

WinPlug 2.1 Users Guide

Version: 0.95

Date: 23-11-1999

Copyright 1999 TUNIX O.S.C., Nijmegen

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without express prior written permission of the publisher.

1. Introduction

The WinPlug Users Guide presents a basic introduction to the WinPlug program and related software. It will show you how to install and run WinPlug and briefly discuss the features of the new release. For in-depth coverage of all the functions and possibilities of WinPlug you are referred to the *WinPlug manual pages*.

1.1 WinPlug 2.1

WinPlug is a program that provides secure tunneling over untrusted networks. Users are authenticated and authorised. WinPlug encrypts the data traffic, providing a safe environment for telecommuters and mobile users who wish to login from a remote location into the company network.

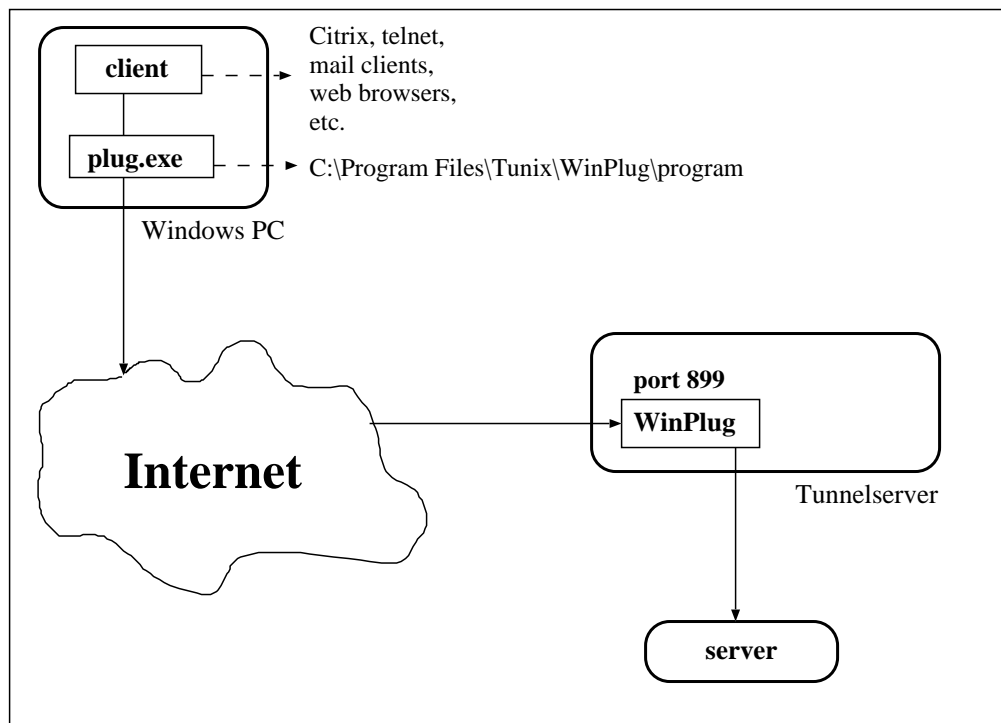


Figure 1 Connection diagram

1.2 New features in release 2.1

Full support for FTP protocol

FTP's backconnect caused commands like `dir`, `get` and `put` to be rejected by previous versions of winplug. Version 2.1 supports FTP connections by monitoring the command channel for such commands and in response opening a backconnect tunnel.

WinPlug 2.1 resides in Windows tray

This avoids that users exit the tunnel software by accident and grants easy access to application icon.

Support for WinSock 2

WinPlug 2.1 uses WinSock2 to allow accessing interface information. WinSock2 is standard on Windows NT and Windows 98. Using WinSock2 on Windows 95 requires an IP stack upgrade available from <ftp://ftp.tunix.nl/pub/mswindows>.

Support for NetBIOS protocol

WinPlug 2.1 accepts incoming requests from any local IP-address (like ethernet and dialup addresses) and not only from `127.*.*.*` addresses. This solves the problems with NetBIOS connections. NetBIOS can now be mediated for Windows/NT clients.

Enhanced GUI

Overview of finished, rejected and open connections. More information on errors.

Improved logging through Audit Trail

The Audit Trail shows a connection's progress from start to finish.

Extra property sheets

Traceroute, system information and overview of local interfaces can be displayed.

Autofocus on authentication window pop-ups

When using authentication, a user can type password without having to click the window first. The authentication module now also supports Safeword tokens and SecureID tokens.

Maximum number tcp-rules increased from 100 to 300

User can specify up to 300 combinations of destination hosts, tunnelserver, user, port and protocol.

Support for specifying separate tunneluser

Apart from defining tunnelserver and tunnelport, tunneluser can also be specified (may or may not be the same as the windows user) in the tunnel configuration. This value may also be overruled from the command line.

Fallback tunnelserver

This versions supports the specification of multiple tunnelservers for a particular destination. This allows access through alternate firewalls *and/or* alternate Internet links (like an ISDN backup).

DNS resolution

Previous versions of WinPlug required that the tunnelserver address could be resolved. This caused connections to fail if DNS delayed or malfunctioned. This featured was removed in this version to avoid this problem.

