



# movianVPN™

*A handheld VPN client specifically designed for mobile and wireless devices*

**Version 1.1.2**

**Alcatel Secure VPN 7130 Gateway Family**

## **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](http://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 Alcatel Secure VPN 7130 Gateway

Introduction	5
<i>The Configuration Process</i>	5
Configuring The Security Policy	6
<i>Local Security</i>	7
<i>Red Security Network</i> - - - - - (Private Network)	8
Adding Users	9
<i>Adding Users in the Black Security Network (Public Network)</i>	9
Configuring Client Services	10
<i>Building the Security Map</i>	11
Configuring the Alcatel Gateway for use with SecurID RSA ACE/Servers	12
<i>Configuring the SecurID Server</i>	12



---

# 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 Alcatel Secure VPN 7130 Gateway

*This chapter explains how to configure the Alcatel Secure VPN 7130 Gateway Family for use with the **movianVPN**. The following sections are included:*

- Introduction
- Configuring Security Policy
- Adding Users
- Configuring Client Services
- Configuring the Alcatel Gateway for use with SecurID RSA ACE/Servers

---

## Introduction

Alcatel Gateway 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 Alcatel Gateway for use with **movianVPN**:

- Install the Alcatel Gateway software on the appropriate computer.
- Set up the Security Policies to allow the Alcatel Gateway to be compatible with **movianVPN**.
- Know the IP address and subnet mask of the VPN.
- Have a list of the names of your users.

## The Configuration Process

Configuring Alcatel Gateway to work with **movianVPN** involves:

- Configuring the Security Policy
- Adding Users
- Configuring Client Services
- Building a Secure Map

## Configuring The Security Policy

To create a security policy that is compatible with the hand held client, you must go to the `tssecdes.cfg` file, and add the following text:

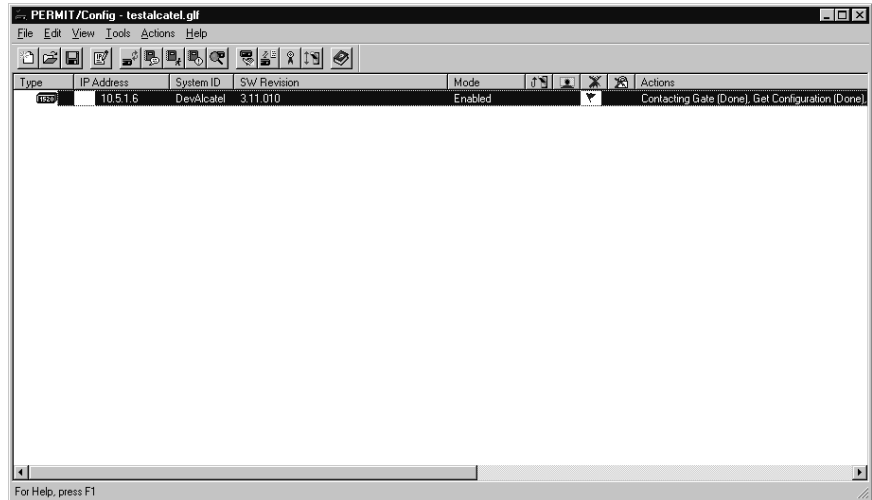
```
begin security-descriptor
  Name    "movianVPN"
  IPsec
  "GROUP 1 ESP DES MINUTES 60
    or ESP DES HMAC SHA MINUTES 60
    or ESP DES HMAC MD5 MINUTES 60
    or ESP 3DES HMAC SHA MINUTES 60
    or ESP 3DES HMAC MD5 MINUTES 60
    or ESP 3DES MINUTES 60
    or ESP DES MINUTES 60
    or ESP NULL HMAC MD5 MINUTES 60
    or ESP NULL HMAC SHA MINUTES 60"
  ISAKMP"
  3DES MD5 MINUTES 60
    or 3DES SHA MINUTES 60
    or DES MD5 MINUTES 60
    or DES SHA MINUTES 60"
end
```

This is an example only. Set up the security policy according to your corporate policy.

