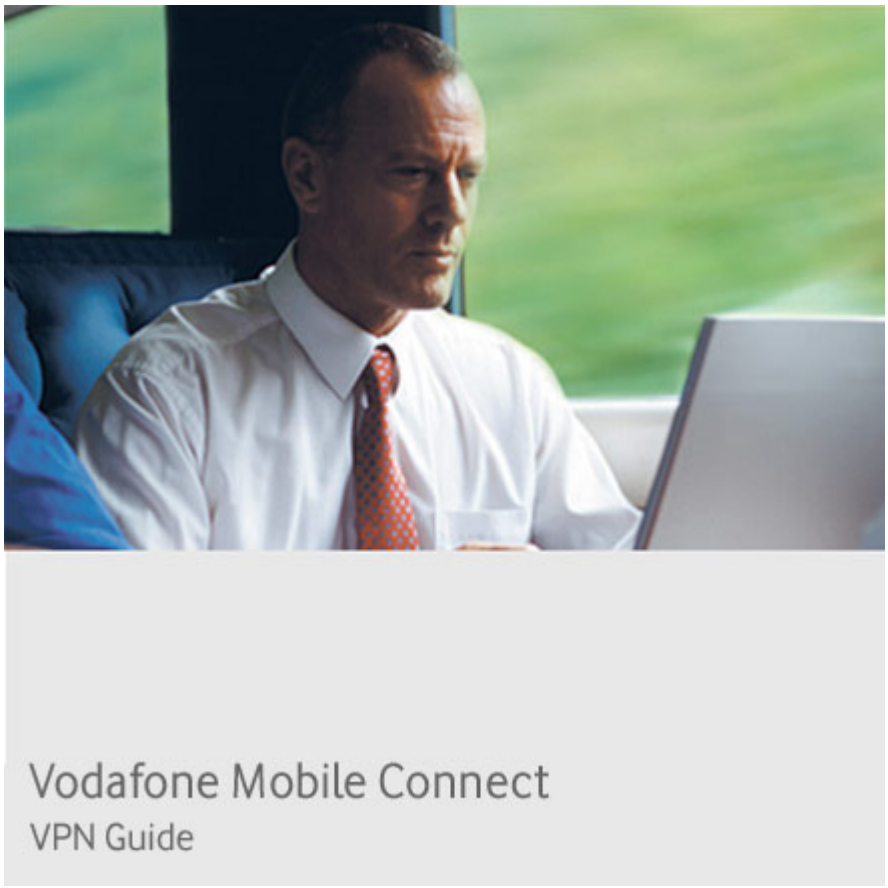
VPN End to End – Cisco – Appendix

Appendix B: Cisco client version 4.8.00.0440

Technical Notes for use with Vodafone Mobile Connect services

Date: **14 May 2007**

Revision No: **3.0**



Scope

This document presents results of installation, configuration, and operations testing of VPN components with the Vodafone Mobile Connect service. The document is not intended to be a tutorial on VPN concepts nor does it supersede or replace the vendor's documentation. The reader is referred to the VPN vendor for definitive guidance on the proper and recommended use of their product. While Vodafone Group has taken care to ensure that the information contained herein is accurate, no responsibility can be accepted for errors, omissions, or inaccuracies.

Document History

Version	Date	Reason
1.0	October 2003	Initial release using GPRS network. Client documentation included in main document.
2.0	May 2006	Creation of separate document for client configuration. Update to new versions of VPN software and focus on 3G network performance.
3.0	May 2007	Update for R9, added logging

File Reference

VPN_Cisco_Appendix_B_Client.doc

Document Authors

Joerg Pfeffer , TECON Terenci

Document Distribution

Public via websites of Vodafone, its Affiliates, and its Partner Networks

Contents

Tables & Figures

1 Executive summary

This Appendix B is in addition to the detailed document for Cisco VPN solutions and describes the set up process in a detailed way with example screen shots taken from the initial processes. It is a companion guide to the Overview (End-to-End) and Appendix A (Concentrator) documents for Cisco VPN solutions.

The client software is common to several Cisco VPN solutions and so is only documented once.

The Cisco VPN client cannot be installed with other VPN clients on the same machine, and the native Microsoft Windows VPN clients will be disabled by this installation.

In addition the implementation into Vodafone Mobile Connect is described as well to call the VPN client from within the Vodafone Mobile Connect application.

Logging and additional functionality is described in the appropriate chapters.

Additional information is available in the vendor's documentation and on the website www.cisco.com.

2 VPN Client Installation and Configuration (Cisco VPN Client 4.8.00.0440)

The Cisco VPN Client can be installed on a Windows 2000 or Windows XP Workstation. Administrator rights on the local machine are needed to install the Software. This client can be used to establish a VPN connection to the Cisco VPN concentrator. Other VPN Clients have to be de-installed.

2.1 VPN Client System requirements

Verify that your computer meets these requirements:

- A single, Pentium®-class processor.
- One of the following operating systems:
  - Microsoft® Windows® 98, or Windows 98 (second edition)
  - Windows ME
  - Windows NT 4.0 (with Service Pack 6 or higher)
  - Windows 2000
  - Windows XP
- Microsoft TCP/IP installed. (Confirm via Start > Settings > Control Panel > Network > Protocols or Configuration.)
- 50 MB hard disk space.
- RAM[1]:
  - 32 MB for Windows 98
  - 64 MB for Windows NT and Windows ME
  - 64 MB for Windows 2000 (128 MB recommended)
  - 128 MB for Windows XP (256 MB recommended)
- To install the VPN Client:
  - CD-ROM drive or a 3.5 inch high-density diskette drive
  - Administrator privileges if installing on Windows NT, 2000 or XP

[1] These are minimums to install and operate the software – additional memory is generally required for satisfactory performance and user experience in typical office applications and configurations.

- To use the VPN Client:

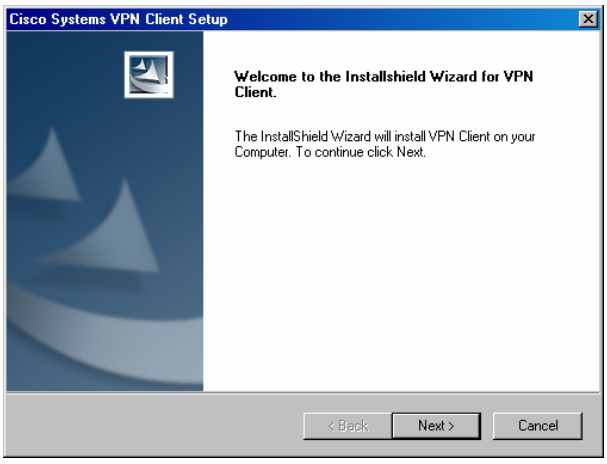
  – Direct network connection (cable or DSL modem and network adapter/interface card)
  – Internal or external modem (such as the Vodafone Mobile Connect datacard or USB modem)

