External Authentication” on page 42
- “DNS Support” on page 45

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 37.

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 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.

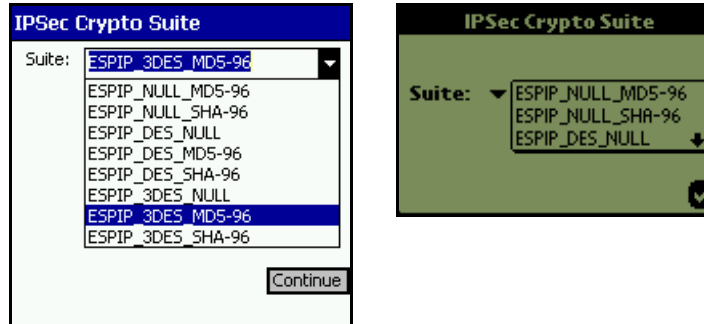
Note: While IPSec is enabled, a lock appears in the bottom right hand corner of the window.



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.

Note: These should match the settings from “Creating a security profile” on page 12.

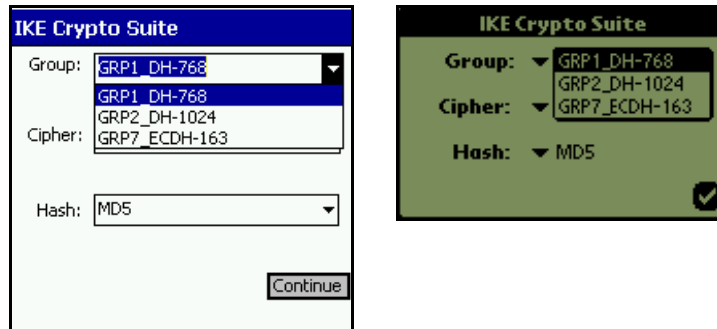


IKE Crypto Suite IKE (Internet Key Exchange) Crypto Suite configures the preferred protocols for exchanging keys.

Note: These should match the settings from “Creating a security profile” on page 12.

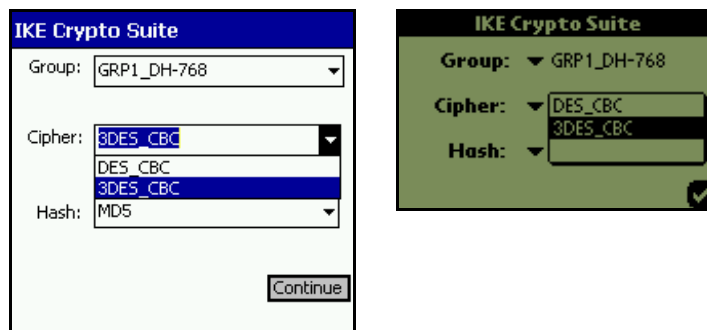
Group

Note: Group refers to the strength of the key encryption negotiation.



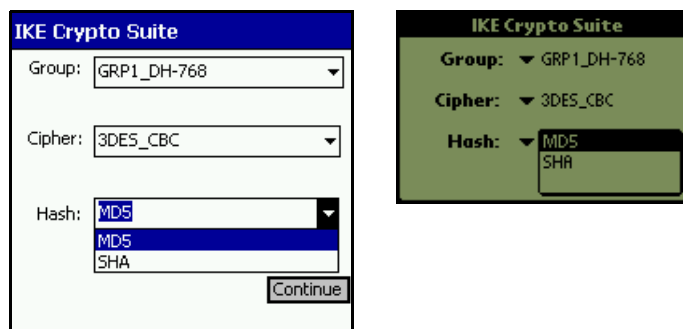
Cipher

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 using the following:

- “Split Tunneling”
- “Perfect Forward Secrecy”
- “External Authentication”
- “DNS Support”

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 and is not encrypted.

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 required to configure the client to enable split tunneling.

