



# **Certicom Handheld VPN Client**

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

**Version 0.6.3**

## **User's Guide**

**(Windows CE/Pocket PC Edition)**

---

The *VPN Client User's Guide* describes how to install, configure, and use the Certicom **VPN Client**.

Also provided with the **VPN Client** is the *Server Configuration Guide*. Aimed at VPN administrators, this guide explains how to configure various VPN servers for use with the the Certicom **VPN Client**.

### **Technical Support**

You can reach Certicom's technical support department by telephone at 1-800-511-8011, by fax at 1-800-474-3877, or by email at [vpn.support@certicom.com](mailto:vpn.support@certicom.com).

### Copyright Notice

© Certicom Corp., 2000. All rights reserved. This documentation contains proprietary information of Certicom and distribution is limited to authorized licensees of Certicom. Any unauthorized reproduction or distribution of this document is strictly prohibited.

Certicom, the Certicom logo, and Certicom Handheld VPN Client are trademarks of Certicom Corp. Certicom Handheld VPN Client 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 patent protection pending.

---

## Introduction

Network Security Basics	1
<i>Virtual Private Networks</i>	1
<i>IPSec</i>	3
<i>Internet Key Exchange</i>	3
Overview of the Certicom Handheld VPN Client	4
<i>How the Client Works</i>	4
<i>Features and Benefits</i>	4
<i>Coming Soon</i>	5
Structure of this Manual	6

## Installation

Overview	7
System Requirements	8
Installing the VPN Client	9
<i>Performing a Manual Installation</i>	10
Uninstalling the VPN Client	12

## Configuring the VPN Client

Basic Configuration	13
<i>Editing Modem Settings</i>	14

---

Configuring the IPSec Security Policy Database	17
<i>Configuring a Connection to Check Point VPN-1</i>	18
<i>Configuring a Connection to the VPN Concentrator</i>	21
<i>Configuring a Connection to the Nortel Contivity</i>	23
<i>Completing Configuration</i>	25
Managing Connections	26
<i>Editing Connection Settings</i>	26
<i>Deleting Connection Settings</i>	26
<i>Editing the Security Policy Database</i>	27
<i>Deleting a Security Policy Database Entry</i>	27

## **Using the VPN Client**

Introduction	29
Connecting to Your ISP	30
Creating a Secure Connection to a VPN	31
Logging Off	32

## **Troubleshooting the VPN Client**

Configuring the VPN Client	33
Using the VPN Client	34
<i>Starting the VPN Client</i>	34

---

*Connecting to a VPN* - - - - - **34**

Other Problems - - - - - **39**

## **Supported Hardware**

Introduction - - - - - **41**

## **Overview of Wireless Networking**

Introduction - - - - - **43**

Types of Wireless Networks - - - - - **44**

## **Glossary**



---

# 1 Introduction

*This chapter is an overview of the Certicom Handheld VPN Client and of network security. This chapter also introduces the concepts of network security, Virtual Private Networks, and IPSec. The following sections are included:*

- *Network Security Basics*
- *Overview of the Certicom Handheld VPN Client*
- *Structure of this Manual*

---

## Network Security Basics

Without a security framework, the standard Internet Protocol (IP) is far too insecure for transmitting confidential traffic. Information that travels over an unprotected IP channel is vulnerable to numerous attacks, including interception, sniffing, spoofing, etc. As well, there is no mechanism for non-repudiation of transmitted information. These principles apply not only to network connections made with desktop PCs, but also when mobile devices like Personal Digital Assistants (PDAs) are added to networks.

In a world of wired and wireless communication and commerce, efficient network security is vital. One of the best ways to secure network traffic is with a Virtual Private Network.

## Virtual Private Networks

A Virtual Private Network (VPN) is a set of individual network sites that sit on top of the Internet. A VPN secures the exchange of data using IP, which ensures that private traffic between the sites in the network is not susceptible to attacks.

The advantages of a VPN include:

- Provides an efficient and inexpensive way of increasing the breadth of a corporate network.
- Ensures the secure exchange of data between corporate headquarters and employees in the field.
- Enables the transmission of confidential data securely using shared links.

Over the last few years, corporate investments in VPNs have grown dramatically. The proliferation of VPNs and mobile devices like PDAs used to access corporate

data is forcing the convergence of these two technologies. To leverage the investment in VPNs and to extend sufficient protection to mobile users, network administrators must include mobile devices in their corporate security plans.