- To connect using a digital certificate for authentication:

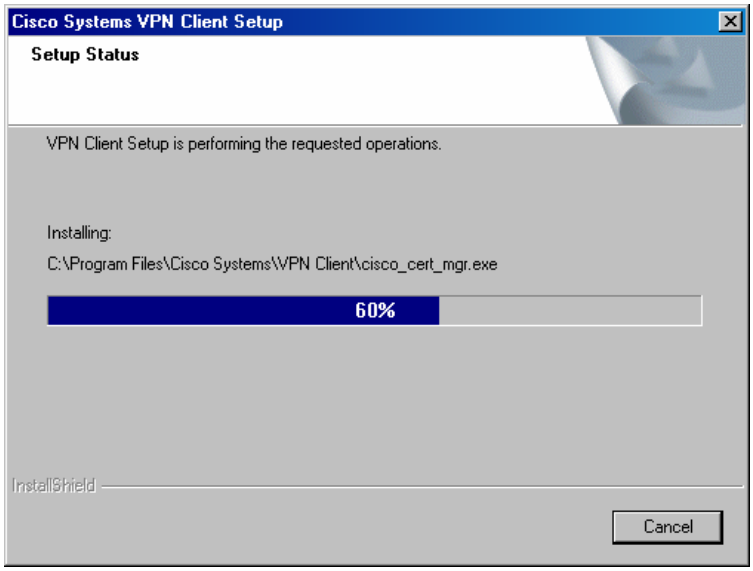
  – A digital certificate signed by one of the following Certificate Authorities (CAs) installed on your PC:
    Baltimore Technologies (www.baltimoretechnologies.com)
    Entrust Technologies (www.entrust.com)
    Microsoft Certificate Services—Windows 2000
    Netscape (Security)
    Verisign, Inc. (www.verisign.com)
  – Or a digital certificate stored on a smart card; the VPN Client supports smart cards via the MS CAPI Interface

2.2 VPN Client installation

- Run the installation program according to the directions given by the program. Keep in mind that the integrated IPSec Subsystem of Windows 2000 and XP will be disabled by the CISCO VPN Client.
  Following slides shows the VPN Client 4.8.00.0440 Installation :
- At the “Setup” window click “Next”

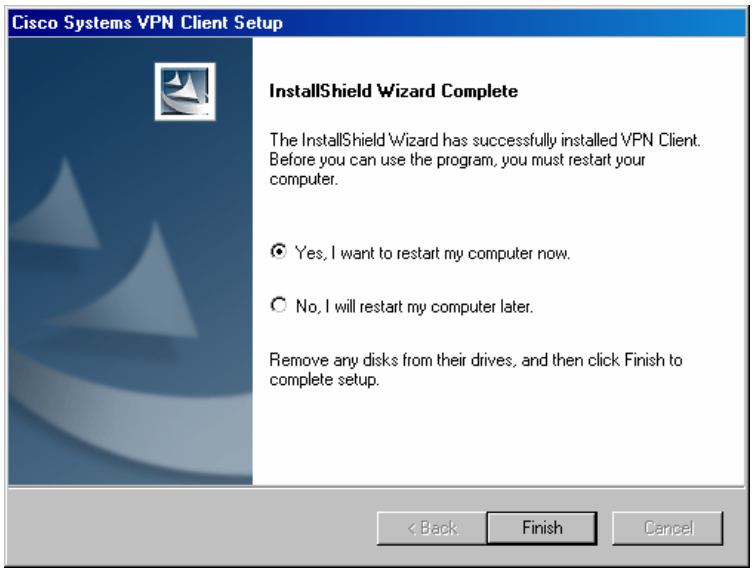


- Follow the screens for “License Agreement” and “Destination and Program Folders” and install the Cisco VPN client.



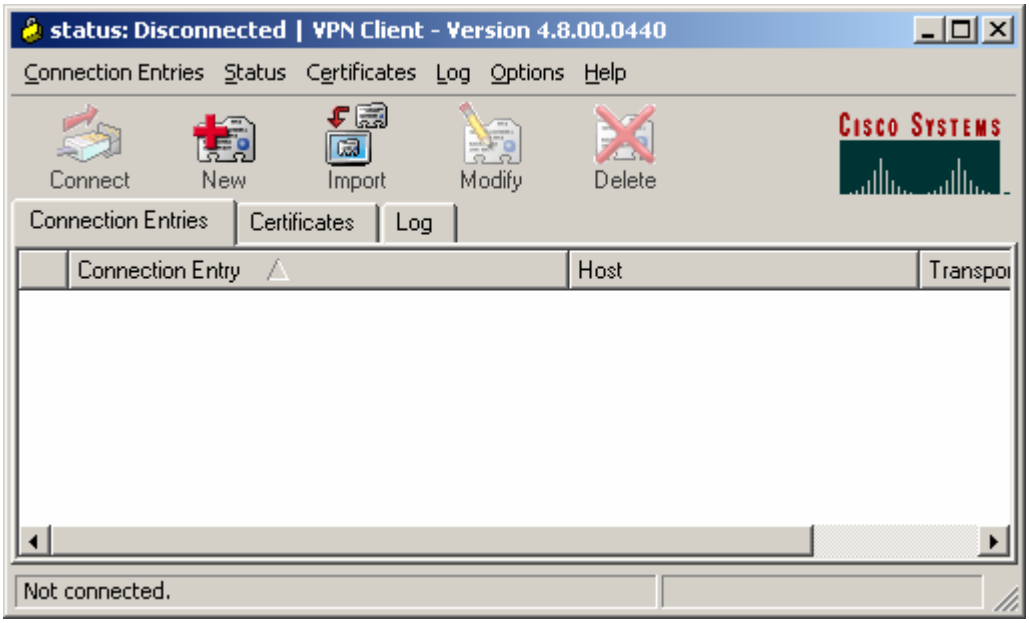
- Setup status

- A Deterministic Network Enhancer will be installed on all available network adapters. Additionally Cisco VPN Client 4.0 creates a new network adapter.