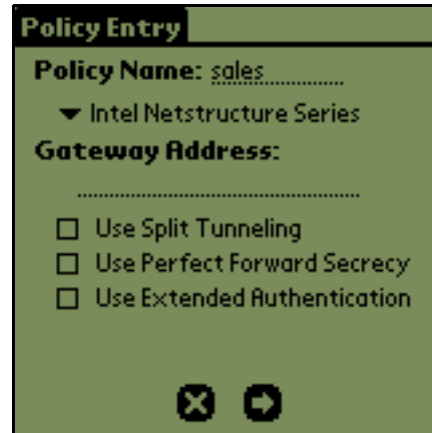
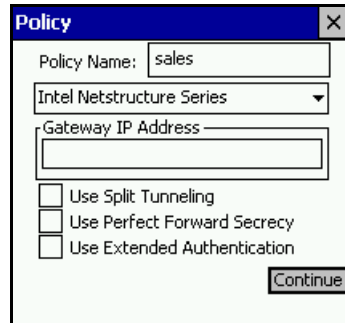
Enabling split tunneling on the gateway

You do not need to make any changes on the gateway to support split tunneling. The **movianVPN** client must be enabled to use the option.

Enabling split tunneling on the movianVPN client

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

1. In the **movianVPN** window, select the policy.
2. Tap **Edit**.
3. Select the **Use Split Tunneling** checkbox.



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

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.

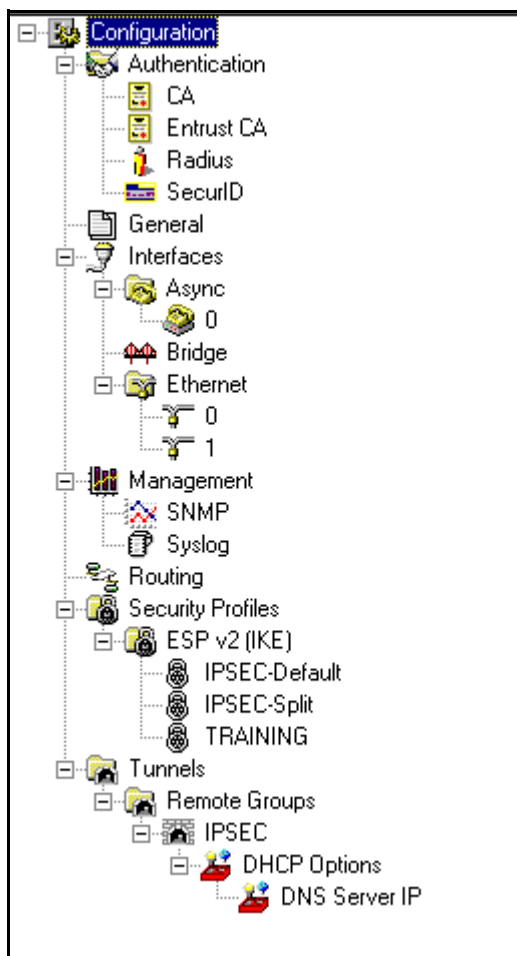
Perfect Forward Security performs the key exchange twice as your handheld device negotiates with the gateway, using the same key material. A new key is created for each step of the Internet Key Exchange (IKE), and each new key is not derived from the previous key. Thus, the previous key or the one following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

Negotiation of the connection will take longer.

Enabling perfect forward secrecy on the gateway

To enable perfect forward secrecy on the gateway:

1. On main menu, go to **Configure** then **Normal Configuration**.
2. In the new window (**Normal Configuration**) menu, go to **Configuration**, then **Security Profiles** then **ESPv2 (IKE)**.



