System Administrators Guide

@TheOffice

1.54

15 May 2003

http://@theoffice.trispen.com

@TheOffice

On-The-Road, away from the office.
This does not have to mean no connection.

@TheOffice provides secure connectivity to the office so it is as if you never left – with regard to connectivity that is. You, on the other hand, are out of the Office.

@TheOffice consists of a Server and Client Software component.

- **@TheOffice Gateway**: this component is installed in the office to which access is required and
- **@TheOffice Client**: this component is installed on the roaming user's PC (typically a notebook computer)

@TheOffice Gateway
The set-up of the gateway is a simple matter requiring only a few parameters to be set.

The users of @TheOffice are administered as part of your Windows Domain or local domain and the Administrator can restrict access to a specific group of users, if required. The Administrator is able to monitor who is connected.
User registration is done based on the user's Windows UserID and password. Once set up, the user can enrol from any PC which has the Client software installed.

@TheOffice Client
On the client side two steps are followed before connecting to the gateway.

- The client is installed on the roaming user's PC.
- The next step is to follow a simple process to enrol the user onto the Gateway.

After enrolment, the user uses the connect dialog to connect to the office network.

While the user is connected, all traffic from the Internet is automatically restricted and only communication with the office network is allowed. This dynamic firewalling feature assures that the user cannot inadvertently become a "router" between the office network and the Internet.
From a user perspective, a simple connect login is all that is required to connect securely to the office. For convenience, the user can also select a dial-up profile to be automatically dialled before connecting to the office.

@TheOffice is extremely simple to use and provides a secure method for getting access to office network resources from anywhere on the Internet.

Access the office anytime, anywhere

Contents

Getting Started

Introduction

As a system administrator, you must have had countless requests from users wanting to access your office resources over the Internet. With the @TheOffice product, not only is it possible to do so without fuss, but you can also rest assured that the increased access is protected by state of the art cryptographic security, ensuring that you do not expose your users and office network to the threats associated with opening the network to the Internet.

@TheOffice consists of two main components.

- The first, @TheOffice Gateway, is installed in your office network to provide a secure access point for network communication between the clients and the office network.
- The Client Software is installed on all user PC's that require secure access to the office network.

@TheOffice authenticates users before allowing access to the office network. This process uses a set of rigorous mathematical algorithms that relies on the secrecy of a user's private key. This private key is stored in a secure profile on the user PC. Only the user needs to know the pass-phrase that protects the user's private key.

Your duties as system administrator will include the management of the users. Fortunately, @TheOffice makes this extremely easy by linking the enrolment and user management tightly with the user management already provided by Microsoft Windows.

This Administration Guide will assist you in preparing for installation, installing the software, configuring your gateway and network access of your firewall, and enable you to assist users with setting up client software and enroling to gain secure access to the corporate network.

System Requirements

Before you install your @TheOffice Gateway and client software, you will have to make sure that the office network environment is suitable. Below is a checklist of requirements for installation of the products.

Hardware

Gateway:

Minimum specification required for operating system and minimum configuration of Pentium III, 128MB RAM, 100MB free HDD space or better. Ethernet card and permanent Internet connection.

Client:

Minimum specification required for operating system and minimum configuration of Pentium, 32MB RAM, 10MB free HDD space or better. Internet connection (WiFi, Cable, ADSL, Satellite, modem, etc.)

Operating System

Before continuing, check that your Operating System is supported:

Operating System	Service Pack	Client supported	Gateway supported
Windows 95	-	No	No
Windows 98	All	Yes	No
Windows ME	-	Yes	No
Windows NT 3.5x	-	No	No
Windows NT 4.x	1, 2, 3	No	No
Windows NT 4.x	4,5,6	Yes	No
Windows 2000	1, 3	Yes	Yes
Windows 2000	2*	Yes	Yes
Windows XP	All	Yes	Yes

* Requires Microsoft Patch: Q301337_W2k_SP3_x86_en.exe
(refer to http://@theoffice.trispen.com for the latest information)

Windows Installer

You can check your current installer version by right-clicking on msiexec.exe and selecting 'properties'. This file can be found in your System Directory, i.e. \WINNT\System32 on NT/2000 or \Windows\System32 on XP or \Windows\System on 9x/ME.

Operating System	Service Pack	Windows Installer required
Windows 95	-	n/a
Windows 98	All	1.20.1827.0 or newer**
Windows ME	-	1.20.1827.0 or newer**
Windows NT 3.5x	-	n/a
Windows NT 4.x	1, 2, 3	n/a
Windows NT 4.x	4, 5, 6	1.20.1827.0 or newer**
Windows 2000	1, 3	Already OK
Windows 2000	2*	Already OK
Windows XP	All	Already OK

* Requires Microsoft Patch: Q301337_W2k_SP3_x86_en.exe
**Download and install newer version if not conforming to requirement (refer to http://@theoffice.trispen.com for the latest information)

Office network requirements

@TheOffice extends the Office LAN to your @TheOffice Clients. The office network where you are going to install the Gateway needs to conform to the following specifications:

- Permanent connection to the Internet must be set up.
- The Gateway PC must be configured on the network.
- Registration to a Domain is optional for user management but if you want to use a domain controller to authenticate users, the Gateway PC must be registered on the Domain.
- It is not necessary for any specific user to be logged in on the gateway.

Firewall Compatibility

The typical @TheOffice Gateway installation is located on the private network portion of your corporate LAN. In order for client users to communicate with the Gateway, it may be necessary to configure the rules on your firewall to allow this access to take place. The Firewall settings section details the required configuration.

The firewall must be able to support filtering of UDP port 500 and should allow UDP fragments through the gateway.

In principle, most firewalls should support the required settings. The @TheOffice Gateway and client were tested with the following Internet firewalls:

Checkpoint Firewall 1	FreeBSD IPFW and OpenBSD ipf
Cisco PIX	Linux IPChains firewall
Cisco IOS firewall	NetSeq Secure Platform

Planning the installation

@TheOffice Gateway has been designed for use in most office LAN environments. Figure 1 shows a typical installation. In this figure, the @TheOffice gateway is installed on the office LAN, and is dedicated for secure remote access purposes.

