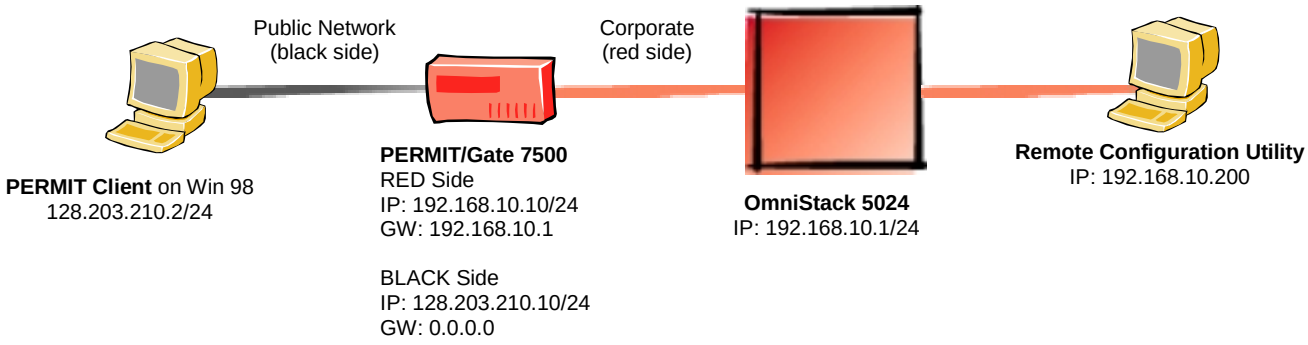
Demo Scenario - VPN Client and VPN Gateway using shared secret

The purpose of this document is to give you a complete set of installation steps to setup a demonstration for a customer. It does not replace any official document and it's mandatory to attend a specific training, which covers all kind of scenarios and details about different environments and configurations. Also, there's much more to know about VPN technology and specifications, as this document covers

Drawing

Following drawing should give you an outline for this scenario. It may be easier to understand what I've done.



Prerequisites

Hardware:

PERMIT/Gate 7500 – Alcatel 713x
OmniStack 5024

Software:

PERMIT/Client for Windows 95/98 version 3.00.021
PERMIT/Config 3.0

Set OmniStack back to factory default

I've used an OmniStack 5024. As I do not need any enhanced configurations, I've decided to let the Stack act as a "simple box".

Logon to the switch

```
This product includes software developed by the University of California,
Berkeley and its contributors.
```

```
Welcome to the Alcatel OmniStack! Version 4.1.2 GA
login    : admin
password: switch (hidden)
```

Delete Configuration files

```
OS-5024 / >rm mpm.cfg
mpm.cfg is a configuration file - if you remove this file,
parameters will not be saved until you reboot; do you want to
remove this? (n) y

File system compaction in progress...
OS-5024 / >rm mpm.cnf
mpm.cnf is a configuration file - if you remove this file,
parameters will not be saved until you reboot; do you want to
remove this? (n) y

File system compaction in progress...
OS-5024 / >
```

Perform a reboot

```
OS-5024 / >reboot
   Confirm? (n) : y
Locking filesystem...locked.
System going down immediately...
switch[40d6add0]: System rebooted by admin
```

Verify group and IP Address

After the switch has been rebooted, log on as ***admin*** with password ***switch***

```
/ % gp
Group                                  Network Address  Proto/
 ID          Group Description        (IP Subnet Mask)  Encaps
(:VLAN ID)                            or (IPX Node Addr)
===== ============================== ================ ========
    1 Default GROUP (#1)              192.168.10.1       IP  /
                                        (ff.ff.ff.00 )    ETH2
/ %
```

Configuring PERMIT/Gate using the Console

While the gateway comes fully configured right out of the box, there are some basic settings required for local conditions. Additionally, you may wish to change some or all of the configuration files. Mostly, the box has been used for different scenarios; it will be the best start to clear the configuration to factory default and start from there.

Console Settings:

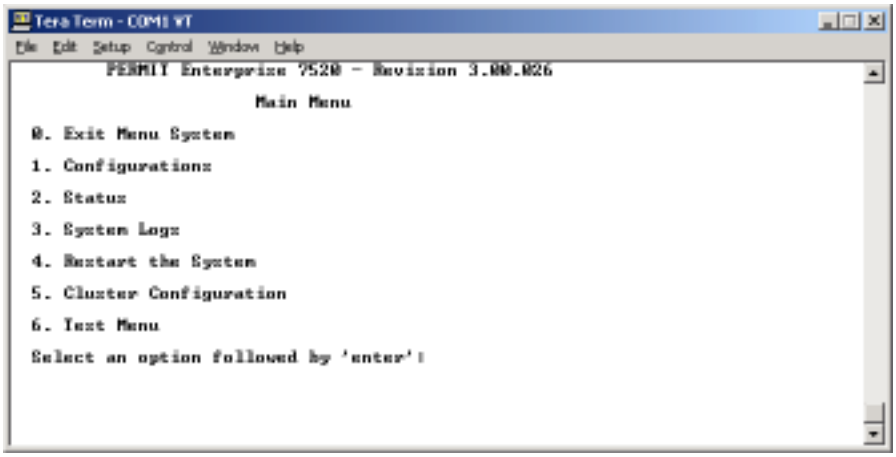
- Bits per second ⇨ 19,200 (factory default of the box)
- Data bits ⇨ 8
- Parity ⇨ None
- Stop bits ⇨ 1
- Flow control ⇨ Xon/Xoff

Terminal Cable Set

The proper cable set consists out of

- DB 9 modular jack (female) – Part No. 40-1314-00 – MADE IN CANADA
- 8-pin flat cable – Part No. 81-2230-0103 – MADE IN CANADA

Open your terminal session and connect to the Gate



Clearing the Gate Settings on PERMIT Enterprise 7520

***Note**: The Dram boot menu differs from Enterprise 7520 to 2500 & 4000 series. If you use one of those, please skip this section and follow the short description to clear the Gate Settings on PERMIT Enterprise 4520 on page 5*

Type user name, ***root***, and password ***permit***. Both are case sensitive. These are the default values with which the Gate is shipped.

```
PERMIT Enterprise 7520 - Revision 3.00.026
                    Main Menu

0. Exit Menu System
1. Configurations
2. Status
3. System Logs
4. Restart the System
5. Cluster Configuration
```

```
  6. Test Menu

  Select an option followed by 'enter': 4

Do you wish to restart the system? (y to confirm)
```

Press **4** to restart the Gateway and watch for the DRAM Boot menu prompt
The DRAM menu is the lowest level that an Administrator can work with the Gateway code

Press **ENTER** as soon as you see the prompt

```
Press 'enter' to access startup menu.......
      Press <CR> to activate the Dram Boot menu
```

Type user name ***root*** and password ***permit*** again

```
Enter user ID:  root

  Enter password: ******
PERMIT Enterprise  - Revision 3.00.026
              Startup

  0. Exit to continue executing application
  1. Operating Mode (En/Dis) Unknown
  2. Clear Configuration
  3. Clear Flash File System

  Select an option followed by 'enter': 2
 This will erase all configuration parameter. Are you sure you want to change
this? ('y' to confirm) y
```

Type **2** to clean the profile
Note*: This re-initializes your non-volatile memory, deleting configuration information in the process and resets your Gateway to factory default.*
Type **y** to confirm the clean action

```
PERMIT Enterprise  - Revision 3.00.026Startup
  0. Exit to continue executing application
  1. Operating Mode (En/Dis) Unknown
  2. Clear Configuration
  3. Clear Flash File System

  Select an option followed by 'enter': 0

nvs: Initializing parameter storage area. Please wait...
nvs: Examining region 0...
```

A bunch of logging messages appear during the boot process, when you see the last two lines, like following, press RETURN and type user ***root*** and password ***permit*** to continue with the configuration steps

```
2001/06/25 09:20:58 Monitor Evnt: Black port link: NO LINK
2001/06/25 09:20:58 Monitor Evnt: Red port link: NO LINK


  Enter user ID:  root
  Enter password: permit (is hashed with asterisks)
```

Continue with Step "***Configuring IP Addresses***"

Clearing the Gate Settings on PERMIT Enterprise 4520

1. Open your terminal session and connect to the Gate
2. Press **ENTER** as soon as you see the prompt "*Press <CR> to activate the Dram Boot menu*"
3. Type user name ***root*** and password ***permit*** again
4. Type **cl** to clean the profile
5. Type **y** to confirm the clean action
6. When Dram prompt returns, type **ex** to exit Dram an continue the boot process
7. After the system finishes booting, the logging screen displays the message ***"Red port link: 10MB XX"***
8. Press ENTER and, in response to the prompts, type user ***root*** and the password ***permit***
9. The Main menu appears