3. Select the default security profile (**IPSecDefault**).

The screenshot shows a configuration window with the following settings:

- Authentication:** Key (dropdown), Public Key (bits): (dropdown)
- IKE Section:**
 - Algorithm: 3-DES (168-bit key) (dropdown)
 - Authentication: HMAC MD5 (dropdown)
 - Key Lifetime (time): 1 (dropdown) hour(s) (dropdown)
 - (Kbytes): 20,480 (dropdown)
 - DH Group: 7 - ECC 1024 Bit (dropdown)
 - Aggressive Mode
- IPSec Section:**
 - ESP Algorithm: 3DES (168-bit key) (dropdown)
 - ESP Authentication: HMAC MD5 (dropdown)
 - Authentication Header: None (dropdown)
 - Key Lifetime (time): 1 (dropdown) hour(s) (dropdown)
 - (Kbytes): 20,480 (dropdown)
 - Secondary Authentication: None (dropdown)
 - Perfect Forward Secrecy (highlighted with a dashed border and an arrow)
 - Tunnel AH Mode
 - Tunnel ESP Mode
- Keypair and Client Settings:**
 - Keypair: 15 (dropdown) second(s) (dropdown)
 - Timeout: 1 (dropdown) hour(s) (dropdown)
 - Client Timeout: 1 (dropdown) hour(s) (dropdown)
 - Client Keypair: 15 (dropdown) second(s) (dropdown)
- Advanced Options:**
 - UDP Encapsulation Port: 2233 (dropdown)
 - Propose Higher Security
 - Set Commit Bit
 - Split Tunneling
 - Preserve TOS Bits

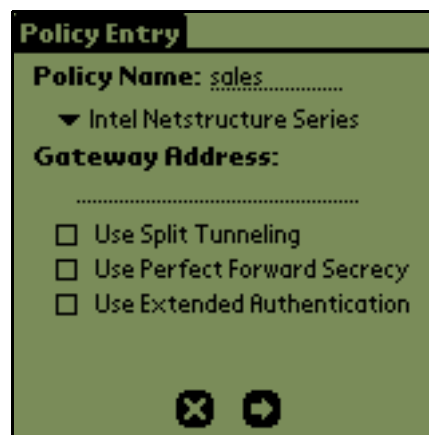
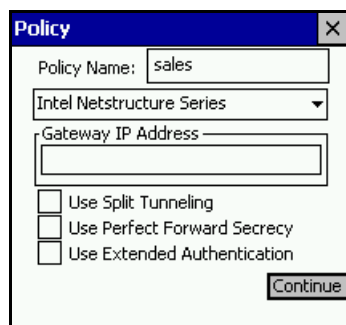
4. Select the **Perfect Forward Secrecy** checkbox.
5. On the main menu, go to **File**, then **Commit** to save the settings.

Enabling perfect forward secrecy on the movianVPN client

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

To enable perfect forward secrecy on the **movianVPN** client:

1. In the **movianVPN** window, select the policy.
2. Tap **Edit**.
3. Select the **Use Perfect Forward Secrecy** 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 Secrecy will be enabled for the policy.

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.

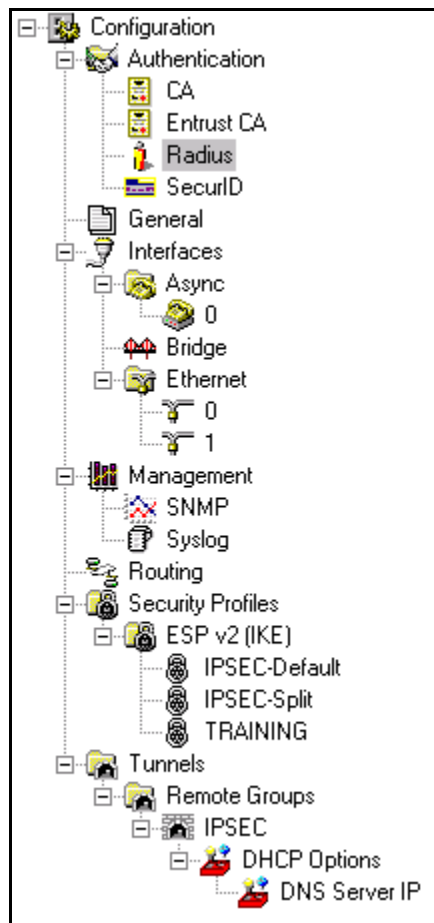
The easiest way to set up to set up Radius authentication is to create a Radius user account. The **movianVPN** client user then uses "Radius" as the group name and the user password from the Radius user account as the group password. The username and user password would be from the authentication server.

movianVPN client must be configured to support external authentication.

