Release Notes for Check Point® VPN-1 SecureClient for Pocket PC 2003 (build 0131)

January 2004

In This Document:

IMPORTANT
Check Point recommends that customers stay up-to-date with the latest service packs and versions of security products, as they contain security enhancements and protection against new and changing attacks.

IMPORTANT
Before you begin installation, read the latest available version of these release notes at:
http://www.checkpoint.com/techsupport/downloads.jsp

Introduction

Check Point VPN-1 SecureClient for Pocket PC 2003 is based on SecureClient 4.1 SP5. SecureClient for Pocket PC 2003 contains the SecuRemote VPN capabilities of Authentication and Encryption, and additionally functions as corporate desktop FireWall, enforcing a Security Policy configured by the system administrator.

The user experience is very much the same as in the Desktop version. There have been some modifications to adapt the product to suit the Pocket PC 2003 environment (e.g., smaller display resources, smaller memory consumption, etc).

PKCS#12 certificates can be used for authentication.

Note - This release is only for the Windows Mobile 2003 based Pocket PC.

Supported Configuration

Processor

- Intel StrongARM processor family
- Intel® PXA250 XScale Applications Processor family

Tested Devices

The following devices are supported:

- HP/Compaq iPAQ Pocket PC 2003 - series 4150,4350,3950,5450, 5550, 2210,
- Dell AXIM X5 Pocket PC 2003

Versions supported (but not tested) on the following platforms:

- Other devices running Pocket PC 2003, Operating System on Intel StrongArm SA1110 processor
- Other devices running Pocket PC 2003, Operating System on Intel® PXA250 XScale Applications Processor

Devices Not Supported

- All HTC Himalaya models (XDA II, MDA II, Qtek 2020, i-Mate, Orange SPV1000)
- HP/Compaq iPAQ 5500 with Pocket PC 2003 ROM upgrade

Tested Communication Cards

- TRENDNet TE-CF100 10/100MBps CompactFlash Fast Ethernet Adapter
- Socket Communications CF Wireless LAN Card
- Linksys WCF 12
- Sierra AirCard 750
- Sierra AirCard 555
- SanDisk Connect Wi-Fi SD Card

- Socket Communications CF Bluetooth Adapter
- Socket Communications Serial Adapter

Supported Features

The following section outlines many of the familiar features that are supported in Pocket PC 2003 SecureClient. These features are listed because of their importance and/or because their implementation in the Pocket PC 2003 SecureClient is somewhat different from their implementation in the SecureClient Desktop version.

1. MEP (Multiple Entry Point). The client supports MEP in the full overlap, proper subset and backup gateways configurations (see the *VPN-1 Administrator's Guide* for version 4.1).
2. UDP encapsulation. The client supports UDP encapsulation for NAT device traversal of IPSec.
3. Split DNS & Encrypted DNS. Same as in Desktop version.
4. Secure Authentication API (SAA). Same as in Desktop client. The DLL provided *MUST* match the device platform (OS Configuration) and processor type.
5. Microsoft ActiveSync. Pocket PC 2003 devices can be synchronized with the Host PC using Microsoft ActiveSync. This can be done with a serial cable, USB, infrared, modem, BlueTooth or network connection.

   Synchronization with a serial cable, USB, BlueTooth and infrared is enabled by default, regardless of the client's Security Policy.

   Modem and Network synchronization are treated like any other IP connection, and may be encrypted or blocked according to the Security Policy and topology.

   Un-encrypted ActiveSync Connections:

   When SecureClient detects un-encrypted ActiveSync communication attempts, the user is asked to Allow or to Reject the communication. If the user chose to always Allow or Reject this communication (by choosing **Do not ask me again**), it is possible to change this setting via the **Policy** menu of SecureClient (**ActiveSync: Allow All, ActiveSync: Ask User, ActiveSync: Block All**).

   Extra care should be taken when serial, USB, BlueTooth and Infrared ActiveSync operation is enabled. ActiveSync uses a specific pre-defined IP address for the PDA, which is 192.168.55.101. The administrator should make sure that the IP address 192.168.55.101 is not used by any device on the network.

   SecureClient for Pocket PC 2003 accepts connections that were initiated using this IP (when the user chose to Allow un-encrypted ActiveSync connections) regardless of the client's Security Policy and topology.

ActiveSync Pass-Through Connections

A well-known feature of ActiveSync is Pass-Through Connections, in which the PDA connects through the serial, USB, BlueTooth and infrared link to an outside network through the Host PC. This enables the PC to act as a generic network proxy by performing Network Address Translation.

