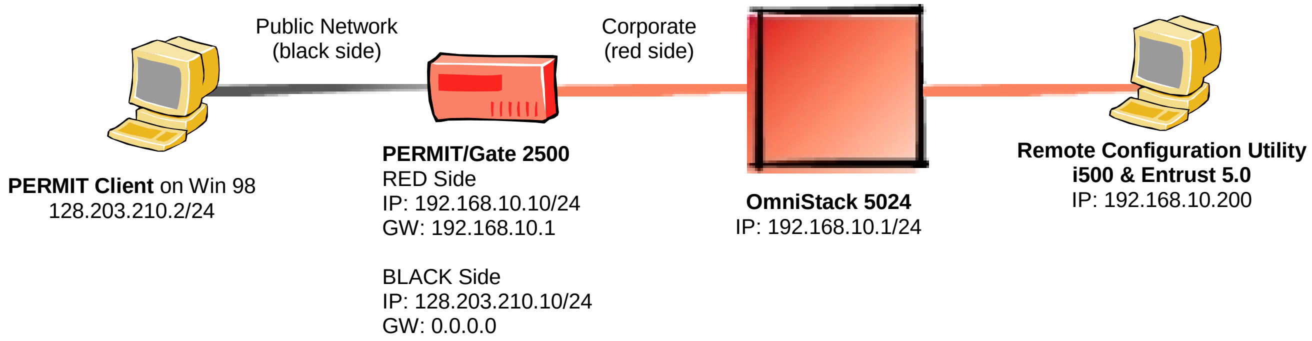
Demo Scenario - VPN Client and VPN Gateway using Certificates

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 2500 – Alcatel 713x
OmniStack 5024

Software:

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

Document:

Installing i500 & Entrust 5.0 ⇨ http://www.bemsel.com/omnitip_collection/i500_Entrust5_v1.2.pdf

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:

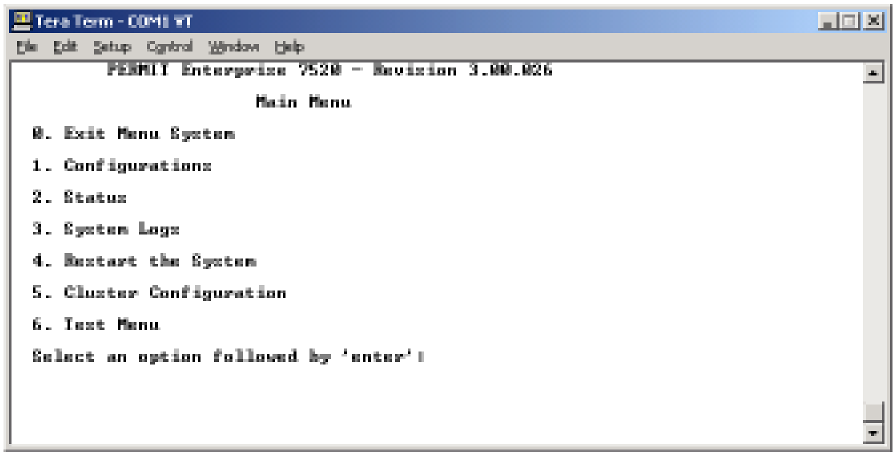
▪ Bits per second	➪ 19,200 (factory default of the box)
▪ Data bits	➪ 8
▪ Parity	➪ None
▪ Stop bits	➪ 1
▪ Flow control	➪ Xon/Xoff

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



```
        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':
```

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
t
his? ('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
```

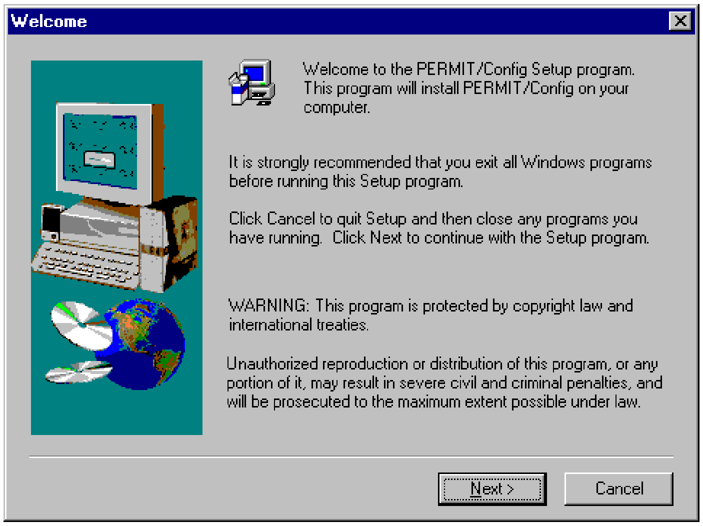
```
           PERMIT Enterprise 7520 - Revision 3.00.026

                         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.



Welcome

Welcome to the PERMIT/Config Setup program. This program will install PERMIT/Config on your computer.

It is strongly recommended that you exit all Windows programs before running this Setup program.

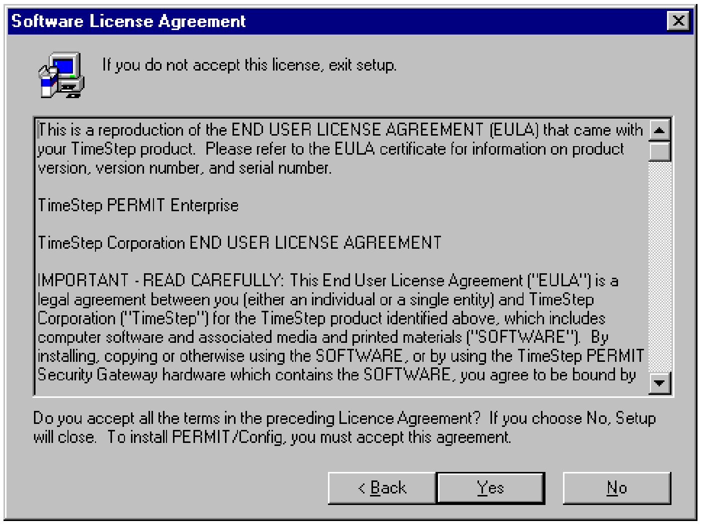
Click Cancel to quit Setup and then close any programs you have running. Click Next to continue with the Setup program.

WARNING: This program is protected by copyright law and international treaties.

Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

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



Software License Agreement

If you do not accept this license, exit setup.

This is a reproduction of the END USER LICENSE AGREEMENT (EULA) that came with your TimeStep product. Please refer to the EULA certificate for information on product version, version number, and serial number.

TimeStep PERMIT Enterprise

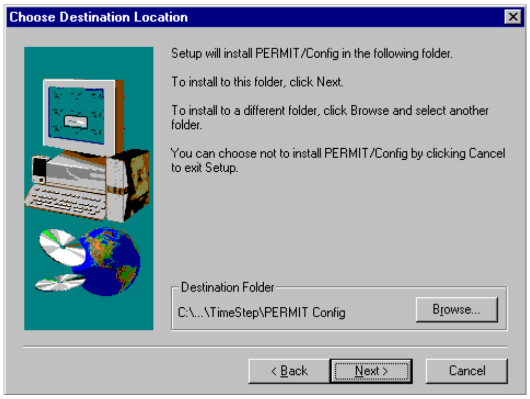
TimeStep Corporation END USER LICENSE AGREEMENT

IMPORTANT - READ CAREFULLY: This End User License Agreement ("EULA") is a legal agreement between you (either an individual or a single entity) and TimeStep Corporation ("TimeStep") for the TimeStep product identified above, which includes computer software and associated media and printed materials ("SOFTWARE"). By installing, copying or otherwise using the SOFTWARE, or by using the TimeStep PERMIT Security Gateway hardware which contains the SOFTWARE, you agree to be bound by

Do you accept all the terms in the preceding Licence Agreement? If you choose No, Setup will close. To install PERMIT/Config, you must accept this agreement.

This technical document has been created and evaluated by myself with the purpose to help friends to get into new technology and installations. There is no financial interest, however, please respect the copyright.

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



Choose Destination Location

Setup will install PERMIT/Config in the following folder.

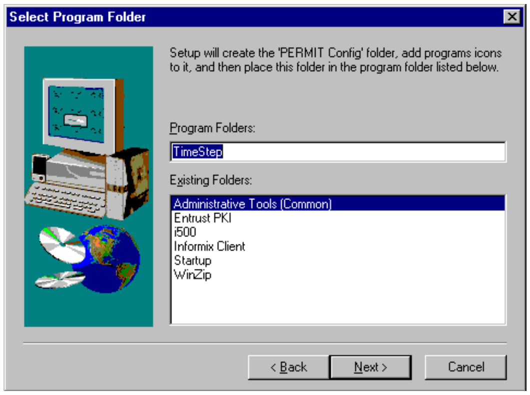
To install to this folder, click Next.

To install to a different folder, click Browse and select another folder.

You can choose not to install PERMIT/Config by clicking Cancel to exit Setup.

Destination Folder
C:\...\TimeStep\PERMIT Config

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



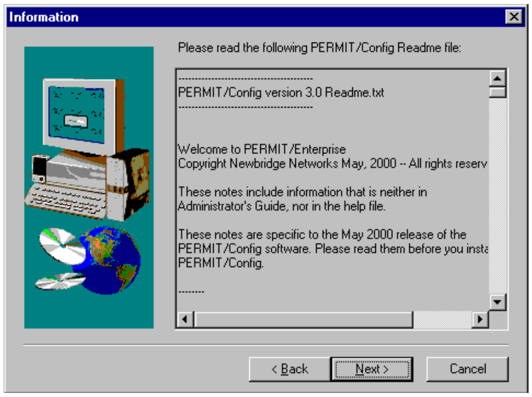
Select Program Folder

Setup will create the 'PERMIT Config' folder, add programs icons to it, and then place this folder in the program folder listed below.

Program Folders:
TimeStep

Existing Folders:
Administrative Tools (Common)
Entrust PKI
i500
Informix Client
Startup
WinZip

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

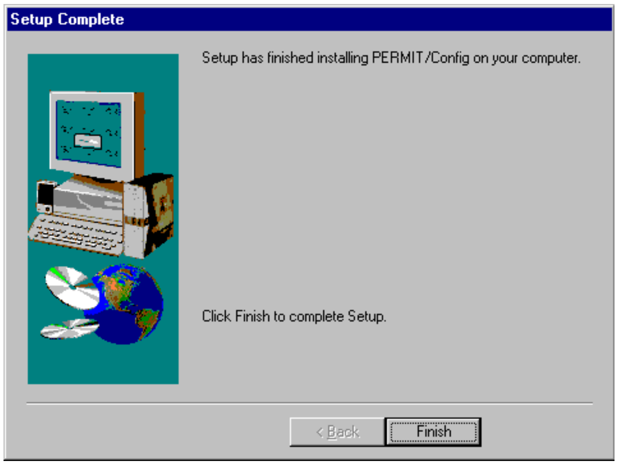


Information

Please read the following PERMIT/Config Readme file:

```
-------------------------------------------
PERMIT/Config version 3.0 Readme.txt
-------------------------------------------


Welcome to PERMIT/Enterprise
Copyright Newbridge Networks May, 2000 -- All rights reserv

These notes include information that is neither in
Administrator's Guide, nor in the help file.

These notes are specific to the May 2000 release of the
PERMIT/Config software. Please read them before you insta
PERMIT/Config.

--------
```

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



Setup Complete

Setup has finished installing PERMIT/Config on your computer.

Click Finish to complete Setup.

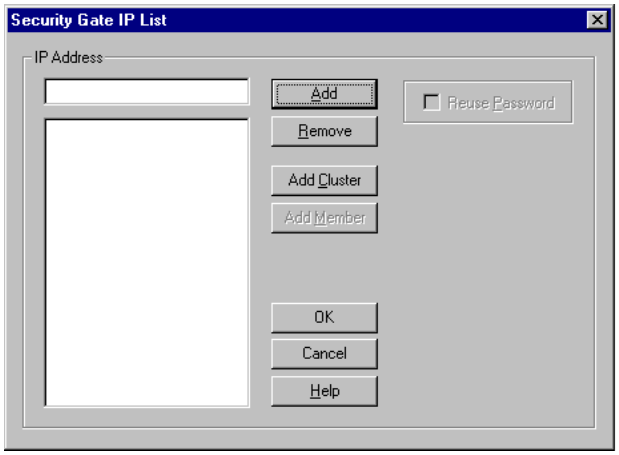
Click **FINISH**

Exit the install utility, when not exiting automatically

This completes the installation phase.