Network error logging

Previous versions of WinPlug showed network errors in the *audit trail*. To make them more visible to ordinary users, errors are now displayed in a popup window.

Timeouts

Busy WinPlug tunnelservers could be trashed by unused tunneling processes that where left if connections where not properly shutdown. This version supports timeouts on tunnelservers.

Compatibility

Older clients can connect to a version 2.1 tunnelserver. Version 2.1 clients can not connect to older versions of the tunnelserver.

1.3 WinPlug Features

- *Multiplexing (only 1 port used for tunneling)*
The previous versions of WinPlug used up to ten ports for tunneling. This release can use different ip addresses that can be mapped onto internal servers, even if the portnumbers are the same. The mapping is shown in paragraph 1.7.2.
- *User based permissions*
The firewall administrator can specify which user is allowed to do what, based on username, final destination and type of service. This is an improvement over the older 1.x versions which would give all WinPlug users the same privileges.

- *Session key generated with Diffie-Hellman*
Per session a random key is generated (i.e. keys are used for a single session only). This key is negotiated between the client and the server using the Diffie-Hellman algorithm. After the handshake a kind of proxy connection is established.
- *Support for strong authentication*
WinPlug can enforce strong authentication. When WinPlug is started, the user authenticates him/herself through a shared secret key which can either be stored on the PC's harddisk or on a chipcard. Next to this standard authentication the user may have to authenticate strongly using a tancode or a hardware token such as a dongle.
- *Support for automatic updates*
The system administrator can put new releases of the client on the firewall. The WinPlug client will detect updates and will present the user with a pop-up window asking whether or not he/she wants to update. The pop-up window will appear every time WinPlug is started, until the user relents and updates the client...
- *Support for NAT*
WinPlug supports various forms of Network Address Translation. Possible configurations include the original sender's address and the tunnelserver's address.

1.4 Installation of the WinPlug client

Installing the WinPlug client is fairly straightforward. Below we describe the procedure using the imaginary user `dilbert`. First, the tunnelserver's administrator generates a WinPlug disk for a new user. This disk contains everything user `dilbert` needs: the software, a shared secret and a pre-configured setup.

Before the install `dilbert` has to make sure that any other instances of WinPlug that are running, are shut down. The new client can otherwise not be installed properly.

User `dilbert` then runs `A:\SETUP.EXE` from the disk.

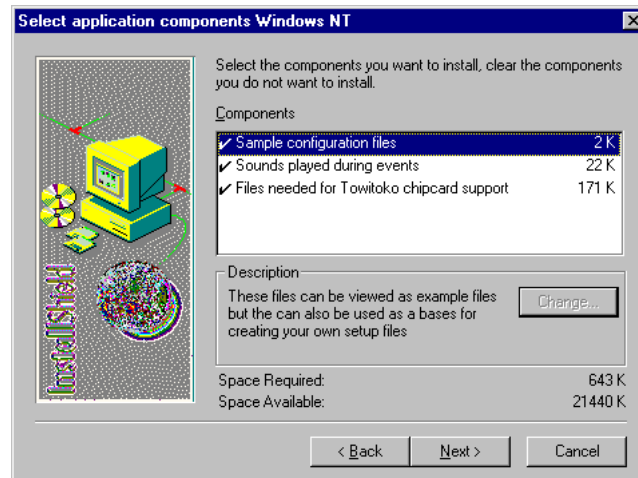


Figure 2 Installing applicational components

Here the user chooses which optional components he wants to install.

WinPlug offers the following in sound support: there are three different sound effects (respectively for starting, stopping and receiving an incoming connection).

The Towitoko smartreader is discussed in paragraph 1.5.

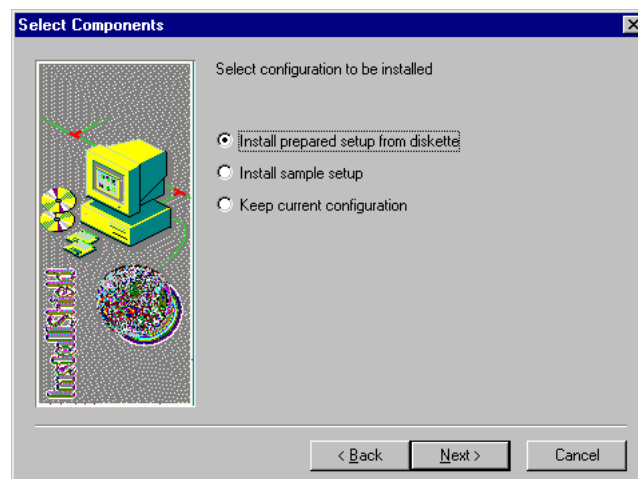


Figure 3 Choosing a configuration

This speaks more or less for itself. The pre-configured setup is available from disk, as is a sample setup (which contains several examples). These two options overwrite any old configuration files. It is also possible to keep existing configuration files. For beginning users the *prepared setup from*

disk is recommended.