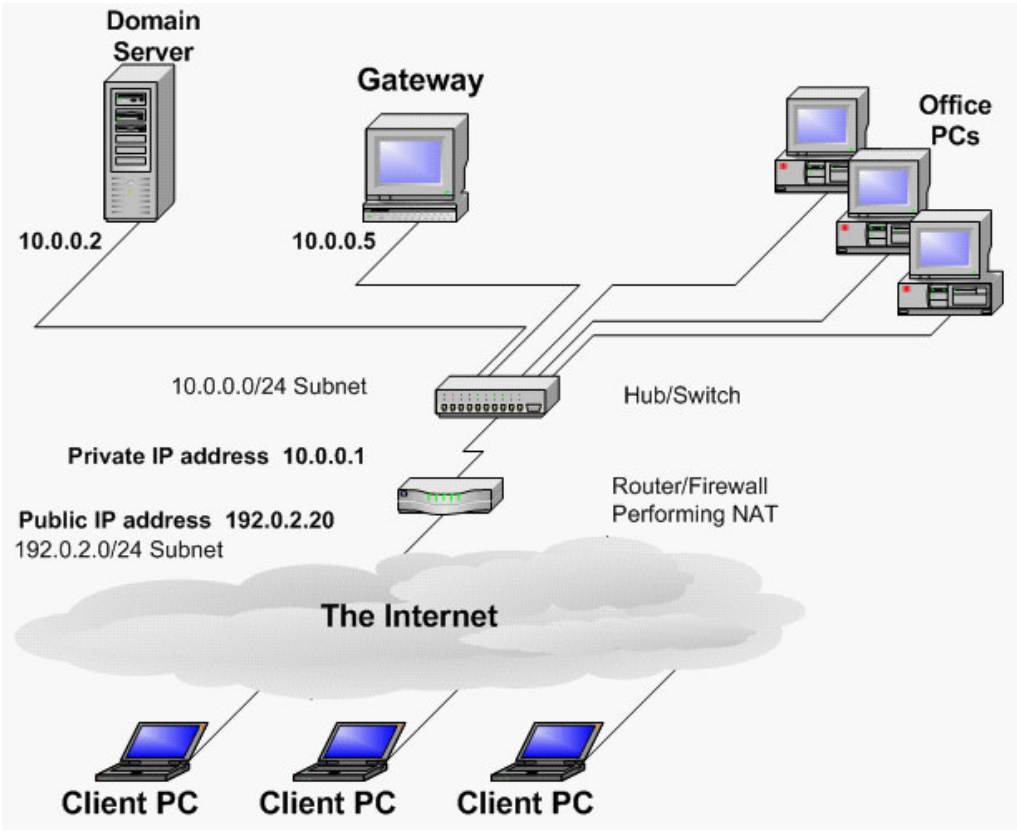

Figure 1: Typical Office network with Dedicated @TheOffice Gateway installation

In smaller offices, the @TheOffice Gateway could be installed on the office server itself, reducing the need for an additional hardware platform. This is only recommended in cases where the office server is under-utilised as encryption places a processing overhead on the server. For installations where more than 10 office users are connecting to the office server, a dedicated PC is recommended.

The Firewall settings should be checked and configured as described in the Firewall settings section.

NOTE: In order for your @TheOffice Gateway to be able to query the domain controller, the Gateway PC must be registered on the domain. It is also important to verify that the domain controller has the group "Pre-Windows 2000 compatible access", and that either the user "Everyone" or the Gateway PC is a member of the group.

The Gateway

Securing the Gateway

Security includes physical access and software access security.

Physical access should be managed carefully as the Gateway is used as an access point to the internal network.

Software access will come into play when the physical access has been breached or those with legal physical access abuse the system. The user access to the Gateway should be limited to the minimum set of users. If the Gateway is used for nothing else then access should be limited to administrators only.

Installing the Software

You need to be logged in as a user with administrator rights to install the software. To start the installation process, simply double-click on the installation executable. The installation process is simple and requires little interaction, simply follow the prompts. Once installed the PC requires a reboot to start up the gateway services.

Gateway Date and Time

The Certificates used in the connection process use time as a reference for their validity. It is important that both client and gateway PCs have the correct time and time zone set-up. The maximum time discrepancy is set at 30 minutes. If the discrepancy is larger an error will be displayed.

Configuration

To start the Gateway Configuration Console select

Start
Programs
@TheOffice Gateway
Gateway Management User Interface

from the Start Menu.

The first step in the configuration is to provide information about the installation. Click on the Configuration button:

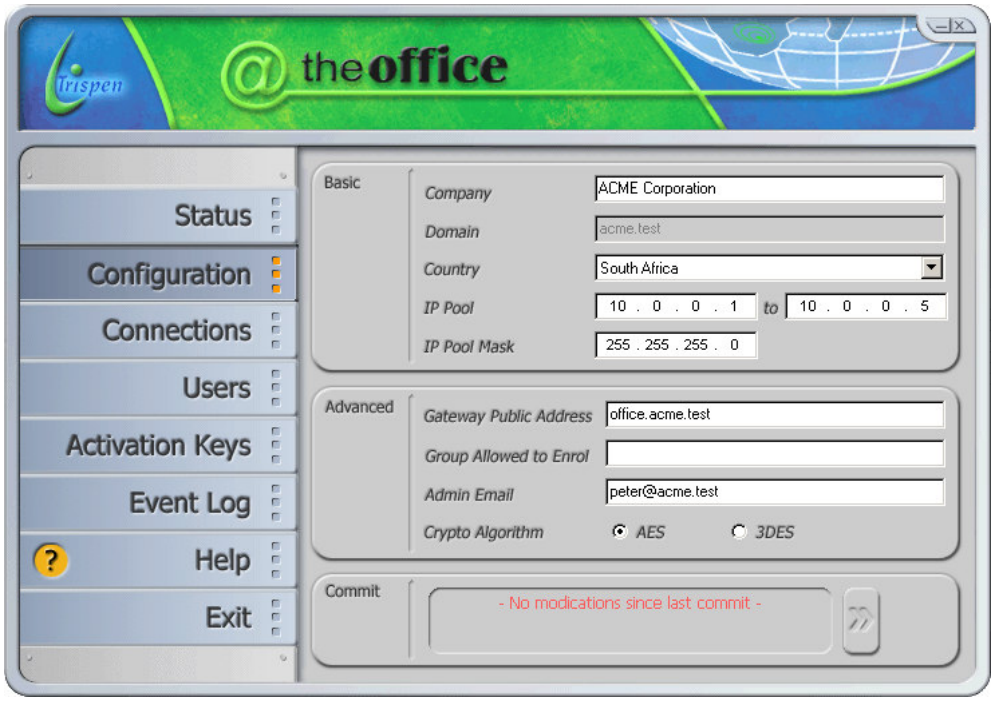

Figure 2: @TheOffice Gateway configuration

Basic Configuration

The Configuration screen initially contains default values. In many cases, you can use the default values. The fields should be filled in as follows:

1. **Company:** The name of your company. @TheOffice uses the company name that is recorded as the licensed owner of the workstation. It can be changed to reflect the correct name of the organisation.

   NOTE: Changing the Company name will re-generate your Root Certificate and invalidate all of your enrolled users! Users will then have to enrol again. If the Company name is changed back to the original Company the users will be re-instated.

2. **Domain:** The domain in which this PC resides. @TheOffice uses this Windows domain to identify users when they enrol for remote access and connect. This information is retrieved automatically.
3. **Country:** Choose the country in which you are located. This value will be used in the generation of your gateway certificate.

