Contents

Table of Contents

Logs & Reports
Preferences

Installation

To start the XGate 2.0 installation, insert the XGate 2.0 Installation CD into your computer's CD or DVD drive.

When the Installation Options screen appears, select the New Installation option.

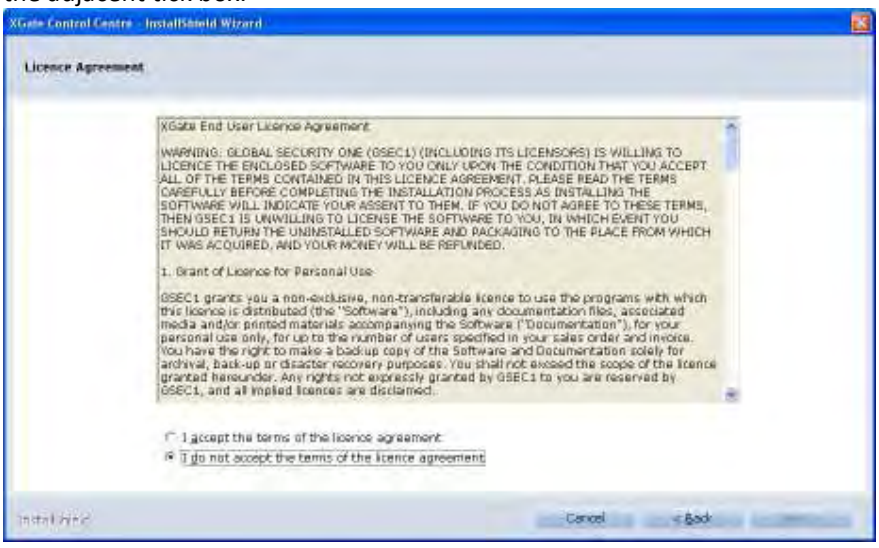
If your installation does not start:
1) Go to My Computer.
2) Go to your CD / DVD drive (labeled as: XGateV2.0 Setup)
3) Double click the XGate Setup file

Welcome

The Welcome screen will appear.

Licence Agreement

Please read the agreement and select I accept the terms of the licence agreement by ticking the adjacent tick box.



Installation Location

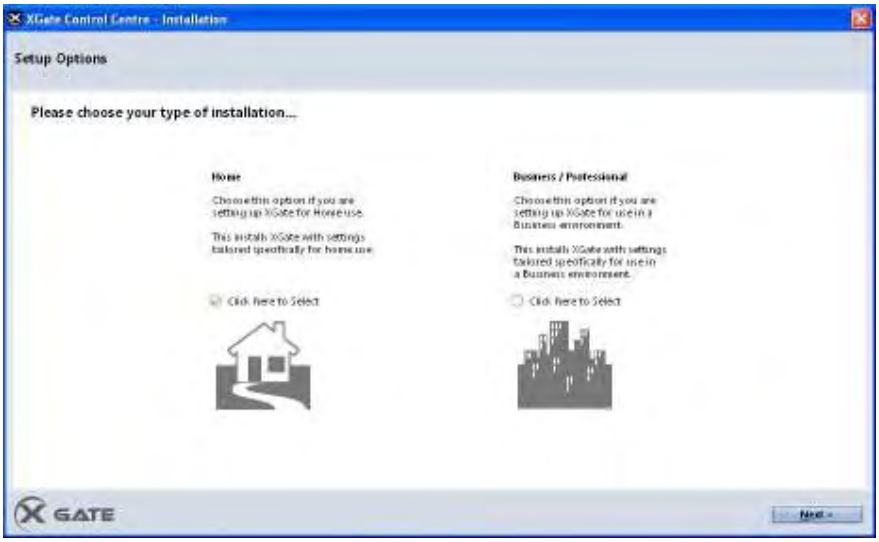
If you wish to change the location of where XGate installs on your Hard Drive, click the Change button.

XGate Connection Verification

A diagram will appear showing you how XGate should be connected. Ensure your setup is correct and press Verify Setup. If all is correct, a green tick will appear.