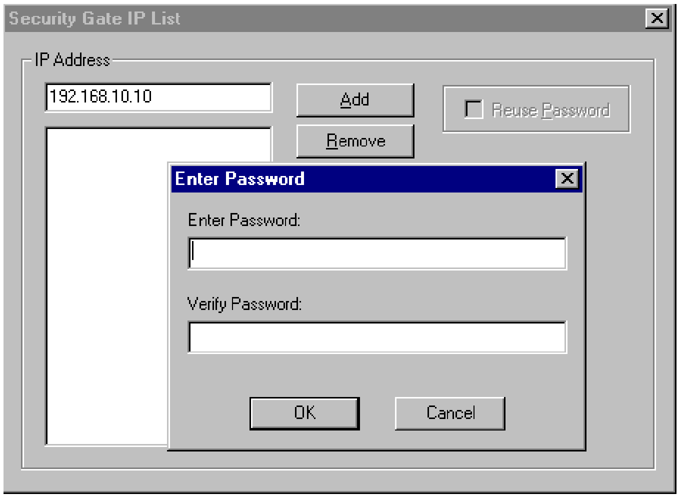
Configuring the Utility

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



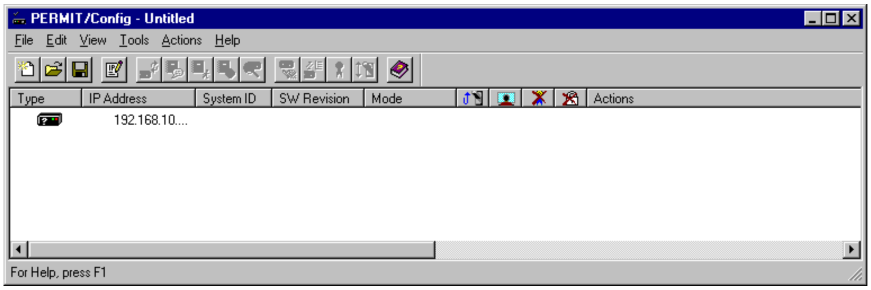
Security Gate IP List

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



IP Address: 192.168.10.10

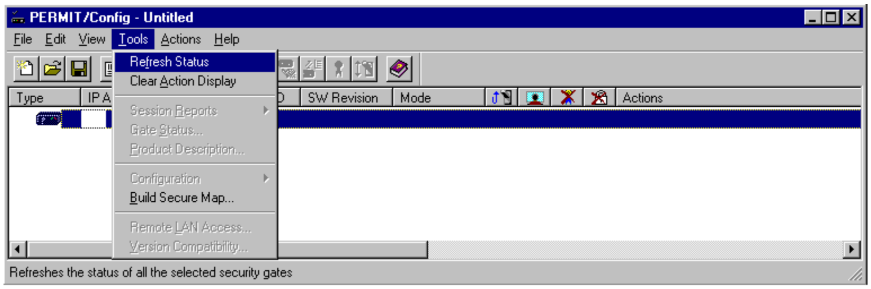
Type the IP Address ***192.168.10.10*** and click **ADD.** A new window pops up, type and confirm the password for accessing the Gate. Remember “***remote***”, which has been set earlier in the section “***Configuring for Remote Access***” and click on **OK**.



Type	IP Address	System ID	SW Revision	Mode	Actions
	192.168.10....				

For Help, press F1

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



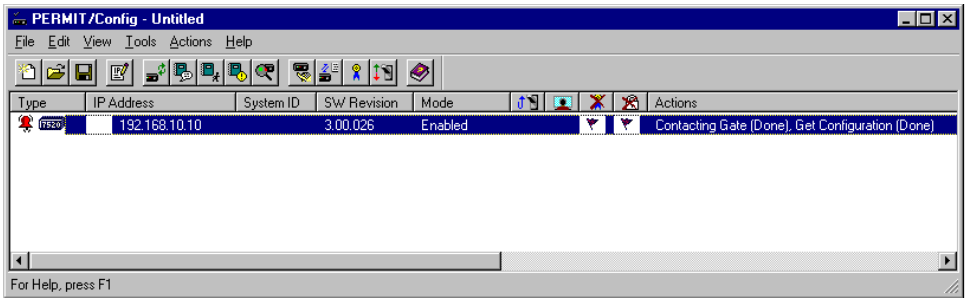
Refreshes the status of all the selected security gates

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



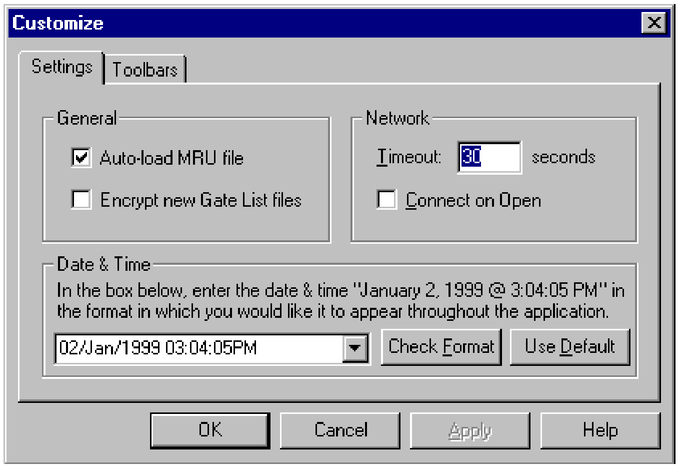
Type	IP Address	System ID	SW Revision	Mode	Actions
7520	192.168.10.10		3.00.026	Enabled	Contacting Gate (Done), Get Configuration (Done)

For Help, press F1

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***



General

☑ Auto-load MRU file

☐ Encrypt new Gate List files

Network

Timeout: 30 seconds

☐ Connect on Open

Date & Time

In the box below, enter the date & time "January 2, 1999 @ 3:04:05 PM" in the format in which you would like it to appear throughout the application.

02/Jan/1999 03:04:05PM

On the Settings tab:

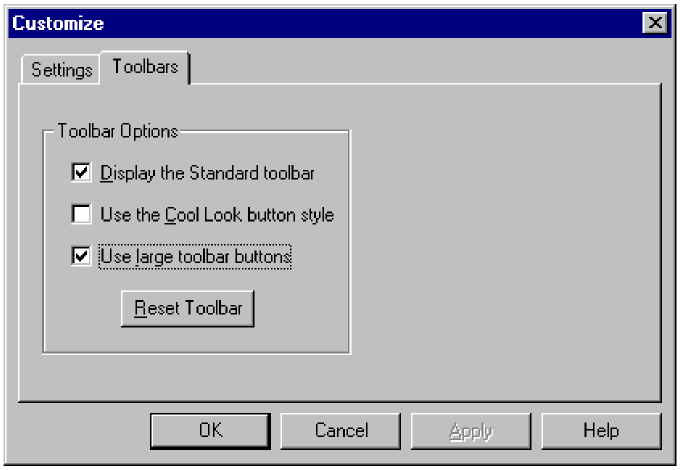
Ensure that the Autoload MRU file check box is selected. This will automatically load the Most Recently Used gateway list file when started.

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



Customize

Settings | Toolbars

Toolbar Options

☑ Display the Standard toolbar

☐ Use the Cool Look button style

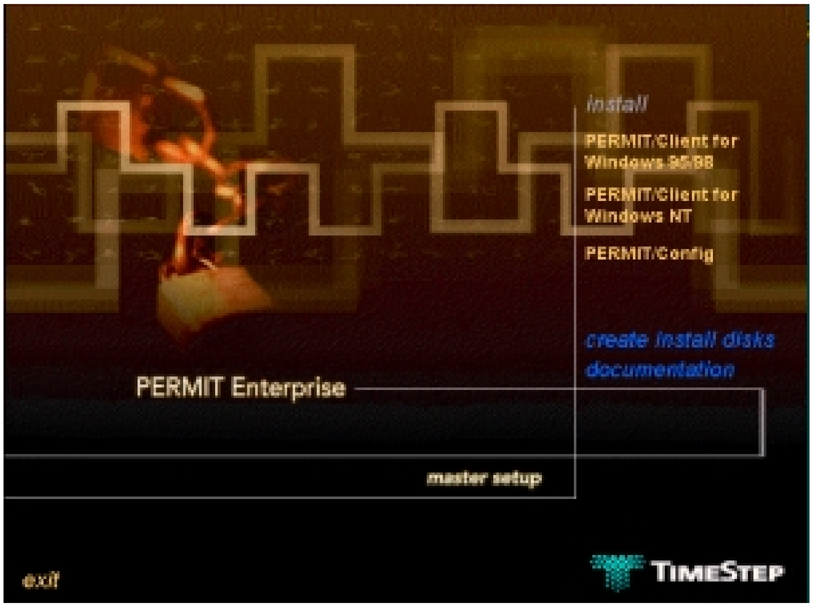
☑ Use large toolbar buttons

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

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

Installing the Secure VPN Client

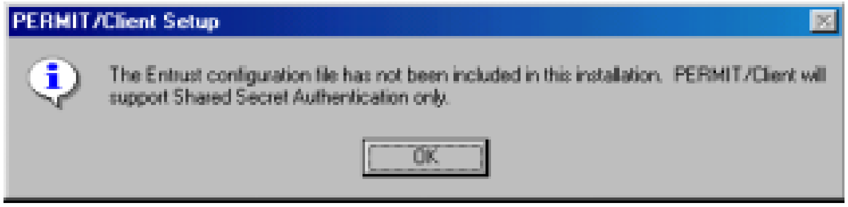
Start the Secure VPN Client setup program
When inserting the CD ROM and Auto-Play is enabled, TimeStep's Master setup window should open automatically.



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

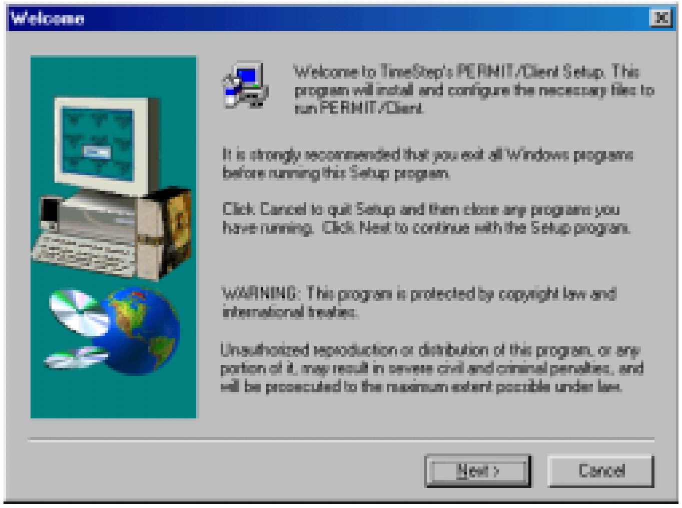
- PERMIT Client 95	➩ does work with Windows 95 and 98
- PERMIT Client NT	➩ does work with Windows NT 4.0 only

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



The Entrust configuration file has not been included in this installation. PERMIT/Client will support Shared Secret Authentication only.

Click **OK** to bypass the warning message about the utility being unable to find entrust.ini. I will add the entrust.ini later in this document.



Welcome to TimeStep's PERMIT/Client Setup. This program will install and configure the necessary files to run PERMIT/Client.

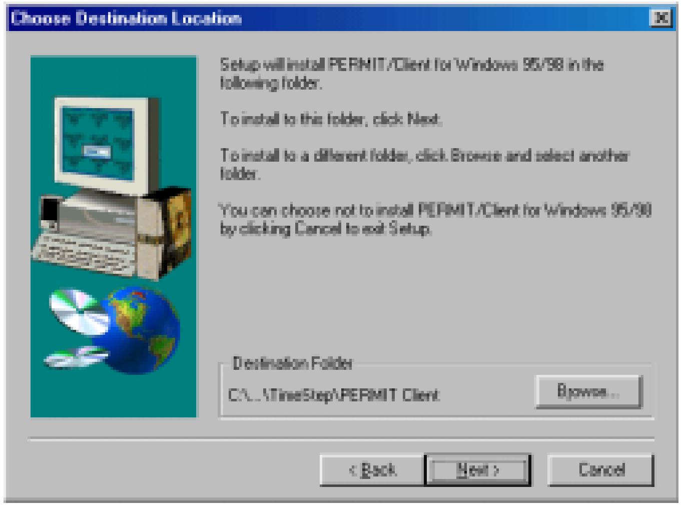
It is strongly recommended that you exit all Windows programs before running this Setup program.