   NOTE: Changing the Country will re-generate your Root Certificate and invalidate all of your enrolled users! Users will then have to enrol again. If the Country is changed back to the original Country the users will be re-instated.

4. **IP Pool:** The IP pool is the range of IP addresses that will be issued dynamically when users connect to your office network. The range must be sufficient to cover the number of users expected to connect. You must choose a range of addresses that you are certain is not in use in the network. The range must preferably be from the same subnet as the office network you are accessing.
5. **IP Pool mask:** This is the address mask that will be given to client PCs when they connect to the office. The setting you select here should fit in with your office network's IP addressing design.

6. **Commit:** The Commit button will record all of the settings you have selected and prepare the Gateway for operation. The status message will indicate the success or failure of the commit with appropriate error messages on failure.

Advanced Configuration

This section allows the administrator to fine tune the gateway to meet specific requirements.

1. **Gateway Public Address:** Enter the IP address or DNS name of the public address where users will connect to the Gateway. If your gateway is located behind a NAT device, enter the static NAT address you have mapped for this gateway or a DNS name that resolves to the static NAT address.
2. **Group allowed to enrol:** You can restrict your remote access to a specific group of domain users or a group of local users. This is handy if you are part of a large domain and you would like to control access to one department (or to a group of users that you create especially for remote access). If the gateway resides in a domain the default is domain users, which includes all the users registered in the domain. If the gateway does not reside in a domain the default is users registered on the gateway itself. Should you wish to restrict access to a group of local users when the gateway resides in a domain, use LOCAL\{group name}. Using LOCAL\ will give access to all users registered on the local machine.

   Domain specified

   Empty = Default of "Domain Users"

   "LOCAL\<group>" = use local <group>

   "LOCAL\" = use local "Users" group

   "<group>" = use specified <group> on domain

   Domain not specified (i.e. not in a domain)

   Empty = default of local "Users" group

   "LOCAL\<group>" = use local <group>

   "LOCAL\" = use local "Users" group

   "<group>" = use local <group>
3. **Admin Email:** Enter the email address to be used as the contact email address in the Welcome Memo as described in Gateway Status section. This email address is also used during the 'Refresh expiry dates" process when the license is updated.
4. **Crypto Algorithm:** Select the desired crypto algorithm.
5. **Commit:** The Commit button will record all of the settings you have selected and prepare the Gateway for operation. The status message will indicate the success or failure of the commit with appropriate error messages on failure.

What to do next

Now that you have configured your gateway, you should test the operation of the gateway.

If you have not yet set-up the Firewall refer to the Firewall settings section and ensure that the correct connectivity is available to the gateway..

To test whether the gateway is 'visible' from the Internet, you can make use of a test tool which checks if the gateway is visible from the Internet. It can be found at http://www.@theoffice.trispen.com/atTheOffice/gw_test.htm.

To test whether enrolment is possible, you should install the client on a test PC and enrol to the gateway. Refer to the Client section for help on this.

NOTE: If you are connecting to the gateway from the office network where the gateway is installed, you should be able to enrol but you will not be able to connect to the gateway. To connect to the gateway, you have to be 'away' from the office; in other words you need to connect from another network such as the Internet.

To ensure that the gateway can complete the refresh license process when activation keys are added or updated perform the "Refresh expiry dates" process as described in 'Registering activation keys' section.

If you have any problems at this point, consult with the Frequently Asked Questions section

Managing the Gateway

Gateway Status

The status screen (Figure 3) displays important information about @TheOffice Gateway.

Figure 3: Status screen

1. **Connected users:** This displays the number of users that are currently connected to the gateway. For detail about who is connected, you can view the Connections screen.
2. **Active users:** This displays the total number of users that are currently enrolled to access your LAN securely. To view details on the enrolled users, you can view the Users screen.
3. **Allowed users:** This shows the number of users you are licensed for. Refer to Obtaining activation keys section if more users are required to connect to the gateway.
4. **System events:** Important system events are displayed in this window.
5. **Verification Matrix:** This matrix is a fingerprint of your gateway. To ensure that users enrol to the correct gateway, they are presented with this matrix on enrolment. You need to provide the matrix to your users, and they are then required to enter two of the cells when they enrol. The Welcome Memo, described in the Gateway Status section, includes the matrix.
6. **Generate Welcome Memo:** To make life easier for you as a system administrator, you can generate a welcome document that contains the verification matrix and gateway details. Click on the >> button to edit the Welcome Memo. You may customise the wording of the document and save your changes. Support and administration contact details should be included in the document.

Connections

The Connections screen displays the currently active connections. These are users that are currently securely connected to the office network.

Each connected user is listed with their virtual IP Address and time online. Further statistics are displayed on the right hand pane when a user is selected.

Each connection and disconnection is also logged in the event log.

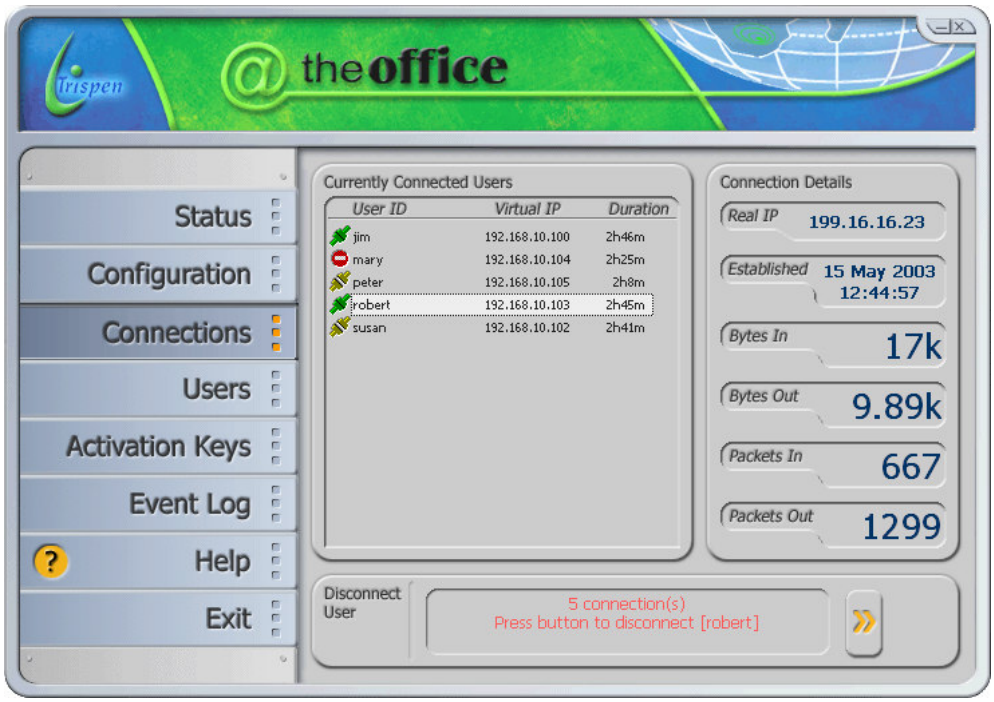

Figure 4: Viewing connections

To disconnect a user, you can click on the user and press >> to execute the function. This will immediately terminate the user session. The user status, shown as disconnected, will remain on the list for 3 minutes.

