



movianVPN™

A handheld VPN client specifically designed for mobile and wireless devices

Version 1.1.2
Symantec (AXENT) Power VPN

Server Configuration Guide



Certicom(R), Certicom logos, movian (tm), movianVPN (tm) are trademarks of Certicom Corp. All other trademarks used are the property of their respective owners.

The *Server Configuration Guide* describes how to configure various VPN servers for use with **movianVPN**.

Other documentation provided with **movianVPN** includes the *movianVPN User's Guide*. The *User's Guide* describes how to install, configure, and use **movianVPN**.

General Inquiry

The **movianVPN** general inquiry may be contacted at 510-780-5100. For further product information visit our website at www.moviansecurity.com.

ALL INFORMATION CONTAINED IN THIS DOCUMENT ARE PROVIDED "AS IS" WITHOUT WARRANTY OR CONDITIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. CERTICOM DISCLAIMS ANY LEGAL LIABILITY OR RESPONSIBILITY FOR THE ACCURACY, COMPLETENESS, OR USEFULNESS OF ANY INFORMATION, PROCEDURE, METHOD, APPARATUS, PRODUCT, OR PROCESS POSTED HERE. NEITHER CERTICOM, ITS EMPLOYEES, NOR ITS ASSOCIATES ASSUMES ANY RESPONSIBILITY FOR LOSS OR DAMAGES RESULTING FROM THE USE OF INFORMATION CONTAINED IN THE DOCUMENTATION. CERTICOM ASSUMES NO RESPONSIBILITY FOR ERRORS OR OMISSIONS IN THIS DOCUMENTATION.

WITH RESPECT TO ONLY LIMITATION OF DIRECT DAMAGES, UNLESS SPECIFICALLY STATED OTHERWISE IN A LICENSE AGREEMENT EXECUTED BETWEEN YOU AND CERTICOM, YOU AGREE THAT ANY LIABILITY ON THE PART OF CERTICOM FOR BREACH OF THE WARRANTIES CONTAINED HEREIN OR ANY OF THE OTHER PROVISIONS OF THIS AGREEMENT OR ANY OTHER BREACH GIVING RISE TO LIABILITY OR IN ANY OTHER WAY ARISING OUT OF OR RELATED TO THIS AGREEMENT FOR ANY CAUSE OF ACTION WHATSOEVER AND REGARDLESS OF THE FORM OF ACTION (INCLUDING BREACH OF CONTRACT, STRICT LIABILITY, TORT INCLUDING NEGLIGENCE OR ANY OTHER LEGAL OR EQUITABLE THEORY), SHALL BE LIMITED TO YOUR DIRECT DAMAGES IN AN AMOUNT NOT TO EXCEED ONE (\$1.00) US DOLLAR

YOU AGREE THAT IN NO EVENT WILL CERTICOM BE LIABLE FOR DAMAGES IN RESPECT OF INCIDENTAL, ORDINARY, PUNITIVE, EXEMPLARY, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES EVEN IF CERTICOM HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES INCLUDING, BUT NOT LIMITED TO, BUSINESS INTERRUPTION, LOST BUSINESS REVENUE, LOST PROFITS, FAILURE TO REALIZE EXPECTED SAVINGS, ECONOMIC LOSS, LOSS OF DATA, LOSS OF BUSINESS OPPORTUNITY OR ANY CLAIM AGAINST YOU BY ANY OTHER PARTY. BECAUSE SOME JURISDICTIONS DO NOT ALLOW THE LIMITATIONS ON IMPLIED WARRANTIES OR THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATIONS MAY NOT APPLY TO YOU.

BY USING THIS DOCUMENTATION, YOU AGREE TO BE BOUND BY THE TERMS AS STATED HEREIN. IF YOU DO NOT ACCEPT THESE TERMS AND CONDITIONS, YOU MUST DELETE THIS DOCUMENT AND NOT MAKE ANY USE OF IT.