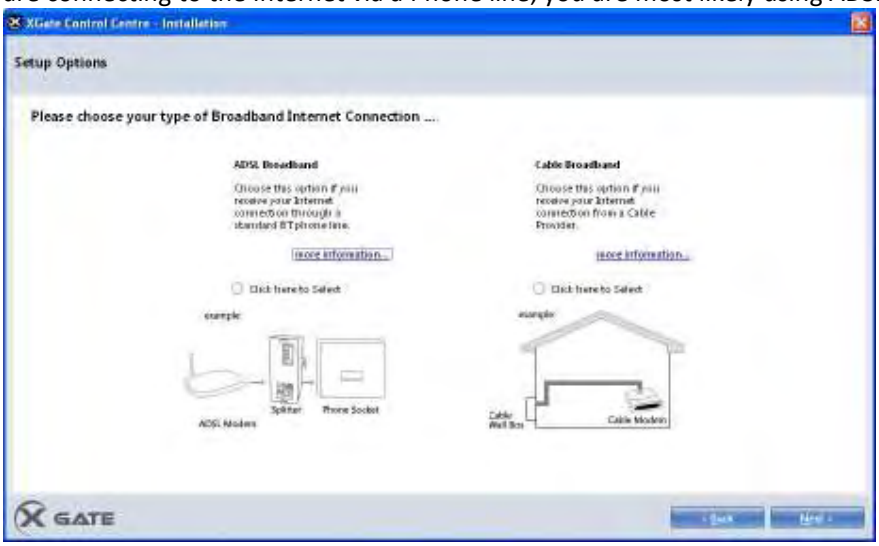
Home or Business

Select whether you are installing at home or at a business by ticking the appropriate tick box. For the purposes of this manual, only the Home mode will be covered.



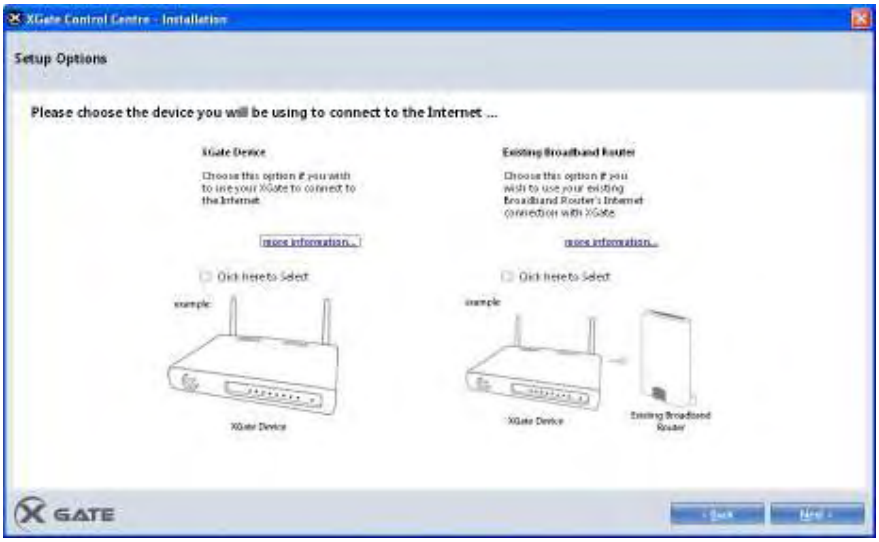
ADSL or Cable

Select whether you are installing XGate on an ADSL or Cable broadband connection. If you are connecting to the Internet via a Phone line, you are most likely using ADSL.