The time of disconnection may be viewed by selecting the user and viewing the message in the "Disconnect User" box.

NOTE: Be aware that this might cause data loss for the user who is disconnected, as the applications in use might not be able to recover from a sudden network disconnection. This action is equivalent to unplugging the network cable connecting the user to the office network.

Users

You can use the “Users” menu to manage attributes related to @TheOffice users.

Users are automatically verified against the domain group specified in the configuration step above. You will only see a user in this menu once the user has enrolled.

Once a user is registered, you can change the attributes or policies relating to that user in this menu. Figure 5 below depicts the User management screen.

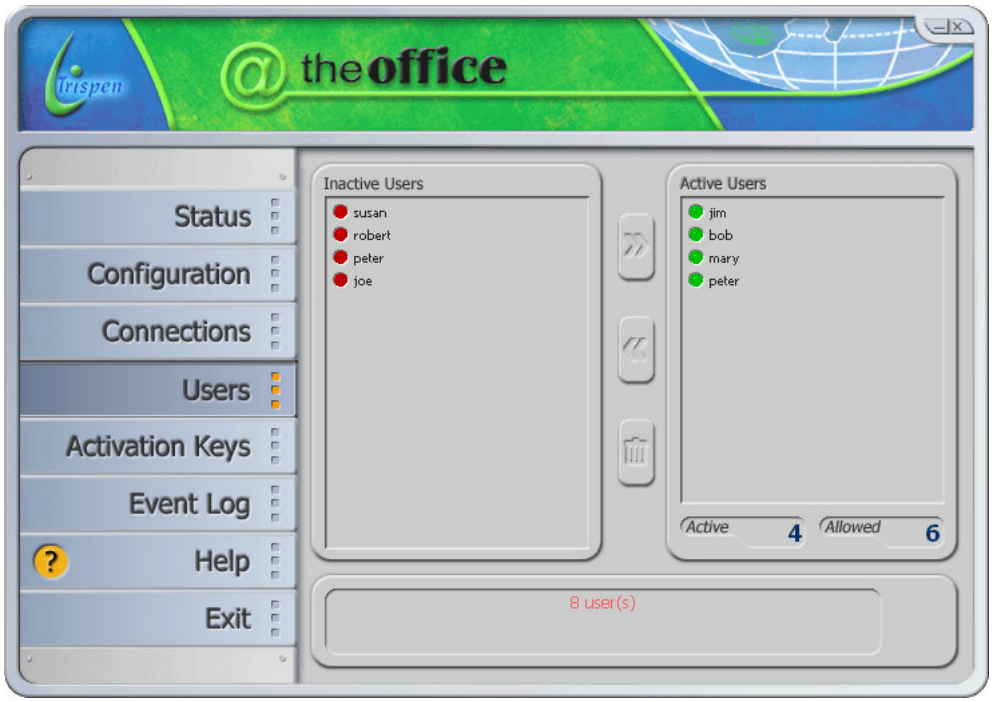

Figure 5: User Management

Description of the fields on this screen:

Inactive Users

Users are listed here:

- after they have successfully enrolled and the active list has reached the limit of the gateway license noted in the allowed box; or
- they have been deactivated by the administrator.

Active Users

An active user is one that has enrolled, is licensed and currently authorised to connect to your office network.

Allowed Users

The number of allowed users displayed is the total number of currently licensed users. The Active user list will never have more than the number of allowed users.

Changing users status (active/inactive)

Users can be moved between active and inactive states subject to the limits of the allowed number of active users in the active column. The user is selected and the >> and. << buttons are used to move the user to the other state. Should the user be in the active column and connected deactivating the user will also disconnect the user.

NOTE: Be aware that this might cause data loss for the user who is disconnected, as the applications in use might not be able to recover from a sudden network disconnection.

Deleting a User

A user is deleted by selecting the user and clicking on the bin button to complete delete process. Should the user be connected the disconnection process will be performed before deleting the user. This process is permanent and the user must re-enrol if access to the gateway is required.

Activation Keys

The @TheOffice license model allows organizations flexibility in purchasing only the required number of usage licenses for users of the secure remote access service.

Usage is enabled by means of activation keys. You will receive these keys when you pay for the service. These activation keys are also called tokens.

The keys are managed using the **"Activation Keys"** menu option.

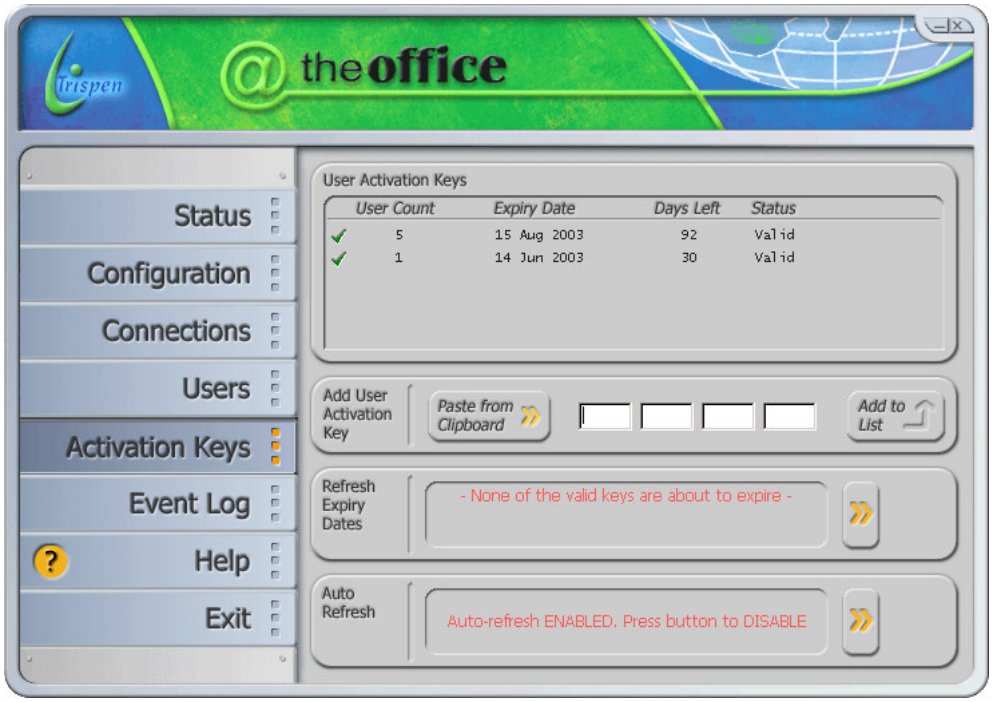

Figure 6: Management of Activation Keys

Obtaining activation keys

To add additional users or extend the usage of existing users, you will have to purchase additional user licenses. You can order additional user licenses online and the activation keys will be delivered to you electronically. Connect to http://@theoffice.trispen.com and purchase additional usage keys.