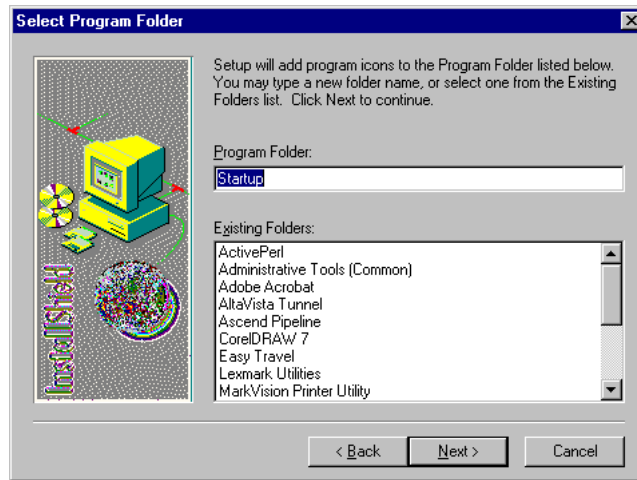


Figure 4 Selecting a Program Folder

Placing WinPlug in the Startup Folder will cause the program to start automatically everytime the PC is booted. Placing it in a different folder is also possible but the user will have to start WinPlug manually.

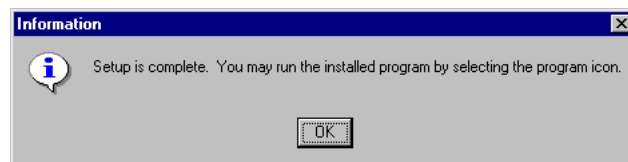


Figure 5 Setup complete

And that's all there is to it.

1.5 Installing chipcard readers

WinPlug supports the Towitoko chipcard reader. A chipcard can be used to store the shared secret or for authentication of the user. For installation of the Towitoko chipcard reader we refer to the Towitoko manual. The website of Towitoko can be found at <http://www.towitoko.com>.



Figure 6 Towitoko external chip drive

More information about the usage of chipcards is available on request via email to sales@tunix.nl.

1.6 Running WinPlug

In this paragraph we describe a sample session of WinPlug and briefly discuss some things you might run into.

1.6.1 Starting WinPlug

WinPlug can be started manually, via a menu or a DOS shell, or it can be started automatically. The latter requires WinPlug to be placed in the Windows Startup Folder. When WinPlug is started a splash screen is displayed. WinPlug can also be configured to start as an icon (which may be desirable when it starts automatic). The splash screen is still shown in this case.

1.6.1.1 The tray icon

When WinPlug is started it places an icon in the Windows tray. This icon has three options:

- Show control panel
This will show the control panel window (unless that window was iconified). A double-click on the tray icon itself will also pop up the control panel.
- About TUNIX/VPN for Windows
The About window shows version information and some useful email information.
- Exit VPN server
This will end your WinPlug session. If there are active connections WinPlug pops up a warning screen that all connections are to be closed.

1.6.2 A sample WinPlug session: retrieving mail with Eudora

We will now show a sample session where we will use the Eudora mailclient to retrieve email over the Internet from a mailserver on an internal network. We will assume that the WinPlug configuration is prepared for this setup and that WinPlug is running.

1.6.2.1 Preparing Eudora

The mailclient used in this sample is Eudora Light 3.06. In order to prepare Eudora for use with WinPlug 2.1 we must first set some options.

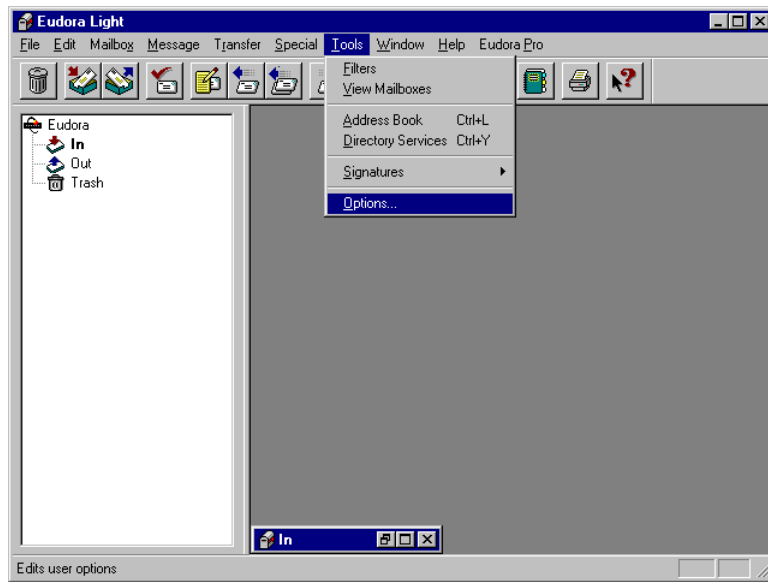


Figure 7 Eudora Tools - Options

In an ordinary situation the SMTP server is a host of your ISP. In this case we set the servername to 127.0.0.1. Normally, this address points back to your own PC, but WinPlug is running now and will see to it that Eudora ends up at the right server.