Click Cancel to quit Setup and then close any programs you have running. Click Next to continue with the Setup program.

WARNING: This program is protected by copyright law and international treaties.

Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

Click **NEXT**



Choose Destination Location

Setup will install PERMIT/Client for Windows 95/98 in the following folder.

To install to this folder, click Next.

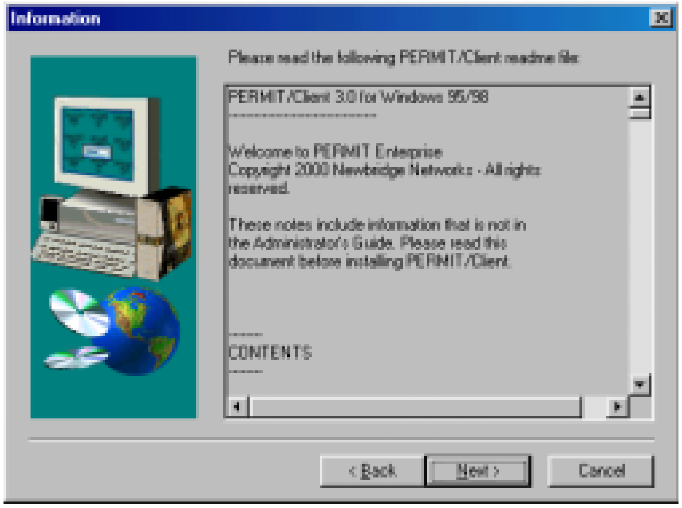
To install to a different folder, click Browse and select another folder.

You can choose not to install PERMIT/Client for Windows 95/98 by clicking Cancel to exit Setup.

Destination Folder

C:\...\TimeStep\PERMIT Client

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



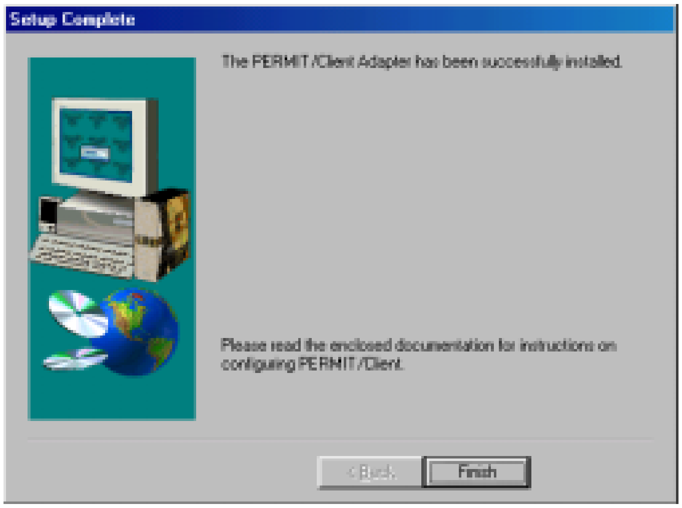
Information

Please read the following PERMIT/Client readme file:

```
PERMIT/Client 3.0 for Windows 95/98
-----------------------------------

Welcome to PERMIT Enterprise
Copyright 2000 Newbridge Networks - All rights
reserved.

These notes include information that is not in
the Administrator's Guide. Please read this
document before installing PERMIT/Client.



--------
CONTENTS
--------
```

Scan the readme notes and click **NEXT**

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



Setup Complete

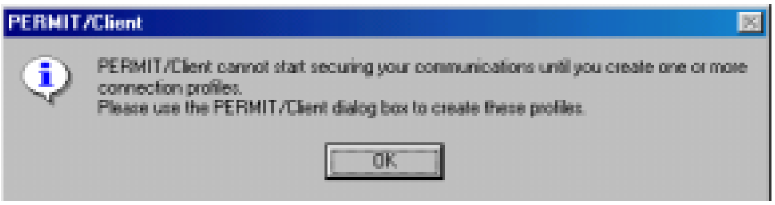
The PERMIT/Client Adapter has been successfully installed.

Please read the enclosed documentation for instructions on configuring PERMIT/Client.

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 binded to this new adapter as well.*



PERMIT/Client

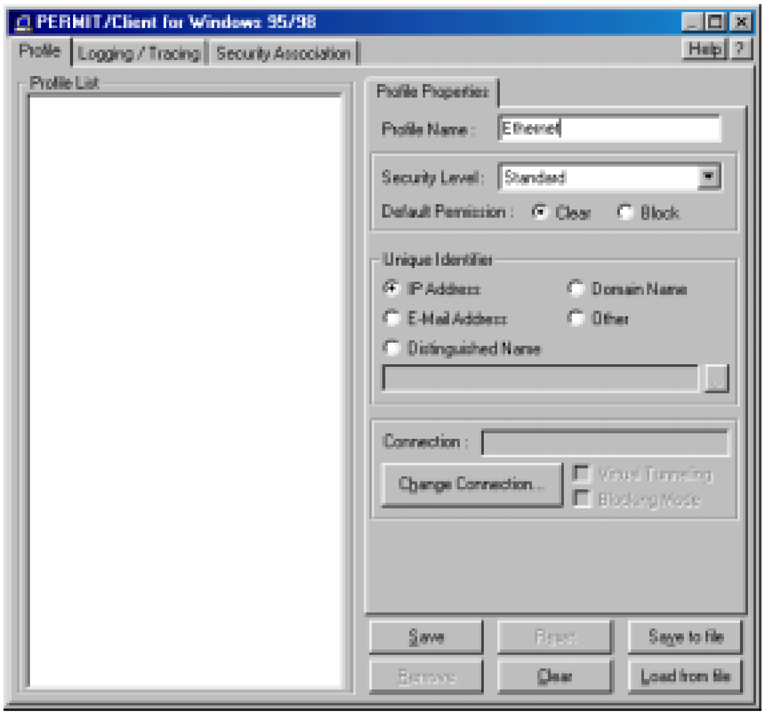
PERMIT/Client cannot start securing your communications until you create one or more connection profiles.
Please use the PERMIT/Client dialog box to create these profiles.

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



Profile Name : Ethernet

Security Level : Standard

Default Permission : ● Clear ○ Block

Unique Identifier

● IP Address ○ Domain Name

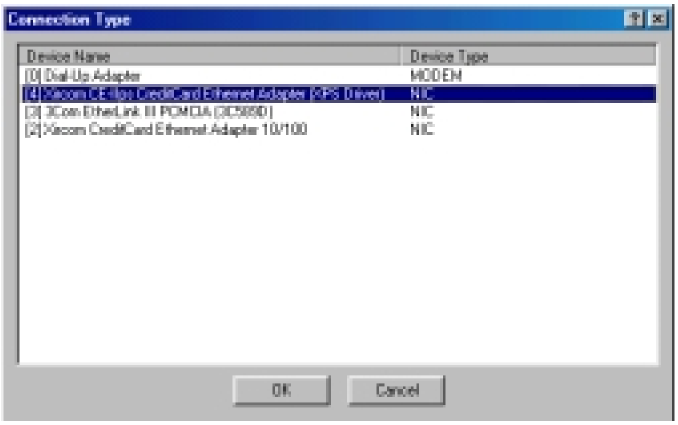
○ E-Mail Address ○ Other

○ Distinguished Name

Connection :

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

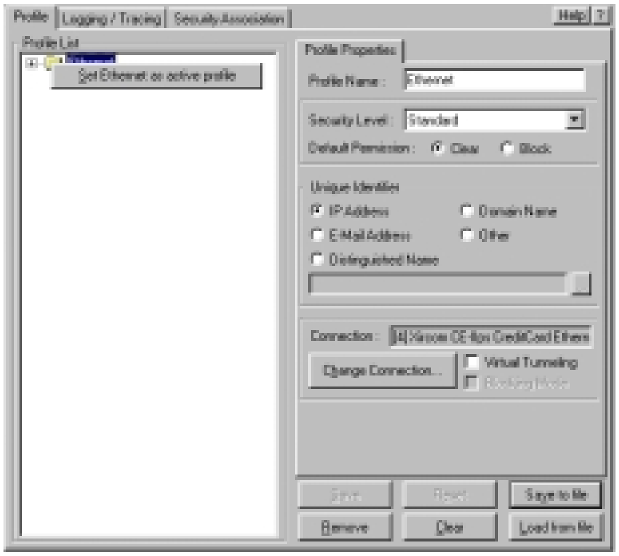
Click **CHANGE CONNECTION**
Select the Network Interface Card



Device Name	Device Type
[0] Dial-Up Adapter	MODEM
[4] Xircom CE-IIps CreditCard Ethernet Adapter (RPS Driver)	NIC
[3] 3Com EtherLink III PCMCIA (3C589D)	NIC
[2] Xircom CreditCard Ethernet Adapter 10/100	NIC

***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



Profile Name : Ethernet

Security Level : Standard

Default Permission : ● Clear ○ Block

Unique Identifier

● IP Address ○ Domain Name

○ E-Mail Address ○ Other

○ Distinguished Name

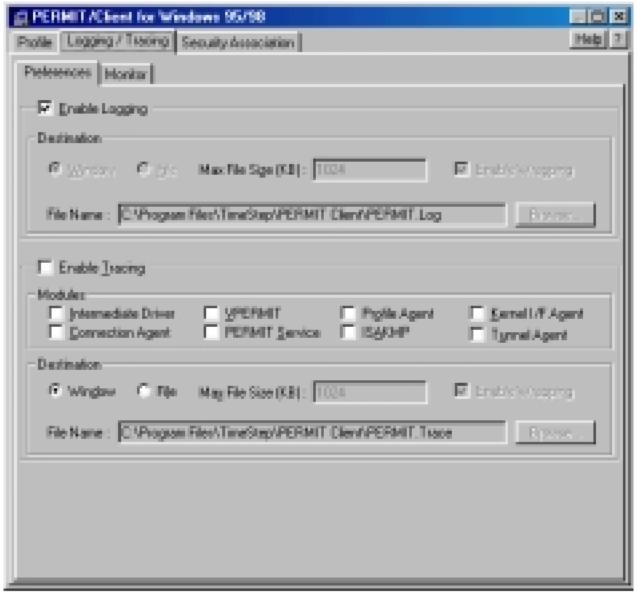
Connection : [4] Xircom CE-4ps CreditCard Ethern

