



movianVPN™

A handheld VPN client specifically designed for mobile and wireless devices

Version 1.1.2
Radguard cIPro Series

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.



Table of Contents

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 RadGuard cIPro Series Gateway

Introduction-	5
<i>The Configuration Process</i>	5
Configuring The Policies To Secure Traffic	7
<i>Setting the Policy Table</i>	7
<i>Selecting the editor settings</i>	8
<i>Activating the Policy Table</i>	8
Adding Clients	9
<i>Setting the Remote Networks</i>	9
<i>Adding Clients</i>	9
<i>Configuring Client Security-</i>	10
Adding Client Groups and Defining Security Policy	11
<i>Selecting the Client Groups</i>	11



<i>Security Policy</i>	-----	12
<i>Group Configurations</i>	-----	13

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 RadGuard cPro Series Gateway

This chapter explains how to configure the RadGuard cPro Series Gateway for use with the **movianVPN**. The following sections are included:

- Introduction
- Configuring the Policy to Secure Traffic
- Adding Clients
- Adding Client Groups and Defining Security Policies

Introduction

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

Before you configure the cPro for use with **movianVPN**:

- Install the RadGuard software on the appropriate computer.
- Set up the default access rules. This includes specifying a name for the default network object, and configuring an IP address and network mask.
- Know the IP address and subnet mask of the VPN.
- Have a list of the names of your users.

The Configuration Process

Configuring the cPro involves setting parameters for:

- Configuring the policy to secure traffic. (By default it will choose all)
- Adding clients
- Adding client groups and defining security policies
- Configuring IPSec and IKE

Note: This chapter only covers the configuration tasks specific to interoperability with **movianVPN**. For detailed configuration information, refer to the *cPro User Guide*.

Configuring The Policies To Secure Traffic

In order to configure new clients and client groups for the cIPro gateway, you must set the policies to be used to secure the transport of information. Configuring these policies involves:

- Setting the Policy Table
- Selecting the editor settings
- activating the Policy Table

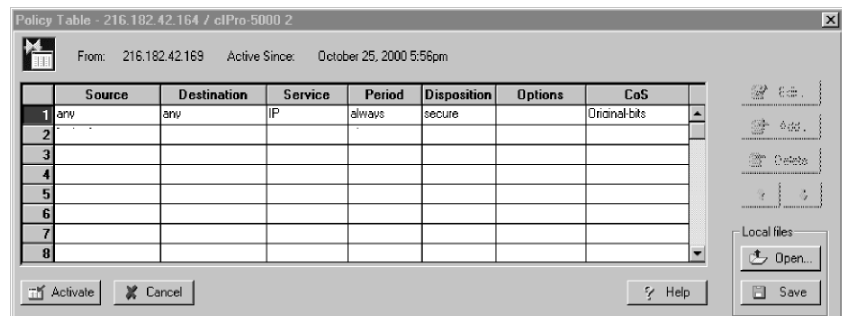
Setting the Policy Table

The policy table sets all the policy requirements necessary to secure traffic.

To set the PolicyTable:



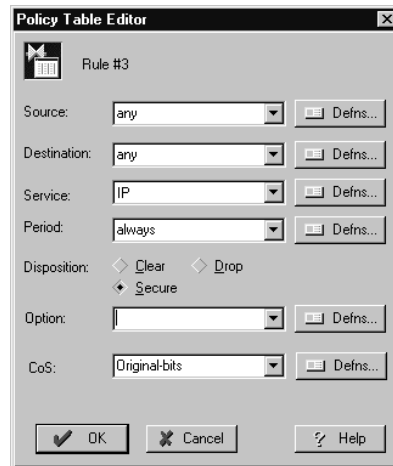
1. Display the RadGuard management program on the appropriate computer.
2. Select **Policies** from the Main menu.
3. From the drop down menu, select **Policy Table**. The Policy table appears.
4. Highlight a line in the table, and click **add**. The Policy Table Editor appears.



Selecting the editor settings

The Policy Table Editor sets all the policy security information for the Policy Table

- In the Editor, set all the rules for the gateway security.
 - In the Source box type a name (or in some cases an IP address).
 - Under Destination, select from the destination drop down box. Select the definition of host that defines destination (normally All).
 - Under Service, select from the service drop down box. this means defining the type of service.



- For Period, select from the period drop down box. Define the time period during which the current rule is effective.
 - In the Disposition box define activity (e.g. secure, clear or drop).
 - The Options selection drop down menu allows for additional criteria for specifying a packet.
 - The COS (Class of Service) supplies an additional selection of 3 options in the COS drop down menu.
- When you have concluded setting all the rules in the editor, click **OK**.
 - The Policy Table will appear, displaying all the information which you set in the editor.