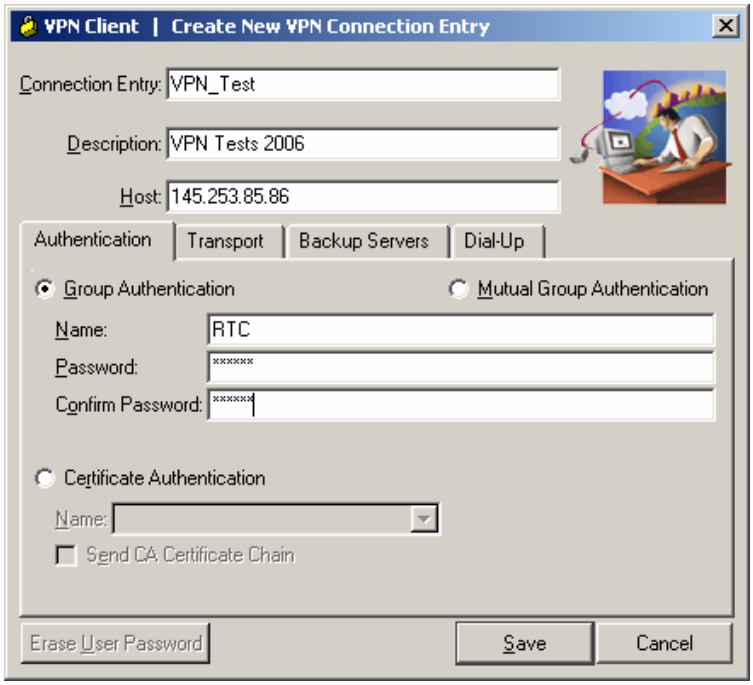


- Click “Finish” to complete the installation

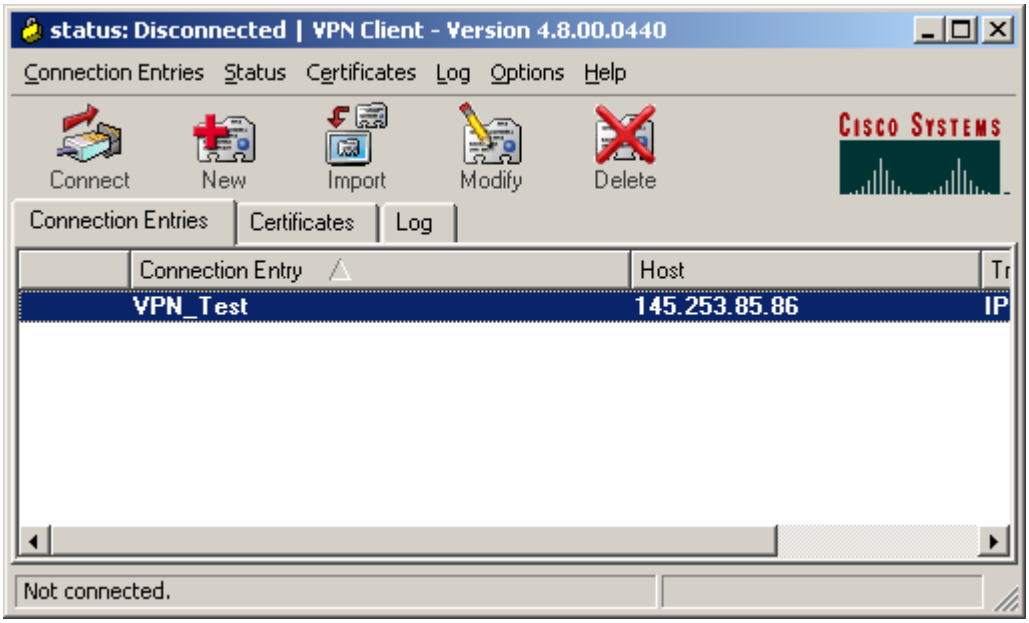
2.3 Configuring a new Client connection (VPN Client 4.8.00.0440)



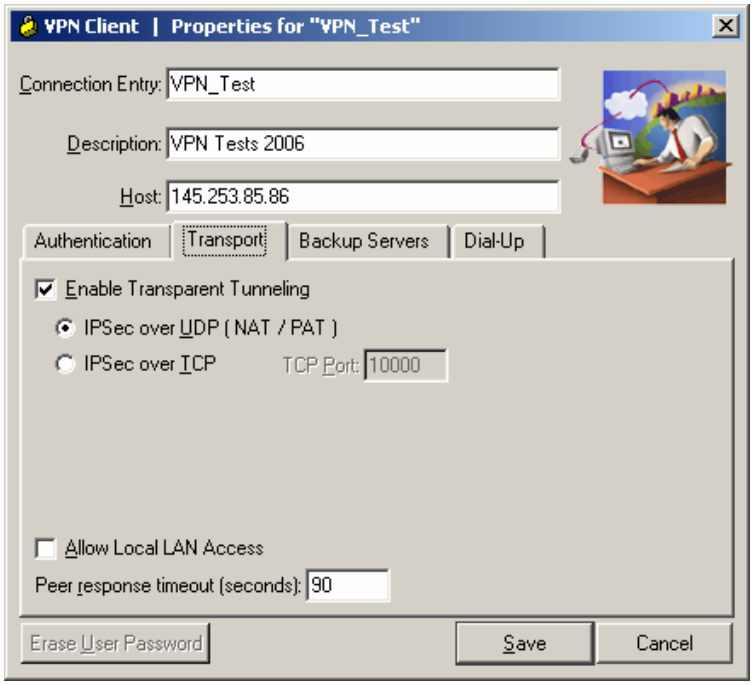
- Start the VPN client and click the button “New” to define a new profile



- Enter the name and an optional description, the VPN Concentrator's external IP address, the Group Authentication and click "Save". The basic configuration is now completed.



- To modify the configuration click "Modify" button or select "Modify…" from the right-click context menu.



- On the “Transport” tab you can choose to use ‘IPSec over UDP’ or TCP.

3 Configuration & Connection Using VMC Software

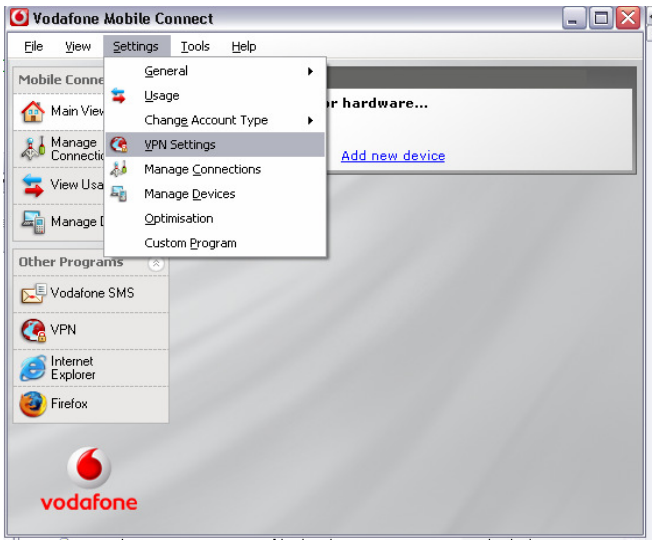
This chapter is used to describe possible configuration possibilities for using the VPN client in conjunction with the current released Vodafone Mobile Connect application.

First you need to build up a connection using your VMC. Insert the SIM into your datacard (or USB modem) and open the Vodafone Mobile Connect application.

Note: The new R9 of Vodafone Mobile Connect software offers the same features but with a different user interface. This document will be updated in due course with full demonstration of the steps using R9.

