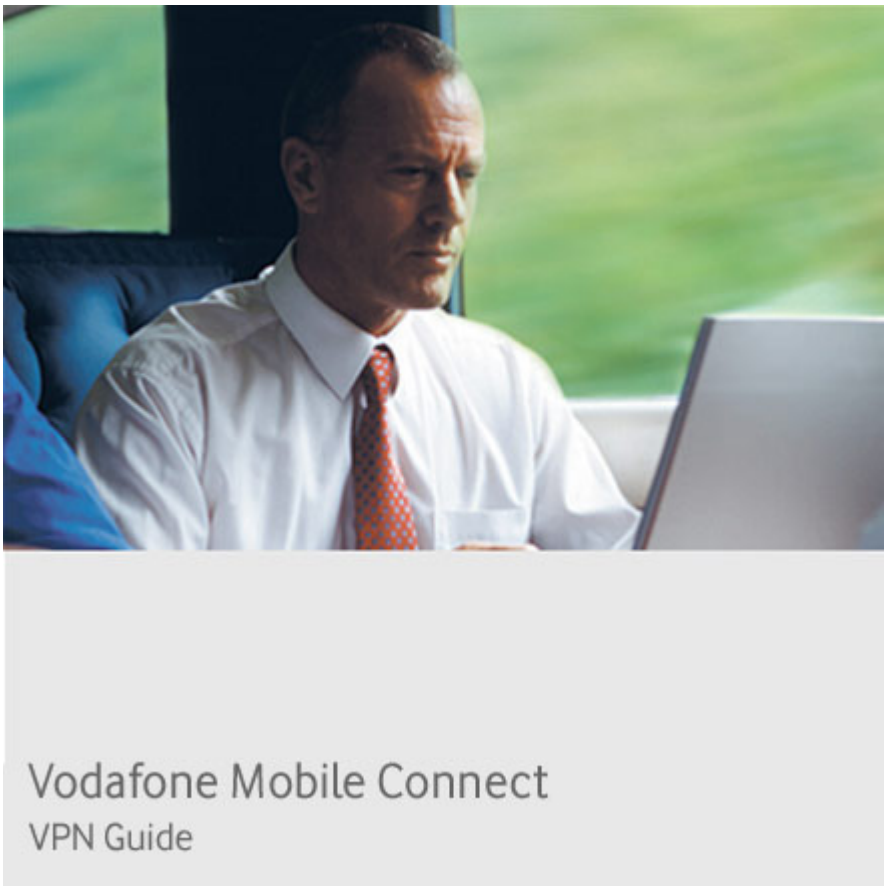
VPN End to End – Appendix B: MS Windows 2003 L2TP/IPSec Client

Appendix B: MS Windows 2003 L2TP/IPSec Client

Technical Notes for use with Vodafone Mobile Connect services

Date: **14 May 2007**

Revision No: **3.0**



© VODAFONE GROUP 2007

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	Minor edits and R9 updates.

File Reference

VPN - MS_2003_L2TP_IPSec_Appendix_B_Client.doc

Document Authors

Joerg Pfeffer, TECON Terenci
Miroslaw Grzesica, TECON Terenci

Document Distribution

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

© Vodafone Group 2007.

Other than as permitted by law, no part of this document may be reproduced, adapted, or distributed, in any form or by any means, without the prior written consent of Vodafone Group Plc.

Contents

1 Executive summary 4

2 VPN Client Installation and Configuration (MS XP VPN L2TP/IPSec Client connection) 5

2.1 VPN Client System requirements.....5

2.2 VPN Client installation and configuration 5

2.3 Configuring a new Client connection (Microsoft 2003 VPN L2TP IPSec Client) 11

2.4 How to configure L2TP/IPSec connection by using Preshared Key Authentication 15

3 Configuration & Connection Using VMC Software.....29

3.1 Establish the connection (VMC R9) 30

3.2 Establish the connection (VMC R7 and earlier) 30

3.3 Configure VMC for the VPN Client.....31

3.4 Establishing a mobile VPN connection 32

4 Configuring the VPN Client to start automatically 34

4.1 Testing Results & Observations.....34

4.2 “Keep-alive” Frequency.....34

5 Connections to Different Services.....35

5.1 Connect to MS Exchange mail server / Outlook.....35

5.2 Connect to file server 36

Tables & Figures

Figure 1 – Mapping Network Drive for VPN Access 36

Figure 2 – File Transfer between LAN and local drives 36

© VODAFONE GROUP 2007

1 Executive summary

This Appendix B is in addition to the overview document for Microsoft 2003 L2TP/IPSec and describes the set up process of the VPN Client in a detailed way with example screen shots taken from the initial processes. It is a companion guide to 'Appendix A: VPN - MS_2003_L2TP_IPSec_Appendix_A_Concentrator.doc'.

- Initial installation of the client software is reviewed.
- Configuration of the VPN client using sample parameters is illustrated
- The default configuration for the client is to start up manually. Options for automatic start-up are presented.
- Integration of the VPN Client with Vodafone Mobile Connect software is illustrated along with frequently used configuration settings
- Connections to corporate applications and file servers are illustrated
- Monitoring and logging of connection status is illustrated.

Further information is available from the vendor documentation and website www.microsoft.com.

© VODAFONE GROUP 2007

2 VPN Client Installation and Configuration (MS XP VPN L2TP/IPSec Client connection)

The Microsoft VPN client is integrated in the Windows XP systems Network connection manager.

2.1 VPN Client System requirements

Since the Microsoft Windows VPN client is integrated in the operating system, the computer must meet the requirements for Windows XP described on following web pages:

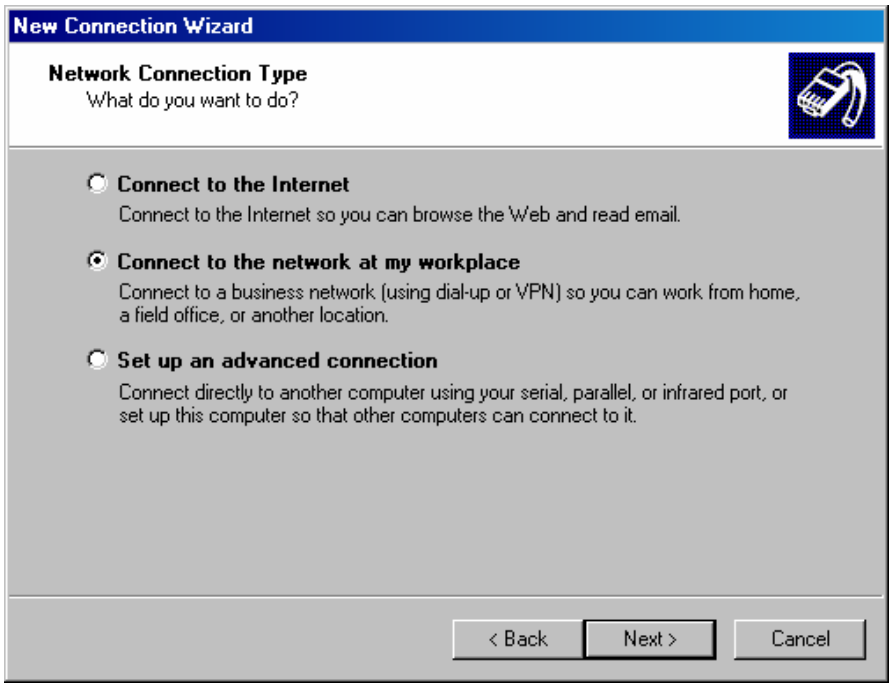
http://www.microsoft.com/windowsxp/home/upgrading/sysreqs.mspx

http://www.microsoft.com/windowsxp/pro/upgrading/sysreqs.mspx

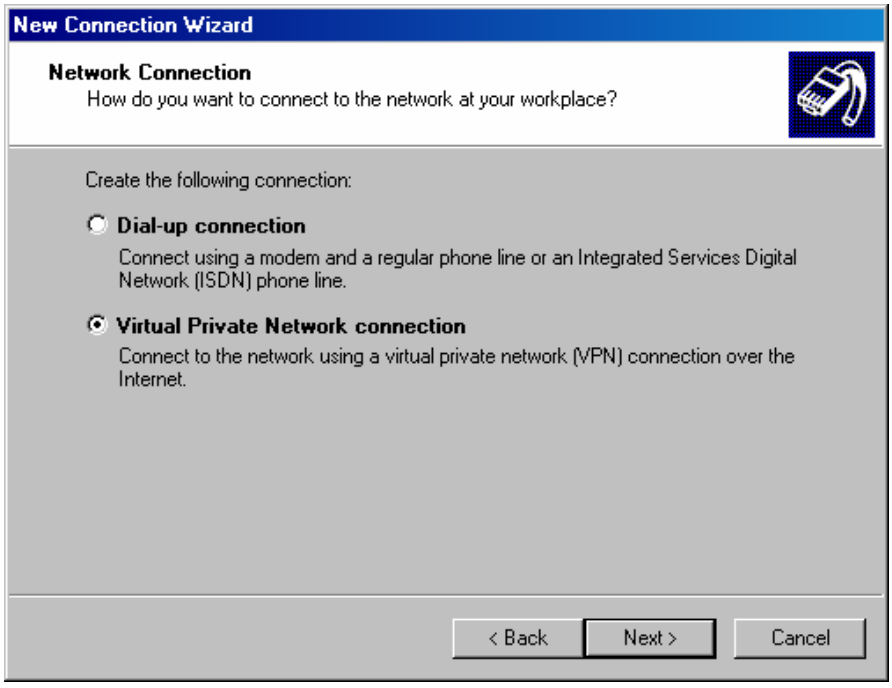
2.2 VPN Client installation and configuration

- Setup the Microsoft 2003 VPN L2TP/IPSec connection from a new Network connection with VPN connection type:
- At the “New connection wizard” window click “Next”

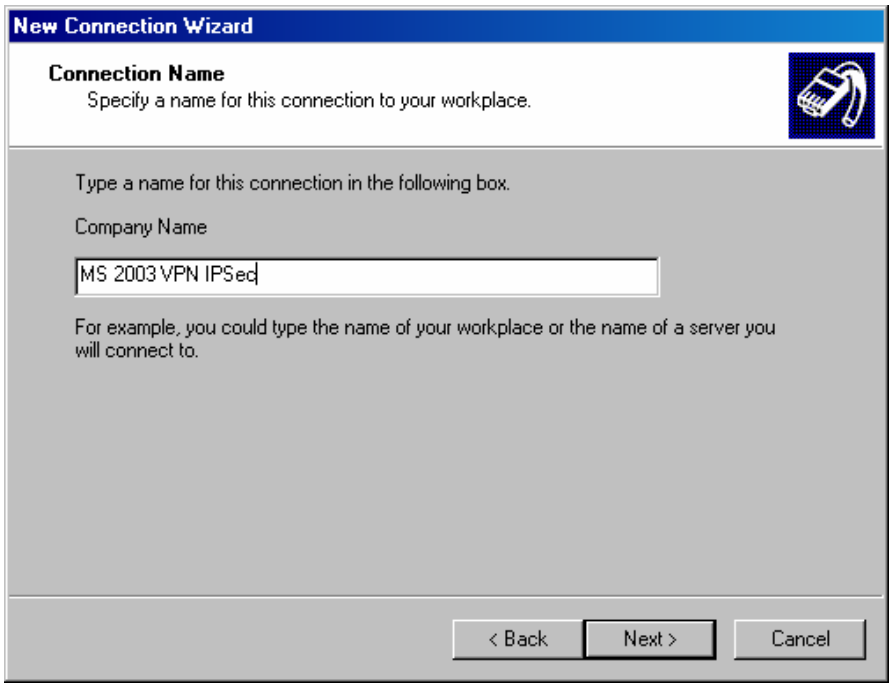
- The radio button “Connect to the network at my workplace” and click “next”.