Registering activation keys

An activation key looks something like this:

abdc-2hij-oafd-2jds

On receipt, the simplest method to activate your users is

1. Open the activation keys menu page
2. Select the activation key in the email or web page you have received
3. Press **Ctrl-C** or **Edit > Copy** from the menu bar in your mail application.
4. Click on the Paste From Clipboard button to transfer the activation key you have copied in step 3.
5. Click on the "Add user activation Key" button to add the key to the list of keys that will be registered.
6. Add all activation keys you have received by repeating these steps (in case there are more than one)
7. Now click on the button in the "Refresh expiry dates" panel to update your license.
8. Wait for the request to finish and the view the status message

---

NOTE 1: you have 5 minutes to perform the "Refresh expiry dates" function before the new key is removed from the list. Should this happen the activation key should be re-entered and the license updated using the "Refresh expiry dates" function.

NOTE 2: the user currently logged into the computer hosting the gateway requires access to the Internet so that the expiry dates can be refreshed at the licensing server. The http proxy settings for Internet Explorer will be used if available.

What happens when activation keys expire

If an activation key expires, the number of active users will be reduced automatically by the amount of users provided by the key. The gateway will automatically determine which users to de-activate, based on least frequently used status. To change the user selection, use the Users menu option and rearrange the users that are currently active / inactive to meet your requirements. Of course you can also purchase additional activation keys to increase the number of active users.

The expired activation keys will be automatically deleted soon after the expiry date.

Auto refresh of Activation keys

This option, when enabled, relieves the administrator of having to manually refresh the activation keys. This function is triggered when an activation key is 6 days from expiry and performs a "Refresh expiry dates" action regularly until the activation key in question is either updated or has expired.

Event Log

Event logs are useful in the event that something does not work as expected and to keep a trace of events for audit purposes.

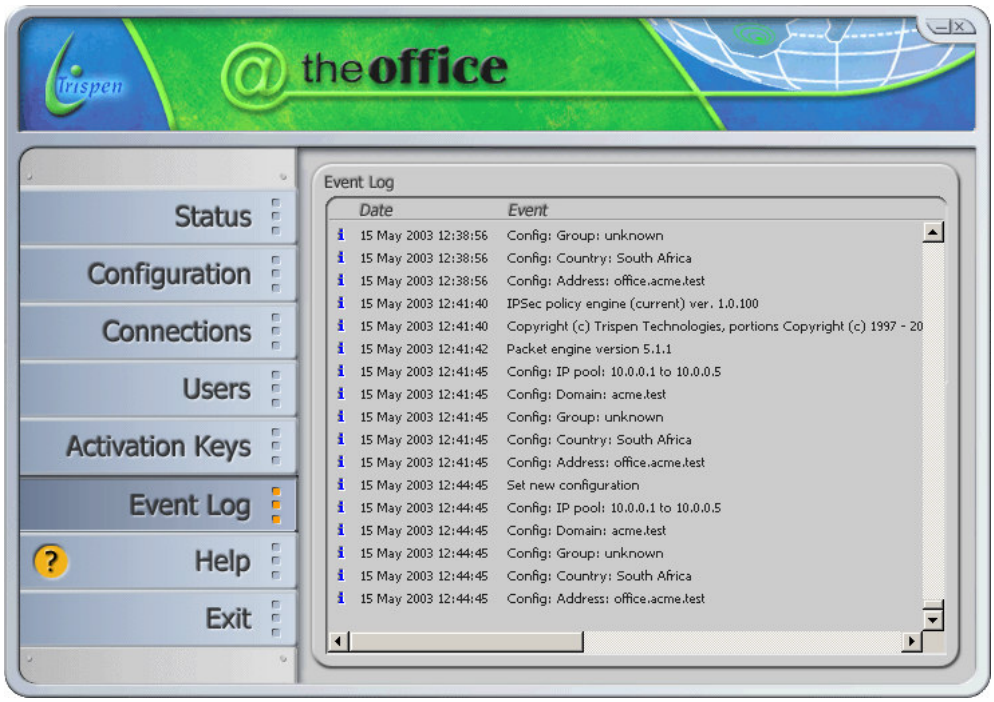

Figure 7: Event log screen

Exit

The Exit menu option closes the gateway console. It is not required to keep the console active for successful operation of the gateway. The service component of @TheOffice Gateway will remain active even when the console is not running.

The Client

Installation

The installation process is started by simply running the client executable. The installation process is simple and requires little interaction and following the prompts. After a reboot of the machine to complete the installation the client is ready for use. On completion of the installation process the enrol process is started automatically.

NOTE: For Windows NT, 2000 and XP you should be logged in as a user with administrator rights before you install the software.

Enrolment

Before any connections can be made to the gateway, you have to enrol to identify yourself. You will not be required to enrol every time you connect, only when connecting for the first time from a specific PC.

The enrolment screen (activated by right-clicking on the @ tray-icon and selecting Enrol) will appear.

The help text on the screen will guide you through the enrolment process. Once all information on a section is complete, use the button to advance to the next step.

NOTE: During the enrolment process you will reference the Welcome memo which you should have received from the gateway administrator.

Step 1: Connecting and verifying the Gateway

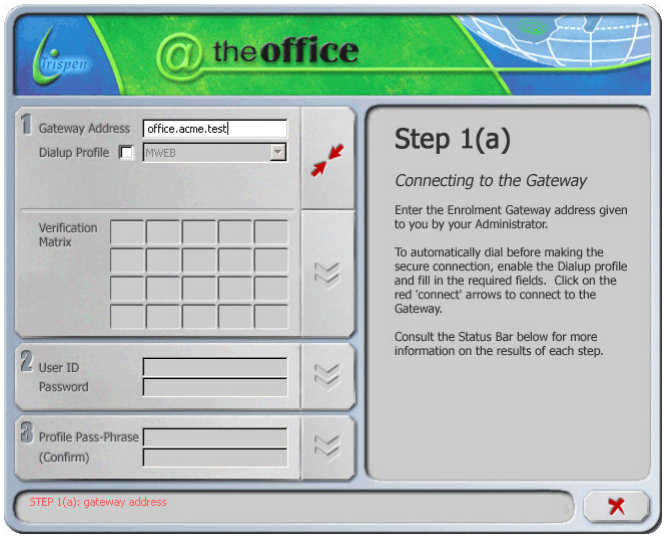

Figure 8: Client Enrol – Gateway address

Enter the Gateway address as provided in the Welcome memo. You may select an existing dial-up profile to be linked to your @TheOffice connection profile. Further information may be required in the dial-up session for the connection to be established.