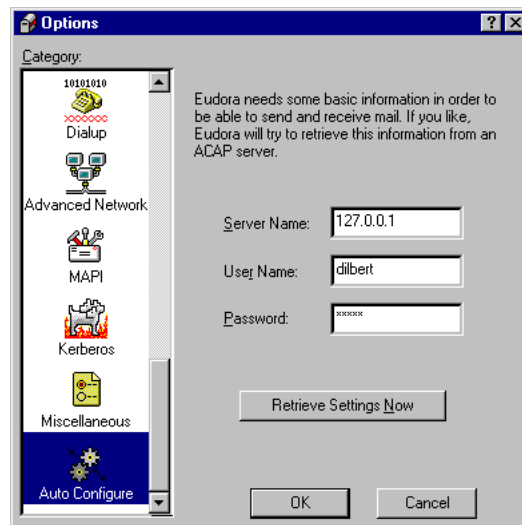


Figure 8 Setting Eudora options (I)

Likewise, the POP account is filled out as follows:

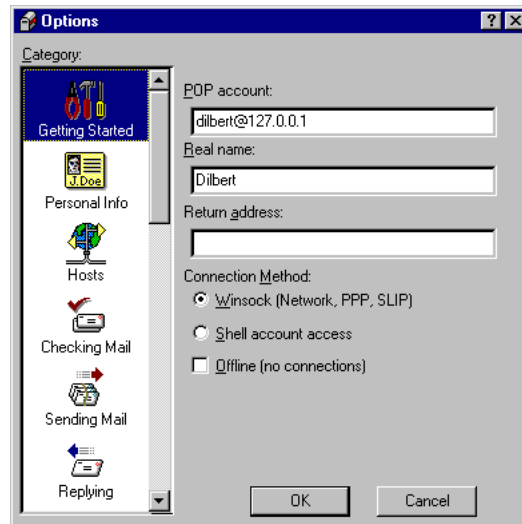


Figure 9 Setting Eudora options (II)

The POP account is now `dilbert@127.0.0.1`. There is not a POP server on your local PC, but WinPlug knows that it has to forward the connection to the POP server through the tunnelserver.

1.6.2.2 Retrieving the mail

Now we are all set to retrieve the email.

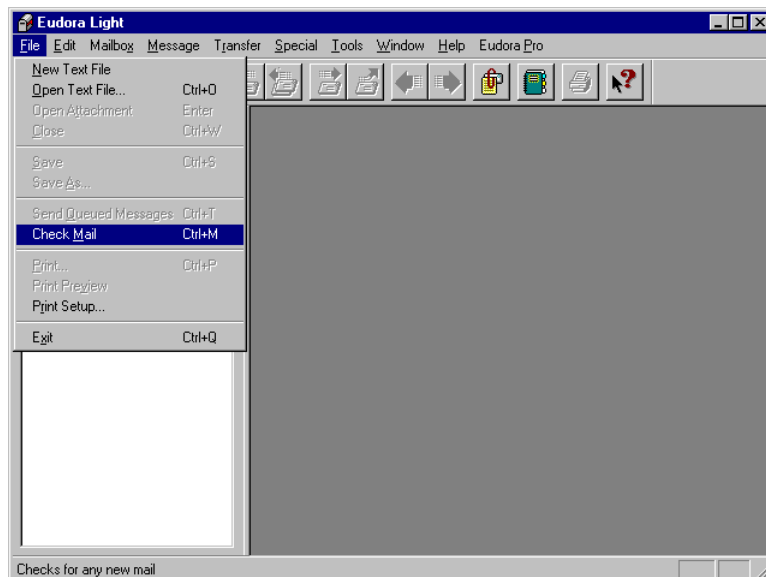


Figure 10 Checking email

Eudora assumes that the POP-server will require a password to be given for `dilbert` so it prompts for it.



Figure 11 Entering your Eudora password

A tunnel may require additional authentication (configuration dependent), so when Eudora starts a connection, `dilbert` may be prompted for authentication.

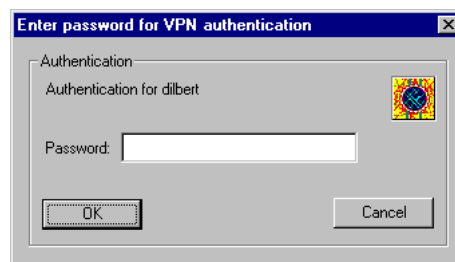


Figure 12 The authentication screen

This pop-up window always appears on top so it can't be missed. After `dilbert` has typed his password the screen disappears and the Eudora connection is established. Eudora can now start retrieving the mail.



Figure 13 Eudora logging into POP server

When `dilbert` now wants to check his mail *again*, he is not prompted for authentication anymore. Only if there haven't been any WinPlug connections for a certain amount of (configurable) time `dilbert` has to authenticate himself again.

Eudora doesn't know better than that it is talking to a POP server. In reality it is talking to one end of WinPlug and WinPlug takes care of the rest.

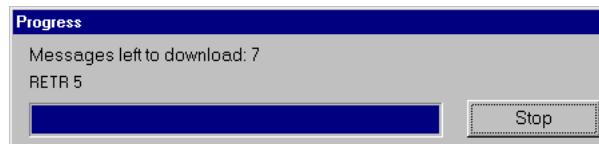


Figure 14 Eudora downloading email messages

The email messages are downloaded through a secure tunnel. Casual observers sniffing the network (or networks in between) will see nothing but encrypted data traffic.



Figure 15 New mail

The magical moment! The mail has arrived.