The following diagram illustrates a connection to a VPN using mobile and wireless devices:

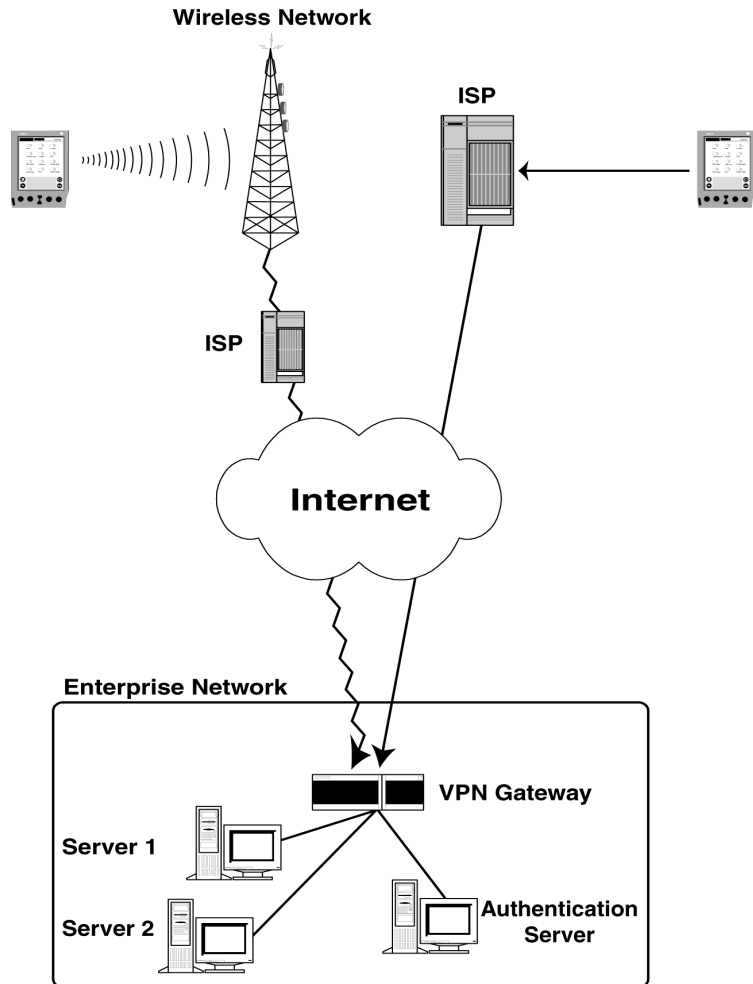


FIGURE 1. Connecting to a VPN with mobile/wireless devices

All data passing through a VPN travels over a secure route called an *encrypted IP tunnel*. A firewall surrounding each site in the network adds further protection. When information leaves a site, the VPN encrypts the data packet. When

information comes from a remote user, the VPN decrypts the packet, and then routes the packet to its destination within the network.

The engines used to provide security are *IPSec* and *Internet Key Exchange*.

## IPSec

IPSec is an IP security protocol defined by the Internet Engineering Task Force, and is the basis for securing a VPN. IPSec is a set of security standards for online communications that ensures data travelling across a network is secure, confidential, and authentic. An IPSec implementation operates on a host computer, or in a security gateway in conjunction with a network firewall.

Two protocols form the basis of IPSec:

- **Authentication Header (AH)**, which is designed to ensure the integrity of the information being sent, and authenticate its origin. AH only provides authentication. It does not provide privacy.
- **Encapsulating Security Payload (ESP)**, which performs the same functions as the Authentication Header. ESP also provides privacy by encrypting data, and provides protection to the traffic flow.

Central to IPSec is a Security Association (SA). An SA is a simple connection over which security services can travel. The SA is identified by a combination of the IP destination address, and either the Authentication Header or Encapsulated Security Payload. When an SA exists, the sender and receiver hold the algorithm and keys needed to authenticate a message. The algorithm and keys are not included in the authentication header.

## Internet Key Exchange

Internet Key Exchange (IKE) is the IPSec security infrastructure. IKE authenticates endpoints and negotiates encryption keys. It also negotiates the security protocols and algorithms between a remote user and a VPN.

When you access a VPN, the system confirms your identity and determines how to encrypt communications. There are two authentication modes.