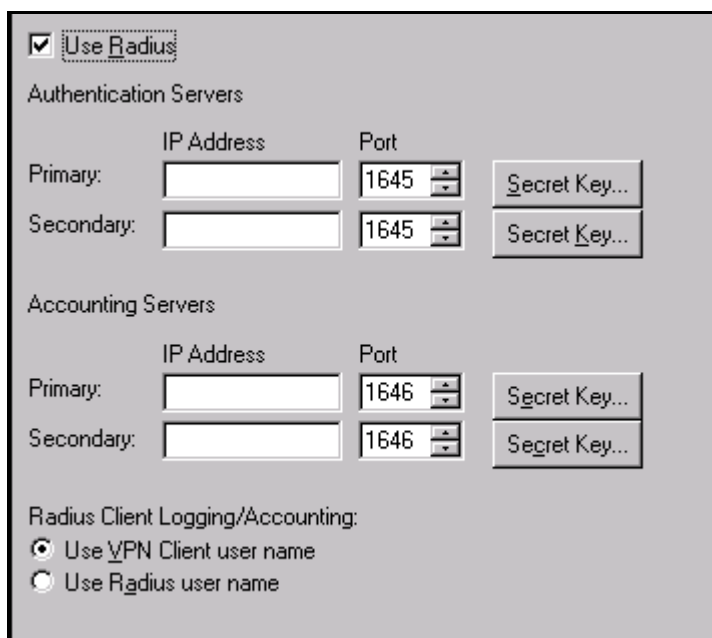
Setting up an external Radius authentication server

To set up a Radis authentication server:

1. On the main menu, go to **Configuration**, then **Authentication**.



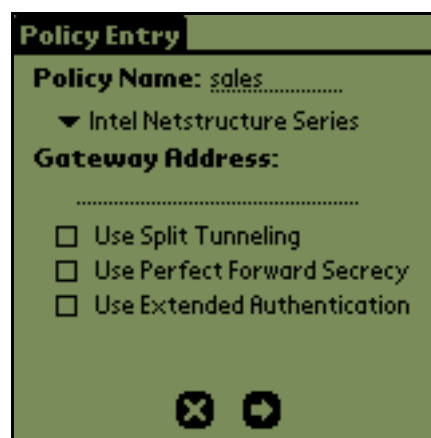
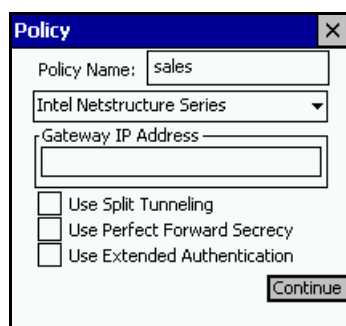
2. Select **Radius**.



3. Select the **Use Radius** checkbox.
4. Enter the **Primary IP address** and **port number** of the Radius server.
5. Add a **Radius** user (see **Create a user** in chapter 3).
6. Set **Secondary Authentication** field to **Radius**.
7. On the main menu, go to **File**, then **Commit** to save the settings.

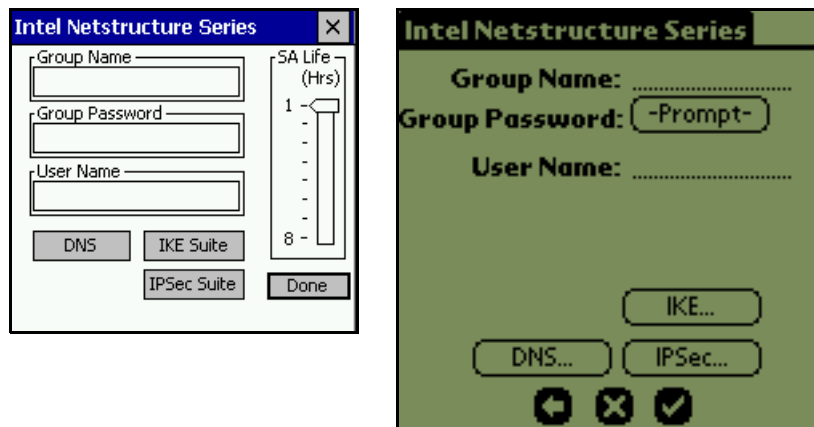
Enabling external authentication on the movianVPN client

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



4. 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, only User Name and Password fields will appear..



