

movianVPN™

Version 3.0.5

Deployment Guide for ReefEdge Connect Server 100 VPN Gateway

PUB-0200-2000
May 20, 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
Adding a user to the group	13
Adding a user to a group	14
Setting a static pre-shared key	16
Creating a movianVPN policy for your gateway	17
Before you begin	17
Creating the policy	18
Testing the policy	22
If the connection failed	23
Logging out of the gateway	24
Appendix A: Using the Diagnostic Tools	25
Accessing diagnostic tools	25
Ping	26
Using Ping with a client	26

IPSec Status Log	27
Viewing IPSec Status for a client	27
IP Packet Statistics Log.	28
Viewing IP Packet Statistics for a client	28
Appendix B: Glossary of Terms	29
Appendix C:	
Client configuration worksheet	33
Information required for client configuration	33
Information required for creating a policy	34

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:

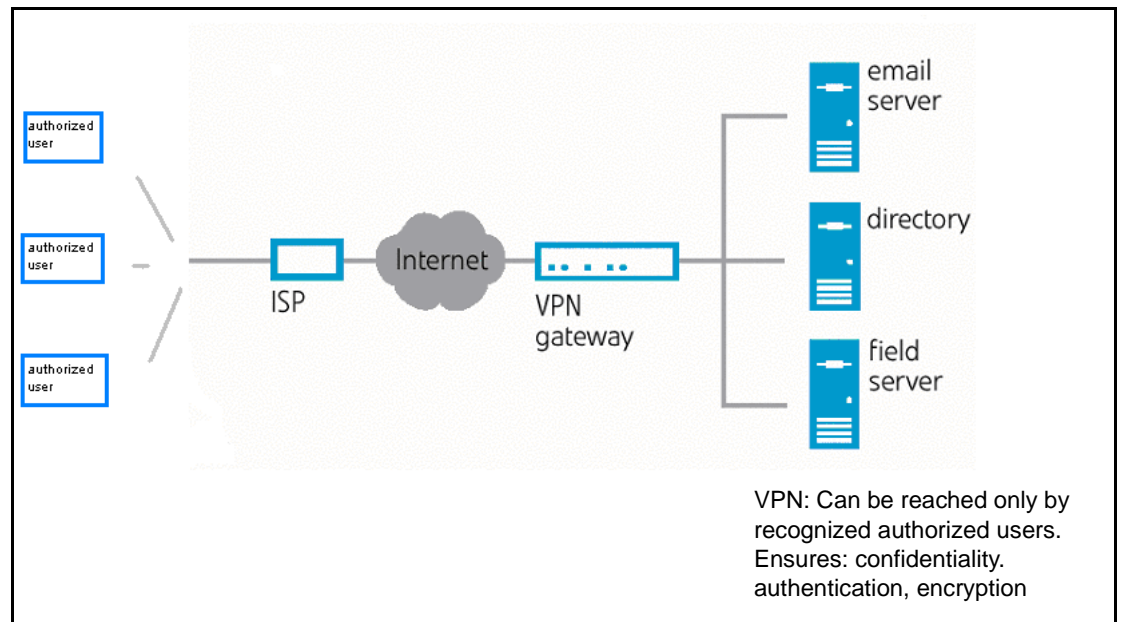
- **Intranet VPN:** Between a central corporate site and branch offices
- **Remote access VPN:** Between a central corporate site and individual remote users (the **movianVPN** model)
- **Extranet VPN:** Between an enterprise and its business partners, suppliers, and customers