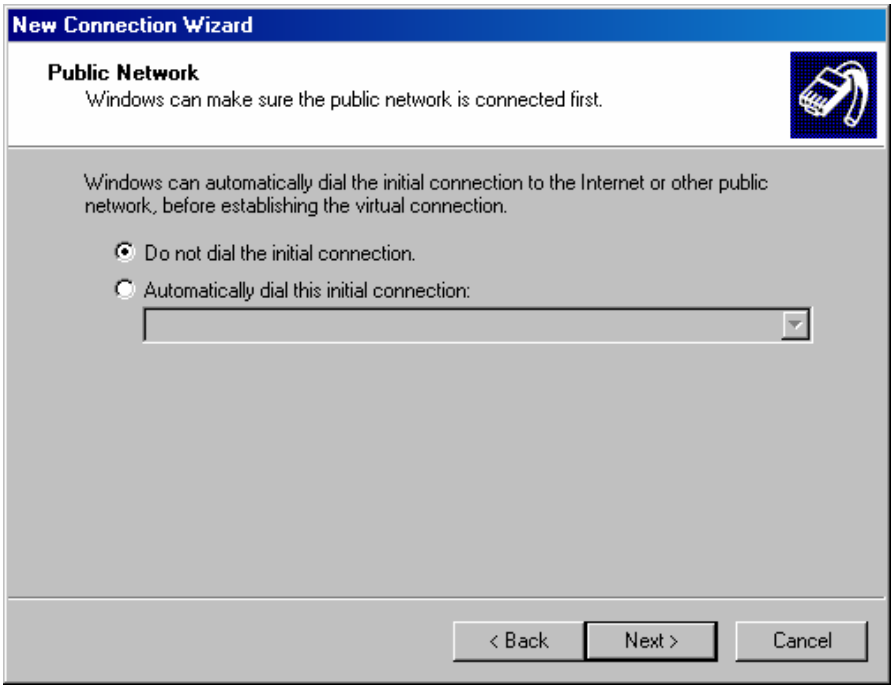
- For the network connection on the next screen please chose “Virtual Private network Connection” and click “next”.



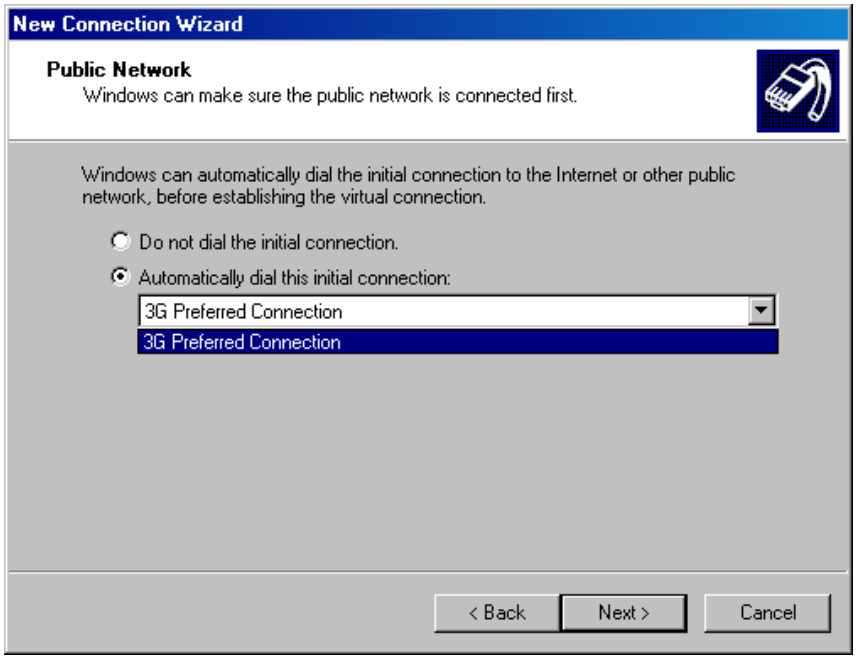
- At the next screen a name for the VPN connection must be entered. Please enter your preferred name for this Microsoft VPN connection and click “Next”



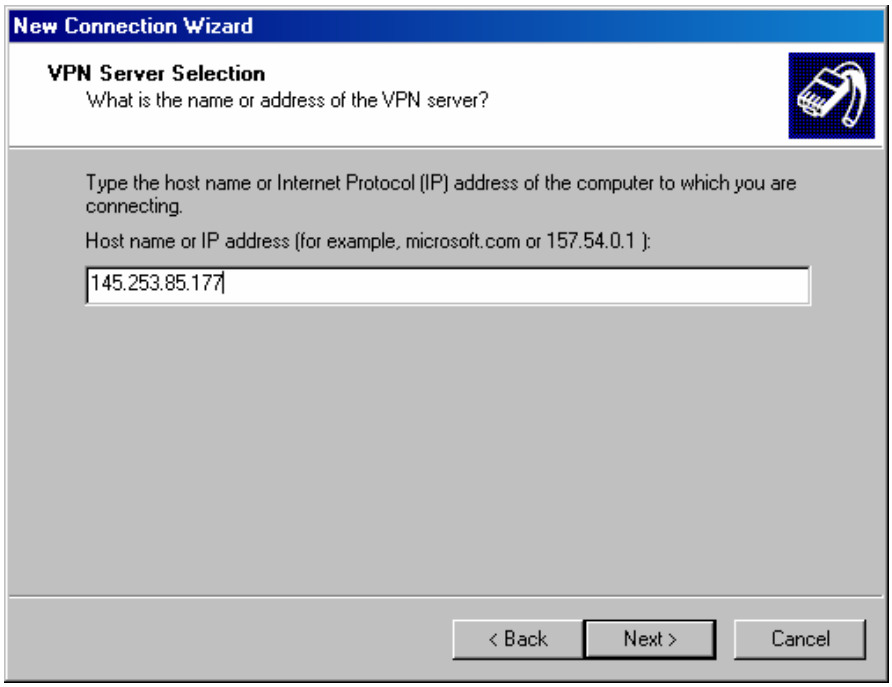
- For automatically dial a connection from a pre defined connection profile select the radio button “automatically dial this initial connection” and choose the preferred connection profile, otherwise the current connection is used.



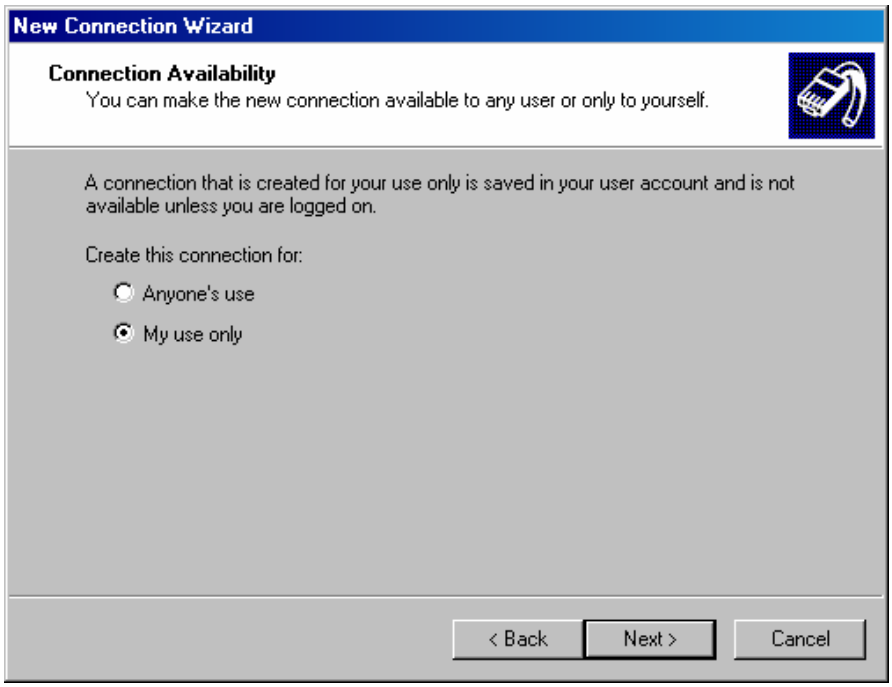
- Chose the preferred connection for automatic dial.



- After clicking “next” the Host name or IP address to the server you are connecting for VPN usage has to be entered.



- On the next screen a possibility is given to choose whether the connection is created for “anyone’s use” or only “my use”.



- After clicking the “next” button the connection wizard will be completed.

- After clicking finish the new connection starts with prompting for username and password

- After entering the correct credentials for the Microsoft VPN L2TP/IPSec user the connection can be established by clicking “Connect”

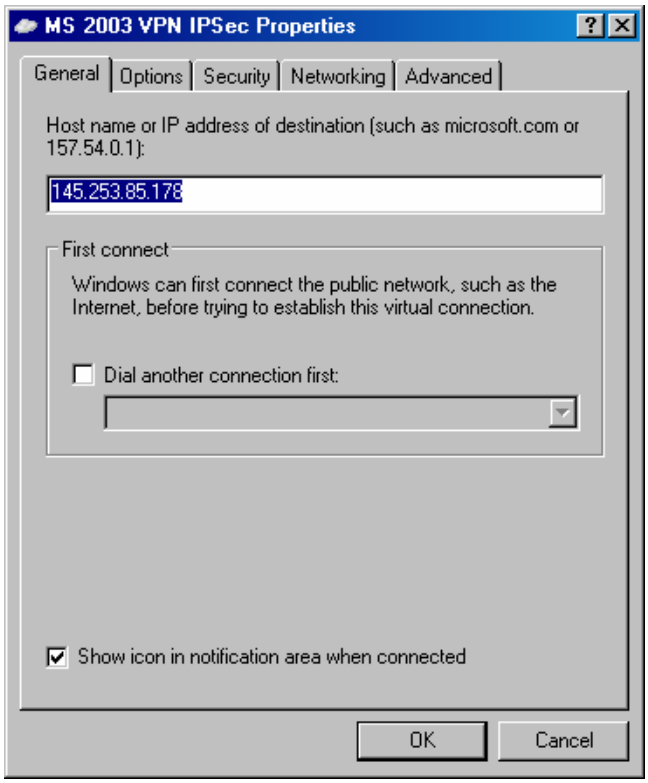
© VODAFONE GROUP 2007

2.3 Configuring a new Client connection (Microsoft 2003 VPN L2TP IPSec Client)

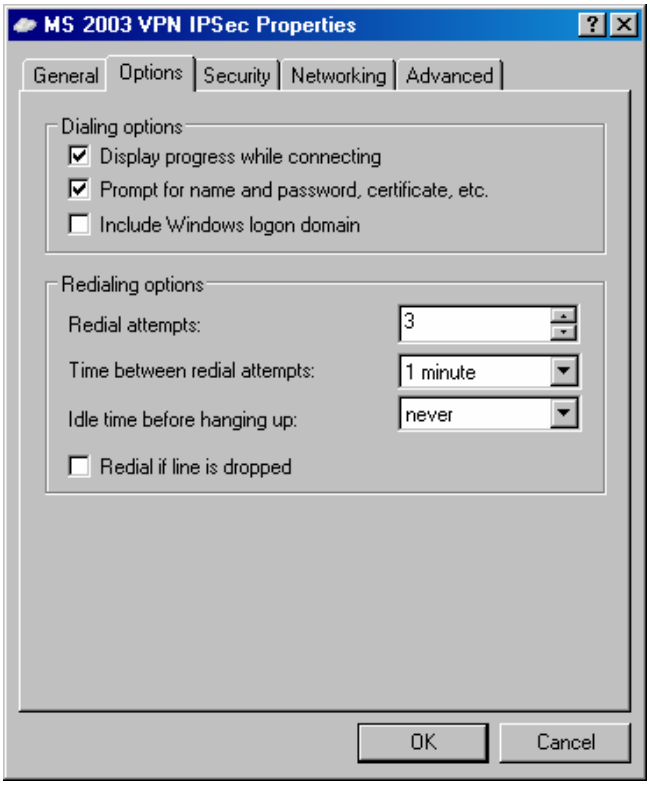
In this example, the client is configured for a typical scenario. The setup here is matched to the configuration of the Microsoft 2003 VPN described in the document in appendix A: “VPN - MS_2003_L2TP_IPSec_Appendix_A_Concentrator.doc “

- After starting the VPN connection profile this profile could be configured as shown in the following steps.