- **Main mode**, which only reveals your identity once secure communication is established. This is a secure, but slow method of authentication.
- **Aggressive mode**, which reveals your identity before secure communication is established. Aggressive mode is faster than Main mode, and is the preferred mode for IKE.

There are various mechanisms to authenticate users at the VPN gateway. Popular authentication mechanisms include user name and password, digital certificates, SecureID, and smart cards.

## Overview of the Certicom Handheld VPN Client

The Certicom **Handheld VPN Client** is a fully configurable GUI-based application that runs on PDAs running the Palm™ and PocketPC platforms. You can use it to securely connect to a VPN over a wired or wireless connection with a handheld device. With the **VPN Client**, 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 the **VPN Client**, you can connect to a VPN via a wireless network that supports data services 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 the **VPN Client**. The **VPN Client** then decrypts the message. Note that this is a two-way process — any information you send using the **VPN Client** is encrypted before it reaches the tunnel, and is decrypted by the VPN gateway.

Once connected, you can use the software on your PDA 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

The **VPN Client** 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.
- Interoperability with popular VPN systems, including Check Point VPN-1, the Cisco VPN Concentrator 3000 Series family and the Nortel Contivity Extranet Switch.
- Use of an IKE-based IPSec protocol.
- Operates on Windows CE/Pocket PC devices.

## Coming Soon

Future releases of the VPN Client will feature:

- Interoperability with a wider range of VPN servers, including gateways from Alcatel, AXENT Technologies, Enterasys Networks, and Spring Tide Networks.
- Support for handheld computers running EPOC from Symbian.
- Split tunnelling capability, which allows users to browse the World Wide Web without disabling or closing down a secure connection to a VPN.
- Connection authentication using X.509 certificates.
- Support for RSA encryption and signatures.
- A mechanism for automatically updating the VPN Client by connecting to a dedicated Certicom Web site.
- Additional authentication mechanisms, such as SecurID, smart cards, tokens, etc.
- Security policy management capabilities.
- An online Help system.

## Structure of this Manual

The *VPN Client User's Guide* is divided into five chapters and three appendices:

- Chapter 1, **Introduction**, offers an overview of network security basics and introduces the **VPN Client**.
- Chapter 2, **Installation**, explains how to install, uninstall, and start the **VPN Client**.
- Chapter 3, **Configuring the VPN Client**, discusses how to add connection settings, configure the security policy database for each supported VPN, and how to manage connections.
- Chapter 4, **Using the VPN Client**, explains how to connect to, and disconnect from, a VPN.
- Chapter 5, **Troubleshooting**, covers solutions to common problems you may encounter while using the **VPN Client**.
- Appendix A, **Supported Hardware**, lists the Windows CE and Pocket PC devices that can run the **VPN Client**.
- Appendix B, **Overview of Wireless Networking**, offers a brief introduction to wireless networks and how they work.
- Appendix C, **Glossary**, defines the terms used throughout this manual.

---

# 2 Installation

*This chapter explains how to install the VPN Client on your Pocket PC device. The following sections are included:*

- *Overview*
- *System Requirements*
- *Installing the VPN Client*
- *Uninstalling the VPN Client*

---

## Overview

The VPN Client is distributed in an archive named **Handheld\_VPN\_CE\_01\_b00xxxx.zip**, where **xxxx** is the release date of the current version. For example, **1230**.

The distribution contains the following:

- The VPN Client files for installation on your Windows CE or Pocket PC handheld.
- The documentation for the VPN Client.
- A beta program feedback form.
- A program to install these files on to your hard drive.

## System Requirements

To install and run the **VPN Client**, it is recommended that your desktop computer and Windows CE device have the following minimum configurations:

Computer	Processor Speed	Operating System	Other
Desktop PC	200 Mhz	Windows 95/98/ NT/2000	Under 2 Mb of hard drive space for installation
Windows CE/ Pocket PC device	n/a	Windows CE	Under 200 Kb of memory

You will also need a copy of Microsoft ActiveSync 3.1 installed on your desktop computer, which comes with all Windows CE/Pocket PC devices. You can also download it from <http://www.microsoft.com/pocketpc/>.

The **VPN Client** operates on the following handhelds and Pocket PC devices running Windows CE. For a list of supported hardware, see Appendix A.

