

movianVPN™

Version 4.0

User's Guide for Palm OS

PUB-0200-2030
RN-0002
February 27, 2004

Copyright © 2000-2004 Certicom Corp. All rights reserved.

Certicom, the Certicom logo, movianVPN, and the movianVPN logo are trademarks of Certicom. 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.
Information subject to change.

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) U.S. 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

Copyright © 2000-2004 Certicom Corp. 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. Information subject to change.

Introduction	1
Introducing movianVPN	1
Using this document	2
VPNs	3
Gateway servers	3
IPSec	4
Handheld devices	4
movianVPN	6
Gateway access	6
Interoperability	7
Supported devices	7
Supported VPN gateways	7
Supported Features	7
Installing movianVPN	9
Installation Requirements	9
System requirements	9
Communications Requirements	9
Standard Palm Devices vs. Tungsten-C, Tungsten-T3	9
Installing movianVPN	10
Extracting the files	10
Installing the files	10
Configuration (Standard Palm Devices)	12
Setting connection preferences	12
Setting network preferences	14
Configuration (Tungsten-C, Tungsten-T3 Devices)	16
Setting network preferences	16
Checking the movianVPN version number	18
Standard Palm Devices	18
For Tungsten-C, Tungsten-T3 Devices	19
Licensing movianVPN	20
Licensing movianVPN	20
Checking your current license type	20
Reaching movianVPN support	20
Uninstalling movianVPN	21
Verifying Your Setup	23
Configuration Check	23
Step 1: Verify Your Connection Settings	24

Verifying your connection preferences (Standard Palm Devices)	24
Verifying your network preferences (Standard Palm Devices)	25
Step 2: Verify Your Internet Connection	26
Step 3: Provide a policy for your gateway	27
Importing a policy from a policy file (Standard Palm Devices)	27
Creating your own policy file using movianVPN	27
Step 4: Creating a Policy	28
Step 5: Global Options (Standard Palm Devices)	29
NAT Keepalive	29
Allow Auto Power Off	29
Step 6: Connection Options (Standard Devices)	30
Setting Connection Options (Standard Palm Devices)	30
Step 7: Verifying your policy	31
Policy window checkboxes	31
Editing the policy checkboxes	34
Using IPSec (Standard Palm Devices)	34
Policy gateway access settings	35
Creating a Policy	39
Creating Policies for Tungsten-C, Tungsten-T3 Devices	39
Creating a policy for an Alcatel Secure VPN Series gateway	41
Creating a policy for an Avaya VSU VPN Series	45
Creating a policy for a Check Point VPN-1 gateway	49
Creating a policy for a Cisco Unified Client Framework, Cisco Secure PIX Firewall VPN, or a Cisco IOS Easy VPN gateway	53
Creating a policy for a Cisco VPN Concentrator 3000 gateway	57
Creating a policy for a CoSine IPSX gateway	61
Creating a policy for a Cylink Nethawk gateway	66
Creating a policy for an Intel Netstructure Series gateway	70
Creating a policy for a Lucent Brick Firewall VPN gateway	74
Creating a policy for a Netscreen Series gateway	78
Creating a policy for a Nortel Contivity Series gateway	83
Creating a policy for a ReefEdge Connect Server gateway	88
Creating a policy for a Secure Computing Sidewinder gateway	92
Creating a policy for a Symantec (Axent) Power VPN gateway	96
Running movianVPN	101
Overview: Running movianVPN	101
Logging in to the gateway	102
Contacting The Gateway: Standard Palm Devices	102

Contacting The Gateway: Tungsten C, Tungsten T3	103
Authentication and Key Negotiation (Standard Palm Devices)	103
Changes to movianVPN screen when connected (Standard Palm Devices).	105
Troubleshooting logging on to the gateway.	107
Ping (Standard Palm Devices)	108
Ping (Tungsten-C, Tungsten-T3 Devices).	109
Error messages	111
Using movianVPN (Standard Palm Devices).	113
Working with applications.	113
Disabling and Enabling IPsec.	113
Logging out of the gateway	115
Logging out of the gateway (Standard Palm Devices)	115
Closing movianVPN (Standard Palm Devices)	116
Appendix A: Using the Diagnostic Tools	117
Accessing diagnostic tools	117
Ping (Standard Palm Devices)	118
Ping (Tungsten-C, Tungsten-T3 Devices).	119
View Log (Standard Palm Devices)	121
View IPsec Status (Standard Palm Devices).	122
View IP packet Statistics (Standard Palm Devices)	123
Appendix B: Troubleshooting (Standard Palm Devices)	125
Setting Connection Options	125
Additional messages	127
Appendix C: Glossary of Terms	129
Appendix D: Information worksheet	133
Information required for client configuration	133
Information required for policy creation.	134
Appendix E: Installing a movianVPN License	135



1

Introduction

Introducing 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.

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

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

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

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

Using this document

This User Guide is for the Palm OS version of **movianVPN**. It provides information on:

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

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

VPNs

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

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

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

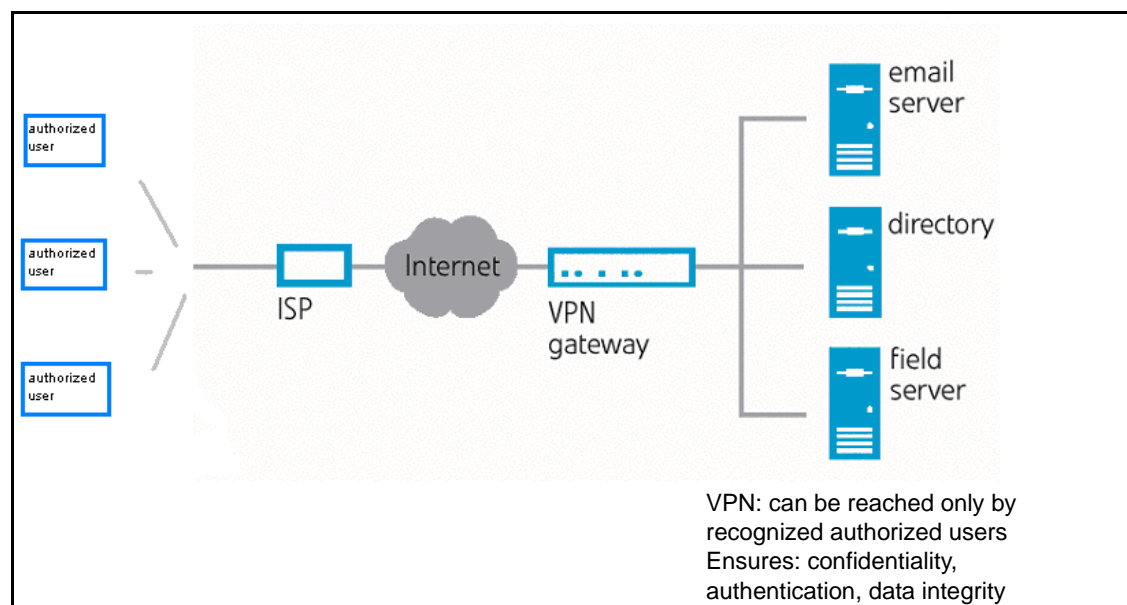
- **Intranet VPN:** Between a central corporate site and branch offices
- **Remote access VPN:** Between a central corporate site and individual remote users (the **movianVPN** model)
- **Extranet VPN:** Between an enterprise and its business partners, suppliers, and customers

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

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

Gateway servers

The VPN is accessed through a "VPN gateway server," a computer which recognizes authorized users and their passwords. The gateway server gives users access to the application servers for e-mail and other confidential information "behind" the gateway (that is, 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

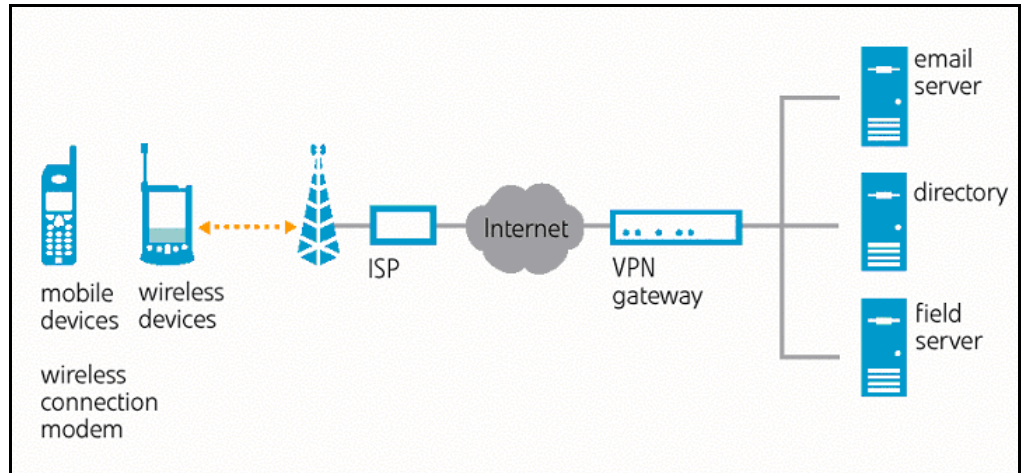
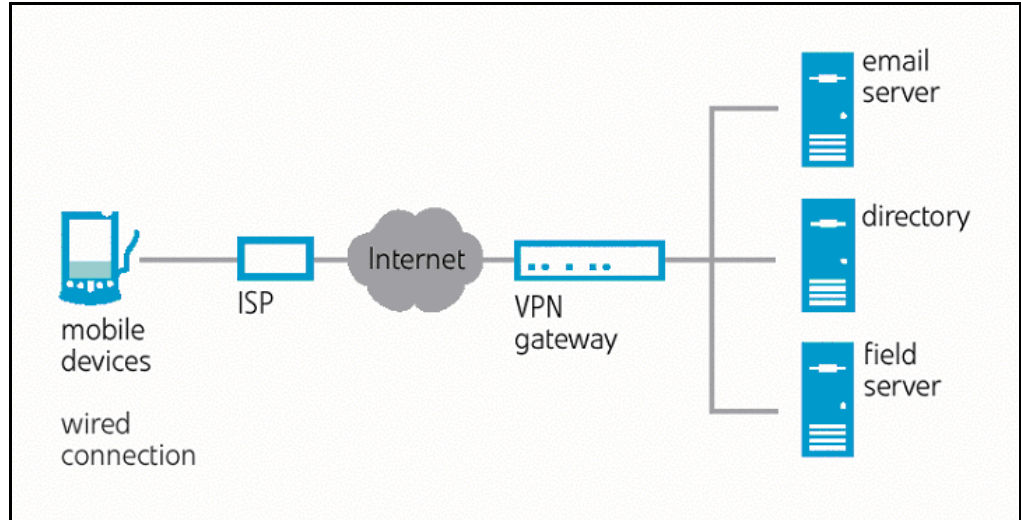
Using **movianVPN**, a traditional VPN can also have handheld devices added to the configuration.

Handheld devices can connect to the VPN by several options:

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

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

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



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

movianVPN

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

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

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

Gateway access

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

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

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

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

Interoperability

Supported devices For a list of supported devices, please refer to the website located at <http://www.certicom.com/vpnsupport>

Supported VPN gateways For a list of supported VPN gateways, please refer to the website located at <http://www.certicom.com/gatewaysupport>

Supported Features For a list of supported features, please refer to the website located at <http://www.certicom.com/vpnfeatures>

2

Installing movianVPN

Installation Requirements

Installing **movianVPN** is a simple process of:

- Obtaining the **movianVPN** software from the Internet
- Extracting the files to a designated folder
- Installing the application on your hard drive
- Synchronizing your handheld device using HotSync, to transfer the **movianVPN** files to the handheld
- Setting your network and connection preferences

If **movianVPN** has already been installed on your handheld device and your connection preferences have been pre-configured, you can move on to “Verifying Your Setup” on page 23.

System requirements

To install and run **movianVPN**, your desktop computer and handheld device should have the following as a minimum:

Computer	Operating System	Other
Desktop PC	Windows 95/98/NT/2000/XP	<ul style="list-style-type: none">• 4 MB of available disk space• Palm Desktop
Handheld	Palm OS 3.5 and up	<ul style="list-style-type: none">• 400 kB of available memory

Communications Requirements

To connect to a VPN, you will also require:

- A modem for land line or wireless connection to a dial-up Internet Service Provider or
- Hardware to connect to a wireline (Ethernet) or wireless Local Area Network (LAN)
- Account with an Internet Service Provider and/or wireless data provider

Standard Palm Devices vs. Tungsten-C, Tungsten-T3

This document uses the phrase "Standard Palm Devices" to refer to all Palm devices other than the Tungsten-C and Tungsten-T3 models, whose operation differs slightly from the majority of Palm products.

Installing movianVPN

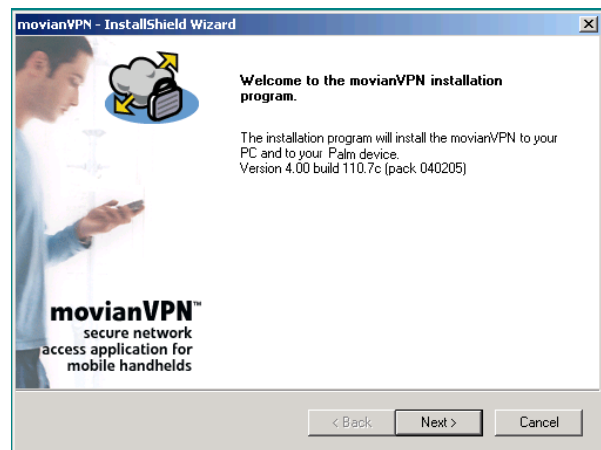
The **movianVPN** installation is a three step process. You must:

- Obtain the **movianVPN** files from <http://www.certicom.com>
- Extract the files into a folder on your hard drive
- Synchronize your handheld device with your computer, installing the **movianVPN** files onto the handheld device

Extracting the files

Once the download is complete, you can extract the **movianVPN** files onto your hard drive.

1. Go to the folder containing the **movianVPN** executable obtained from the Certicom website.
2. Launch the executable file by double-clicking it. The **movianVPN** Install Wizard will extract the files needed to install **movianVPN** onto your hard drive.

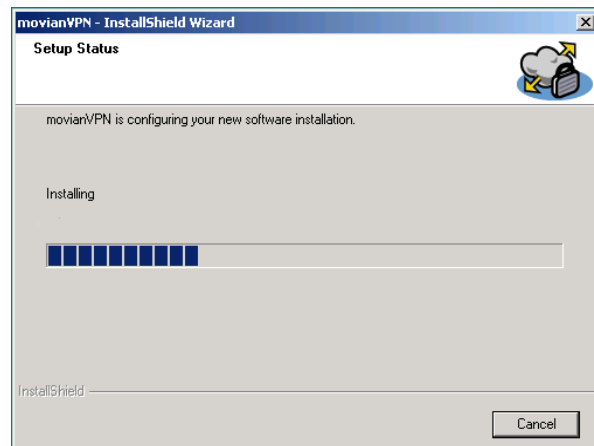


Installing the files

Once the files have been extracted, they can be installed on your hard drive.

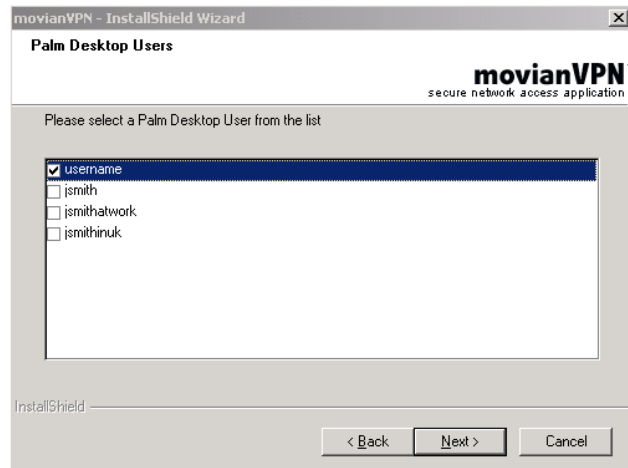
*Note: Do not HotSync until the installation has completed and you have clicked **Finish**.*

1. Once the files have been extracted, the **movianVPN** Installation Wizard will open to guide you through the steps to install **movianVPN**.
2. Click **Next** to continue.
3. The **movianVPN** Setup window will open the License Agreement. Read the License Agreement and click **Yes** to agree or click **No** to cancel the installation.
4. Use the default or select a location for your program folder, and click **Next**.



- If you have several HotSync profiles, you will be prompted to select the profile you wish to use with **movianVPN**.

*Note: If the profile name contains any special characters, the name will not be found and a partial list of profiles will appear. Profile names creating using any of the following characters will **not** be found:*
 /\ ; ? * . " > <



- Select the profile you wish to use. Click **Next**.

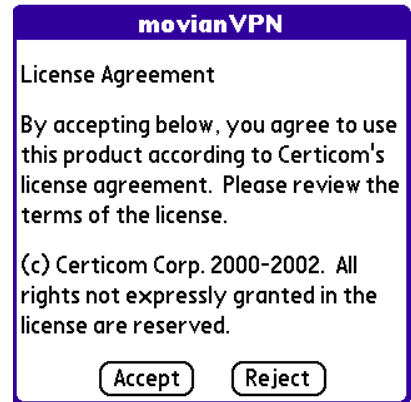
*Note: If you wish to use **movianVPN** with more than one profile, you will have to install the application again and select the other profile.*

- Click **Install**. The **Install Wizard** will configure the application.
- Click **Finish** to complete the installation.

The folder location for **movianVPN** documentation will automatically open. **movianVPN** will be automatically installed on your handheld device the next time you perform a HotSync. For information on options for synchronizing your handheld Palm OS device, please refer to the Palm Desktop documentation.

Configuration (Standard Palm Devices)

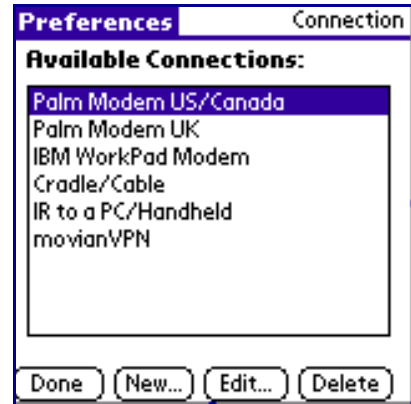
When you open **movianVPN**, the license agreement appears. Tap **Accept** if you agree to the terms of the license; tap **Reject** if you do not.



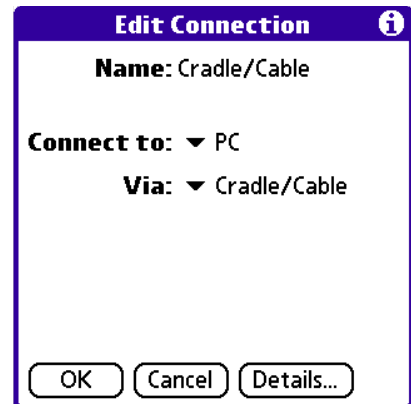
Setting connection preferences

1. The **Connection Preferences** window appears. This window allows you to configure the hardware you use to connect to the internet. Select the **movianVPN** connection from the options listed.

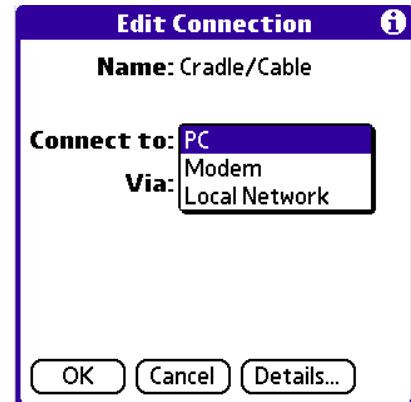
*Note: You can access the **Connection Preferences** window while **movianVPN** is running by selecting **Options** then **Connection Prefs** from the **movianVPN** menu bar.*



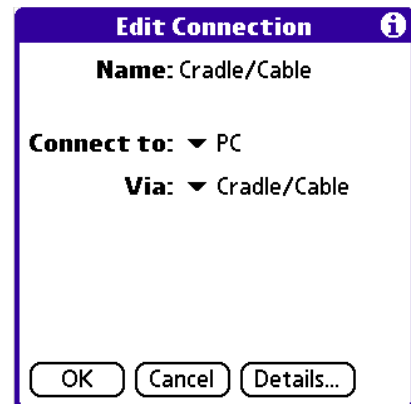
2. Tap the **Edit** button to edit your connection. The **Edit Connection** window opens.



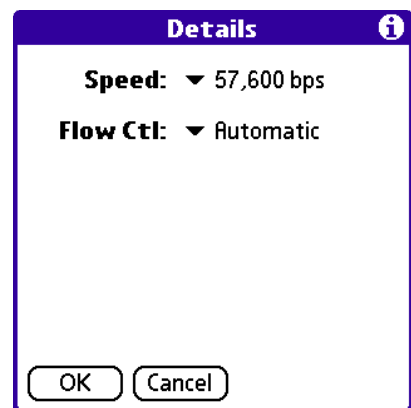
- Open the "**Connect to:**" list and select what you wish to connect your device to.



- Open the "**Via**" list and select the means your handheld uses to communicate with your desired connection. Select IPsec for all non-Treo devices.



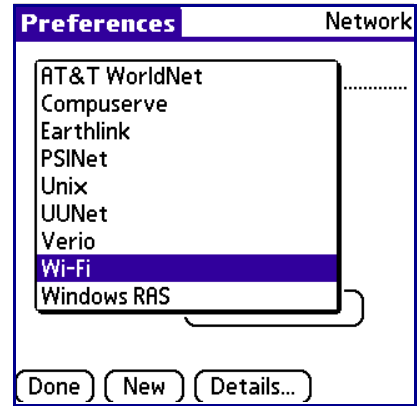
- Open the **Details** window by tapping the "**Details...**" button. The contents of this window depends upon your connection type. Details specific to your connection are displayed, along with the ability to change these options to different values. Here, for example, the user has connected to a LAN, and they may configure the speed of the connection or change the type of flow control. Tap **OK** to continue when you are satisfied with the values selected. Tap **OK** on the **Edit Connection** window to proceed.



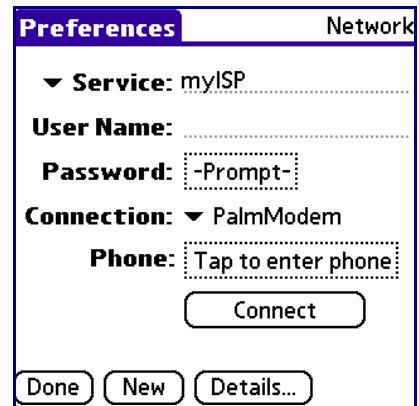
Setting network preferences

- Tap **Done** to complete your system setup. The **Network Preferences** window appears. This window is used to configure your internet connection. Select the service you are using from the **Service** menu.

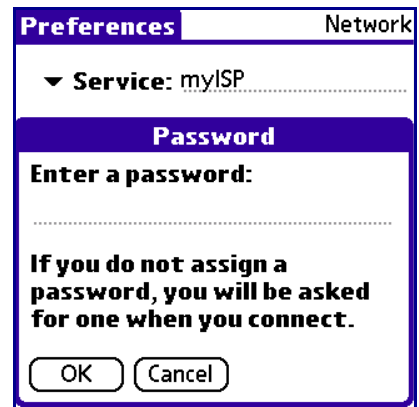
Note: You can also access the **Network Preferences** window while movianVPN is running by selecting **Options** then **Network Prefs** on the movianVPN menu bar.



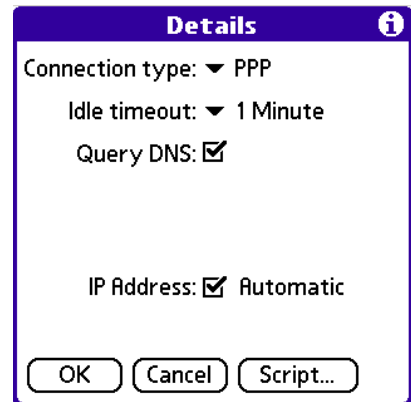
- Create a new network entry by tapping the **New** button at the bottom of the screen. Tap the text box at **Service** and enter the name of your ISP.
- Select the **movianVPN** connection type from the list of connection types.
- Enter your account name in the **User Name** field.



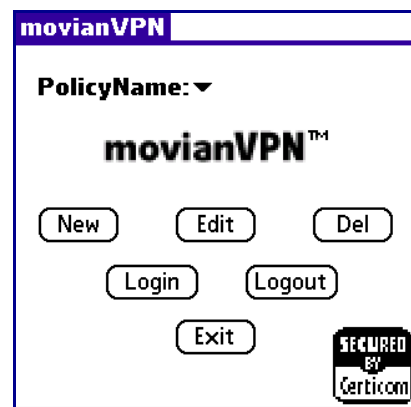
- If you have been instructed to store your password in your **Preferences**, tap **Prompt** and enter your password for logging onto your ISP account. Tap **OK** to store the password or tap **Cancel** to abort his procedure. If you do enter a password, the **Password** field's value changes to **Assigned**. To delete or change the password, tap on **Assigned** and edit the field.



11. Open the **Details** window by tapping the "**Details...**" button. This window shows specific configuration options for your internet connection. Tap on **OK** to save your changes, or **Cancel** to exit with no changes..



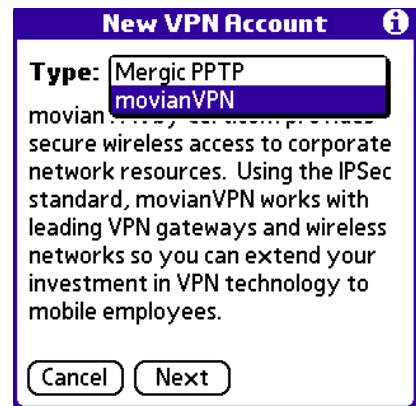
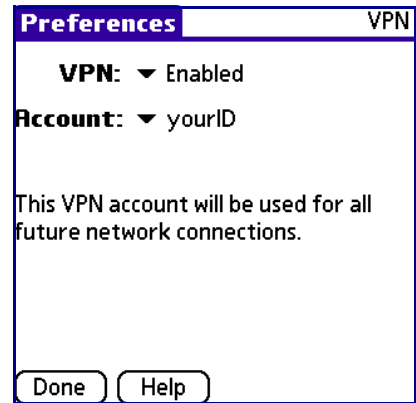
12. Tap the **Done** button to proceed to the main **movianVPN** window.



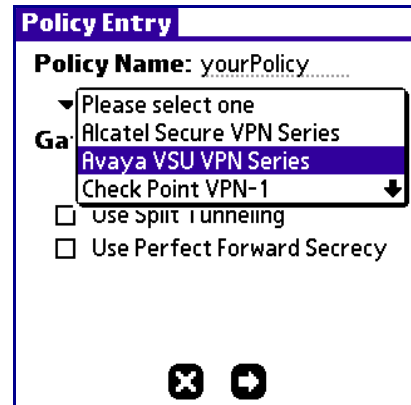
Configuration (Tungsten-C, Tungsten-T3 Devices)

Setting network preferences

1. There are two ways to add a VPN account. The first is to choose the Prefs icon from the Applications screen, and then select VPN. You must then Enable the VPN by selecting "Enabled" from the pulldown list for the "VPN" field. Then, tap the "- Tap to Add - " field. The second is to choose VPN Setup from the Application screen, then tap the 'Next' button.
2. The next window allows you to choose the type of VPN Account you wish to create. Choose **movianVPN** from the pulldown list and press the "Next" button.
3. Enter a name for your policy in the **Policy Name** field.



4. Select your gateway from the pulldown list. Any options available for that gateway will now be displayed on the Policy Entry form.



Policy Entry



Policy Name: yourPolicy.....

Ga: ▼ Please select one

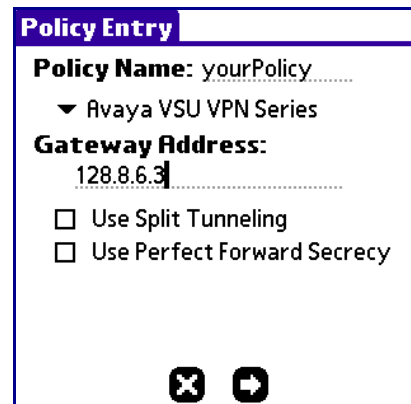
- Alcatel Secure VPN Series
- Avaya VSU VPN Series**
- Check Point VPN-1

Use Split Tunneling

Use Perfect Forward Secrecy

5. Enter in your gateway's IP address.
6. From here, you may complete your configuration by referring to the appropriate section detailing your gateway's configuration options, located in the section "Creating a Policy" beginning on page 39.



Policy Entry



Policy Name: yourPolicy.....