---

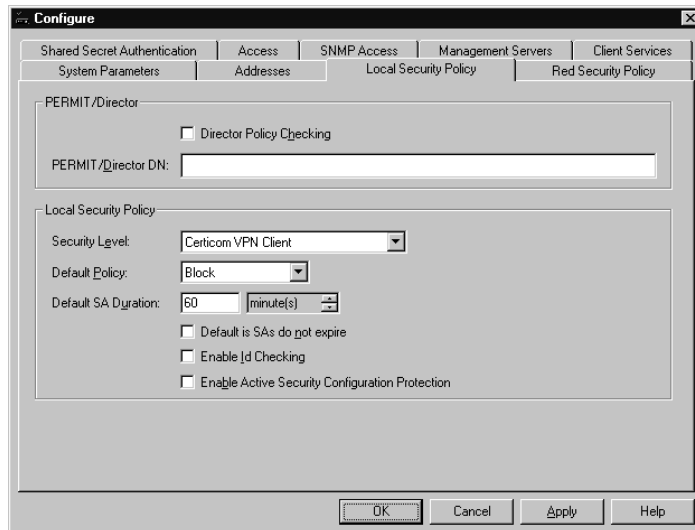
NOTE: Do not use the identity or Perfect Forward Secrecy keywords under your ISAKMP policy. The Certicom handheld client does not recognize Perfect Forward Secrecy, and requires shared secret mode which is incompatible with the keyword. For more information on updating the security descriptor, see your Alcatel Gateway documentation.

---

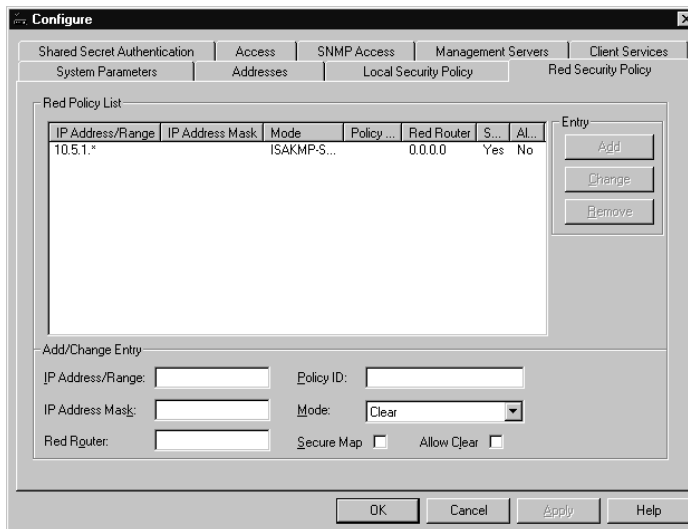


## Local Security

1. Display the PERMIT/Config management program on the appropriate computer.
2. Click on the “Get Configuration” line in the management program to open the Configure window.



3. Once in the Configure window, cClick on the “Local Security Policy” tab.
4. Select “Security Level”.
5. Select the name of the policy from the security descriptor file. (E.g. **movianVPN**).
6. Click “Apply”.



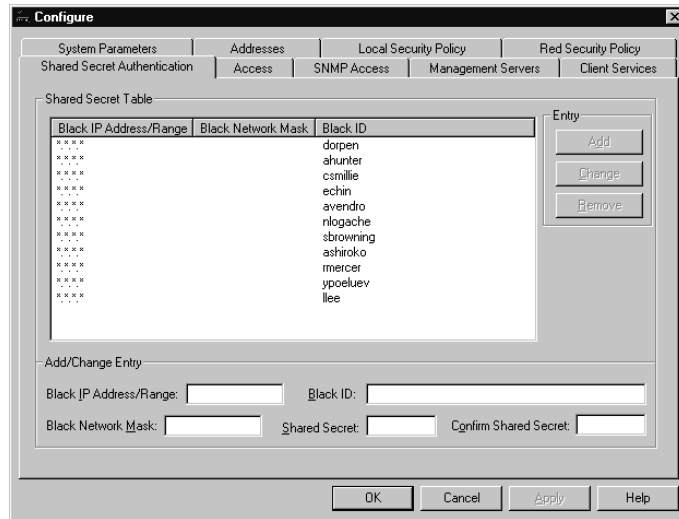
## Red Security Network (Private Network)