In short, the differences are:

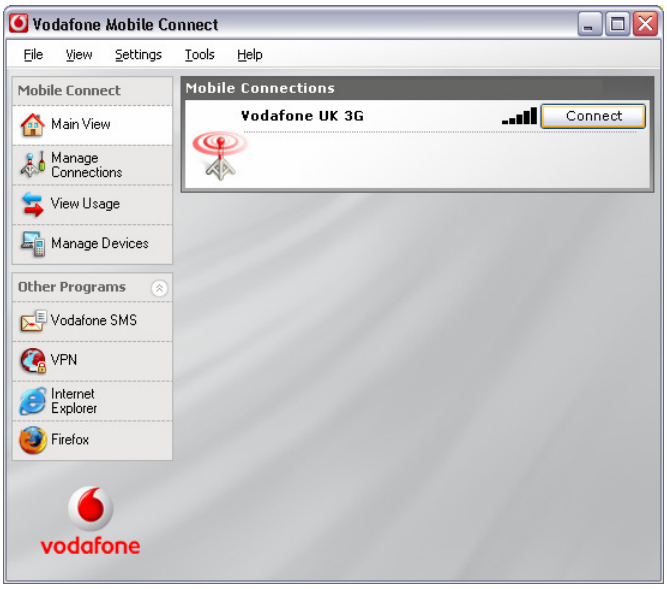
1. The '**Connect**' button is found in the 'Mobile Connections' window of the main screen.
2. The VPN button is found in the '**Other Programs**' section on the left side of the main view. If the Vodafone Mobile Connect software is not visible, it may need to be expanded from the mini view or from the icon in the Windows Notification Area (system tray).
3. The VPN settings can be modified using the **Settings** | **VPN Settings** commands from the main menu. This dialog will be initiated automatically the first time the VPN button is selected for the user to associate the button with the correct VPN software.



3.1 Establish the connection (VMC R9)

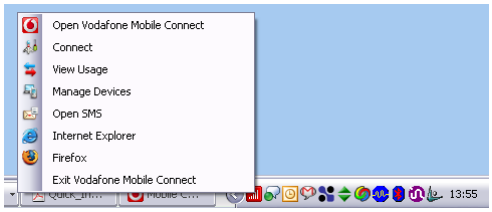
With a SIM card inserted into your datacard (or USB modem), to establish a connection:

1. In the main view, use the **Connect** button, or



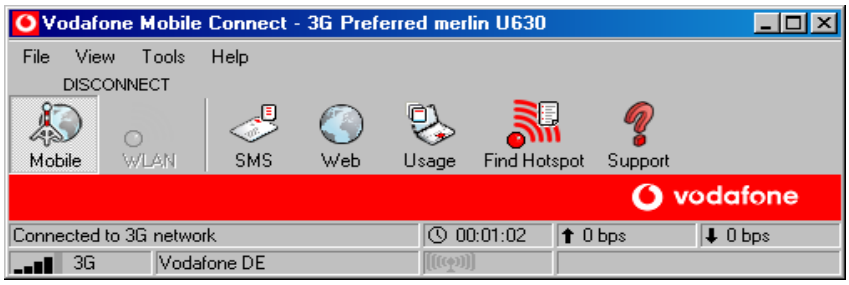
2. In the mini-view, use the **Connect** button, or

3. From the Windows Notification Area (system tray), right-click and select **Connect**.



3.2 Establish the connection (VMC R7 and earlier)

With a SIM card inserted into your datacard (or USB modem), to establish a connection:

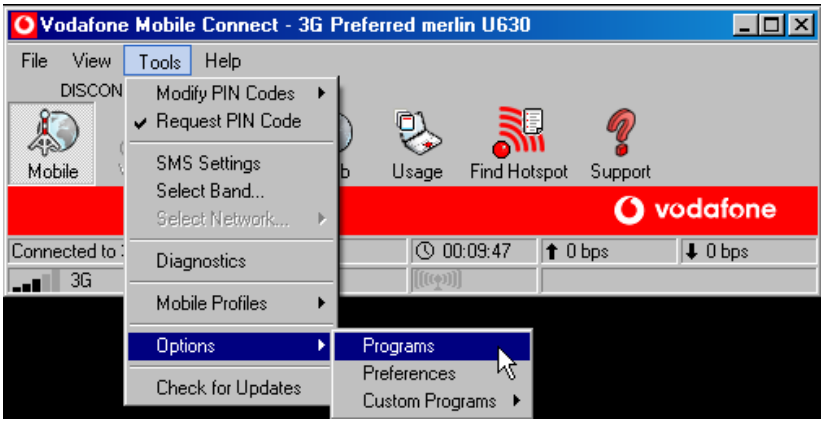


Press the **Mobile** button in the CONNECT/DISCONNECT area of the toolbar

3.3 Configure VMC for the VPN Client

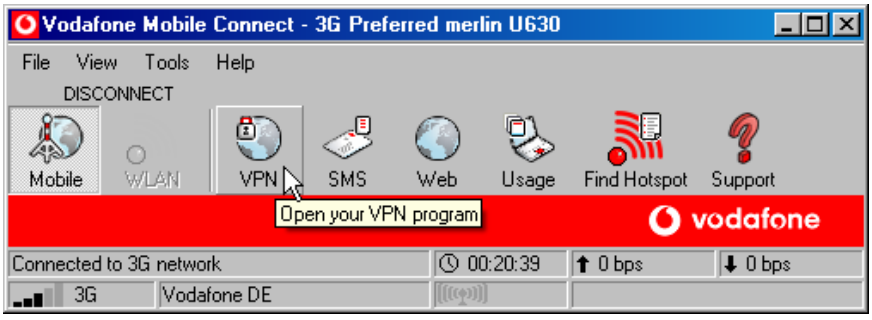
Note: The following steps apply to the legacy version of Vodafone Mobile Connect software R7 and earlier. See notes above on the process using the new R9 version.

- Configure your VPN client as follows to start it from within the VMC software.

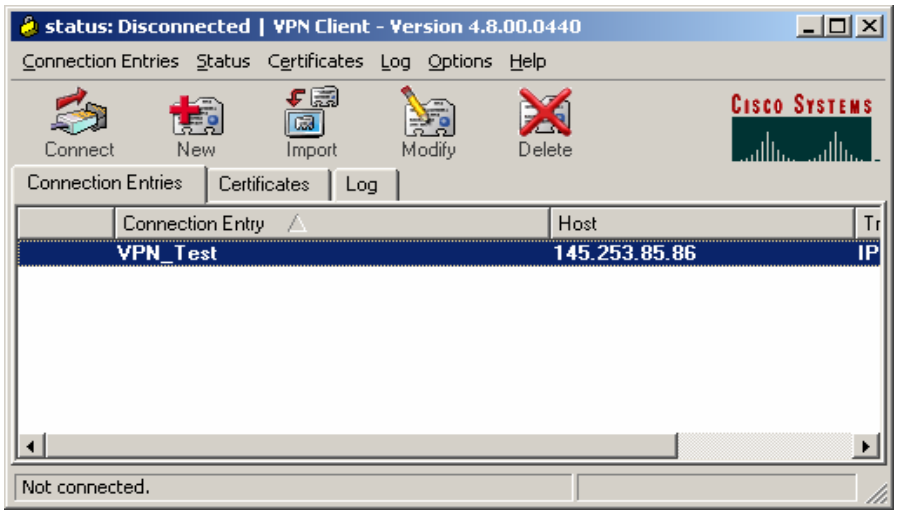


- Choose Tools | Mobile Profiles | Options | Programs
- Check the radio button “other” and select “Browse” to open your VPN client from the file system