☐ Virtual Tunneling

☐ Blocking Mode

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



☑ Enable Logging

Destination

● Window ○ File Max File Size (KB) : 1024 ☑ Enable Wrapping

File Name : C:\Program Files\TimeStep\PERMIT Client\PERMIT.Log

☐ Enable Tracing

Modules

☐ Intermediate Driver ☐ VPERMIT ☐ Profile Agent ☐ Kernel I/F Agent

☐ Connection Agent ☐ PERMIT Service ☐ ISAKMP ☐ Tunnel Agent

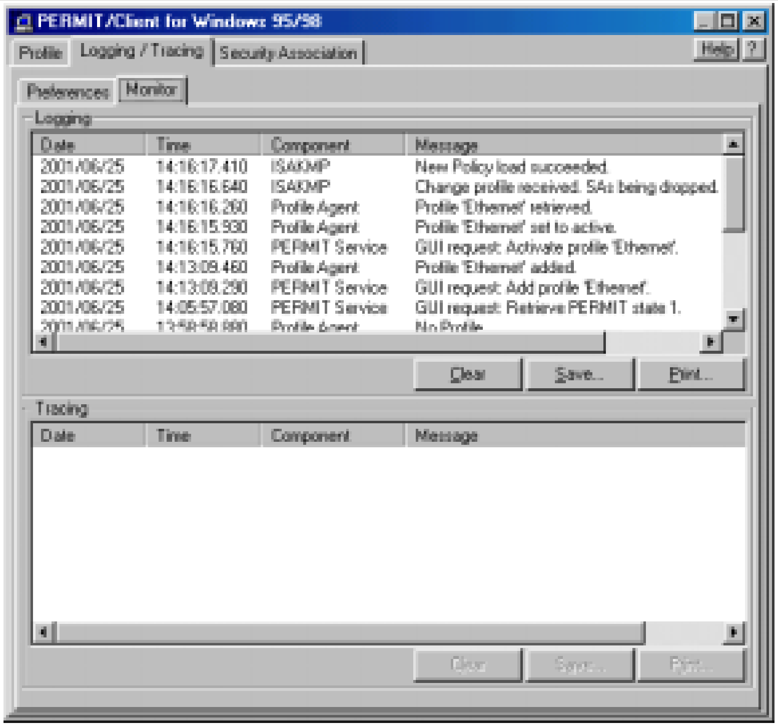
Destination

● Window ○ File Max File Size (KB) : 1024 ☑ Enable Wrapping

File Name : C:\Program Files\TimeStep\PERMIT Client\PERMIT.Trace

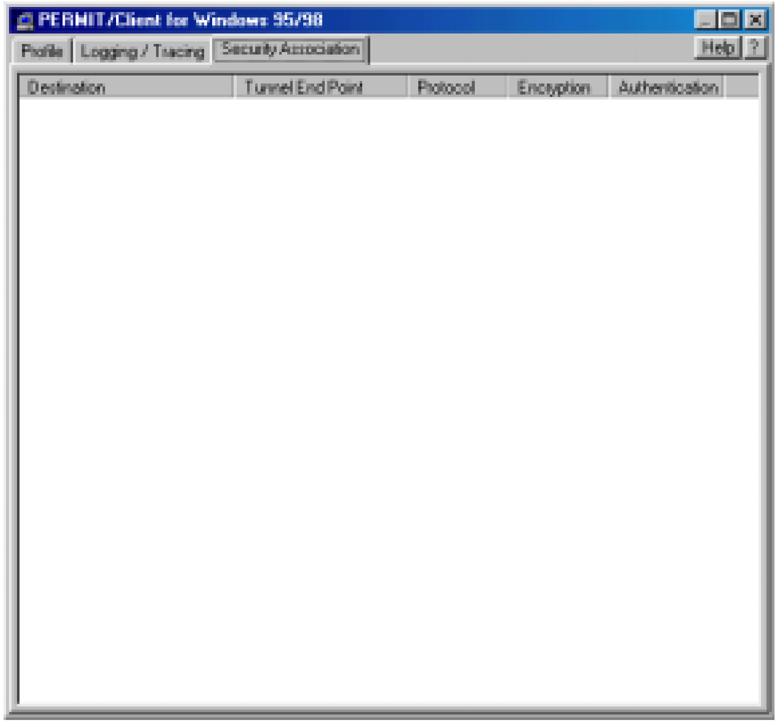
Ensure that the Enable logging checkbox is selected

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



```
Date        Time          Component        Message
2001/06/25  14:16:17.410  ISAKMP           New Policy load succeeded.
2001/06/25  14:16:16.640  ISAKMP           Change profile received. SAs being dropped.
2001/06/25  14:16:16.260  Profile Agent    Profile 'Ethernet' retrieved.
2001/06/25  14:16:15.930  Profile Agent    Profile 'Ethernet' set to active.
2001/06/25  14:16:15.760  PERMIT Service   GUI request: Activate profile 'Ethernet'.
2001/06/25  14:13:09.460  Profile Agent    Profile 'Ethernet' added.
2001/06/25  14:13:09.290  PERMIT Service   GUI request: Add profile 'Ethernet'.
2001/06/25  14:05:57.080  PERMIT Service   GUI request: Retrieve PERMIT state 1.
2001/06/25  13:58:58.880  Profile Agent    No Profile
```

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



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

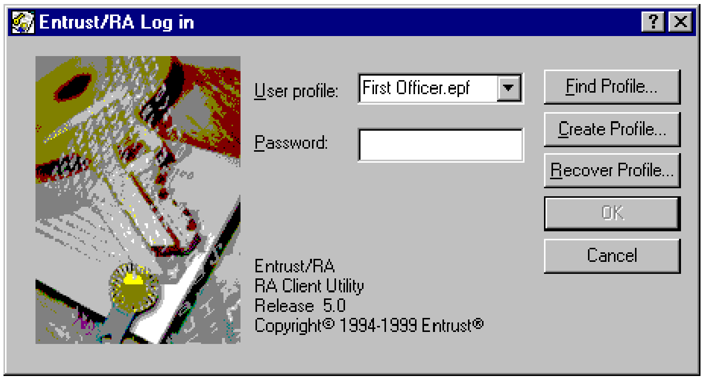
Before you can start using PKI, you have to have i500 and Entrust installed. For instructions on how to achieve this installation, I refer to my Technical Tip: "Installing i500 and Entrust 5.

http://www.bemsel.com/TechTip/RB_i500_Entrust5_v1.2.pdf

Adding Users and Gateways for PKI use

Make sure Entrust Service is up and running. To do so, open the control panel, click on Services and look for Entrust/Authority Service. Verify, that this service is running.

Logon to the Entrust RA and use "First Officer"



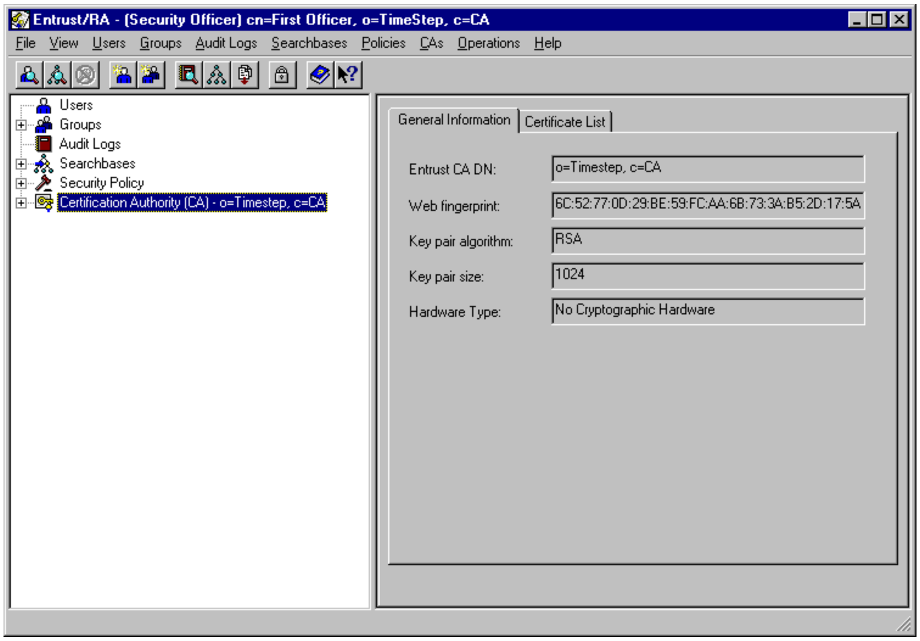
Entrust/RA Log in

User profile: First Officer.epf

Password:

Entrust/RA
RA Client Utility
Release 5.0
Copyright© 1994-1999 Entrust®

When logged on, you see the main window



Entrust/RA - (Security Officer) cn=First Officer, o=TimeStep, c=CA

File View Users Groups Audit Logs Searchbases Policies CAs Operations Help
Users
Groups
Audit Logs
Searchbases
Security Policy
Certification Authority (CA) - o=Timestep, c=CA
General Information
Certificate List

Entrust CA DN: o=Timestep, c=CA

Web fingerprint: 6C:52:77:0D:29:BE:59:FC:AA:6B:73:3A:B5:2D:17:5A

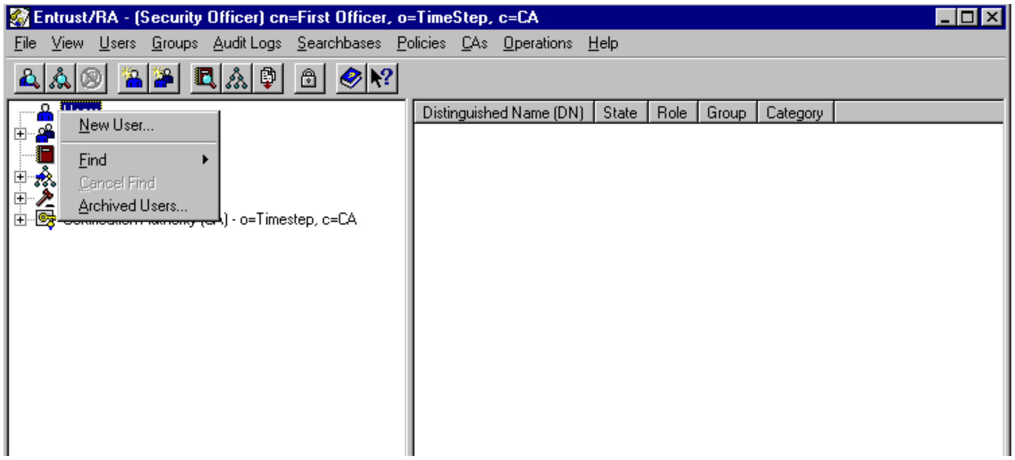
Key pair algorithm: RSA

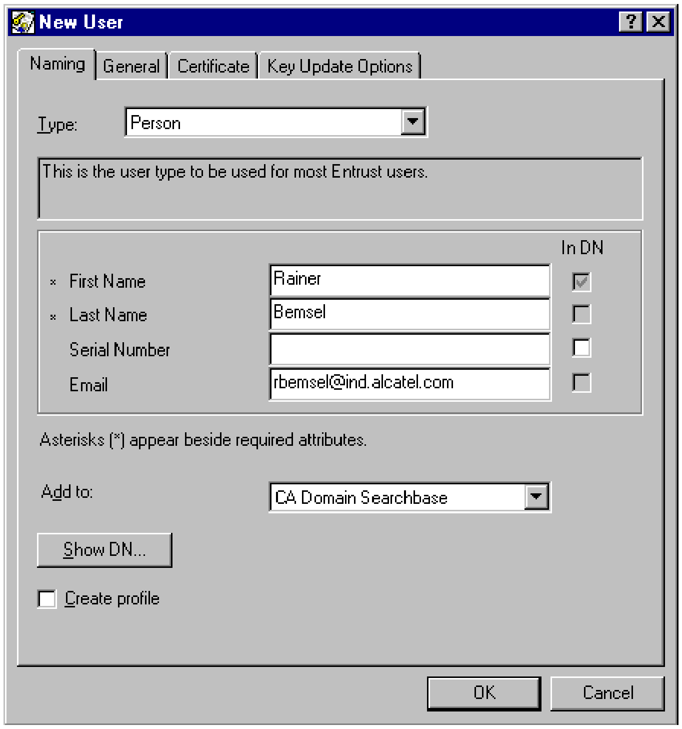
Key pair size: 1024

Hardware Type: No Cryptographic Hardware

Add User

Right click Users in the left plane and select ***NEW USER***


Entrust/RA - (Security Officer) cn=First Officer, o=TimeStep, c=CA
File View Users Groups Audit Logs Searchbases Policies CAs Operations Help
New User...
Find
Cancel Find
Archived Users...
) - o=Timestep, c=CA
Distinguished Name (DN)
State
Role
Group
Category


New User

Naming | General | Certificate | Key Update Options

Type: Person

This is the user type to be used for most Entrust users.

		In DN
* First Name	Rainer	☑
* Last Name	Bemsel	□
Serial Number		□
Email	rbemsel@ind.alcatel.com	□

Asterisks (*) appear beside required attributes.

Add to: CA Domain Searchbase

Show DN...

□ Create profile

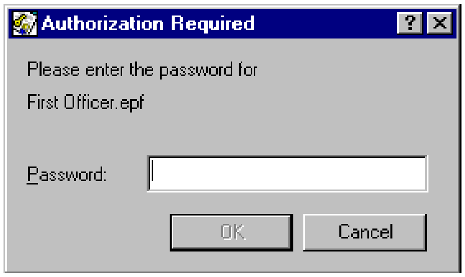
OK Cancel

Type in following mandatory values

First Name	**Rainer**
Last Name	**Bemsel**

You could use any name, just make sure you remember, when configuring VPN Client

You will be asked to confirm the password to be allowed of creating this user

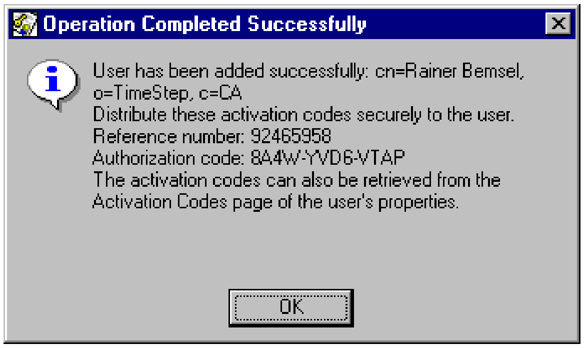


Please enter the password for
First Officer.epf

Password:

Select the ***Enable*** for Entrust Checkbox

Finally, you will get a Reference Number and an Authorization Code to request your certificate later on.