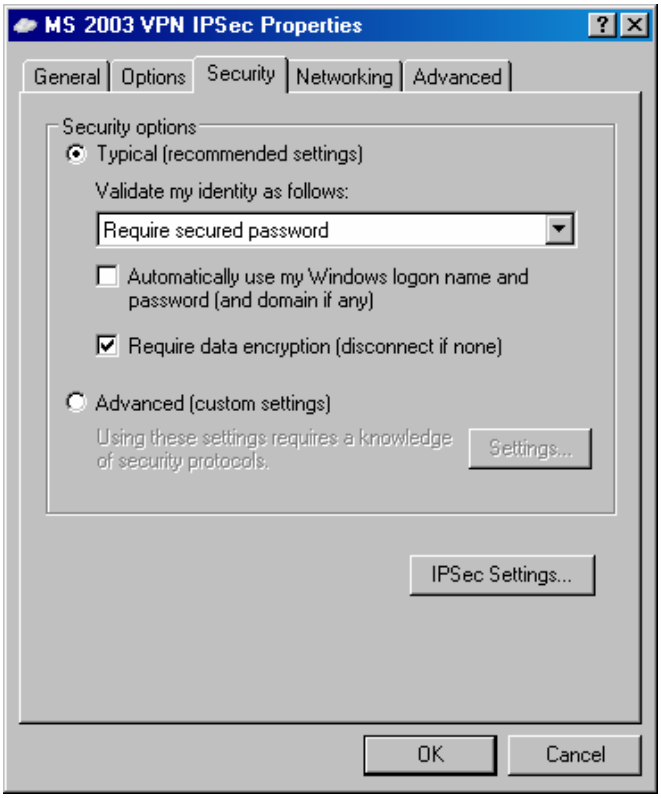
- Click on the “Properties” button to get the configuration tabs for the MS 2003 VPN connection and the first Tab “General”.



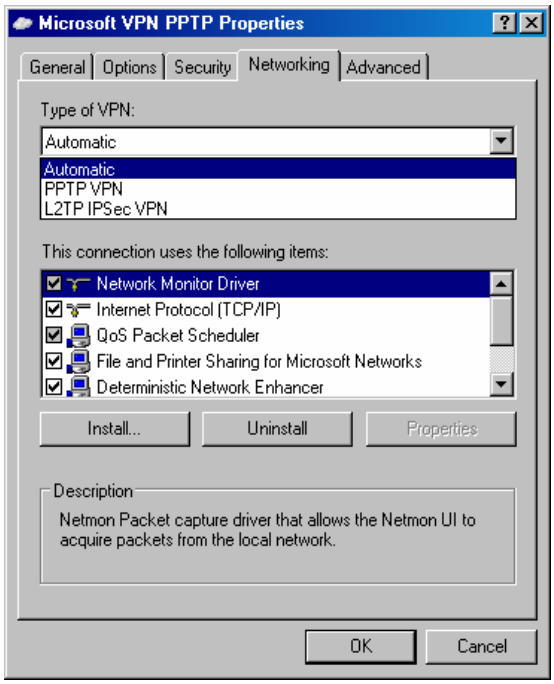
- The “Options” Tab provides the following screen:

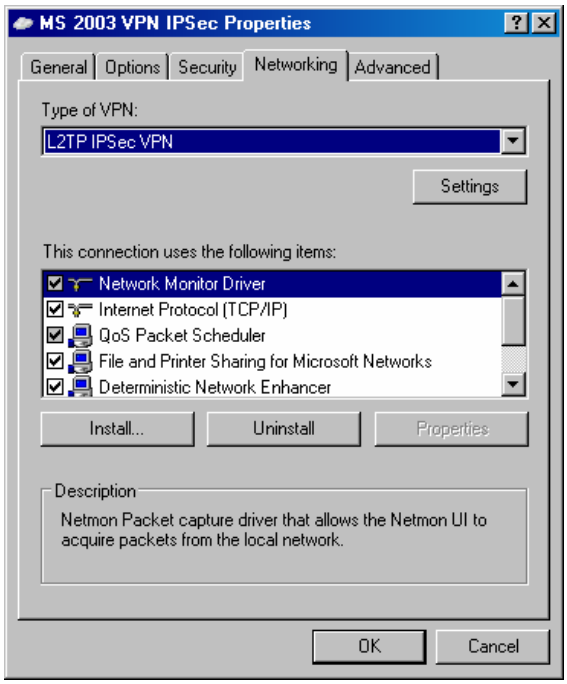


- The “Security” Tab provides the following screen:



- The “Networking” Tab provides the following screen:

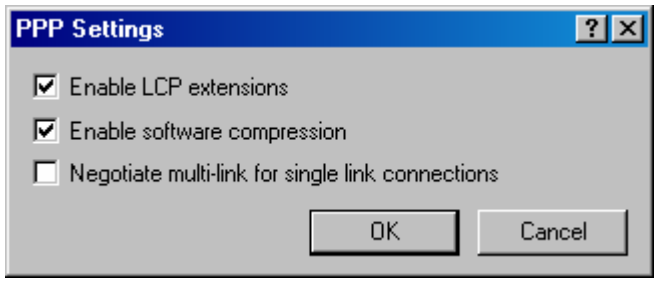




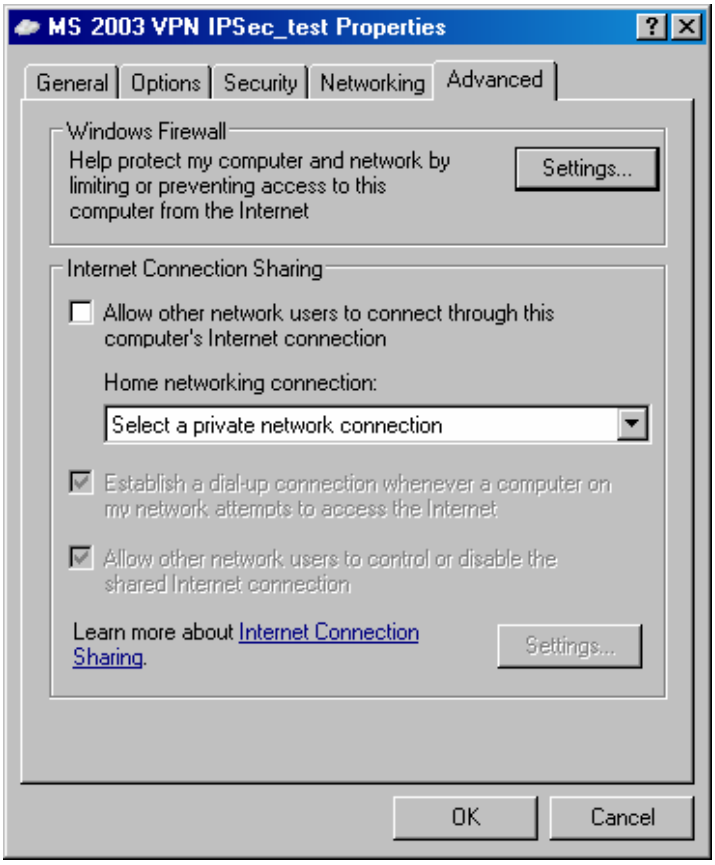
© VODAFONE GROUP 2007

- After choosing the Type of VPN: Here L2TP IPSec VPN it is possible to configure via the “settings” button following settings for the connection:

1. Enable LCP extensions
2. Enable software compression
3. Negotiate multi-link for single link connections



- The “Advanced” Tab provides the following screen:



© VODAFONE GROUP 2007

2.4 How to configure L2TP/IPSec connection by using Preshared Key Authentication

For correct IPSec VPN usage, following Registry Keys must be modified as follows:

To add the ProhibitIpSec registry value to your Windows 2000-based computer, follow these steps:

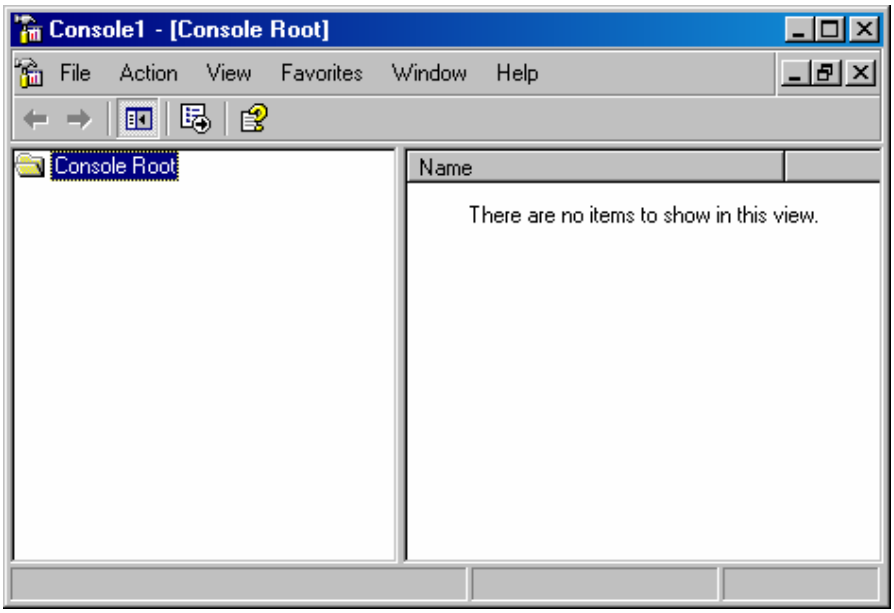
1. Click **Start**, click **Run**, type regedt32, and then click **OK**.
2. Locate, and then click the following registry subkey:
   HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Rasman\Parameters
3. On the Edit menu, click Add Value.
4. In the Value Name box, type ProhibitIpSec.
5. In the Data Type list, click REG_DWORD, and then click OK.
6. In the Data box, type 1, and then click OK.
7. Quit Registry Editor, and then restart your computer.

See http://support.microsoft.com/kb/240262/en-us for more information.

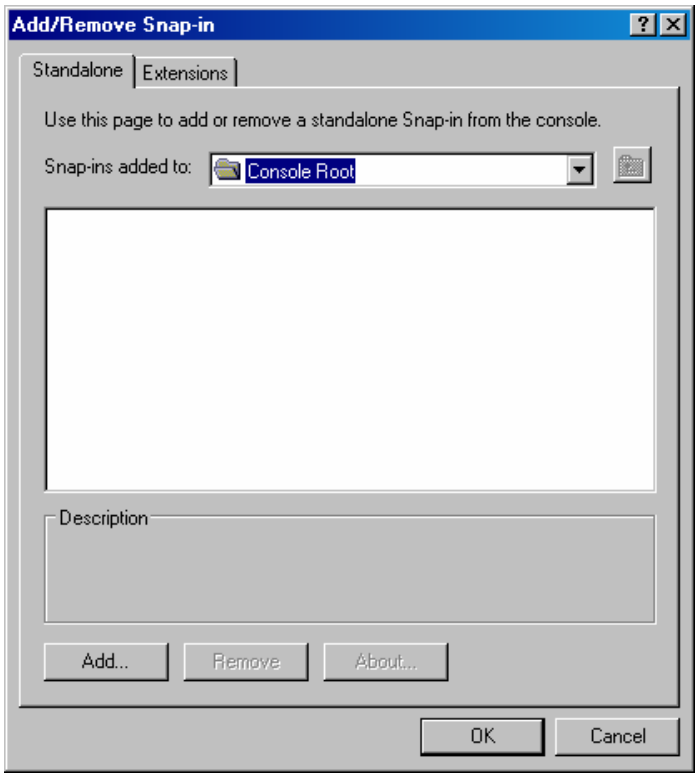
© VODAFONE GROUP 2007

2.4.1 How to create an IPSec policy for use with L2TP/IPSec Connections by using a preshared key

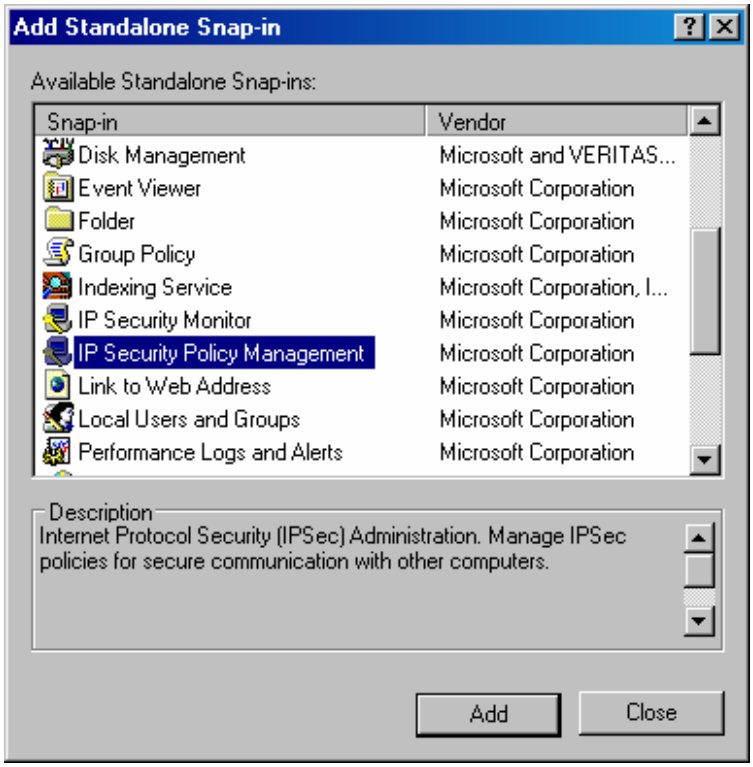
Click “Start” and select “Run” -> type in MMC to open the snap in console:



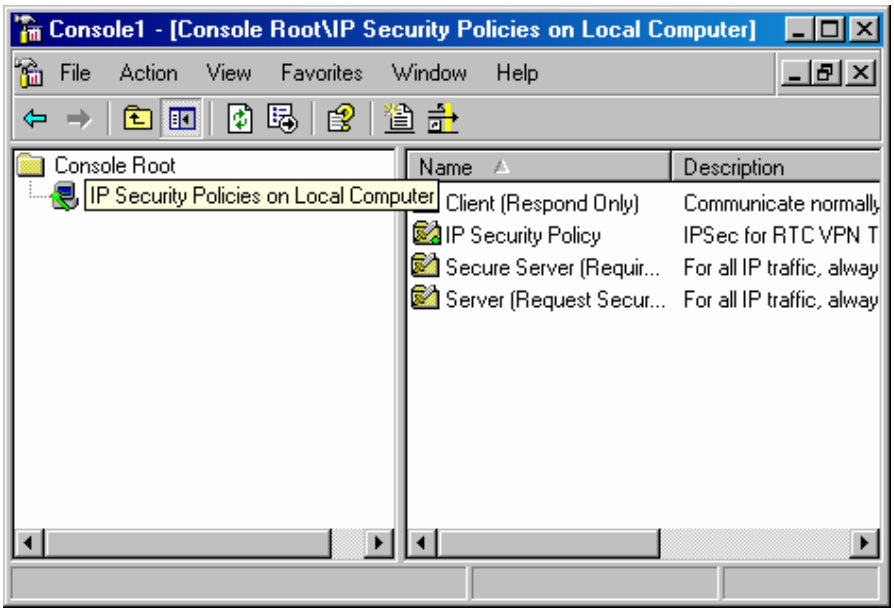
Select File and Add/Remove snap in!



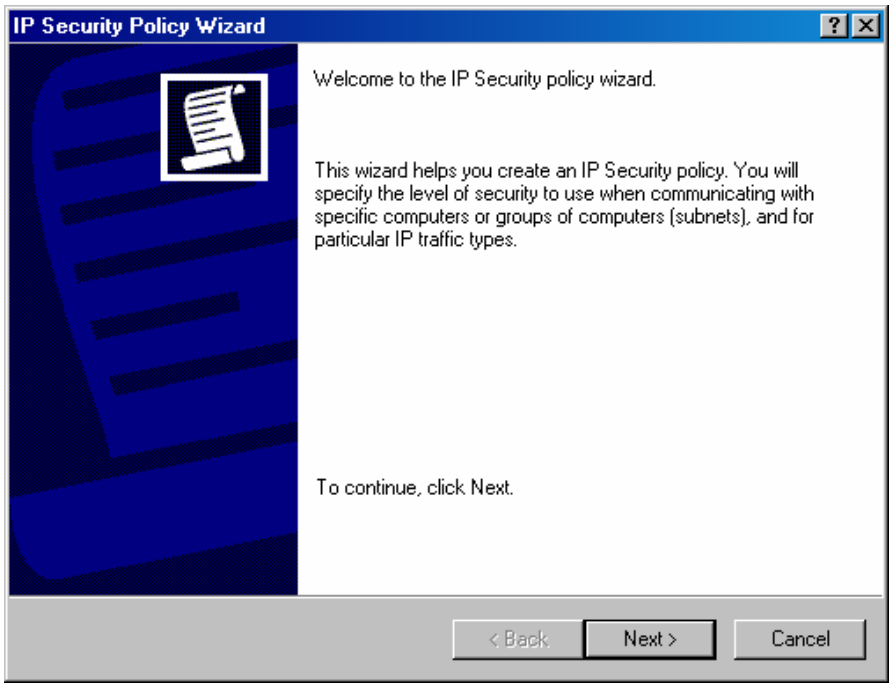
Click “add” and select "IP Security Policy Management" then click "add".



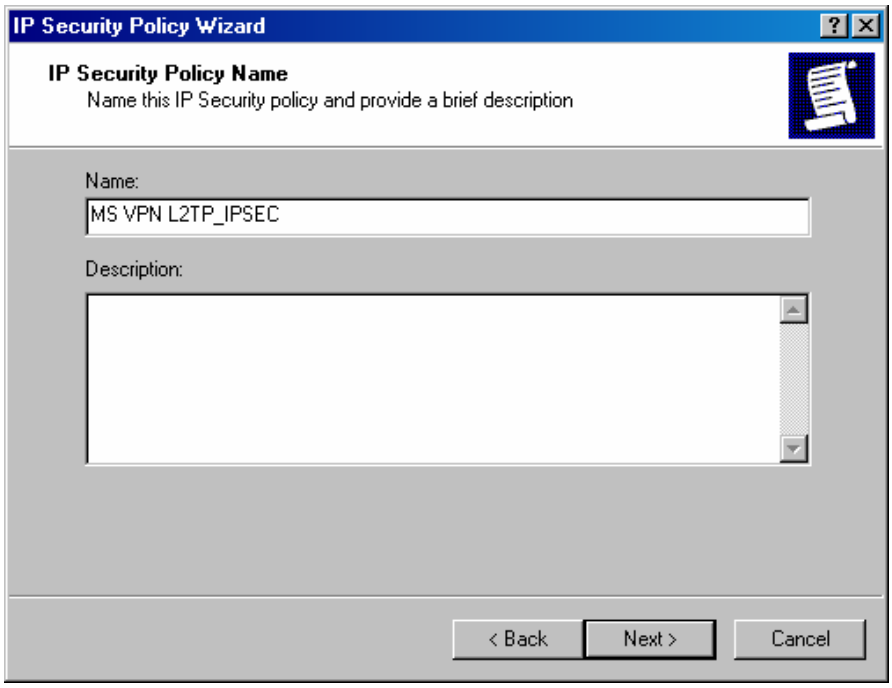
Confirm the previous screens with finish and click close.



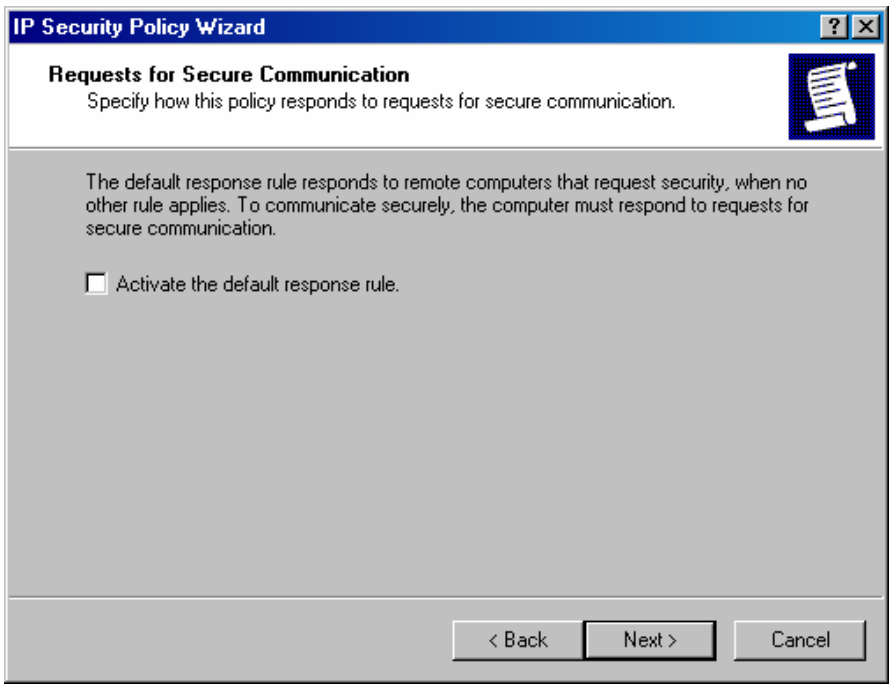
Right click the “IP security policies on local computer” and select "create IP security policy" and follow the screens



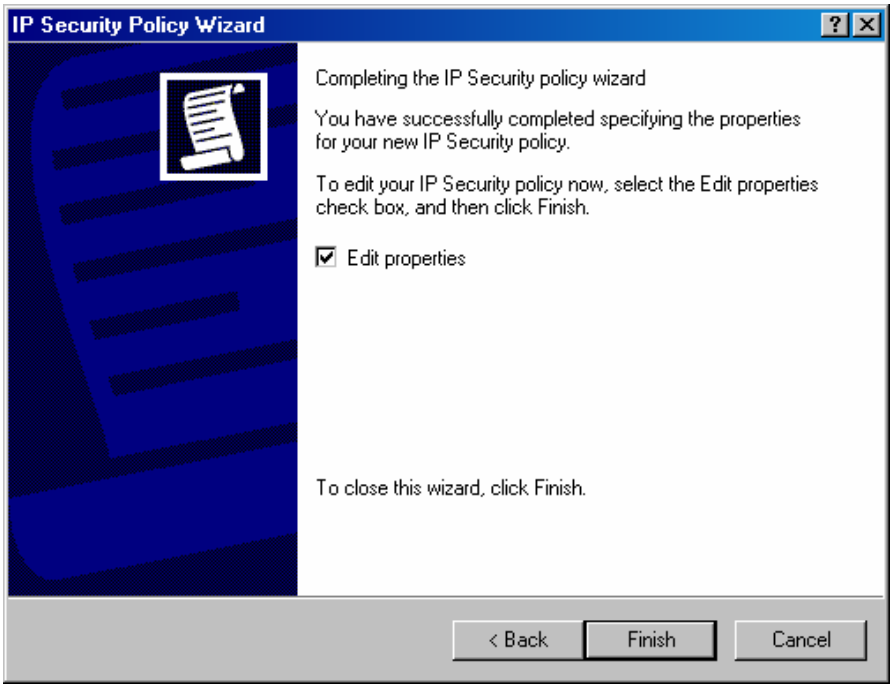
Click “Next” to step further.