▼ Avaya VSU VPN Series

Gateway Address:
128.8.6.3

Use Split Tunneling

Use Perfect Forward Secrecy

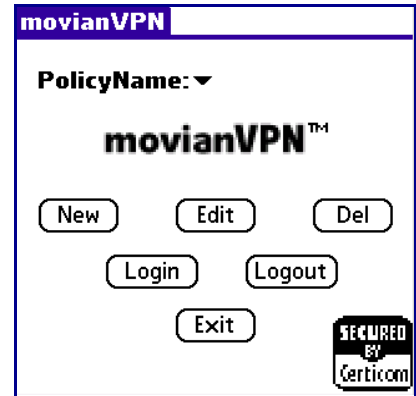
Checking the movianVPN version number

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

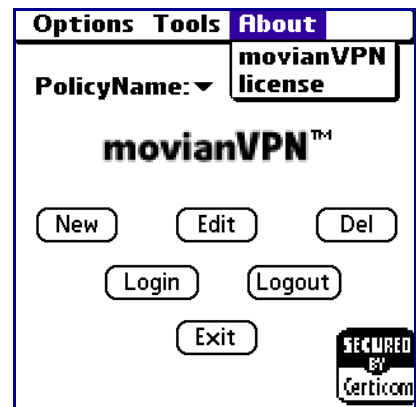
To check your **movianVPN** version number:

Standard Palm Devices

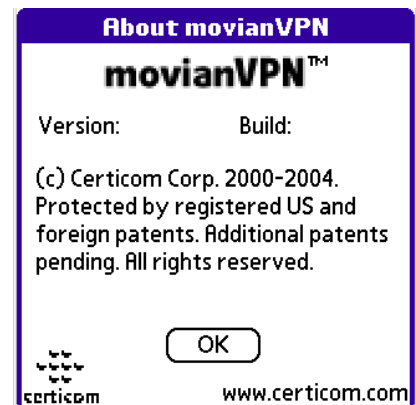
1. Open the **movianVPN** application.



2. Open the main menu by tapping **movianVPN** in the upper toolbar and then tap **About** to open the **About** menu.

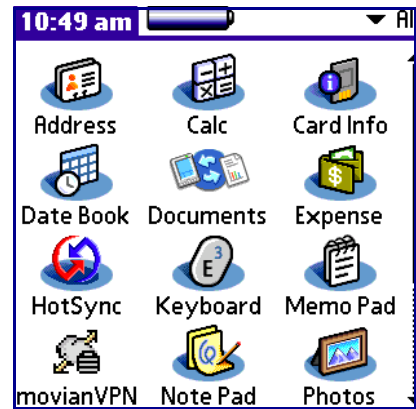


3. Tap **About movianVPN**. The **About movianVPN** window appears. This window contains the information regarding version and build required for technical support.
4. Tap **OK** to close the window and return to **movianVPN**.



For Tungsten-C,
Tungsten-T3
Devices

1. From your **Applications** screen, tap the **movianVPN** button.



2. This opens the **About movianVPN** window. The information you will need is the **Version** number and the **Build** number. Tap OK to exit this screen.



Licensing movianVPN

While it is possible to run the **movianVPN** software without a license, you cannot login to your gateway without a license. There are two types of license; evaluation and full. In the final seven days of an evaluation license, you will be informed of the number of days remaining each time you login to the VPN gateway. To activate **movianVPN** for a longer period, you must obtain a full license.

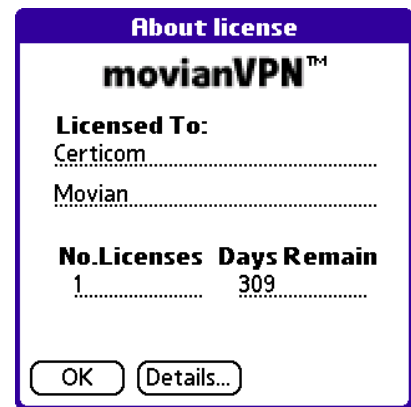
Licensing movianVPN

To obtain a licens for **movianVPN**, visit <http://www.certicom.com/buymovian> and contact one of our channel partners. Once you purchase a license, you will receive another installer which will activate your device for the duration of your subscription. For more information, please refer to “Appendix E: Installing a movianVPN License” on page 135

Checking your current license type

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

1. Open the **movianVPN** application.
2. Tap **movianVPN** in the upper toolbar and tap **About** in the toolbar that appears.
3. Select the **About license** menu option. The **About license** window appears and displays the type of license, number of licenses, and days remaining in the evaluation copy. The **About license** window shows the current information on whether the installation is licensed or for evaluation, the number of licenses, and the days remaining.
4. Tap **OK** to close the **About license** window.



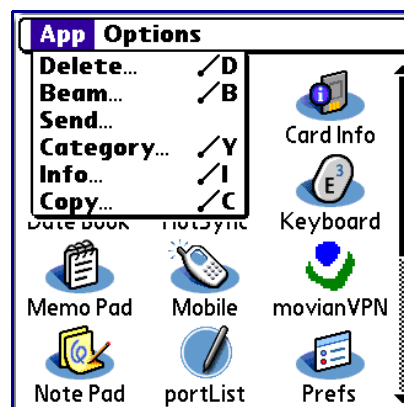
Reaching movianVPN support

Please refer to the package release notes.

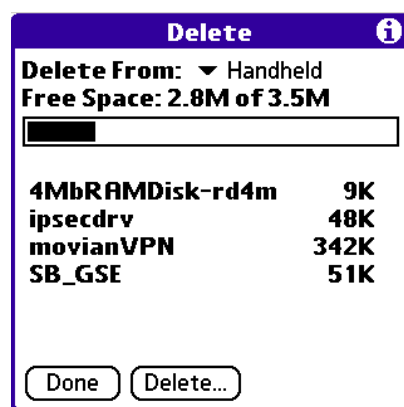
Uninstalling movianVPN

To remove **movianVPN** from your handheld device, follow the steps below.

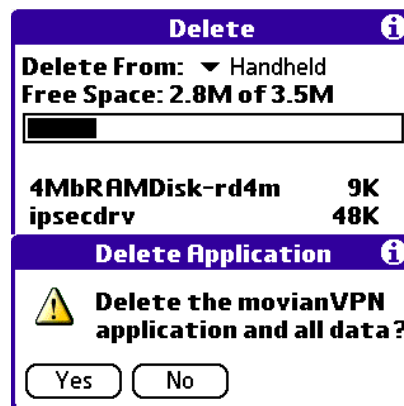
1. Tap the **Applications** icon on your handheld device. Open the **App** menu by selecting it.



2. Open the **Delete** window by choosing **Delete** from the **App** menu. The **Delete** window appears and displays the applications that can be deleted from your handheld device.



3. Select **movianVPN**. Tap **Delete**. The **Delete Application** confirmation window appears.
4. Tap **Yes** to continue with the deletion of **movianVPN**; tap **No** to leave **movianVPN** installed.
5. In the **Delete** window, select **SB_GSE** and confirm the deletion as done above for **movianVPN**.
6. If **ipsecdrv** appears in the **Delete** window, select it and remove it from your device.
7. Tap **Done**. The **movianVPN** application and its assorted library files have been removed.



3

Verifying Your Setup

Configuration Check

Before you can use **movianVPN** to connect to your VPN gateway you must complete the following steps:

- Verify your connection and network settings.
- Verify your connection to the internet.
- Configure a policy to connect to the VPN gateway.

If you are using **movianVPN** in a corporate setting, your handheld device may have already been configured to connect to the internet and a **movianVPN** policy created to allow you to access the gateway. If this is the case, you can go to “Running movianVPN” on page 101.

Step 1: Verify Your Connection Settings

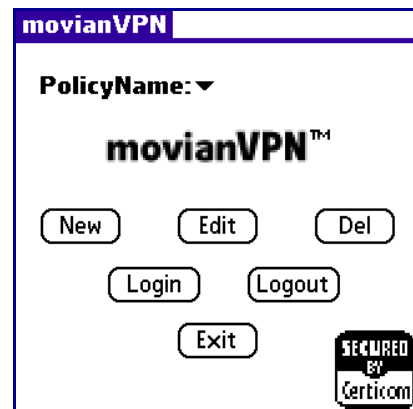
You should verify your communications hardware settings and the settings you use to connect to your ISP.

Verifying your connection preferences (Standard Palm Devices)

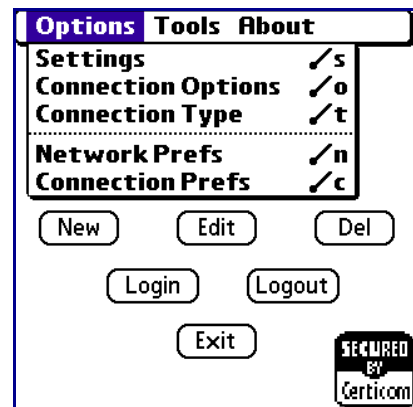
The **Connection Preferences** window allows you to configure the hardware you use to connect to the internet. The **Connection Preferences** window appears after the license window when you first start **movianVPN**. For more information, see page 12.

You can access the **Connection Preferences** window when **movianVPN** is running.

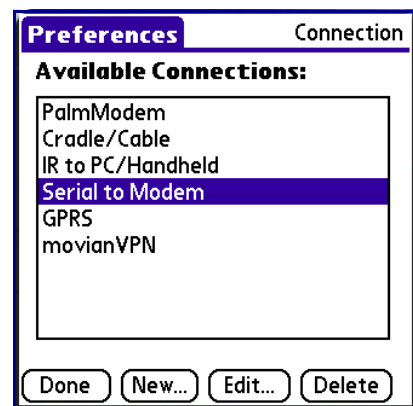
1. Tap the **movianVPN** tab in the top toolbar to open the menu bar.



2. Open the **Options** menu. Select **Connection Prefs**. This opens the **Connection Preferences** window.



3. Select **movianVPN** from the list and tap the **"Edit..."** button. Confirm the settings for your communications hardware. For more information on the settings, see page 12.

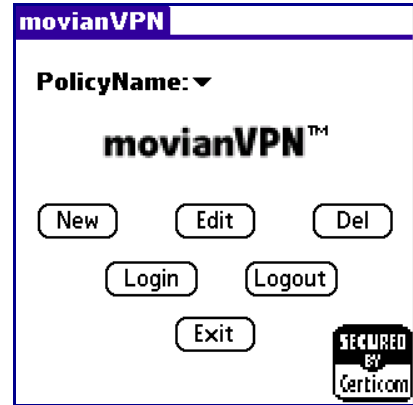


Verifying your network preferences (Standard Palm Devices)

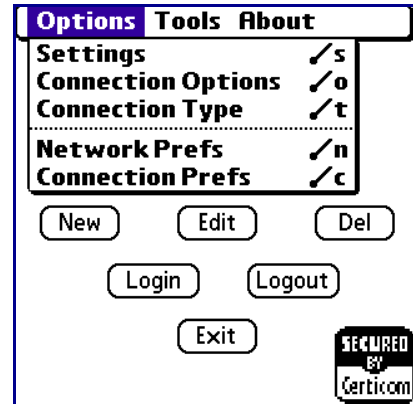
The **Network Preferences** window allows you to configure your ISP settings. The **Network Preferences** window appears after the **Connection Preferences** window when you first start **movianVPN**. For more information, see page 12.

You can also access the **Network Preferences** window when **movianVPN** is running.

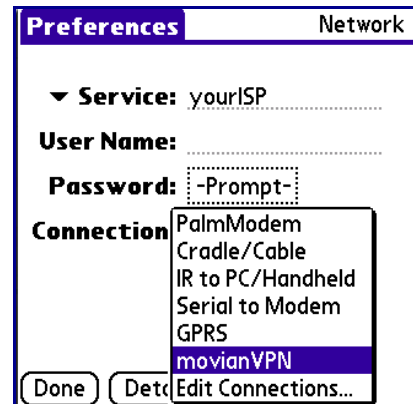
1. In **movianVPN**, tap the **movianVPN** tab in the top toolbar.



2. Open the **Options** menu. Select **Network Prefs**. The **Network Preferences** window appears.



3. Ensure that the **Connection** field is set to **movianVPN**. If not, you can tap the arrow at the Connection field and select it from the pull-down list. If you have been provided the other settings, say, by an administrator, please ensure that the values in the **Preferences** window match accordingly.



Step 2: Verify Your Internet Connection

Before **movianVPN** can connect to the VPN gateway, you must have an active connection to the Internet via ISP.

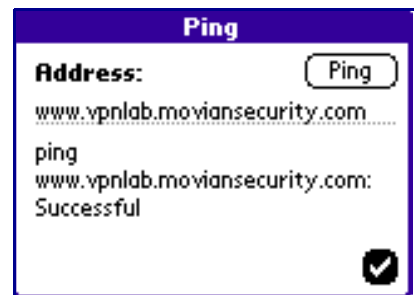
You can check your internet connection independently of having the **movianVPN** in operation.

***Note:** To set up your internet connection, refer to the documentation which accompanied your handheld device regarding its operating system, access card, and modem configuration.*

To check that your internet connection is working after a successful dial-up to your ISP, use the ping tool.

To ping a server:

1. Tap the **movianVPN** tab.
2. Open the **Tools** menu and select **Ping** from the list. The **Ping** window appears.
3. Enter either the IP address or domain name of a known internet host, such as `www.yahoo.com`.
4. Tap the **Ping** button. The Ping window will display the results.
5. If the ping is successful, your connection is open.
6. If the ping operation fails to reach the host, you will receive an error message.
7. Tap the checkmark button to close the ping application.



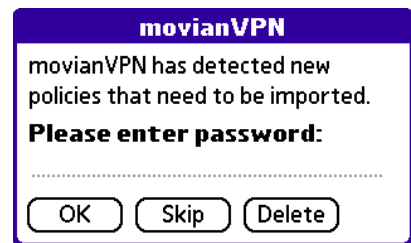
Step 3: Provide a policy for your gateway

Note: You may provide a policy for your gateway in one of two ways: you may import it from a policy file, or you may create a policy using your client software. To create a policy for your gateway, you will require information specific to your gateway, which may have been supplied by your network administrator. This information may be supplied to you in a form such as that shown in “Appendix D: Information worksheet” on page 133.

Importing a policy from a policy file (Standard Palm Devices)

If you have been provided with a policy file, you will not be required to create a policy using the client software. Just HotSync the file, named **vpolimp.pdb**, and restart **movianVPN**.

1. If a password has been set to protect the policy file, you will be prompted to enter the password. Enter the password and tap the **OK** button to import the policy. Press **Skip** if you do not wish to import the policy at this time; you will be prompted for the password the next time you launch **movianVPN**. If you no longer wish to import the policy, press the **Delete** button to remove the import policy from your device.



2. Provided the import was successfully completed, a message indicating the policy has been successfully imported will be displayed. Tap OK to close this message window.



Note: If you enter an incorrect password, you must restart the **movianVPN** application to enter the password again.

Creating your own policy file using movianVPN

For detailed instructions on how to create a policy compatible with your gateway, please refer to the next chapter.

Step 4: Creating a Policy

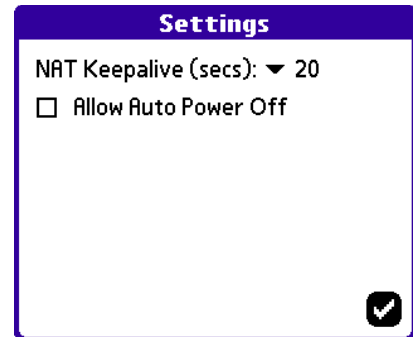
Next you will need to create a policy that is specific to the VPN gateway that you are connecting to. Please follow the instructions appropriate to your gateway found in the section “Creating a Policy” on page 39. After you have done that, please consult the remainder of this chapter for further information regarding connection options and verifying your policy.

Step 5: Global Options (Standard Palm Devices)

There are several options that may be configured for **movianVPN** that apply regardless of the policy that is in use. These are configured by opening the **Options** menu and selecting **Settings**.

There are two options that may be configured.

Note: Please note that these Global options do not apply to Tungsten-C and Tungsten-T3 devices.



NAT Keepalive

NAT, or Network Address Translation, is a method of connecting multiple computers to an IP network (e.g. the Internet) using only one IP address. This allows home users and small businesses to connect their computers to a single network for a lower cost by sharing a single access point rather than paying for each connection. NAT-T is a non-proprietary version of NAT that has been modified such that machines sharing a single IP address can still make use of programs that require each machine to have a separate IP address for identification purposes (networked games, for example). **movianVPN** currently supports NAT-T on the following gateways:

- Cisco VPN Concentrator 3000 v3.6
- Cisco Secure PIX Firewall VPN Gateway v6.1.1
- Netscreen VPN Gateway v3.0
- CoSine VPN Gateway 4.01

NAT-T will automatically be negotiated if it is enabled on one of the above gateways. The only option available in **movianVPN** is the NAT Keepalive value. NAT Keepalive is used to ensure that the NAT mapping on the NAT gateway does not expire while you are using applications that rely upon the mappings. While the default value should be sufficient, you may wish to decrease the value if you encounter problems with applications that rely upon NAT while using a gateway that has NAT-T enabled.

Allow Auto Power Off

On earlier Palm devices, if the device goes into sleep mode while connected, the connection is lost and you must log off and then log on again to re-establish your connection to the VPN. Later units, such as the Tungsten-W, do not lose their connection after the device goes to sleep and is re-activated.

You can prevent your device from powering down while you are connected by selecting the **Allow Auto Power Off** option. When it is selected, the power off timer is disabled, and a message to this effect appears in the **movianVPN** application window. Be forewarned that your machine will not shut off while this option is selected, and therefore your battery will be drained until you disable this feature.

Step 6: Connection Options (Standard Devices)

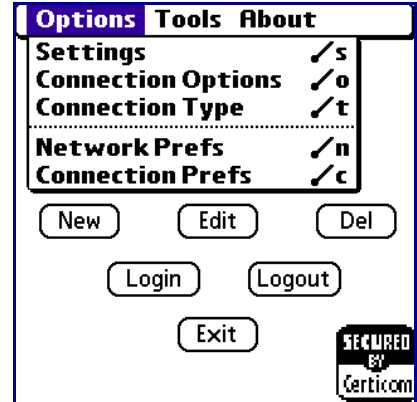
Setting Connection Options (Standard Palm Devices)

There are two connection options that may be set in **movianVPN**:

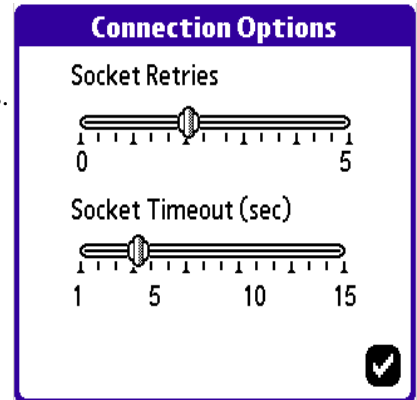
- **Socket Retries** – the number of times **movianVPN** will attempt to connect.
- **Socket Timeout** – the amount of time allowed before an attempt is considered to be a failure.

To set your connection options:

1. Open the **Options** menu. Select **Connection Options** from the menu. The **Connection Options** window appears.



2. Set the values for **Socket Retries** and **Socket Timeout** using the sliders.
3. Tap the checkmark button to save your values.



Step 7: Verifying your policy

Once your policy has been created, you may need to review settings and options.

Policy window checkboxes

For the majority of Palm devices, policies are accessed by entering the policy name on the main screen and tapping the **Edit** button.

To edit a policy on a Tungsten-C or Tungsten-T3 device, tap the VPN button in the Preferences window and then select "Edit Accounts" and select which account you wish to edit from the list that appears, clicking "Edit" to proceed to the **Policy Entry** window.

The **Policy Entry** window presents you with a different set of configurable options, dependent upon the type of gateway selected. These options appear as checkboxes in the **Policy Entry** window. The options that are supported are:

- Split Tunneling
- Perfect Forward Secrecy
- Extended Authentication

Certain options may be required to be enabled for a particular gateway. In these cases, the option will be automatically selected when the policy is created and cannot be deselected, as this would result in an invalid policy configuration.

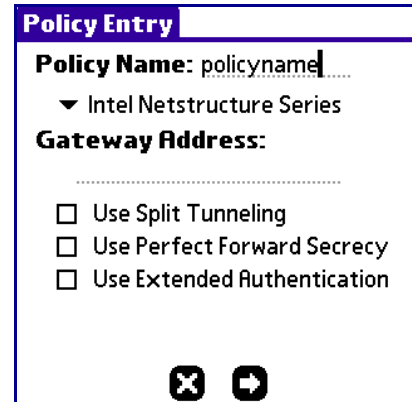
A particular gateway need not support all of the options. Only the options that a gateway supports are shown on its **Policy Entry** screen.

Split Tunneling

On gateways which support it, you can enable Split Tunneling. When split tunneling is enabled, you can freely access the Internet and securely access 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. If the communication is not directed to or received from identified subnets on the VPN, the traffic goes directly through the ISP to the internet and is not encrypted. All packets sent to or from the VPN and its identified subnets are encrypted. Split tunneling secures sensitive VPN traffic, while allowing less sensitive material to flow normally.

When Split Tunneling is selected, packets to inside the VPN are encrypted; packets to outside the VPN are 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.



Perfect Forward Secrecy

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

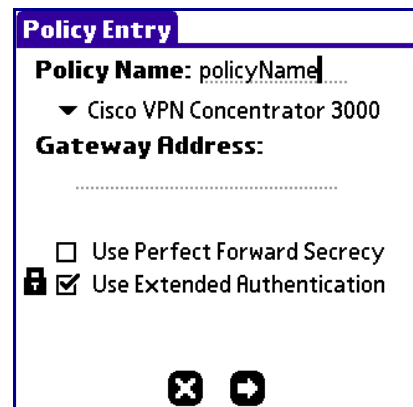
Perfect Forward Secrecy performs the key exchange twice as your handheld device negotiates with the gateway, using the same key material. A new key is created for each step of the Internet Key Exchange (IKE), and each new key is not derived from the previous key. The previous key or the one following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

Negotiation of the connection will take longer.

Extended Authentication

Extended Authentication requires the user to supply an additional User Password or another form of additional authentication when you log onto the gateway. Extended Authentication can be used to require an additional password or a passcode associated with a tokencard, depending on the type of gateway.

Extended Authentication is always required for some gateways. In those instances, Extended Authentication is selected and the option is locked, with a locked icon displayed beside the checkbox.



Storing Your Extended Authorization Password

Some gateways provide a feature that allows you to store your password during extended authentication. This feature appears as a checkbox in the Extended Authentication window.

Warning: Storing your password on the device is an insecure practice. Anyone that uses your device will be able to use your network connection.

Not all gateways support this feature.



Changing SecurID passcodes

SecurID tokencodes provide one form of extended authentication that operates with **movianVPN**. A tokencode (a small electronic device with a display window) and the VPN server are programmed to simultaneously generate a new number at set intervals; the server and the tokencode generate the same number, by using the same algorithm.

To log in to the gateway, you must supply the same number that the server is using as a key. The number will be prefaced by your PIN number as a user.

The PIN number may be up to six numbers, with its length determined by your network administrator. For more information on using tokencodes, contact your administrator.

If you are using SecurID for Extended Authentication, you may be asked to change your PIN code when you login to the gateway. The system will ask whether you want to have a generated passcode or select one yourself.

After several failed attempts, the SecurID may be put in NEXTTOKEN mode. When in this mode, after the user enters the code successfully, the user will be asked to wait until the token changes, and to then enter their new tokencode. After entering the code, tap the OK button to continue.

The screenshot shows a dialog box titled "IKE Status Messages" with a "Reply" header. The main text reads: "Wait for token to change, then enter the new tokencode:". Below this, there is a "Name: echins" field and a "Reply:" input field. At the bottom, there are "OK" and "Cancel" buttons.

The SecurID may also be put into NEWPIN mode. When in this mode, after you enter the code successfully, you will be asked to enter a new PIN. Enter it and tap the OK button.

The screenshot shows a dialog box titled "IKE Status Messages" with a "Reply" header. The main text reads: "Enter a new PIN having from 4 to 6 digits:". Below this, there is a "Name: echins" field and a "Reply:" input field. At the bottom, there are "OK" and "Cancel" buttons.

You must wait for the next token, and then enter the code using your new PIN.

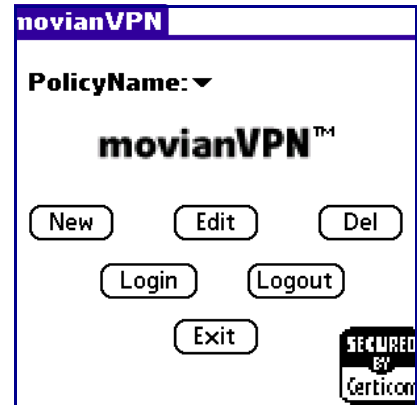
The screenshot shows a dialog box titled "IKE Status Messages" with a "Reply" header. The main text reads: "PIN Accepted. Wait for the token code to change, then enter the new passcode:". Below this, there is a "Name: echins" field and a "Reply:" input field. At the bottom, there are "OK" and "Cancel" buttons.

Editing the policy checkboxes

If you need to make any changes to the policy checkbox options, you must edit the policy before logging in.

To make changes to the policy checkbox options:

- 1a. (Standard Palm Devices) When you open **movianVPN**, select the policy you wish to edit from the **Policy Name** list and tap the **Edit** button. This results in the **Policy Entry** window opening.
- 1b. (Tungsten-C, Tungsten-T3) Tap the **VPN** icon in the Preferences window and then select "Edit Accounts". Select the account you wish to edit from the list that appears, clicking "Edit" to proceed to the **Policy Entry** window.
2. Set the options for your policy as desired.
3. Tap the arrow icon. The **Gateway Identification** page appears.
4. Tap the checkmark button. The **movianVPN** window appears.
5. Tap the **Login** button to connect to the gateway using the new settings.



Note: It is recommended that if settings were provided to you by an administrator, that you use those settings for your policy.

Using IPSec (Standard Palm Devices)

While using **movianVPN**, you can change whether IPSec is enabled or disabled during your session with the gateway. When IPSec is not enabled, your data will not be encrypted. This will allow you to access servers and websites outside the Virtual Private Network, on the Internet, but you 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. You can freely access the Internet and securely access the corporate intranet at the same time. (For more information, see “Split Tunneling” on page 31.)

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

For more information in IPSec and IPSec protocols, see “IPSec” on page 4 and “Disabling and Enabling IPSec” on page 113.

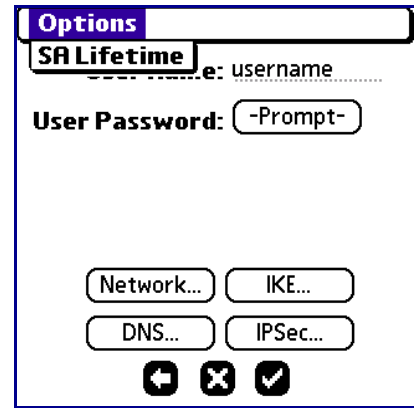
Policy gateway access settings

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

The following may be configured, depending on your gateway:

- DNS
- IKE Crypto Suite
- Network Properties
- IPsec Crypto Suite

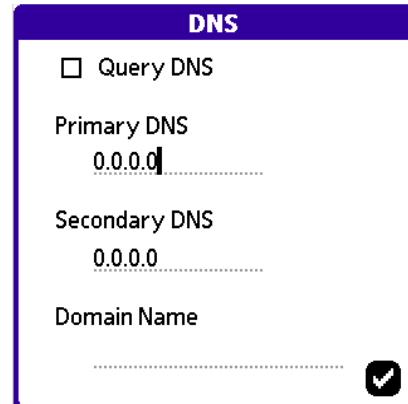
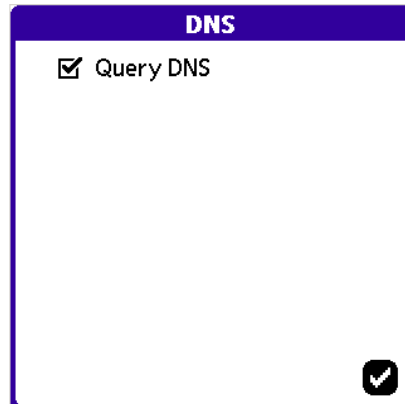
The DNS, IKE Crypto Suite, Network Properties, and IPsec Crypto Suite values are configured when creating a policy. They can also be changed by tapping the **Edit** button in the **movianVPN** window before logging in.



DNS

Domain Name System (DNS) settings are used to identify particular computers or parts of the network you access by **movianVPN**. Some gateways supply this information to the handheld device during key negotiation.

If **Query DNS** is selected, 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.



IKE Crypto Suite

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

Note: These values should be not be changed unless you have be directed to do so by your network administrator.

Group

Group refers to the strength of the key encryption negotiation.

IKE Crypto Suite

Group: ▼ GRP1_DH-768
GRP2_DH-1024

Cipher: ▼ GRP7_ECDH-163

Hash: ▼ MD5

Cipher

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

IKE Crypto Suite

Group: ▼ GRP1_DH-768

Cipher: ▼ DES_CBC
3DES_CBC

Hash: ▼

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.

IKE Crypto Suite

Group: ▼ GRP1_DH-768

Cipher: ▼ 3DES_CBC

Hash: ▼ MD5
SHA

Network Properties

The fields in the **Network Properties** window identify primary and secondary subnet IP addresses and masks. These are the network subnets that you access as part of the VPN.

Packets sent to these subnets are encrypted when Split Tunneling is selected.

The screenshot shows the 'Network Properties' window with a 'Protected Networks' section. It contains a table with two columns: 'IP Address' and 'Subnet Mask'. There are three rows, each with '0.0.0.0' in both columns. A checkmark is visible in the bottom right corner of the window.

IP Address	Subnet Mask
0.0.0.0	0.0.0.0
0.0.0.0	0.0.0.0
0.0.0.0	0.0.0.0

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 values should not be changed unless you have been instructed to do so.

The screenshot shows the 'IPSec Crypto Suite' window. It features a 'Suite:' dropdown menu with three options: 'ESPIP_NULL_MD5-96', 'ESPIP_NULL_SHA-96', and 'ESPIP_DES_NULL'. A checkmark is visible in the bottom right corner of the window.