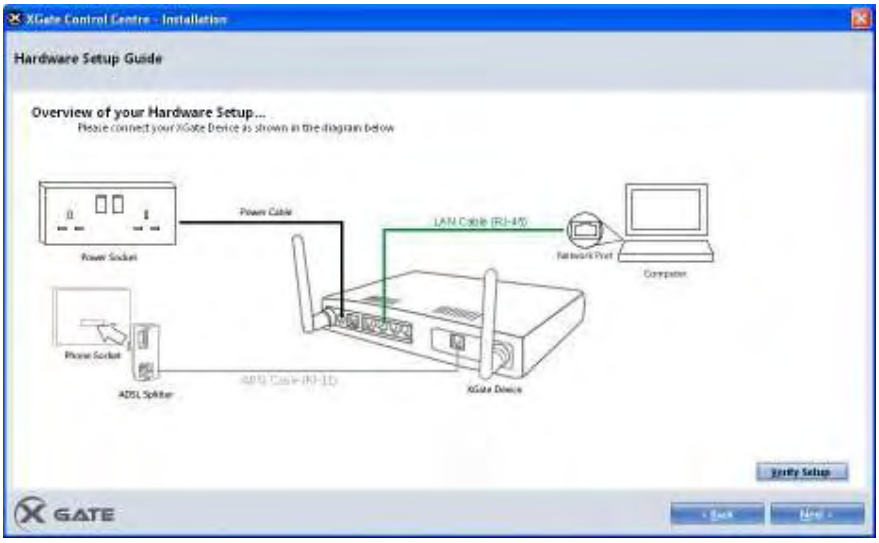
XGate or Existing Router

Select whether you wish to solely use your XGate to connect to the Internet or wish to use your existing router with XGate instead. Unless your existing router has specific features you wish to keep using, XGate is the recommended choice.



Hardware Setup Guide

Another diagram will be shown, this time showing how the XGate will be physically connected. Please follow the diagram shown on-screen. Press Verify Setup to verify the connection.



Login Details

Type in a Password that you would like to use to login to the XGate Control Centre. Please use a password that is memorable but also secure. Your Internet Security may be compromised if someone can guess your XGate Control Centre password. Please set a secret question and answer in case you forget your login password.

Registration

Enter your Activation key. You can find this key on the inside of your XGate CD Case.

Chat Room Alerts and Secure Banking

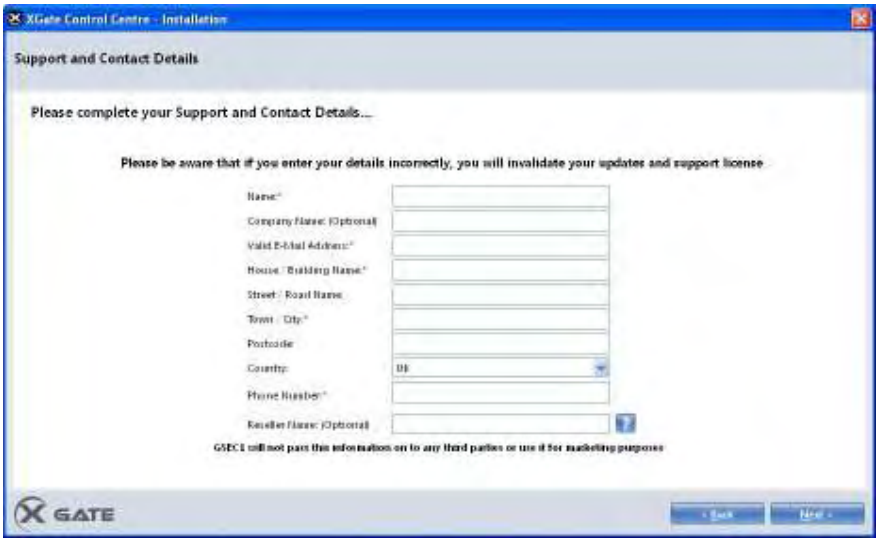
To use Chat alerts, enter your mobile phone number or e-mail address.

To use Secure Banking, select the bank by clicking on its name and pressing the Add button.

Note: If you do not wish to use one or both of the features tick the respective I do not want to use this feature tick box.

Support Details

Please enter your Support details. This allows us to contact you with appropriate measures if a serious security outbreak occurs.