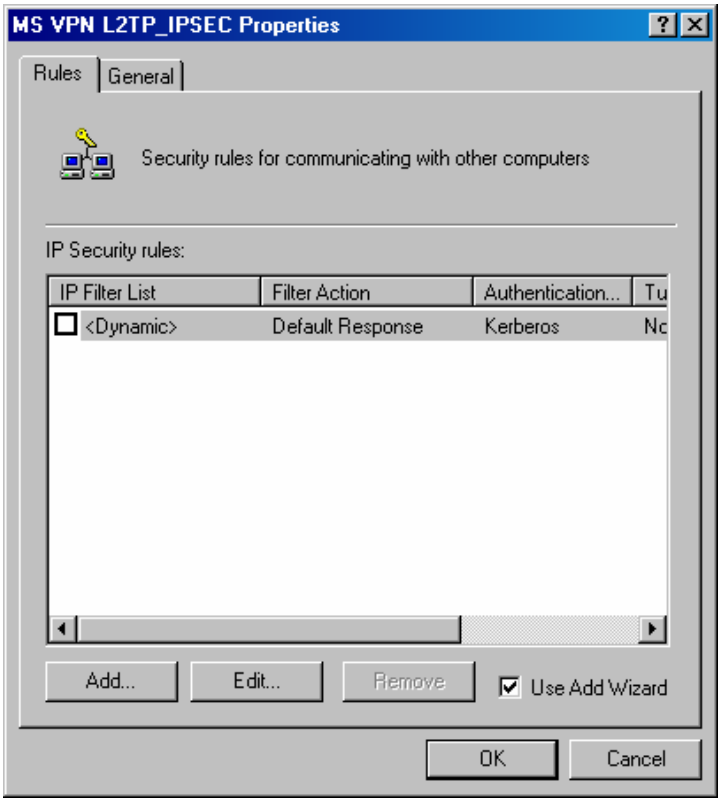
Type in a name and description for this policy then continue by clicking “Next”.



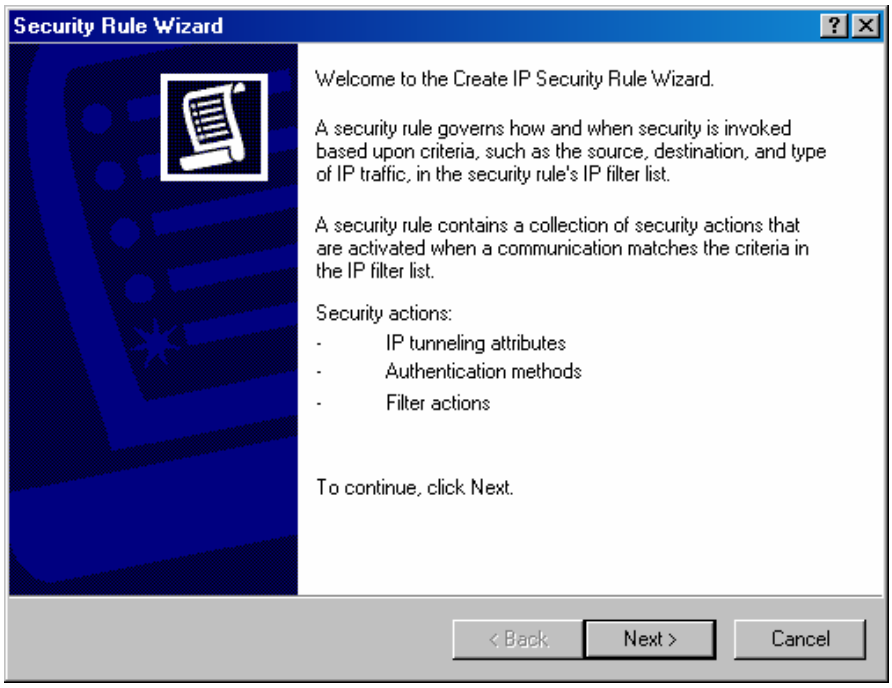
Clear the check box for "activate the default response rule" and click "next".



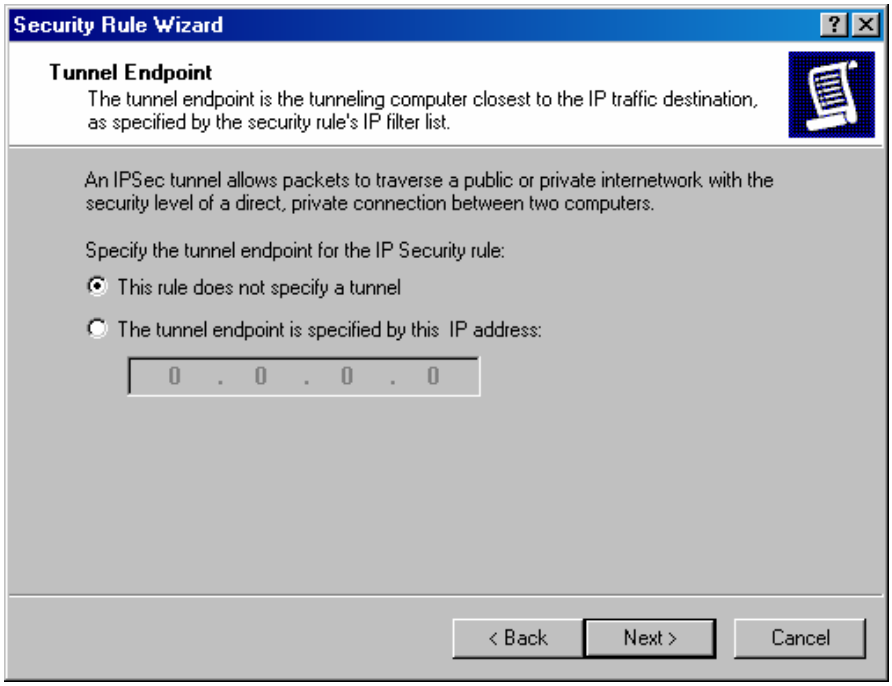
Click "finish"



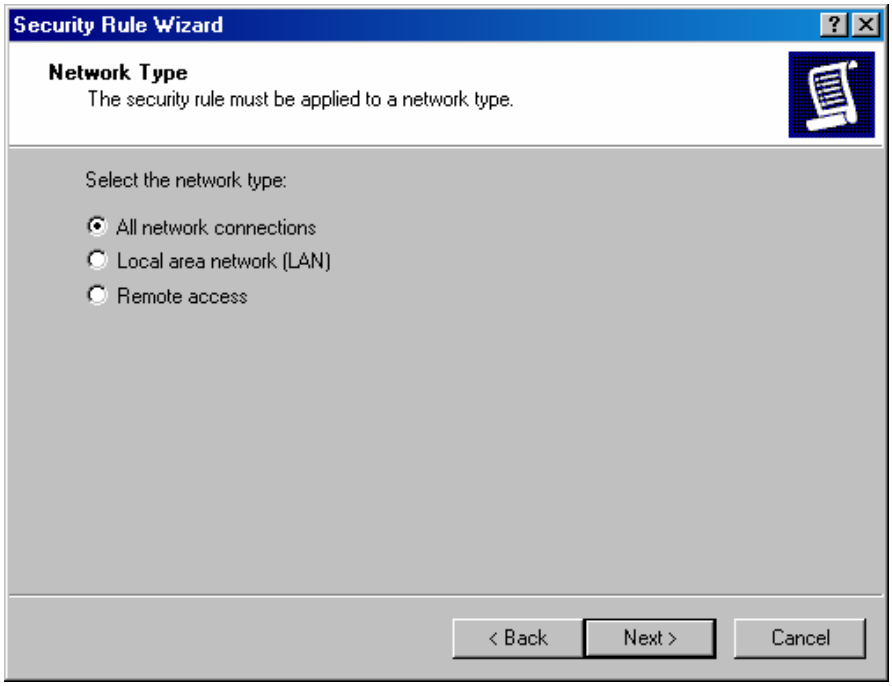
At the created policy window click on "add" to create a security rule and follow the screens with filling in the needed details. It is recommended to use the “Use Add Wizard” and follow the screens.



Click “Next”.

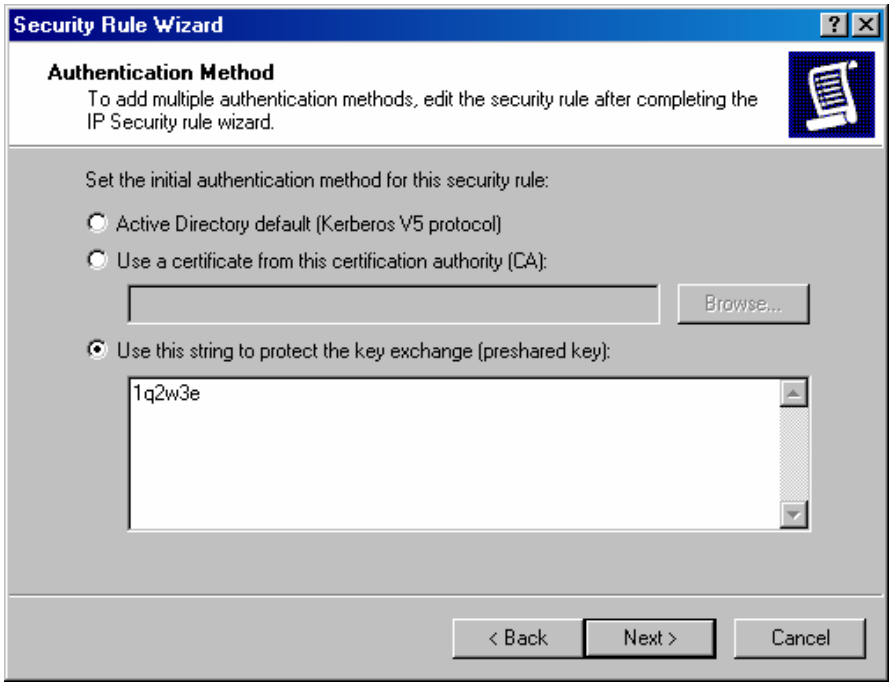


Select the Radio Button “This rule does not specify a tunnel”

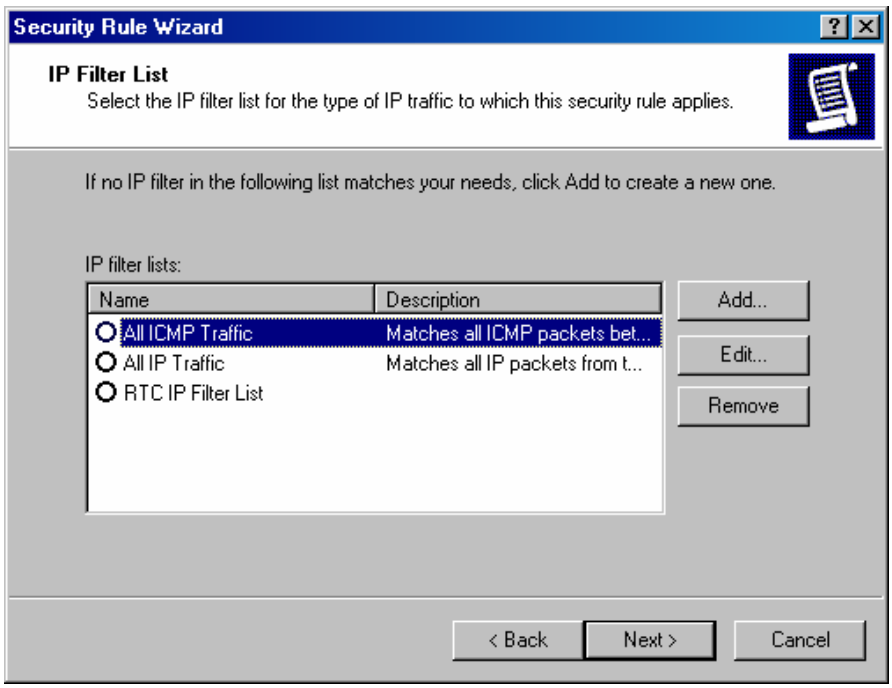


Select “All network connections” and click “Next”.