SA Life

The Security Association or SA is a limited-lifetime statement of the negotiated security policies between the communicating devices, such as session keys and agreed encryption algorithms. The SA Life slide bar is used to set a time-out limit on access to the gateway by the client software.

Time-outs are also dependent on the gateway, which may also have an automatic time-out for users. The client's SA is a proposal only; if the gateway's time-out limit is lower, the gateway's time-out will come into effect.

The default SA Life setting is one hour.

Note: For more information on time-outs for handheld devices and the VPN gateway, contact your network administrator.

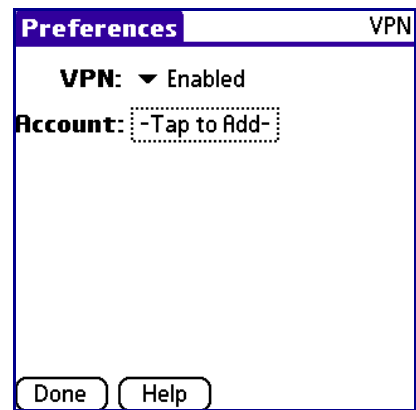
4

Creating a Policy

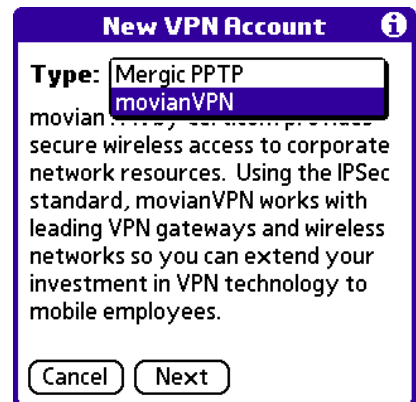
Creating Policies for Tungsten-C, Tungsten-T3 Devices

If you are creating a policy for a Tungsten C or Tungsten T3 device, you will do this a slightly different way than for a standard Palm device.

1. There are two ways to add a VPN account. The first is to choose **Prefs** from the **Applications** screen, and then select **VPN**. You must then Enable the VPN by selecting "Enabled" from the pulldown list for the "VPN" field. Then, tap the "Tap to Add" field. The second way to add a VPN account is to choose **VPN Setup** from the Application screen, then tap the 'Next' button.



2. The **New VPN Account** window allows you to choose the type of VPN Account you wish to create. Choose **movianVPN** from the pulldown list and press the "Next" button to take you to the **Policy Entry** screen.



3. Enter a name for your policy in the "Policy Name" field. You may now select your gateway from the pulldown list and enter in the gateway address. For detailed instructions on configuring a policy for a specific gateway, please see the appropriate section in the next chapter.



The screenshot shows a dialog box titled "Policy Entry". It contains a text input field for "Policy Name" with the text "yourPolicy" entered. Below this is a dropdown menu with the text "Please select one". Underneath the dropdown is a label "Gateway Address:" followed by a dotted line indicating an input field. At the bottom right of the dialog box are two icons: a square with an 'X' and a square with a right-pointing arrow.

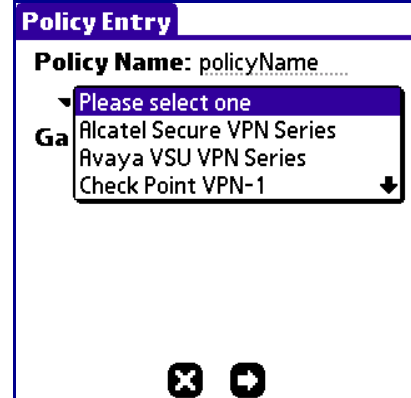
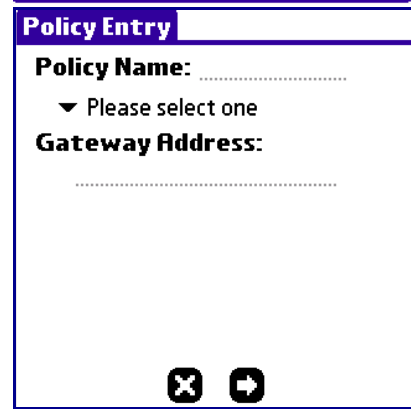
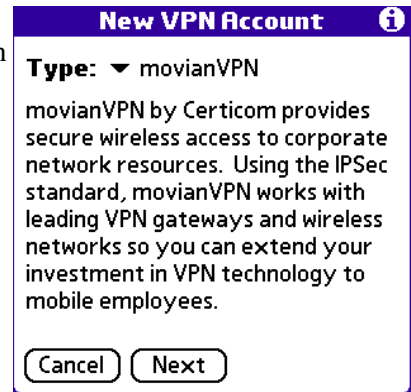
Creating a policy for an Alcatel Secure VPN Series gateway

To create a policy for an **Alcatel Secure VPN Series** gateway you will require the following information:

- Gateway IP address
- Checkbox status for Split Tunneling, Perfect Forward Secrecy and Extended Authentication
- A combination of group name, group password, user name and user password, depending on whether Extended Authentication is selected
- IKE Suite, DNS and IPSec Suite settings
- SA life setting

To create a policy for an **Alcatel Secure VPN Series** gateway:

- 1a. (Standard Palm Device) Open the **movianVPN** application, and tap **New** to open the **Policy Entry** window.
- 1b. (Tungsten-C, Tungsten-T3) Select **VPN** from the Preferences window, ensure that VPN is set to enabled, and tap the "Tap to Add" button. On the **New VPN Account** screen, select **movianVPN** as the type, and tap **Next** to continue to the **Policy Entry** window.
2. Enter a name for the policy in the **Policy Name** field.
3. Open the list of gateways by tapping the "Please select one" arrow. Select **Alcatel Secure VPN Series** from the list. Checkboxes for the policy options appear.



4. Enter the network address for your gateway in the **Gateway Address** field.

Note: If you were provided with values for these fields by an administrator, please use them.

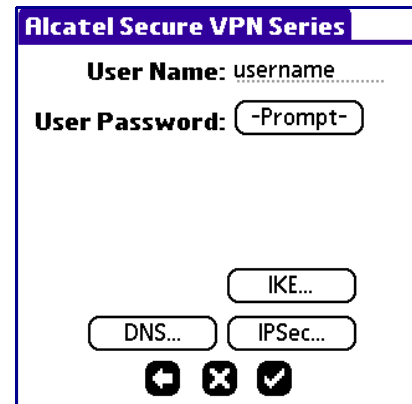
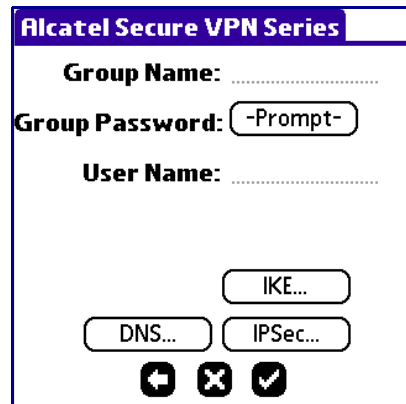
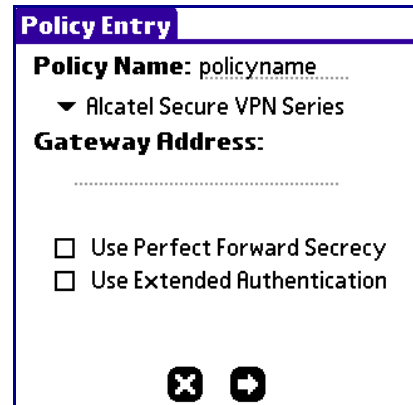
5. Select **Use Perfect Forward Secrecy** if you wish to use perfect forward secrecy. (For more information, see “Perfect Forward Secrecy” on page 32.)
6. Select **Use Extended Authentication** if you wish to enable extended authentication.

Note: When you connect to the gateway you will be asked for further authentication. For more information, see “Extended Authentication” on page 32.

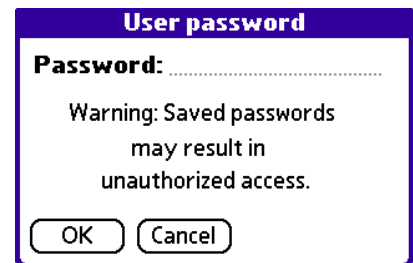
7. Tap the arrow button to return to the **Alcatel Secure VPN Series** window.

Note: If you have selected Extended Authentication you will be asked for a Group Name and Password as well as the User Name (you supply the password when logging in). If you have not selected Extended Authentication, you will be asked for User Name and User Password.

8. Enter the group name and user name in the **Group Name** and **User Name** fields.
– OR –
Enter your user name in the **User Name** field.



9. If you have been instructed to save your password, tap **Prompt** in the **Group Password** or **User Password** field (whichever appears in the **Alcatel Secure VPN Series** window). The **User password** window appears. Otherwise, please skip the following step if you do not wish to save your password.



10. Enter your password and tap **OK** to store it, or **Cancel** if you wish to exit without saving your password. If you save your password, the **User Password** field in the **Alcatel Secure VPN Series** window contains the value "Assigned". To delete or

edit the password, tap "Assigned", then leave the field blank to delete the password, or enter a new password. Tap **OK** to save your changes.

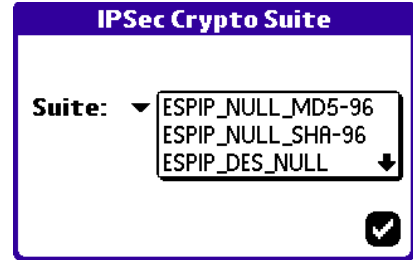
Note: If you do not save your password, you will be asked for it when you login to the gateway.

11. Tap the "IKE..." button to open the **IKE Crypto Suite** window. (For more information, see "IKE Crypto Suite" on page 36.)
12. Set your crypto suite settings by selecting your desired values from each of the pull-down lists for the **Group**, **Cipher**, and **Hash** fields.

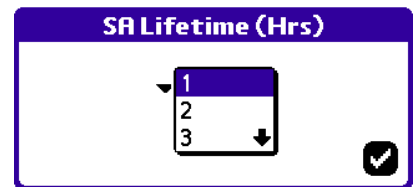
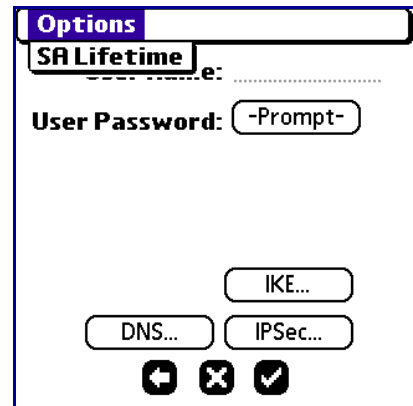
13. Tap the checkmark button to return to the **Alcatel Secure VPN Series** window.
14. Tap the "DNS..." button to open the **DNS** window. If "Query DNS" is deselected, further fields appear. (For more information, see "DNS" on page 35.)
15. If you were directed to do so, deselect "Query DNS" and enter the primary and secondary DNS addresses and the domain name in the appropriate fields.

16. Tap the checkmark button to return to the **Alcatel Secure VPN Series** window.

17. Tap the "IPSec..." button to open the **IPSec Crypto Suite** window. (For more information, see "IPSec Crypto Suite" on page 37.)
18. Set the value of the **Suite** field by selecting one of the crypto suite options from the list.
19. Tap the checkmark button to return to the **Alcatel Secure VPN Series** window.
20. Tap the **movianVPN** tab at the top of the window. Choose **SA Lifetime** from the **Options** menu.



21. Set the **SA Lifetime** by selecting a value from the list. (For more information, see "SA Life" on page 37.)
22. Tap the checkmark button to return to the **Alcatel Secure VPN Series** window.
- 23a. (Standard Palm Devices) Tap **Done**. The **movianVPN** application window appears. Tap the **Login** button to connect to the gateway.
- 23b. (Tungsten-C, Tungsten-T3 Devices) Tap the checkmark to return to the Preferences window. Tap **Done** to begin using your device with the new settings.



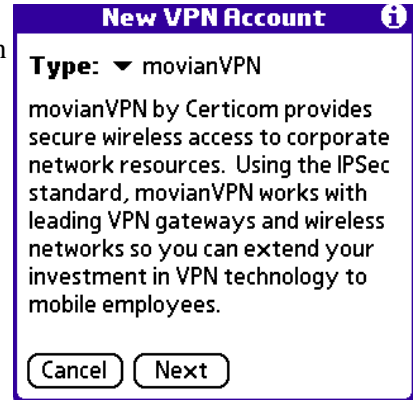
Creating a policy for an Avaya VSU VPN Series

To create a policy for an **Avaya VSU VPN Series** gateway you will require the following information:

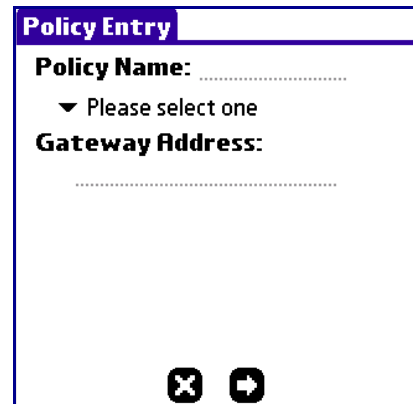
- Gateway IP address
- Checkbox status for Split Tunneling and Perfect Forward Secrecy
- User name and user password
- Network, IKE Suite, DNS, and IPSec Suite settings
- SA life setting

To create a policy for an **Avaya VSU VPN Series** gateway:

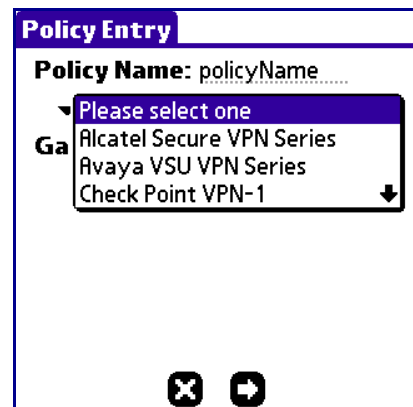
- 1a. (Standard Palm Device) Open the **movianVPN** application, and tap **New** to open the **Policy Entry** window.
- 1b. (Tungsten-C, Tungsten-T3) Select **VPN** from the Preferences window, ensure that VPN is set to enabled, and tap the "Tap to Add" button. On the **New VPN Account** screen, select **movianVPN** as the type, and tap **Next** to continue to the **Policy Entry** window.



2. Enter a name for the policy in the **Policy Name** field.



3. Open the list of gateways by tapping the "Please select one" arrow. Select **Avaya VSU VPN Series** from the list. Checkboxes for gateway policy options appear.



4. Enter the network address of your gateway into the **Gateway Address** field.
Note: If you were provided with values for these fields by an administrator, please use them.
5. Select **Use Split Tunneling** if you wish to enable split tunneling. (For more information, see “Split Tunneling” on page 31.)
6. Select **Use Perfect Forward Secrecy** if you wish to enable perfect forward secrecy. (For more information, see “Perfect Forward Secrecy” on page 32.)
7. Tap the arrow button to continue to the **Avaya VSU VPN Series** window.
8. Enter your account name in the **User Name** field.

9. If you wish to store your user password, tap **Prompt** in the **User Password** field; otherwise, please skip the following step.

10. The **User password** window appears. Enter your password and tap **OK**. In the **Avaya VSU VPN Series** window, the **User Password** field now appears with the value "**Assigned**". To delete or edit the password, tap **Assigned**, and leave the field blank to remove the password, or enter a new password. Tap **OK** to save your changes.

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

11. Tap the "Network" to open the **Network Properties** window. (For more information, see "Network Properties" on page 37.)
12. Enter the IP addresses and subnet masks for the primary and secondary subnets.
13. Tap the checkmark button to return to the **Avaya VSU VPN Series** window.
14. Tap the "IKE..." button to open the **IKE Crypto Suite** window. (For more information, see "IKE Crypto Suite" on page 36.).

Network Properties	
Protected Networks	
IP Address	Subnet Mask
0.0.0.0	0.0.0.0
0.0.0.0	0.0.0.0
0.0.0.0	0.0.0.0

15. Set your crypto suite settings by selecting your desired values from each of the pull-down lists for the **Group**, **Cipher**, and **Hash** fields.

IKE Crypto Suite

Group: ▾ GRP1_DH-768
GRP2_DH-1024
GRP7_ECDH-163

Cipher: ▾ GRP7_ECDH-163

Hash: ▾ MD5

IKE Crypto Suite

Group: ▾ GRP1_DH-768

Cipher: ▾ DES_CBC
3DES_CBC

Hash: ▾

IKE Crypto Suite

Group: ▾ GRP1_DH-768

Cipher: ▾ 3DES_CBC

Hash: ▾ MD5
SHA

16. Tap the checkmark button to return to the **Avaya VSU VPN Series** window.
17. Tap the "DNS..." button to open the **DNS** window. If **Query DNS** is deselected, further fields appear. (For more information, see "DNS" on page 35.).
18. If you have been directed to do so, deselect **Query DNS** and enter the primary and second DNS addresses in the **Primary DNS** and **Secondary DNS** fields. Enter your domain name in the **Domain Name** field.

DNS

Query DNS

DNS

Query DNS

Primary DNS
0.0.0.0

Secondary DNS
0.0.0.0

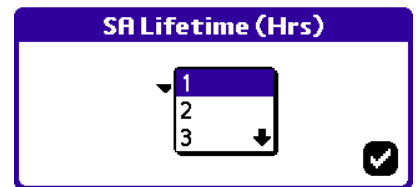
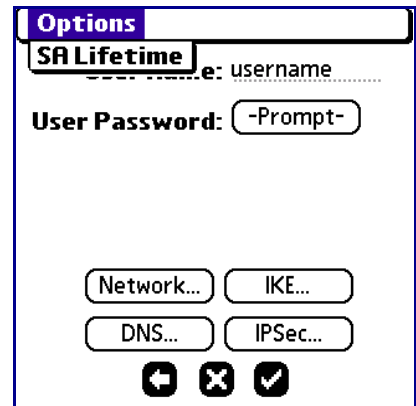
Domain Name
.....

19. Tap the checkmark button to return to the **Avaya VSU VPN Series** window.

20. Tap the "IPSec..." button to open the **IPSec Crypto Suite** window. (For more information, see "IPSec Crypto Suite" on page 37.)
21. Set the value of the **Suite** field by selecting one of the crypto suite options from the list.
22. Tap the checkmark button to return to the **Avaya VSU VPN Series** window.
23. Tap the **movianVPN** tab at the top of the window. Select **SA Lifetime** from the **Options** menu.



24. Set the **SA Lifetime** by selecting a value from the list. (For more information, see "SA Life" on page 37.)
25. Tap the checkmark button to return to the **Avaya VSU VPN Series** window.
- 26a. (Standard Palm Devices) Tap **Done**. The **movianVPN** application window appears. Tap the **Login** button to connect to the gateway.
27. (Tungsten-C, Tungsten-T3 Devices) Tap the checkmark to return to the Preferences window. Tap **Done** to begin using your device with the new settings.



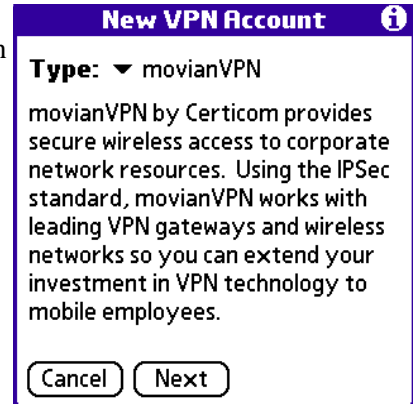
Creating a policy for a Check Point VPN-1 gateway

To create a policy for a **Check Point VPN-1** gateway you will require the following information:

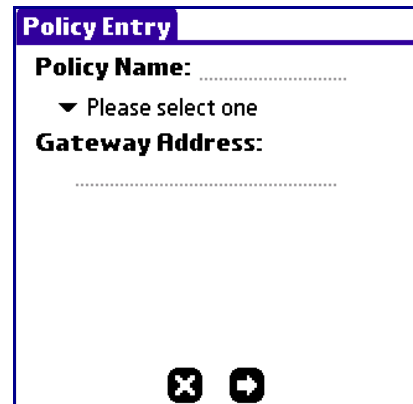
- Gateway IP address
- Checkbox status for Split Tunneling
- User name and user password
- Network, IKE Suite, DNS and IPSec Suite settings
- SA life setting

To create a policy for a **Check Point VPN-1** gateway:

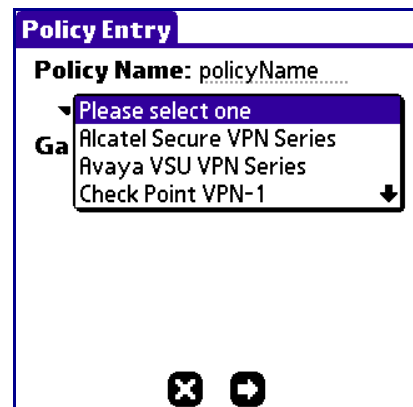
- 1a. (Standard Palm Device) Open the **movianVPN** application, and tap **New** to open the **Policy Entry** window.
- 1b. (Tungsten-C, Tungsten-T3) Select **VPN** from the Preferences window, ensure that VPN is set to enabled, and tap the "Tap to Add" button. On the **New VPN Account** screen, select **movianVPN** as the type, and tap **Next** to continue to the **Policy Entry** window.



2. Enter a name for the policy in the **Policy Name** field.



3. Open the list of gateways by tapping the "Please select one" arrow. Select **Check Point VPN-1** from the list. Checkboxes for policy options appear.



4. Enter the network address of your gateway in the **Gateway IP Address** field.

Note: If you were provided with values for these fields by an administrator, please use them.

5. Select **Use Split Tunneling** if you wish to enable split tunneling. (For more information, see “Split Tunneling” on page 31.)

6. Tap the arrow button to return to the **Check Point VPN-1** window.
7. Enter your account name in the **User Name** field.

8. If you wish to save your user password as a part of your policy, tap **Prompt** in the **User Password** field. This opens the **User password** window. Otherwise, please skip the following step.

9. Enter your password and tap **OK**. In the **Check Point VPN-1** window, the User Password now appears as **Assigned**. To delete or edit the password, tap **Assigned**, and leave the field blank to delete the password or enter a new password. Tap **OK** to save your changes.

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

10. Tap the **Network** button to open the **Network Properties** window. (For more information, see “Network Properties” on page 37.)
11. Enter the IP addresses and subnet masks for the primary and secondary subnets.
12. Tap the checkmark button to return to the **Check Point VPN-1** window.
13. Tap the **"IKE..."** button to open the **IKE Crypto Suite** window. (For more information, see “IKE Crypto Suite” on page 36.)

Network Properties	
Protected Networks	
IP Address	Subnet Mask
0.0.0.0	0.0.0.0
0.0.0.0	0.0.0.0
0.0.0.0	0.0.0.0

14. Set your crypto suite settings by selecting your desired values from each of the pull-down lists for the **Group**, **Cipher**, and **Hash** fields.

IKE Crypto Suite

Group: ▾ GRP1_DH-768
GRP2_DH-1024
GRP7_ECDH-163

Cipher: ▾ GRP7_ECDH-163

Hash: ▾ MD5

IKE Crypto Suite

Group: ▾ GRP1_DH-768

Cipher: ▾ DES_CBC
3DES_CBC

Hash: ▾ MD5
SHA

IKE Crypto Suite

Group: ▾ GRP1_DH-768

Cipher: ▾ 3DES_CBC

Hash: ▾ MD5
SHA

15. Tap the checkmark button to return to the **Check Point VPN-1** window.
16. Tap the **"DNS..."** button to open the **DNS** window. If **Query DNS** is deselected, further fields appear. (For more information, see “DNS” on page 35.)
17. If instructed to do so, deselect **Query DNS**. Enter the primary and secondary DNS addresses in the **Primary DNS** and **Secondary DNS** fields, and the domain name in the **Domain Name** field.

DNS

Query DNS

DNS

Query DNS

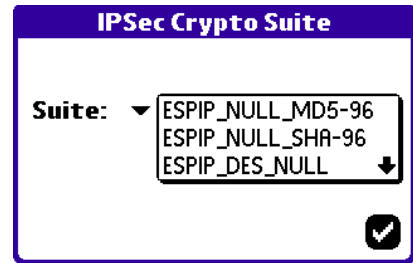
Primary DNS
0.0.0.0

Secondary DNS
0.0.0.0

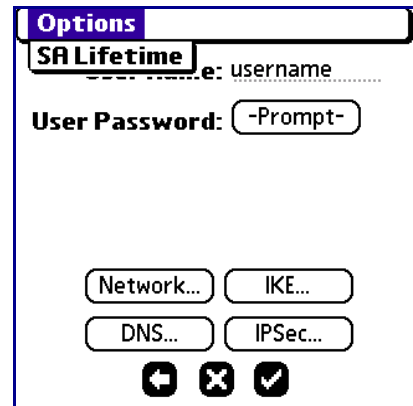
Domain Name
.....

18. Tap the checkmark button to return to the **Check Point VPN-1** window.

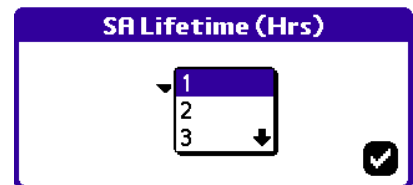
19. Tap the "IPSec..." button to open the **IPSec Crypto Suite** window. (For more information, see "IPSec Crypto Suite" on page 37.)
20. Set the value of the **Suite** field by selecting one of the crypto suite options from the list.
21. Tap the checkmark button to return to the **Check Point VPN-1** window.
22. Tap the **movianVPN** tab at the top of the window. The **Options** menu appears. Select **SA Lifetime** to configure the SA Lifetime value.



23. Set the **SA Lifetime** by selecting a value from the list. (For more information, see "SA Life" on page 37.)
24. Tap the checkmark button to return to the **Check Point VPN-1** window.



- 25a. (Standard Palm Devices) Tap **Done**. The **movianVPN** application window appears. Tap the **Login** button to connect to the gateway.
26. (Tungsten-C, Tungsten-T3 Devices) Tap the checkmark to return to the Preferences window. Tap **Done** to begin using your device with the new settings.



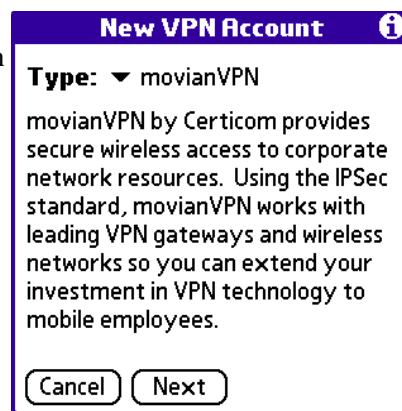
Creating a policy for a Cisco Unified Client Framework, Cisco Secure PIX Firewall VPN, or a Cisco IOS Easy VPN gateway

To create a policy for a **Cisco Unified Client Framework**, **Cisco Secure PIX Firewall VPN**, or **Cisco IOS Easy VPN** gateway you will require the following information:

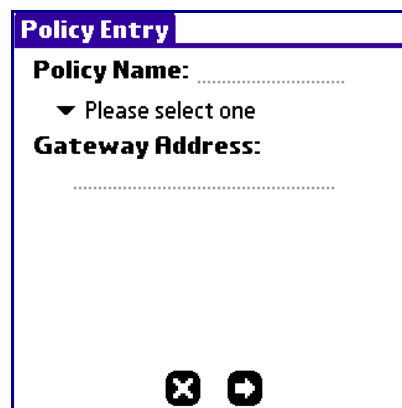
- Gateway IP address
- Enable either/both of Perfect Forward Secrecy and Extended Authentication
- Group name, group password, user name and user password
- IKE Suite, DNS, and IPSec Suite settings
- SA life setting

To create a policy for a **Cisco Unified Client** gateway:

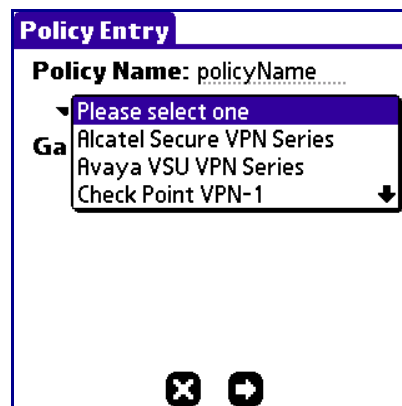
- 1a. (Standard Palm Device) Open the **movianVPN** application, and tap **New** to open the **Policy Entry** window.
- 1b. (Tungsten-C, Tungsten-T3) Select **VPN** from the Preferences window, ensure that VPN is set to enabled, and tap the "Tap to Add" button. On the **New VPN Account** screen, select **movianVPN** as the type, and tap **Next** to continue to the **Policy Entry** window.