ADDITIONAL TERMS AND CONDITIONS MAY APPLY TO YOU AS PER THE SOFTWARE LICENSE AGREEMENT THAT YOU MAY HAVE EXECUTED WITH CERTICOM.

Copyright Notice

© Certicom Corp. 2000, 2001. 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."

"Certicom(R), Certicom logos, movian (tm), movianVPN (tm) are trademarks of Certicom Corp. The movianVPN is covered by one or more of the following U.S. Patents: 6,078,667 , 6,049,815, 5,999,626, 5,955,717, 5,933,504, 5,896,455, 5,889,865, 5,787,028, 5,761,305, 5,600,725, 4,745,568, and corresponding foreign patents. Additional patents pending.



Introduction

Overview of the movianVPN - - - - -	1
<i>How the Client Works</i> - - - - -	1
<i>Features and Benefits</i> - - - - -	1
Overview of the Configuration Process - - - - -	3

Configuring the Symantec (AXENT) PowerVPN

Introduction- - - - -	5
<i>The Configuration Process</i> - - - - -	5
Base Components - - - - -	7
Access Control - - - - -	12
Virtual Private Networks - - - - -	14
Monitoring Controls - - - - -	16



1 Introduction

*This chapter is an overview of the process of configuring a Virtual Private Network (VPN) for use with the **movianVPN**. The following sections are included:*

- Overview of **movianVPN**
- Overview of the Configuration Process

Overview of the **movianVPN**

The Certicom **Handheld VPN Client** is a fully configurable GUI-based application you can use to securely connect to a VPN over a wired or wireless connection. With **movianVPN**, you can access and exchange e-mail, as well as acquire Sales Force Automation and Enterprise Resource Planning data with little risk of the information being intercepted or of unauthorized users penetrating your system.

How the Client Works

Using **movianVPN**, you can connect to a VPN via a wireless network or with a conventional telephone line that dials into an Internet Service Provider. When you connect to the VPN, the VPN gateway encrypts the information using IPSec and sends it through the tunnel to **movianVPN**. **movianVPN** then decrypts the message. Note that this is a two-way process — any information you send using **movianVPN** is encrypted before it reaches the tunnel, and is decrypted by the VPN gateway.

Once connected, you can use the software on your Palm™ organizer or Win CE device to access the information you need. You can send and receive messages with an e-mail client, or you can download the latest corporate information with a Web browser.

Features and Benefits

movianVPN offers the following features and benefits:

- An intuitive graphical user interface which allows you to easily configure the Client and connect to a VPN.
- Uses a 163-bit Elliptic Curve Cryptosystem (ECC) algorithm, as well as 768-bit and 1024-bit Diffie-Hellman algorithms. These algorithms can quickly generate keys and secure the data sent through IP tunnels. ECC provides a high level of

security with less code and a smaller encryption key than other well-known encryption methods. It also ensures fast connections to gateways supporting ECC. Diffie-Hellman also provides strong security, and ensures interoperability.

- Use of an Internet Key Exchange (IKE)-based IPsec protocol.
- Runs on both major hand-held platforms: the Palm™ organizer and the PocketPC™ (Win CE).



Overview of the Configuration Process

Before remote users can communicate with a VPN using the **movianVPN**, you must modify the configuration of the target VPN. Specifically:

- Configuring the internal and external interfaces with the appropriate IP addresses.
- Configuring the public interface and default gateway.
- Creating and applying client policies and filters.
- Setting up a pool of IP addresses.
- Enabling IPSec and IKE for a user group or set of user groups.

Note: The parameters you must configure will differ depending on the VPN server you are using, and on your needs.



2 Configuring the Symantec (AXENT) PowerVPN

This chapter explains how to configure the Symantec (Axent) Power VPN server for use with the movianVPN. The following sections are included:

- Introduction
- Base Components
- Access Control
- Virtual Private Network
- Monitoring Controls

Introduction

The Power VPN does not interoperate with **movianVPN** out of the box. You must configure the interfaces and security settings on the VPN before users can make connections with **movianVPN**.