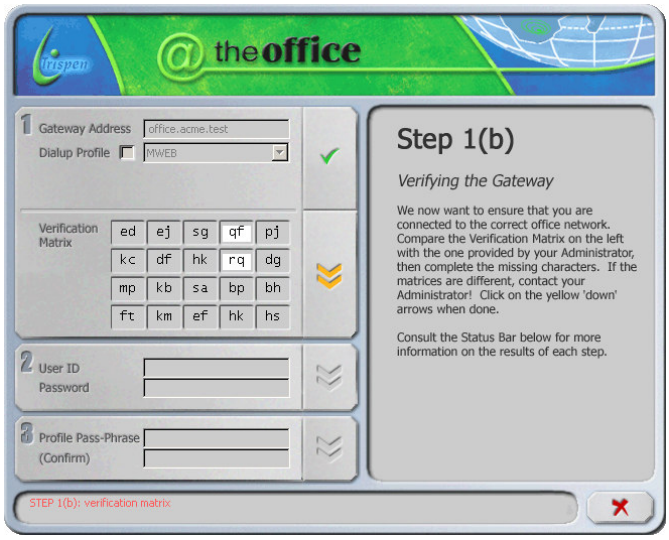

Figure 9; Client Enrol – Gateway verification

The verification matrix is a digital fingerprint of your gateway. For security reasons, you have to validate that the matrix matches the one provided in the Welcome memo. You should be careful to check that the matrix you received has in fact been received from your system administrator, to guard against an impostor setting up a gateway to reveal your User ID and password.

Step 2: Identifying Yourself

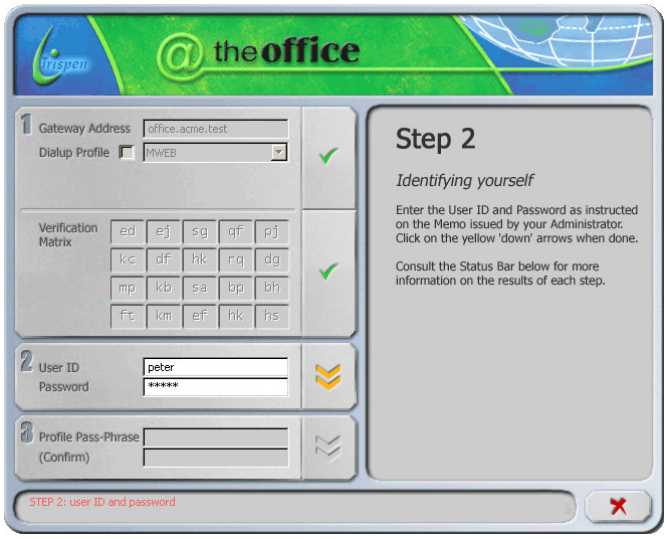

Figure 10; Client Enrol – Windows UserID and Password

Enter the UserID and password as described in the Welcome memo. This will check that you are authorised to use the services of the gateway. If you have chosen the correct UserID and password you will be allowed to proceed to the next step.

Step 3: Set Personal Pass-phrase

The next step is to select your personal pass-phrase (see Figure 11). This pass-phrase should be picked carefully, and remembered. Some tips on good pass-phrases are:

- Select a sentence or phrase rather than a single word. Pass-phrases can be full sentences such as “Office Connection Rox”
- You could use slang words or alternative spelling for words, to make guess attempts difficult. You can also use numbers instead of words e.g. “Connex 2day plz”

NOTE: Your Pass-phrase protects against unauthorised use of your @TheOffice profile. Remember that the pass-phrase is case sensitive! A Pass-phrase like “HELLO” is different to “Hello

---

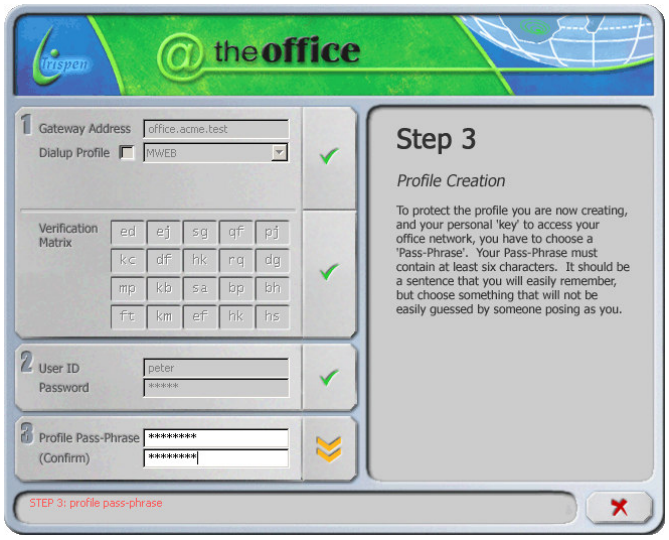

Figure 11: Client Enrol - Selecting your pass-phrase

Once you click on the button, your enrolment request will be processed and you will now be a registered user and can connect to the office.

Step 4: Enrolment Complete! Lets GO

You should see the welcome screen (Figure 12). Follow the instructions to connect to the office network.

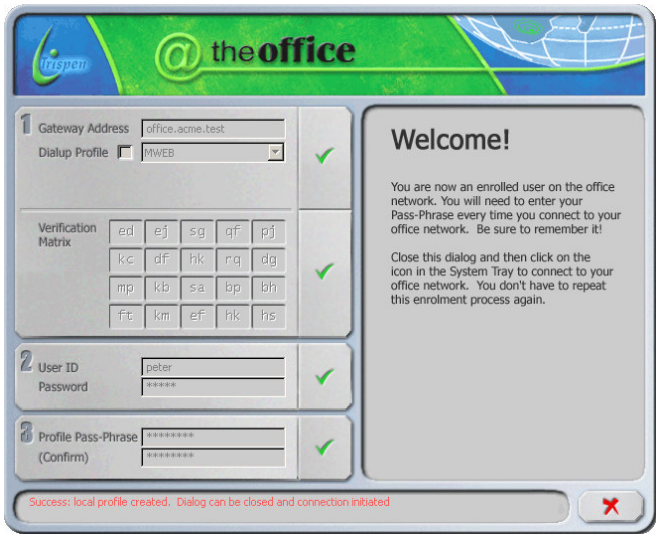

Figure 12: Client Enrol – Enrolment Complete

Connecting and Disconnecting

Once enrolled as a valid @TheOffice user, you can now connect to your office network.

To start the connection, right click on the tray-icon and select Connect.

You can also double-click on the tray icon.