Configuring IP Addresses

Choose Configurations ⇨ **1**

```
              PERMIT Enterprise 7520 - Revision 3.00.026

                          Main Menu

       0. Exit Menu System
       1. Configurations
       2. Status
       3. System Logs
       4. Restart the System
       5. Cluster Configuration
       6. Test Menu

       Select an option followed by 'enter': 1
```

From the Configurations Menu choose Addresses ⇨ **1**

```
                PERMIT Enterprise 7520 - Revision 3.00.026

                          Configurations

        0. Exit Menu
        1. Addresses
        2. Management Servers
        3. Network Security Policy
        4. System Configuration
        5. Access Configuration
        6. Client Services
        7. Files
        8. Master Keys

        Select an option followed by 'enter': 1
```

Change IP Address on Black Side ⇨ **2**

```
              PERMIT Enterprise 7520 - Revision 3.00.026

                          Addresses

      0. Exit Menu
      1. Black/Red LAN MAC Addresses   ->     00:a0:90:00:82:55 / 56
      2. Black IP Address                      1.1.1.53
      3. Black Subnet Mask                     255.0.0.0
      4. Black Default Router                  0.0.0.0
      5. Red IP Address                        2.1.2.48
      6. Red Subnet Mask                       255.0.0.0
      7. Red Default Router                    0.0.0.0

        Select an option followed by 'enter': 2

      Enter a new parameter: 128.203.210.10
       The unit will need to be restarted.
            Are you sure you want to change this? ('y' to confirm) y
```

Change Subnet Mask on Black Side ⇨ **3**

```
      PERMIT Enterprise 7520 - Revision 3.00.026
      << Current configuration requires a restart to take effect. >>
                          Addresses

        0. Exit Menu
```

```
1. Black/Red LAN MAC Addresses   ->     00:a0:90:00:82:55 / 56
2. Black IP Address                     128.203.210.10
3. Black Subnet Mask                    255.0.0.0
4. Black Default Router                 0.0.0.0
5. Red IP Address                       2.1.2.48
6. Red Subnet Mask                      255.0.0.0
7. Red Default Router                   0.0.0.0

  Select an option followed by 'enter': 3
Enter a new parameter: 255.255.255.0
 The unit will need to be restarted.
      Are you sure you want to change this? ('y' to confirm) y
```

Change IP Address on Red Side ⇨ **5**

```
          PERMIT Enterprise 7520 - Revision 3.00.026
<< Current configuration requires a restart to take effect. >>
                        Addresses

0. Exit Menu
1. Black/Red LAN MAC Addresses   ->     00:a0:90:00:82:55 / 56
2. Black IP Address                     128.203.210.10
3. Black Subnet Mask                    255.255.255.0
4. Black Default Router                 0.0.0.0
5. Red IP Address                       2.1.2.48
6. Red Subnet Mask                      255.0.0.0
7. Red Default Router                   0.0.0.0

  Select an option followed by 'enter': 5
Enter a new parameter: 192.168.10.10
 The unit will need to be restarted.
      Are you sure you want to change this? ('y' to confirm) y
```

Change Subnet Mask on Red Side ⇨ **6**

```
          PERMIT Enterprise 7520 - Revision 3.00.026
<< Current configuration requires a restart to take effect. >>
                        Addresses

0. Exit Menu
1. Black/Red LAN MAC Addresses   ->     00:a0:90:00:82:55 / 56
2. Black IP Address                     128.203.210.10
3. Black Subnet Mask                    255.255.255.0
4. Black Default Router                 0.0.0.0
5. Red IP Address                       192.168.10.10
6. Red Subnet Mask                      255.0.0.0
```

```
          7. Red Default Router                    0.0.0.0


        Select an option followed by 'enter': 6
      Enter a new parameter: 255.255.255.0
       The unit will need to be restarted.
            Are you sure you want to change this? ('y' to confirm) y
```

Change Default Router on Red Side ⇨ **7**

```
                PERMIT Enterprise 7520 - Revision 3.00.026
      << Current configuration requires a restart to take effect. >>
                              Addresses

        0. Exit Menu
        1. Black/Red LAN MAC Addresses   ->     00:a0:90:00:82:55 / 56
        2. Black IP Address                     1.1.1.53
        3. Black Subnet Mask                    255.0.0.0
        4. Black Default Router                 0.0.0.0
        5. Red IP Address                       2.1.2.48
        6. Red Subnet Mask                      255.0.0.0
        7. Red Default Router                   0.0.0.0

        Select an option followed by 'enter': 7
      Enter a new parameter: 192.168.10.1
       The unit will need to be restarted.
            Are you sure you want to change this? ('y' to confirm) y
```

The following screen shows the addressing configuration after new IPs have been entered.

```
                PERMIT Enterprise 7520 - Revision 3.00.026
      << Current configuration requires a restart to take effect. >>

                              Addresses

        0. Exit Menu
        1. Black/Red LAN MAC Addresses   ->     00:a0:90:00:82:55 / 56
        2. Black IP Address                     128.203.210.10
        3. Black Subnet Mask                    255.255.255.0
        4. Black Default Router                 0.0.0.0
        5. Red IP Address                       192.168.10.10
        6. Red Subnet Mask                      255.255.255.0
        7. Red Default Router                   192.168.10.1

  Select an option followed by 'enter': 0
```

```
                PERMIT Enterprise 7520 - Revision 3.00.026
          << Current configuration requires a restart to take effect. >>
                                Configurations

            0. Exit Menu
            1. Addresses
            2. Management Servers
            3. Network Security Policy
            4. System Configuration
            5. Access Configuration
            6. Client Services
            7. Files
            8. Master Keys

            Select an option followed by 'enter': 0


                PERMIT Enterprise 7520 - Revision 3.00.026
          << Current configuration requires a restart to take effect. >>
                                Main Menu

          0. Exit Menu System
          1. Configurations
          2. Status
          3. System Logs
          4. Restart the System
          5. Cluster Configuration
          6. Test Menu

          Select an option followed by 'enter': 4


          The configuration has changed.
          Do you wish to restart the system? (y to confirm) y

Restarting ..........
```

Configuring for Remote Access

```
                PERMIT Enterprise 7520 - Revision 3.00.026

                                Main Menu

            0. Exit Menu System
            1. Configurations
            2. Status
            3. System Logs
            4. Restart the System
```

```
5. Cluster Configuration
6. Test Menu

Select an option followed by 'enter': 1


        PERMIT Enterprise 7520 - Revision 3.00.026

                    Configurations

  0. Exit Menu
  1. Addresses
  2. Management Servers
  3. Network Security Policy
  4. System Configuration
  5. Access Configuration
  6. Client Services
  7. Files
  8. Master Keys

  Select an option followed by 'enter': 5



        PERMIT Enterprise 7520 - Revision 3.00.026

                  Access Configuration

    0. Exit Menu
    1. Remote Access
    2. Console Access
    3. SNMP Access

    Select an option followed by 'enter': 1
```

Make sure, that Network Access is set to "***All***" and use as the access password ***remote***

```
        PERMIT Enterprise 7520 - Revision 3.00.026

                    Remote Access

    0. Exit Menu
    1. Network Access (none/all/list)       All
    2. Trusted IP Address 1                 0.0.0.0
    3. Trusted IP Address 2                 0.0.0.0
    4. Trusted IP Address 3                 0.0.0.0
    5. Access Password                      *****
```

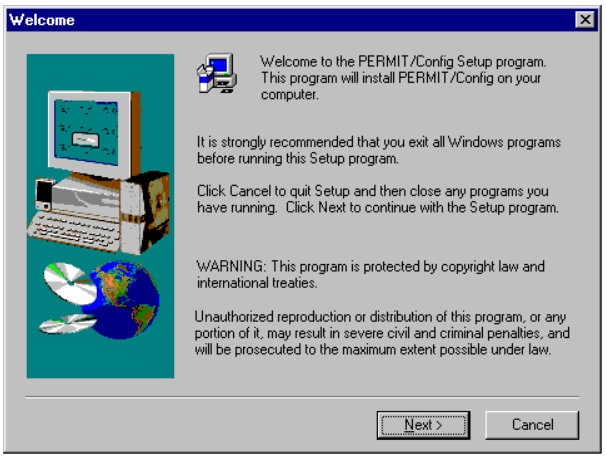
```
Select an option followed by 'enter': 5

Enter a new password: ****** ⇦ remote
Reenter the password: ****** ⇦ remote

This may disrupt remote access. Are you sure? (y to confirm) y
```

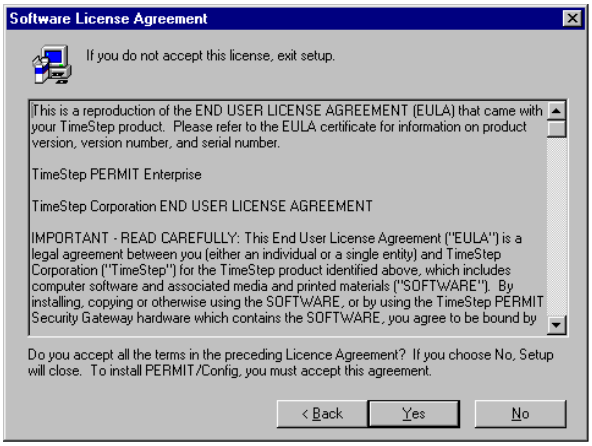
Installing the Remote Configuration Utility

Start the PERMIT/Config setup program
When inserting the CD ROM and Auto-Play is enabled, TimeStep's Master setup window should open automatically.