1. In using the Configure window to set up the Alcatel gate, the Red Security setting represents the private network. Once the security policy has been set in the Configure windows, click on the “Red Security” tab.
2. Set the “IP Address/Range” to the network address of the subnet you want to access.
3. Select the “IP Address Mask” to set the network mask.
4. Next, set the “Red Router”. If the gateway is not directly connected to the subnet you are configuring, insert the IP address of the router that is connected to the subnet being configured.
5. Set the “Mode” entry to ISAKMP-shared.
6. Finally, enable “Secure Map”.
7. Click “Add”
8. Click “Apply”

## Adding Users

### Adding Users in the Black Security Network (Public Network)

1. In order to add users to Alcatel Gateway, you must have previously set the security policy and security level by selecting both from the Security Descriptor. In this step, the authentication window displays the Black security, or public networks and users.
2. Click on the “Shared Secret Authentication” tab.



3. In the “Black IP Address/Range”, type in the necessary IP address. This could be any IP address.
4. In the “Black ID” space, type in the user name.
5. In the “Shared Secret” space, type in the password.

---

NOTE: The user name and password must be the same as those in the PDA being utilized.

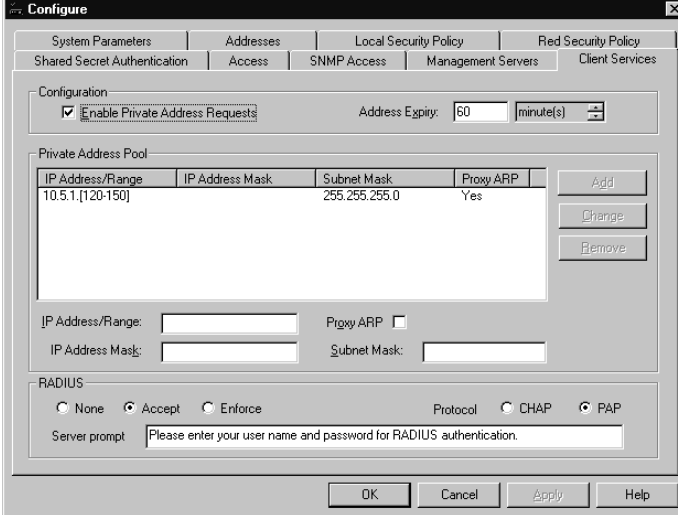
---

6. The “Confirm Shared Secret” field is an exact copy of the “Shared Secret” field. this setting is just a confirmation of the initial shared secret.
7. CLick on the “Add” button.
8. For additional users, repeat all the above steps. After each completion click on the “Add” button.
9. After all users are selected, click on “Apply”.

## Configuring Client Services

The next step is to set up the client services.

1. Click on the “Client Services” tab.
2. Click “Enable Private Address Requests”.



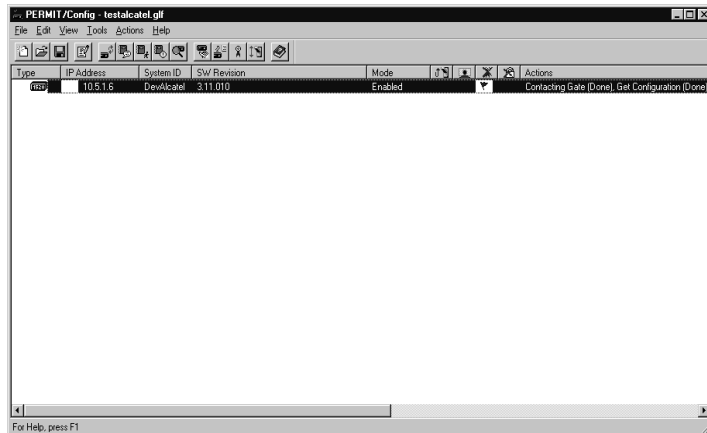
IP Address/Range	IP Address Mask	Subnet Mask	Proxy ARP
10.5.1.[120-150]	255.255.255.0	255.255.255.0	Yes

3. Enter the IP Address/Range. If you wish to enter a private IP address pool, consult your documentation.
4. Click “Apply”.
5. Click “OK”.