User has been added successfully: cn=Rainer Bemsel, o=TimeStep, c=CA
Distribute these activation codes securely to the user.
Reference number: 92465958
Authorization code: 8A4W-YVD6-VTAP
The activation codes can also be retrieved from the Activation Codes page of the user's properties.

Click OK to accept the ***Operation Completed Successfully*** info box

Add Gateway

Right click Users in the left plane and select **NEW USER**

Type ***Omni*** in the First Name box and ***Tip*** in the Last Name box

Select the ***Enable*** for Entrust Checkbox

Click OK to accept the ***Operation Completed Successfully*** info box

From the Setup Information tab, note the Reference Number and Authorization Code for use in this scenario. In reality you would deliver the information direct to the User in order to have the user authorized

Configure VPN Gateway for Getting Certified

Two steps are required to set the authentication level to ISAKMP-Certificate.

- Check Time and date on the Gate (Differences more than one hour between CA and Gate certificate request will fail)
- Change the Red Security Policy for that connection

Check Time and change, when necessary

Logon to console of the Gate

```
PERMIT Enterprise 2520 - 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 2520 - 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': 4
```

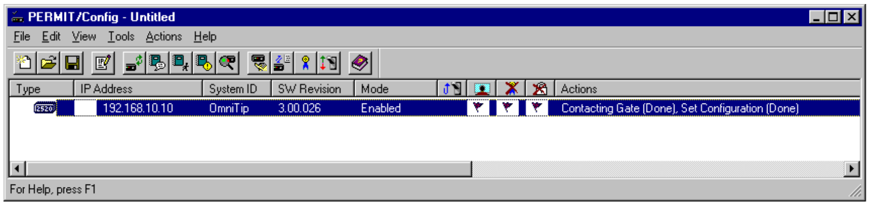
```
PERMIT Enterprise 2520 - Revision 3.00.026
            System Configuration

   0. Exit Menu
   1. System Parameters
   2. System Information

  Select an option followed by 'enter': 1


PERMIT Enterprise 2520 - Revision 3.00.026
            System Parameters

   0. Exit Menu
   1. Date and Time                       2000/12/14 09:33:07
   2. Time Zone [GMT offset]              -5:00
   3. Console Idle Timeout (minutes)      5
   4. Baud Rate                           19200
   5. Operating Mode (En/Dis)             Enable
   6. MTU Size                            1500
   7. Ethernet Setting (Black/Red)        10Mb HD/10Mb HD
   8. Ethernet Status (Black/Red)         10Mb HD/10Mb HD

  Select an option followed by 'enter': 1

  Enter a new parameter: 2001/07/10 09:24:00


PERMIT Enterprise 2520 - Revision 3.00.026
                  System Parameters

   0. Exit Menu
   1. 1. Date and Time                    2001/07/10 09:24:00
   2. 2. Time Zone [GMT offset]           -5:00
   3. 3. Console Idle Timeout (minutes)   5
   4. 4. Baud Rate                        19200
   5. 5. Operating Mode (En/Dis)          Enable
   6. 6. MTU Size                         1500
   7. 7. Ethernet Setting (Black/Red)     10Mb HD/10Mb HD
   8. 8. Ethernet Status (Black/Red)      10Mb HD/10Mb HD

  Select an option followed by 'enter': 2

  Enter a new parameter: +1

PERMIT Enterprise 2520 - Revision 3.00.026
                  System Parameters


   0. Exit Menu
   1. 1. Date and Time                    2001/07/10 09:24:10
```

```
 2. 2. Time Zone [GMT offset]          1:00
 3. 3. Console Idle Timeout (minutes)  5
 4. 4. Baud Rate                       19200
 5. 5. Operating Mode (En/Dis)         Enable
 6. 6. MTU Size                        1500
 7. 7. Ethernet Setting (Black/Red)    10Mb HD/10Mb HD
 8. 8. Ethernet Status (Black/Red)     10Mb HD/10Mb HD

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

Using PERMIT/Config to configure VPN Gateway for certificates

Ensure that Client is disabled

Activate the Configuration Utility and refresh the status

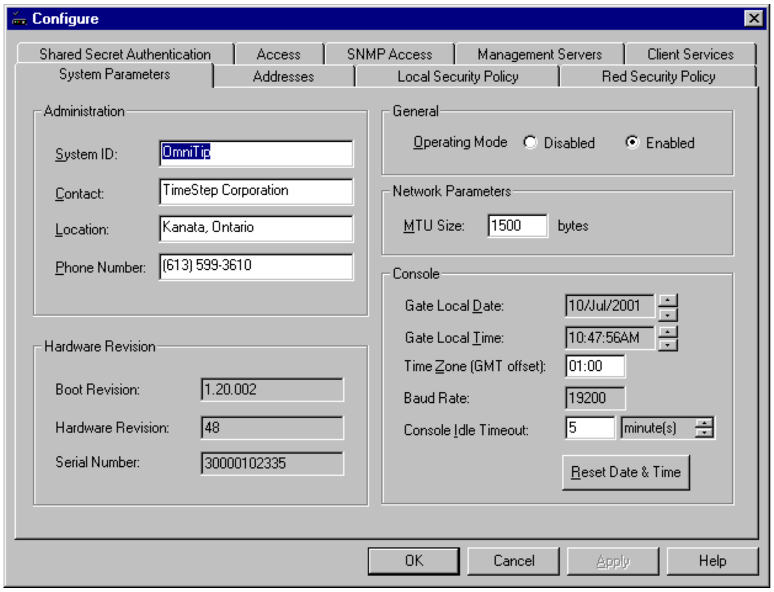


PERMIT/Config - Untitled

Type	IP Address	System ID	SW Revision	Mode	Actions
2520	192.168.10.10	OmniTip	3.00.026	Enabled	Contacting Gate (Done), Set Configuration (Done)

For Help, press F1

Open the Configure Window by ACTIONS ⇨ CONFIGURE



Configure

Administration

System ID: OmniTip

Contact: TimeStep Corporation

Location: Kanata, Ontario

Phone Number: (613) 599-3610

Hardware Revision

Boot Revision: 1.20.002

Hardware Revision: 48

Serial Number: 30000102335

General

Operating Mode ○ Disabled ● Enabled

Network Parameters

MTU Size: 1500 bytes

Console

Gate Local Date: 10/Jul/2001

Gate Local Time: 10:47:56AM

Time Zone (GMT offset): 01:00

Baud Rate: 19200

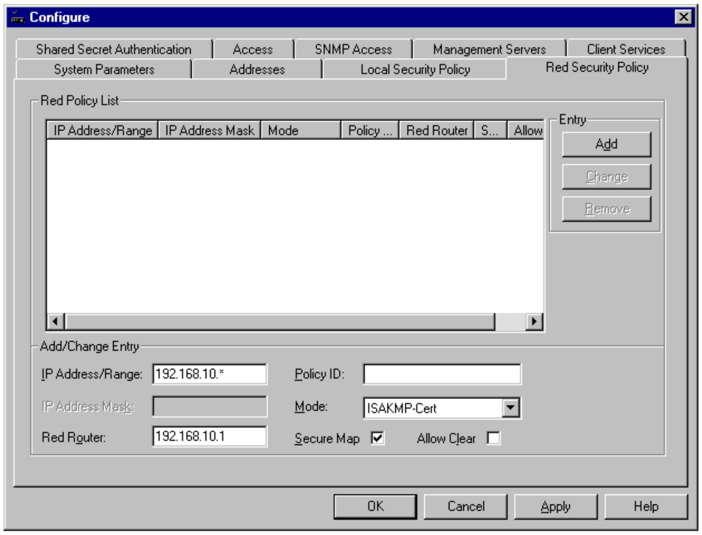
Console Idle Timeout: 5 minute(s)

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. Also make sure, that the gateways time, date and time zone matches the entrust authority and X.500. A difference of more than 59 minutes will fail the certification of the gateway

RED SECURITY POLICY

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

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



IP Address/Range: 192.168.10.*

Policy ID:

IP Address Mask:

Mode: ISAKMP-Cert

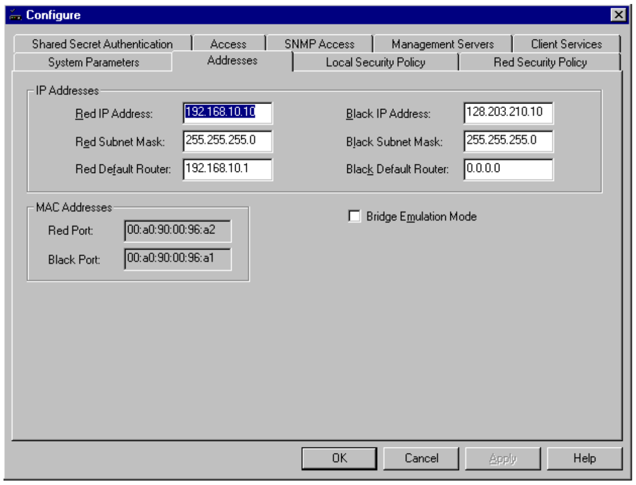
Red Router: 192.168.10.1

Secure Map ☑ Allow Clear ☐

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



Red IP Address: 192.168.10.10

Red Subnet Mask: 255.255.255.0

Red Default Router: 192.168.10.1

Black IP Address: 128.203.210.10

Black Subnet Mask: 255.255.255.0

Black Default Router: 0.0.0.0

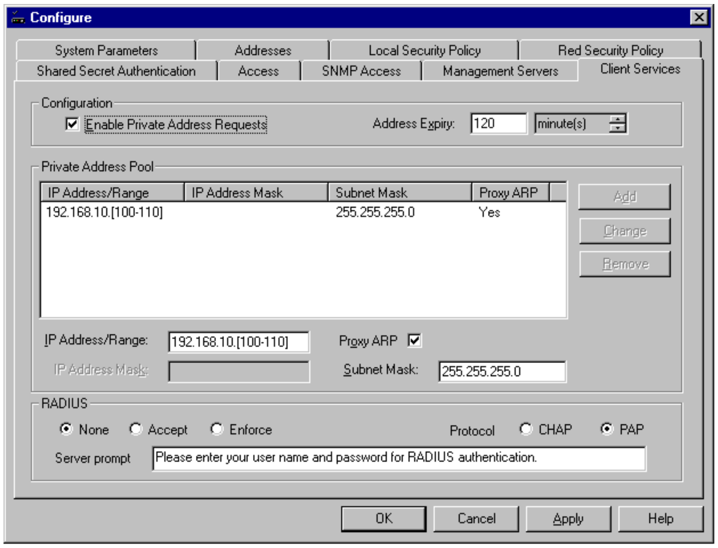