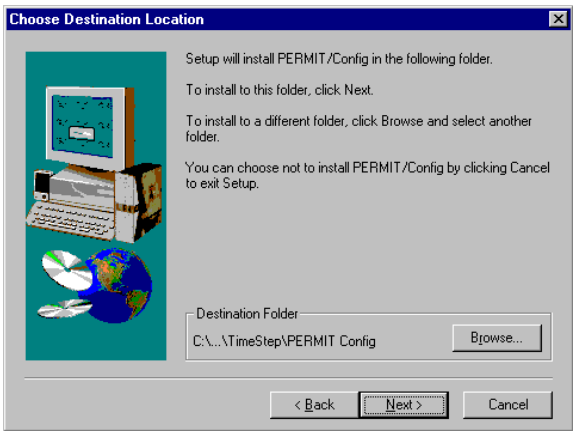


When Auto-Play is disabled, then start the setup program out of the directory ***disk1*** from the proper directory

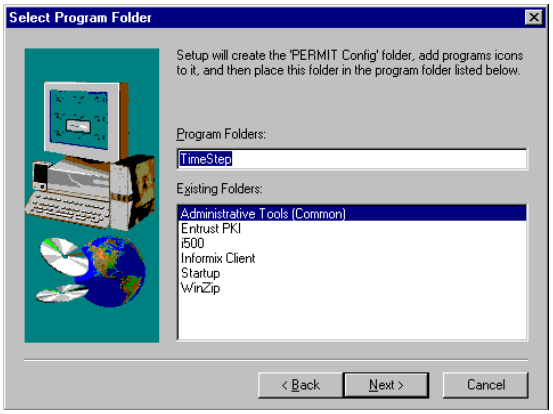
Click **NEXT** to accept the Welcome screen



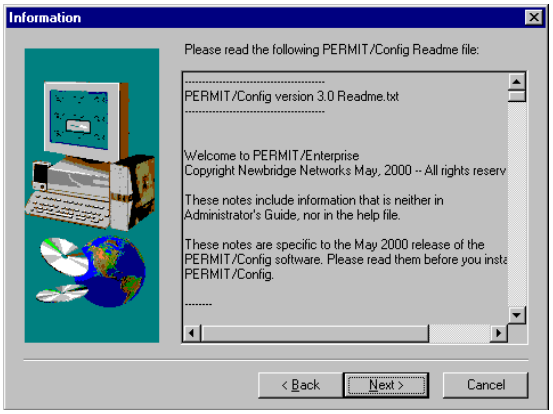
Click **YES** to accept the terms of the License Agreement



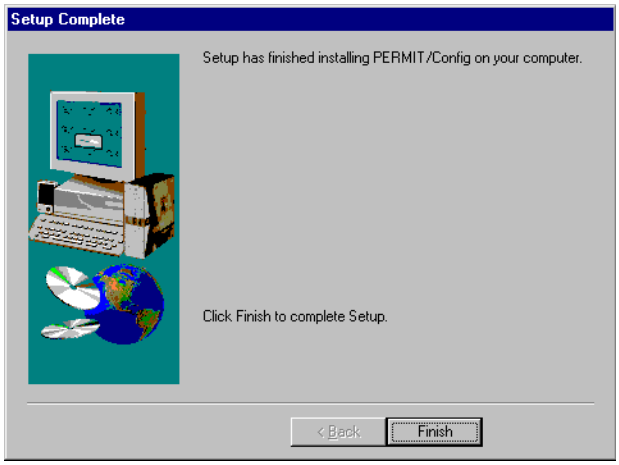
Click **NEXT** to accept the default Destination location for the files



Click **NEXT** to accept the default Program Folder for the Start menu



Scan the readme notes and then click **NEXT**



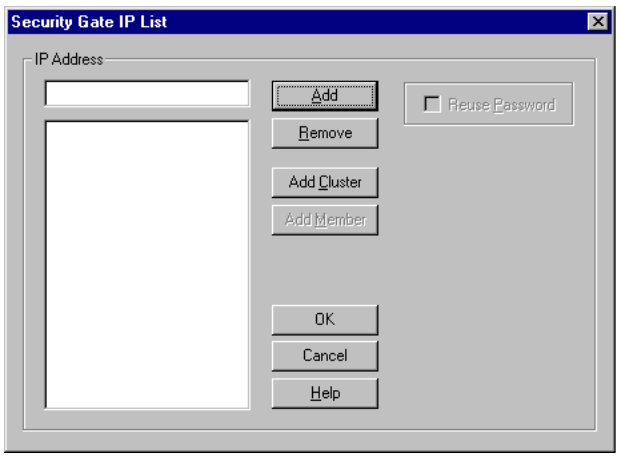
Click **FINISH**

Exit the install utility, when not exiting automatically

This completes the installation phase.

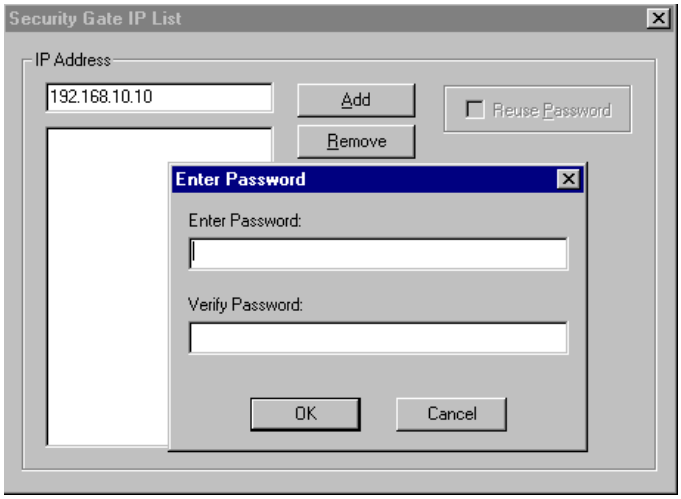
Configuring the Utility

Click the start button from the Programs menu, choose TimeStep ⇨ PERMIT/Config ⇨ PERMIT/CONFIG

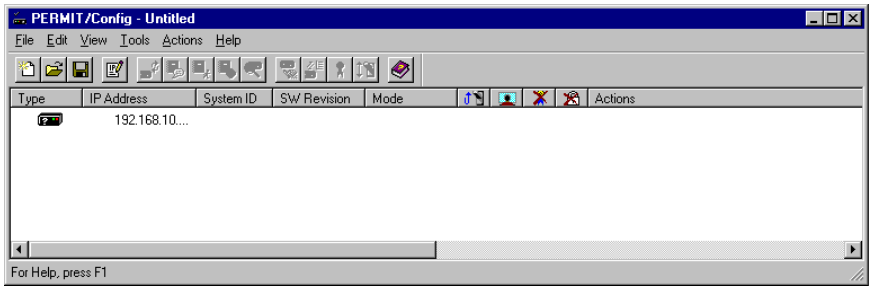


When you start PERMIT/Config with no gateway list file specified, it presents the Security Gate IP List box. Use this box to indicate the addresses of the Gateways you wish to access. Be sure to enter the IP

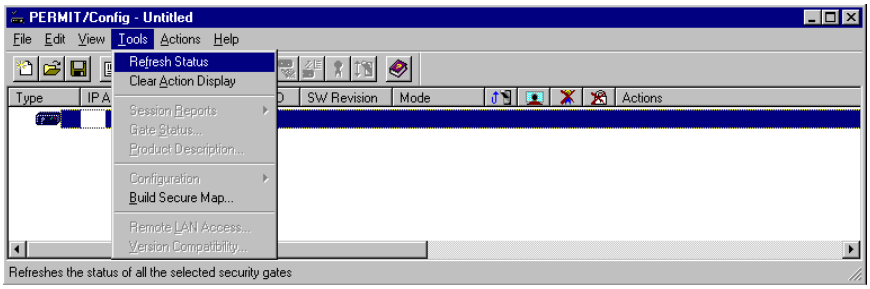
of the appropriate side of the Gateway. In this scenario, the PERMIT/Config is connected on the red side, and therefore you have to use ***192.168.10.10*** as the appropriate IP Address



Type the IP Address ***192.168.10.10*** and click **ADD.** A new window pops up, type and confirm the password for accessing the Gate. Remember "***remote***", which has been set earlier in the section "***Configuring for Remote Access***" and click on **OK**.