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

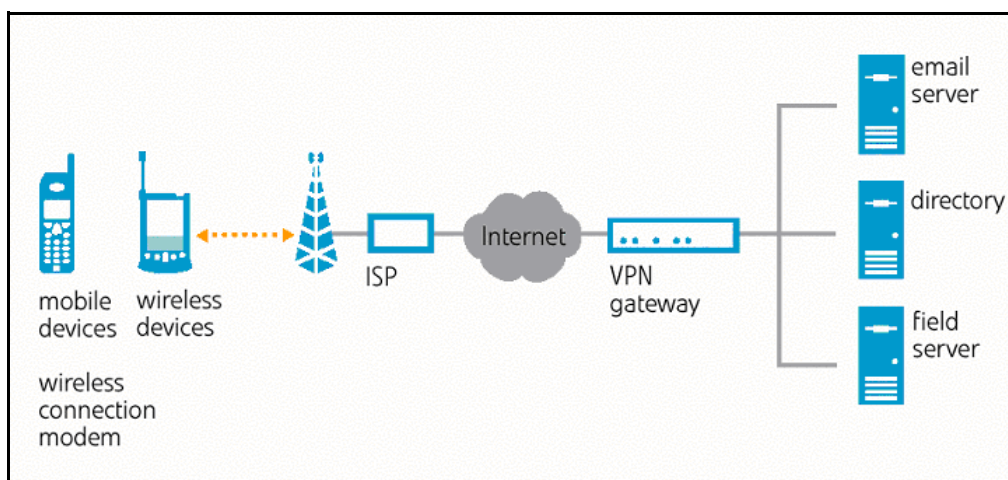
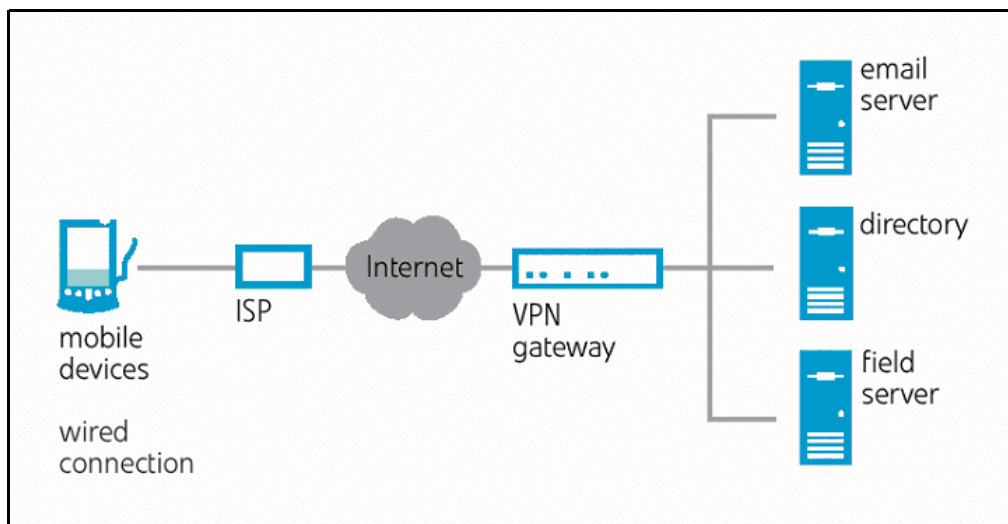
Using **movianVPN**, a traditional VPN can also have handheld devices added to the configuration without compromising network security.

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 ReefEdge Connect Server 100 VPN 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
ReefEdge	Connect Server 100	2.6.0 Beta

Connections

The following specific connections have been tested for interoperability:

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

Supported devices

- Handheld PC 2000 (Windows CE OS)
- Pocket PC v3.0 (Windows CE OS)
- Pocket PC 2002 (Windows CE OS)

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.

Gateway software

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

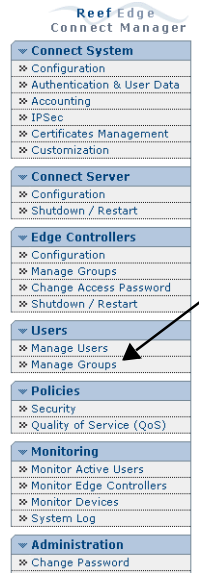
Note: If you have an older version of the software, you should upgrade. Please see the documentation for your gateway for the procedure.