You will be presented with the connection wizard:

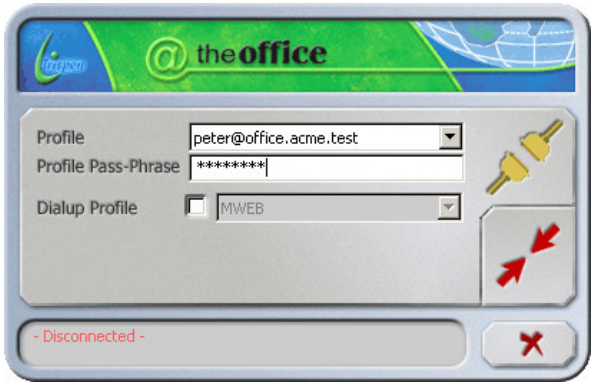

Figure 13: Client Connect

After you have selected the appropriate profile and entered the pass-phrase you selected on enrolment, click on the button to complete the connection.

If you would like to use a different dialup profile for the connection, you may change that before connecting. The selection will be available if you have one or more Windows dialup profiles set up.

Once connected, the Wizard will indicate that you are connected (see Figure 14). To disconnect, click on the button. You can hide the connect dialog by clicking on the button.

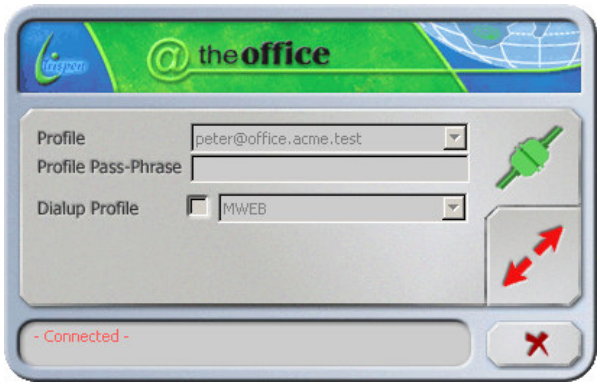

Figure 14: Client Connected

Connecting from another PC

If you need to connect to the office from another PC, you have to enrol again from that PC. This step does not create a completely new profile, instead it re-uses part of the profile stored on the gateway When you enrol from a second or further PC's, your pass-phase remains the same on all PC's. You must use the pass-phrase with which you enrolled the first time.

Certificate Expiry

The certificate used to connect to the gateway has a limited life for security reasons. You will be prompted with a message indicating that your certificate is about to expire. This occurs when you connect and your certificate is within the last 3 months of its lifetime. You will be able to continue connecting to the gateway until the certificate has expired but you are required to go through the enrolment process again to renew the certificate. This can be done at any time after the notification of expiry of the certificate.

Advanced Profile Management

The advanced option of the client is used when you have several profiles and wish to delete or change the pass-phrase of a profile.

To start the connection, right click on the tray-icon and select **Advanced**. This will display the dialogue as shown in Figure 15

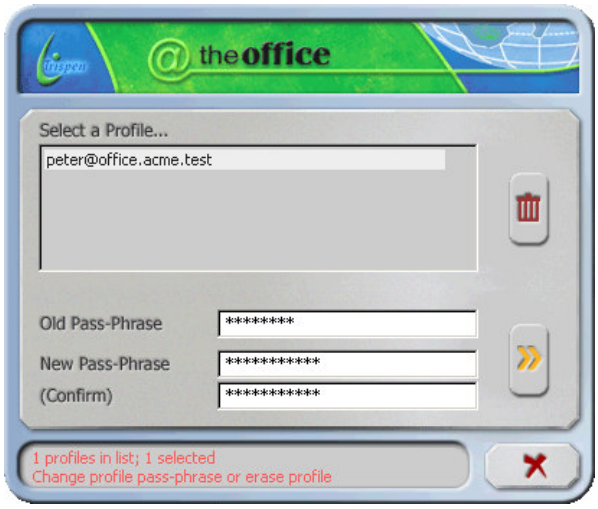

Figure 15: Client Advanced Options

To **Delete** a profile:
simply select the profile and click the bin to remove it from the list.

To **Change the pass-phrase** of a profile:
simply select the profile and enter the old pass-phrase followed by the new pass-phrase and a confirmation of the new pass-phrase. The **>>** button will commit the changes.

NOTE: the password is only changed on the current workstation. The gateway and other workstations holding a copy of the user profile will have the pass-phrase as set previously.

Firewall settings

Background

Why do I need to change the firewall settings

@TheOffice Clients need to connect to the @TheOffice Gateway. In most cases your office network will be screened from the Internet by means of a firewall or packet filtering router. To allow the required communication through the firewall, you will have to update the rules on the firewall.

What types of firewall can be used

Since @TheOffice requires direct communications between the Client and Gateway, firewalls that only allow connections via a proxy connection is not supported. It is possible however to use firewalls that make use of network address translation (NAT), as long as a public address is statically mapped to allow access to the Gateway PC from the Internet.

Configuring the firewall

Incoming Firewall rules required

@TheOffice uses UDP port 500 to communicate with all clients. You need to set up a filtering rule on your firewall to allow this port through the firewall. To avoid unnecessary exposure of your office network, the firewall rules should be very specific.

You need to set up the following rules:

- Allow: UDP From [anywhere][any port] To [GW IP][Port 500]
- Allow: UDP From [GW IP] [Port 500] To [anywhere] [any port]
- Allow: UDP fragments From [anywhere] To [GW IP]
- Allow: UDP fragments From [GW IP] To [anywhere]
- Allow: ICMP Type 3 (destination unreachable) From [anywhere] To [GW IP]
- Allow: ICMP Type 3 (destination unreachable) From [GW IP] To [anywhere]

NOTE: Future versions of @TheOffice will not require UDP fragments and ICMP traffic rules. Check with http://@theoffice.trispen.com for more information.

Outgoing firewall rules

In order for the gateway to connect to the licensing server, your firewall needs to allow outgoing HTTP and HTTPS connections. Most firewalls will already be configured to allow this type of traffic.

How do I test if it is working

The easiest test would be to perform the tests as described in Gateway ‘What to do next’ section.

Frequently Asked Questions

What do I need to use @TheOffice

You need a PC in your office to run the Gateway Software and your office needs a permanent Internet connection. Of course you need to install the client software on all PC's that want to connect securely to your office; these too need Internet access. You can download both of these software packages from http://@theoffice.trispen.com, where you can also purchase Activation tokens to use this software.

How do I Install … ?

Before installation, refer to the section [Planning the installation] and [Firewall settings]

To install the Gateway, refer to [The Gateway]

To Install the Client Software refer to [The Client]

Why can I not refresh my activation keys?

Invalid activation keys entered

If invalid or expired activations keys are entered the licensing server will reject them. Ensure that a valid key is entered.

The Gateway does not have Internet access

For the Gateway to refresh the activation keys and include new activation keys, Internet access is required to the licensing server. The gateway will attempt to use the Internet Explorer proxy settings, if they exist, of the user operating the Gateway user interface.