Now you can see the Gate with IP Address listed on PERMIT/Config.

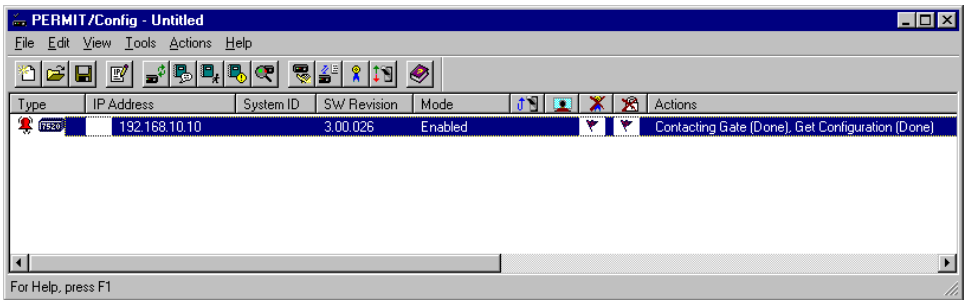


Highlight the new added Gateway and click on Tools in the Menu Bar ⇨ Refresh Status

This will contact the Gateway and retrieve the configuration.

When seeing on Actions

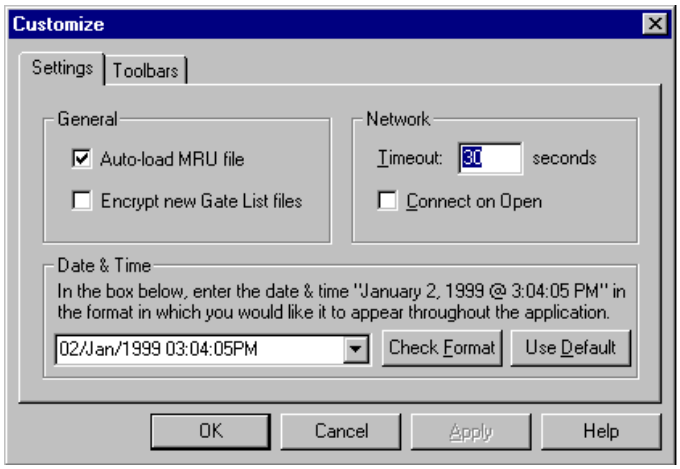
- Contacting Gate (Done)
- Get Configuration (Done),
  You have verified access to the gate



***Note**: It is useful to save this into a Gateway List File (GLF). Otherwise, the next time you open the Utility you will have to re-enter the Gate IP address and password.*

Setting Preferences

From the File menu click ***Preferences***



On the Settings tab:

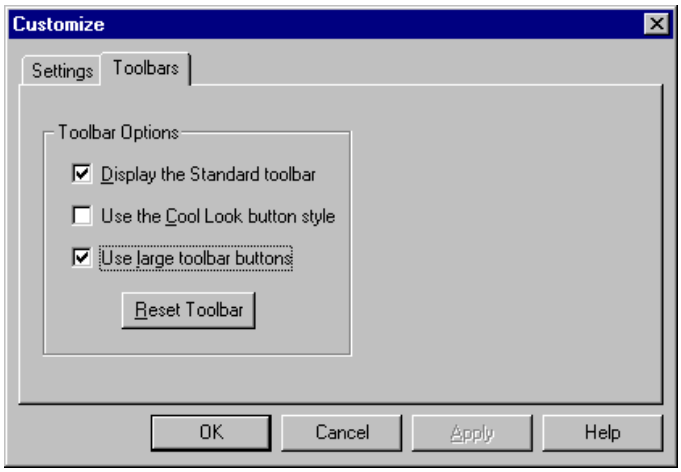
Ensure that the Autoload MRU file check box is selected. This will automatically load the Most Recently Used gateway list file when started.

Leave the Encrypt new Gate List files check box clear
***Note**: This option causes the utility to prompt for an encryption password when saving a new gateway list file and to prompt for the password, when opening the file*

Leave Timeout at its default value of 30 seconds

Leave the ***connect on open*** check box clear

Click on ***Toolbars*** tab



Click the ***Use large toolbar buttons*** check box

Click **Apply** and **OK** to close the Customize box

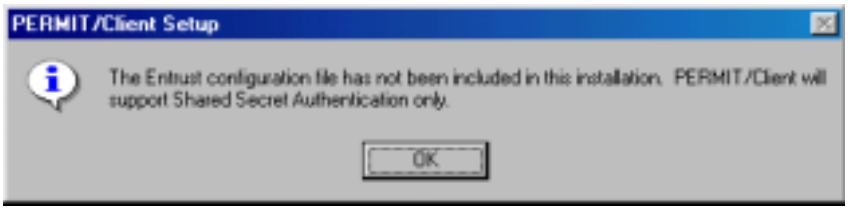
Installing the Secure VPN Client

Start the Secure VPN Client setup program
When inserting the CD ROM and Auto-Play is enabled, TimeStep's Master setup window should open automatically.

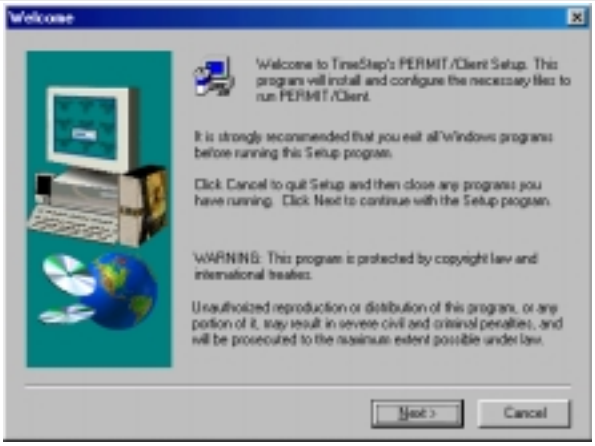
When Auto-Play is disabled, then start the setup program out of the directory ***disk1*** from the proper directory – otherwise choose the proper client version

- PERMIT Client 95 ⇨ does work with Windows 95 and 98
- PERMIT Client NT ⇨ does work with Windows NT 4.0 only

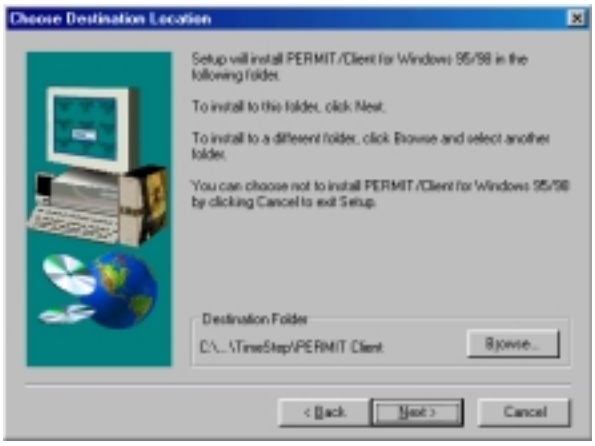
(When having Windows 2000, please obtain the latest version of PERMIT Client, which supports W2K)



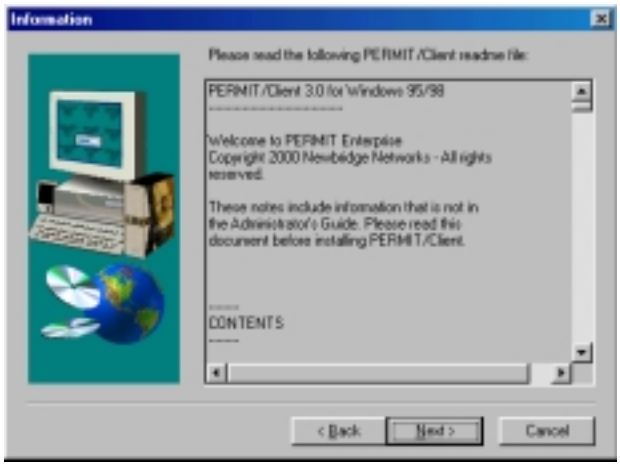
Click **OK** to bypass the warning message about the utility being unable to find entrust.ini.