Activating the Policy Table

By activating the Policy Table, you set the policy security for the gateway.

- If you are sure that the information displayed in the Policy Table is correct, click **Activate**.

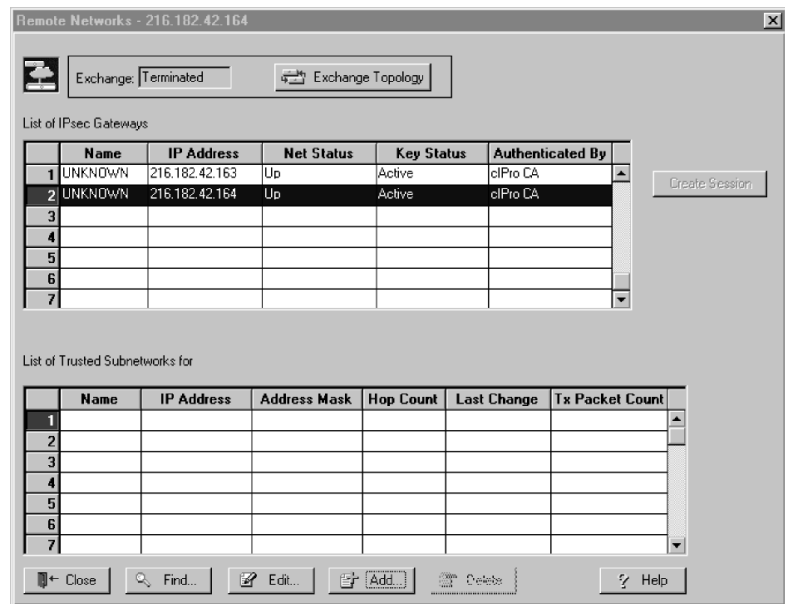
Adding Clients

For users to access the VPN, you must set the remote networks, and then add groups and clients to the system. Adding Clients involves:

- Setting the Remote Networks
- Adding Clients
- Configuring Client Security

Setting the Remote Networks

Setting the Remote Networks table defines the list of IPsec gateways.



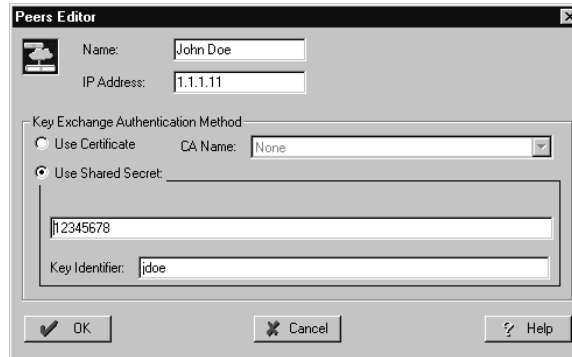
1. From the RadGuard main management menu, select **Network** from the menu.
2. Two windows will be displayed. Select the upper window. Highlight a line in the upper window, and click **Add**. The Peers Editor will appear.

Adding Clients

You can add as many clients as needed.

1. In the Name field type the description or name of the account.

- The IP Address field, in the mode we use this gateway, is not used. However, for this configuration to work there must be some IP entry here, and it has to be unique for each user. (E.g. 2.2.2.2, 2.2.2.3, 2.2.2.4)



Configuring Client Security

- Always select Use Shared Secret.
- Directly below the Use Shared Secret selection, type in the password for the user selected below.
- IN the Key Identifier field, enter the user name. This name must be the same as the user name listed in the remote device (E.g. P.D.A.).
- When you are sure of all the information in the Peers Editor, click OK.

Adding Client Groups and Defining Security Policy

This section defines the client groups configuration and security policy. Certain rules for VPN client access are set here.

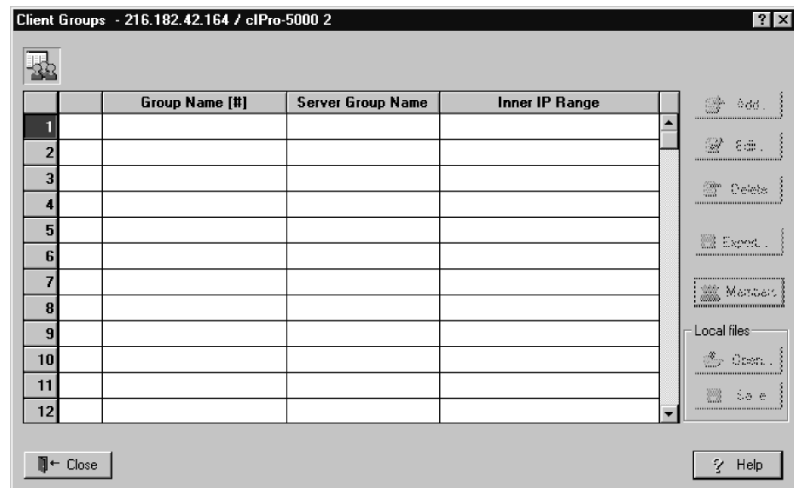
Adding Client Groups involves:

- Selecting the Client Groups
- Security Policy
- Setting the group configurations.