Red Port: 00:a0:90:00:96:a2

Black Port: 00:a0:90:00:96:a1

☐ Bridge Emulation Mode

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

It is possible to assign an IP address on the internal (red) LAN to remote connections once the connection has been authenticated. This is a Private Address Request. You enter a range or pool of address you wish to make available in the PAR pool.



Configuration

☑ Enable Private Address Requests

Address Expiry: 120 minute(s)

Private Address Pool

IP Address/Range	IP Address Mask	Subnet Mask	Proxy ARP
192.168.10.[100-110]		255.255.255.0	Yes

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

Proxy ARP ☑

IP Address Mask:

Subnet Mask: 255.255.255.0

RADIUS

● None ○ Accept ○ Enforce

Protocol ○ CHAP ● PAP

Server prompt: Please enter your user name and password for RADIUS authentication.

Click the ***Client Services*** tab
In the configuration frame, select the ***Enable Private Address Request*** checkbox

In the Private Address Pool frame, type the appropriate address range (**192.168.10.[100-100]**

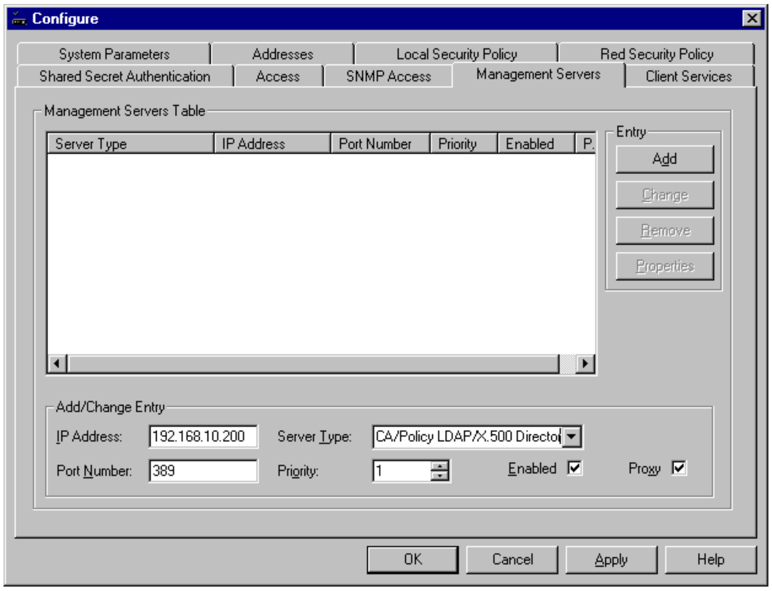
Select ***Proxy Arp*** check box

Type **255.255.255.0** in the ***Subnet Mask*** box

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

Click on **Apply**

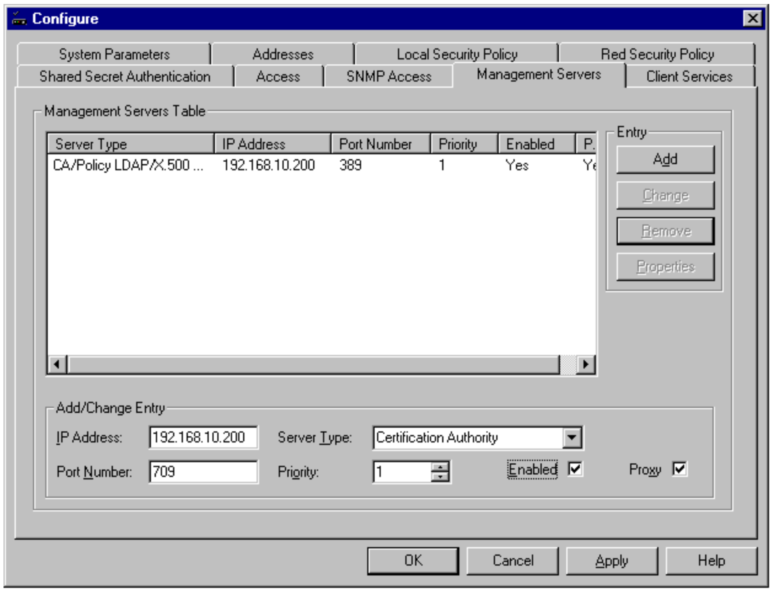
Add Management Server



Server Type	IP Address	Port Number	Priority	Enabled	P.

IP Address: 192.168.10.200 Server Type: CA/Policy LDAP/X.500 Directo
Port Number: 389 Priority: 1 Enabled ☑ Proxy ☑

Click on ***Management Servers*** tab
Type the IP Address of the desired server in the IP Address, **IP: 192.168.10.200**
Choose on ***Server Type*** : CA/POLICY LDAP/X.500 Directory
The Port number will be preset to the default value of 389
Make sure ***Enabled*** and ***Proxy*** Checkbox is set
Click on **Add**



Server Type	IP Address	Port Number	Priority	Enabled	P.
CA/Policy LDAP/X.500 ...	192.168.10.200	389	1	Yes	Ye

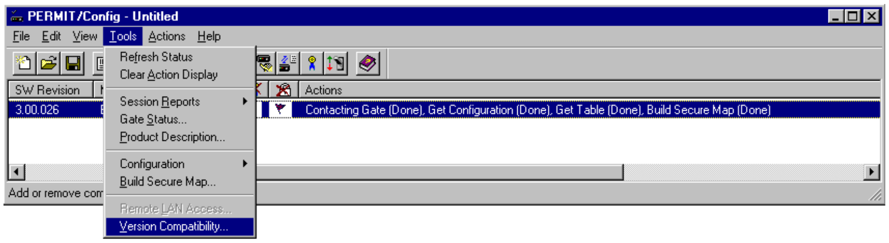
IP Address: 192.168.10.200 Server Type: Certification Authority
Port Number: 709 Priority: 1 Enabled ☑ Proxy ☑

This technical document has been created and evaluated by myself with the purpose to help friends to get into new technology and installations. There is no financial interest, however, please respect the copyright.

Now, choose another Server Type, which is Certification Authority
Also, the Port number will change to its default value of 709
Make sure Enabled and Proxy Checkbox is set
Click on **Add** and **Apply**

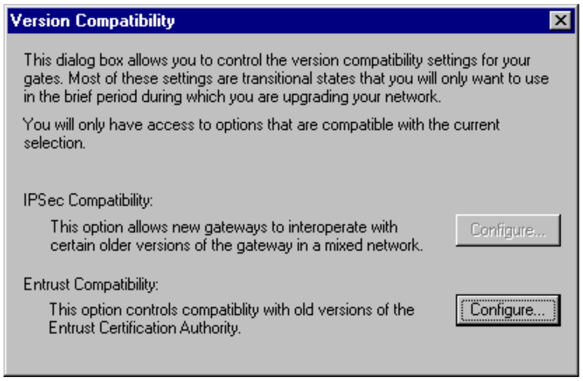
Next thing to do is to verify the used Version and maybe change to Version 4.

To do so, **click** on Tools ⇨ Version Compatibility



Contacting Gate (Done), Get Configuration (Done), Get Table (Done), Build Secure Map (Done)

Click on **Configure** Button of Entrust Compatibility



This dialog box allows you to control the version compatibility settings for your gates. Most of these settings are transitional states that you will only want to use in the brief period during which you are upgrading your network.

You will only have access to options that are compatible with the current selection.

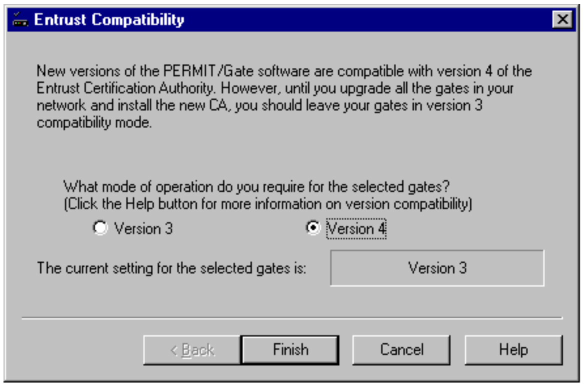
IPSec Compatibility:

This option allows new gateways to interoperate with certain older versions of the gateway in a mixed network.

Entrust Compatibility:

This option controls compatiblity with old versions of the Entrust Certification Authority.

You will see the current setting for the selected gates, which may show Version 3.



New versions of the PERMIT/Gate software are compatible with version 4 of the Entrust Certification Authority. However, until you upgrade all the gates in your network and install the new CA, you should leave your gates in version 3 compatibility mode.

What mode of operation do you require for the selected gates?
(Click the Help button for more information on version compatibility)

○ Version 3 ● Version 4

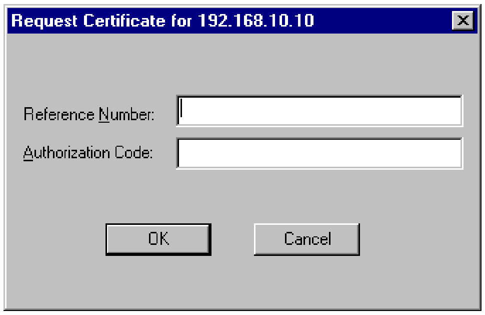
The current setting for the selected gates is: Version 3

To **change** the version, click on ***Version 4*** and click **Finish**

That’s pretty much everything to be set.

Now it time to get the gateway certified.

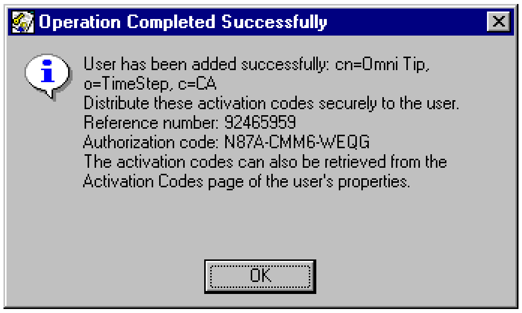
Go to Actions on the menu bar and click on **Recertify Now**



Request Certificate for 192.168.10.10

Reference Number:

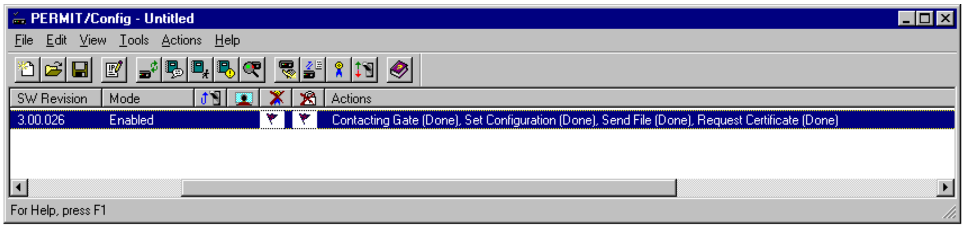
Authorization Code:



Operation Completed Successfully

User has been added successfully: cn=Omni Tip, o=TimeStep, c=CA
Distribute these activation codes securely to the user.
Reference number: 92465959
Authorization code: N87A-CMM6-WEQG
The activation codes can also be retrieved from the Activation Codes page of the user's properties.

The right picture shows the final confirmation, when creating a new user (in this case for the gateway itself) using Entrust Registration Authority. You should have written it down, or you still can go back to Entrust RA to verify the Reference Number and Authorization Code.

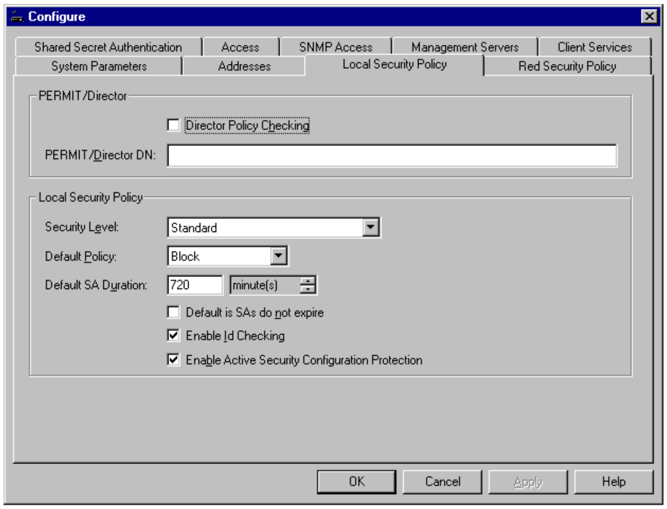


PERMIT/Config - Untitled