Click **NEXT**

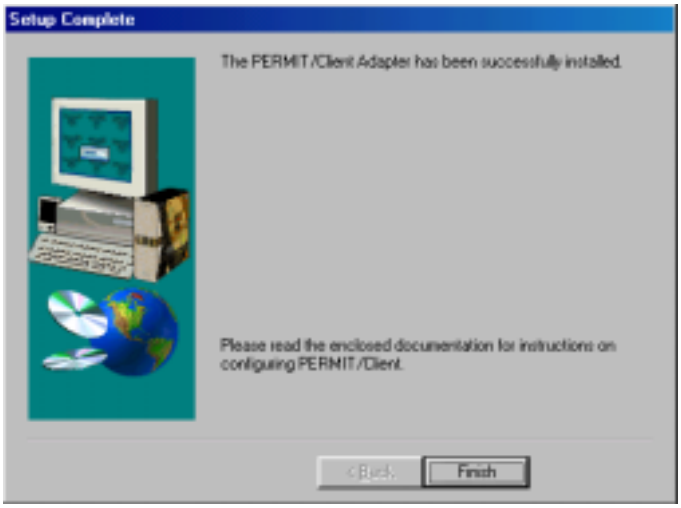


Click **NEXT** to accept the default Destination Folder



Scan the readme notes and click **NEXT**

Click **NEXT** to accept the default Program Folder
(A progress bar appears)



Click **FINISH**

Windows displays the Network Configuration Utility briefly and then restarts the computer. When Windows restart, it returns to the configuration process and displays this message.

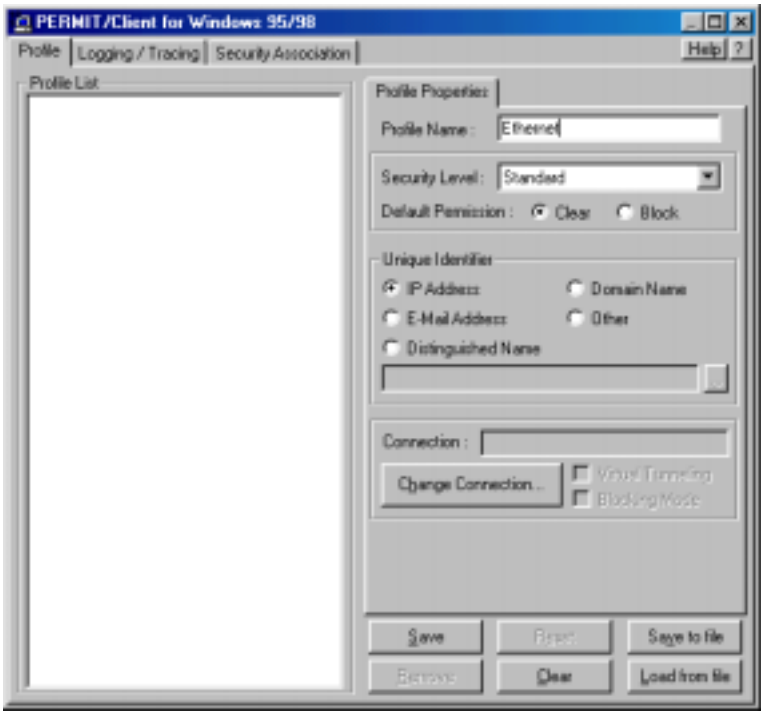
Note: *During the installation process before, there has a new Client (Client for TimeStep Virtual Private Networking) been added on the network configuration and a new adapter, called TimeStep Virtual Adapter, and not to forget, TCP/IP has been bind to this new adapter as well.*

Click **OK**

The Secure VPN Client places a TimeStep icon in the Tool tray at the right end of the Taskbar, once the complete installation and initial configuration has been finished.

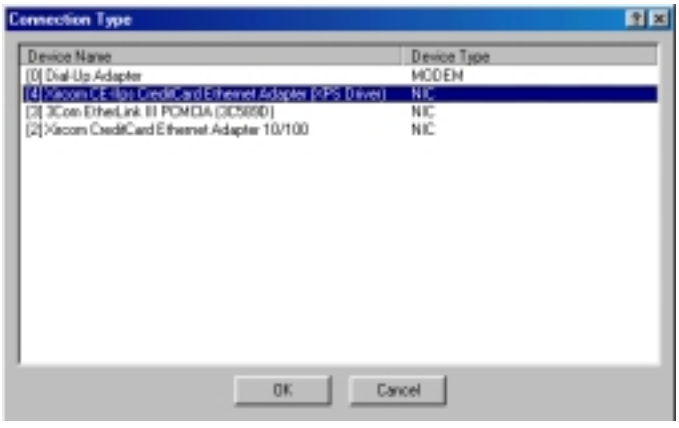
Configuring the Secure VPN Client for Ethernet use

After successful installation, the following dialog box appears



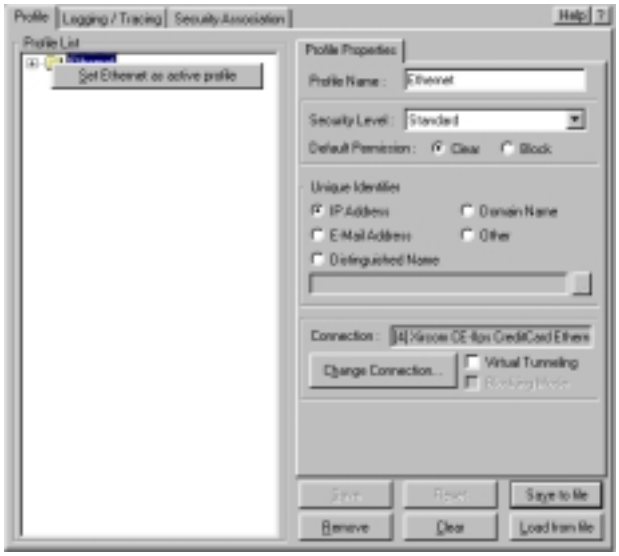
Type ***Ethernet*** in the Profile Name box. You can use any other Profile Name as well.
LEAVE *Security Level*, ***Default Permission*** and ***Unique Identifier*** at their default values

Click **CHANGE CONNECTION**
Select the Network Interface Card



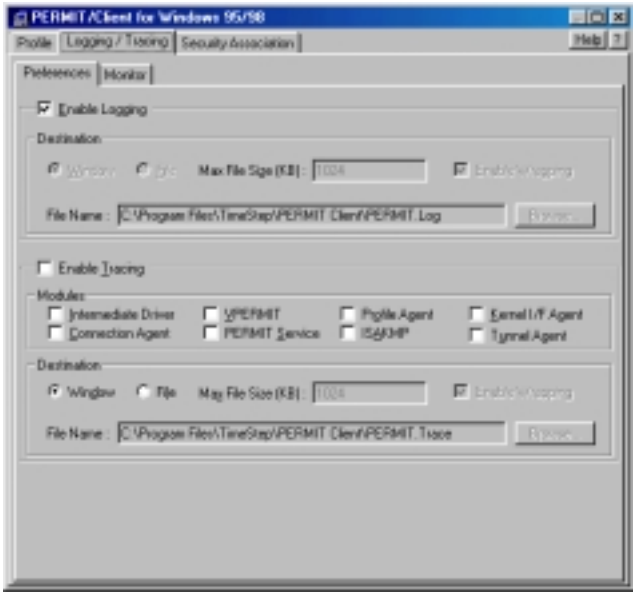
***Note**: You may see different values in your Connection Type Window. Choose the appropriate.*

Click **SAVE** and the profile name appears in the Profile List in the left plane



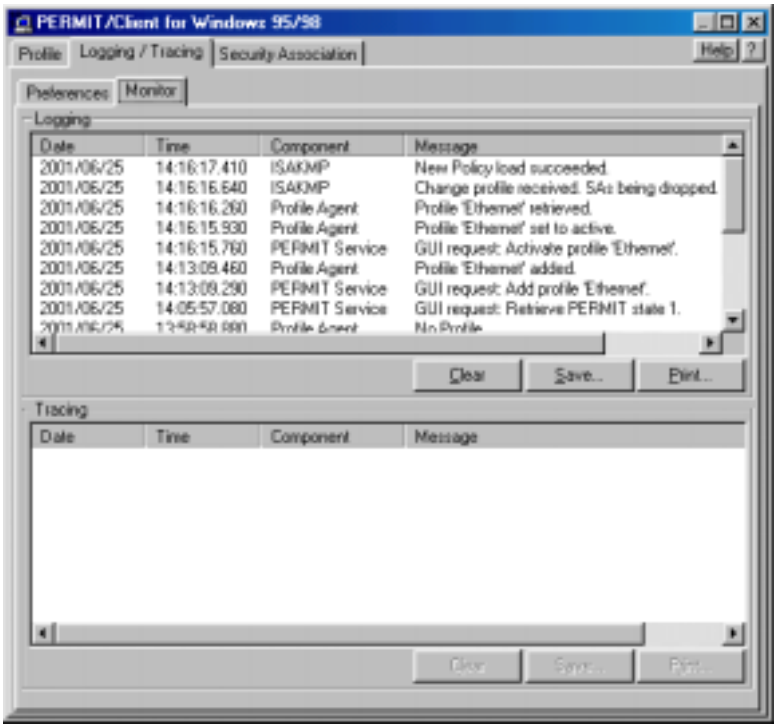
Right Click the profile tin the left plane and click **SET *"Ethernet"*** as active profile, and a red check mark should appear *(It is possible to have multiple profiles, where it may be necessary to identify one as the active profile)*