1.6.2.3 Upgrading client software

WinPlug automatically detects if the tunnelserver has a new release of the client available and will ask `dilbert` whether he wants to download it. This question will typically pop-up after successful authentication.

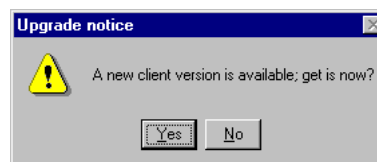


Figure 16 The upgrade notice

When `dilbert` clicks `No`, he isn't bothered with this question again until WinPlug is started the next time. When the answer is `'Yes'` the new client is downloaded as the file `newclient.exe` and put in the directory `C:\Program Files\tunix\winplug\config`. In order to install the new client, exit WinPlug (right-click the tray icon, select `Exit VPN Server`) and execute `newclient.exe`. You are prompted for a password which has been supplied by the network administrator.

1.6.3 The WinPlug control panel

The control panel is the main screen while WinPlug is running. It shows several things.

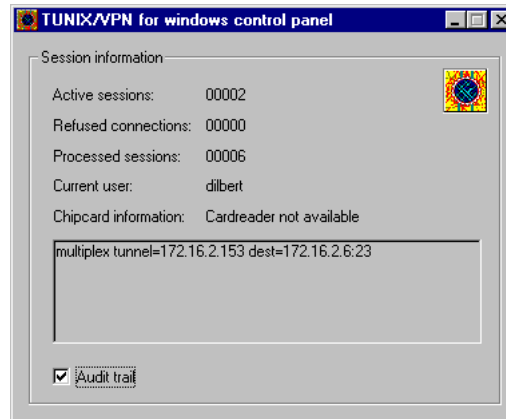


Figure 17 The WinPlug control panel

- Active Sessions
This is the number of sessions that are currently active through the tunnel. A session is a TCP connection.
- Refused connections
This is the number of connections that were refused by WinPlug on the PC. Typically, this means connections that were made to from another PC to the user's PC. The first denied connection pops up the following warning:

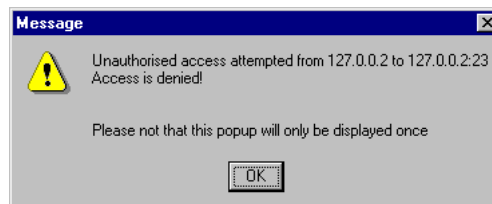


Figure 18 Unauthorized access warning

Processed sessions

This is the number of sessions `dilbert` already has had. Here we see that `dilbert` already has had 6 connections. Note that an FTP session typically uses a session for each command, while a TELNET connection always takes up one WinPlug session.

WinPlug remembers the number of sessions for as long as it is running. It always starts with zero active, refused and processed sessions. Also, when WinPlug is restarted, the numbers are reset to zero.

- `Current User`
This is the username which has been used to logon to the Windows system. A chipcard with a different username will overrule this. If there is no `tunneluser` directive specifying a different name in the WinPlug configuration file, this will be the username which is used for the next session of WinPlug.
- `Chipcard Information`
Speaks for itself. The default username for WinPlug is the one used to logon to the system (this is also the name that is shown when there is no Chipcard Reader present).
- `The info window`
The window shows brief messages about WinPlug's status and what it is doing. It will show, for instance, the buildup of tunnels and the number of bytes transferred during a session.
- `Audit trail`
When this box is checked, WinPlug will produce logging, to the logfile and to the Audit Trail window. Unchecked, WinPlug logging is inactive. WinPlug has at the most two logfiles, the current log (`C:\tmp\debug.out`) and the previous log (`C:\tmp\debug.out.txt`). Activating the Audit Trail will cause the current logfile to be moved to the previous one (thereby overwriting the 'old previous' logfile) and a new current logfile to be opened.

It is possible that this box is grey when WinPlug is started. This means you can't check or uncheck the box (whether or not you can do this is configurable). WinPlug always remembers the setting of the Audit Trail.

Clicking the right mouse button on the title bar of the Control Panel pops up an option screen.

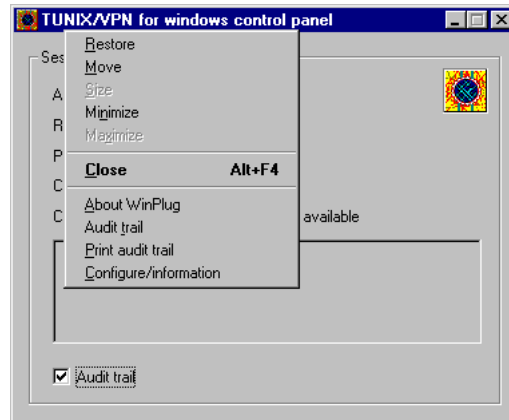


Figure 19 Control panel options

The four options pertinent to WinPlug are:

- About WinPlug
This will show you the version number of the WinPlug client and some useful email information.

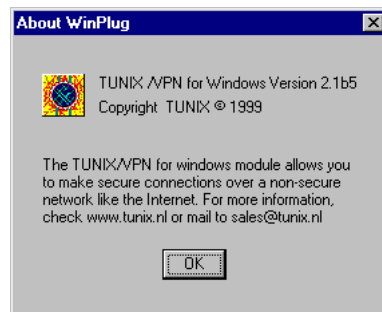


Figure 20 About WinPlug

- Audit trail
The audit trail is the debugging log. The audit trail shows the last part of the logfile `/tmp/debug.out`. When the Audit Trail window is opened, and new messages are added to the logfile, the scrollbar will automatically move down to show these messages.