- Select your Cisco VPN client here “vpngui.exe” and chose “Open”.
- Confirm your configuration with “OK”



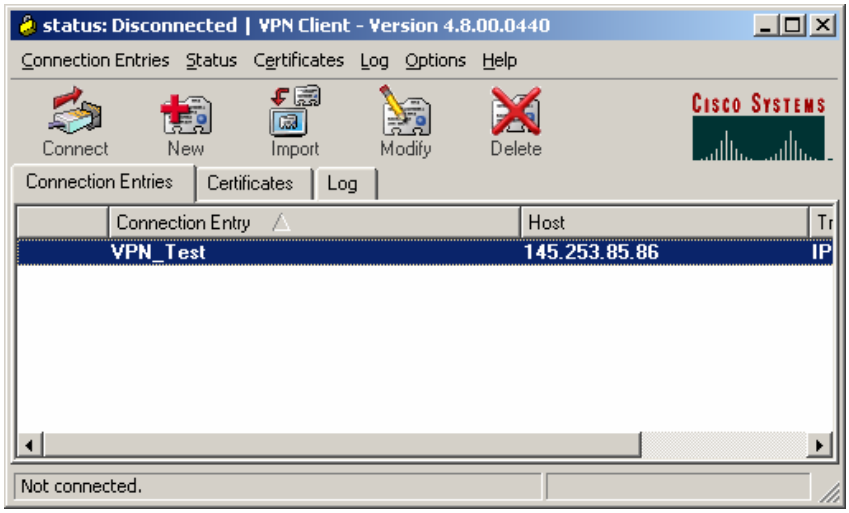
- Click the “Mobile” button on the main Dashboard screen.
  After you build up your preferred connection, click the “VPN” button to open your configured VPN Client



- Click “Connect” in the main dialog and the client will open the connection to the concentrator, ask for user name and password and establish the IPSec session.

4 Configuring the VPN Client to start automatically

By default Cisco VPN Client has to be started manually. It is possible to change the starting option e.g. from the Run-Key of the Registry. Also the connection to the Concentrator, by default, must be made manually by pressing the “Connect” button in the VPN Client.



The connection establishment can be changed to connect automatically. Cisco VPN Client supports AutoInitiation. To configure this, the file vpnClient.ini placed in the folder “C:\Program Files\Cisco Systems\VPN Client” has to be modified. By using AutoInitiation auto reconnect is available with the option AutoInitiationRetryInterval.

Example:

```
[Main]
ConnectOnOpen=1
AutoInitiationEnable=1
AutoInitiationRetryInterval=3
AutoInitiationList=RTC_VPN

[RTC_VPN]
Network=192.168.2.0
Mask=255.255.255.0
ConnectionEntry=RTC_VPN (points to a connection profile named RTC_VPN.pcf)
```

4.1 Testing Results & Observations

This chapter shows recognised issues during our tests and configurations regarding the Cisco client used for the test scenarios and connections using different types of server configurations, such as described in the main documents. Furthermore Known issues/problems are described in the main documents in the "Troubleshooting" chapter of the appropriate document.

4.1.1 Local LAN Transport status

During our tests we recognised, that on the "Tunnel Details" Tab within the statistics view is a display error as the "Local LAN:" setting is not displayed correctly. Regardless of the configuration of the client and its settings there is no way to get the "Local LAN:" field updated. This affects the Cisco VPN Client version 4.6 as well. The general functionality is not reduced, since this is only display behaviour on the field "Local LAN:" used for the Statistics view.

This field is described as follows in the Cisco Help/feature description as follows:

Cisco client help / feature description:
Local LAN Access--Whether access to your local area network while the tunnel is active is enabled or disabled.

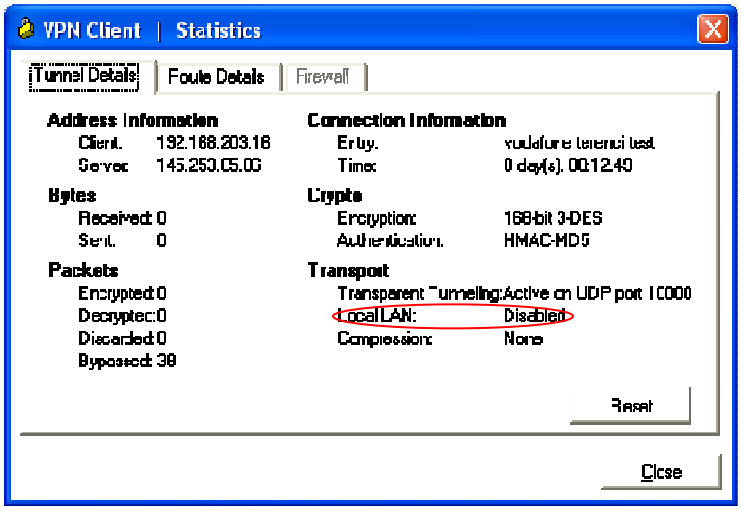


Figure 1 - VPN Client Display for Local LAN settings

4.1.2 Route Details Display

Furthermore the “Route Details” Tab is not showing entries for the “Local LAN Routes”. This field is left empty, even the connected Networks are not shown within this field.

This field is described as follows in the Cisco Help/feature description as follows:

Cisco client help / feature description:
Local LAN Routes
The Local LAN Routes box shows the network addresses of the networks you can access on your local LAN while you are connected to your organization's private network through an IPSec tunnel. You can access up to 10 networks on the client side of the connection. A network administrator at the central site must configure the networks you can access from the client side. For information on configuring Local LAN Access on the VPN 3000 Concentrator, refer to VPN Client Administrator Guide, Chapter
Network--The IP address of the excluded route.