Gateway	Product	Supported software versions
ReefEdge	Connect Server 100	2.6.0 Beta

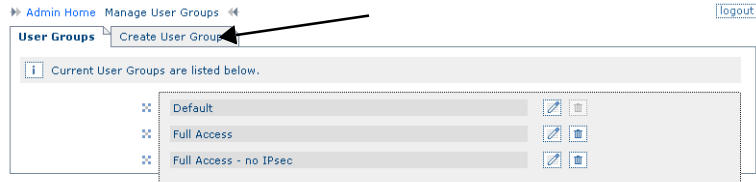
Creating a new group

To create a user group, follow these steps:

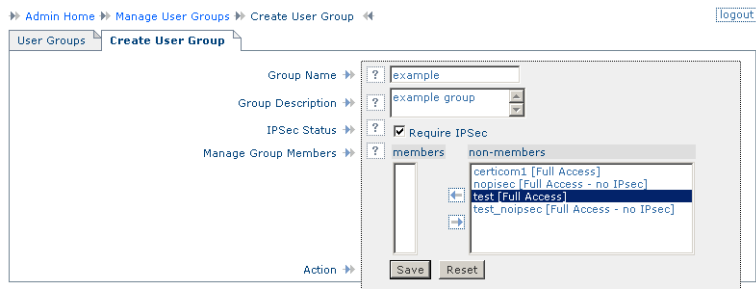
1. In the **Navigation** menu, locate the **Users** heading and click **Manage Groups**.



The *User Groups* screen appears:



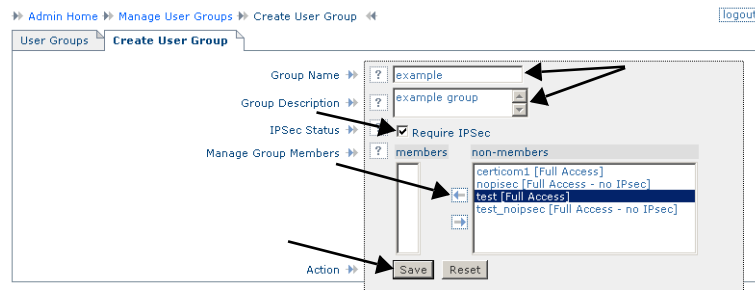
2. Click the **Create User Group** tab. The *Create User Group* screen appears:



3. Enter a group name in the **Group Name** field and (optionally) a brief description of the group in the **Group Description** field.
4. Activate the checkbox labeled **Require IPsec** to force users in the group to use IPsec encryption to access the network.

Adding a user to the group

5. To add users to the group, select users in the **non-members** panel and click the left arrow. This moves the users to the **members** panel. Note that the groups to which a user currently belongs are shown in square brackets next to the user's name.

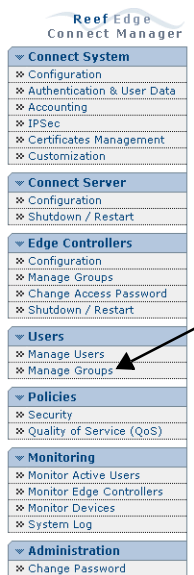


6. Click the **Save** button to save the new user group.

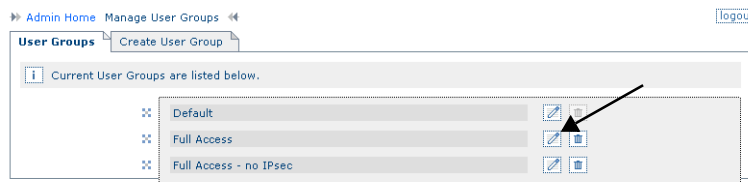
Adding a user to a group

To add a user to an existing group, follow these steps:

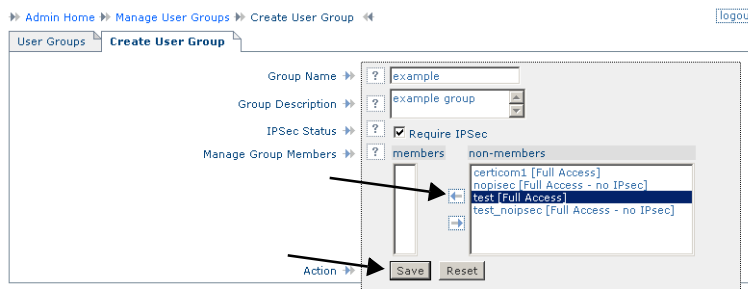
1. In the **Navigation** menu, locate the **Users** heading and click **Manage Groups**.