Before you configure Power VPN for use with **movianVPN**:

- Install the Raptor Management Console on the appropriate computer.
- Set up the Local Host.
- Log in to the management server.
- Know the IP address and subnet mask of the VPN.
- Have a list of the names of your users.

The Configuration Process

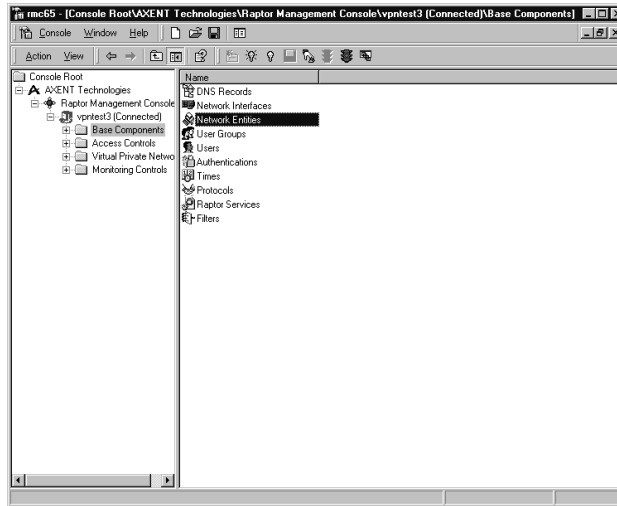
Configuring Power VPN Server to work with **movianVPN** involves:

- Setting up the “Base Components”, including the security gateway, security groups, and authentication and the IKE user group.
- Establishing the “Access Control” for rules to access the VPN.
- Presenting the VPN policies and protocols.

Note: This chapter only covers the configuration tasks specific to interoperability with the **VPN Client**. For detailed configuration information, refer to the appropriate Symantec documentation.

Base Components

- From the Management Server, select “Base Components”.



- Right click on “Network Entities”.
- Click on the “Security Gateway” tab.
- The “New Security Gateway Properties” window now appears.



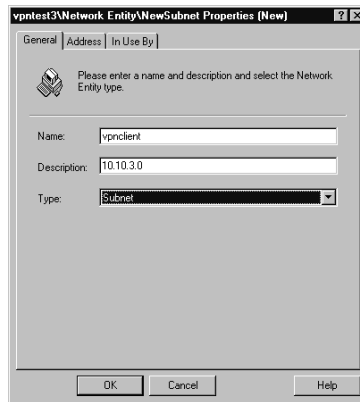
- Click on the “General” tab.
- In the “Name” field, type a name to describe the gateway access point on the public side.
- Click on the “Security Gateway” tab.



- In the “IP Address” field, select the IP address of the external network.

NOTE: Make sure that the “Enable IKE” box is selected.

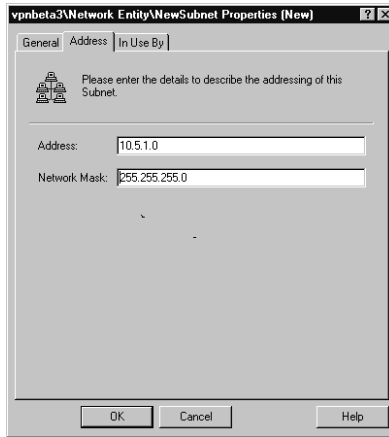
- Click “OK”.
- From the Management console select “Base Components”, and then right click on “Network Entities”.
- Select “New” and then “Subnet”.
- Click on the “General” tab.