SW Revision	Mode	Actions
3.00.026	Enabled	Contacting Gate (Done), Set Configuration (Done), Send File (Done), Request Certificate (Done)

For Help, press F1

In the Configuration tab, click on Security Level and choose **STANDARD**



Configure

PERMIT/Director

□ Director Policy Checking

PERMIT/Director DN:

Local Security Policy

Security Level: Standard

Default Policy: Block

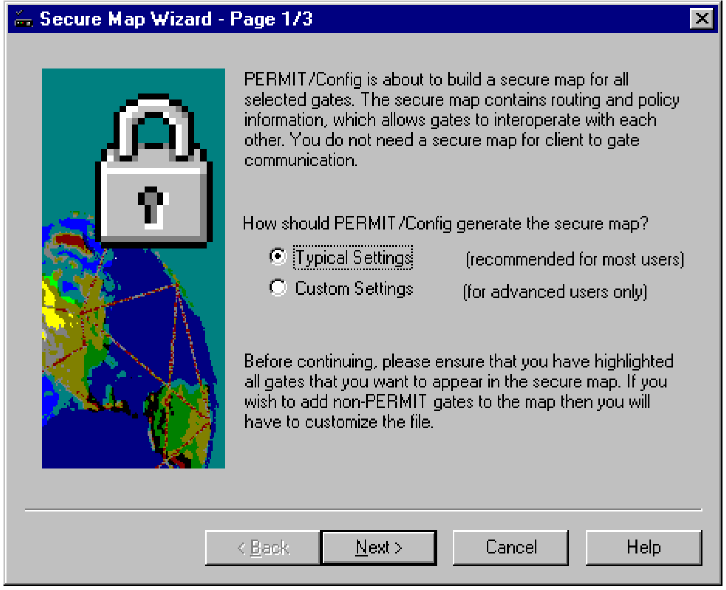
Default SA Duration: 720 minute(s)

□ Default is SAs do not expire

☑ Enable Id Checking

☑ Enable Active Security Configuration Protection

Don’t forget to build the secure map. To do so, **click** on ***Tools* ⇨ *Build Secure Map***.



Secure Map Wizard - Page 1/3

PERMIT/Config is about to build a secure map for all selected gates. The secure map contains routing and policy information, which allows gates to interoperate with each other. You do not need a secure map for client to gate communication.

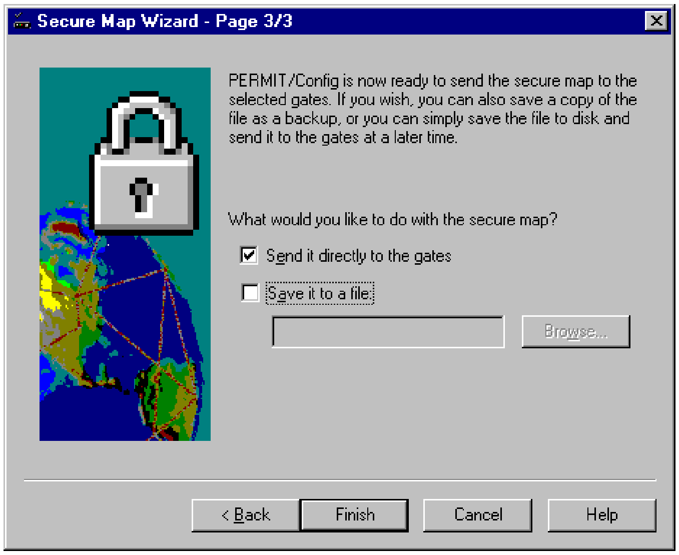
How should PERMIT/Config generate the secure map?

● Typical Settings (recommended for most users)

○ Custom Settings (for advanced users only)

Before continuing, please ensure that you have highlighted all gates that you want to appear in the secure map. If you wish to add non-PERMIT gates to the map then you will have to customize the file.

Send it directly to the gate.



Secure Map Wizard - Page 3/3

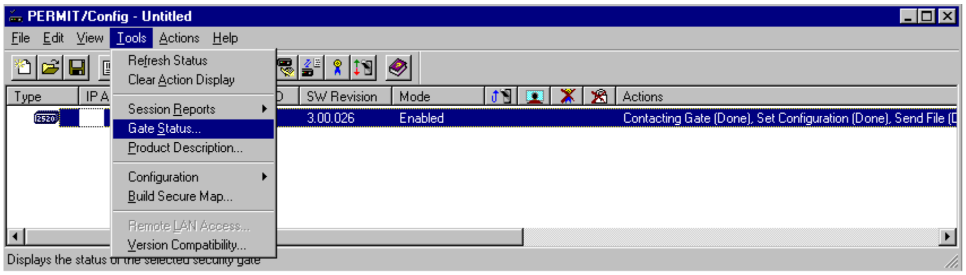
PERMIT/Config is now ready to send the secure map to the selected gates. If you wish, you can also save a copy of the file as a backup, or you can simply save the file to disk and send it to the gates at a later time.

What would you like to do with the secure map?

☑ Send it directly to the gates

☐ Save it to a file:

Finally, to verify everything is OK, click on Tools ⇨ Gate Status



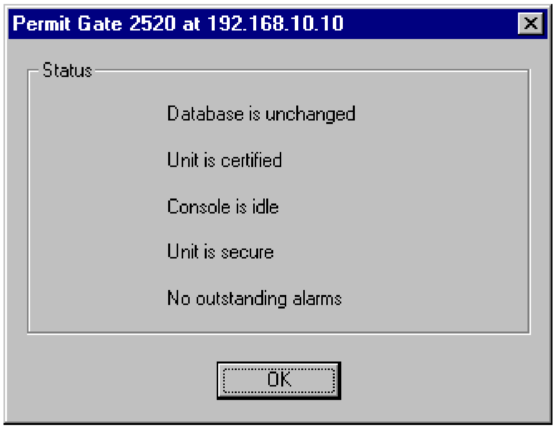
3.00.026 Enabled Contacting Gate (Done), Set Configuration (Done), Send File (D

Displays the status of the selected security gate

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

You should see:

- Unit is certified
- Unit is secure



Permit Gate 2520 at 192.168.10.10

Status

Database is unchanged

Unit is certified

Console is idle

Unit is secure

No outstanding alarms

OK

Enabling and Configuring Virtual Tunneling on Client using Certificates

Because I was using the Original Setup out of “Setup Scenario – Client/Gate using Shared Secret”, there some changes to be done manually, that would not have to be made when installing Certificate authentication directly. In the case you prefer to install Certificate authentication directly make sure you have entrust.ini copied

NOTE*: To enable Entrust authentication, you must obtain an entrust.ini file. The entrust.ini file points to the Entrust CA server and the X.500 server (which stores certificates), and lists the path to the directory containing the user’s Entrust profiles. PERMIT/Client creates this directory as part of the installation process, and when storing a newly created certificate. The Entrust/Manager software stores the entrust.ini file in the Entrust directory on the Entrust CA server.*

Disable PERMIT/Client in the tool tray

Create the folder **C:\Program Files\Entrust\Entrust Profile** (in accordance with the path indicated in the entrust.ini file

This folder will hold the .epf file containing the Entrust certificate for your Client when it is certified.

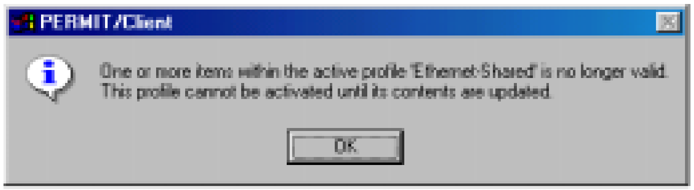
```
[Entrust Settings]
; the long timeout is needed for first time init with luna ca
ClientSocketTimeout=240
;Authority=192.168.10.200+829
Manager=128.203.210.10+709
Server=128.203.210.10+389
DefaultProfileLocation=c:\Program Files\Entrust\Entrust Profile
EncryptWith=Cast
ClientType=Heavy
MaximumCrossCertNodes=20
CrossCertCACacheSize=5
ArlCacheEnabled=1
CrossCertCRLCacheSize=8
CrossCertCACacheEnabled=1
CrossCertARLCacheSize=8
CrossCertDebug=0
CrlCacheEnabled=1
CertificateCacheEnabled=1
CertificateCacheSize=50
SearchBase=o=TimeStep,c=CA
SigningKey=RSA-1024
DefaultCredentials_time_req=43200
DefaultContext_time_req=3600
ProgDir=
InstallDir=
CA Distinguished Name=o=TimeStep,c=CA
```

The Manager's and Server's IP Address should point to the black side of the gate, as the gate acts as proxy. Also, Create a new folder, where you will store the certificate CRL's. This is stated on "***Default ProfileLocation***"

Once done with it, I recommend doing a reboot of your workstation in order the entrust.ini has been read. Also, your client window may look different, or you may even get an error, that you have to create a profile first, before you can use PERMIT/Client

At the end of the reboot, login to Windows

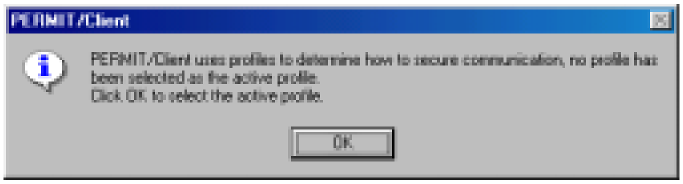
The following warning may appears



PERMIT/Client

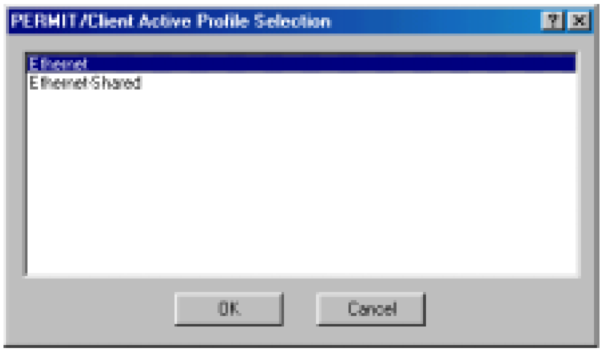
One or more items within the active profile 'Ethernet-Shared' is no longer valid.
This profile cannot be activated until its contents are updated.

Click **OK -** A second warning appears

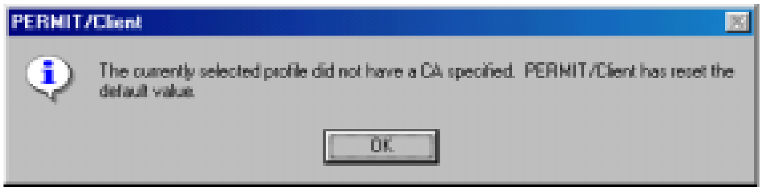