Broadband Configuration

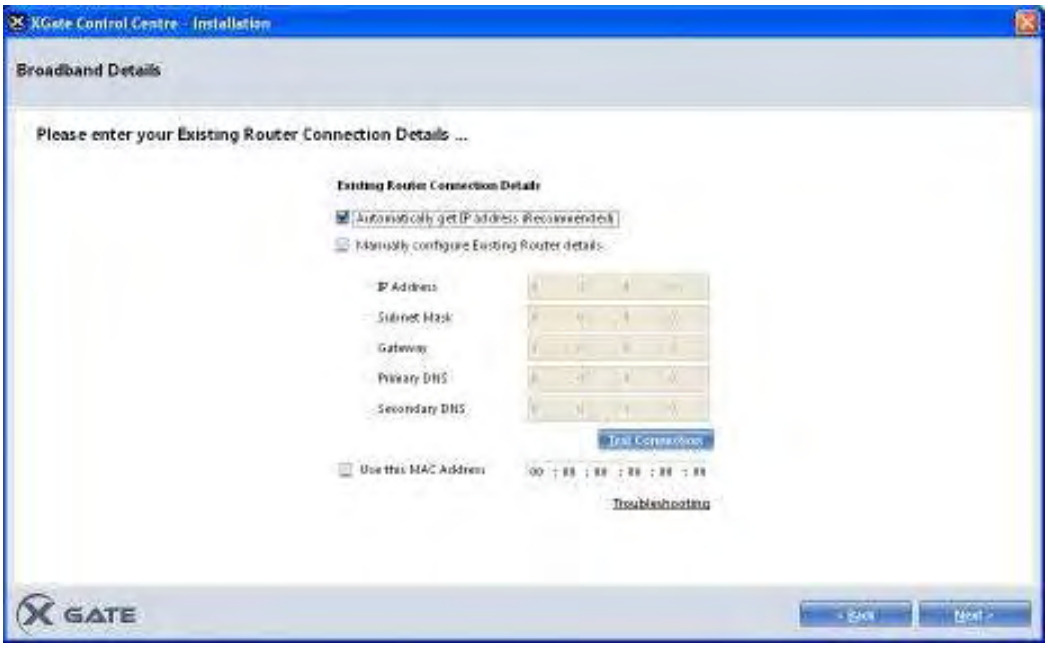
The Broadband Configuration screen will differ according to the options you selected earlier in the Installation process. All configuration screens are shown below.

Cable Configuration

In the majority of cases, you can leave the selection as Automatically get my IP Address. If your Cable Broadband Provider provided you with an IP Address, tick assign static IP Address and fill in the fields with the details your Broadband provider gave you.

Existing Router

If your Router has DHCP mode enabled, you can leave the selection as Automatically get my IP address tick box. If your existing Router has DHCP disabled, then you will need to specify the IP Address details. Consult your router configuration or manufacturer documentation for more information.

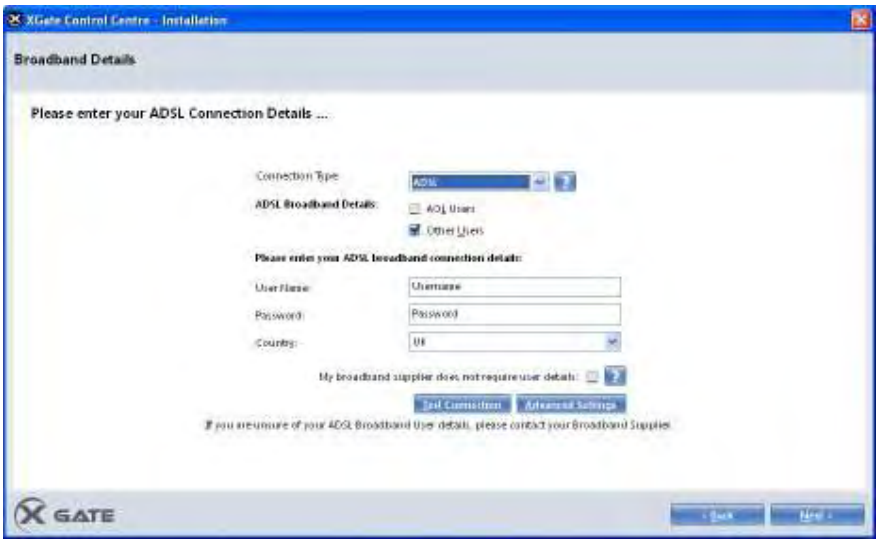


ADSL

Choose your connection type by clicking the arrow and then clicking on your type of ADSL connection.

Provide the Username and Password that your Broadband Provider has given you. If you are unsure of these details please contact your Broadband Provider. Some ADSL connections do not require a username and password. In these cases, tick My broadband supplier does not require user details.

Press Test Connection to test your Internet connectivity to ensure that all details you provided are correct.