Pass-Through connections will be enabled if un-encrypted ActiveSync connections are enabled (as described in the section above).

6 Topology download (**New Site** and **Update Site**) is supported in the following ways:

- *Unauthenticated,* if the option **Respond to unauthenticated topology requests** is enabled on the Management station, topology data is not authenticated and not encrypted (it is signed, however).

  This method is supported only when the Site is defined as the Management server, and it is of version NG FP1 or older (NG FP2 Management no longer supports this method).
- *Authenticated*, the user defines the Site as one of the Gateways. The user needs to have an IKE pre-shared secret defined.

Topology User

If you are not using IKE pre-shared secrets for general authentication and encryption, you can define a Topology User (for New Site and Update Site operations) in the following way:

Define one user (with IKE authentication enabled) to be used by all remote users only for defining and updating sites. You should block encryption capabilities for this user. To implement this workaround, proceed as follows:

a In the **Location** tab of the user's User Properties window, set **Source** and **Destination** to *None*.

b In the **Time** tab of the user's **User Properties** window, uncheck all the days.

c In the **Desktop Security** tab of the **Properties Setup** window, uncheck **Respond to unauthenticated topology requests**.

7 Certificates. Currently only PKCS#12 format certificates are supported

In order to use certificates, you must import the certificate files into your device, typically by using the ActiveSync application. On the Hand Held PC you can place the certificate files anywhere on your device. On the Pocket PC, you should place them under one of the browsable folders, namely **Business**, **Personal** or **Templates**.

If you are using a certificate file in order to authenticate, SecureClient will prompt you for the file name. A file browser is displayed and can be used to find the certificate file. Once you've entered the file name, you can view the certificate details of both the user and CA certificates, provided you have entered the correct password.

Customers using Entrust Digital ID's in the `*.epf` format need to export them into `*.p12` format using the Entrust Entelligence 6.0 **Export** feature on their desktop before synchronizing the `*.p12` file to the PocketPC device. The **Export** feature is accessed by right clicking on the Entrust key Tray icon and selecting **Entrust Options**.

Users must have their account configured with suitable export policies by their PKI administrator before the PKCS#12 **Export** feature is enabled in Entrust Entelligence. Please refer to the Entrust document *Desktop Admin Guide 6.0* for configuration instructions for Entrust/Authority 5.0 and 6.0. Relevant sections are titled *Export to PKCS#12* and *Enabling the Export Certificate Type.*

8 Enabling IKE Over TCP. In order to determine whether to attempt IKE over TCP or not, the file `userc.C.txt` should be edited to include the following line in its options section:

```
:support_tcp_ike (true)
```

In this case, IKE over TCP operation is possible, depending on the Gateway configuration and operational state. In order to turn this option off, either erase this line from `userc.C.txt`, or replace it with:

```
:support_tcp_ike (false)
```

Installing and Uninstalling the Client

1 When customizing the installation package, system administrators may want to create a customized Installation Package with their own `userc.C.txt` file. Note that the file name is different from the Desktop version in order to allow editing in the Pocket PC/ The file should be named `userc.C.txt` and not `userc.C` (as in the Desktop version).

2 Installation instructions

a If the Installation Package is zipped, unzip it.

b Switch or modify the `userc.C.txt` file located in **Program Files\CheckPoint\SecureClient\Users** according to the desired specifications.

c. Run setup.exe on the Host PC. The new userc.C.txt file will be installed with this package (including the changes made). If the device is connected via ActiveSync, SecureClient will be installed on the device at this point. Otherwise it will be installed the next time the device connects via ActiveSync.

d. Once SecureClient is installed in this fashion, it can be installed via ActiveSync on any device that is connected to this Host PC via the **Tools->Add/Remove Programs** menu in ActiveSync.

3. Uninstalling the client. In general, it is recommended to uninstall the client via **Tools->Add/Remove Programs** menu in the **ActiveSync** window on your Host PC. It is also possible to uninstall the client on the device itself. In the Pocket PC devices this is possible via **Settings->System->Remove Programs**, and in the HandHeld devices via **Settings->Control Panel->Remove Programs**. This method can be used if the client cannot connect to the Host PC, or if the client was uninstalled already from the Host PC.

Unsupported Features and Possible Workarounds

The following features are available in the Desktop version of the VPN-1 SecureClient and NOT available in the current Pocket PC 2003 version. Some of the listed limitations will be lifted in subsequent releases.

1. FWZ encryption scheme. Use IKE/IPSec instead.
2. Secure Configuration Verification (SCV). SCV is not enforced in this version of the client.
3. External Authentication Message is not supported in this version.
4. Office mode.