PERMIT/Client uses profiles to determine how to secure communication, no profile has been selected as the active profile.
Click OK to select the active profile.

Click **OK**
If you worked with PERMIT/Client before, you may have the possibility to choose an Active Profile

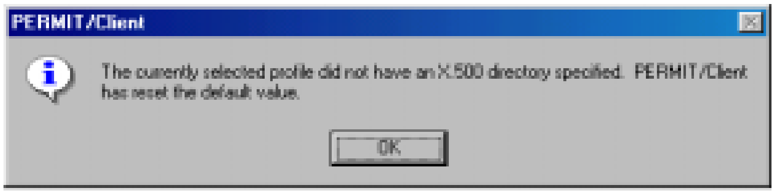


Select the ***Ethernet-Shared*** profile and click **OK**



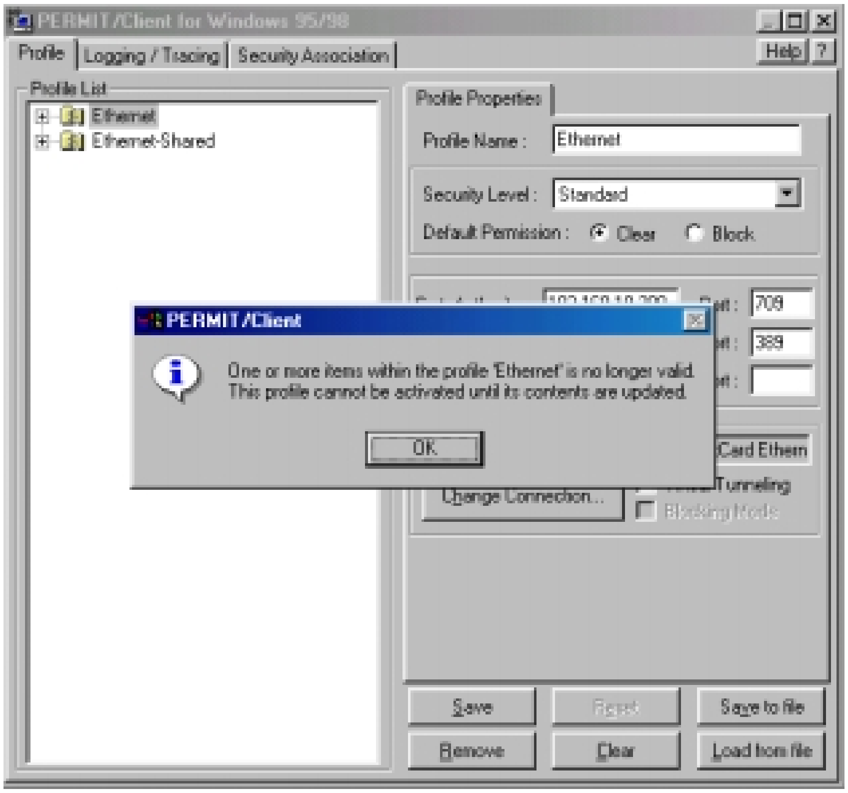
The currently selected profile did not have a CA specified. PERMIT/Client has reset the default value.

Click **OK** to confirm use of default CA



The currently selected profile did not have an X.500 directory specified. PERMIT/Client has reset the default value.

Click **OK** to confirm use of default x.500
NOTE*: This may have to be done twice*



Profile Name : Ethernet

Security Level : Standard

Default Permission : ● Clear ○ Block

Port : 709

Port : 389

Port :

PERMIT /Client

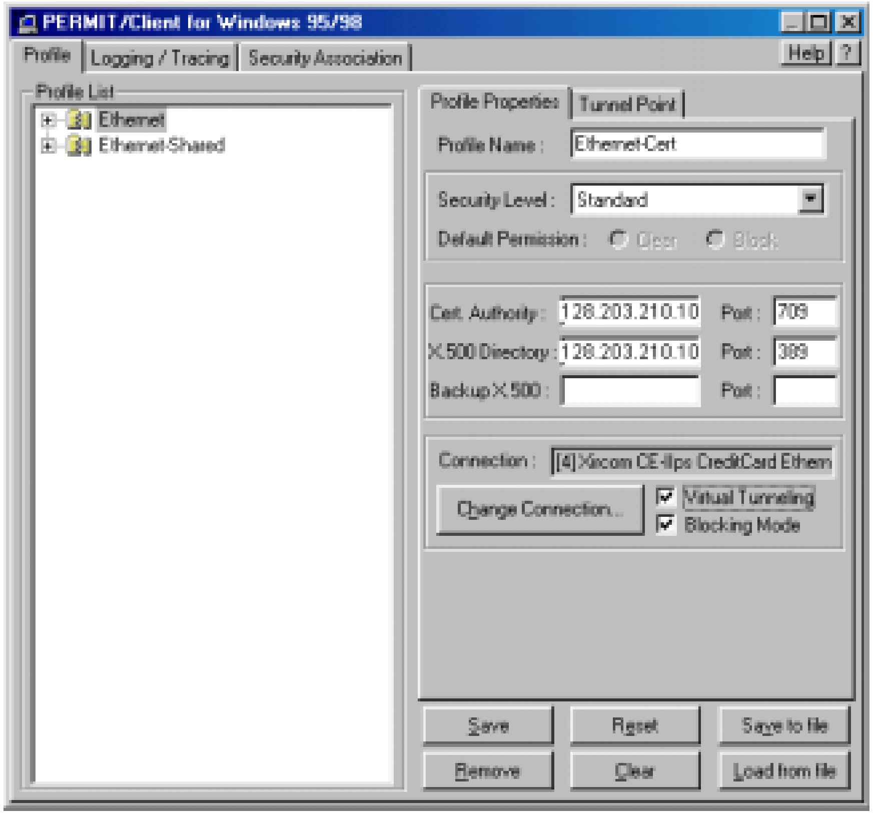
One or more items within the profile 'Ethernet' is no longer valid.
This profile cannot be activated until its contents are updated.

OK

The Profile warning box reappears

Click **OK**

Observe the “broken” profile icon indication the change to certificate mode as well as the additional information in the Profile Properties sub tab. The Unique Identifier frame has been replaced by the display of the IP Address andPort assignment of the CA and the X.500 Directory



Profile Name : Ethernet-Cert

Security Level : Standard

Default Permission : ○ Clear ○ Block

Cert. Authority : 128.203.210.10 Port : 709

X.500 Directory : 128.203.210.10 Port : 389

Backup X.500 : Port :

Connection : [4] Xircom CE-IIps CreditCard Ethern

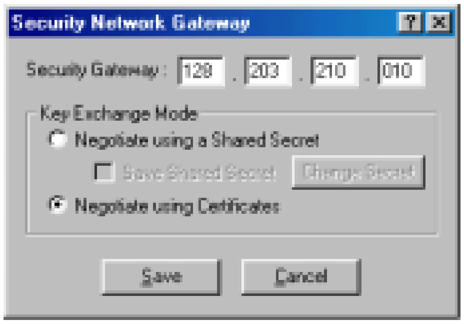
☑ Virtual Tunneling

☑ Blocking Mode

Change the profile name to Ethernet-Cert.
Note: The Certificate Authority should be
Ensure the Virtual Tunneling check box is selected

Click the Tunnel Point tab

Double click the entry in the Security Gateway box and confirm Security Gateway IP matches the Black ip of your Gate



Security Gateway : 128 . 203 . 210 . 010

Key Exchange Mode

○ Negotiate using a Shared Secret

□ Save Shared Secret Change Secret

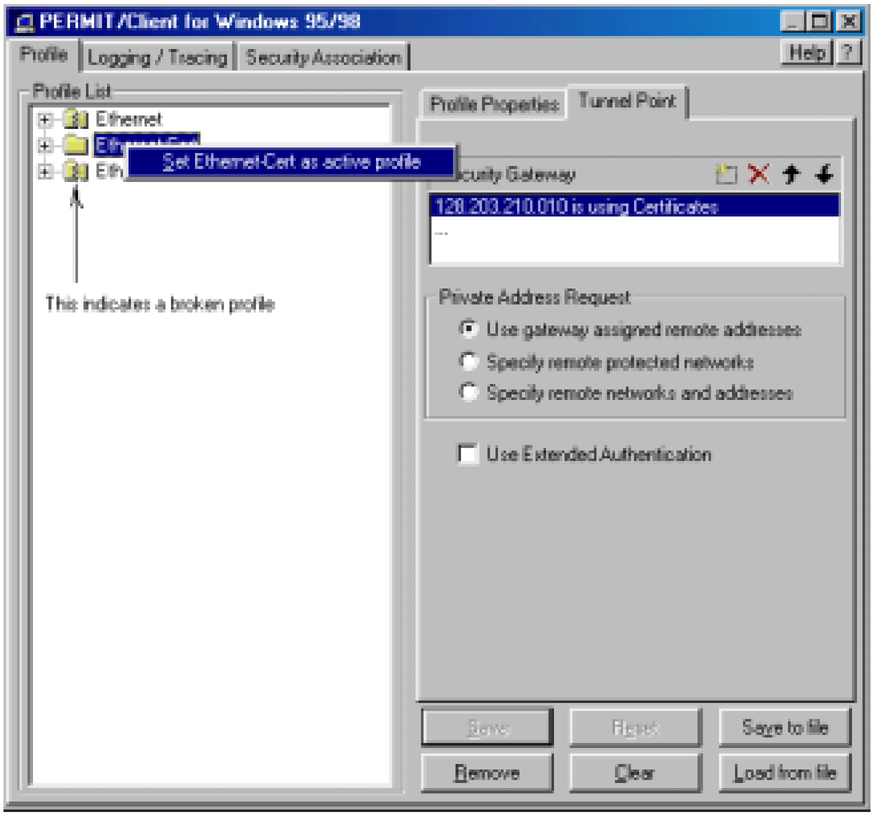
● Negotiate using Certificates

In the Key Exchange Mode frame, select Negotiate using Certificates

Click SAVE

Click SAVE TO FILE and give the profile a name of your choice (you may want to copy this profile to diskette)

Right click the Ethernet-Cert profile in the Profile List and activate this new profile



This indicates a broken profile

128.203.210.010 is using Certificates

Private Address Request

● Use gateway assigned remote addresses

○ Specify remote protected networks

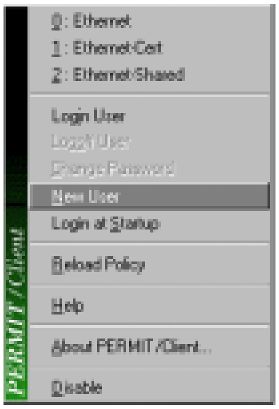
○ Specify remote networks and addresses

□ Use Extended Authentication

Close the client profile window

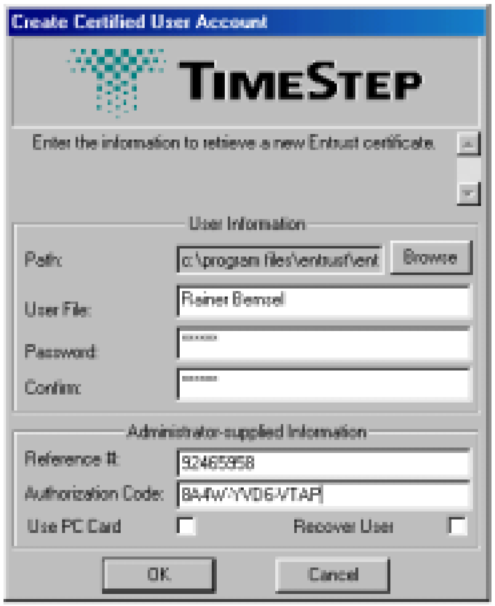
Re-enable the Client

Right click the TimeStep "T" in the tool tray



Click New User

The Certified User Account window appears



Create Certified User Account

Enter the information to retrieve a new Entrust certificate.

User Information

Path: c:\program files\entrust\ent

User File: Rainer Bemsel

Password: ******

Confirm: ******

Administrator-supplied Information

Reference #: 92465958

Authorization Code: 8A4W-YVD6-VTAP

Use PC Card □

Recover User □

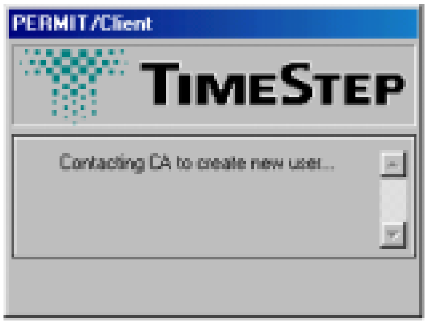
In the User File box, type a name of your choice

This will be the file that contains your Entrust profile. The extension epf will automatically be added to the filename you type.

Type and confirm TimeStep1 as the password

Type the Reference Number and Authorization Code you recorded for your Client 1

Click OK



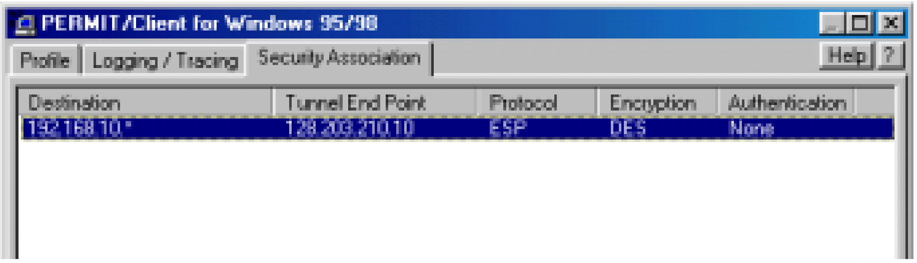
PERMIT/Client

Contacting CA to create new user...

Watch the Console screen if it is available for messages as the Certification process is completed

Wait for the desktop to reappear and for the TimeStep “T” in the tool tray to turn green with a black border indicating certificate authentication with a virtual tunnel

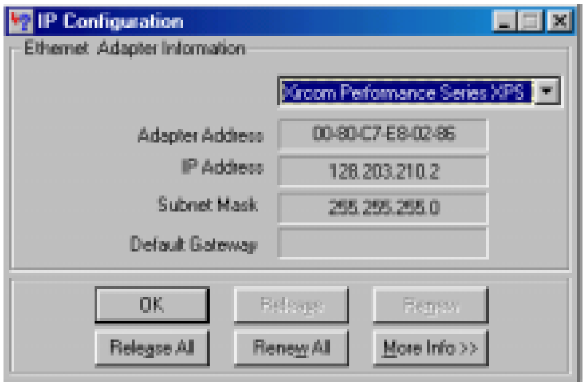
When the new use has been created, it will setup a Security Association, which can be verified by double-clicking the **"T"** and than click on Security Association tab.



Destination	Tunnel End Point	Protocol	Encryption	Authentication
192.168.10.*	128.203.210.10	ESP	DES	None

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

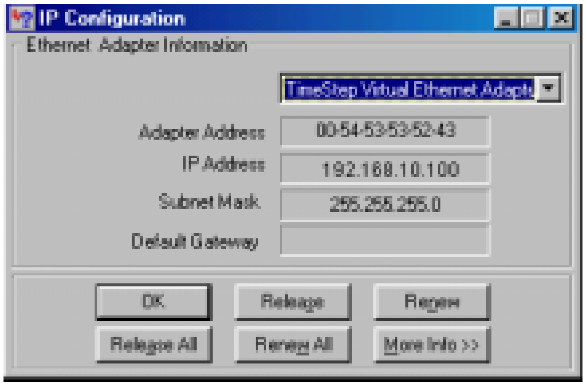
Run Winipcfg (or ipconfig) and check the adapter list. First, you will see the active Network Interface associated with an IP address out of the black range. My client is using ***128.203.210.2***, while there's another Adapter, which is interesting.



Xircom Performance Series XPS

Adapter Address: 00-80-C7-E8-02-86
IP Address: 128.203.210.2
Subnet Mask: 255.255.255.0
Default Gateway:

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



TimeStep Virtual Ethernet Adapt

Adapter Address: 00-54-53-53-52-43
IP Address: 192.168.10.100
Subnet Mask: 255.255.255.0
Default Gateway:

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.