2. Enter a name for the policy in the **Policy Name** field.



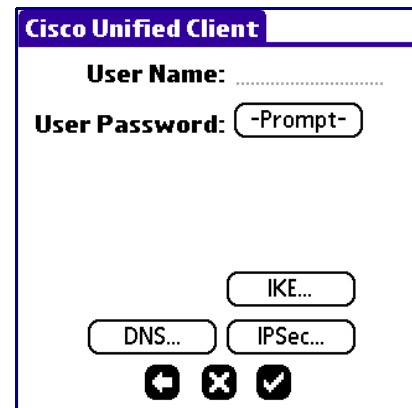
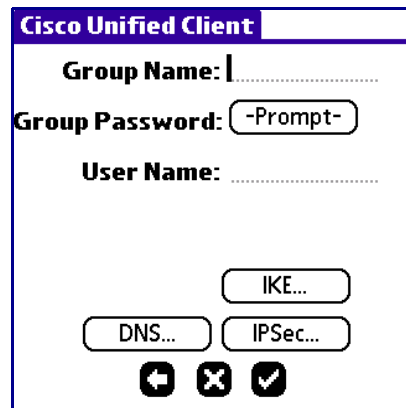
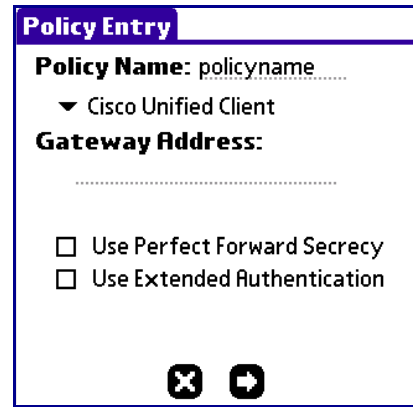
3. Open the list of gateways by tapping the "Please select one" arrow.



4. Select **Cisco Unified Client** from the list. The **Gateway Address** field and the gateway policy security option checkboxes appear.
5. Enter the network address for your gateway in the **Gateway Address** field.

Note: If you have been given instructions on how to fill in these fields, please follow them.

6. Select **Use Perfect Forward Secrecy** if you wish to enable perfect forward secrecy. (For information, see “Perfect Forward Secrecy” on page 32.)
7. Select **Use Extended Authentication** if you wish to enabled extended authentication. For more information, see“Extended Authentication” on page 32.
8. Tap the arrow button to open the **Cisco Unified Client** window.
9. If extended authentication is enabled, enter your group name and user name in the **Group Name** and **User Name** fields.
 – OR –
 If extended authentication is disabled, enter your user name in the **User Name** field.

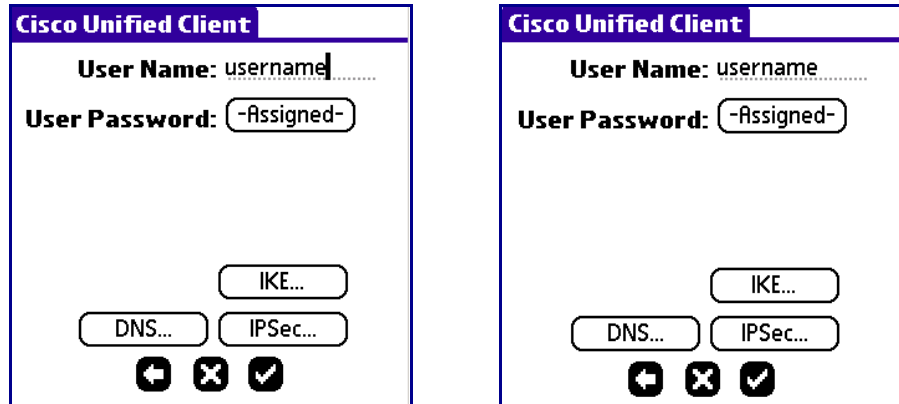


10. If you wish to store your user password, tap **Prompt** in which ever of the **User Password** or **Group Password** fields is on your form. This opens the **User password** window. If you do not wish to store your password, please skip the following step.

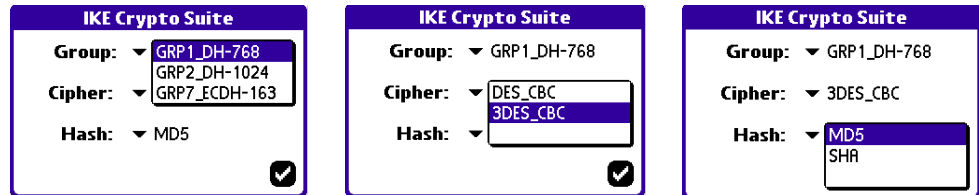


11. In the **Cisco Unified Client** window, the **User Password** or **Group Password** (if extended authentication is enabled) field now contains the value "Assigned". To delete or edit the password, tap **Assigned**, either leave the field blank to delete or enter a new password, and tap **OK** to return to the **Cisco Unified Client** window.

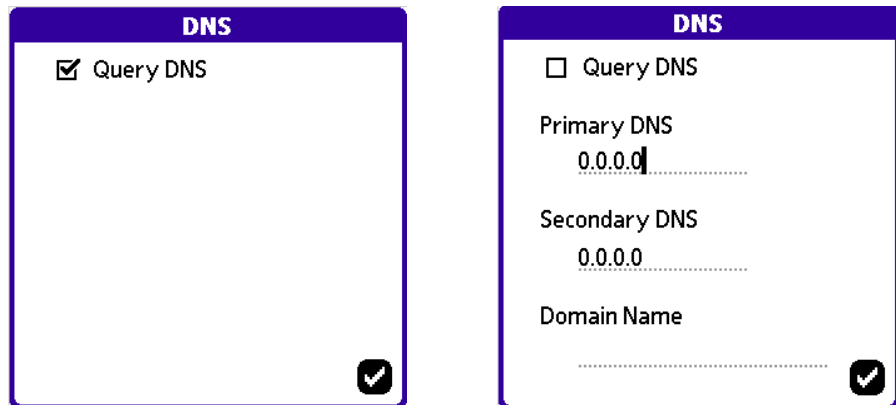
Note: If you do not save your password in your policy, you will be asked for it when you log in to the gateway.



12. Enter your account name into the **User Name** field.
Note: When you log in to the gateway you will be asked for your User password.
13. Tap the **"IKE..."** button to open the **IKE Crypto Suite** window. (For more information, see **"IKE Crypto Suite"** on page 36.)
14. Set your crypto suite settings by selecting your desired values from each of the pull-down lists for the **Group**, **Cipher**, and **Hash** fields.



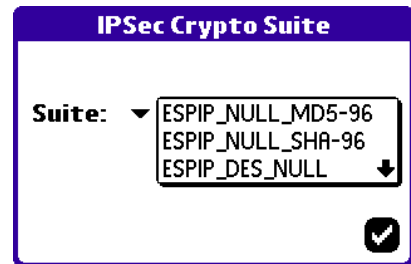
15. Tap the checkmark button to return to the **Cisco Unified Client** window.
16. Tap the **"DNS..."** button to open the **DNS** window. If **Query DNS** is deselected, further fields will appear. (For more information, see **"DNS"** on page 35.).



17. If directed to do so, deselect **Query DNS** and enter the primary and secondary DNS addresses and the gateway domain name in the appropriate fields.

18. Tap the checkmark button to return to the **Cisco Unified Client** window.

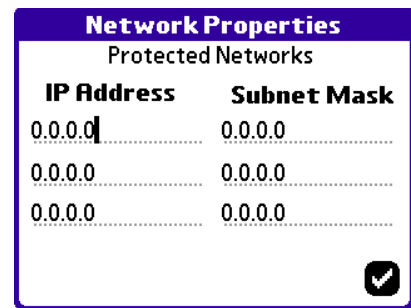
19. Tap the "**IPSec...**" button to open the **IPSec Crypto Suite** window. (For more information, see "IPSec Crypto Suite" on page 37.)



20. Open the list of available crypto suites by clicking the arrow beside the **Suite** field. Select your desired crypto suite from the list.

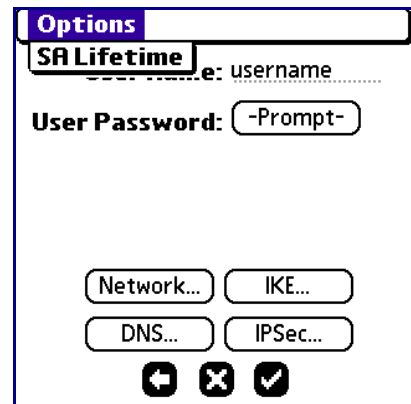
21. Tap the checkmark button to return to the **Cisco Unified Client** window.

22. Tap the "**Network...**" button to open the **Network Properties** window.



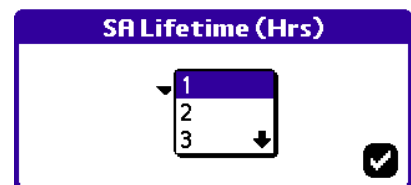
23. Enter the IP addresses and subnet masks for your VPN. Tap the checkmark button to return to the **Cisco Unified Client** window.

24. Open the **movianVPN tab** at the top of the window. The **Options** menu appears. Select **SA Lifetime** from the menu to set the SA lifetime value.



25. Set the **SA Lifetime** by selecting a value from the list. (For more information, see "SA Life" on page 37.)

26a. (Standard Palm Devices) Tap **Done**. The **movianVPN** application window appears. Tap the **Login** button to connect to the gateway.



27. (Tungsten-C, Tungsten-T3 Devices) Tap the checkmark to return to the Preferences window. Tap **Done** to begin using your device with the new settings.

Creating a policy for a Cisco VPN Concentrator 3000 gateway

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

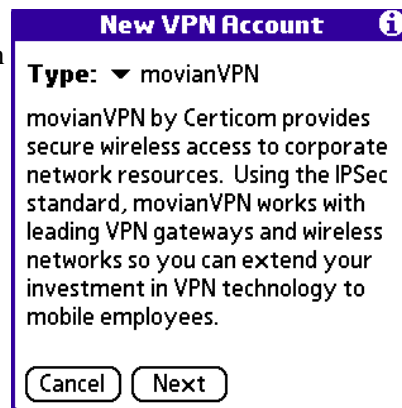
- Gateway IP address
- Checkbox status for Use Perfect Forward Secrecy
- Group name, group password, user name and user password

Note: You will be asked for the user password when you log in to the gateway.

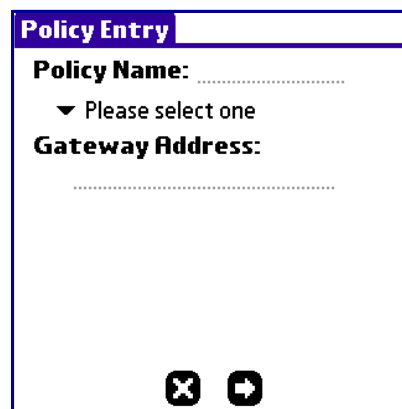
- IKE Suite, DNS and IPSec Suite settings
- SA life setting

To create a policy for a **Cisco VPN Concentrator 3000** gateway:

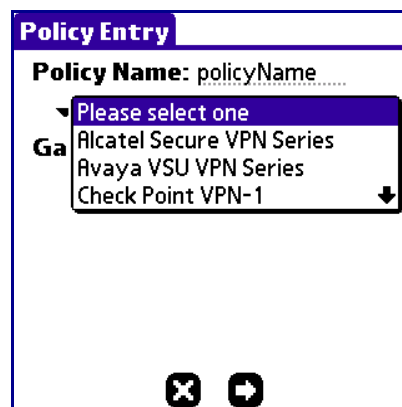
- 1a. (Standard Palm Device) Open the **movianVPN** application, and tap **New** to open the **Policy Entry** window.
- 1b. (Tungsten-C, Tungsten-T3) Select **VPN** from the Preferences window, ensure that VPN is set to enabled, and tap the "Tap to Add" button. On the **New VPN Account** screen, select **movianVPN** as the type, and tap **Next** to continue to the **Policy Entry** window.



2. Enter a name for the policy in the **Policy Name** field.



3. Open the list of gateways by tapping the "Please select one" label. Select **Cisco VPN Concentrator 3000** from the list. The gateway policy security option checkboxes appear.



4. Enter network address of your gateway in the **Gateway Address** field.

Note: If you have been given values for these fields by an administrator, please use them.

*Note: Use **Extended Authentication** is selected by default and locked as required by the Cisco VPN Concentrator 3000 gateways. When you connect to the gateway, you will be asked for further authentication. For information on **Extended Authentication**, see “**Extended Authentication**” on page 32.*

5. Select **Use Perfect Forward Secrecy** if the option is desired. (For more information, please see “**Perfect Forward Secrecy**” on page 32.)
6. Tap the arrow button to continue to the **Cisco VPN Concentrator 3000** window.
7. Enter your group name in the **Group Name** field.

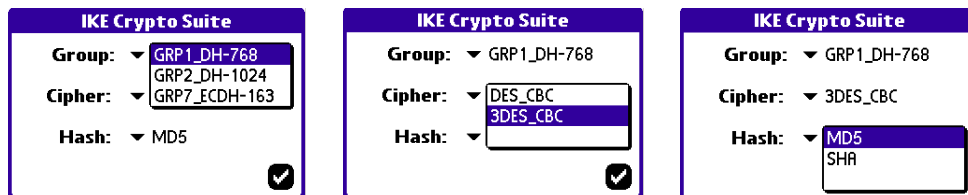
8. If you wish to save your password as a part of your policy, tap **Prompt** in the **Group Password** field to open the **User password** window. If you do not wish to store your password, please skip the following step.

9. Enter your password and tap **OK**. In the **Cisco VPN Concentrator 3000** window, the Group Password now appears as **Assigned**. To delete or edit the password, tap **Assigned** then leave the password field blank to delete your password, or enter a new password. Tap **OK** to save your changes.

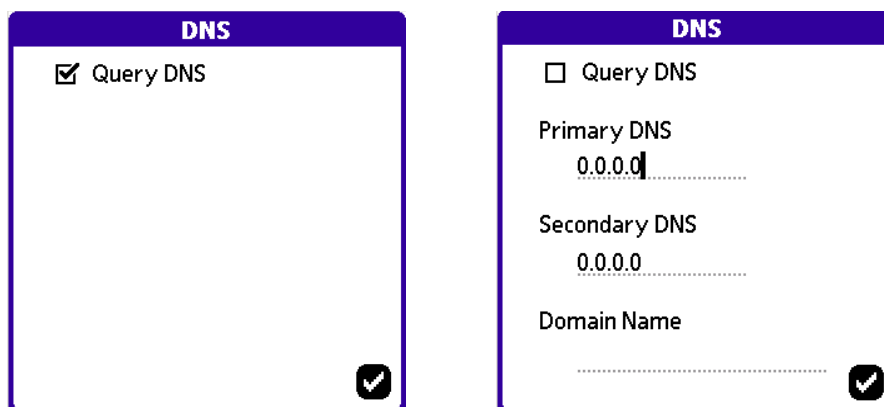
10. Enter your account name into the **User Name** field.

Note: When you log in to the gateway you will be asked for your User password.

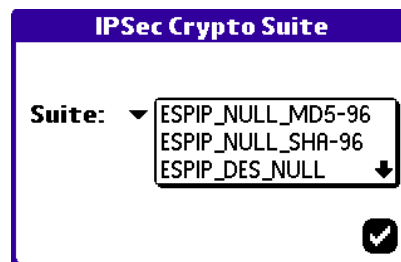
11. Tap the "IKE..." button in the **Cisco VPN Concentrator 3000** window. The **IKE Crypto Suite** window appears. (For more information, see "IKE Crypto Suite" on page 36.).
12. Set your crypto suite settings by selecting your desired values from each of the pull-down lists for the **Group**, **Cipher**, and **Hash** fields.



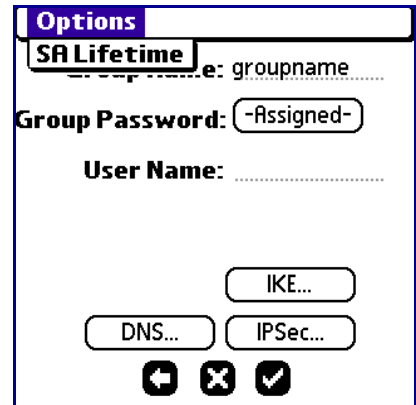
13. Tap the checkmark button to return to the **Cisco VPN Concentrator 3000** window.
14. Tap the "DNS..." button to open the **DNS** window. If **Query DNS** is deselected, further fields will appear. (For more information, please see "DNS" on page 35.).
15. If you were instructed to do so, deselect **Query DNS** and enter the gateway's primary and secondary DNS addresses and the gateway's domain name in the **Primary DNS**, **Secondary DNS**, and **Domain Name** fields.



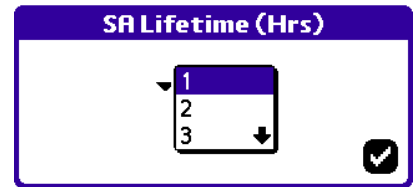
16. Tap the checkmark button to return to the **Cisco VPN Concentrator 3000** window.
17. Tap the "IPSec..." button to open the **IPSec Crypto Suite** window. (For more information, please see "IPSec Crypto Suite" on page 37.).
18. Set the value of the **Suite** field by selecting one of the crypto suite options from the list.
19. Tap the checkmark button to return to the **Cisco VPN Concentrator 3000** window.



20. Tap the **movianVPN** tab to reveal the **Options** menu.
21. Select **SA Lifetime** from the **Options** menu.



22. Set the **SA Lifetime** by selecting a value from the list. (For more information, see “SA Life” on page 37.)
23. Tap the checkmark button to return to the **Cisco VPN Concentrator 3000** window.
- 24a. (Standard Palm Devices) Tap **Done**. The **movianVPN** application window appears. Tap the **Login** button to connect to the gateway.
25. (Tungsten-C, Tungsten-T3 Devices) Tap the checkmark to return to the Preferences window. Tap **Done** to begin using your device with the new settings.



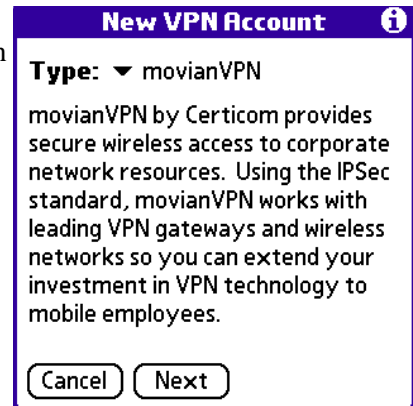
Creating a policy for a CoSine IPSX gateway

To create a policy for a **CoSine IPSX** gateway you will require the following information:

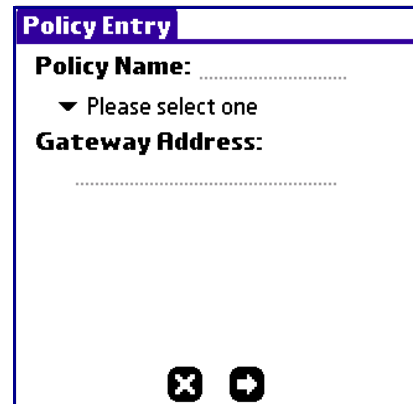
- Gateway IP address
- Whether any/all of Split Tunneling, Perfect Forward Secrecy, and Extended Authentication should be enabled
- A combination of User name and group password, depending upon whether extended authentication is enabled
- Network, IKE Suite, DNS and IPSec Suite settings
- SA life setting

To create a policy for a **CoSine IPSX** gateway:

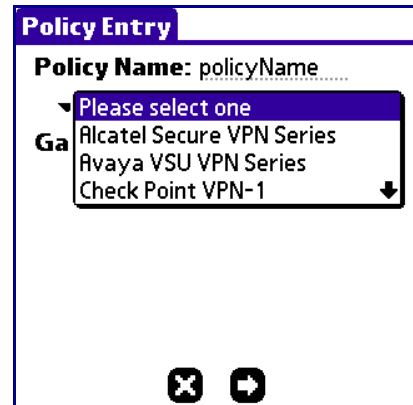
- 1a. (Standard Palm Device) Open the **movianVPN** application, and tap **New** to open the **Policy Entry** window.
- 1b. (Tungsten-C, Tungsten-T3) Select **VPN** from the Preferences window, ensure that VPN is set to enabled, and tap the "Tap to Add" button. On the **New VPN Account** screen, select **movianVPN** as the type, and tap **Next** to continue to the **Policy Entry** window.



2. Enter a name for the policy in the **Policy Name** field.



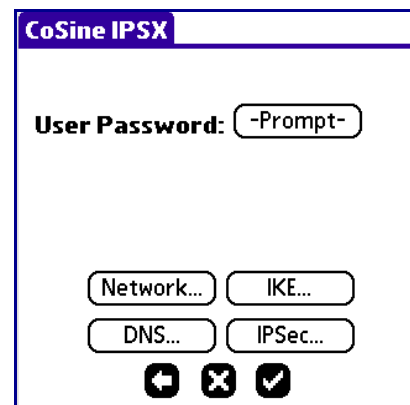
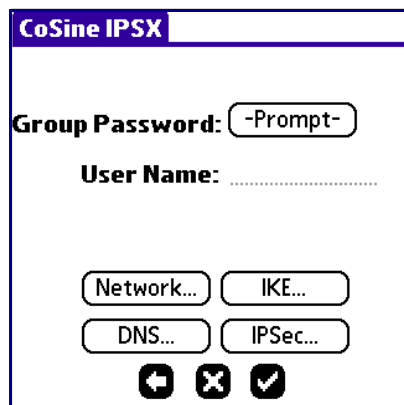
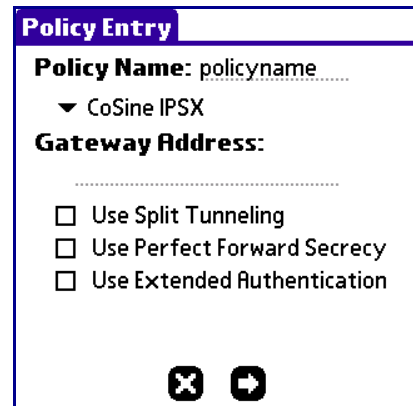
- Open the list of gateways by tapping the "Please select one" arrow. Select **CoSine IPSX** from the list. Checkboxes for policy options appear.



- Enter the network address of your gateway in the **Gateway Address** field.

Note: If you were provided with values for these fields by an administrator, please use them.

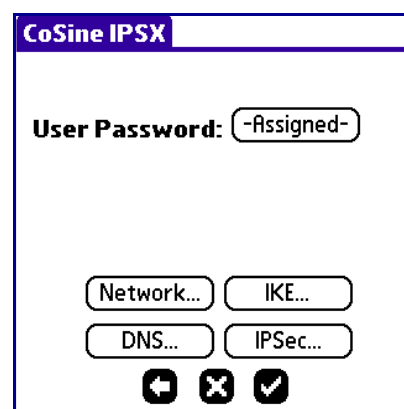
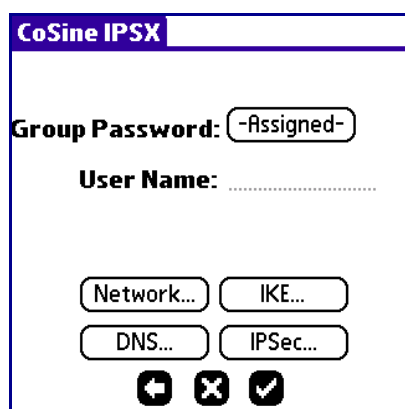
- Select **Use Split Tunneling** if you wish to enable split tunneling. (For more information, see "Split Tunneling" on page 31.)
- Select **Use Perfect Forward Secrecy** if you wish to enable perfect forward secrecy. (For more information, see "Perfect Forward Secrecy" on page 32.)
- Select **Use Extended Authentication** if you wish to enable extended authentication. (For more information, see "Extended Authentication" on page 32.)
- Tap the arrow button to return to the **CoSine IPSX** window.
- If extended authentication is enabled, enter your user name in the **User Name** field.
– OR –
If extended authentication is disabled, carry on to the next step.



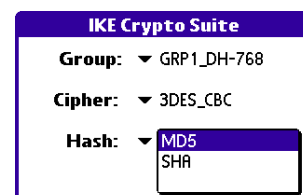
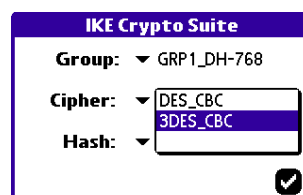
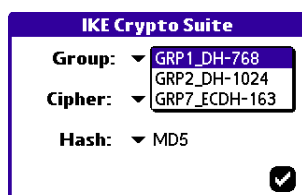
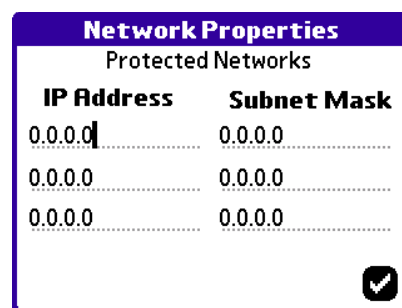
- If you have been instructed to save your password, tap **Prompt** in the **Group Password** field to open the **User password** window. Otherwise, skip the following step.
- Enter your password and tap **OK** to store it, or **Cancel** if you wish to exit without saving your password. If you save your password, either the password field in the **CoSine IPSX** window contains the value "**Assigned**". To delete or edit the password, tap "**Assigned**", then leave the field blank to delete the password, or enter a new password. Tap **OK** to save your changes.



Note: If you do not save your password in your policy, you will be asked for it when you log in to the gateway.

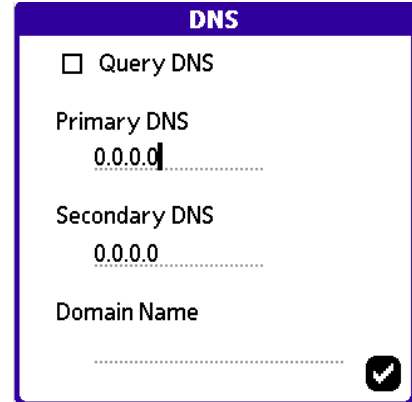
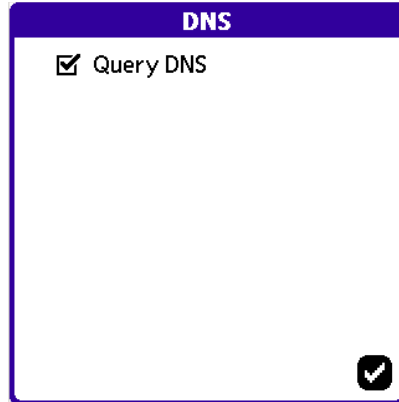


- Tap the "Network" button to open the **Network Properties** window. (For more information, see "Network Properties" on page 37.)
- Enter the IP addresses and subnet masks for the primary and secondary subnets.
- Tap the checkmark button to return to the **CoSine IPSX** window.
- Tap the "IKE..." button to open the **IKE Crypto Suite** window. (For more information, see "IKE Crypto Suite" on page 36.)
- Set your crypto suite settings by selecting your desired values from each of the pull-down lists for the **Group**, **Cipher**, and **Hash** fields.



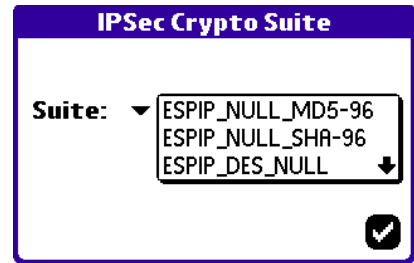
- Tap the checkmark button to return to the **CoSine IPSX** window.

18. Tap the "DNS..." button to open the **DNS** window. If **Query DNS** is deselected, further fields appear. (For more information, see "DNS" on page 35.)
19. If you were directed to do so, deselect **Query DNS** and enter the primary and secondary DNS addresses and your domain name in the appropriate fields.



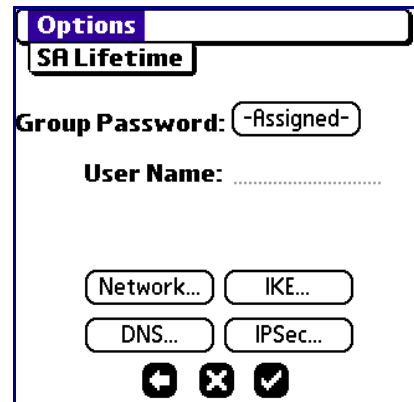
20. Tap the checkmark button to return to the **CoSine IPSX** window.

21. Tap the "IPSec..." button to open the **IPSec Crypto Suite** window. (For more information, see "IPSec Crypto Suite" on page 37.)

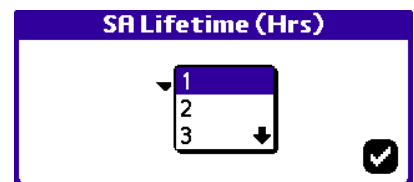


22. Set the value of the **Suite** field by selecting one of the crypto suite options from the list.
23. Tap the checkmark button to return to the **CoSine IPSX** window.

24. Tap the **movianVPN** tab at the top of the window. The **Options** menu appears. Select **SA Lifetime** to set the SA lifetime time-out value.



25. Set the **SA Lifetime** by selecting a value from the list. (For more information, see "SA Life" on page 37.)



26. Tap the checkmark button to return to the **CoSine IPSX** window.

- 27a. (Standard Palm Devices) Tap **Done**. The **movianVPN** application window appears. Tap the **Login** button to connect to the gateway.

28. (Tungsten-C, Tungsten-T3 Devices) Tap the checkmark to return to the Preferences window. Tap **Done** to begin using your device with the new settings.