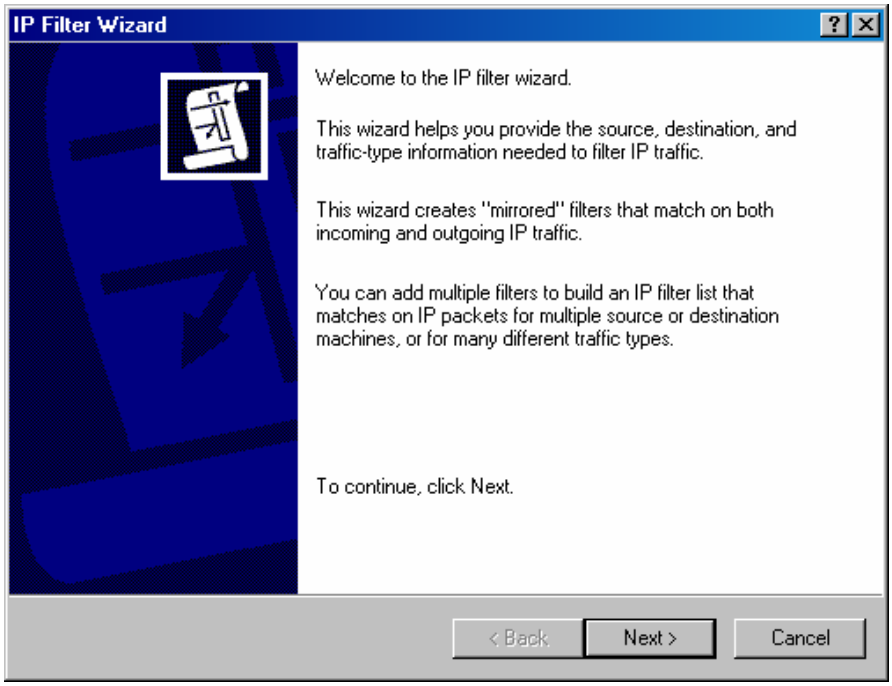
© VODAFONE GROUP 2007



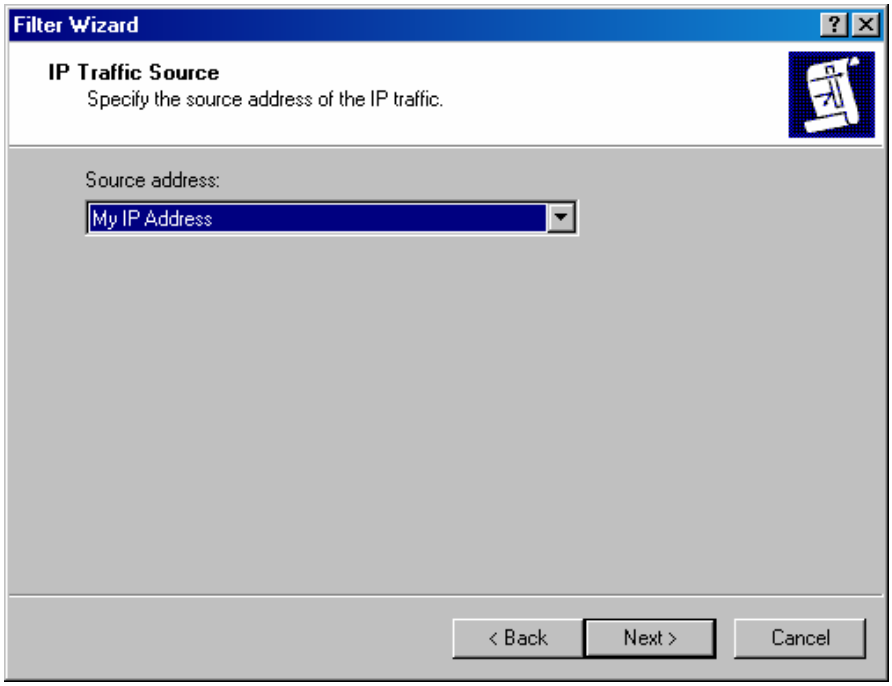
Enter the provided “Preshared Key” and click “Next”. Following screen provides IP Filter Lists and it is necessary to add a Filter.



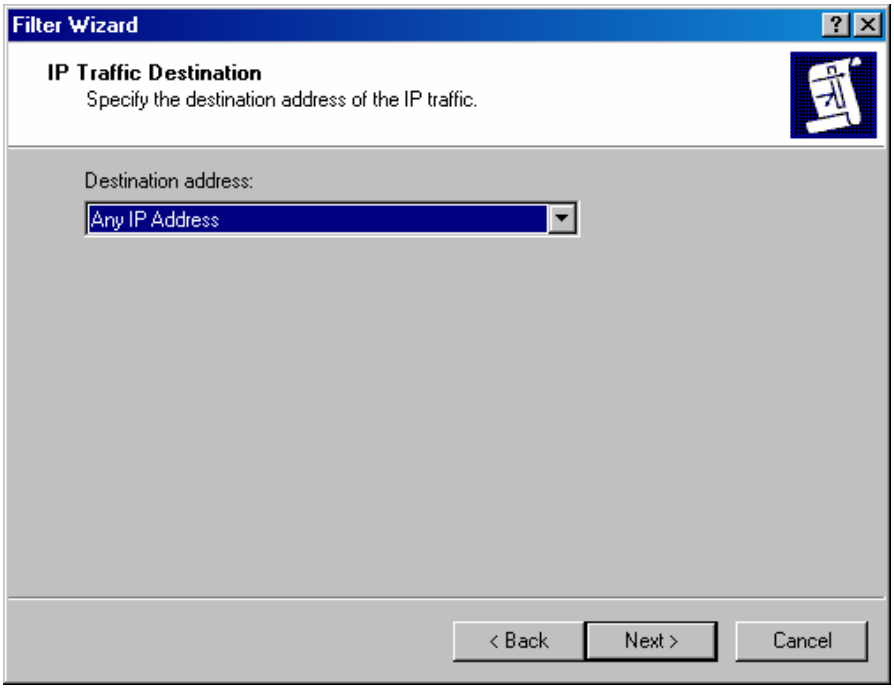
Click “Add” to start the “IP Filter Wizard”



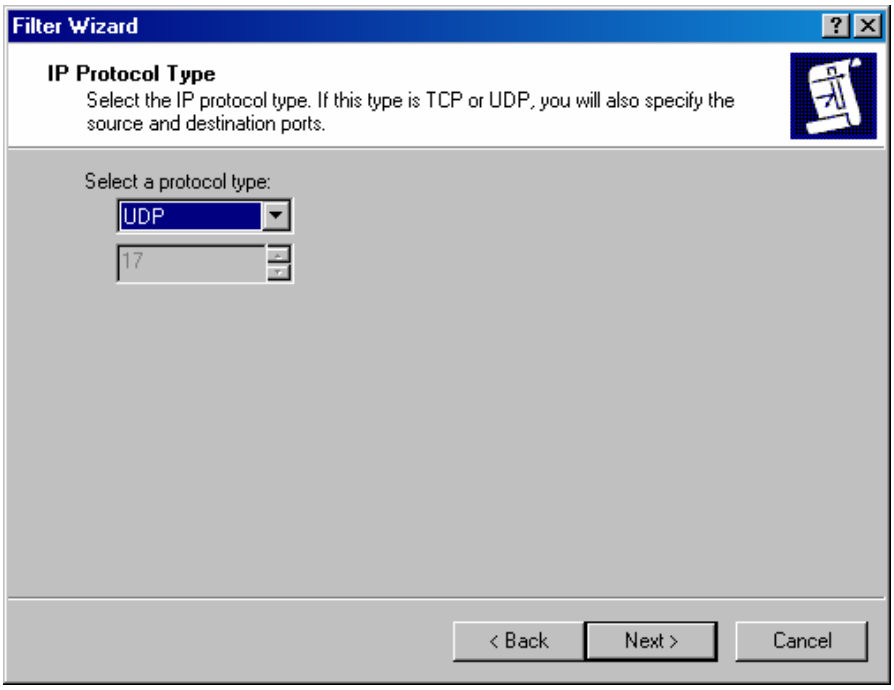
Confirm the window with “Next”



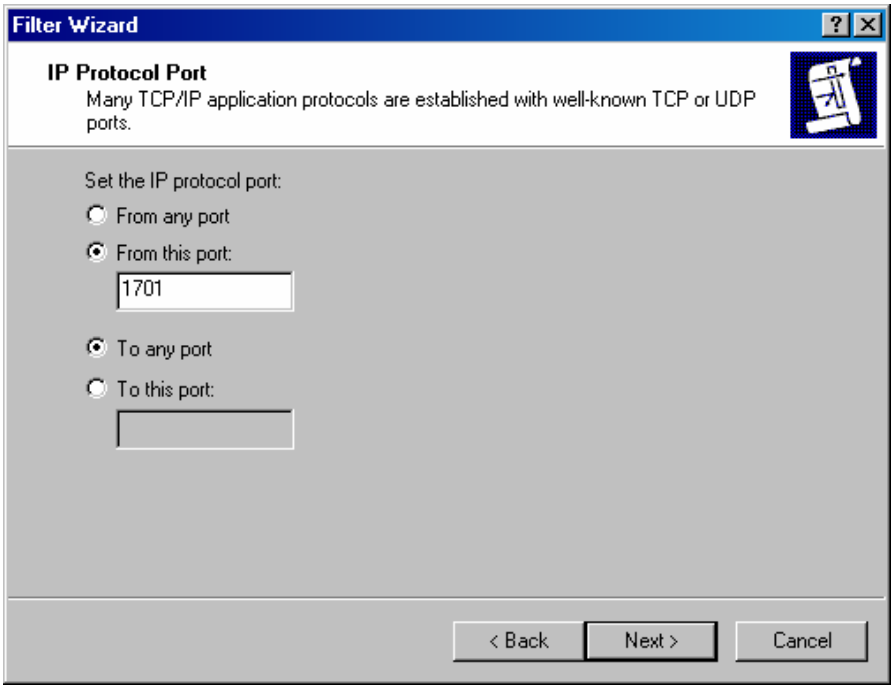
Select “My IP Address” for the source address and click “Next”



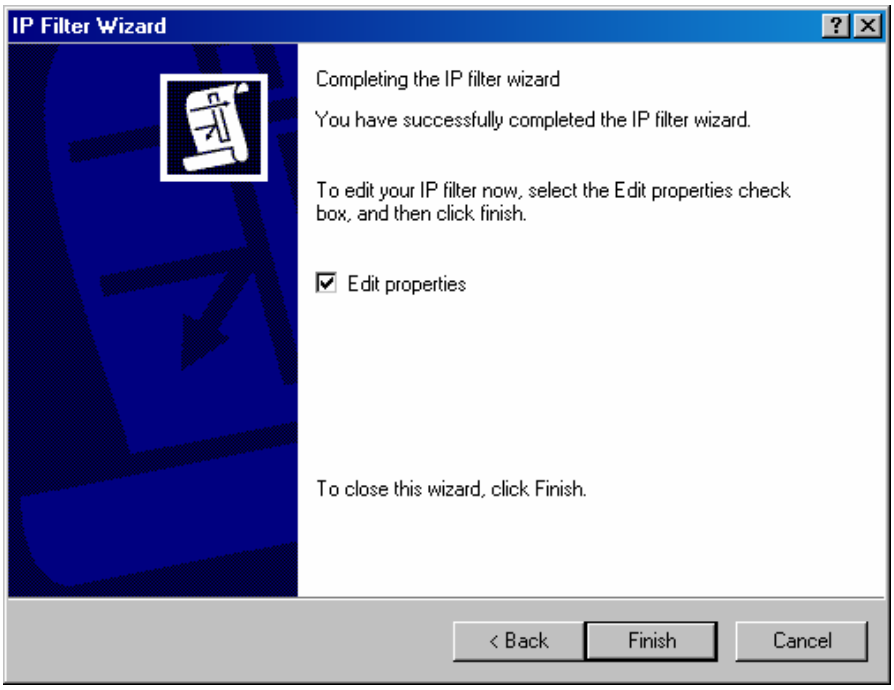
Select “Any IP Address” for the Destination address.