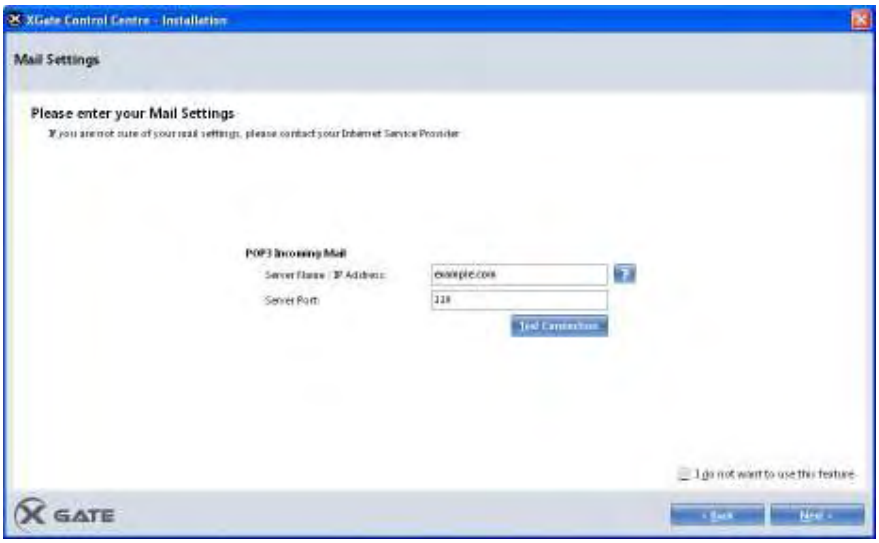


Note: As a guide, here are the maximum speeds for each type of ADSL connection:

Up to 8Mb – ADSL
Up to 12Mb – ADSL 2
Up to 24Mb – ADSL2+

Mail Settings

Type in the Server or IP address and port of your POP3 mail server. If you are unsure of what your mail server address is, contact your Mail provider. In some cases your Mail provider may also be your Broadband Provider.

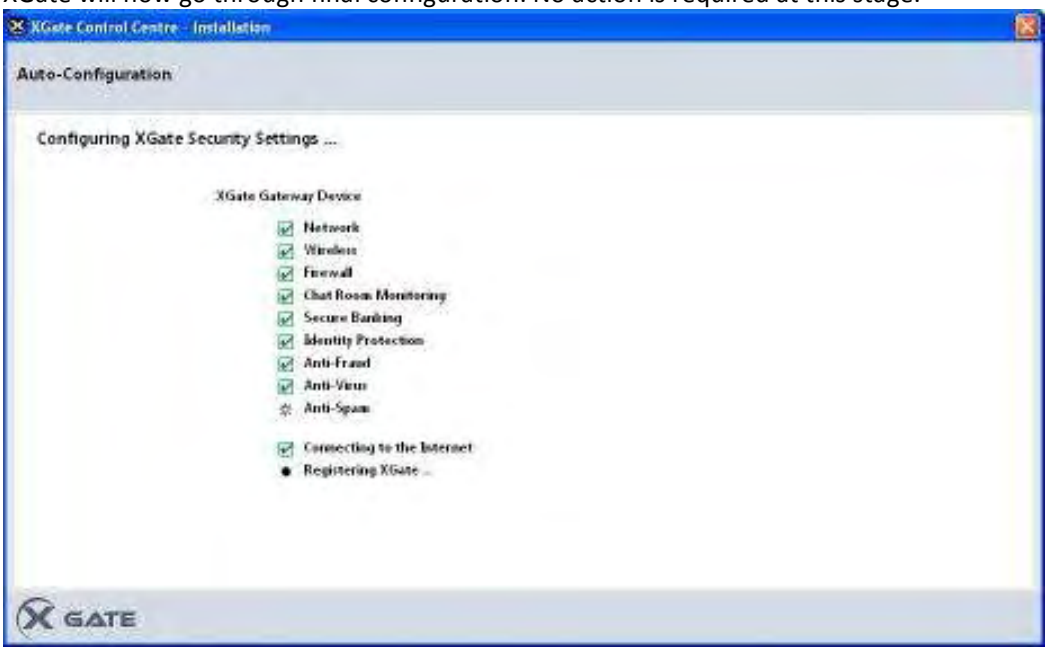


Note: If you do not wish to use XGate's POP3 Proxy, tick the I do

not want to use this feature tick box. Please be aware that if you do not use the POP3 Proxy then you will also be unable to use the Anti-Spam Feature. However POP3 can be configured later in the XGate Control Centre.

Auto Configuration

XGate will now go through final configuration. No action is required at this stage.