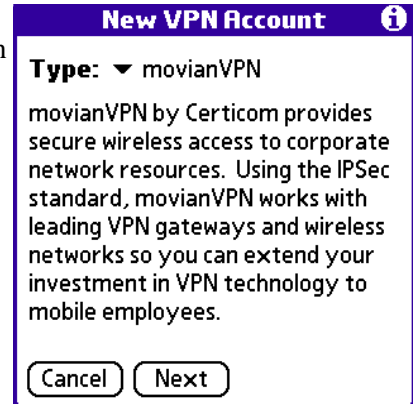
Creating a policy for a Cylink Nethawk gateway

To create a policy for a **Cylink Nethawk** gateway you will require the following information:

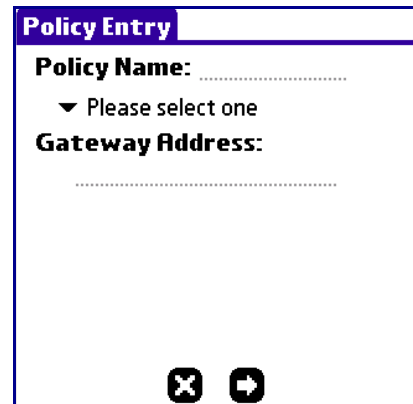
- Gateway IP address
- Checkbox status for Split Tunneling and Perfect Forward Secrecy
- User name and user password
- Network, IKE Suite, DNS and IPSec Suite settings
- SA life setting

To create a policy for a **Cylink Nethawk** gateway:

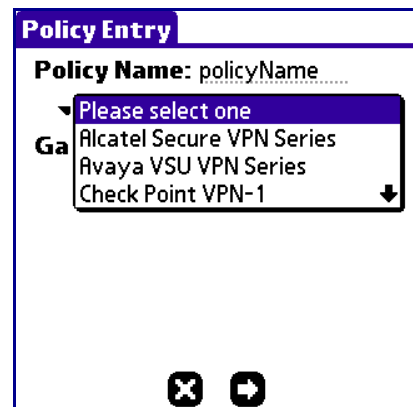
- 1a. (Standard Palm Device) Open the **movianVPN** application, and tap **New** to open the **Policy Entry** window.
- 1b. (Tungsten-C, Tungsten-T3) Select **VPN** from the Preferences window, ensure that VPN is set to enabled, and tap the "Tap to Add" button. On the **New VPN Account** screen, select **movianVPN** as the type, and tap **Next** to continue to the **Policy Entry** window.



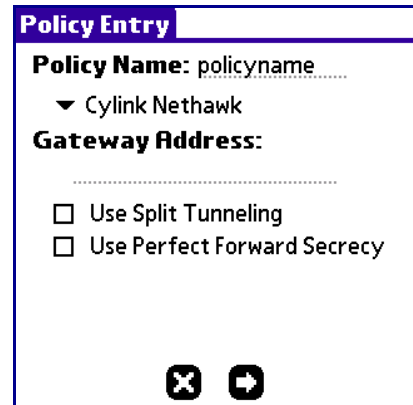
2. Enter a name for the policy in the **Policy Name** field.



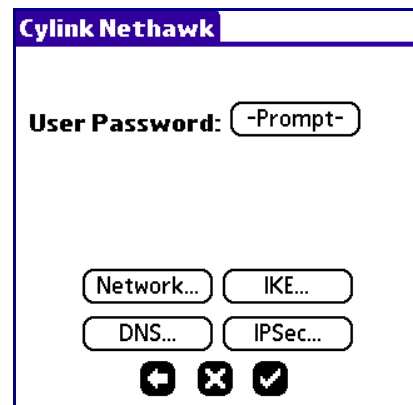
3. Open the list of gateways by tapping the "Please select one" arrow.



4. Select **Cylink Nethawk** from the list. The **Gateway Address** field and the gateway policy security option checkboxes appear.
5. Enter the network address of your gateway into the **Gateway Address** field.
Note: If you have been given instructions on how to fill in these fields, please follow them.
6. Select **Use Split Tunneling** if you wish to enable split tunneling. (For more information, see “Split Tunneling” on page 31.)
7. Select **Use Perfect Forward Secrecy** if you wish to enable perfect forward secrecy. (For more information, see “Perfect Forward Secrecy” on page 32.)
8. Tap the arrow icon to open the **Cylink Nethawk** window.
9. Enter the account name into the **User Name** field.



10. If you wish to store your user password, tap **Prompt** in the **User Password** field. This opens the **User password** window. If you do not wish to store your password, please skip the following step.
11. Enter your gateway password and tap **OK**.
12. In the **Cylink Nethawk** window, the **User Password** field now contains the value "**Assigned**". To delete or edit the password, tap **Assigned**, either leave the field blank to delete or enter a new password, and tap **OK** to return to the **Cylink Nethawk** window.



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

13. Tap the "Network" button to open the **Network Properties** window. (For more information, see "Network Properties" on page 37.)
14. Enter the IP addresses and subnet masks of the primary and secondary subnets.
15. Tap the checkmark button to return to the **Cylink Nethawk** window.
16. Tap the "IKE..." button to open the **IKE Crypto Suite** window. (For more information, see "IKE Crypto Suite" on page 36.)
17. Set your crypto suite settings by selecting your desired values from each of the pull-down lists for the **Group**, **Cipher**, and **Hash** fields.

Network Properties	
Protected Networks	
IP Address	Subnet Mask
0.0.0.0	0.0.0.0
0.0.0.0	0.0.0.0
0.0.0.0	0.0.0.0

IKE Crypto Suite

Group: ▾ GRP1_DH-768
GRP2_DH-1024
GRP7_ECDH-163

Cipher: ▾ GRP7_ECDH-163

Hash: ▾ MD5

IKE Crypto Suite

Group: ▾ GRP1_DH-768

Cipher: ▾ DES_CBC
3DES_CBC

Hash: ▾ MD5
SHA

IKE Crypto Suite

Group: ▾ GRP1_DH-768

Cipher: ▾ 3DES_CBC

Hash: ▾ MD5
SHA

18. Tap the checkmark button to return to the **Cylink Nethawk** window.
19. Tap the "DNS..." button to open the **DNS** window. If **Query DNS** is deselected, further fields appear. (For more information, see "DNS" on page 35.)

DNS

Query DNS

DNS

Query DNS

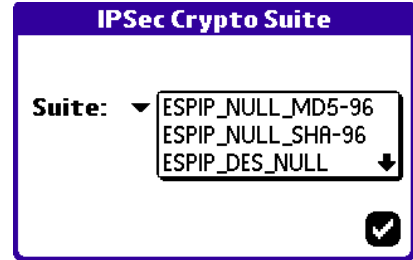
Primary DNS
0.0.0.0

Secondary DNS
0.0.0.0

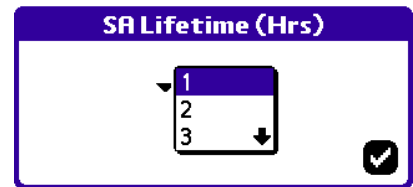
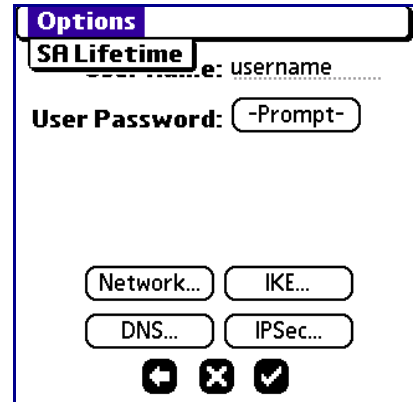
Domain Name
.....

20. If directed to do so, deselect **Query DNS** and enter the primary and secondary DNS addresses and your domain name in the appropriate field.
21. Tap the checkmark button to return to the **Cylink Nethawk** window.

22. Tap the "IPSec..." button to open the **IPSec Crypto Suite** window. (For more information, see "IPSec Crypto Suite" on page 37.)
23. Open the list of available crypto suites by clicking the arrow beside the **Suite** field. Select your desired crypto suite from the list.
24. Tap the checkmark button to return to the **Cylink Nethawk** window.
25. Tap the **movianVPN** tab at the top of the window. The **Options** menu appears. Select **SA Lifetime** from the menu to set the SA lifetime value.



26. Set the **SA Lifetime** by selecting a value from the list. (For more information, see "SA Life" on page 37.)
27. Tap the checkmark button to return to the **Cylink Nethawk** window.
- 28a. (Standard Palm Devices) Tap **Done**. The **movianVPN** application window appears. Tap the **Login** button to connect to the gateway.
29. (Tungsten-C, Tungsten-T3 Devices) Tap the checkmark to return to the Preferences window. Tap **Done** to begin using your device with the new settings.



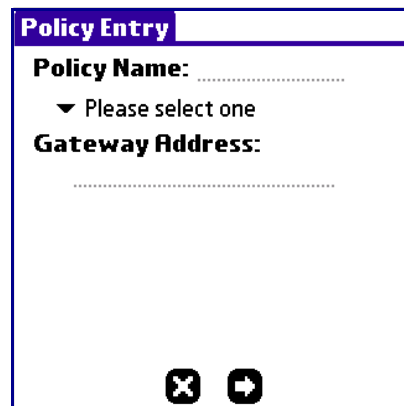
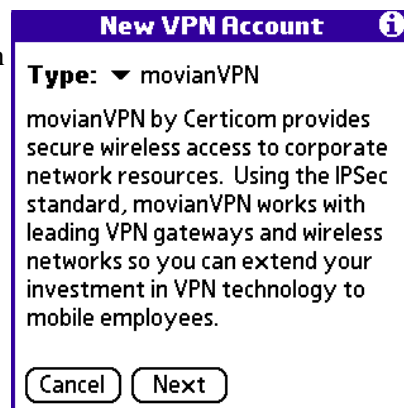
Creating a policy for an Intel Netstructure Series gateway

To create a policy for an **Intel Netstructure Series** gateway you will require the following information:

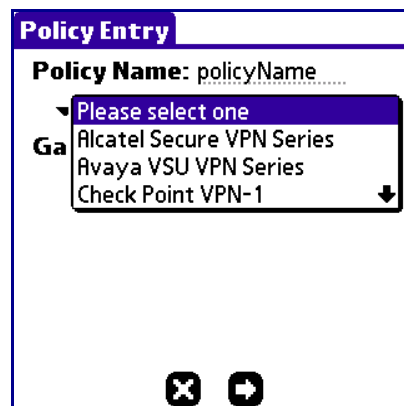
- Gateway IP address
- Checkbox status for Split Tunneling, Perfect Forward Secrecy, and Extended Authentication
- A combination of group name, group password, user name and user password, depending on the authentication selected
- IKE Suite, DNS, and IPSec Suite settings
- SA life setting

To create a policy for an **Intel Netstructure Series** gateway:

- 1a. (Standard Palm Device) Open the **movianVPN** application, and tap **New** to open the **Policy Entry** window.
- 1b. (Tungsten-C, Tungsten-T3) Select **VPN** from the Preferences window, ensure that VPN is set to enabled, and tap the "Tap to Add" button. On the **New VPN Account** screen, select **movianVPN** as the type, and tap **Next** to continue to the **Policy Entry** window.
2. Enter a name for the policy in the **Policy Name** field.



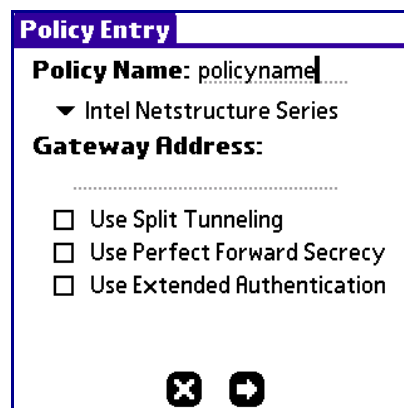
- Open the list of gateways by tapping the "Please select one" arrow. Select **Intel Netstructure Series** from the list. Checkboxes for gateway policy options appear.



- Enter the IP address for your gateway in the **Gateway Address** field.

Note: If you were provided values for these fields by an administrator, please use them.

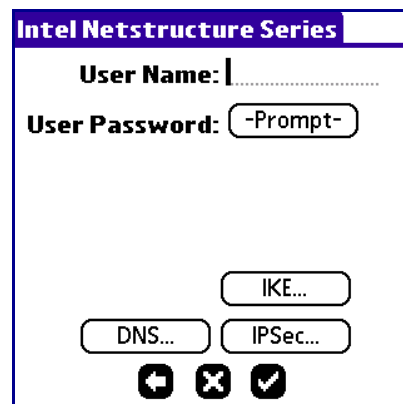
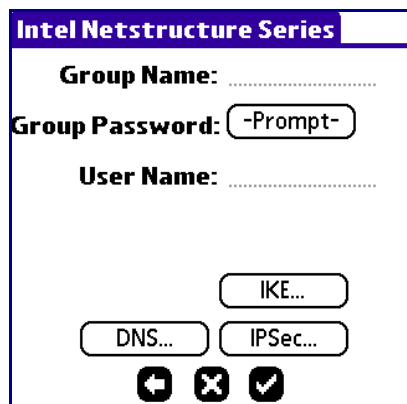
- Select **Use Split Tunneling** if you wish to enable split tunneling. (For more information, see "Split Tunneling" on page 31.)
- Select **Use Perfect Forward Secrecy** if you wish to enable perfect forward secrecy. (For more information, see "Perfect Forward Secrecy" on page 32.)
- Select **Use Extended Authentication** if you wish to use extended authentication. (For more information, see "Extended Authentication" on page 32.)



Note: When you connect to the gateway you will be asked for further authentication.

- Tap the arrow button to continue to the **Intel Netstructure Series** screen.

Note: If you have selected Extended Authentication you will be asked for a Group Name and Password as well as the User Name (you supply the password when logging in). If you have not selected Extended Authentication, you will be asked for User Name and User Password.



- Enter your group name and user name in the **Group Name** and **User Name** fields.

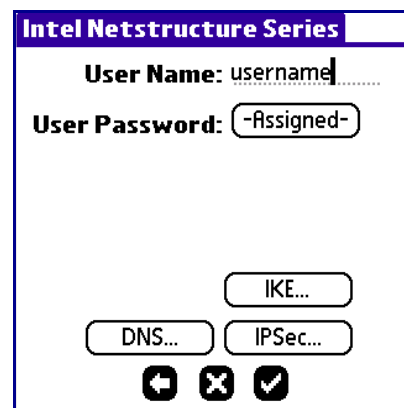
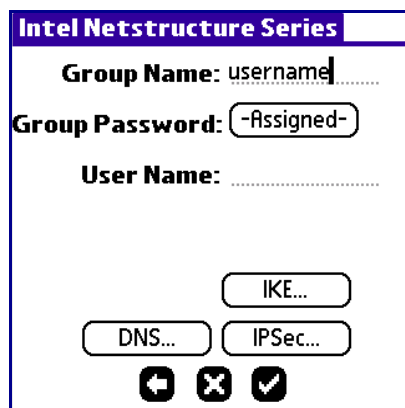
– OR –

Enter your user name in the **User Name** field.

- If you wish to save your password as part of your policy, tap **Prompt** at the password field, which opens the **User Password** window. Please skip the following step if you do not wish to save your password.

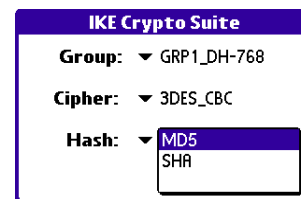
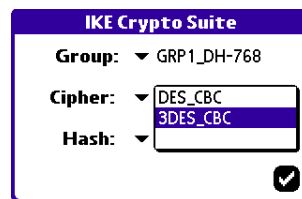
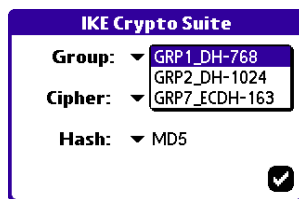


- Enter your password and tap **OK**. In the **Intel Netstructure Series** window, the appropriate password field now appears as **Assigned**. To delete or edit the password, tap **Assigned**, then leave the field blank to delete the password, or enter a new password, and tap **OK** to save your changes.



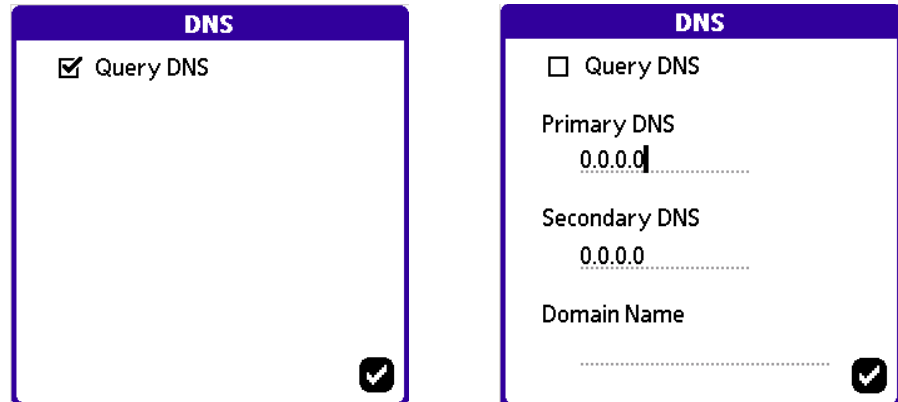
Note: If you do not store your password, you will be asked for it when you log into the gateway.

- Tap the "IKE..." button to open the **IKE Crypto Suite** window. (For more information, see "IKE Crypto Suite" on page 36.)
- Set your crypto suite settings by selecting your desired values from each of the pull-down lists for the **Group**, **Cipher**, and **Hash** fields.



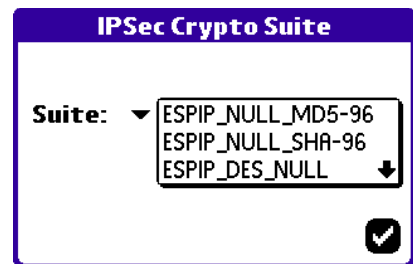
- Tap the checkmark button to return to the **Intel Netstructure Series** window.
- Tap the "DNS..." button to open the **DNS** window. If **Query DNS** is deselected, further fields appear. (For more information, see "DNS" on page 35.).

- If instructed to, deselect the **Query DNS** box and enter the primary and secondary DNS addresses and domain name into the appropriate fields.



- Tap the checkmark button to return to the **Intel Netstructure Series** window.

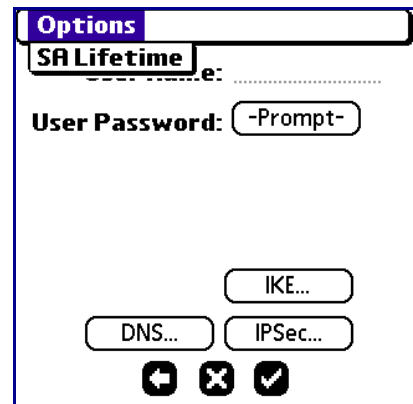
- Tap the "IPSec..." button to open the **IPSec Crypto Suite** window. (For more information, see "IPSec Crypto Suite" on page 37.)



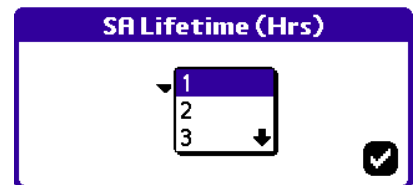
- Set the value of the **Suite** field by selecting one of the crypto suite options from the list.

- Tap the checkmark button to return to the **Intel Netstructure Series** window.

- Tap the **movianVPN** tab at the top of the window. The **Options** menu appears. Select **SA Lifetime** from the menu.



- Set the **SA Lifetime** by selecting a value from the list. For more information, see "SA Life" on page 37.



- Tap the checkmark button to return to the **Intel Netstructure Series** window.

- (Standard Palm Devices) Tap **Done**. The **movianVPN** application window appears. Tap the **Login** button to connect to the gateway.

- (Tungsten-C, Tungsten-T3 Devices) Tap the checkmark to return to the Preferences window. Tap **Done** to begin using your device with the new settings.

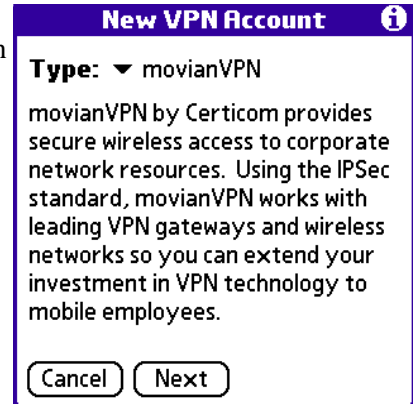
Creating a policy for a Lucent Brick Firewall VPN gateway

To create a policy for a **Lucent Brick Firewall VPN** gateway you will require the following information:

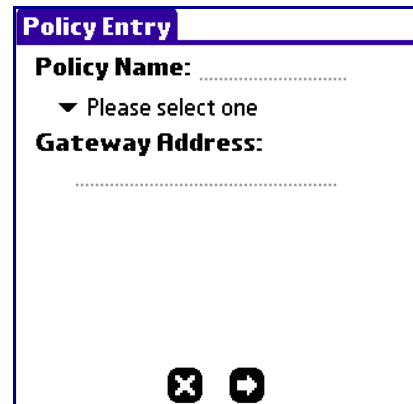
- Gateway IP address
- Checkbox status for Split Tunneling and Perfect Forward Secrecy
- Group name, group password, user name and user password
- Network, IKE Suite, DNS and IPSec Suite settings
- SA life setting

To create a policy for a **Lucent Brick Firewall VPN** gateway:

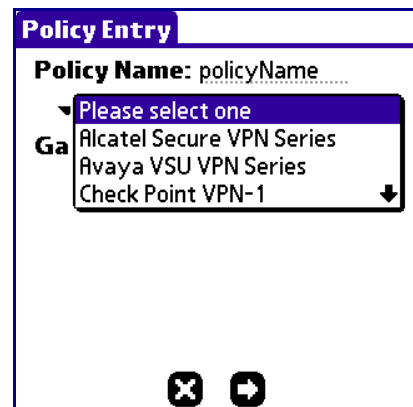
- 1a. (Standard Palm Device) Open the **movianVPN** application, and tap **New** to open the **Policy Entry** window.
- 1b. (Tungsten-C, Tungsten-T3) Select **VPN** from the Preferences window, ensure that VPN is set to enabled, and tap the "Tap to Add" button. On the **New VPN Account** screen, select **movianVPN** as the type, and tap **Next** to continue to the **Policy Entry** window.



2. Enter a name for the policy in the **Policy Name** field.



3. Open the list of gateways by tapping the "Please select one" arrow.



4. Select **Lucent Brick Firewall VPN** from the list. The **Gateway Address** field and the gateway policy security option checkboxes appear.

5. Enter the network address for your gateway into the **Gateway Address** field.

Note: If you were provided with values for these fields by an administrator, please use them.

6. Select **Use Split Tunneling** if the option is desired. (For information, see “Split Tunneling” on page 31).

7. Select **Use Perfect Forward Secrecy** if the option is desired. (For information, see “Perfect Forward Secrecy” on page 32.)

Note: Use Extended Authentication is selected by default and locked as required by the Lucent Brick Firewall VPN gateways. When you connect to the gateway, you will be asked for further authentication. For information on Extended Authentication, see “Extended Authentication” on page 32.

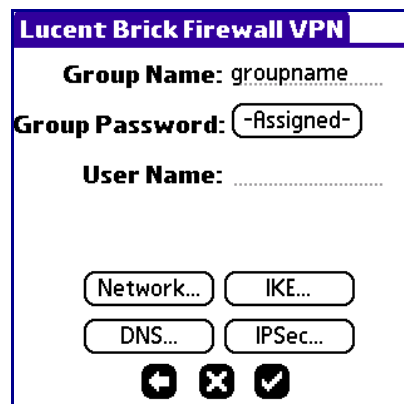
8. Tap the arrow icon to return to the **Lucent Brick Firewall VPN** window.

9. Enter your group name and user name into the **Group Name** and **User Name** fields.

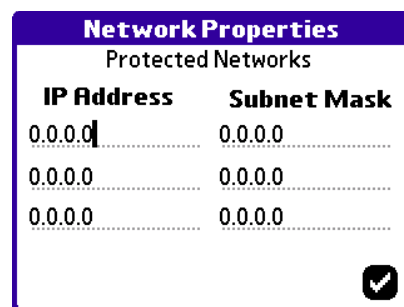
10. If instructed to save your group password, tap **Prompt** at the **Group Password** field. The **User password** window appears. Otherwise, please skip the following step.

- In the **Lucent Brick Firewall VPN** window, the **Group Password** field now contains the value "Assigned". To delete or edit the password, tap **Assigned**, either leave the field blank to delete or enter a new password, and tap **OK** to return to the **Lucent Brick Firewall VPN** window.

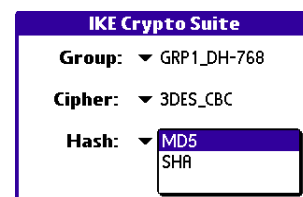
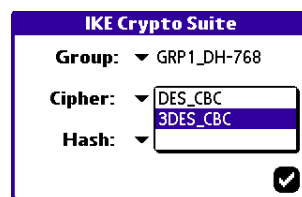
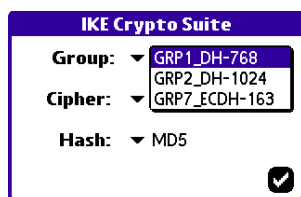
Note: You will be asked for the User Password for extended authentication when you log in to the gateway.



- Tap the "Network" button in the **Lucent Brick Firewall VPN** window. The **Network Properties** window appears. (For more information, see "Network Properties" on page 37.)

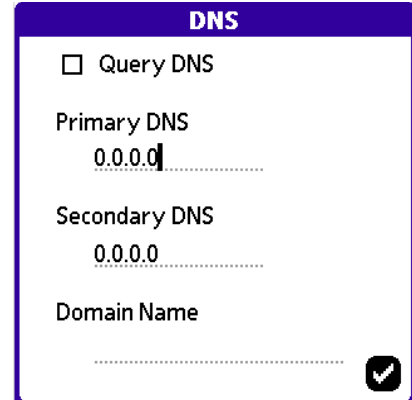
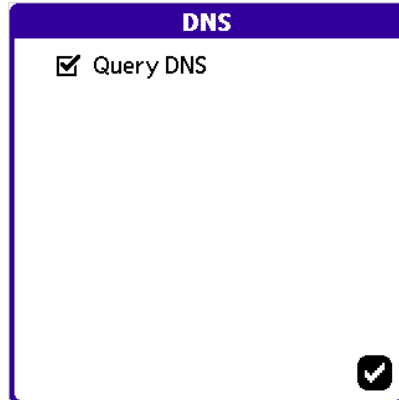


- Enter the IP addresses and subnet masks for the primary and secondary subnets.
- Tap the checkmark button to return to the **Lucent Brick Firewall VPN** window.
- Tap the "IKE..." button to open the **IKE Crypto Suite** window. (For more information, see "IKE Crypto Suite" on page 36.)
- Set your crypto suite settings by selecting your desired values from each of the pull-down lists for the **Group**, **Cipher**, and **Hash** fields.



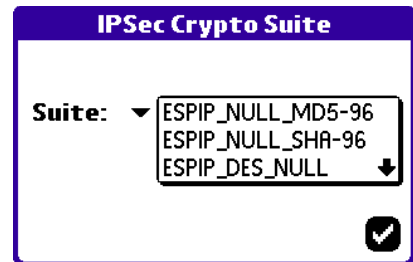
- Tap the checkmark button to return to the **Lucent Brick Firewall VPN** window.
- Tap the "DNS..." button to open the **DNS** window. If **Query DNS** is deselected, further fields appear. (For more information, see "DNS" on page 35).

19. If directed to do so, deselect **Query DNS** and enter primary and secondary DNS addresses and your gateway's domain name in the fields that appear.



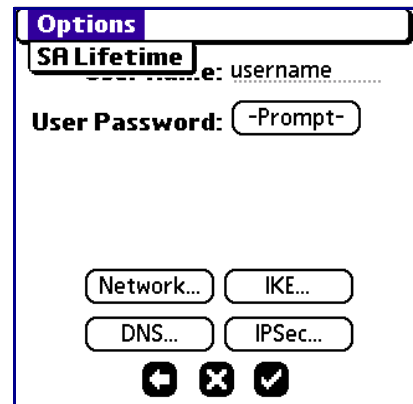
20. Tap the checkmark button to return to the **Lucent Brick Firewall VPN** window.

21. Tap the "IPSec..." button to open the **IPSec Crypto Suite** window. (For more information, see "IPSec Crypto Suite" on page 37.)

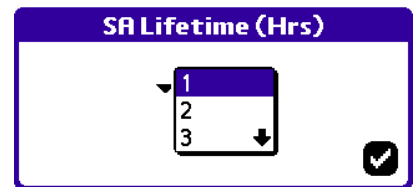


22. Set the value of the **Suite** field by selecting one of the crypto suite options from the list.
23. Tap the checkmark button to return to the **Lucent Brick Firewall VPN** window.

24. Tap the **movianVPN** tab at the top of the window. The **Options** menu appears. Select **SA Lifetime** to set the SA lifetime time-out value.



25. Set the **SA Lifetime** by selecting a value from the list. (For more information, see "SA Life" on page 37.)



26. Tap the checkmark button to return to the **Lucent Brick Firewall VPN** window.

- 27a. (Standard Palm Devices) Tap **Done**. The **movianVPN** application window appears. Tap the **Login** button to connect to the gateway.

28. (Tungsten-C, Tungsten-T3 Devices) Tap the checkmark to return to the Preferences window. Tap **Done** to begin using your device with the new settings.