To connect to a VPN, you need:

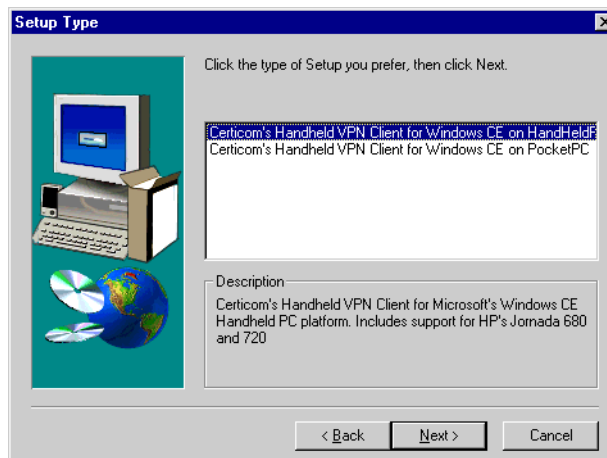
- For a connection over a land line, a compatible serial modem.
- For a wireless connection, a supported mobile phone and appropriate hardware, or a compatible wireless modem.
- An account with an Internet Service Provider and/or a wireless data provider.

## Installing the VPN Client

Before you begin the installation process, ensure that your device is connected to your desktop PC either via a serial cable or the device's USB docking cradle.

To install the VPN Client:

1. Extract the files from the **VPN Client** distribution to a temporary directory using a tool like WinZip™.
2. On the Task Bar, click the **Start** button then click **Run**. The Run dialog appears.
3. In the **Open** field, type:  
`<x>:\<path>\Setup.exe`  
 where <x>:\<path> is the drive and folder into which you extracted the installation files.
4. Click **OK**. The Certicom Handheld VPN Client installation screen appears. Click **Next**.
5. The license agreement appears. Click **Yes**.
6. The following dialog appears:



From the list, choose the appropriate version of the **VPN Client** to install. These are:

- Windows CE handheld PCs.
  - Windows CE/Pocket PC devices.
7. Click **Next**. On the dialog that appears, select the directory into which you want to install the files. By default, the setup program installs the **VPN Client** support files in the following directory:

C:\Program Files\Certicom\Handheld VPN\WinCE\

You can:

- Click **Next** to accept the default directory.
  - Click **Browse** to choose a new directory from the dialog that appears. When you have chosen a directory, close the dialog.
8. Click **Next**. The files are installed on your hard drive. Once this process is complete, the setup program starts the ActiveSync software (used to synchronize you device and your desktop PC) and installs the **VPN Client** files on your device.

The installation program also creates the following folders on your PC:

- **WinCE**, containing the **VPN Client** program files.
  - **Documentation**, containing this guide and the server configuration guide in Adobe Acrobat PDF format.
  - **Feedback**, containing a beta program feedback form in Microsoft Word format.
9. A dialog informing you that installation is complete appears. Click **Finish** to close the dialog.

## Performing a Manual Installation

The **VPN Client** installation program checks for ActiveSync in its default directory (C:\Program Files\Microsoft ActiveSync\). If the installation cannot find ActiveSync, you must perform a manual installation. This involves specifying the path to the ActiveSync application manager (CEAppMgr.exe) and the initialization file required to install the **VPN Client** (VPNclient.ini).

To manually install the **VPN Client**:

1. Determine the drive and folder in which your copy of ActiveSync is installed.
2. On the Task Bar, click the **Start** button then click **Run**. The Run dialog appears.
3. In the **Open** field, type:

<x>:\<path to CEAppMgr.exe>\<path to VPNclient.ini>

where:

- <x>:\ is the drive on which ActiveSync is installed. For example, D:\.
- <path to CEAppMgr.exe> points to the program CEAppMgr.exe. For example Program Files\Microsoft ActiveSync\CEAppMgr.
- <path to VPNclient.ini> points to the initialization file required to install the **VPN Client**. This file will be in the folder which you specified in step 7 above. For example C:\Program Files\Certicom\Handheld VPN\WinCE\VPNclient.ini.

For example, you can type the following in the **Open** field: **"D: \Program**

`Files\Microsoft ActiveSync\CEAppMgr" C:\Program  
Files\Certicom\HandHeld VPN\WinCE\VPNClient.ini`

The path to your ActiveSync software must be surrounded by quotation marks.