The *User Groups* screen appears:



2. Locate the desired group and click its *Edit* icon. The *Edit User Group* screen appears:



3. Add users to the group by selecting users in the **non-members** panel and clicking the left arrow.
4. Click the **Save** button to save the user group.

Setting a static pre-shared key

If you use a pre-shared key for authentication purposes, you must ensure that it is static, i.e. it cannot be changed by the gateway. You do this by changing the pre-shared key rotation policy. The rotation policy refers to how often a user must re-enter the pre-shared key. The rotation policy must be changed so that the user never has to re-enter the shared key unless forced to do so by the administrator.

You must set a pre-shared key and change the pre-shared key rotation policy for each of the users you created in “Adding a user to a group” on page 14.

1. Start an encrypted telnet session with the server (the IP address is that of the gateway):

```
ssh root@111.22.3.44
```

2. Start psql:

```
psql ReefSystem reefuser
```

3. To set a static pre-shared key, type

```
update attribute set atvalue = 'xxxxx' where attable='reefuser'
and atname='psk_key' and atentityfk in (select rurefnum from
reefuser where ruid='yourReefEdgeUserID');
```

'xxxxx' is the pre-shared key and 'yourReefEdgeUserID' is the ID of the user.

4. To make sure the server does not rotate the key (which creates a new one), type

```
update attribute set atvalue='204201939' where attable='ree-
fuser' and atname='psk_expire' and atentityfk in (select
rurefnum from reefuser where ruid='yourReefEdgeUserID');
```

'yourReefEdgeUserID' is the ID of the user.

5. To set the policy value, type

```
update attribute set atvalue='1' where attable='reefuser' and
atname='psk_policy' and atentityfk in (select rurefnum from
reefuser where ruid='yourReefEdgeUserID');
```

'yourReefEdgeUserID' is the ID of the user.

6. Exit psql:

```
\q
```

7. To verify the changes, type:

```
list_reefuser -u yourReefEdgeUserID
```

4

Creating a movianVPN policy for your gateway

Before you begin

This chapter describes how to create a basic movianVPN policy using the movianVPN client software.

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**.*

***Note:** **movianVPN** 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 ReefEdge Connect Server 100 VPN gateway:

- Gateway IP address
- User password
- IKE suite and IPSec settings
- SA life setting

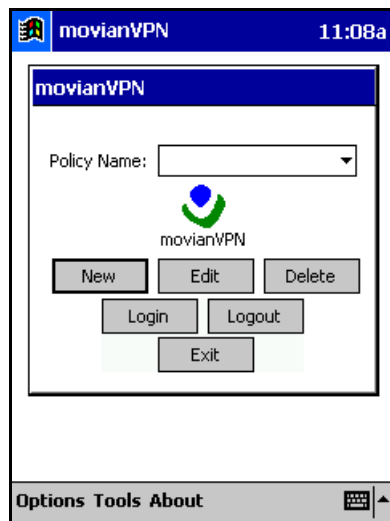
When creating a policy to test the gateway, a basic policy is recommended. For information on creating a policy with advanced features please refer to the *movianVPN User's Guide for WinCE Pocket PC*.

A worksheet is provided in “Appendix C: Client configuration worksheet” on page 33 that can be used to enter the required information and be given to users. The same table appears in the *User's Guides*.

To create a policy for a ReefEdge Connect Server gateway:

1. 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.

The screenshot shows a window titled "Policy" with a close button (X) in the top right corner. Inside the window, there is a text input field labeled "Policy Name:" containing the text "sales". Below it is a dropdown menu with the text "Please select one". Underneath the dropdown is another text input field labeled "Gateway Address:". At the bottom right of the window is a button labeled "Continue".