5. Enter the Group Name, Group Password, and User Name.
6. Tap **Continue** in WinCE OS or tap the checkmark icon in Palm OS.
7. Tap **Done**.

When you log in to the gateway, you will be asked for the User Password supplied by the VPN administrator.

Note: The easiest way to set up to set up Radius authentication is to create a Radius user account. The **movianVPN** client user then uses "Radius" as the group name and the user password from the Radius user account as the group password. The username and user password would be from the authentication server

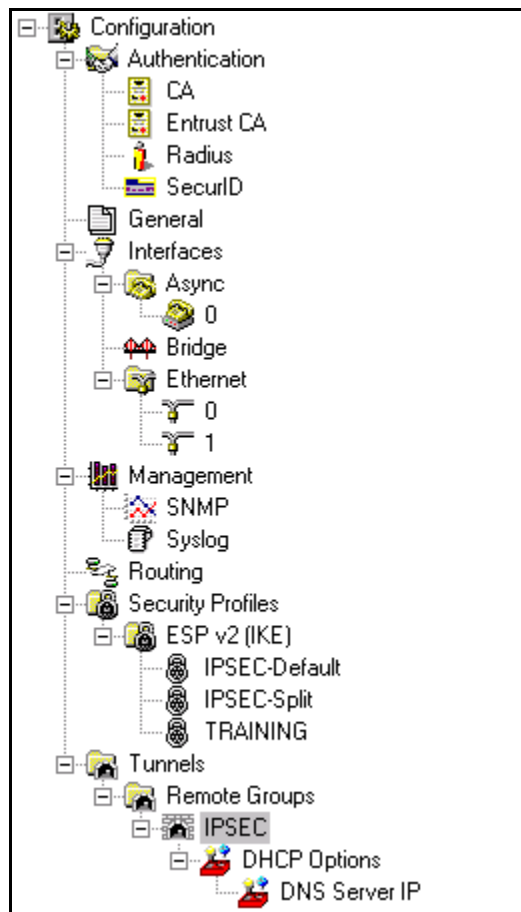
DNS Support

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.

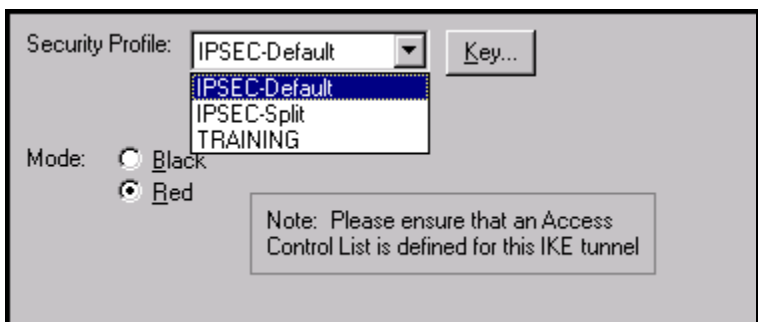
If Query DNS is checked, the handheld device will download the DNS information from the gateway server. If you supply the DNS information, your handheld device's settings will override other information provided by the gateway.