Limitations

Specific limitations of SecureClient on Pocket PC 2003

1. When new adapters are installed on the device, or when adapter properties are changed, SecureClient is not automatically aware of the changes. In order to protect the device properly, the user should use the **Tools >Re-bind Adapters** menu option. The user will then be prompted to restart the device.
2. CAB files are not zipped - since most devices do not include a standard compression application or API.
3. No support for DES encryption. Use 3DES.
4. AES is not supported.

5 Only PKCS#12 format certificates are supported.

6 Once SecureClient is installed, the installation procedures of *other* applications may issue a “Setup Failed” message, indicating that “SecureClient WinCE.NET.CAB is not a valid Windows CE Setup file”. Select OK, and the installation will succeed.

7 Software setup via ActiveSync may fail when a restrictive (block all) policy is selected. The workaround is to select a permissive (accept all) policy during setups. For security reasons it is advisable to disable your network devices during this period.

General limitations of SecureClient

8 The following data items are not encrypted:

- DNS information, unless otherwise configured (see VPN User's Guide).
- Local connections are not encrypted. A connection is “local” if both the IP address of the client and the IP address of the destination (i.e., the server) are both inside the same encryption domain of the same firewalled gateway.

9 `tracert` to a destination in an encryption domain will have limited functionality if the encryption scheme encapsulates packets. All hops before the encrypting gateway will be shown without data (***), since they will not know how to decrypt the ICMP packet. ICMP data will be returned only from the encrypting gateway and beyond.

10 New Security Policies will not be applied to existing connections.

Frequently Asked Questions

1 **Do I need to setup special configuration for my FireWall-1 gateway in order to support the Pocket PC 2003 SecureClient?**

If you are using PKI authentication (certificates) then the answer is no - it is configured the same as any other FireWall-1 4.1 client on the PC. In the other hand, if you are using Hybrid or pre-shared secret authentication, then the IKE Authentication for this FireWall-1 user on the Gateway should be configured to have the Password (Pre-shared secret) checkbox on. It is needed for downloading the topology from the site. This special setting is important especially in FireWall-1 gateways of version NG FP3 and higher.

2 **Is the Client supposed to be able to connect to the Check Point gateway when cradled?**

When cradled, the client may use the ActiveSync pass-through connection mechanism. Since the current version of Pocket PC 2003 SecureClient does not support encryption via pass-through connection, you will be able to authenticate to your gateway, if it allows unencrypted authentication. This means that you will be able to add a new site this way, but not to use VPN (encrypted) communications with it.

3 I cannot bring my communications card (a modem or a LAN card) to operational state with SecureClient installed, whereas it operates well without the client. Is there anything I can do?

There is a workaround that might work in this case: you should cause the SecureClient application to launch after your device driver. It means that you will need to activate SecureClient manually. In order to do it, do the following:

a Via the File Explorer on your device, delete the link file `\Windows\StartUp\SecureClient.`

b After you reboot the device, activate the SecureClient application manually, by clicking the icon (one click on the Pocket PC and double-click on Hand Held devices) at `Program Files\Communication\SecureClient` through the File Explorer.

4 After I tried to un-install SecureClient, I can no longer connect to the outside world: I cannot use my modem card nor any of my Ethernet cards. I can't ActiveSync either. The current IP remains always local (127.0.0.1). How can I regain network operation without hard restarting my device?

You should try the following steps, in this order:

a Try to un-install SecureClient again via **Settings > System >Remove Programs** or **Settings > Control Panel > Remove Programs**.

b Edit your registry settings, provided you have some regedit utility (such as Tascal Regedit). In order to enable the PPP connection (dial-up, and also serial, USB, Infrared or BlueTooth ActiveSync), you should erase the following registry keys or values, if they exist:

i delete `HKEY_LOCAL_MACHINE\Comm\AsyncMac1\Parms\ProtocolsToBindTo`

ii delete `HKEY_LOCAL_MACHINE\Comm\SecureClientWAN`. In order to enable Ethernet connections, you should erase the following:

iii For each LAN *XXXX* adapter you are using (for example, *XXXX* = NE2000), delete the following key:

`HKEY_LOCAL_MACHINE\Comm\XXXX1\Parms\ProtocolsToBindTo`

(for example: `HKEY_LOCAL_MACHINE\Comm\NE20001\Parms\ProtocolsToBindTo`).

iv delete `HKEY_LOCAL_MACHINE\Comm\SecureClientLAN\`

v Now reboot.