Click the ***Logging /Tracing*** tab

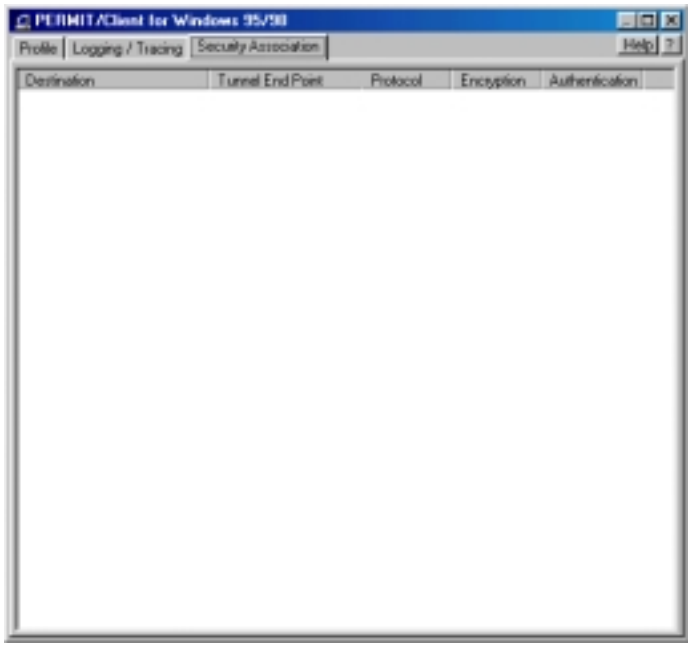


Ensure that the Enable logging checkbox is selected

Within the ***Logging/Tracing tab***, click the ***Monitor tab*** and note the Logging window



Select the ***Security Association tab*** (beside the Logging /Tracing tab)



***NOTE**: There are no Security Associations yet*

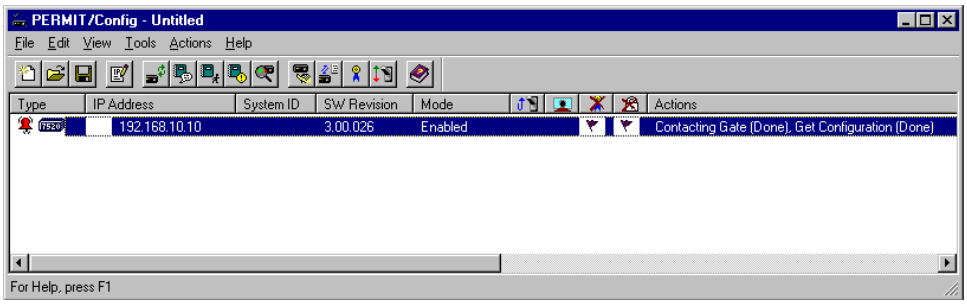
Using PERMIT/Config to configure VPN Gateway for shared secret

Two steps are required to set the authentication level to Shared Secret.

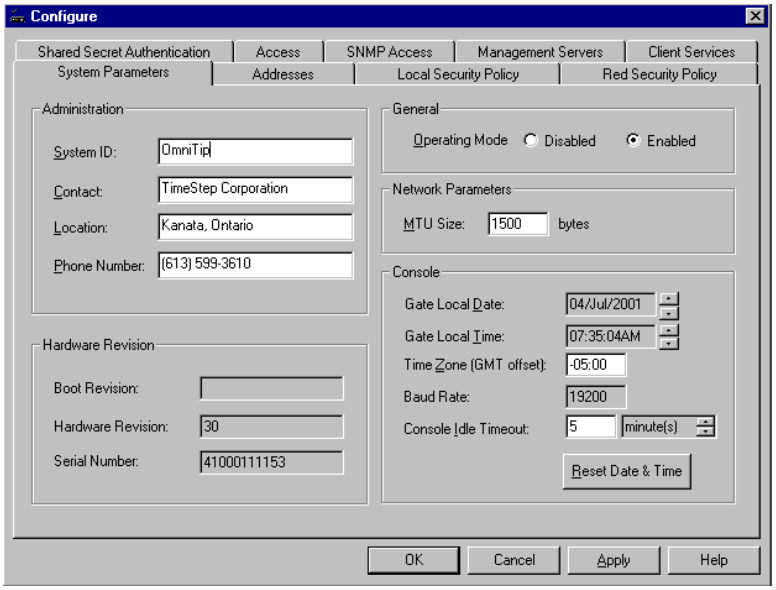
- Change the Red Security Policy for that connection
- Enter the Black-side network identity and the associated secret

Ensure that Client is disabled

Activate the Configuration Utility and refresh the status



Open the Configure Window by ACTIONS ⇨ CONFIGURE

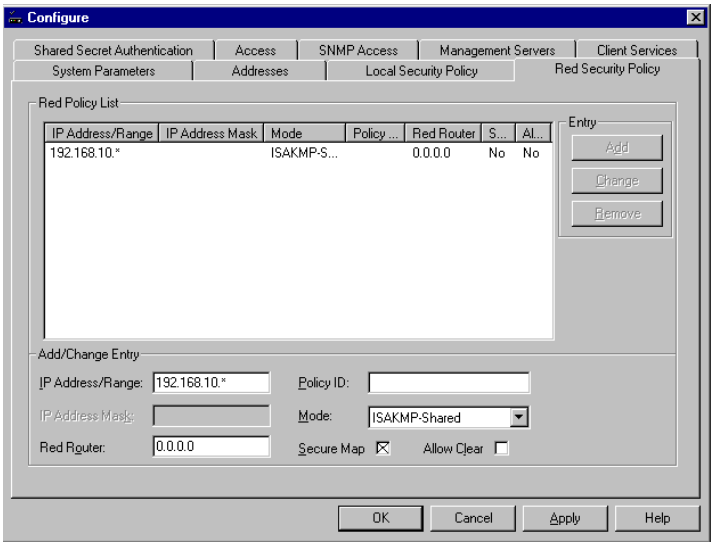


In the System ID box of the Administration frame (***System Parameters*** tab), type a name for your system. This name applies to the Gate, not just to a particular side of the Gate.

RED SECURITY POLICY

Click the ***Red Security Policy*** tab

In the ***Add/Change Entry*** frame, select **ISAKMP-Shared** in the Mode list



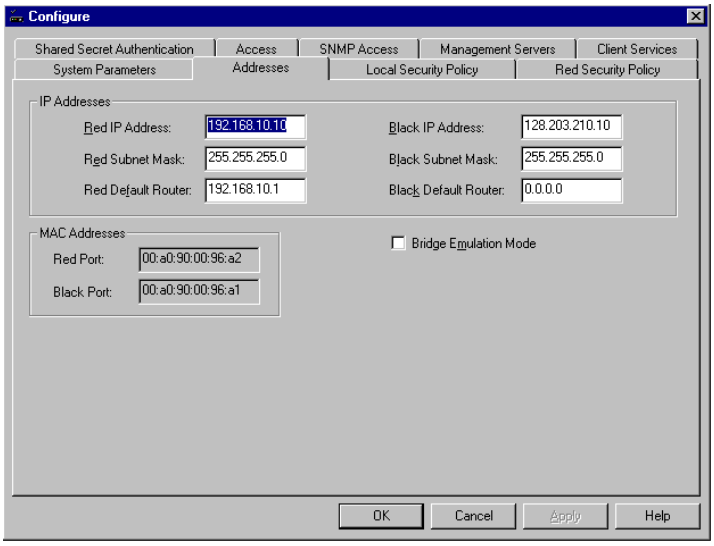
Type the IP Address Range of your protected Network (**192.168.10.***).
IP Address Mask means Subnet Mask, but by putting "*", it will be disabled.

Leave the Policy ID box blank

Make sure you check mark "***Secure Map***", otherwise you won't be able to establish an SA from the Client to the Gate.