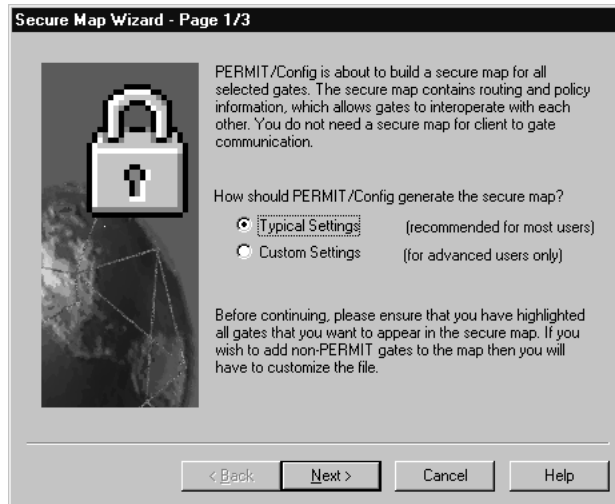


## Building the Security Map

Once you click “OK” at the end of configuring the client services, the PERMIT/Config menu is shown.



1. Once in the PERMIT/Config menu, click on the “Tools” tab.
2. On the pull down menu, Click on “Build Secure Map”.



3. The next screen to appear is the “Secure Map Wizard”.
4. From here, just follow the Secure Map Wizard instructions.

Once all the set-up steps have been followed, and the Secure Map Wizard is completed, the Alcatel Gateway is ready to operate with **movianVPN**.

# Configuring the Alcatel Gateway for use with SecurID RSA ACE/Servers

This section describes how to configure the Alcatel gateway for use with SecurID servers.

## Configuring the SecurID Server

This procedure assumes that you already have a SecurID RSA ACE/Server set up and running. This procedure describes how to configure a SecurID server to recognize the Alcatel gateway as an authentication client.

1. Add the Alcatel gateway to the SecurID host file. If you have a DNS setup on the private network that includes the private IP of the Alcatel gateway, then you may proceed to step 2. To do this:

On the server, change directories to: `WINNT\system32\drivers\etc`

Find the file named **Hosts** (it will have no extension).

In a simple text editor, such as Wordpad, append a line to the file that contains the following information:

```
<Private IP Address of Alcatel Gateway> <tab> <host-name>
```

2. Start the SecurID Administration Tool.
3. Under the New menu item, select Client>AddClient. A dialog box called Add Client will appear. There will be several fields:

Name: Enter the host name or private DNS name of the Alcatel gateway. Hit the tab key to automatically fill in the Network Address field.

Site: You may leave this field blank.

Client Type: Select "Communication Server".

Encryption Type: Select DES. Select the "Open to ALL Locally Known Users" check-box if desired.

4. Once these fields have been filled in, click the Assign/Change Encryption Key button. A dialog called Assign/Change Encryption Key should appear. In the field named Key, type in the server shared-secret (in most cases, the RADIUS password).
5. Click the OK button to close the Assign/Change Encryption Key dialog, and then press OK to close the Add Client dialog.

We suggest you create a test user, or test an existing user after both Server and Gateway have been configured.

## Gateway-side Configuration

The following procedures occur on the Alcatel gateway device



## Adding an Authentication Server

1. Start the PERMIT/Config management program. You will get a list of gateways. Select the gateway you want to configure and then select the Refresh Status command located under the Tools menu item.
2. Double click the gateway you want to configure. The Configure dialog box should appear. Go to the Management Servers section. There will be several fields.
3. In the IP Address field, type in the IP address of the SecurID server.
4. In the Port Number field, type in the Radius port number (1645), or other applicable port number.
5. Under the Server Type field, select RADIUS Authentication Server.
6. Under the Priority field select 1 (unless you are adding a secondary server).
7. Select the Enabled and Proxy checkboxes.
8. Click the Add button. You should be prompted for the Radius sever secret.
9. Click the Client Servers tab.
10. Under the RADIUS heading, there is an Accept pull-down menu. Select either **PAP** or **CHAP**. Enter the desired end-user prompt in the Server Prompt field.

## Adding a Common Radius user

You will want to add a new user called "Radius." Users who authenticate with SecurID can use this user. This user can be added under the Shared Secret Authentication tab.