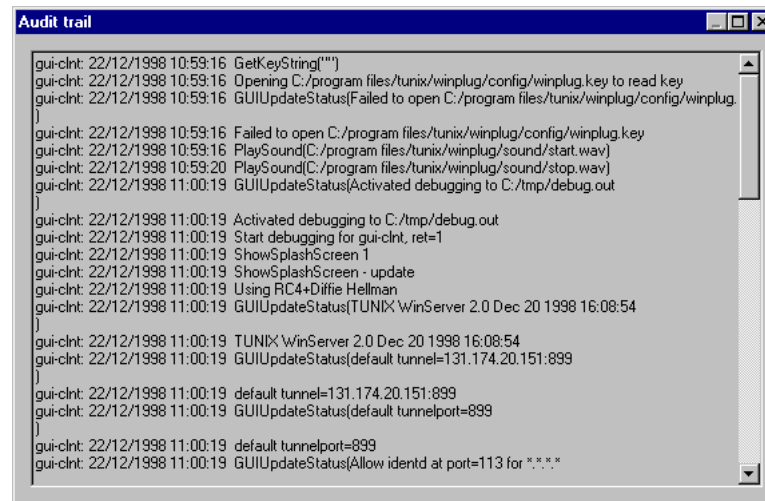


Figure 21 The Audit trail

- Print Audit trail

Hardcopy of the debug log can always come in handy. Apart from the logfile, the configuration file `winplug.cfg` is also printed. A default printer needs to be installed.

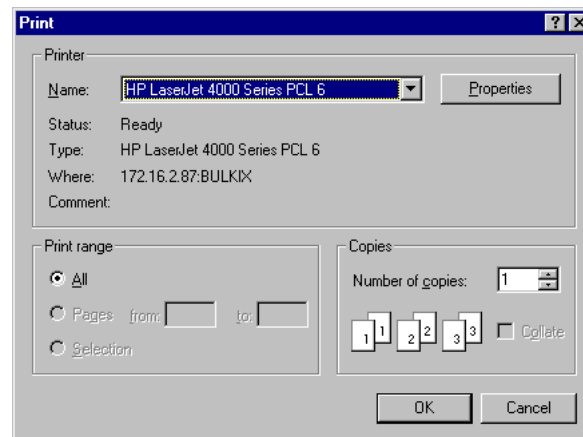


Figure 22 The printer screen

- Configure

This option will show you the configuration screens of WinPlug. The configuration screens are discussed in paragraph 1.7.

1.7 The WinPlug Configuration screens

In this paragraph we briefly discuss the various configuration screens of WinPlug. For more/detailed information we refer to the WinPlug Manual pages. The configuration window's default is to open with the Tunnel Configuration.

1.7.1 User information

The current user's name and secret key can be edited here. If only the username is displayed then it is clear that that user has no shared secret. If 'OK' is clicked then the key file is updated on disk.

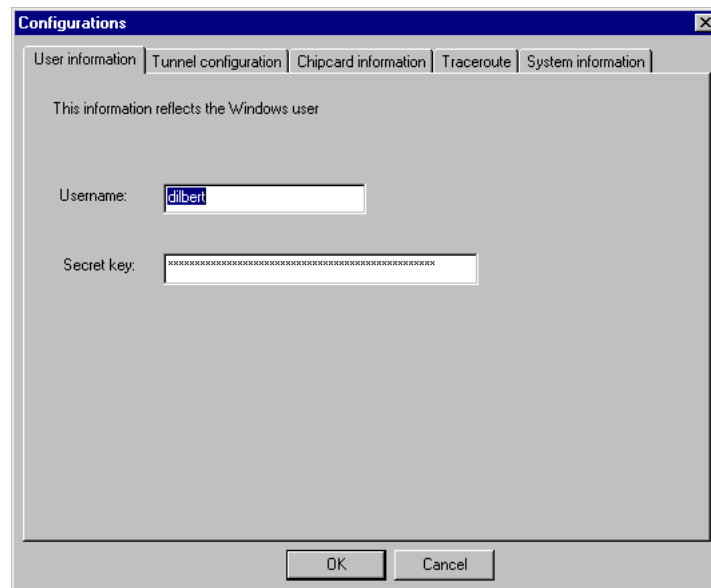


Figure 23 User information

1.7.2 The WinPlug configuration file

The WinPlug configuration is stored in a single configuration file, `winplug.cfg`. This file defines matters such as the current tunnel configuration and various defaults, such as `tunnelserver` and `tunnelport`. For a detailed description of this file, we refer to the `winplug.cfg` (Config Files) manual page.

The WinPlug configuration can be edited and modified via the Tunnel configuration screen.