Enabling DNS support

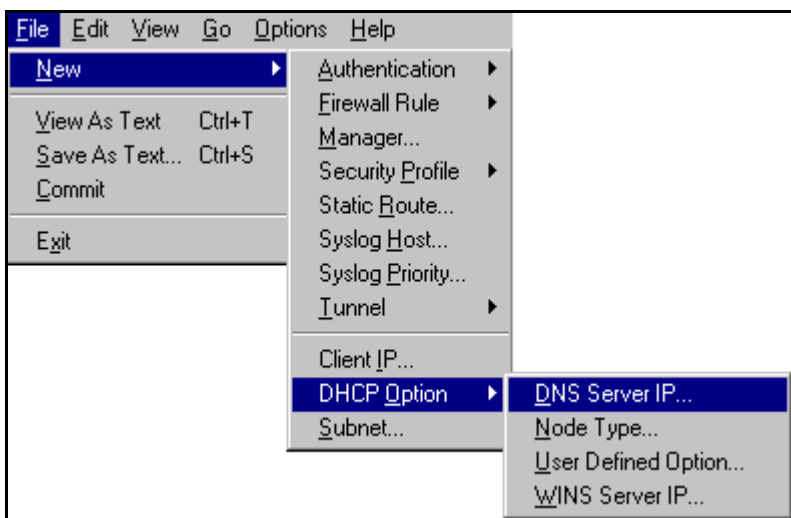
1. On main menu, go to **Configure** then **Normal Configuration**.
2. In the new window (**Normal Configuration**) menu, go to **Configuration**, then **Tunnels**, then **Remote Groups**, then **IPSec**.



3. Select the **IPSecDefault** security profile in the drop-down list:



- On the main menu, select **File**, then **New**, then **DHCP option**.



- Select **DNS ServerIP**.



- Enter the IP address. Click **OK**.
- On the main menu, go to **File**, then **Commit** to save the settings.

Enabling DNS on the movianVPN client

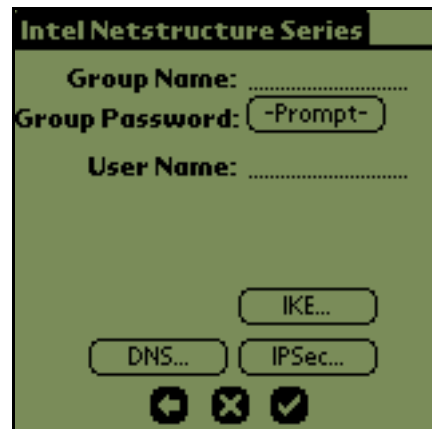
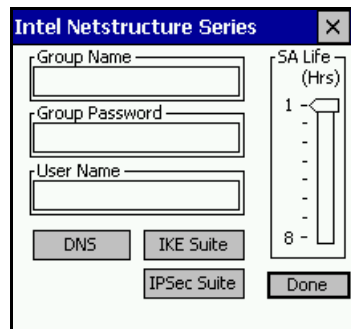
If the client is supplying DNS settings, they must be set on the client software.

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.

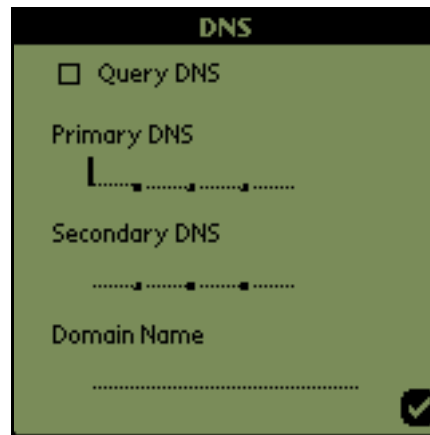
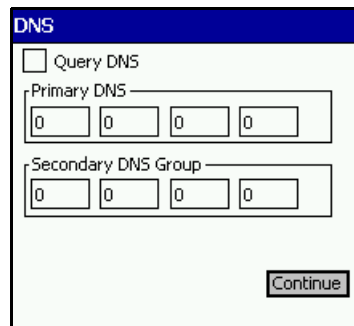
The gateway window will appear

Note: If extended authentication has not been selected, only User Name and Password fields will appear.



4. Tap **DNS ...**

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



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

When you log in to the gateway, the client will provide the DNS settings.