Click **Add**

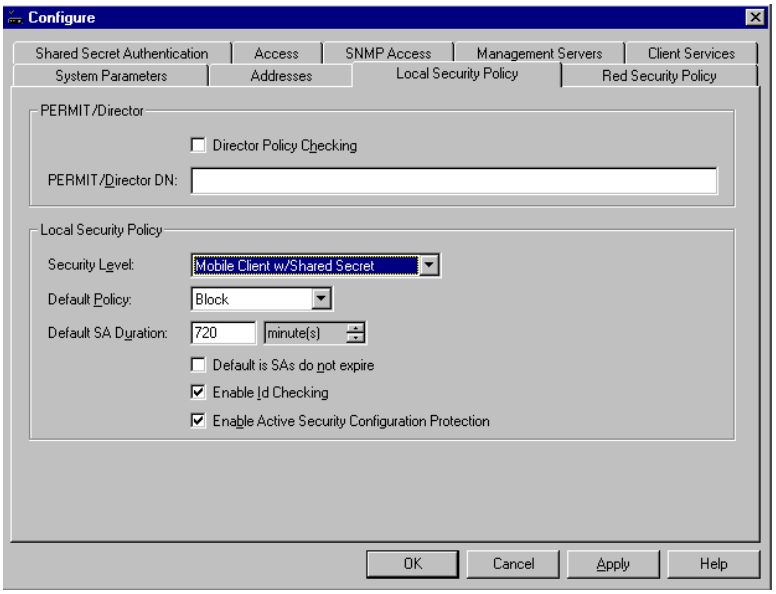
Click the ***Addresses*** tab



There you could see all the IP Address pre-filled. When contacting the Gate for a refresh, this has been retrieved.

LOCAL SECURITY POLICY

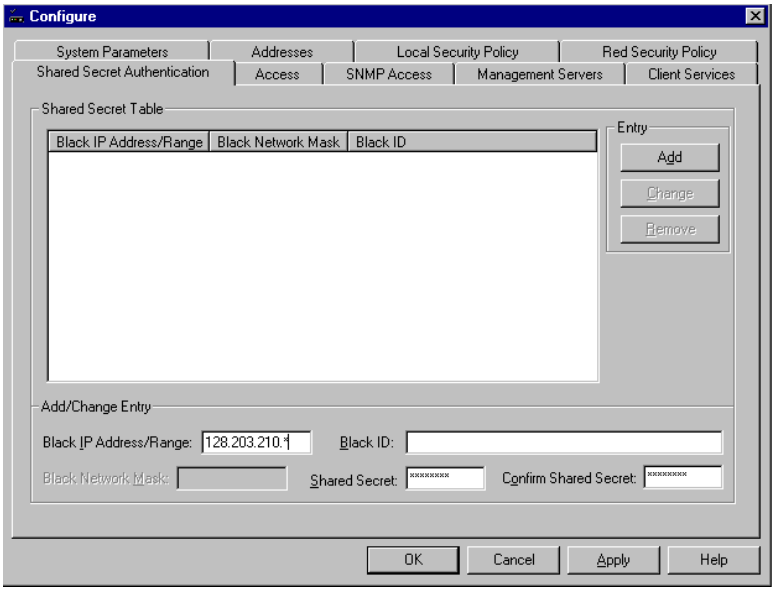
Click the ***Local Security Policy*** tab



Change the security Level to "***Mobile Client w/Shared Secret***" and leave Default Policy to "***Block***"

SHARED SECRET AUTHENTICATION

Click the ***Shared Secret Authentication*** tab



In the ***Add/Change Entry*** frame:

Type the IP range (**128.203.210.*)** in the Black IP Address/Range box.

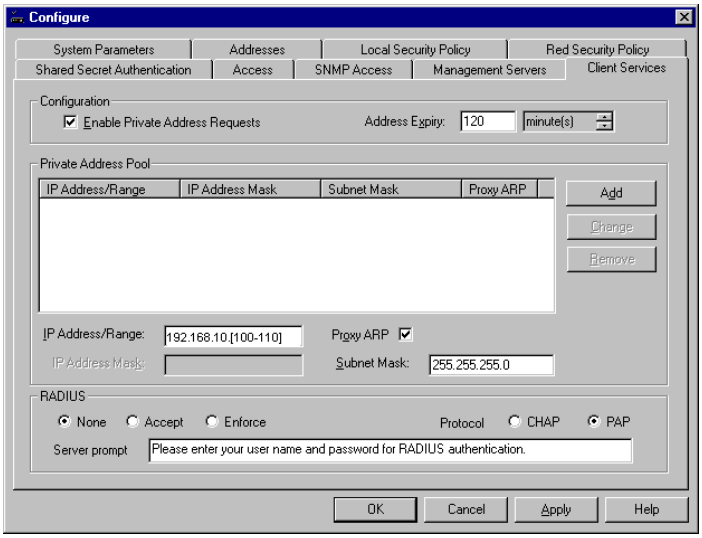
Enter as “shared secret” **secret99** in the Shared Secret box and confirm it in the Confirm Shared Secret box.

In the Entry frame (on the right) click **ADD**

PRIVATE ADDRESS REQUESTS

To enable and configure Private Address Requests, do following:

Click the ***Client Services*** tab



In the ***Configuration*** frame, select the Enable Private Address Requests checkbox

In the ***Private Address Pool*** frame, type the appropriate address range in the IP Address/Range box

Select Proxy ARP check box
Note*: Selecting Proxy ARP check box instruct PERMIT/Gate to respond to ARP requests on behalf of clients with IP address in the private address pool table. Use this checkbox only, when using Private Address Pool*

IP Address/Range **192.168.10.[100-110]**

Type 255.255.255.0 in the Subnet Mask box

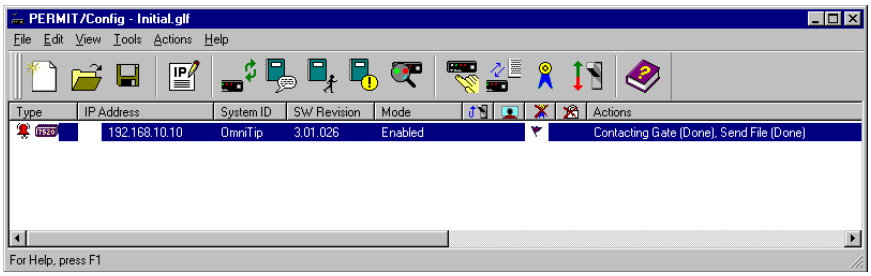
Leave blank the IP Address Mask box

Click **Add** (in the Entry frame, on the right) and than **OK**

Rebuild the secure map by going to TOOLS ⇨ BUILD SECURE MAP

Have ***Typical Settings*** checked and click on **NEXT**

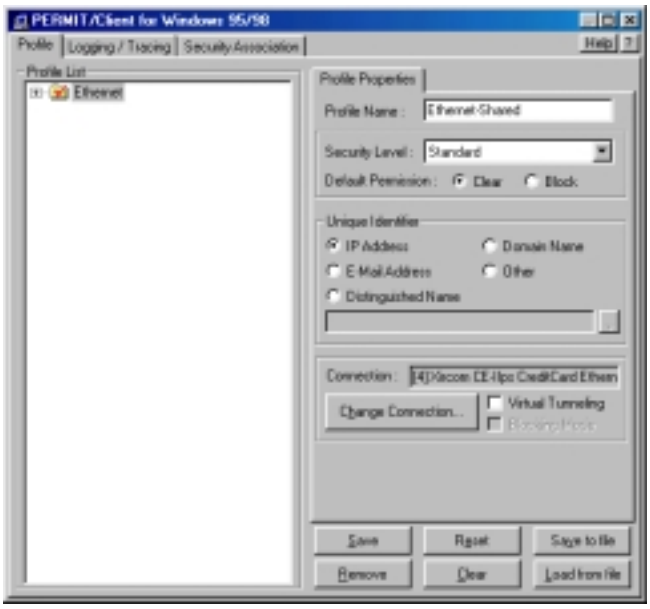
Have the Secure Map send directory to the gates and click on **FINISH**



You should see after file has been uploaded a ***Send File (Done)***

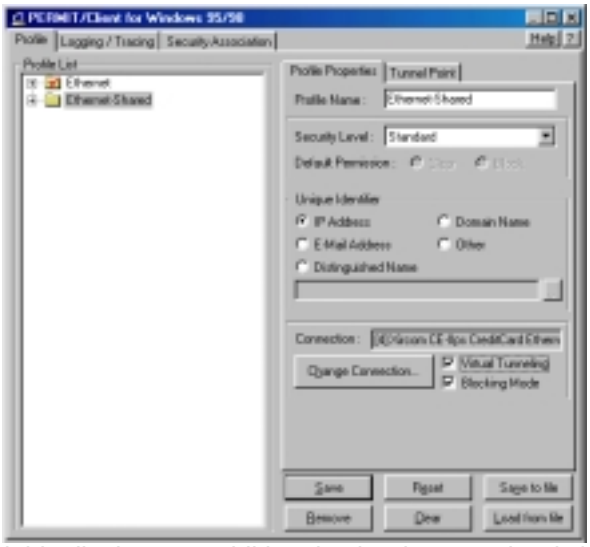
Enabling and Configuring Virtual Tunneling on Client using shared Secret