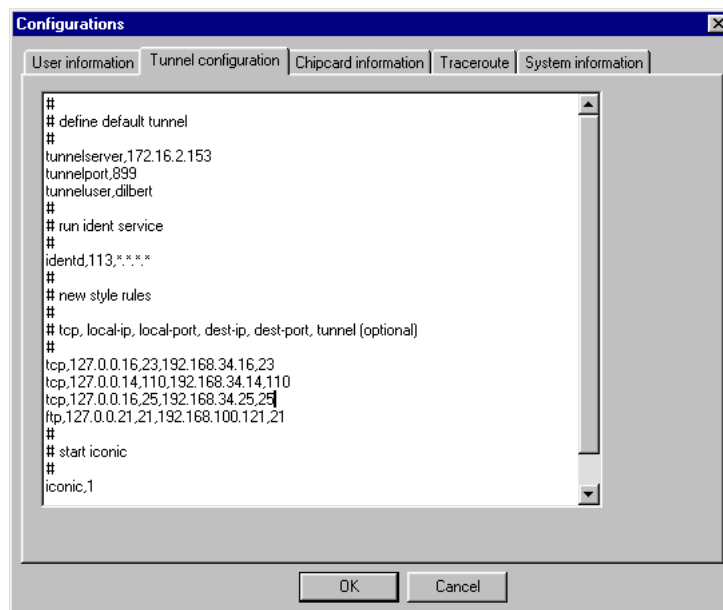
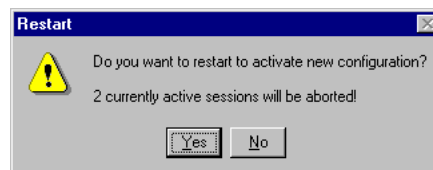


Figure 24 Tunnel configuration

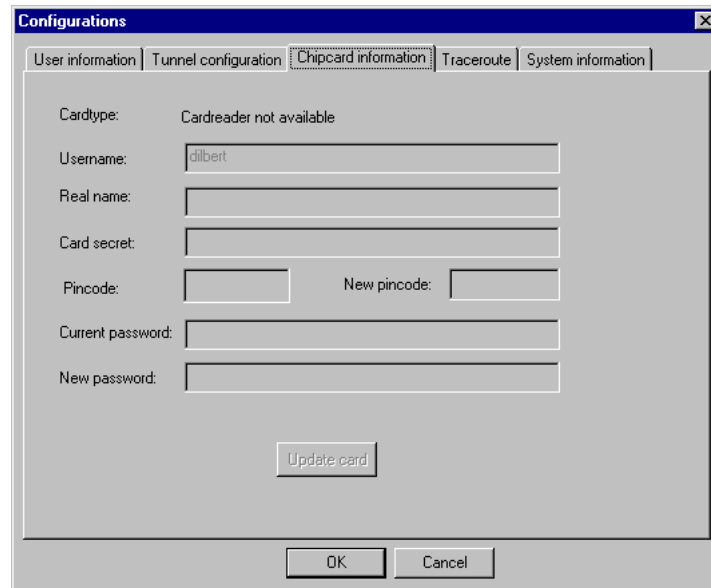
For the syntax details we refer to the WinPlug Manual pages. Clicking the OK button will update the configuration on disk and cause a popup of the following window:



Clicking the 'Yes' button will restart WinPlug and close any active connections. Clicking 'No' will close the configuration window and return the user to the WinPlug control panel. The new configuration won't be active until WinPlug is restarted.

1.7.3 Chipcard information

This screen shows the information about the current chipcard used. If there was no chipcard used, the screen will be grey.



The screenshot shows a Windows-style dialog box titled "Configurations" with a close button (X) in the top right corner. The dialog has five tabs: "User information", "Tunnel configuration", "Chipcard information" (which is selected and highlighted), "Traceroute", and "System information". The main area of the dialog is greyed out, indicating it is disabled. It contains the following fields and labels:

- Cardtype: Cardreader not available
- Username:
- Real name:
- Card secret:
- Pincode: New pincode:
- Current password:
- New password:

At the bottom of the dialog, there are three buttons: "Update card", "OK", and "Cancel".

Figure 25 Chipcard information

1.7.4 Traceroute

This screen allows the user to trace the route IP packages will take to a specified host. The left window takes addresses as input and the right window IP addresses. The 'Update' button will start a traceroute.

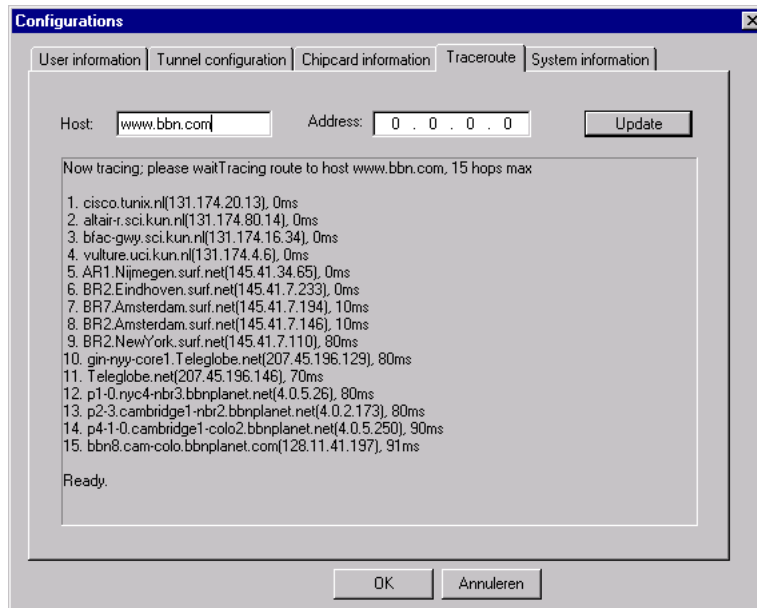


Figure 26 Traceroute

1.7.5 System Information

The system information window shows the information pertinent to the Windows system. Among others, it lists command-line options and all known interfaces at the time of startup.