Why do I need to complete the Verification Matrix

@TheOffice makes use of sophisticated cryptographic technology to ensure that no unauthorised user is allowed access to your office network. Internally, @TheOffice uses public key cryptography. Each user has a key-pair that consists of a private key (protected by your pass-phrase when stored on disk) and a public key. The public keys are presented to the gateway and verified when a user connects.

The Enrolment process sets up a trust relationship between you and your key-pair. To prove to the gateway that you are who you claim to be during enrolment, you have to present your UserID and password.

With Public key technology we can send this information securely to the gateway, but we have to guard against a rogue Gateway receiving your Windows User ID and password!

To prevent this, the Verification Matrix is used. This is a number (digital fingerprint) of the Gateway Public Key that @TheOffice converts into twenty two character pairs.

The Verification Matrix is not a secret, however you must trust the source from which you obtained it. The best option is to receive it from your system administrator directly – this way you know it can be trusted.

Why can't I enrol to the Gateway

Possible problems might be:

Domain controller

In order for your @TheOffice Gateway to be able to query the domain controller, the Gateway PC must be registered on the domain. It is also important to verify that the domain controller has the group "Pre-Windows 2000 compatible access", and that either the user "Everyone" or the Gateway PC is a member of the group.

Incorrect Password used

The user ID and password must match that of the registered user in the domain group as specified in the gateway. Refer to the Advanced Configuration section above for more information.

User not in domain/group specified

All users that require access to the gateway must be included in the access group as specified during the gateway configuration. Refer to the Advanced Configuration section above for more information. If the gateway resides in a domain, the default of "domain users" will include all the users registered in the domain. If the gateway is not in a domain, then the default will be all the users registered on the gateway.

Office Network firewall issues

No access to the Gateway public address. This could be due to firewall configuration issues. Refer to the section on setting up your firewall [Firewall settings] or get assistance from your firewall administrator. You could also use the web based test tool as described in the Gateway 'What to do next' section.

Intermediate firewall setting issues

You might be connecting via a complex network. The gateway should take care of most complexities. However, if the network traffic required by the gateway is blocked somewhere along the way, contact the network administrator of the device filtering the traffic.

Specified IP-Address of Gateway incorrect

The IP address or DNS name of the gateway specified is incorrect and the client cannot connect to the gateway or the gateway is inaccessible from the public network.

NOTE: the IP address or DNS name specified must be accessible from the public network (the Internet). It is also used in the Welcome Memo, as described in the 'Gateway Status' section above, to inform the user of the client which gateway address to use.

Why can’t I connect to the Gateway

At each failed attempt to connect to the gateway the user is presented with an error message stating which part of the process failed. The user must ensure that the correct profile and pass phrase is used when attempting to connect to a gateway. The profile is listed as [user ID]@[gateway address](domain)

Several problem scenarios could occur and are described below.

The User has not enrolled

If the fields in the client connection windows are greyed out, the user has not enrolled to a gateway. The user is required to enrol from the client device from which a connection is required to be made. Remember the first enrolment to the gateway creates a new active user on the gateway and a subsequent enrolment requires that the user enrol using the original pass phrase. Refer to the Client ‘Enrolment’ section.

NOTE: A user can enrol from several PCs to the same gateway. The first enrol process creates a new profile on the gateway, and subsequent enrolments must use the same pass phrase as the first since they are actually using a copy of the initial profile.

I cannot find my profile

The user profile is created on completion of the enrolment process. If several users use a client PC then each user must enrol from that PC so that the user has a valid profile to use during the connection process.

I have a valid profile and cannot connect

A user that has previously enrolled and was able to connect to the gateway may have left another PC connected using his profile. The user may only have two connections to the gateway open at any one time. It is not recommended that users share profiles, as this will reduce the security value of the system.

Another problem could be as simple as using the incorrect pass-phrase.

You might also, in fact, have an invalid profile due to the fact that the gateway has been changed, for example the country changed. Refer to The Gateway Basic Configuration section for more information. This issue is resolved by enrolling again.

Connection attempted on local subnet

Each PC on the network is located on a network with a unique IP Address and operates within a particular subnet, the local portion of the network. Any communications outside of this network is routed via a gateway to reach its destination. @TheOffice requires that the Client and gateway are located in different subnets, and will warn the user if this is not the case. You can therefore not use the Client while you are in the office subnet and need to be outside of your local office network.

Firewall not set-up correctly

The complete route from the client to the gateway needs to allow specific traffic through for the connection take place. This includes the firewalls at (or on) the client and the gateway. It is important that UDP protocol on port 500 is allowed through by the firewalls and NAT devices. Refer to the section describing the Firewall settings for more information. If the enrol process was successful then it is unlikely that the firewall settings are at fault.

Insufficient IP addresses in the IP Pool

Each user is allocated an address from the IP pool as specified during the Basic Configuration of the gateway. If no address is available for the user the connection will be denied and an appropriate error message provided. The gateway administrator can look at the logs to determine how often this problem occurs and take corrective action i.e. increase the size of the IP pool.

Insufficient Licensed Users

For users to connect to the Gateway the administrator has to install Activation Keys that allow a certain number of subscribed users to connect. Once the limit is reached no aditional conenctions will be allowed and the administrator will have to manage the active/inactive user list or install additiaonl Activation Keys.

Already connected more than once

Each user may only connect have up to two connections. Should a connection not disconnect correctly the administrator can cancel the connection from the Connections tab of the Gateway managent application.

Glossary of Terms

PC

Personal computer

Private key

A secret number used in the authentication process. The private key is normally protected by encrypting it with a pass-phrase.

Pass-phrase

Similar to password except that it may contain several words.

Domain

A group of nodes on a network forming an administrative entity.

Firewall

An application or an entire computer (e.g., an Internet gateway server) that controls access to the network and monitors the flow of network traffic. A firewall can screen and keep out unwanted network traffic and ward off outside intrusion into a private network. This is particularly important when a local network connects to the Internet.

UDP
(User Datagram Protocol)

A Transmission Control Protocol/Internet Protocol (TCP/IP) technology that enables an application to send a message to one of several applications running in a destination machine.

Root certificate

The certificate that is trusted by users of a certificate hierarchy. subservient certificates can be verified by using the root certificate. The root certificate cannot be verified cryptographically and is normally installed using another trust mechanism. In @TheOffice, the root certificate of the gateway is installed when the user correctly selects the verification matrix.

IP-Address
(Internetwork Protocol address or Internet address)

A unique number assigned by an Internet authority that identifies a computer on the Internet. The number consists of four groups of numbers between 0 and 255, separated by periods (dots). For example, 192.0.2.20 is an IP address

DNS
(Domain Naming System)

The online distributed database system that serves as the map between names and Internet addresses

NAT
(Network Address Translation)

A functionality provided through the gateway Network Control Program (NCP) to protect the internal Internet Protocol (IP) addressing structure from the Internet IP addresses

Index