6

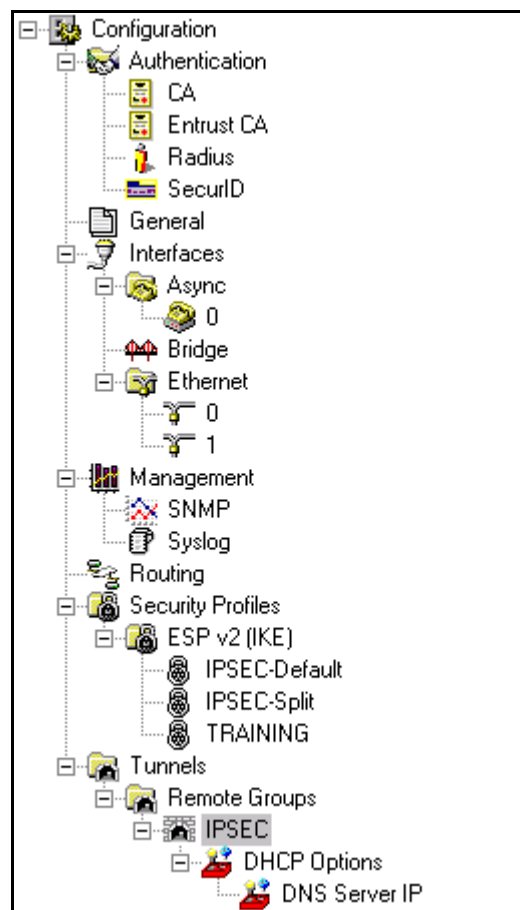
Deploying a pilot scheme

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. On main menu, go to **Configure** then **Normal Configuration**.
2. In the new window (**Normal Configuration**) menu, go to **Configuration**, then **Tunnels**, then **Remote Groups**, then **IPSec**.



- Select the **IPSecDefault** security profile in the drop-down list.

Security Profile: IPSEC-Default [Key...]

Mode: Black Red

Note: Please ensure that an Access Control List is defined for this IKE tunnel

Subnets			Add...
IP Address	Subnet Mask	Include/Exclude	
10.5.1.0	255.255.255.0	Include	

Client IPs			Add...
IP Address/DHCP	Count	DHCP Gateway	
10.5.1.171	9		

- Under **Client IPs**, click Add.

New Client IP

Remote Group: IPSEC [OK]

IP Address (or DHCP): [] [Cancel]

DHCP Gateway: []

Count: 1

- Enter the first **IP address** you want to use.
- Click **Count**, then enter the number of subsequent addresses.
- 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:

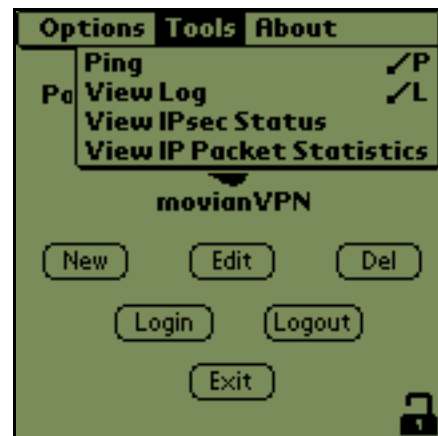
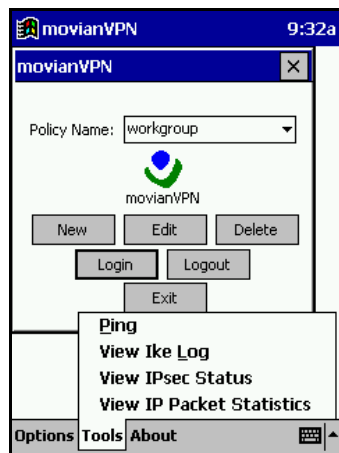
- Ping
- View IPsec Status
- View IP Packet Status

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.