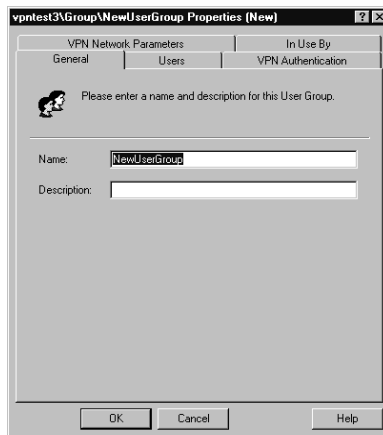
- In the “Name” field type in a name describing the private network.



- Click on the “Address” tab.



- In the “Address” field type in the network address of the subnet to which you want to provide access.
- In the “Network Mask” field type in the entry appropriate to the network address.
- Click “OK”.
- From the Management Console select “Base Components”, and then right click on “User Group”.
- Select “New” and then “New Usergroup” properties.
- Click on the “General” tab.



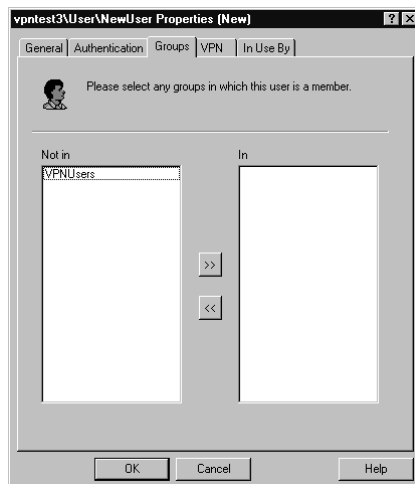
- In the “Name” field, type a description of the VPN users.
- Click “OK”.

- From the Management Console select “Base Components”, and then right click on “Users”.
- Select “New”, then “User”, and finally “New User Properties”.
- Click on the “General” tab.

- In the “Name” field, type in the user name.
- In the “Description” field type in the actual name description.
- In the “User ID” field, type in the appropriate user ID.

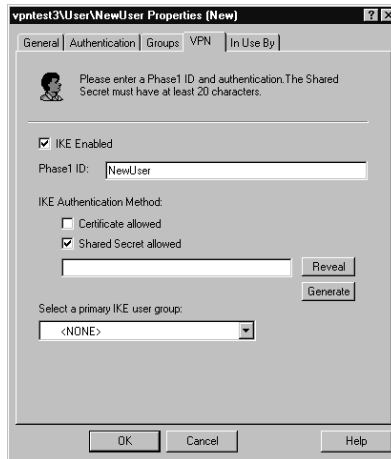
NOTE: This ID must be the same as that listed in the client PDA.

- In the “New User Properties” window, click the “Groups” tab.





- In the “Not In” field, select group(s) from the previous menu, and move it to the “Rule Proprieties” field.
- Click on the “VPN” tab.



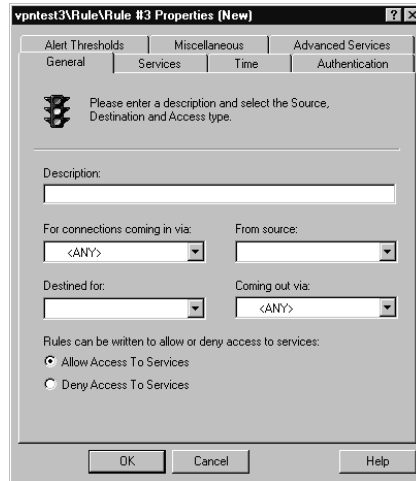
- Select the “IKE enabled” box.
- The user name appears under “Phase 1 ID”.
- Under the “IKE Authentication Method”, select the “Shared Secret allowed” box.
- In the field directly under the shared secret field, type in your password

NOTE: This password must be at least 20 characters long, and must be the same as the password listed in the client PDA.

- If you wish to display the password, click on “Reveal”, and the password will be displayed in plain language in the password window. If you wish to have passwords generated automatically, click on “Generate”.
- Now click on the “New User Properties” tab.
- Right at the bottom of the window, go to “Select a primary IKE user Group”. Click on the pull down menu, and select the VPN user group which you have previously set.
- Click “OK”.