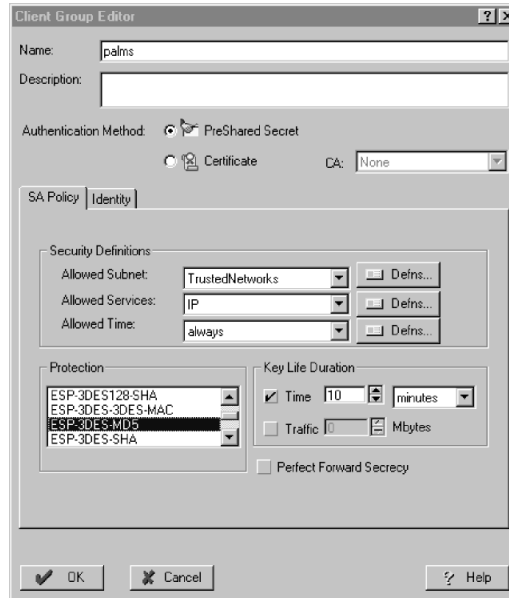
Selecting the Client Groups

The list of client groups and the appropriate authentication method or Certificate Authority are selected here.

1. Return to the RadGuard main management menu, and select Clients from the main menu. From the drop down menu select Client Groups.



2. The Client Groups Display will appear. Highlight a line in the table displayed.
3. Click on **Add** on the Client Groups table. The Client Group Editor is displayed.
 - In the Name field enter the name of the account
 - Select PreShared Secret for Authentication Method.



Security Policy

The security policy selection includes the security definitions, method used for security protection, and the key life duration.

1. Select the SA Policy tab in the Client Security Editor.
 - In the Allowed Subnet field type in the appropriate client subnet.
 - In the Allowed Services field type in IP.
 - In the Allowed Time field type in the allowed time for these security settings.
 - In the Protection field select your appropriate method of security protection.

Note: RadGuard cPro Series gateway only supports 3 DES-MD5 IPsec connection with the Certicom handheld client.

- Under Key Life Duration select Time. Then set the time of the key life.

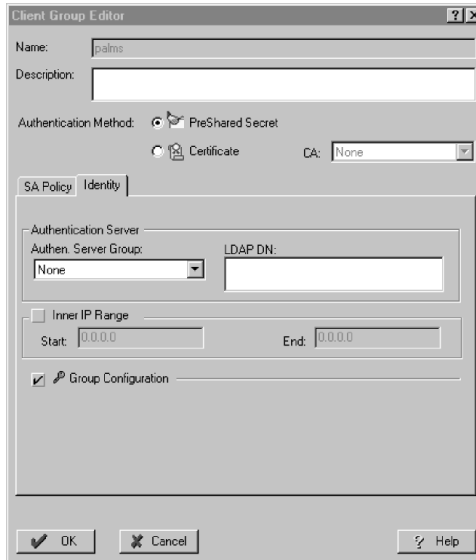
Note: Make sure that Perfect Forward Security is disabled. This is not supported in the Certicom handheld client.

Group Configuration

s

This configuration lists Authentication Server Group, and turns the Group Configuration on or off

1. Select the Identity tab in the Client Group Editor.



The screenshot shows the 'Client Group Editor' dialog box with the following fields and settings:

- Name: palm
- Description: (empty)
- Authentication Method: PreShared Secret, Certificate
- CA: None
- SA Policy: Identity (selected)
- Authentication Server:
 - Authen. Server Group: None
 - LDAP DN: (empty)
- Inner IP Range: (unchecked)
- Start: 0.0.0.0, End: 0.0.0.0
- Group Configuration: (checked)

2. In the Authen Server Group field, select an entry from the pull down menu (E.g. None).
3. Select Group Configuration at the bottom of the Editor. If you are satisfied with all entries, click OK.

Note: RadGuard gateway does not perform any address translations on client IP addresses. This means that any host that you want to connect to in the private network must have a default gateway set to the private IP address of the RadGuard gateway.