Subnet Mask--The subnet mask of the IP address for this route.
Secured Routes

The Secured Routes box shows the following information:
Network-The IP address of the remote private network with which this VPN Client has a security association (SA).
Subnet Mask--The subnet mask of the IP address for this SA

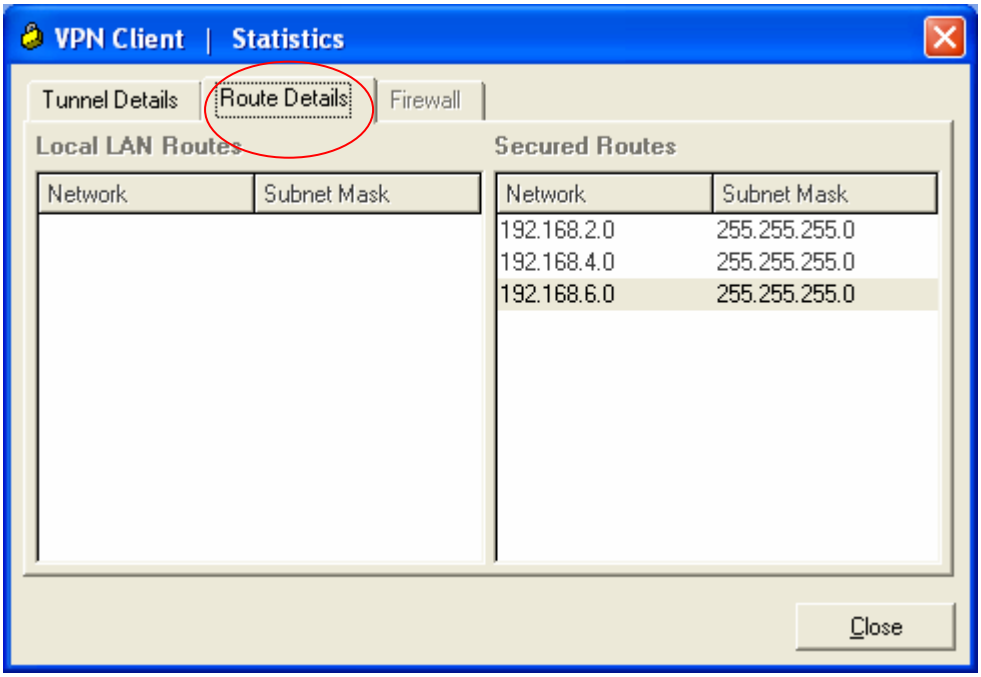
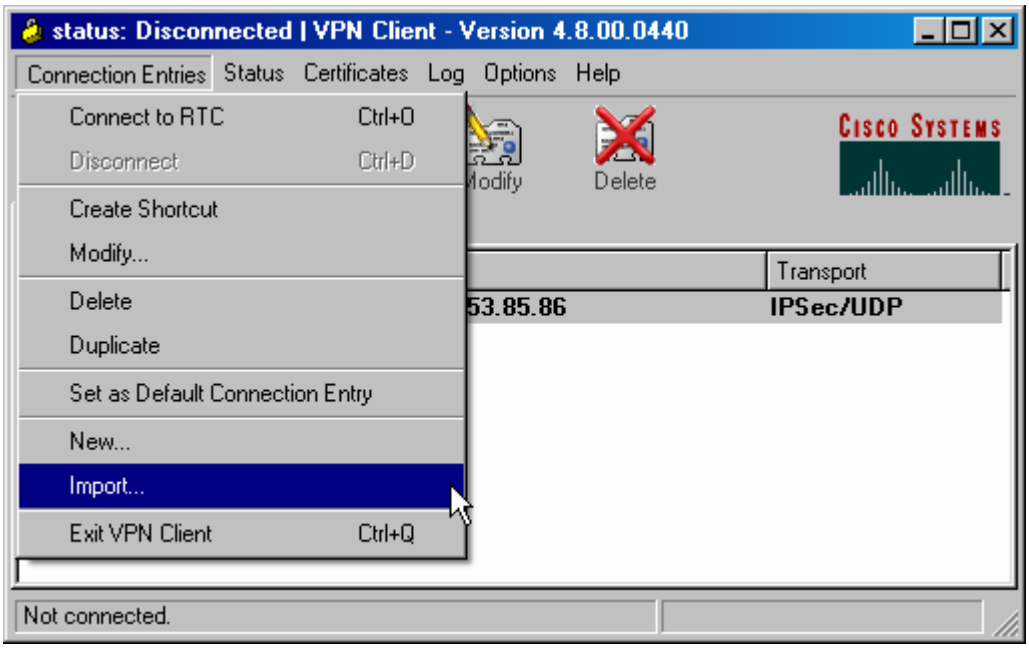


Figure 2 - Route Details tab of VPN Client

4.2 Import a Profile configuration File into Cisco VPN Client 4.8.00.0440

It is possible to pre-configure profiles for e.g. different user groups. Therefore the responsible administrator can deliver different configuration profiles, which could be imported by the user to have the correct configured and working profile available.

The administrator has to configure the needed profiles and deliver the appropriate *.pcf files to the particular users for apply these on their used clients.



Profile configuration file (.pcf file) is placed in “C:\Program Files\Cisco Systems\VPN Client\Profiles”.

5 Connections to Different Services

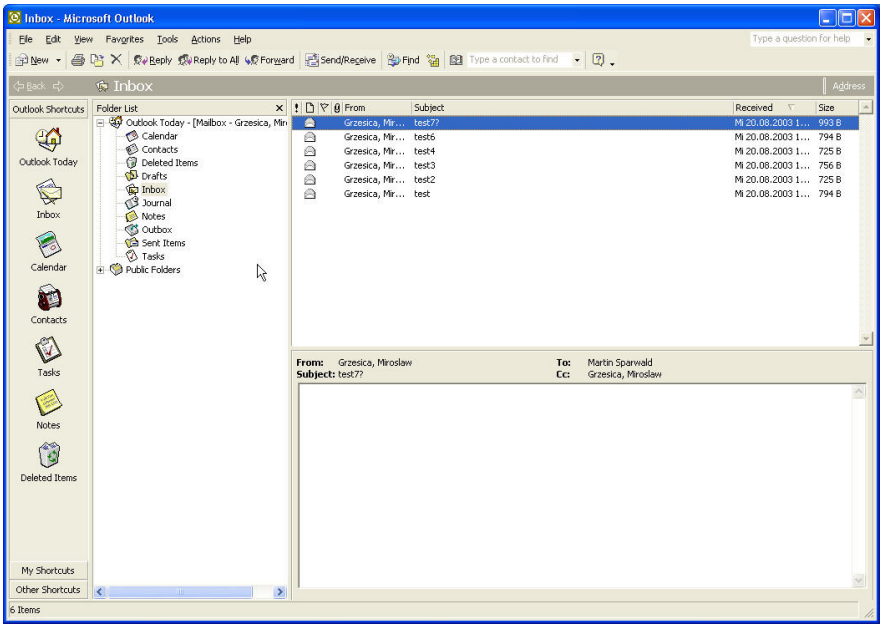
You can connect to all services via the VPN tunnel; you can connect to if you are in your local LAN.

It has to be an internet connection established and the VPN Client has to be started. If these requirements are fulfilled you can use all applications.

5.1 Connect to MS Exchange mail server / Outlook

Due to time-outs and other problems affecting the VPN tunnel, sometimes you have to repeat the connection procedure. The dialog boxes (displayed below) will appear. Click **Retry** till you get a connection to the Exchange Server.