Once you progress past this screen you have completed your XGate installation.

What is XGate?

Unlike traditional Internet Security software that monitors attacks on your computer, XGate monitors and blocks attacks before they can harm and reach your computer, allowing you to enjoy the Internet without worry.

This User Guide contains information on how to customise XGate's settings to achieve maximum network security.

About GSEC1

About Global Security One

Global Security One (GSEC1) is the world pioneer of Internet Security and Network Management (ISM) products, which are designed to provide comprehensive end-to- end security for internal and external network infrastructure of individuals, small to medium Enterprises, Service Providers and public sectors.

GSEC1 is one of the first Internet security vendors to provide the best of breed, unified and integrated security solutions for Gateways, Servers and clients, through its Prodigy™ and XGate™ devices.

GSEC1's radical approach to Internet and Network security ensures total protection and incorporates solutions for a wide range of Internet Security technologies.
To learn more about GSEC1, please visit the GSEC1 website.

Features

Child Chat Room Monitoring
XGate's revolutionary Child Chat Monitoring technology allows parents to monitor and control their children's Internet chat room activities from their mobile phones or e-mails. When required, parents can take control of their computer by using commands from their mobile phone wherever they may be in the world.

Firewall
An advanced business class hardware firewall is integrated into the XGate to stop attacks before they can even reach your computer.

Secure Banking
With support for all major International banks, XGate ensures your connection to the bank is as safe as if you were there yourself.

Identity Protection
The Identity Protection suite monitors all information you send and ensures that your identity remains your own.

Anti-Virus (Triple Engine)
With our revolutionary triple engine Virus Protection, XGate ensures that your computer is three times more secure than any other Virus engine on the market.

Gateway Anti-Virus
Gateway Anti-Virus Protection ensures that Viruses are stopped at your XGate and do not have a chance to reach and infect your internal computers.

Security Sensors
With its revolutionary Sensor technology, XGate sensors monitor all irregular patterns of data and traffic (e.g. from Viruses and Spyware) on all computers behind XGate to guarantee your computer's health.

Category Based Web Filtering
Block indecent and inappropriate websites by using the Intelligent Web Filter, with the flexibility to be able to restrict Internet access at different times of the day.

SPAM Control
The XGate SPAM Engine extracts the SPAM emails you receive and allows you to respond to the emails you do want to see, rather than the ones you don't!

Connect-to-Office VPN
The XGate Connect-to-Office VPN suite provides a secure connection to your company's systems, allowing you to work from home in a secure environment.

Desktop Live View
Desktop Live View gives real-time views of all connected desktops for monitoring and reporting purposes.

Secure Wireless Connectivity

The XGate secure wireless connectivity ensures that your wireless Internet connection is not only lightening fast, but is also the most secure.

Advanced Networking features
XGate Advanced Network configuration ensures that IT professionals have more advanced configuration at their fingertips, such as support for Dynamic DNS, Static Routing, Multiple IP Hosting and many more features included out of the box.

ADSL & Cable Connectivity
A built in ADSL modem capable of speeds of up to 24Mb and support for cable Internet users ensures that XGate meets all your connectivity needs and gives you an all in one solution.

System Requirements

XGate 2.0 Recommended System Requirements

- Pentium 4 processor or AMD equivalent
- 512 MB of RAM
- 100MB of free Hard drive space
- Activated Internet Connection.
- CD-ROM (or DVD) Drive
- Ethernet Network Adapter
- Wireless Connection (optional)

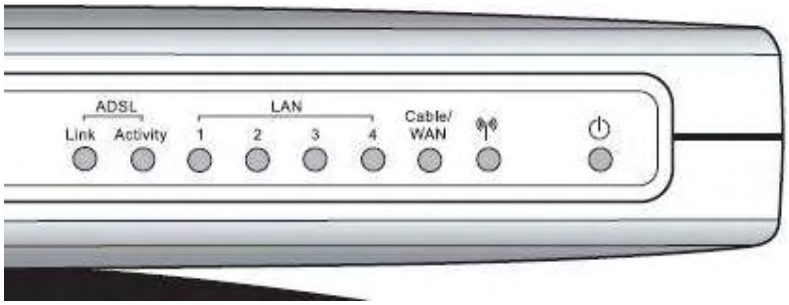
Operating Systems Supported:

- Windows 2000 (Professional)
- Windows XP (Home or Professional)
- Windows Vista (Home Basic, Home Premium, Business or Ultimate)

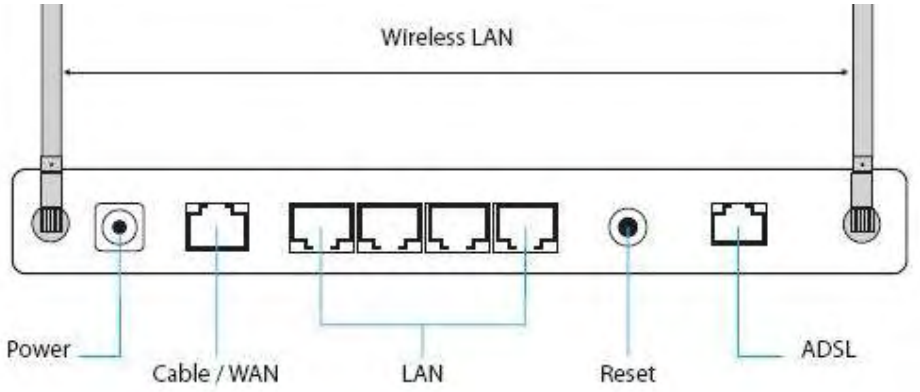
Broadband Modem Support
Cable, ADSL, ADSL2 and ADSL2+

Your XGate 2.0 Device

The picture below shows the front panel of the XGate 2.0 device.



The picture below shows the back of the XGate 2.0 device.



LED	State	Description
Power	On	XGate 2.0 Device is switched on
	Off	XGate 2.0 device is not switched on
ADSL Link	On	The XGate ADSL modem has connected
	Off	The XGate ADSL modem has not connected
ADSL Activity	Flashing	There is data passing through the ADSL connection.
	Off	There is no data passing through the ADSL connection
LAN	On	There is a connection present at the corresponding LAN port
	Off	There no connection present at the corresponding LAN port
Cable/WAN	On	There is a connection present at your Cable/WAN port

	Off	There is no connection present at your Cable/WAN port
Wireless	Flashing	Wireless network traffic is passing through the XGate 2.0 device
	On	XGate Wireless is switched on.
	Off	XGate Wireless is switched off.

XGate Control Centre

The XGate Control Centre is your portal to set up and manage your XGate 2.0 device. For convenience and flexibility, there are two different visual styles incorporated into the XGate Control Centre: Home and Professional.

Home Mode is recommended for novices to intermediated users. It focuses on easy navigation and understanding of the user interface.

Professional Mode is targeted towards the more advanced or business user. It uses the two-pane interface design common in a range of applications. This interface mode is focused on fast navigation.

Logging into the XGate Control Centre
To log in to the XGate Control Centre:
- Double click the XGate Control Centre icon on your Desktop.
- Go to Start > Programs > XGate 2 > XGate 2.0 Control Centre

Closing the XGate Control Centre
To close the XGate Control Centre, click the red cross in the top right of the screen.

Logging Off
Logging off is different than closing the XGate Control Centre. You will be returned to the XGate Login Screen. This maybe useful if, for example, you wish to log in to another XGate 2.0 device.

To Log Off in Home Mode click the Log Off option, which is the last item listed in the Quick Links menu on the right.

To Log Off in Professional Mode click the Log Off button in the top right of the window.

Accessing Help
To access this user guide in the Home mode of the XGate Control Centre, click the Help button in the top right of the window.

In Professional mode, you can access this User guide by clicking the Help button on the left hand side, underneath support and above Status.

Introduction

Firewall

What is a Firewall?

A firewall controls the flow of traffic between computer networks. Most commonly, a firewall acts to protect a private Local Area Network (LAN) from threats originating from a Wide Area Network (WAN) such as the Internet.

Analogy

Imagine a building (your network) with a number of doors (ports / programs). Each door has a guard assigned to it (the firewall) with instructions (firewall rules) on who to allow access, in and out of the building. When someone (a connection) enters or exits the building through one of the doors, the guard inspects them and then decides upon an action, based on the instructions they have been given.

Firewall Features

XGate's Firewall is designed to offer a high level of Internet protection with little setup required.