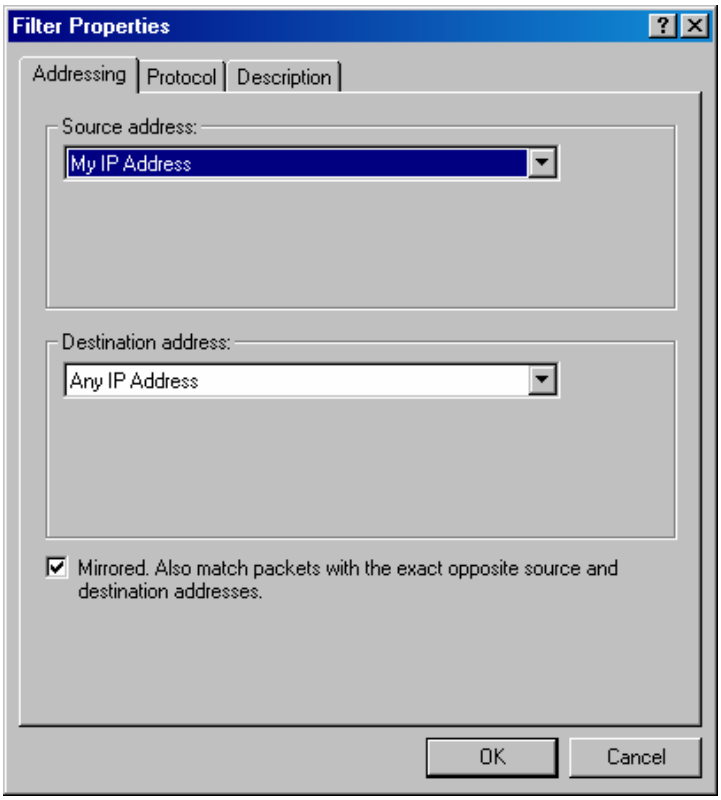
Select “UDP” for the used protocol type and click “Next”.



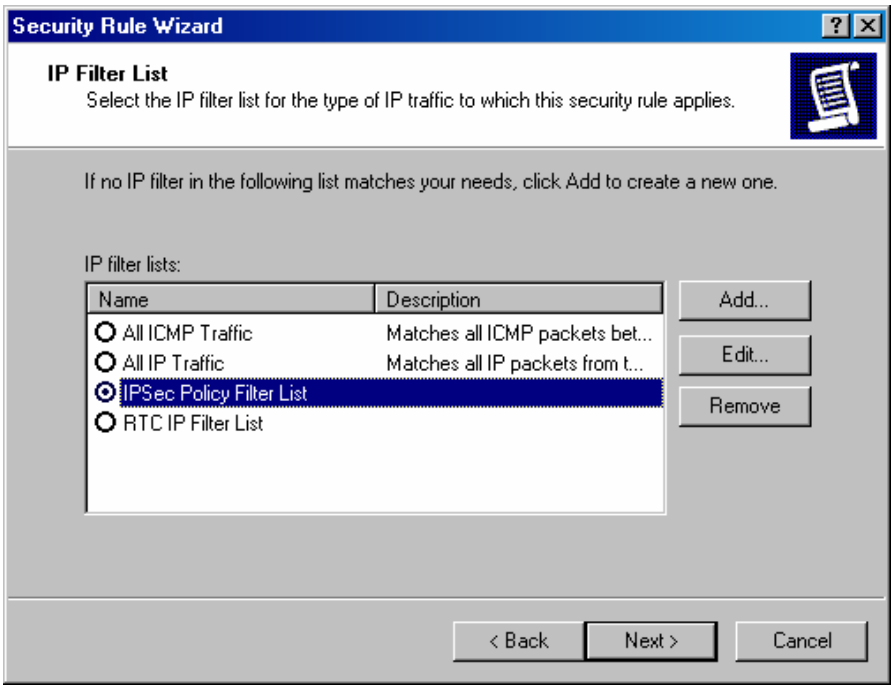
Edit the IP protocol port to “1701” and check the “To any port” radio button and click “Next”



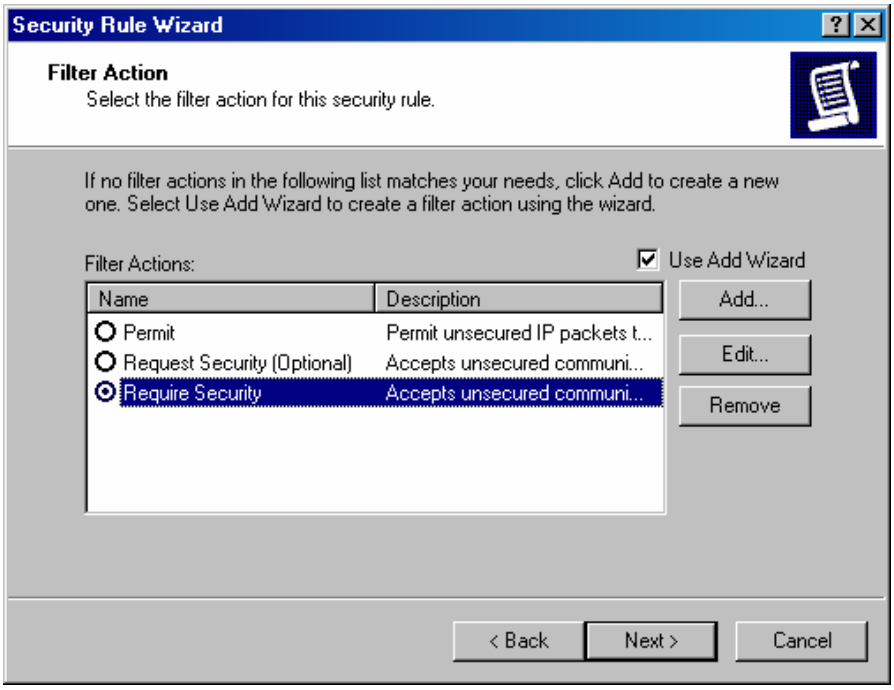
Click “Finish” to exit the wizard (if the “edit properties” is checked, the Filter Properties window is appearing).



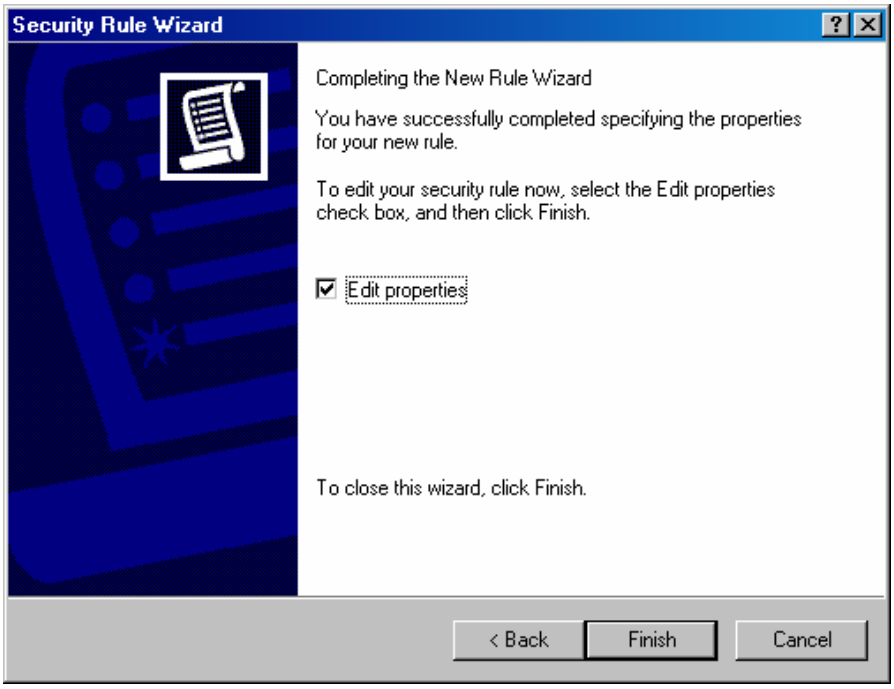
Make sure the “Mirrored. Also match packets with the exact opposite source and destination addresses” is checked! And click “OK”.



Select the newly generated IP Filter and click “Next”

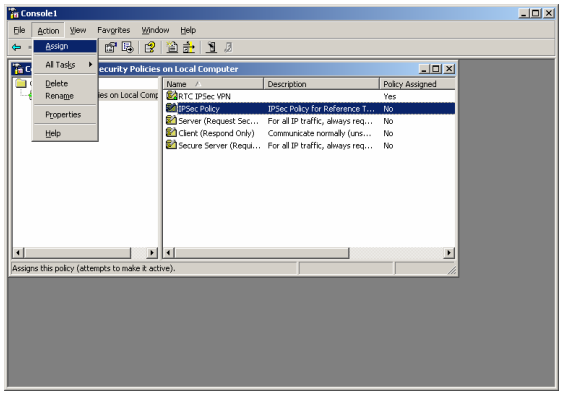


Check the “Require Security” Radio button and click “Next”



Click “Finish” to close the wizard.

Back in the Management Console, you must assign the created IPSec policy by using the menu entry. Highlight the correct policy and select “Action” -> “Assign” from the menu.



3 Configuration & Connection Using VMC Software

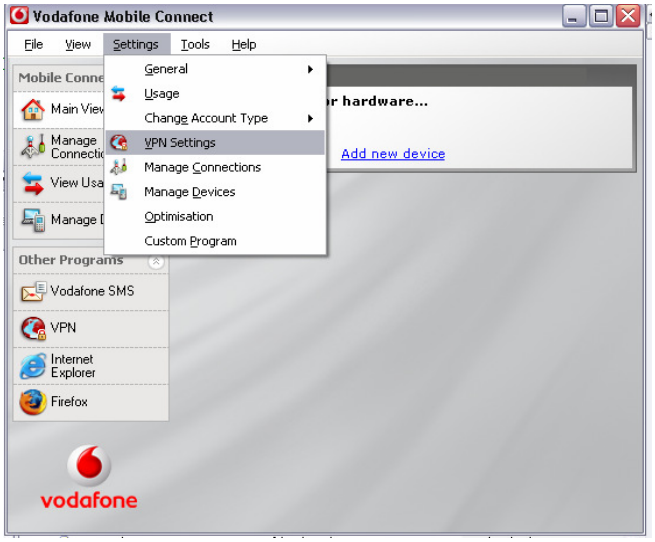
This chapter is used to describe possible configuration possibilities for using the VPN client in conjunction with the current released Vodafone Mobile Connect application.

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:

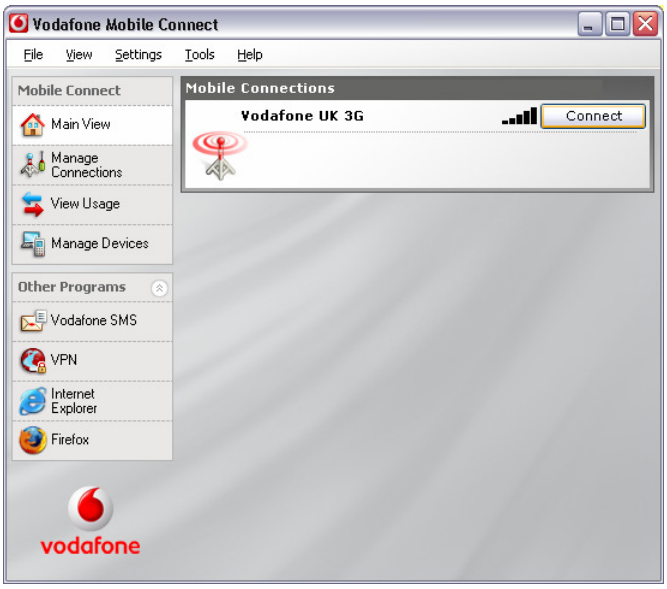
1. The '**Connect**' button is found in the 'Mobile Connections' window of the main screen.
2. The VPN button is found in the '**Other Programs**' section on the left side of the main view. If the Vodafone Mobile Connect software is not visible, it may need to be expanded from the mini view or from the 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)

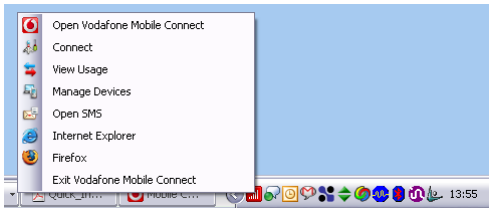
With a SIM card inserted into your datacard (or USB modem), to establish a connection:

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



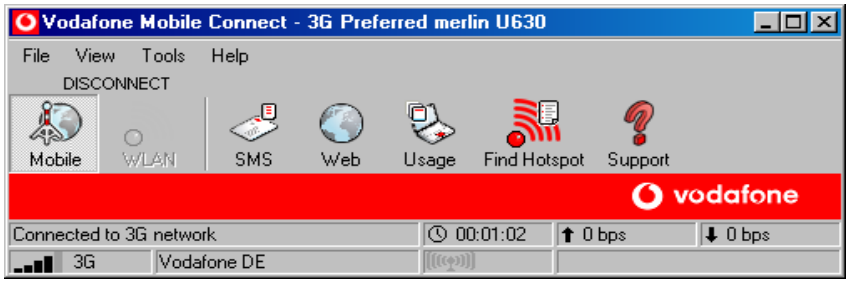
2. In the mini-view, use the **Connect** button, or

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:

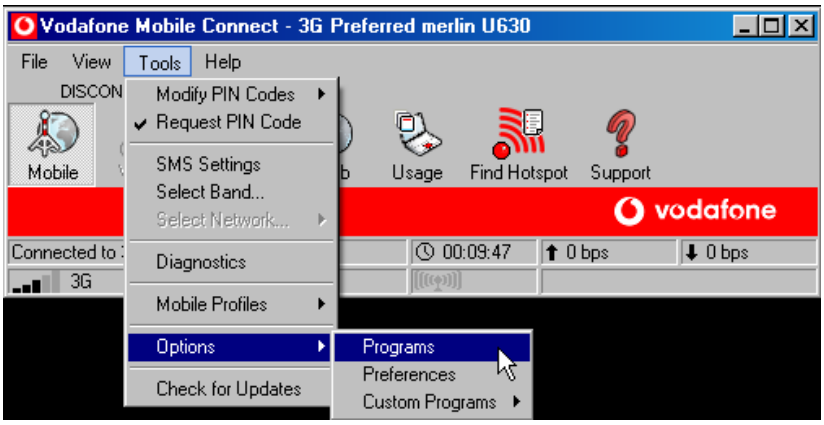


Press the **Mobile** button in the CONNECT/DISCONNECT area of the toolbar

3.3 Configure VMC for the VPN Client

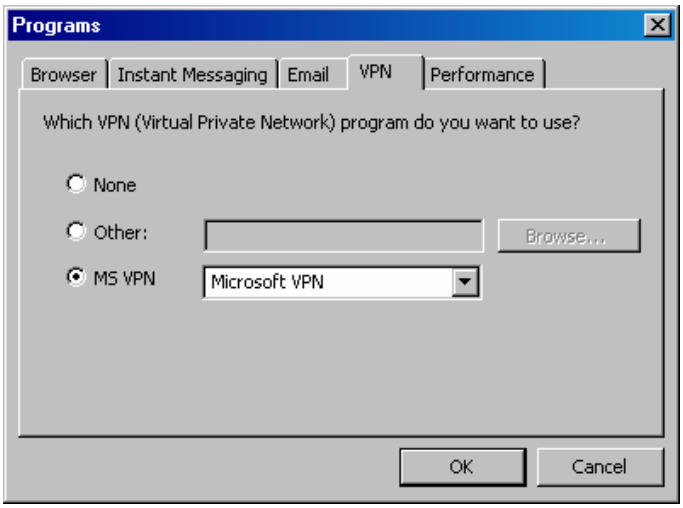
Note: The following steps apply to the legacy version of Vodafone Mobile Connect software R7 and earlier. See notes above on the process using the new R9 version.

- Configure your VPN Client as follows to start it from within the Dashboard.



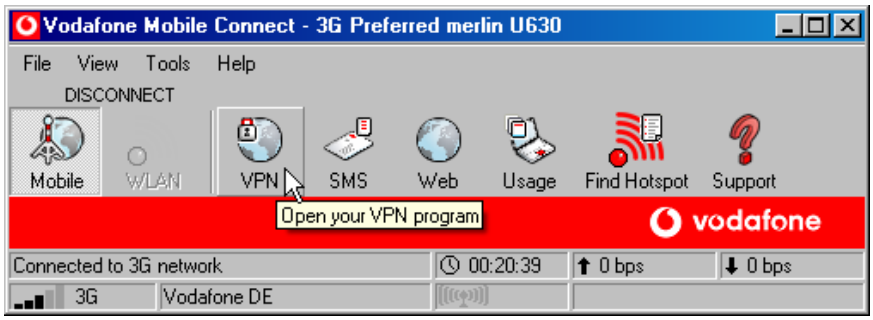
- Choose Tools | Mobile Profiles | Options | Programs and switch to “VPN” Tab

- Check the radio button “MS VPN” and select the generated profile for the Microsoft L2TP/IPSec connection.



- Confirm your configuration with “OK”
- Enter the username and password and click “Connect” in the main dialog and the Client will establish a VPN connection to the Server.

3.4 Establishing a mobile VPN connection



- 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 Microsoft Windows 2003 L2TP/IPSec VPN Client has to be started manually. It is possible to change the starting option to start automatically e.g. from the “Start up” Windows menu. Also the connection to the Server, by default, must be made manually by pressing the “Connect” button in the VPN Client. This can also be changed to connect automatically. In order to achieve this, the user has to change the following settings:

- Make sure the VPN profile is configured properly
- On the connection window select “Save this username and password for the following users:”
- Click on the “Properties” button on the connection window
- On the “general” tab check the box for “Dial another connection first” and select the profile for the Vodafone Mobile connection
- On the “Options” tab deselect the check box for “Prompt for name and password…”
- Using the Windows drag and drop feature you can now copy a shortcut of the VPN connection to the “Start up” Windows menu

The precondition for establishing a connection automatically using the Vodafone Mobile Connect card is an inserted SIM without a PIN or a scenario where the PIN is already entered.

4.1 Testing Results & Observations

Due to our FTP tests, it was necessary to modify browser options within the Internet Explorer as follows:

- Uncheck the “Enable folder view for FTP sites” setting
- Uncheck the “Use Passive FTP (for firewall and DSL modem compatibility” setting
- HTTP 1.1 settings are not necessary, but do not affect the FTP usage

This may not be necessary on other systems.

4.2 “Keep-alive” Frequency

If NAT-Traversal is activated, as is necessary with most countries GPRS and 3G services, the “Keep-alive” packet frequency defaults to 5 seconds. This will cause a comparatively high administrative traffic volume. Setting the “Keep alive” packet frequency to 15 to 30 seconds is fully sufficient.

© VODAFONE GROUP 2007

5 Connections to Different Services

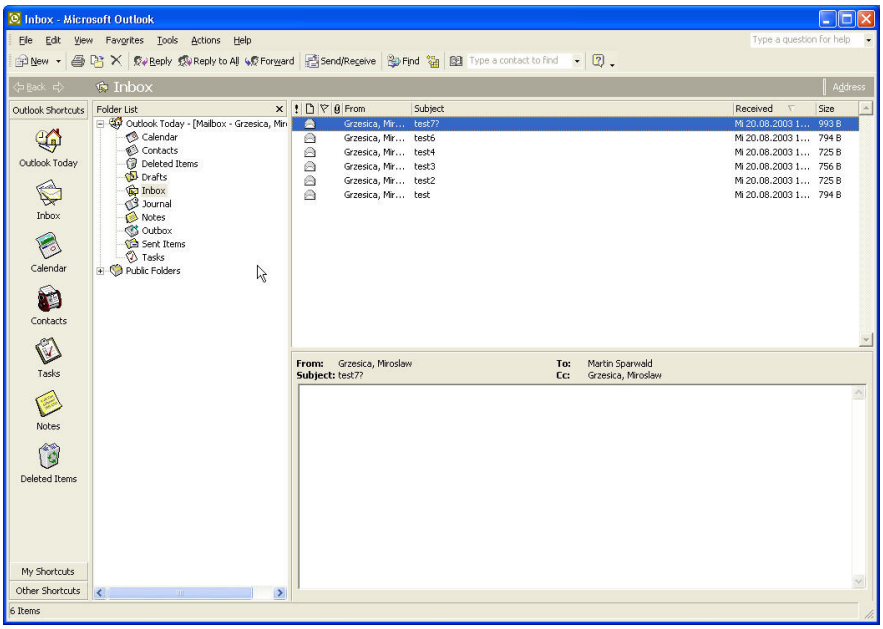
You can connect to all services via the VPN tunnel; you can connect to if you are in your local LAN.

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

Caused on time-outs and other problems depending on 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.

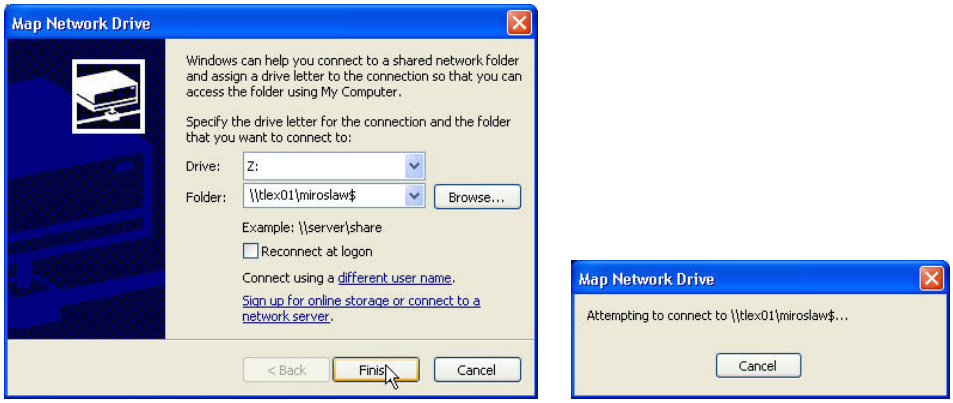


Figure 1 – Mapping Network Drive for VPN Access

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.

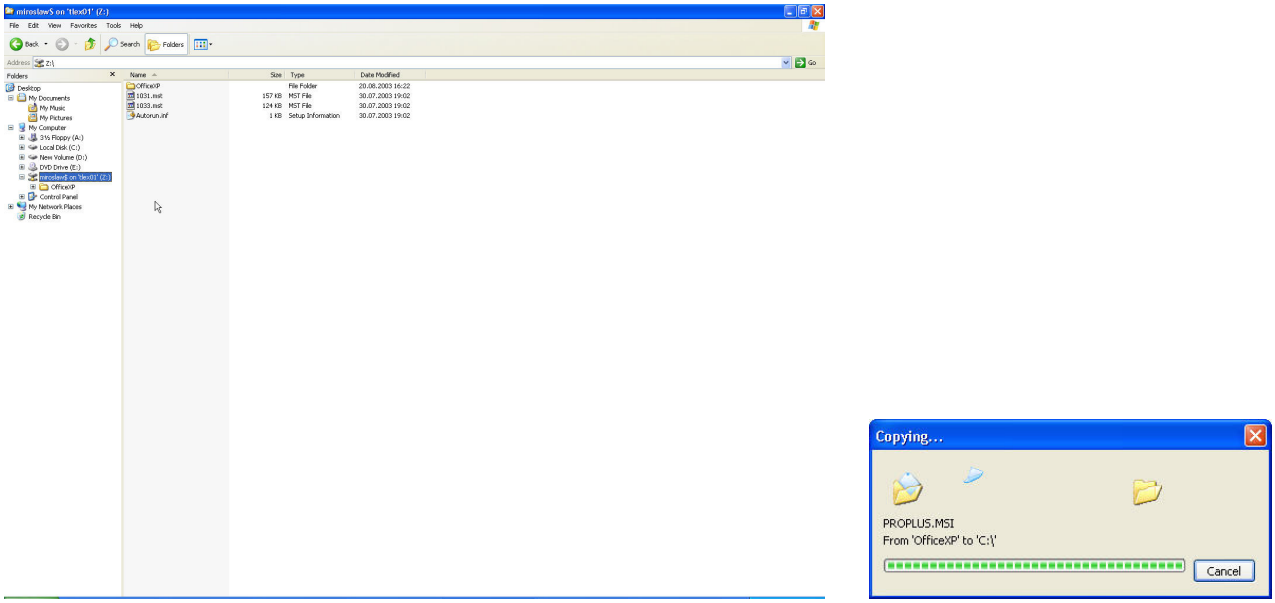


Figure 2 – File Transfer between LAN and local drives

**** End of Document ****