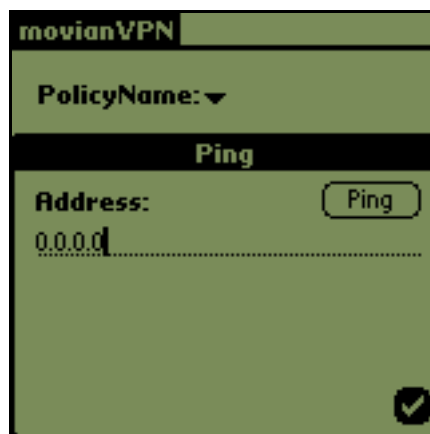
4. To close the window, tap **OK** or the **X** in the top right corner of the Ping window.

Using Ping with a Palm OS client

To ping a server using a Palm OS device:

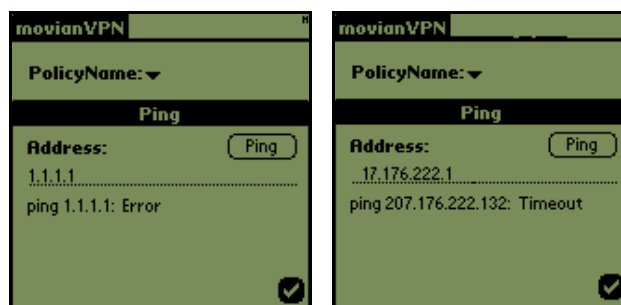
1. Tap the **movianVPN** tab.
2. Tap **Tools** and select **Ping** from the list.

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:

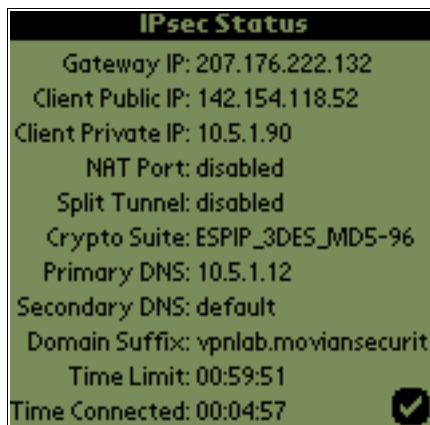
Field	Information
Gateway IP	VPN gateway server IP address
Client Public IP	IP address supplied by ISP
Client Private IP	IP address within the VPN
NAT Port	If NAT is enabled
Split Tunnel	If Split Tunnel is enabled
Crypto Suite	Crypto Suite setting
Primary DNS	DNS setting from VPN gateway or supplied 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.

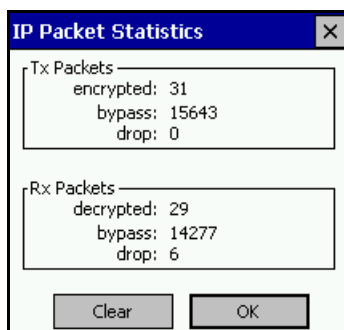
Note: View IP Packet Statistics is only available while the VPN tunnel is up.

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:

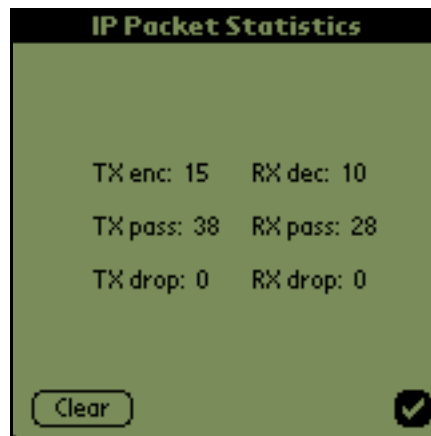
- Encrypted/decrypted
- Bypass: Sent without encryption
- Drop: Dropped from communication

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.

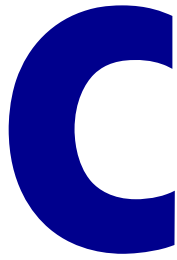
When you select Split Tunneling, packets of data headed to inside the VPN will still be encrypted and forwarded. Packets that are not directed to inside the VPN will not be encrypted, nor is the reply.

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		