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

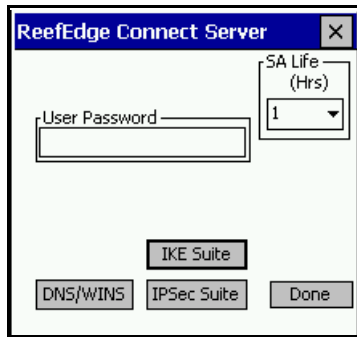
The screenshot shows the same "Policy" window, but the dropdown menu is now open, displaying a list of gateway options: "Netscreen Series", "Nortel Contivity Series", "Radguard cIPro", "ReefEdge Connect Server", and "Secure Computing Sidewinder". The "ReefEdge Connect Server" option is highlighted. The "Continue" button remains at the bottom right.

5. Scroll down and tap the **ReefEdge Connect Server** entry.

The ReefEdge Connect Server Gateway IP address field and the gateway policy security option checkboxes appear.

The screenshot shows the "Policy" window with "ReefEdge Connect Server" selected in the dropdown menu. The "Gateway Address:" field is now visible and empty. Below it are two checkboxes: "Use Certificates (PKI)" which is unchecked, and "Use Perfect Forward Secrecy" which is checked. The "Continue" button is at the bottom right.

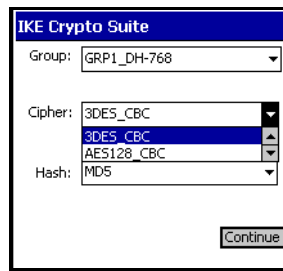
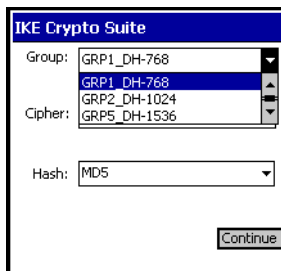
6. Enter the **Gateway IP Address**.
Do not check the **Use Certificates (PKI)** checkbox.
7. Tap **Continue**.
The User Password prompt appears.



Enter the shared key that you set in “Setting a static pre-shared key” on page 16.

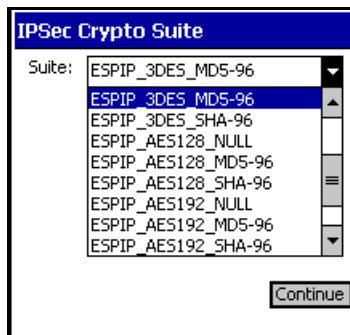
8. Tap the **IKE Suite** button in the ReefEdge Connect Server window.

The IKE Crypto Suite window appears.

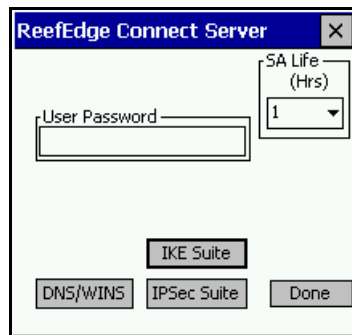


9. Select the settings supplied by your VPN administrator from each of the pull-down lists for **Group**, **Cipher**, and **Hash** fields.
10. Tap **Continue**.
11. Tap the **IPSec Suite** button in the ReefEdge Connect Server window.

The IPSec Crypto Suite window appears.



12. Select the entry from the pull-down list in the **Suite** field.
13. Tap **Continue**.
14. In the ReefEdge Connect Server window, adjust the **SA Life** drop-down to time-out of the gateway as desired.



15. Tap **Done**.

The **movianVPN** application window appears.

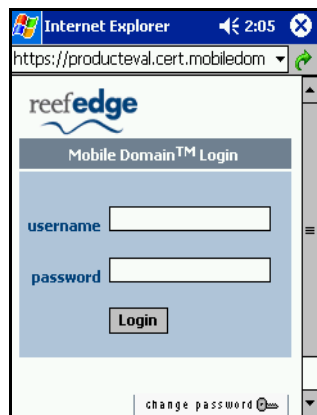
Testing the policy

If you chose to use a pre-shared key as your method of authentication, you must log on to the ReefEdge Mobile Domain before logging on to the gateway.