After connecting successfully to the Exchange Server, you can use MS Outlook like you are connected to your local LAN



5.2 Connect to file server

If a VPN connection is established, you have to map a shared network folder on the file server in the LAN.

The user connecting to the shared network folder must have the permissions (in the local LAN) to connect to this folder.

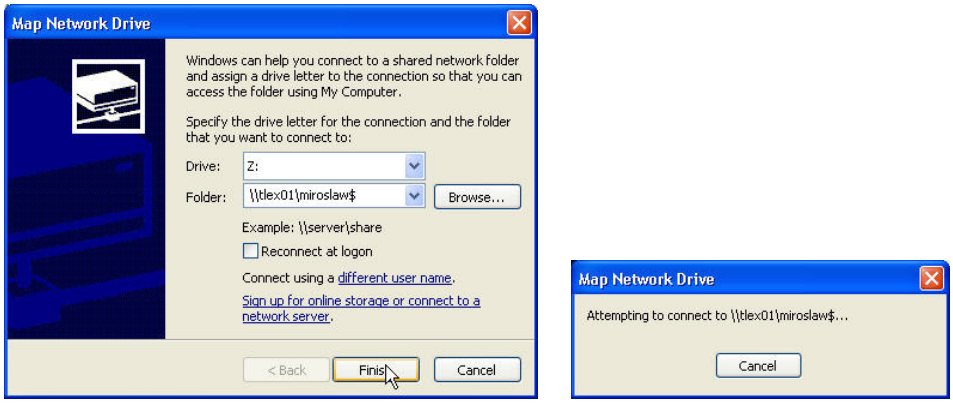


Figure 3 – Mapping Network Drive for VPN Access

After the connection to the file server via VPN is established, the user is able to transfer files between the file server and the local machine like he is connected to the local LAN.

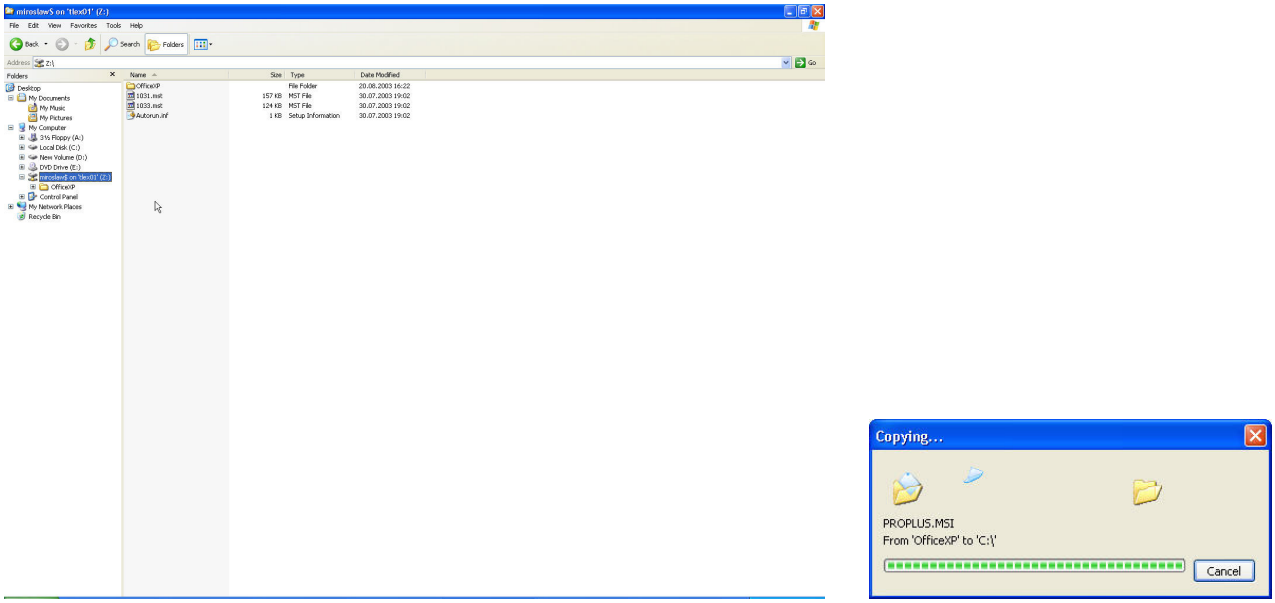


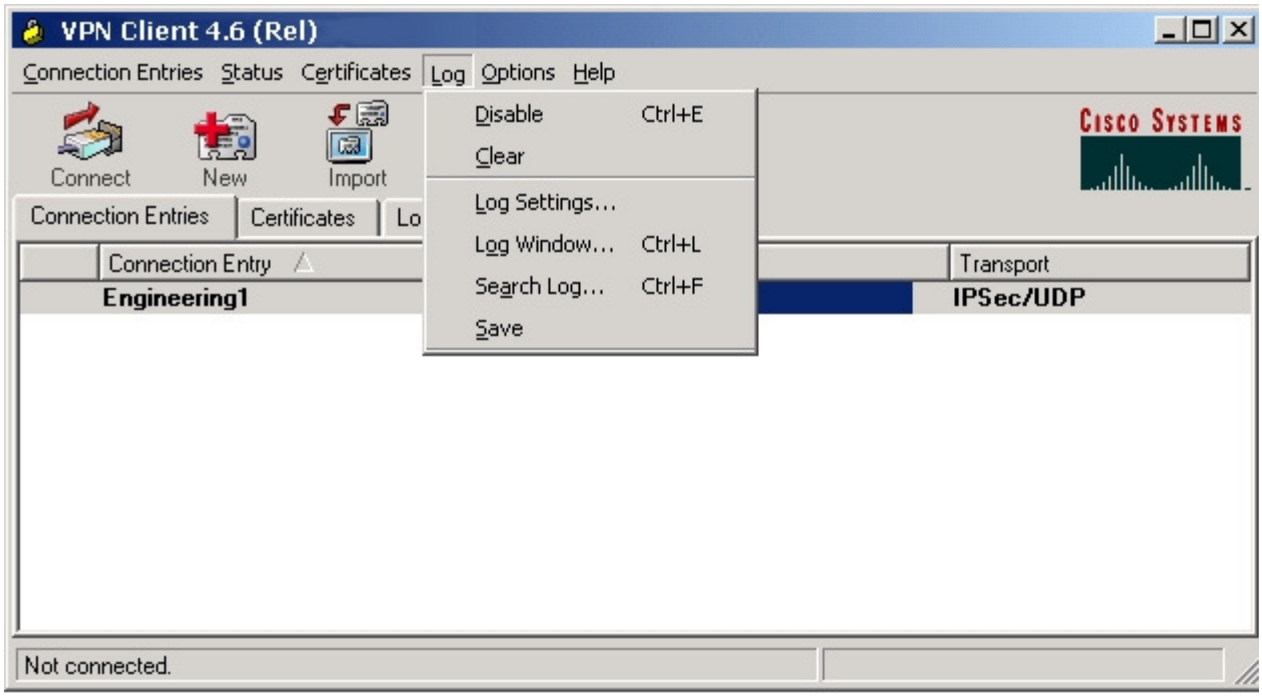
Figure 4 – File Transfer between LAN and local drives