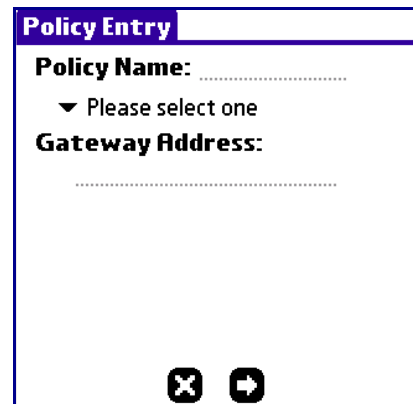
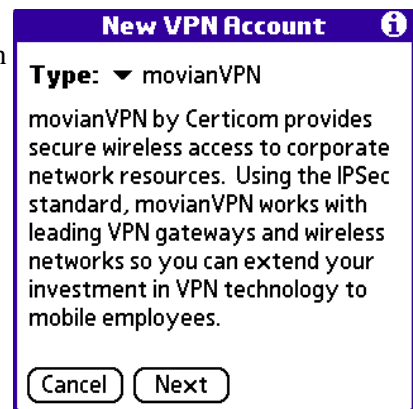
Creating a policy for a Netscreen Series gateway

To create a policy for a **Netscreen Series** gateway you will require the following information:

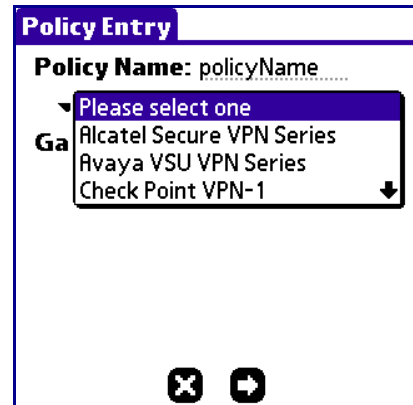
- Gateway IP address
- Whether any/both of Split Tunneling and Perfect Forward Secrecy should be enabled.
- Whether Extended Authentication should be enabled (Netscreen Series v3.0 and up)
- A combination of User name, user password, group name, and group password, depending upon whether extended authentication is enabled
- Network, IKE Suite, DNS and IPSec Suite settings
- SA life setting

To create a policy for a **Netscreen Series** gateway:

- 1a. (Standard Palm Device) Open the **movianVPN** application, and tap **New** to open the **Policy Entry** window.
- 1b. (Tungsten-C, Tungsten-T3) Select **VPN** from the Preferences window, ensure that VPN is set to enabled, and tap the "Tap to Add" button. On the **New VPN Account** screen, select **movianVPN** as the type, and tap **Next** to continue to the **Policy Entry** window.
2. Enter a name for the policy in the **Policy Name** field.



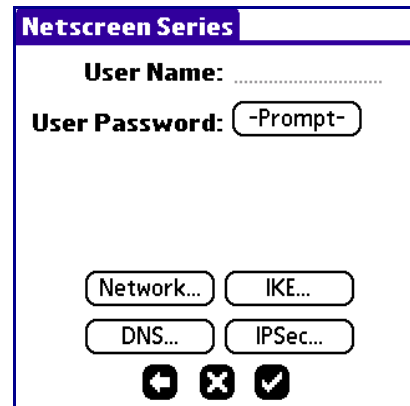
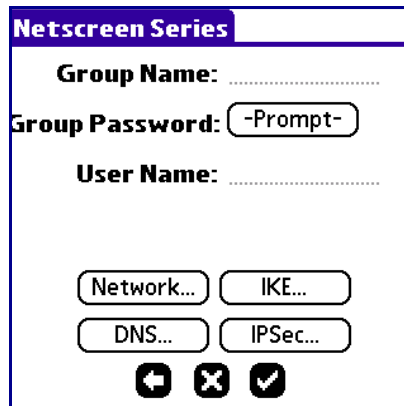
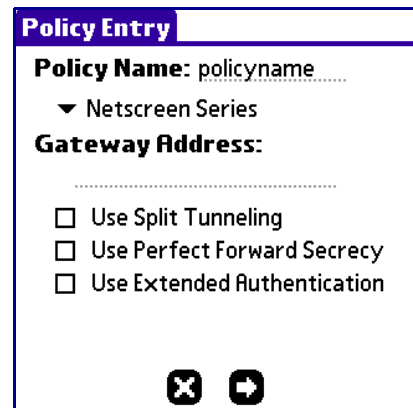
- Open the list of gateways by tapping the "Please select one" arrow. Select **Netscreen Series** from the list. Checkboxes for policy options appear.



- Enter the network address of your gateway in the **Gateway Address** field.

Note: If you were provided with values for these fields by an administrator, please use them.

- Select **Use Split Tunneling** if you wish to enable split tunneling. (For more information, see "Split Tunneling" on page 31.)
- Select **Use Perfect Forward Secrecy** if you wish to enable perfect forward secrecy. (For more information, see "Perfect Forward Secrecy" on page 32.)
- Select **Use Extended Authentication** if you wish to enable extended authentication. (For more information, see "Extended Authentication" on page 32.)
- Tap the arrow button to return to the **Netscreen Series** window.
- If extended authentication is enabled, enter your group name and user name in the **Group Name** and **User Name** fields.
– OR –
If extended authentication is disabled, enter your user name.

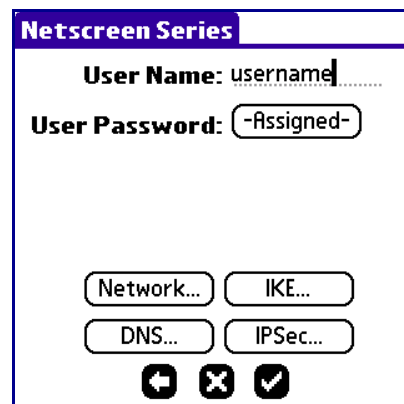
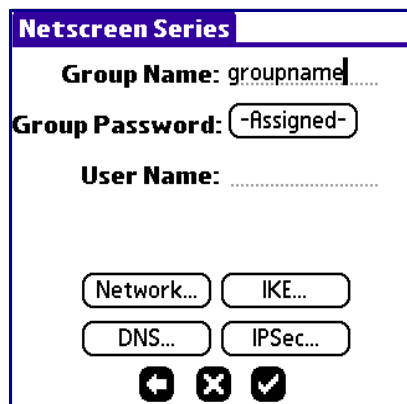


- If you have been instructed to save your password, tap **Prompt** in the **Group Password** or **User Password** field (whichever appears in the **Alcatel Secure VPN Series** window). The **User password** window appears. Otherwise, please skip the following step if you do not wish to store your password.

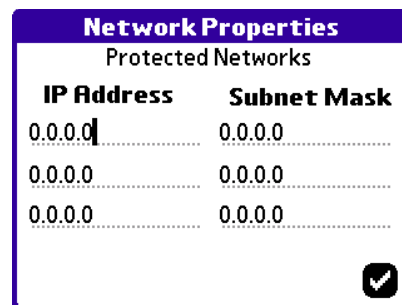


- Enter your password and tap **OK** to store it, or **Cancel** if you wish to exit without saving your password. If you save your password, either the **User Password** or **Group Password** (if extended authentication is enabled) field in the **Netscreen Series** window contains the value "**Assigned**". To delete or edit the password, tap "**Assigned**", then leave the field blank to delete the password, or enter a new password. Tap **OK** to save your changes.

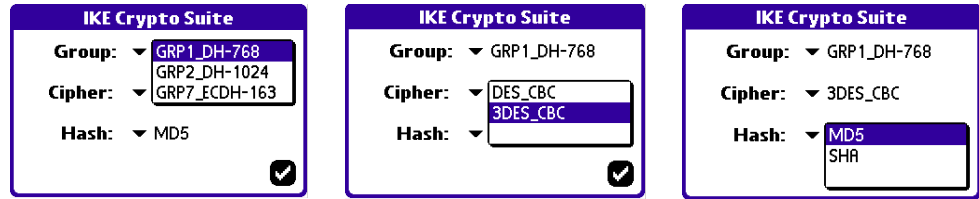
Note: If you do not save your password in your policy, you will be asked for it when you log in to the gateway.



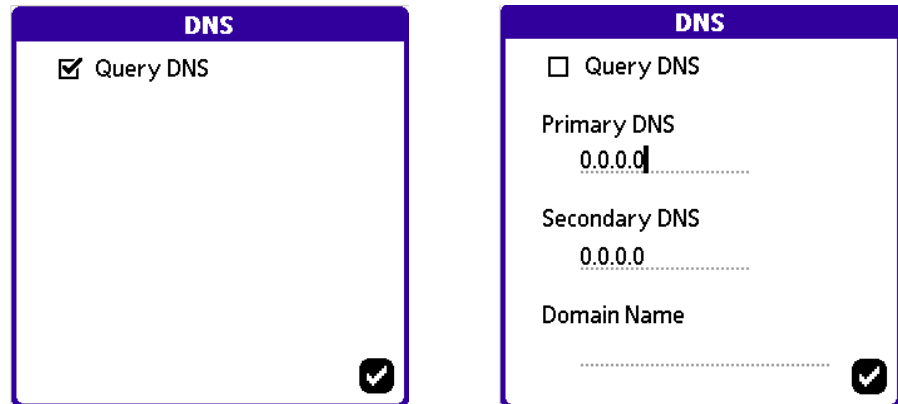
- Tap the "**Network**" button to open the **Network Properties** window. (For more information, see "Network Properties" on page 37.)
- Enter the IP addresses and subnet masks for the primary and secondary subnets.
- Tap the checkmark button to return to the **Netscreen Series** window.
- Tap the "**IKE...**" button to open the **IKE Crypto Suite** window. (For more information, see "IKE Crypto Suite" on page 36.)



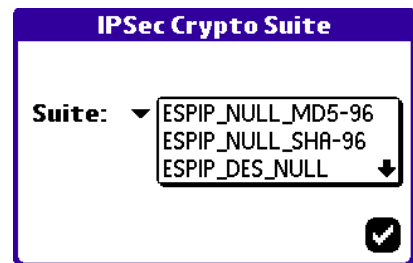
- Set your crypto suite settings by selecting your desired values from each of the pull-down lists for the **Group**, **Cipher**, and **Hash** fields.



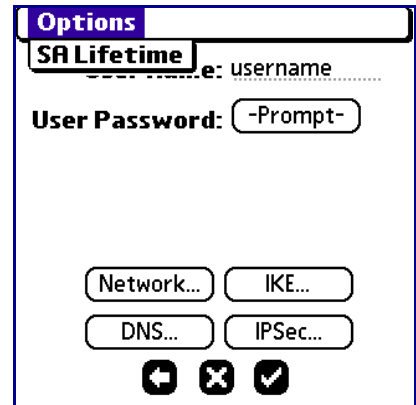
- Tap the checkmark button to return to the **Netscreen Series** window.
- Tap the "DNS..." button to open the **DNS** window. If **Query DNS** is deselected, further fields appear. (For more information, see "DNS" on page 35.).
- If you were directed to do so, deselect **Query DNS** and enter the primary and secondary DNS addresses and your domain name in the appropriate fields.



- Tap the checkmark button to return to the **Netscreen Series** window.
- Tap the "IPSec..." button to open the **IPSec Crypto Suite** window. (For more information, see "IPSec Crypto Suite" on page 37.)
- Set the value of the **Suite** field by selecting one of the crypto suite options from the list.
- Tap the checkmark button to return to the **Netscreen Series** window.

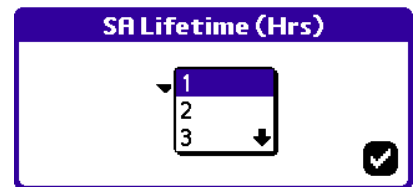


24. Tap the **movianVPN** tab at the top of the window. The **Options** menu appears. Select **SA Lifetime** to set the SA lifetime time-out value.



25. Set the **SA Lifetime** by selecting a value from the list. (For more information, see “SA Life” on page 37.)

26. Tap the checkmark button to return to the **Netscreen Series** window.



- 27a. (Standard Palm Devices) Tap **Done**. The **movianVPN** application window appears. Tap the **Login** button to connect to the gateway.

28. (Tungsten-C, Tungsten-T3 Devices) Tap the checkmark to return to the Preferences window. Tap **Done** to begin using your device with the new settings.

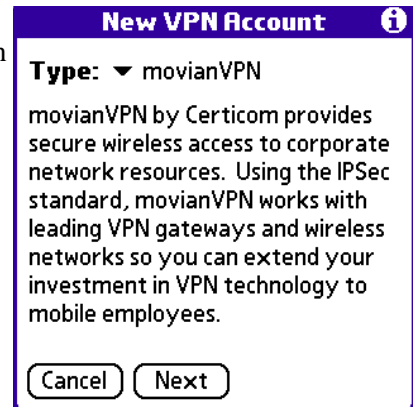
Creating a policy for a Nortel Contivity Series gateway

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

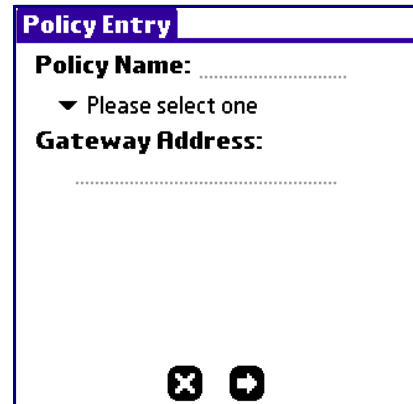
- Gateway IP address
- Checkbox status for Perfect Forward Secrecy
- Checkbox status and selected form of Extended Authentication
- A combination of group name, group password, user name and user password, depending on the authentication selected
- IKE Suite, DNS, and IPSec Suite settings
- SA life setting

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

- 1a. (Standard Palm Device) Open the **movianVPN** application, and tap **New** to open the **Policy Entry** window.
- 1b. (Tungsten-C, Tungsten-T3) Select **VPN** from the Preferences window, ensure that VPN is set to enabled, and tap the "Tap to Add" button. On the **New VPN Account** screen, select **movianVPN** as the type, and tap **Next** to continue to the **Policy Entry** window.



2. Enter a name for the policy in the **Policy Name** field.



- Open the list of gateways by tapping "**Please select one**". Select **Nortel Contivity Series** from the list. Checkboxes for gateway policy options appear in the **Policy Entry** window.

The screenshot shows the 'Policy Entry' window. At the top, there is a header 'Policy Entry'. Below it, the 'Policy Name' field is filled with 'policyName'. A dropdown menu is open, showing the text 'Please select one' and three options: 'Alcatel Secure VPN Series', 'Avaya VSU VPN Series', and 'Check Point VPN-1'. The 'Ga' label is partially visible on the left. At the bottom, there are two icons: a close button (X) and a back button (arrow).

- Enter the IP address of your gateway in the **Gateway Address** field.

Note: If values for these fields were provided to you by an administrator, please use them.

- Select **Use Perfect Forward Secrecy** if you wish to use this option. (For more information, see "Perfect Forward Secrecy" on page 32.)

The screenshot shows the 'Policy Entry' window. The 'Policy Name' field is filled with 'policyname'. The dropdown menu is now closed and shows 'Nortel Contivity Series'. The 'Gateway Address' field is filled with '38.28.28.23'. Below this, there are two checkboxes: 'Use Perfect Forward Secrecy' (unchecked) and 'Use Extended Authentication' (unchecked). At the bottom, there are two icons: a close button (X) and a back button (arrow).

- Select **Use Extended Authentication** if the option is desired. If selected, the **Authentication Type** field appears. You need to select one of the authentication types from the list, which is opened by tapping "**Please select one**".

Note: When you log in to the gateway, you will be asked to enter the selected form of extended authentication. For further information, see "Extended Authentication" on page 32.

- Tap the arrow button to return to the **Nortel Contivity Series** window appears.

The screenshot shows the 'Policy Entry' window. The 'Policy Name' field is filled with 'policyname'. The dropdown menu is closed and shows 'Nortel Contivity Series'. The 'Gateway Address' field is filled with '38.28.28.23'. Below this, there are two checkboxes: 'Use Perfect Forward Secrecy' (unchecked) and 'Use Extended Authentication' (checked). Below the checkboxes is the 'Authentication Type' label and a dropdown menu that is open, showing 'Please select one', 'Username and Password', and 'SecureID'. At the bottom, there are two icons: a close button (X) and a back button (arrow).

Note: If you have selected Extended Authentication you will be asked for a Group Name and Password as well as the User Name (you supply the password when logging in). If you have not selected Extended Authentication, you will be asked for User Name and User Password.

- Enter the your group name and user name in the **Group Name** and **User Name** fields.

– OR –

Enter your user name in the **User Name** field.

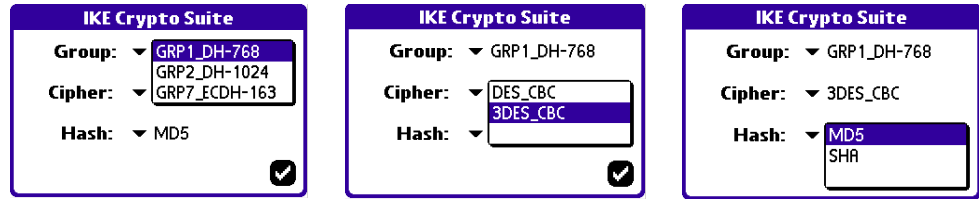
9. If you were instructed to store your password, tap **Prompt** at whichever of the group or user password fields appears – this opens the **User password** window. If you do not wish to store your password, please skip the following step.

10. Enter your password and tap **OK**. In the **Nortel Contivity Series** window, either the **Group Password** or the **User Password** now appears with the value "**Assigned**". To delete or change the password, tap **Assigned**, and then leave the field blank to delete the password, or enter a new password. Tap **OK** to save your changes.

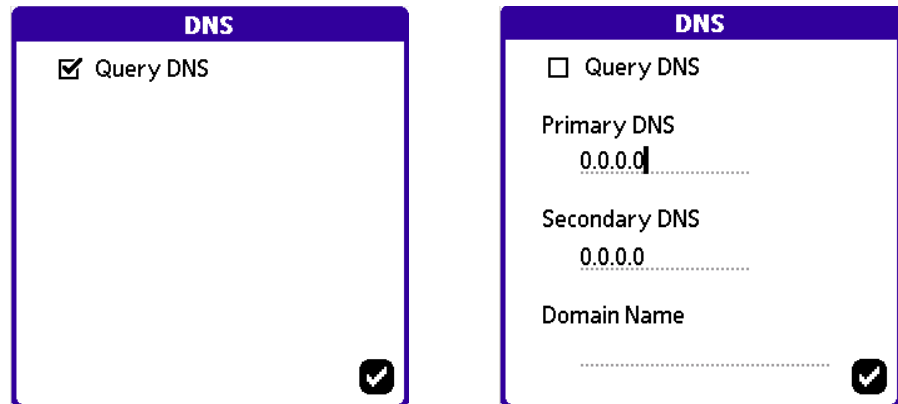
***Note:** If you do not enter the password at this time, you will be asked for it when you log in to the gateway. If Extended Authentication has been selected, you will be asked for your user passcode or your user password upon login (depending on the type of extended authentication being used).*

11. Tap the "**IKE...**" button to open the **IKE Crypto Suite** window. (For more information, see "IKE Crypto Suite" on page 36.).

- Set your crypto suite settings by selecting your desired values from each of the pull-down lists for the **Group**, **Cipher**, and **Hash** fields.



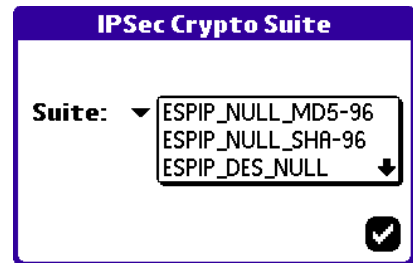
- Tap the checkmark button to close the **IKE Crypto Suite** window.
- Tap the "DNS..." button to open the **DNS** window. If **Query DNS** is deselected, further fields appear. (For more information, see "DNS" on page 35.).



- If you have been instructed to do so, deselect **Query DNS**. Enter the primary and secondary DNS addresses in the **Primary DNS** and **Secondary DNS** fields. Enter the domain name in the **Domain Name** field.

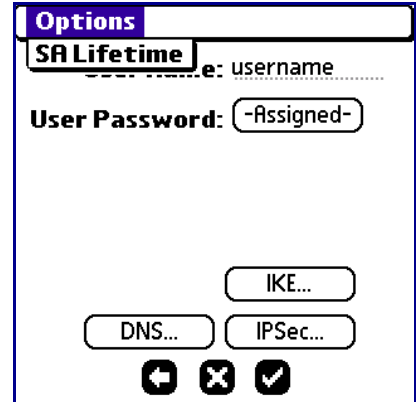
- Tap the checkmark button to return to the **Nortel Contivity Series** window.

- Tap the "IPSec Suite" button to open the **IPSec Crypto Suite** window. (For more information, see "IPSec Crypto Suite" on page 37.)

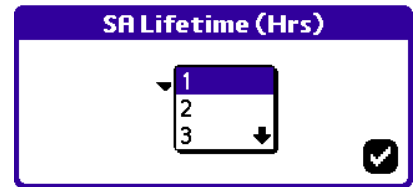


- Set the value of the **Suite** field by selecting one of the crypto suite options from the list.
- Close the **IPSec Suite** window by tapping the checkmark button.

20. Tap the **movianVPN** tab at the top of the window. The Options menu appears.
21. Select **SA Lifetime** from the **Options** menu.



22. Set the **SA Lifetime** by selecting a value from the list. For more information, see “SA Life” on page 37.
23. Close the window by tapping the checkmark button. The **Nortel Contivity Series** window appears.



- 24a. (Standard Palm Devices) Tap **Done**. The **movianVPN** application window appears. Tap the **Login** button to connect to the gateway.
25. (Tungsten-C, Tungsten-T3 Devices) Tap the checkmark to return to the Preferences window. Tap **Done** to begin using your device with the new settings.

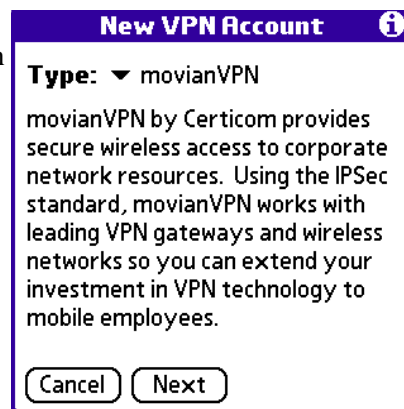
Creating a policy for a ReefEdge Connect Server gateway

To create a policy for a **ReefEdge Connect Server** gateway you will require the following information:

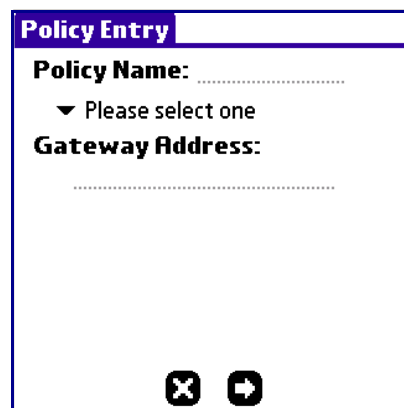
- Gateway IP address
- User password
- IKE Suite, DNS, and IPSec Suite settings
- SA life setting

To create a policy for a **ReefEdge Connect Server** gateway:

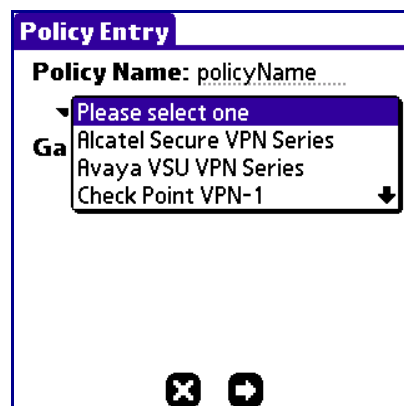
- 1a. (Standard Palm Device) Open the **movianVPN** application, and tap **New** to open the **Policy Entry** window.
- 1b. (Tungsten-C, Tungsten-T3) Select **VPN** from the Preferences window, ensure that VPN is set to enabled, and tap the "Tap to Add" button. On the **New VPN Account** screen, select **movianVPN** as the type, and tap **Next** to continue to the **Policy Entry** window.



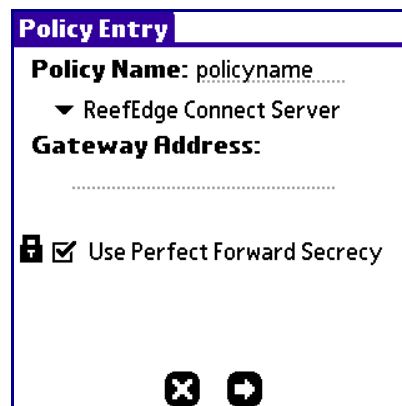
2. Enter a name for the policy in the **Policy Name** field.



3. Open the list of gateways by tapping the "Please select one" arrow.



4. Select **ReefEdge Connect Server** from the list. The **Gateway Address** field and the gateway policy security option checkboxes appear.



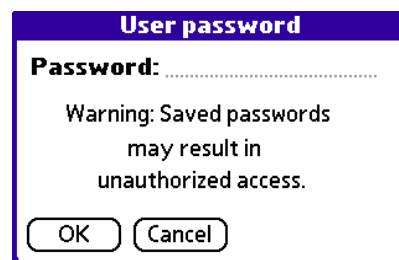
5. Enter the network address for your gateway in the **Gateway Address** field.

Note: If you have been given instructions on how to fill in these fields, please follow them.

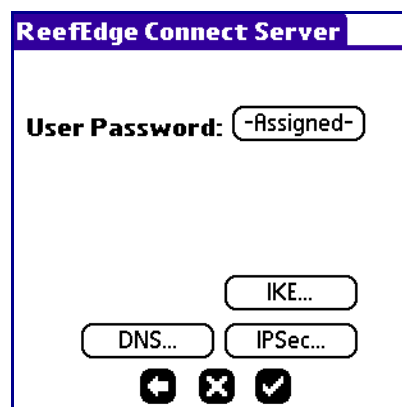
6. **Use Perfect Forward Secrecy** is enabled and locked, as the ReefEdge gateway requires it to be enabled. (For more information, see “Extended Authentication” on page 32.)

7. Tap the arrow button to open the **ReefEdge Connect Server** window.

8. If you wish to store your user password, tap **Prompt** in the **User Password** field. This opens the **User password** window. If you do not wish to store your password, please skip the following step.



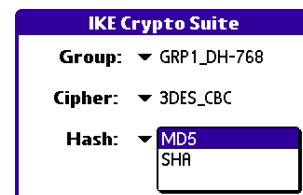
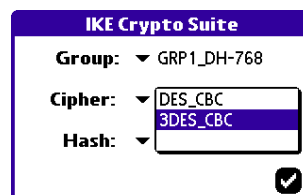
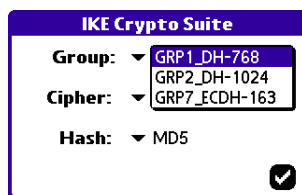
9. In the **ReefEdge Connect Server** window, the **User Password** field now contains the value "Assigned". To delete or edit the password, tap **Assigned**, either leave the field blank to delete or enter a new password, and tap **OK** to return to the **ReefEdge Connect Server** window.



Note: If you do not save your password in your policy, you will be asked for it when you log in to the gateway.

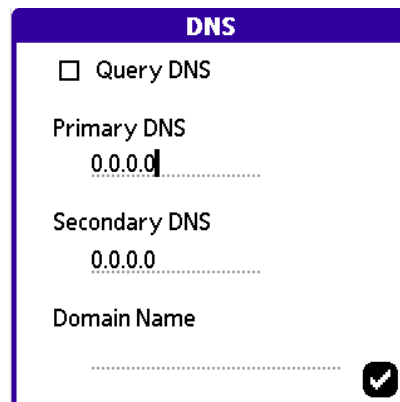
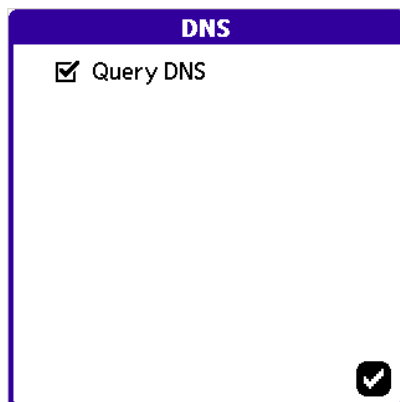
10. Tap the "IKE..." button to open the **IKE Crypto Suite** window. (For more information, see “IKE Crypto Suite” on page 36.)

11. Set your crypto suite settings by selecting your desired values from each of the pull-down lists for the **Group**, **Cipher**, and **Hash** fields.



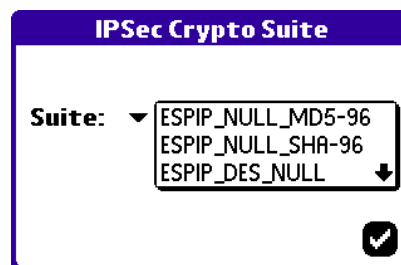
12. Tap the checkmark button to return to the **ReefEdge Connect Server** window.

13. Tap the "DNS..." button to open the **DNS** window. If **Query DNS** is deselected, further fields will appear. (For more information, see "DNS" on page 35.)



14. If directed to do so, deselect **Query DNS** and enter the primary and secondary DNS addresses and the gateway domain name in the appropriate fields.
15. Tap the checkmark button to return to the **ReefEdge Connect Server** window.

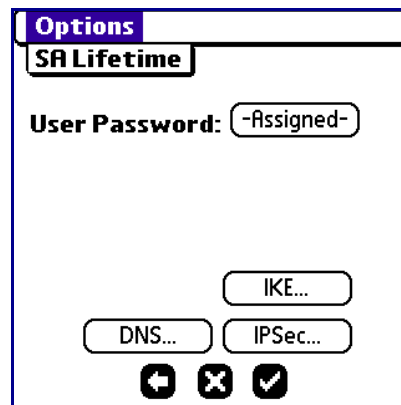
16. Tap the "IPSec..." button to open the **IPSec Crypto Suite** window. (For more information, see "IPSec Crypto Suite" on page 37.)