4. Click OK. The ActiveSync application manager starts and automatically installs the VPN Client.

## Uninstalling the VPN Client

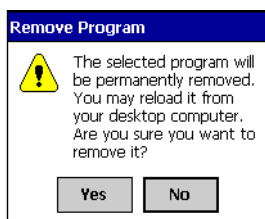
Your Pocket PC device has an automated procedure to uninstall the **VPN Client** program files and libraries.

To uninstall the VPN Client:

1. Tap the Start Menu and select **Settings**. The Settings screen appears.
2. Tap the **System** tab, then tap **Remove Programs** icon. The Remove Programs screen appears.



3. In the list of applications, tap **VPN Client**, then tap **Remove**. The following warning message appears:



4. Tap **Yes**. The **VPN Client** is removed from your device.

---

# 3 Configuring the VPN Client

*This chapter explains how to configure the VPN Client. The following sections are included:*

- *Basic Configuration*
- *Configuring the IPSec Security Policy Database*
- *Managing Connections*

---

## Basic Configuration

Basic configuration of the VPN Client involves setting up:

- Modem settings.
- A server IP address.
- A user name and password.
- A name and value for the pre-shared key.
- A name and password for your user group on the VPN.
- An IP address and subnet mask for the target VPN.

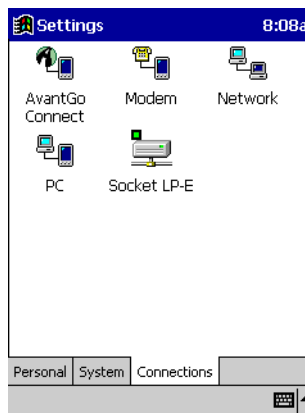
You can perform all basic configuration tasks within the VPN Client GUI.

## Editing Modem Settings

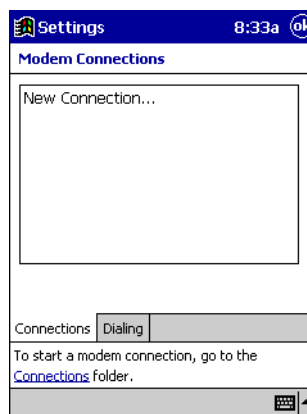
The modem settings control the type of modem you use, and the speed at which the connection is made.

To edit the modem settings:

1. Choose **Settings** from the Start menu, then tap the **Connections** tab. The connection settings screen appears.



2. Tap **Modem**. The Modem Connection screen appears.



3. Tap **New Connection...** The Make New Connection screen appears.

4. Using the keyboard or your handwriting recognition software, input a name for this connection in the **Enter a name for the connection** field.
5. Choose your modem from the **Select a modem** pick list.

**Note:** If you have a plug and play modem, make sure it is attached to your device before configuring the modem settings. If the modem is not attached, it will not appear in the modem list.

6. Select a connection speed from the **Baud Rate** pick list (maximum 19,200 bps).
7. Tap **Next**. The following screen appears.

8. Enter the area code and phone number of your Internet Service Provider in the appropriate fields.
9. Tap **Next**. The following screen appears.



10. Make any changes to the settings on this screen, then tap **Finish**.

## Configuring the IPsec Security Policy Database

The Security Policy Database (SPD) contains a list of entries that determine what security policies are applied to traffic in an encrypted IP tunnel. A security policy is a set of rule rules determining what data can move in and out of the VPN, and when remote users can access the system. The **VPN Client** consults the SPD each time it negotiates a new security association with a VPN, and uses the SPD to determine which traffic to protect with IPsec.

You configure the SPD using one of three templates. Each template is a form containing connection and security information for a VPN. You enter the appropriate information into the fields of the form, and only change that information when the VPN administrator modifies the security parameters of the system.

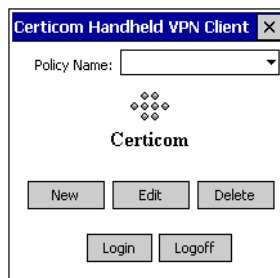
---

**Note:** Contact your VPN administrator for the information required to configure the SPD.

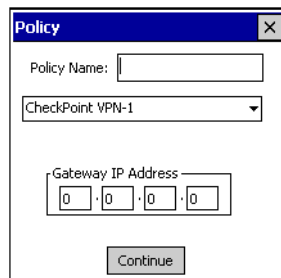
---

To configure the IPsec SPD:

1. Select **VPN Client** from the Start menu. The **VPN Client** main screen appears.



2. Tap **New**. The Policy Entry screen appears.

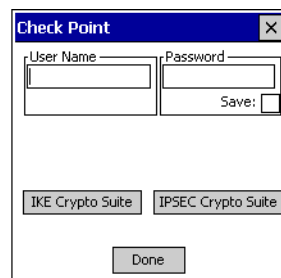


3. Enter a name for this policy in the **Policy Name** field. For example, VPN Access.
4. Select the VPN to which you want to connect from the pick list. Currently supported VPN gateways are:
  - Check Point VPN-1
  - Cisco VPN Concentrator
  - Nortel Contivity
5. Enter the IP address of the system to which you will connect in the **Gateway IP Address** field.
6. Tap **Continue**. The contents of the next screen will depend on the option you chose from the **Gateway Type** pick list.

From here, you can configure the **VPN Client** to work with the VPN gateway to which you are connecting.

## Configuring a Connection to Check Point VPN-1

1. If you chose **Check Point VPN-1** from the pick list of gateway types, the following screen appears:



2. Enter the appropriate information in the following fields:
  - **User Name**—the user name required to log into the VPN.
  - **Password**—the password required to log into the VPN (maximum 40

characters). Check the **Save** option to have the **VPN Client** remember the password. If you do not specify a password, you will be prompted for your password each time you log in.

3. Tap **IKE Crypto Suite** to select the level of cryptography to use during an IKE session. The following screen appears:



4. Select one of the following Diffie-Hellman groups (used to establish an encryption key for a communication session) from the **Group** pick list. The groups are listed from least secure to most secure:
  - **GRP 1\_DH-768**—generates an IPsec security association key using 768-bit numbers. Select this group if the VPN uses DES-56 as the encryption algorithm.
  - **GRP2\_DH-1024**—generates an IPsec security association key using 1024-bit numbers. Select this group if the VPN uses 3DES-128 as the encryption algorithm.
  - **GRP7\_ECDH-163**—a Certicom-implemented group that uses a combination of Diffie-Hellman and a 163-bit Elliptic Curve Cryptosystem (ECC) algorithm. ECC provides superior encryption, and is quickly generated on a handheld device.
5. Select one of the following encryption ciphers from the **Cipher** pick list:
  - **DES\_CBC**—DES encryption with cipher block chaining (in which previously-encrypted blocks modify the encryption of subsequent blocks).
  - **3DES\_CBC**—Triple DES encryption with cipher block chaining (in which previously-encrypted blocks modify the encryption of subsequent blocks).
6. Select one of the following hashing algorithms to ensure data integrity from the **Hash** pick list:
  - **MD5**—use the MD5 one-way hashing algorithm.
  - **SHA**—use the Secure Hash Algorithm, which generates 160-bit output, giving it added security.
7. Tap **Continue** to save the changes.

8. Tap **IPSec Crypto Suite** to select the level of cryptography to use for the IPSec connection. The following screen appears:



9. Select one of the following IPSec suites from the **Suite** pick list:
- **ESPIP\_NULL\_MD5-96**—the IPSec connection is not encrypted, but 96-bit MD5 is used for data integrity.
  - **ESPIP\_NULL\_SHA-96**—the IPSec connection is not encrypted, but 96-bit SHA-1 is used for data integrity.
  - **ESPIP\_DES\_NULL**—the connection is encrypted using DES, with no data integrity.
  - **ESPIP\_DES\_MD5-96**—the IPSec connection will be encrypted using DES with 96-bit MD5 for data integrity.
  - **ESPIP\_DES\_SHA-96**—the IPSec connection will be encrypted using DES with 96-bit SHA-1 for data integrity.
  - **ESPIP\_3DES\_NULL**—the connection is encrypted using Triple DES, with no data integrity.
  - **ESPIP\_3DES\_MD5-96**—the IPSec connection will be encrypted using Triple DES with 96-bit MD5 for data integrity.
  - **ESPIP\_3DES\_SHA-96**—the IPSec connection will be encrypted using Triple DES with 96-bit SHA-1 for data integrity.
10. Tap **Continue** to save the changes.

For instructions on how to finish configuring the **VPN Client**, see page 25.