6 Logging

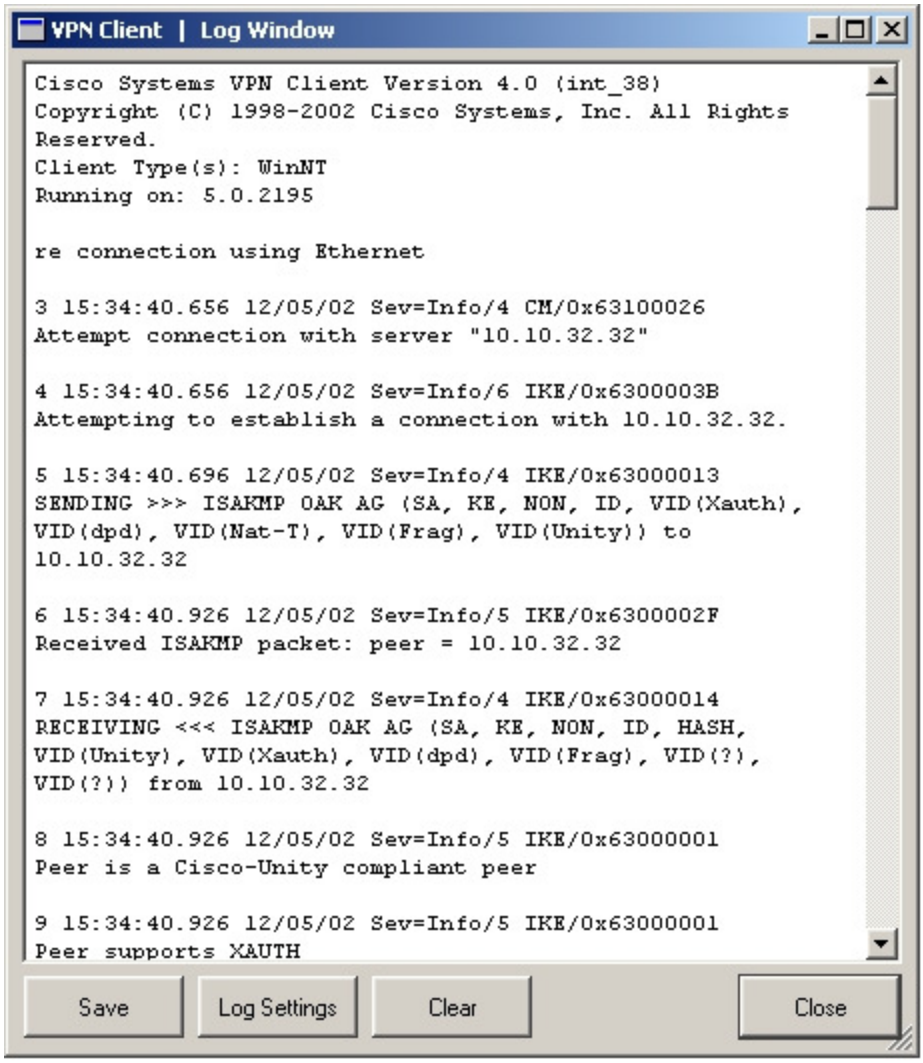
For more information please refer to the Cisco VPN Client's documentation.

6.1 Logging Client (client side)

A connection log is maintained by the client and is accessible from the 'Logs' menu item.

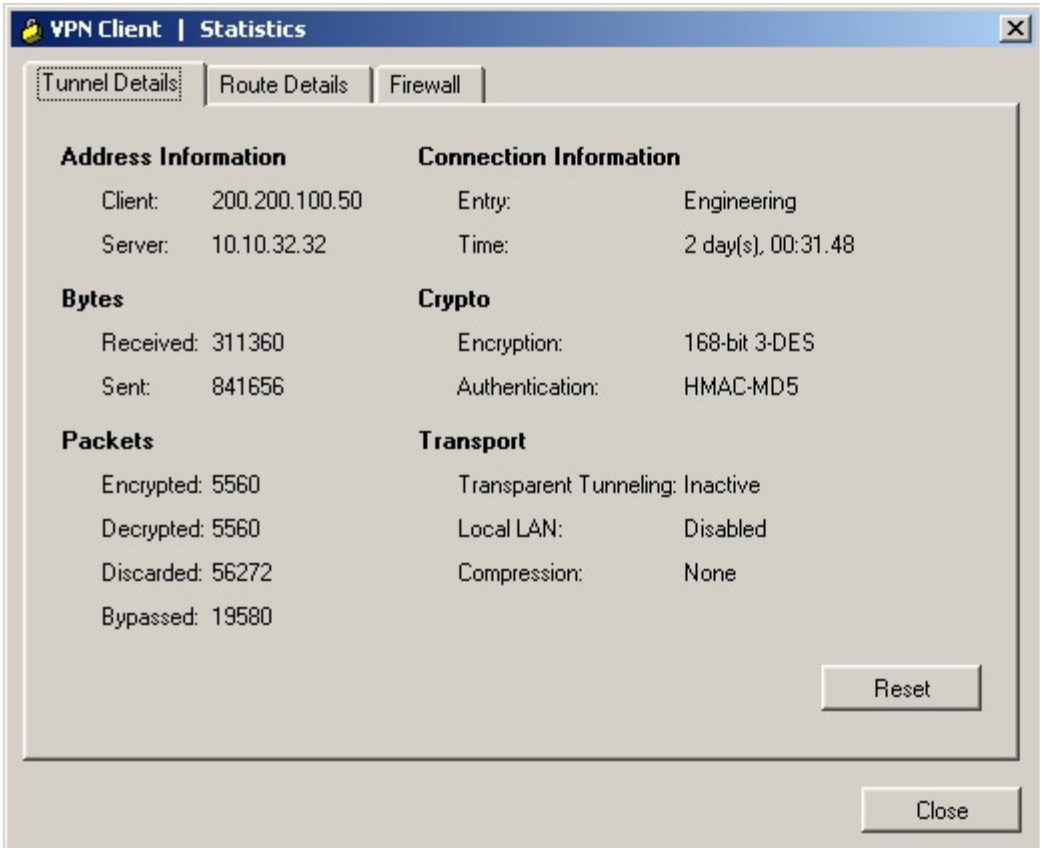


The log file can be searched, saved, and printed. The level of detail recorded in the log is controlled by the 'Log Settings…' option from the main menu or from the log window:



6.2 Connection Statistics (client side)

Statistics about the current connection are available from the ‘Statistics’. Menu option:



*** End of Document ***