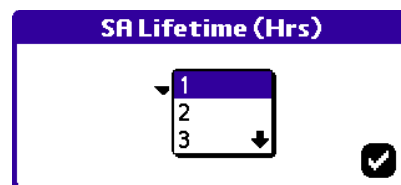
17. Open the list of available crypto suites by clicking the arrow beside the **Suite** field. Select your desired crypto suite from the list.

18. Tap the checkmark button to return to the **ReefEdge Connect Server** window.

19. Open the **movianVPN tab** at the top of the window. The **Options** menu appears. Select **SA Lifetime** from the menu to set the SA lifetime value.



20. Set the **SA Lifetime** value by selecting a value from the list. (For more information, see "SA Life" on page 37.)



21. Tap the checkmark button to return to the **ReefEdge Connect Server** window.

- 22a. (Standard Palm Devices) Tap **Done**. The **movianVPN** application window appears. Tap the **Login** button to connect to the gateway.

23. (Tungsten-C, Tungsten-T3 Devices) Tap the checkmark to return to the Preferences window. Tap **Done** to begin using your device with the new settings.

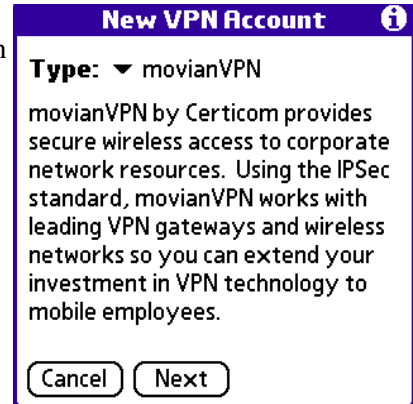
Creating a policy for a Secure Computing Sidewinder gateway

To create a policy for a **Secure Computing Sidewinder** gateway you will require the following information:

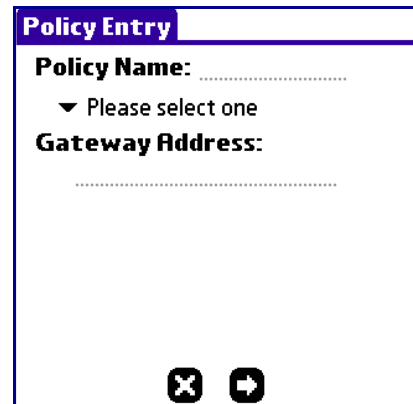
- Gateway IP address
- Checkbox status for Split Tunneling and Perfect Forward Secrecy
- Group name, group password, user name, and user password
- Network, IKE Suite, DNS, and IPSec Suite settings
- SA life setting

To create a policy for a **Secure Computing Sidewinder** gateway:

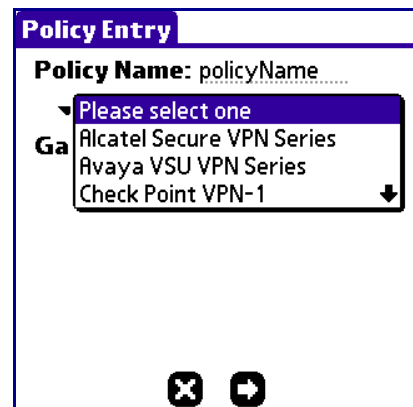
- 1a. (Standard Palm Device) Open the **movianVPN** application, and tap **New** to open the **Policy Entry** window.
- 1b. (Tungsten-C, Tungsten-T3) Select **VPN** from the Preferences window, ensure that VPN is set to enabled, and tap the "Tap to Add" button. On the **New VPN Account** screen, select **movianVPN** as the type, and tap **Next** to continue to the **Policy Entry** window.



2. Enter a name for the policy in the **Policy Name** field.



3. Open the list of gateways by tapping the "Please select one" arrow.



4. Select **Secure Computing Sidewinder** from the list. The **Gateway Address** field and the gateway policy security option checkboxes appear.

5. Enter the network address of your gateway in the **Gateway Address** field.

Note: If you have been given instructions for how to fill in these fields by an administrator, follow them.

6. Select **Use Split Tunneling** if you wish to enable split tunneling. (For more information, see “Split Tunneling” on page 31.)

7. Select **Use Perfect Forward Secrecy** if the option is desired. (For more information, see “Perfect Forward Secrecy” on page 32.)

Note: Use Extended Authentication is selected by default and locked as required by the Secure Computing Sidewinder gateways. When you connect to the gateway, you will be asked for further authentication. For more information, see “Extended Authentication” on page 32.

8. Tap the arrow icon to return to the **Secure Computing Sidewinder** window.

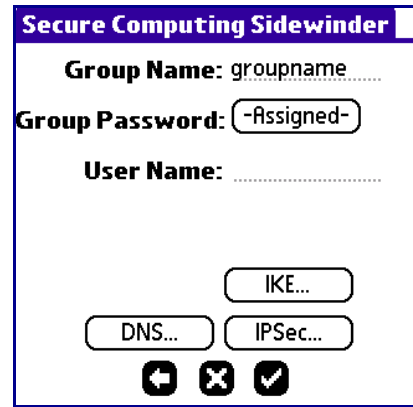
9. Enter your group and user names into the **Group Name** and **User Name** fields.

10. If you wish to store your user password, tap **Prompt** in the **Group Password** field. This opens the **User password** window. If you do not wish to store your password, please skip the following step.

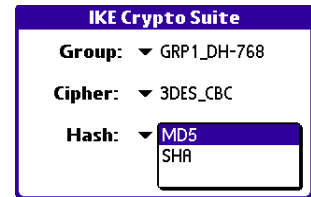
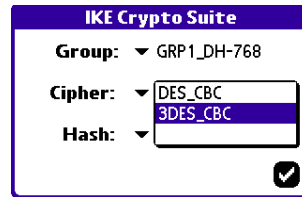
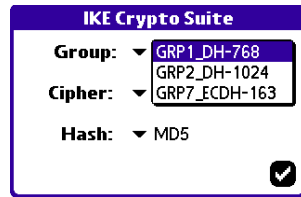
- In the **Secure Computing Sidewinder** window, the **Group Password** field now contains the value "Assigned". To delete or edit the password, tap **Assigned**, either leave the field blank to delete or enter a new password, and tap **OK** to return to the **Secure Computing Sidewinder** window.

Note: You will be asked for the User Password when you log in to the gateway.

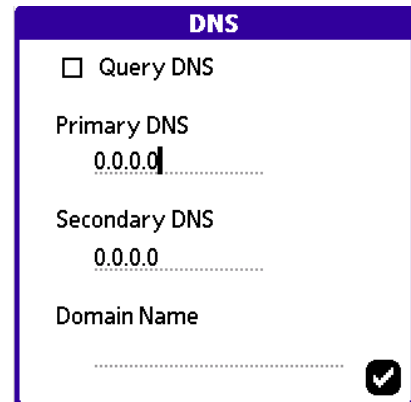
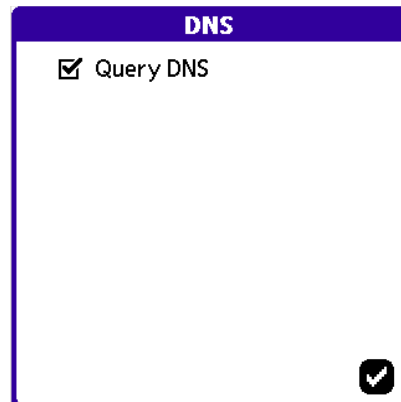
- Tap the "IKE..." button to open the **IKE Crypto Suite** window. (For more information, see "IKE Crypto Suite" on page 36.)



- Set your crypto suite settings by selecting your desired values from each of the pull-down lists for the **Group**, **Cipher**, and **Hash** fields.



- Tap the checkmark button to return to the **Secure Computing Sidewinder** window.
- Tap the "DNS..." button to open the **DNS** window. If "Query DNS" is not selected, further fields appear. (For more information, see "DNS" on page 35.).

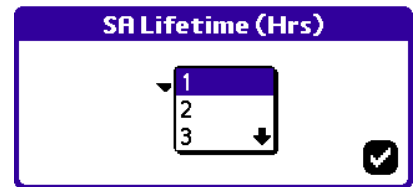
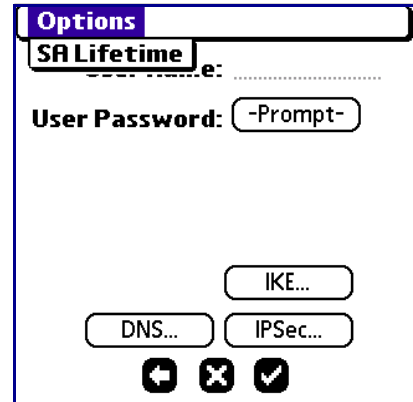


- If directed to do so, deselect **Query DNS** and enter the primary and secondary DNS addresses in the **Primary DNS** and **Secondary DNS** fields, and the domain name in the **Domain Name** field.
- Tap the checkmark button to return to the **Secure Computing Sidewinder** window.

18. Tap the "IPSec..." button to open the **IPSec Crypto Suite** window. (For more information, see "IPSec Crypto Suite" on page 37.)
19. Open the list of available crypto suites by clicking the arrow beside the **Suite** field. Select your desired crypto suite from the list.
20. Tap the checkmark button to return to the **Secure Computing Sidewinder** window.
21. Tap the **movianVPN** tab at the top of the window to reveal the **Options** menu. Select **SA Lifetime** from the menu to set the SA lifetime value.



22. Set the **SA Lifetime** by selecting a value from the list. For more information, see "SA Life" on page 37.
23. Tap the checkmark button to return to the **Secure Computing Sidewinder** window.
- 24a. (Standard Palm Devices) Tap **Done**. The **movianVPN** application window appears. Tap the **Login** button to connect to the gateway.
25. (Tungsten-C, Tungsten-T3 Devices) Tap the checkmark to return to the Preferences window. Tap **Done** to begin using your device with the new settings.



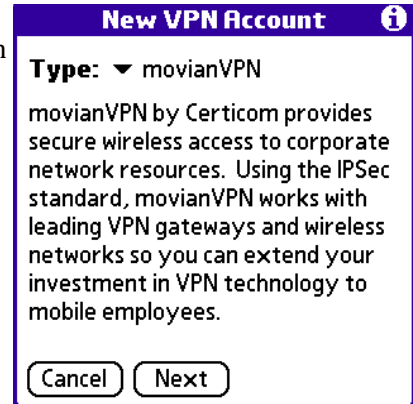
Creating a policy for a Symantec Power VPN gateway

To create a policy for a **Symantec Power VPN** gateway you will require the following information:

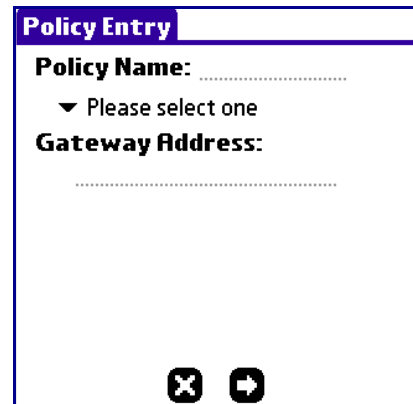
- Gateway IP address
- Checkbox status for Split Tunneling and Perfect Forward Secrecy
- User name and user password
- Network, IKE Suite, DNS, and IPSec Suite settings
- SA life setting

To create a policy for a **Symantec Power VPN** gateway:

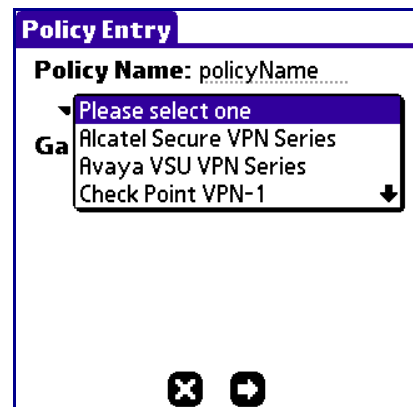
- 1a. (Standard Palm Device) Open the **movianVPN** application, and tap **New** to open the **Policy Entry** window.
- 1b. (Tungsten-C, Tungsten-T3) Select **VPN** from the Preferences window, ensure that VPN is set to enabled, and tap the "Tap to Add" button. On the **New VPN Account** screen, select **movianVPN** as the type, and tap **Next** to continue to the **Policy Entry** window.



2. Enter a name for the policy in the **Policy Name** field.



3. Open the list of gateways by tapping the "Please select one" arrow. Select **Symantec Power VPN** from the list. Checkboxes for gateway policy options appear.



4. Enter the network address for your gateway in the **Gateway Address** field.

Note: If you were provided with values for these fields by an administrator, please use them.

5. Select **Use Split Tunneling** if you wish to enable this option. (For more information, see “Split Tunneling” on page 31.)
6. Select **Use Perfect Forward Secrecy** if you wish to enable this option. (For more information, see “Perfect Forward Secrecy” on page 32.)
7. Tap the arrow button to open the **Symantec Power VPN** window.
8. Enter your account name in the **User Name** field.

9. If you wish to save your password as part of your policy, tap **Prompt** at the **User Password** field which opens the **User password** window. If you do not wish to save your password, please skip the following step.

10. Enter your password and tap **OK** to store it, or **Cancel** if you wish to exit without saving your password. If you save your password, the **User Password** field in the **Symantec Power VPN** window contains the value "**Assigned**". To delete or edit the password, tap **Assigned**, then leave the field blank to delete the password, or enter a new password. Tap **OK** to save your changes.

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

11. Tap the "Network..." button to open the **Network Properties** window. (For more information, see "Network Properties" on page 37.)
12. Enter the IP addresses and subnet masks for the primary and secondary subnets.
13. Tap the checkmark button to return to the **Symantec Power VPN** window.
14. Tap the "IKE..." button to open the **IKE Crypto Suite** window. (For more information, see "IKE Crypto Suite" on page 36.)
15. Set your crypto suite settings by selecting your desired values from each of the pull-down lists for the **Group**, **Cipher**, and **Hash** fields.

Network Properties
Protected Networks

IP Address	Subnet Mask
0.0.0.0	0.0.0.0
0.0.0.0	0.0.0.0
0.0.0.0	0.0.0.0

IKE Crypto Suite

Group: ▾ GRP1_DH-768
GRP2_DH-1024
GRP7_ECDH-163

Cipher: ▾ GRP7_ECDH-163

Hash: ▾ MD5

IKE Crypto Suite

Group: ▾ GRP1_DH-768

Cipher: ▾ DES_CBC
3DES_CBC

Hash: ▾

IKE Crypto Suite

Group: ▾ GRP1_DH-768

Cipher: ▾ 3DES_CBC

Hash: ▾ MD5
SHA

16. Tap the checkmark button to return to the **Symantec Power VPN** window.
17. Tap the "DNS..." button to open the **DNS** window. If **Query DNS** is deselected, further fields appear. (For more information, see "DNS" on page 35.)
18. If instructed to do so, deselect **Query DNS** and enter the primary and secondary DNS addresses in the **Primary DNS** and **Secondary DNS** fields, and the domain name in the **Domain Name** field.

DNS

Query DNS

DNS

Query DNS

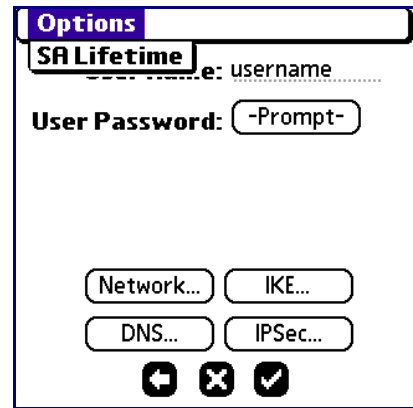
Primary DNS
0.0.0.0

Secondary DNS
0.0.0.0

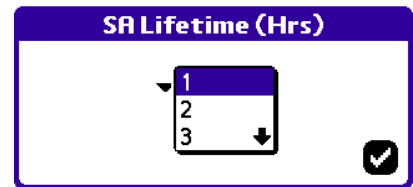
Domain Name
.....

19. Tap the checkmark button to return to the **Symantec Power VPN** window.

20. Tap the "IPSec..." button to open the **IPSec Crypto Suite** window. (For more information, see "IPSec Crypto Suite" on page 37.)
21. Set the value of the **Suite** field by selecting one of the crypto suite options from the list.
22. Tap the checkmark button to return to the **Symantec Power VPN** window.
23. Tap the **movianVPN** tab at the top of the window. The **Options** menu appears. Select **SA Lifetime** to configure the SA Lifetime value.



24. Set the **SA Lifetime** by selecting a value from the list. (For more information, see "SA Life" on page 37.)
25. Tap the checkmark button to return to the **Symantec Power VPN** window.
- 26a. (Standard Palm Devices) Tap **Done**. The **movianVPN** application window appears. Tap the **Login** button to connect to the gateway.
27. (Tungsten-C, Tungsten-T3 Devices) Tap the checkmark to return to the Preferences window. Tap **Done** to begin using your device with the new settings.



5

Running movianVPN

Overview: Running movianVPN

Running **movianVPN** is a simple process of:

- Logging in to the VPN gateway
- Using the VPN gateway to access the VPN
- Logging out of the VPN

Logging in to the gateway

To successfully log in to the VPN gateway, the following must occur:

- **movianVPN** contacts the gateway
- You must supply further authentication if requested (for some gateways)
- Keys will be negotiated and accepted
- You will be logged in to the gateway

Warning: When you are logged in to the gateway, the timed power off is disabled to prevent the handheld device from powering off and inadvertently losing the connection before you have logged out from the gateway. If the handheld device is not connected to a power source, the battery may be drained.

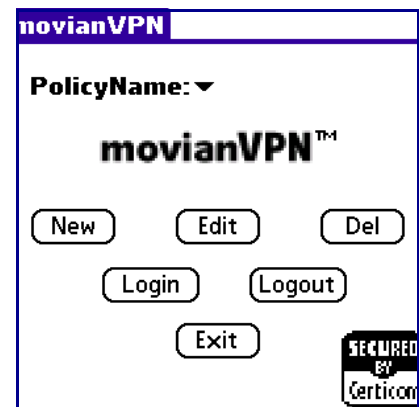
Contacting The Gateway: Standard Palm Devices

The last policy used to log on to the gateway will appear as the default selection when you launch **movianVPN**. If you have more than one **movianVPN** policy available, to select another policy tap the arrow to make the pull-down list appear, and tap the policy you want to use.

Note: If you are unsure which policy to select, ask your network administrator.

To log in the gateway:

1. Open the **movianVPN** application.
2. Tap the **movianVPN** icon. The **movianVPN window** will appear.
3. The last policy used will appear as the default selection when you launch **movianVPN**. Select a different policy from the **Policy Name** pull-down menu, if desired.



4. Tap **Login**. The **IKE - Logging On** window appears and displays your connection progress while connecting to the LAN or to a Dial-up connection.

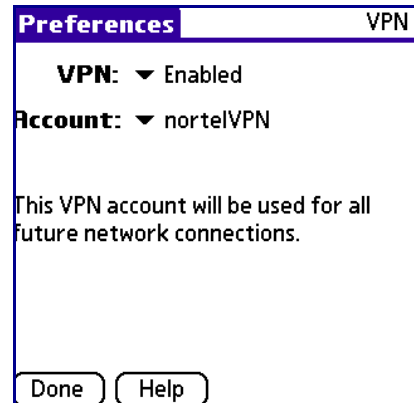
Note: The messages that appear in the Service Connection Progress dialog box depends upon the type of connection.



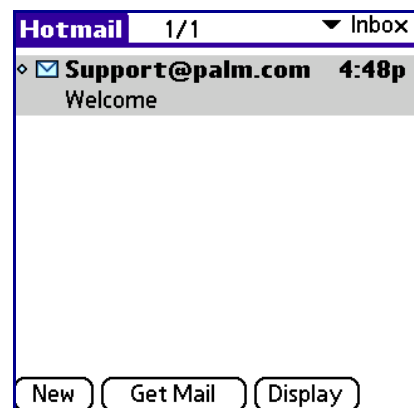
Contacting The Gateway: Tungsten C, Tungsten T3

For the Tungsten C, and Tungsten W devices, running **movianVPN** is slightly different than with a standard Palm device. Running **movianVPN** is a simple process of:

1. Ensure that **movianVPN** is enabled, and you are using the correct policy for your gateway. To verify that **movianVPN** is enabled, select **Prefs** from the **Applications** page, and select **VPN** from the **Preferences** page to see the **VPN preferences** page. In this example, the VPN is enabled and the policy chosen is for a Nortel Contivity Series gateway.



2. Launch your network application, such as your e-mail client. **movianVPN** will automatically be used to encrypt/decrypt network traffic once you are connected. When you close your network application, **movianVPN** is also shut down.



Authentication and Key Negotiation (Standard Palm Devices)

After **movianVPN** has contacted the gateway, depending on the gateway you may be asked for further authentication. The type of authentication requested depends on the gateway and the policy settings. If your gateway is configured to require extended authentication, you will be asked for a password or passcode. Otherwise, you will not be prompted to enter any further information.

Note: Please note that this section does not apply for Tungsten-C and Tungsten-T3 devices.

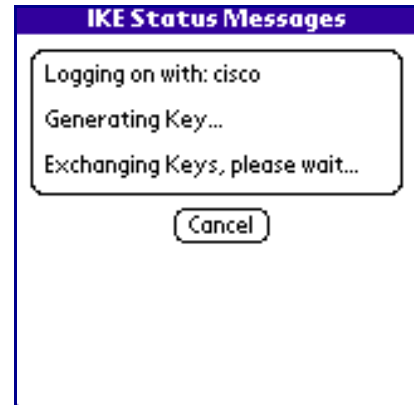
1. Enter your password or SecurID passcode, if you are requested to do so.

Note: For information on changing your PIN, see "Extended Authentication" on page 32

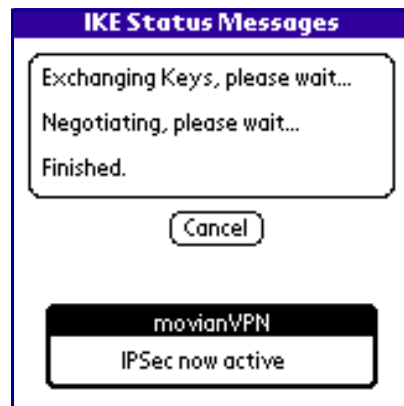


2. Tap the **OK** button. The gateway will generate, exchange, and negotiate keys for connecting. The **IKE Status Messages** window displays your progress.

***Warning:** If you attempt to cancel at this stage, it may not be effective. It is recommended you wait until the button indicates **OK** for the connection, tap the checkmark icon, and then logout from the **movianVPN** window to ensure your session on the gateway is properly closed.*



3. Enter your user password if your gateway requires you to do so.
4. When the connection is established, you are informed that IPSec is active, and the **Cancel** button changes to **OK**. Tap the **OK** button to use your connection.



Changes to movianVPN screen when connected (Standard Palm Devices)

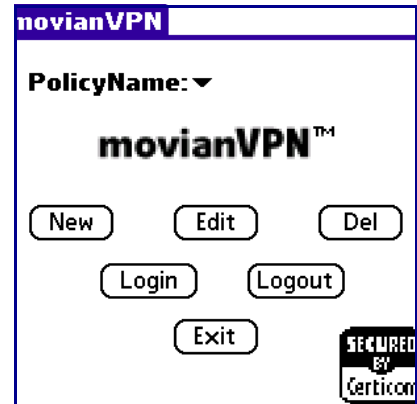
When you are connected to the gateway, there will be changes to the **movianVPN** window on your handheld device.

Note: Please note that these display changes do not apply to Tungsten-C and Tungsten-T3 devices.

Power off timer disabled

The **movianVPN** window adds a notification that "**Power off timer disabled**" is in effect. This is to prevent the handheld device from shutting down automatically while you are still logged on to the gateway. If your connection is closed before you log out from the gateway, you may not be able to log back in until the gateway's automatic time-out has logged you off.

Warning: If your handheld device is not attached to a power source, the battery may be drained.

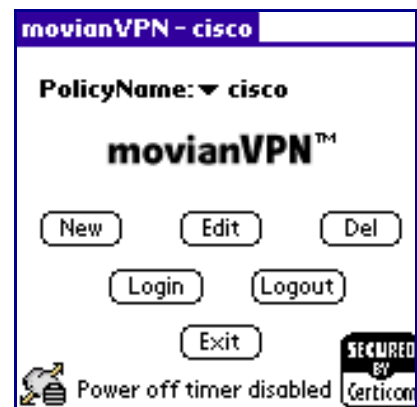


movianVPN secure connection icon

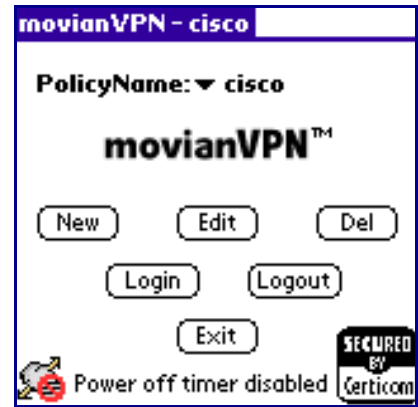
When **movianVPN** is not connected, there is no connection in the the **movianVPN** window.



After you have logged on to the gateway, a lock appears in the lower lefthand corner when the **movianVPN** connection is secure.



If IPsec is disabled, the lock appears, but is crossed out to show that the connection is not secure.



Troubleshooting logging on to the gateway

If you experience difficulty while logging in to the gateway, review your policy and connection type settings. If your settings have been provided to you by an administrator, please ensure that they have been set correctly.

If after checking policy and connection type settings and reviewing the error messages below you are still unable to log in, contact your administrator or support team.

Helpful hints

- If **movianVPN** cannot negotiate a connection to the gateway although the settings appear correct, check that the group name, group password and user name do not have a trailing space after the entry.
- If your dial-up connection is normally made from a particular location, such as home or from the office, you may or may not be required to include a 9 or make other changes in the dialing number. Verify that the dialing prefix for your connection is accurate.
- If your settings are correct but you cannot connect to your gateway, the gateway may be down or inaccessible for some reason. You can ping the gateway to determine whether it is available. For more information, see “Appendix A: Using the Diagnostic Tools” on page 117.
- Changes made to the gateway may result in a failure to establish a VPN tunnel. If the gateway is available when pinged but you cannot connect, contact your gateway administrator.
- If you can connect to your VPN gateway but not download e-mail or reach another server within the intranet, you can ping the server to determine whether it is available. For more information, see “Appendix A: Using the Diagnostic Tools” on page 117. If you cannot reach the server, contact your support staff.
- If you receive "No reply" as an error message, the gateway may be unavailable or there may be too much delay and the gateway times-out the attempted connection. Contact your support staff for more information.
- **movianVPN** uses an auto-detect feature to detect the software driver for your communications hardware. If movianVPN cannot detect the driver, it displays an error message and attempts to use the serial port driver instead. movianVPN allows you to turn off the auto-detect feature and explicitly select which driver you want to use. See “Error messages” on page 111.

Ping (Standard Palm Devices)

You may use the **ping** utility to determine whether you are able to connect to a particular server. To ping a server:

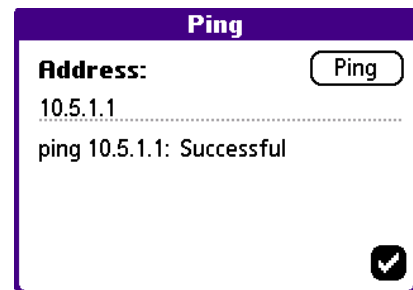
1. Tap the **movianVPN tab**.
2. Open the **Tools** menu. Tap the **Ping** menu item. The opens up the **Ping** window. Enter the address of the server you wish to test connectivity with, and tap the **Ping** button to ping the server.



3. If you are unable to ping the specified server, an error message is displayed.



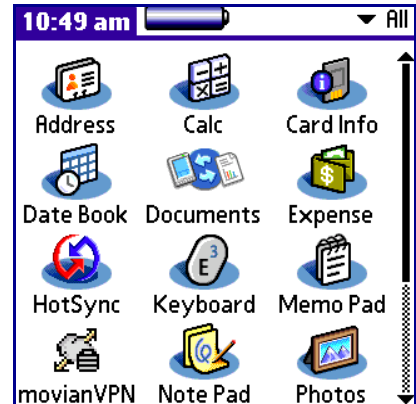
4. A message is displayed if you successfully ping the server.
5. Tap the checkmark icon to exit the Ping tool.



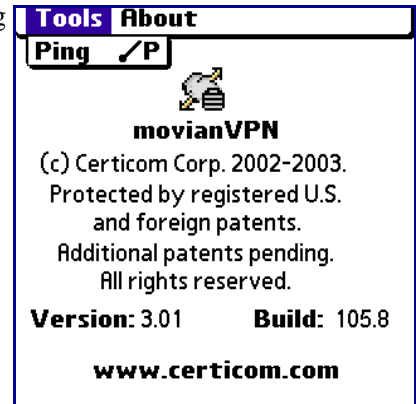
Ping (Tungsten-C, Tungsten-T3 Devices)

You may use the **ping** utility to determine whether you are able to connect to a particular server. To ping a server:

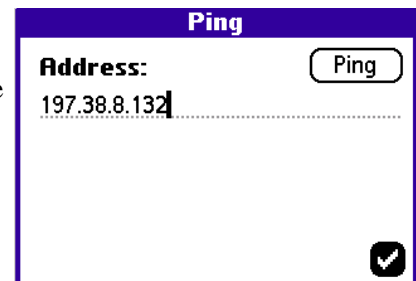
1. From your **Applications** screen, tap the **movianVPN** button.