## Configuring a Connection to the VPN Concentrator

1. If you chose **Cisco VPN Concentrator** from the pick list of gateway types, the following screen appears:

The screenshot shows a window titled "Altiga" with the following fields and controls:

- User Name**: A text input field.
- Password**: A text input field with a **Save:** checkbox to its right.
- Group Name**: A text input field.
- Group Password**: A text input field with a **Save:** checkbox to its right.
- IKE Crypto Suite**: A button.
- IPSEC Crypto Suite**: A button.
- Done**: A button at the bottom center.

2. Enter the appropriate information in the following fields:
  - **User Name**—the user name required to log into the VPN.
  - **Password**—the password required to log into the VPN (maximum 40 characters). Check the **Save** option to have the **VPN Client** remember the password. If you do not specify a password, you will be prompted for your password each time you log in.
  - **Group Name**—the name of the user group to which you belong. Contact your VPN administrator for this information.
  - **Group Password**—the password of the user group to which you belong. Check the **Save** option to have the **VPN Client** remember the password. If you do not specify a group password, you will be prompted for the password each time you log in. Contact your VPN administrator for this information.
3. Tap **IKE Crypto Suite** to select the level of cryptography to use during an IKE session. The following screen appears:

The screenshot shows a window titled "IKE Crypto Suite" with the following fields and controls:

- Group**: A dropdown menu with "GRP1\_DH-768" selected.
- Cipher**: A dropdown menu with "3DES\_CBC" selected.
- Hash**: A dropdown menu with "MD5" selected.
- Continue**: A button at the bottom center.

4. Select one of the following Diffie-Hellman groups (used to establish an encryption key for a communication session) from the **Group** pick list. The groups are listed from least secure to most secure:
  - **GRP 1\_DH-768**—generates an IPsec security association key using 768-bit numbers. Select this group if the VPN uses DES-56 as the encryption algorithm.

- **GRP2\_DH-1024**—generates an IPSec security association key using 1024-bit numbers. Select this group if the VPN uses 3DES-128 as the encryption algorithm.
  - **GRP7\_ECDH-163**—a Certicom-implemented group that uses a combination of Diffie-Hellman and a 163-bit Elliptic Curve Cryptosystem (ECC) algorithm. ECC provides superior encryption, and is quickly generated on a handheld device.
5. Select one of the following encryption ciphers from the **Cipher** pick list:
    - **DES\_CBC**—DES encryption with cipher block chaining (in which previously-encrypted blocks modify the encryption of subsequent blocks).
    - **3DES\_CBC**—Triple DES encryption with cipher block chaining (in which previously-encrypted blocks modify the encryption of subsequent blocks).
  6. Select one of the following hashing algorithms to ensure data integrity from the **Hash** pick list:
    - **MD5**—use the MD5 one-way hashing algorithm.
    - **SHA**—use the Secure Hash Algorithm, which generates 160-bit output, giving it added security
  7. Tap **IPSec Crypto Suite** to select the level of cryptography to use for the IPSec connection. The following screen appears:



8. Select one of the following IPSec suites from the **Suite** pick list:
  - **ESPIP\_NULL\_MD5-96**—the IPSec connection is not encrypted, but 96-bit MD5 is used for data integrity.
  - **ESPIP\_NULL\_SHA-96**—the IPSec connection is not encrypted, but 96-bit SHA-1 is used for data integrity.
  - **ESPIP\_DES\_NULL**—the connection is encrypted using DES, with no data integrity.
  - **ESPIP\_DES\_MD5-96**—the IPSec connection will be encrypted using DES with 96-bit MD5 for data integrity.
  - **ESPIP\_DES\_SHA-96**—the IPSec connection will be encrypted using DES with 96-bit SHA-1 for data integrity.
  - **ESPIP\_3DES\_NULL**—the connection is encrypted using Triple DES, with no data integrity.
  - **ESPIP\_3DES\_MD5-96**—the IPSec connection will be encrypted using

Triple DES with 96-bit MD5 for data integrity.

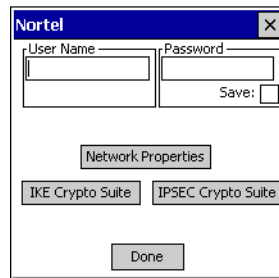
- **ESPIP\_3DES\_SHA-96**—the IPSec connection will be encrypted using Triple DES with 96-bit SHA-1 for data integrity.