Access Control

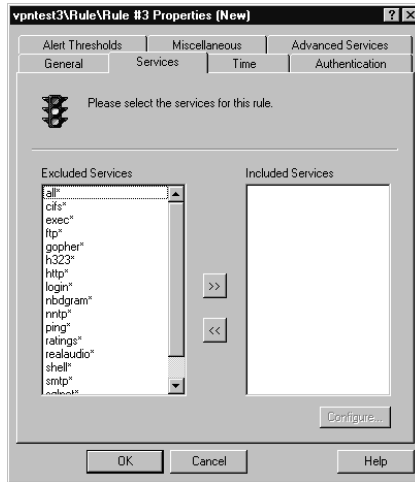
- From the management console, select “Access Controls”, and right click on “Rules”. The “Rule Properties” window appears (Rules are numbered automatically).
- Click on the “General” tab.



- In the “Description” field type in a text description of the service rules.
- In the “For connections coming in via” field type in any VPN.
- In the “Destined for” field type in the internal subnet which you have previously selected.
- In the “Coming out via” field type in the network interface connected to the private network.

NOTE: The “Access to Services” box must be selected.

- Now click on the “Services” tab.
- Normally, under “Excluded Services” you should select all. However, for more detailed control of VPN services, you may select individual services (instead of all) for the “Included Services” field.
- Now move your selection to the “Included Services” field.



NOTE: At this point, if you are using an integrated fire wall, you will need a second rule. This will require you to again do all the steps as above under “Access Controls”.

Virtual Private Networks

- From the management console, select “Virtual Private Networks”.
 - Double click on “IKE Policy”.
 - Double click on “Global_IKE_policy”. Set these parameters according to your corporate security policy.
 - Click “OK”
-
- From the management console, select “Virtual Private Networks”.
 - Right click on “VPN Policies”. Select “New”.
 - Now the “New VPN Policy Properties” window appears.
 - Click on the “General” tab.
 - In the “Name” field, type in the policy name.
 - In the “Encapsulation Protocol” field, type in IPSEC/IKE.
 - Enable the box entitled “Pass Traffic from the Secure Tunnel to the Proxy Services (Required for NAT)”.
 - Now click on the IPSEC/IKE” tab. Set all the fields in this selection according to your corporate security policy.
 - Click on the “Advanced” tab.
 - Make sure that the “Tunnel Mode” is enabled, and that “Perfect Forward Secrecy” is disabled.

NOTE: Certicom handheld VPN Client does not support “perfect forward secrecy”.

Click “OK”.

- From the Management Console, select “Virtual Private Networks”.
- Click on “Secure Tunnel”.
- Select “New” and then “SecureTunnel”. The “New SecureTunnel Properties” window is now displayed.
- Click on the “Description” tab.
- In the “Name” field, type in the description of the tunnel.



- In the “Local Entity” field, type in the network entity describing the private network which has been chosen.
- In the “Local Gateway” field, enter the network entity for the gateway.
- In “Remote Entity”, type in the User group previously created.
- At the bottom, under “VPN Policy”, select the policy previously created for handheld client.
- Click “OK”.

Monitoring Controls

- From the management console, select “Access Controls”.
- Double click on “Address Transform”.
- Double click on “VPN tunnel exit transform”. The “VPN Tunnel Exit Transform Properties” window should now be displayed.
- Click on the “Definition” tab.
- In the “Coming in via” field, select <ANY VPN>
- In the “From Client” field, select “Universe”.
- In the “To Server” field, select “Internal_LAN”.
- In the “Going Out Via” field, select the appropriate network interface.
- Under the “Client Address Transform” section, check off the “Use Gateway Address” box.

NOTE: For more control over client address, consult your VPN documentation for setting up a NAT pool.

Click “OK”.

- On the Raptor Management Console, select “Action”.
- Now select “All Tasks”.
- Finally, select “Save and Reconfigure”.