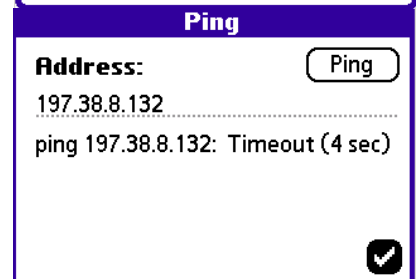
2. Open the **movianVPN** menu by either tapping the **Menu** button, or by tapping the **movianVPN** tab.



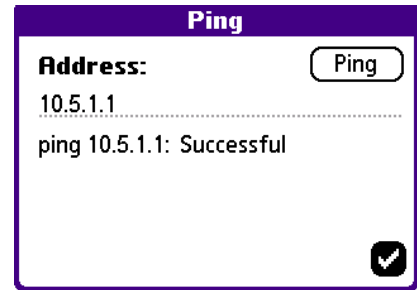
3. Tap the **Ping** menu item. This opens up the **Ping** window. Enter the address of the server you wish to test connectivity with, and tap the **Ping** button to ping the server.



4. If you are unable to ping the specified server, an error message is displayed.



- 5. A message is displayed if you successfully ping the server.



Error messages

While logging on to the gateway you may receive error messages such as the following:

Driver not found

If **movianVPN** cannot find the software driver for your communications hardware, a dialog box opens and a default driver may be used instead.

movianVPN allows you to disable the auto-detect feature and explicitly select which driver you want to use.

To select the driver, select **Options** then **Connection Type** on the menu bar. Tap on the arrow and select your driver from the list. Tap the checkmark icon to complete your selection.

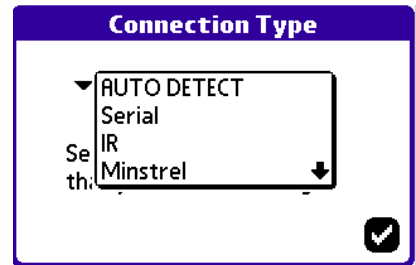
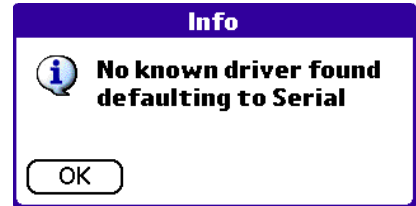
You must shut down **movianVPN** and reset your device for the change to take effect.

If you see the error message again, contact technical support.

Not using movianVPN connection

If you have not set your connection to use the **movianVPN** connection profile, you may encounter an error message. If this occurs, ensure that the **Connection** field in the **Network Settings->Preferences** window is set to **movianVPN**.

For more information see “Verifying your network preferences (Standard Palm Devices)” on page 25.



Dial-up connection fails

You may receive the following messages while connecting using dial-up:



If the connection cannot be established you can:

- Check that the dial-up number is correct.
- Check that the physical connections have been properly made for the dial-up.
- Check that the handheld device is not currently connected to HotSync on your computer.
- Check the connections properties for the dial-up options are correct.
- Contact your support staff for assistance and information. You may not have logged out of the gateway during your last session, and the gateway automatic time-out has not yet occurred.

LAN connection fails

You may encounter error messages while connecting to the gateway through a LAN.

If the LAN connection cannot be established, you can:

- Check that the handheld device is not currently connected to HotSync on your computer.
- Contact your network administrator for assistance and information. It is possible that you may not have logged out of the gateway during your last session, and the gateway's automatic time-out has not yet occurred.



Password Request Appears Repeatedly

You may have entered the password incorrectly for Extended Authentication.

Authorization Failed

After entering your extended authorization password or code, you may receive a message that negotiation has failed.

If the password or SecurID entered for Extended Authentication is incorrect, authorization fails and the connection to the gateway will not be made.

- You may be entering the wrong password or additional code for your username.
- You may not have logged out of the gateway during your last session, and the gateway automatic time-out has not yet occurred.
- Contact your administrator for assistance and information.

Using movianVPN (Standard Palm Devices)

Once you have logged in to the gateway, you can begin working with the applications. If you want to access the Internet outside of your VPN, you can deselect IPsec.

Working with applications

Once you have logged in to the gateway, you will be able to access and download information and utilize applications.

To access applications:

1. Select the desired program icon from the Palm OS window.

Disabling and Enabling 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**, you can select and deselect IPsec during your session with the gateway. While IPsec is deselected, you will be able to access servers and websites outside of the VPN, but you 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 by the VPN or by elsewhere on the Internet. Split Tunneling allows you to freely access the Internet and securely access the corporate intranet at the same time. For more information see “Split Tunneling” on page 31 or contact your support staff.

Warning: While IPsec is deselected, your connection is not secure. Transmitted data is not encrypted.

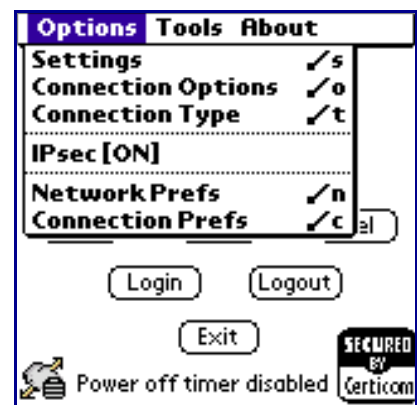
Disabling and enabling IPsec

IPsec can be disabled and enabled in **movianVPN** while connected to a gateway. While IPsec is enabled, you will not be able to reach servers outside the VPN.

To disable or enable IPsec:

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

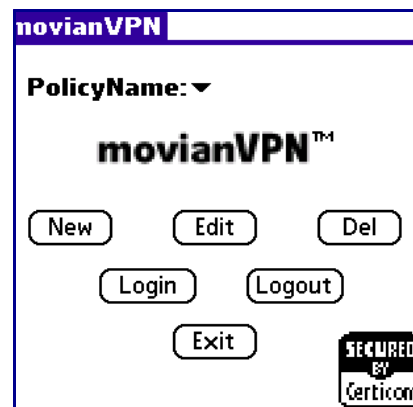
Warning: Your connection will not be secure and data will not be encrypted.



3. Tap **OK**. When **IPSec** is disabled, the cloud icon in the bottom lefthand corner has an X through it.

4. To re-enable **IPSec**, tap the **movianVPN** tab and select **IPsec**.

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



Logging out of the gateway

To log out of **movianVPN**, you must logout of your session on the gateway and then close your connection to your Internet Service Provider or to the wireless network.

Note: Depending on your account settings, if you do not logout of the gateway first, the server will not close your session; until session is closed you will not be able to log back onto the server. The server can be set to log you off automatically after a set time. More information can be obtained from your support staff.

Note: If you are using a Tungsten-C or Tungsten-T3 device, you do not need to log out of the gateway or close **movianVPN**, as these steps are unnecessary for your device.

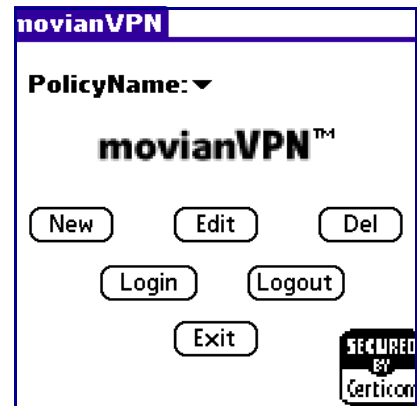
Logging out of the gateway (Standard Palm Devices)

Note: If you have already closed **movianVPN**, you can re-open the application and logout before closing the connection.

To log out of the gateway:

1. Tap the **movianVPN** icon in the lower taskbar in the menu window
2. In the **movianVPN** window, tap the **Logout** button.

Note: Confirm that the Policy Name field contains the active policy name.



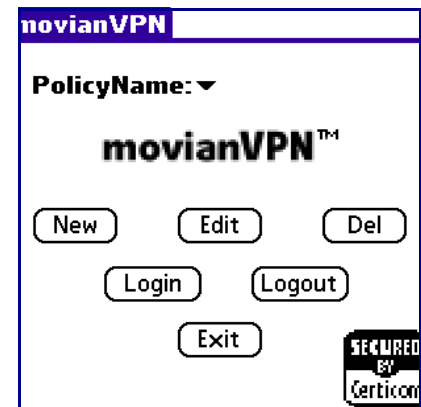
3. The **IKE** window will appear and display the progress of the logoff
4. When the log off is complete, tap **OK** to exit **movianVPN**.



Closing movianVPN (Standard Palm Devices)

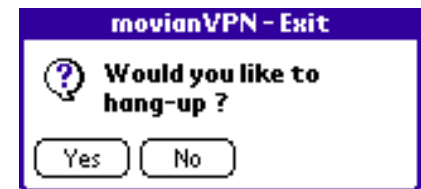
To close **movianVPN**:

1. Tap the **Exit** button in the **movianVPN** window.



2. You will be asked if you want to hang up.
3. Tap **Yes** to drop your connection and exit **movianVPN**.

Note: If you close **movianVPN** before logging out of the gateway, you can re-open the application and log out.



A

Appendix A: Using the Diagnostic Tools

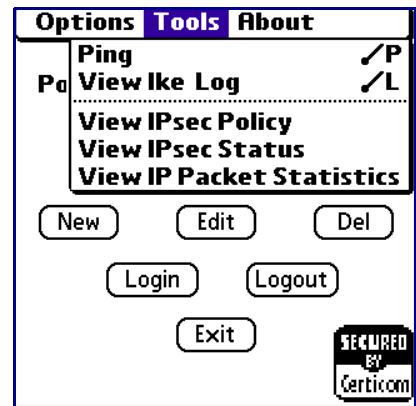
Accessing diagnostic tools

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

- Ping
- View IKE Log
- View IPsec Status
- View IP Packet Status

To access the diagnostic tools:

1. In the **movianVPN** window, tap the **movianVPN** tab.
2. Open the **Tools** menu.
3. Tap the diagnostic tool you want to open.



Ping (Standard Palm Devices)

Use **Ping** to determine whether you are able to contact a particular server. To ping a server:

1. Tap the **movianVPN tab**.
2. Open the **Tools** menu 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. If the ping fails to reach the server, an error message will be displayed.



6. Tap the checkmark icon to exit the Ping tool.

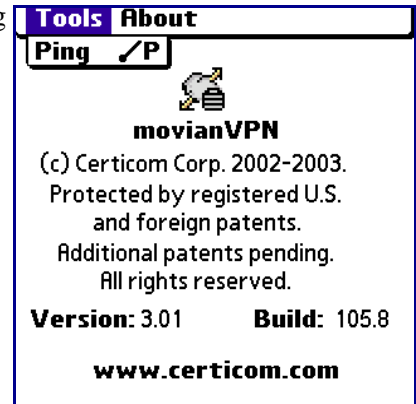
Ping (Tungsten-C, Tungsten-T3 Devices)

You may use the **ping** utility to determine whether you are able to connect to a particular server. To ping a server:

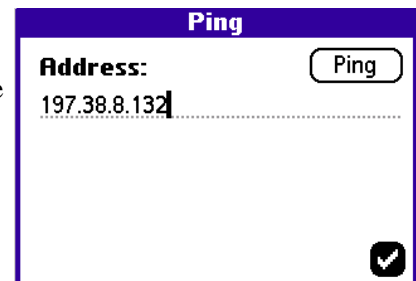
1. From your **Applications** screen, tap the **movianVPN** button.



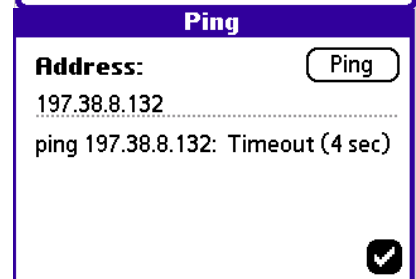
2. Open the **movianVPN** menu by either tapping the **Menu** button, or by tapping the **movianVPN** tab.



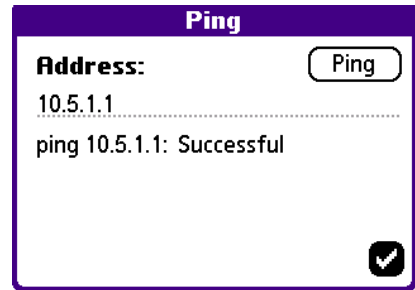
3. Tap the **Ping** menu item. This opens up the **Ping** window. Enter the address of the server you wish to test connectivity with, and tap the **Ping** button to ping the server.



4. If you are unable to ping the specified server, an error message is displayed.



- 5. A message is displayed if you successfully ping the server.



View Log (Standard Palm Devices)

The IKE log is used primarily for diagnostic purposes. It provides information on the steps taken in negotiating and exchanging keys.

Note: The IKE log is cleared automatically when you exit the client and no information will be available when you log in again.

To view IKE Log:

1. Tap the **movianVPN tab**.
2. Tap **Tools** and select **View IKE Log** from the list. The **Log** window appears.
3. Tap **Clear** to clear the log, if desired.
4. Tap **Done** to close the window.



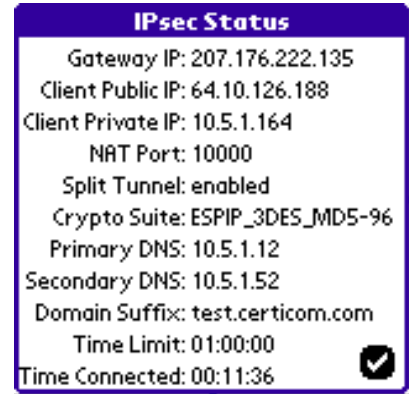
View IPsec Status (Standard Palm Devices)

IPSec Status can be used to confirm that a tunnel is available and provide information.

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

To view IPsec status:

1. Tap the **movian VPN tab**.
2. Tap **Tools** and select **View IPSec Status** from the list. The **IPsec Status** window appears. This window provides status information on the handheld device and gateway.
3. Tap the checkmark icon to close the window



The **IPSec Status** window provides 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

View IP packet Statistics (Standard Palm Devices)

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 network support department may ask you to clear the statistics while debugging; this would 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.

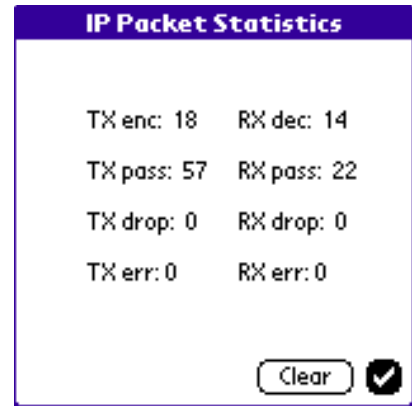
Note: View IP Packet Statistics is only available while the VPN tunnel is up.

To view IP Packet Statistics:

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 to close the window.

The fields indicate the following information on transmitted encrypted packets:

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



B

Appendix B: Troubleshooting (Standard Palm Devices)

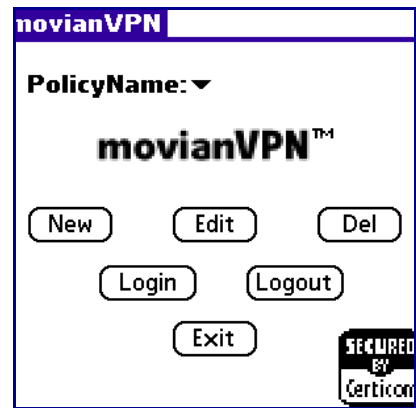
Setting Connection Options

If you are having trouble receiving a reply from your VPN gateway or ISP mobile connection because of a weak signal or busy network, you can try adjusting the socket options.

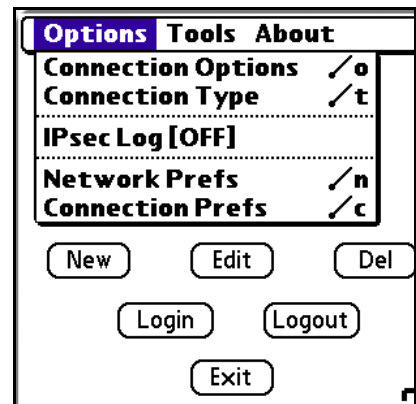
- **Socket Retries** option sets the number of times **movianVPN** will attempt to connect.
- **Socket Timeout** option sets the time the system will allow before considering each attempt to be a failure.

To set your connection options:

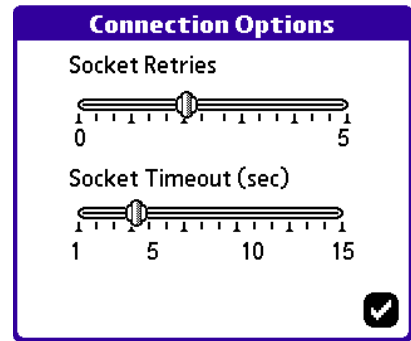
1. Tap the **movianVPN** tab in the top toolbar of the **movianVPN** application window.



2. Open the **Options** menu.



3. Select **Connection Options** from the menu. The **Connection Options** window appears.
4. Tap the arrow and select your connection type from the pull-down list.
5. Set the values for **Socket Retries** and **Socket Timeout** using the sliders.
6. Tap the checkmark button to save your values.



Additional messages

The following messages may also appear while you are logging in to the gateway. Contact support for assistance and information.

Couldn't find Net Library!

This message appears when the client was unable to find the network library on the system, normally caused by problems with the version of Palm OS being used.

Couldn't open Network Library!

This message appears when the client was unable to open an active PPP connection, normally caused by problems with Internet connection. Check the connection without the client.

Could not send()! Exiting.

This message appears when the client was unable to send data, normally caused by a problem with the network connection. This could be caused by the connection dropping or any of the socket errors (see below).

Failed to find/create IPsec SP database!

This message appears when the client was unable to find or create the Ipsec policy database, normally caused by a problem with available memory on the device. It may be caused by the database being corrupted and a flag being active that locks the database. Contact your support staff for and assistance and information.

Failed to receive reply

This message appears when the client did not receive a response from the gateway, normally caused by the gateway being unavailable or if the group ID or password are incorrect.

Negotiation Failed

This message appears when some part of the negotiation process failed. This may occur if there is a poor quality connection to the gateway. Check your policy settings. If it happens repeatedly, contact your support staff for assistance and information.

Please contact your help desk.

This message appears after the connection fails. If it appears repeatedly after you have attempted the troubleshooting described above in “Troubleshooting logging on to the gateway” on page 107, contact your support staff for assistance and information.

C

Appendix C: Glossary of Terms

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

Extended Authentication	<p>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.</p> <p>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.</p>
Gateway	<p>A gateway is the server which recognizes and authenticates a user attempting to access a VPN.</p>
Hash Numbers	<p>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.</p>
IKE Internet Key Exchange protocol	<p>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.</p>
IPSec	<p>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.</p>
ISP Internet Service Provider	<p>A company providing dial-up connections to access the Internet.</p>
Key	<p>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.</p>

Perfect Forward Secrecy	<p>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.</p> <p>Perfect Forward Secrecy creates new keys for each step of the Internet Key Exchange (IKE). Negotiation of the connection will take longer.</p>
PDA Personal Digital Assistant	<p>Personal Digital Assistants (PDAs) are handheld personal computing devices.</p>
Policy	<p>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.</p>
SA Security Association	<p>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.</p>
Split Tunnelling	<p>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.</p> <p>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.</p>
Tunnel	<p>A tunnel is created to securely send encrypted information directly from one computer to another.</p>
VPN Virtual Private Network	<p>A Virtual Private Network or VPN is used to provide secure, encrypted communication between specific computers on a wider network.</p>

D

Appendix D: Information worksheet

Information required for client configuration

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

Not all fields will apply for your specific gateway.

Information required for policy creation

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:
		Domain Name:
IKE Suite		Group:
		Cipher:
		Hash:
Group Name		
Group Password		
User Name		
User Password		
User Passcode (SecurID)		
Network Properties		Primary Subnet IP Address:
		Primary Subnet Mask:
		Secondary Subnet IP Address:
		Secondary Subnet Mask:
		Tertiary Subnet IP Address:
		Tertiary Subnet Mask:
IPSec Suite		
SA Lifetime		
Options > Connection Type		
Options > Dial-up RAS entry		

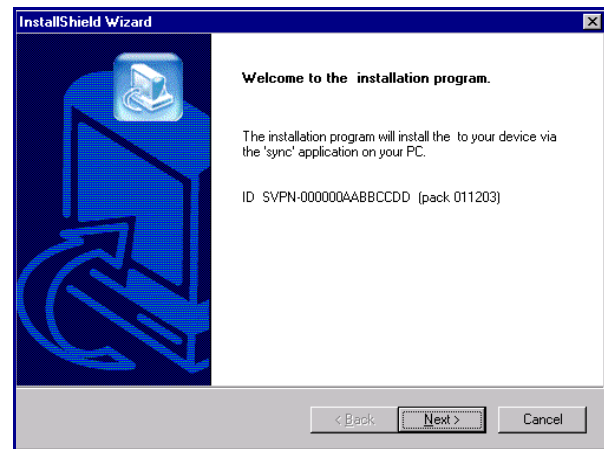
E

Appendix E: Installing a movianVPN License

To obtain a licensed copy of **movianVPN**, visit <http://www.certicom.com> and contact one of our channel partners.

When you have the installer for the licensed version of **movianVPN**, follow the steps below.

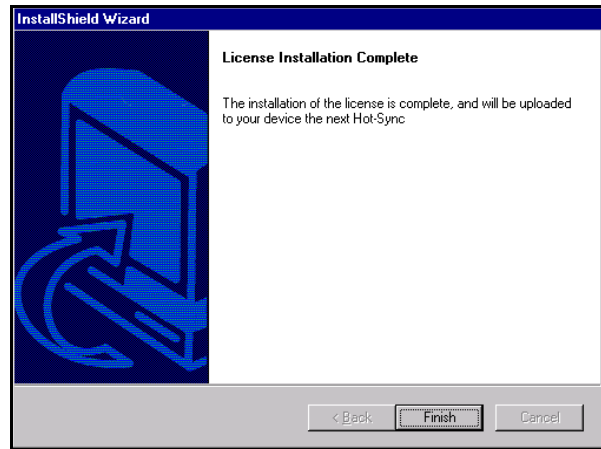
1. On your PC, click on the license icon to start the installer. The install screen appears.



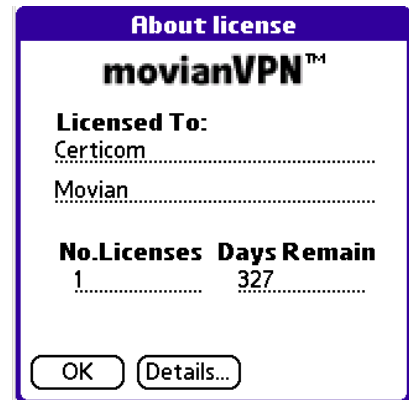
2. Click **Next**. The license agreement screen will appear.



3. Click **Yes** to accept the license.



4. When you HotSync, the new license will appear on your device. Tap **movianVPN** in the upper toolbar and tap **About License** in the toolbar that appears to view the new license.



Index

A

- Alcatel Secure VPN Series gateway, *41*
 - policy, *41*
- authentication, *4*
 - key, *6*
- Avaya VSU VPN Series gateway, *45*
 - policy, *45*

C

- Check Point VPN-1 gateway, *49*
 - policy, *49*
- checkboxes
 - editing options, *34*
- Cipher (IKE Crypto Suite), *36*
- Cisco Unity with Cisco 3000 v3.0 gateway, *53, 88*
- Cisco VPN Concentrator 3000 gateway
 - policy, *57*
 - Unity policy, *53*
- connections
 - supported, *7*
- creating policies, *27*

D

- devices
 - handheld and wireless, *4*
 - supported, *7*
 - synchronizing, *11*
 - synchronizing on installation, *11*
- diagnostic tools
 - accessing, *117*
 - Ping, *118*
 - View IKE Log, *121*
 - View IP Packet Statistics, *123*

View IPSec Status, *122*

- DNS, *35*
 - query gateway, *35*
- Domain Name System. *see* DNS

E

- encryption, *4, 6*
 - key, *6*
- evaluation license, *20*
- Extended Authentication, *32*
 - SecurID, *33*
- extranet VPN, *3*

G

- gateway
 - accessing, *6, 27*
 - creating policies, *27*
 - DNS query, *35*
 - IPSec, *34*
 - policies, *27*
 - policy settings, *35*
 - server modes, *35*
 - settings
 - DNS, *35*
 - Extended Authentication, *32*
 - IKE Crypto Suite, *35, 36*
 - IPSec Crypto Suite, *35, 37*
 - Network Properties, *35, 37*
 - Perfect Forward Secrecy, *32*
 - SA Life, *37*
 - Split Tunneling, *31*
 - Split Tunneling, *31*
- gateway servers, *3*
 - accessing, *6*
- gateways

Alcatel Secure VPN Series, *41*
Avaya VSU VPN Series, *45*
Check Point VPN-1, *49*
Cisco Unity with Cisco 3000 v3.0, *53, 88*
Cisco VPN Concentrator 3000, *53, 57*
Intel Netstructure Series, *70*
Lucent Brick Firewall VPN, *74*
Netscreen Series, *61, 78*
Nortel Contivity Series, *83*
policies, *27*
Radguard cIPro gateway, *66*
Secure Computing Sidewinder, *92*
Symantec Power VPN, *96*
Group (IKE Crypto Suite), *36*

H

handheld devices
 connecting to VPN, *4*
Hash (IKE Crypto Suite), *36*
hash numbers, *36*
HotSync, *11*
 to install movianVPN, *11*

I

IKE Crypto Suite, *36*
 Cipher, *36*
 Group, *36*
 Hash, *36*
installation, *10, 11*
 on handheld device, *11*
 synchronizing your device, *10, 11*
 uninstalling, *21*
Intel Netstructure Series gateway, *70*
 policy, *70*
intranet VPN, *3*
IP Packet Statistics, *123*
IPSec, *4, 34, 113*

 and Split Tunneling, *34, 113*
 communication process, *6*
 disabling, *34, 113*
 enabling, *34, 113*
 using, *34*

IPSec Crypto Suite, *37*

IPSec Status, *122*

K

keys
 authentication, *6*
 encryption, *6*
 exchange protocols, *36*
 IKE Crypto Suite, *36*

L

licensing, *12, 16, 20*
 evaluation, *20*
 license agreement, *12, 16*
 license type, *20*
Lucent Brick Firewall VPN gateway, *74*
 policy, *74*

M

movianVPN, *6*
 client software, *6*
 getting started, *23*
 installation requirements, *9*
 installing, *10, 11*
 license agreement, *12, 16*
 licensing, *20*
 overview, *1*
 policies, *6, 27*
 support, *20*
 system requirements, *9*
 uninstalling, *21*

version number, *18*

N

Netscreen Series gateway, *61, 78*

policy, *61, 78*

Network Properties, *37*

Nortel Contivity Series gateway, *83*

policy, *83*

O

overview

getting started, *23*

movianVPN, *1*

P

passcode, *32*

changing, *33*

passwords

Extended Authentication, *32*

Perfect Forward Secrecy, *32*

key, *32*

PIN code

SecurID, *33*

Ping, *118*

policies, *6*

checkboxes

editing, *34*

creating, *27*

Alcatel Secure VPN Series, *41*

Avaya VSU VPN Series, *45*

Check Point VPN-1, *49*

Cisco Unity with Cisco 3000 v3.0, *53, 88*

Cisco VPN Concentrator 3000, *53, 57*

Intel Netstructure Series, *70*

Lucent Brick Firewall VPN, *74*

Netscreen Series, *61, 78*

Nortel Contivity Series, *83*

Radguard cIPro, *66*

Secure Computing Sidewinder, *92*

Symantec Power VPN, *96*

Extended Authentication, *32*

Perfect Forward Secrecy, *32*

required information, *133*

settings

DNS, *35*

Extended Authentication, *32*

IKE Crypto Suite, *36*

IPSec Crypto Suite, *37*

Perfect Forward Secrecy, *32*

SA Life, *37*

Split Tunneling, *31*

Split Tunneling, *31*

verifying, *31*

R

Radguard cIPro gateway, *66*

policy, *66*

remote access VPN, *3*

S

SA Life, *37*

Secure Computing Sidewinder gateway, *92*

policy, *92*

SecurID, *33*

changing passcodes, *33*

PIN codes, *33*

token codes, *32*

Security Association (SA) Life, *37*

servers

gateway, *3, 6*

Split Tunneling, *31*

overview, *31*

support

reaching, *20*

Symantec Power VPN gateway, *96*

policy, *96*

synchronizing devices, *11*
 to install movianVPN, *11*
system requirements, *9*

T

tokencode
 SecurID, *32*
tunneling, *3, 4*

U

uninstalling
 movianVPN, *21*

V

verifying
 policies, *31*
version number, *18*

View IKE Log, *121*
View IP Packet Statistics, *123*
View IPSec Status, *122*
Virtual Private Network. *see* VPN

VPN, *3*
 accessing, *6*
 extranet, *3*
 forms, *3*
 gateway access, *6*
 gateway servers, *3, 6*
 intranet, *3*
 overview, *3*
 remote access, *3*
 tunneling, *3, 4*
 using, *3*
 wireless and handheld devices, *4*

W

wireless and handheld devices
 connecting to VPN, *4*