Open Permit/Client Profile Window



For further scenarios, change the Profile Name to Ethernet-Shared (I will use this basic settings for other OmniTips as well)

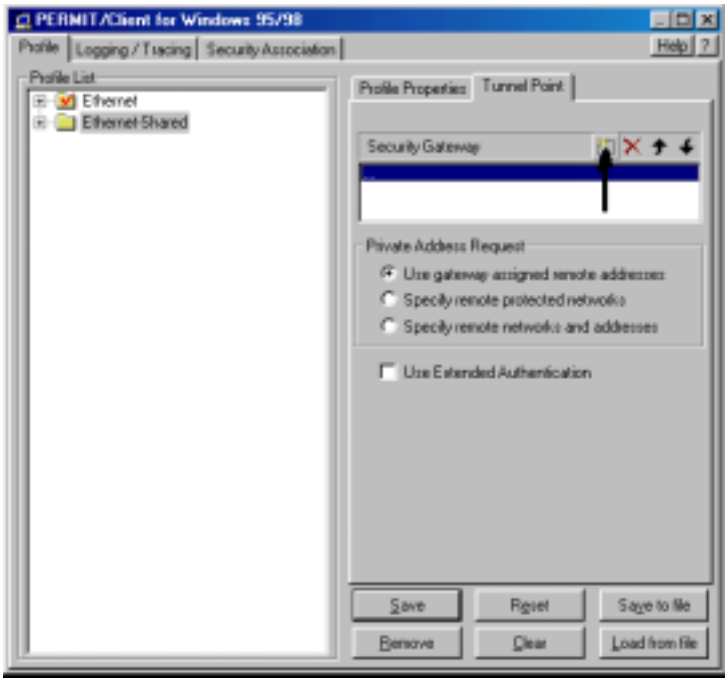
Select the Virtual Tunneling check box and change Security Level to **Mobile Client w/Shared Secret**



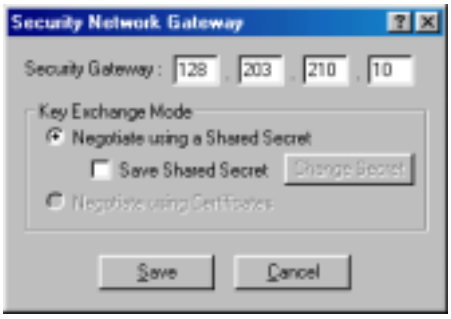
(This displays an additional sub-tab, Tunnel Point)

Click the Tunnel Point tab

In the Security Gateway box, click the New/Edit button on the box header ….



…. this will open a new window



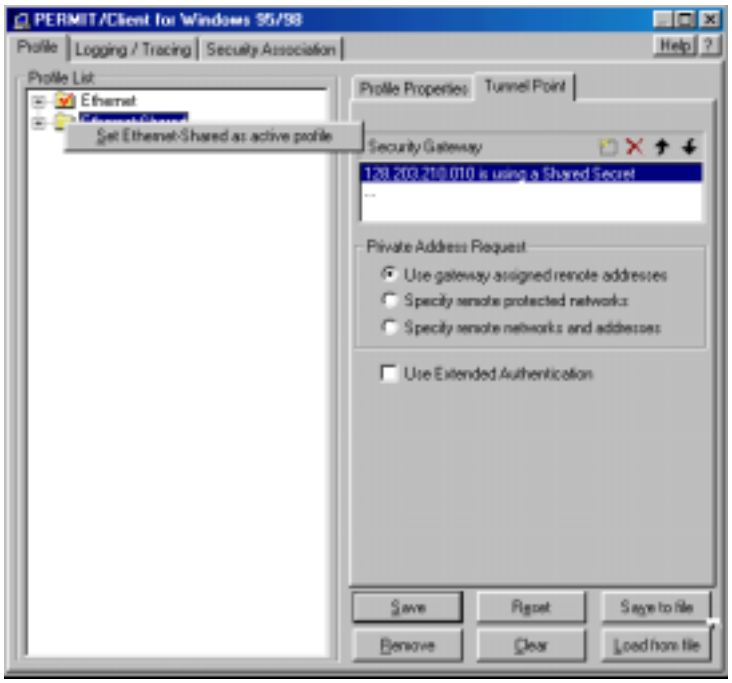
In the Security Network Gateway box, type the IP address of the Black side of your Gate

Ensure Negotiate using a Shared Secret is selected
***Note**: Do not select the Save Share Secret check box, as you are not using extended authentication*

Click **Save**

Negotiate using Certificate is grayed out, because we installed the Client without having an entrust.ini available.

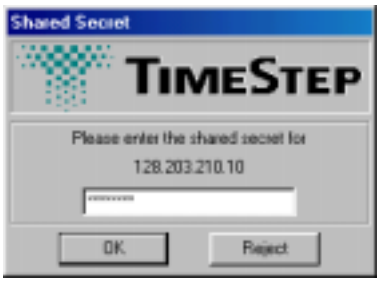
Right click the Ethernet-Shared profile in the Profile List and select Set "***Ethernet-Shared***" as active profile



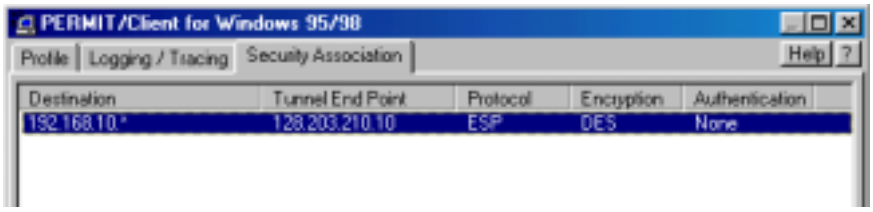
Click **Save**

Clear the Disable setting on the ***TimeStep tool*** tray popup

The ***Shared Secret*** popup appears

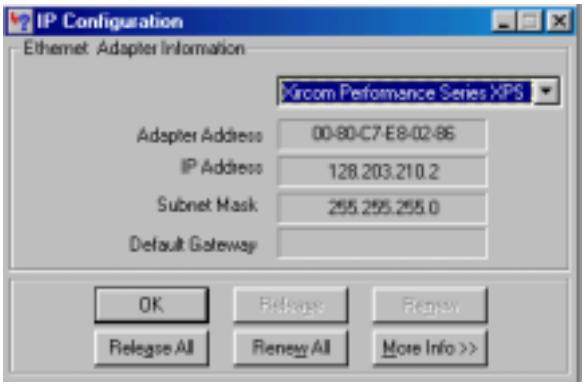


Type the “shared secret” **secret99** and then click OK
Select the ***Security Association tab*** (beside the Logging /Tracing tab)

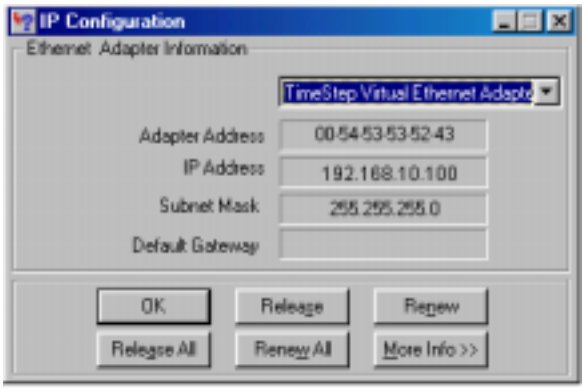


You should now see a Security Association, where Destination points to the red-side of your gate and the Tunnel End Point is actually the Interface’s IP of the black-side

Run Winipcfg (or ipconfig) and check the adapter list. First, you will see the active Network Interface associated with an IP address out of the black range. My client is using ***128.203.210.2***, while there’s another Adapter, which is interesting.



The TimeStep Virtual Private Ethernet Adapter has been added to the list of adapters and has the IP address assigned by the Gate from its Private Address Pool



An this guy is using an IP Address out of the PAR Pool (similar to DHCP), we have defined at the Private Address Requests, during the Gate Configuration.

Well, that's it. You should now ping from the Client PC to the Remote Configuration Utility PC. The first Ping packet may time out, because of Proxy ARP. Let the ping run with "-t" and disable the VPN Client. You will see an immediate "Destination unreachable". Reactive the VPN client, get the shared secret in, and enjoy how the tunnels is re-established and the ping is going to succeed again.