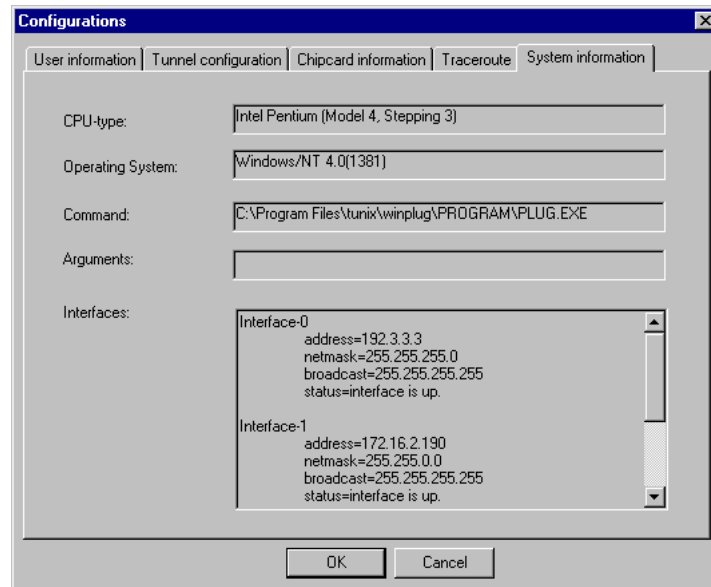


Figure 27 System Information

1.8 Additional network services

In this chapter we will discuss the additional services that are provided by the WinPlug package.

1.8.1 Identd

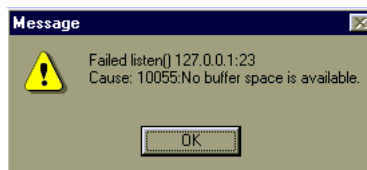
WinPlug can be used to provide a `identd` service conforming to the RFC1413 identification specifications. In order to activate this service, a line like `identd,113,172.16.2.*` or `identd,113,172.16.2.0/24` must be added to the WinPlug configuration. The first keyword specifies the service, the second keyword is the portnumber on which the service should run (113 is standard) and the last parameters specifies the range of hosts that is allowed to query this service. Filename pattern matching or a subnet mask notation is used to verify the IP-address.

1.8.1.1 Windows note

An identd client will provide an identd server with a portnumber. In a multi-user environment this portnumber should be matched against the list of ports that have an established connection associated with it. The name returned will be the name of the user holding that port. In a single-user environment like MS Windows, there is no need (and no way) to retrieve this information. Therefore the user returned by the WinPlug identd server is the user that is currently running the WinPlug identd service (the MS Windows username) or the name on the chipcard that is currently inserted into the chipcard reader (if present).

1.9 Troubleshooting

The following error keeps popping up:



This so-called WSAENOBUFFS error is most common on Win95 systems. It occurs when the system lacks resources to map all the tcp ports it should listen to. It is possible to increase the maximum number of connections by adding a registry entry. Using RegEdit, add a value called `MaxConnections` to the following registry key:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\VxD\MSTCP
```

For Win95, the value should be added as a DWORD. For Win98, the value should be added as a string. However, if adding the value as a DWORD does not solve the problem, try adding the value as a string. In both cases try a value of 512.

I login as user dilbert but the WinPlug console says I'm user dogbert.
Dogbert's chipcard could be in the card reader. Remove it before starting WinPlug.

*A connection attempt fails; the Audit trail says
Protocol error on challenge and Remote tunnel authentication FAILED.*

The ticket mechanism probably failed, due to `dogbert`'s chipcard. The id on the chipcard is not the same as the one you logged on with. Remove the chipcard from the card reader and start WinPlug again, OR, add the directive

```
tunneluser,dogbert
```

in the WinPlug configuration file. This will force WinPlug to use `dogbert` as `tunneluser`.

User `dilbert` is not authorised for tunnel usage.

Check whether user `dilbert` has an entry in `winplug.key`.

Current user `dilbert` cannot present shared secret, service is denied



Figure 28 Warning

User `dilbert` may have a key on the tunnelserver but he has no entry in `winplug.key` on his PC. Add `dilbert`'s entry and start WinPlug again.

The Audit trail shows nothing: it is empty

On the WinPlug console, check the Audit trail box. This will start the Audit trail again.

1.10 Disclaimer

The authentication, protocol and encryption algorithms which are used for VPN are carefully designed and implemented by TUNIX. TUNIX cannot guarantee (as this goes for every supplier of VPN products) that the methods used are capable of withstanding a cryptographic analysis of an organisation with unlimited means who wants to decode the data traffic.