9. Tap **Continue** to save the changes.

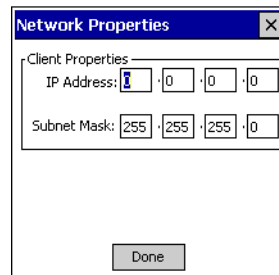
For instructions on how to finish configuring the **VPN Client**, see page 25.

## Configuring a Connection to the Nortel Contivity

1. If you chose **Nortel Contivity** from the from the pick list of gateway types, the following screen appears:



2. Enter the appropriate information in the following fields:
  - **User Name**—the user name required to log into the VPN.
  - **Password**—tap the button to enter the password required to log into the VPN (maximum 40 characters). Check the **Save** option to have the **VPN Client** remember the password. If you do not specify a password, you will be prompted for your password each time you log in.
3. Tap **Network Properties**. The following screen appears:



Enter the appropriate information in the following fields:

- **IP Address**—the IP address of your **VPN Client**. Contact your VPN administrator for this address.
- **Subnet Mask**—the subnet mask of your **VPN Client**. The default is 255.255.255.0, a commonly-used subnet mask. Check with your VPN administrator if you are unsure of the VPN subnet mask.

4. Tap **Done** to close the screen.
5. Tap **IKE Crypto Suite** to select the level of cryptography to use during an IKE session. The following screen appears:



6. Select one of the following Diffie-Hellman groups (used to establish an encryption key for a communication session) from the **Group** pick list. The groups are listed from least secure to most secure:
  - **GRP 1\_DH-768**—generates an IPSec security association key using 768-bit numbers. Select this group if the VPN uses DES-56 as the encryption algorithm.
  - **GRP2\_DH-1024**—generates an IPSec security association key using 1024-bit numbers. Select this group if the VPN uses 3DES-128 as the encryption algorithm.
  - **GRP7\_ECDH-163**—a Certicom-implemented group that uses a combination of Diffie-Hellman and a 163-bit Elliptic Curve Cryptosystem (ECC) algorithm. ECC provides superior encryption, and is quickly generated on a handheld device.
7. Select one of the following encryption ciphers from the **Cipher** pick list:
  - **DES\_CBC**—DES encryption with cipher block chaining (in which previously-encrypted blocks modify the encryption of subsequent blocks).
  - **3DES\_CBC**—Triple DES encryption with cipher block chaining (in which previously-encrypted blocks modify the encryption of subsequent blocks).
8. Select one of the following hashing algorithms to ensure data integrity from the **Hash** pick list:
  - **MD5**—use the MD5 one-way hashing algorithm.
  - **SHA**—use the Secure Hash Algorithm, which generates 160-bit output, giving it added security

9. Tap **IPsec Crypto Suite** to select the level of cryptography to use for the IPsec connection. The following screen appears:



10. Select one of the following IPsec suites from the **Suite** pick list:
  - **ESPIP\_NULL\_MD5-96**—the IPsec connection is not encrypted, but 96-bit MD5 is used for data integrity.
  - **ESPIP\_NULL\_SHA-96**—the IPsec connection is not encrypted, but 96-bit SHA-1 is used for data integrity.
  - **ESPIP\_DES\_NULL**—the connection is encrypted using DES, with no data integrity.
  - **ESPIP\_DES\_MD5-96**—the IPsec connection will be encrypted using DES with 96-bit MD5 for data integrity.
  - **ESPIP\_DES\_SHA-96**—the IPsec connection will be encrypted using DES with 96-bit SHA-1 for data integrity.
  - **ESPIP\_3DES\_NULL**—the connection is encrypted using Triple DES, with no data integrity.
  - **ESPIP\_3DES\_MD5-96**—the IPsec connection will be encrypted using Triple DES with 96-bit MD5 for data integrity.
  - **ESPIP\_3DES\_SHA-96**—the IPsec connection will be encrypted using Triple DES with 96-bit SHA-1 for data integrity.
11. Tap **Continue** to save the changes.

For instructions on how to finish configuring the **VPN Client**, see below.

## Completing Configuration

1. Tap **Done** on the VPN configuration screen to save the configuration. You are returned to the main screen.
2. Tap the Close button in the top-right corner of the screen to exit the program, or tap **Login** to connect to the VPN.

---

**Note:** To make subsequent changes to the SPD, choose the policy to edit on the main **VPN Client** screen, tap **Edit**, and follow the above steps.

---