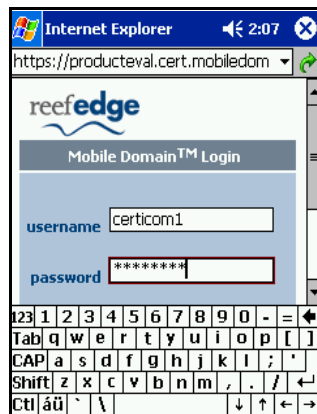
If you chose to use certificates as your method of authentication, you must log on to the ReefEdge Mobile Domain **after** logging on to the gateway.

To log on to the ReefEdge Mobile Domain, follow the steps below:

1. Open Internet Explorer and enter the URL `http://mobile.domain`. The Mobile Domain Login page is displayed.



2. Enter your username and password.



3. Tap Login. You are now logged in to the ReefEdge Mobile Domain.



1. To log in to the gateway, open the main **movianVPN** window and tap **Login**. The IKE Messages display connection progress in generating and exchanging keys. If the connection is successful, the following screen appears.



2. 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's Guide for WinCE Pocket PC and Handheld PC* for information on verifying your policy and troubleshooting logging in to the gateway

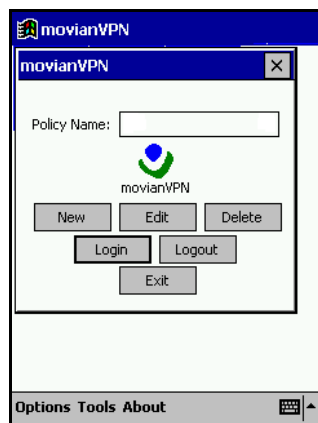
If the settings are correct and the connection is not successful:

- 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.

A

Appendix A: Using the Diagnostic Tools

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

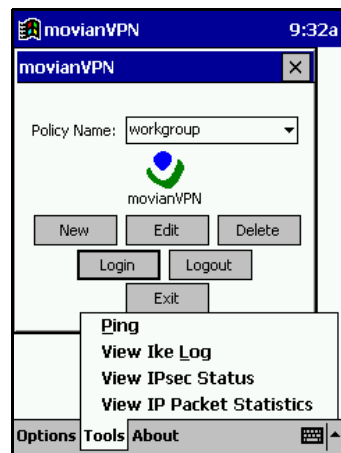
- Ping
- View IPsec Status
- View IP Packet Status

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
 - Tap **Tools** in the lower tool bar



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.

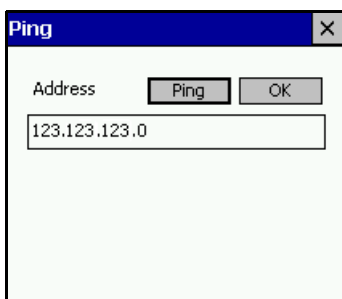
Note: If the first attempt fails, ping the server twice.

Using Ping with a client

To ping a server from your 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.

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 client

To view IPsec status on your 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	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.

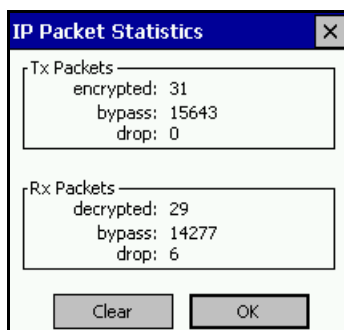
Note: View IP Packet Statistics is only available while the VPN tunnel is up.

Viewing IP Packet Statistics for a client

To view IP Packet Statistics with your 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

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.

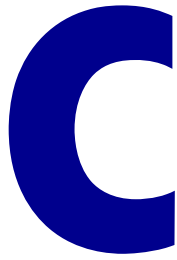
When you select Split Tunneling, packets of data headed to inside the VPN will still be encrypted and forwarded. Packets that are not directed to inside the VPN will not be encrypted, nor is the reply.

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		