Within the Firewall Module are the following features:

Basic Firewall Security:
Enables you to quickly and easily configure their firewall settings.

Firewall Rules:
Allows you to set rules to control the flow of data between XGate and the Internet.

Programs and Applications:
Specify the ports used by programs for use within the Firewall Rules.

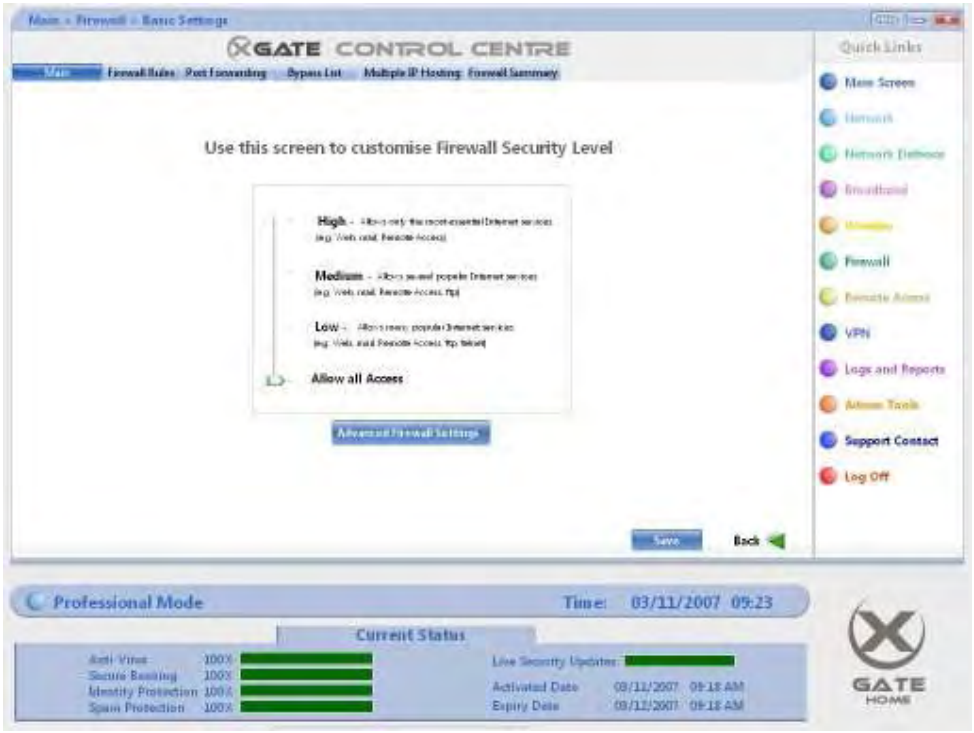
Port Forwarding:
Forward /translate data as it passes from one port to another, through your XGate 2.0 device.

Multiple IP Hosting:
Host Multiple Domains under a Shared IP Address.

Firewall Summary
View, print, save or e-mail an overview of all your Firewall Settings.

Basic Firewall Security Level

This screen allows control over the security level of XGate's Firewall. From here you can set the Firewall level as High, Medium, Low or Allow all Access. Below is a full description of what each category contains.



High

Service	Protocol	Port Number
DNS	UDP and TCP	53
Telnet Login	TCP	23
SSH Login	TCP	22
FTP Login	TCP	20 and 21
NTP	UDP & TCP	123
HTTPS	TCP	443
SMTP	TCP	25
POP3	TCP	110

Medium

Service	Protocol	Port Number
RTSP	UDP and TCP	554
IRC	UDP and TCP	194
Yahoo Messenger	TCP	5050
MSN Messenger	TCP	1863
AOL Messenger	TCP	5190
ICQ Messenger	TCP	4400

Low

Service	Protocol	Port Number
Rtelnet	UDP and TCP	107
Trace Route	UDP and TCP	33434
Imap	TCP	143
IPP	TCP	631
Radius	TCP	1812
RSync	TCP	873

Allow All Access

This allows all outbound access through your XGate 2.0 device.

Introduction

Firewall Rules

What is a Firewall Rule?

Firewall Rules in XGate are instructions that allow, deny or reject access to traffic entering or leaving your network.

Analogy

Firewall Rules are similar to instructions given to a security guard (Firewall). These instructions (firewall rules) detail which door (port) a person (data) is allowed to enter or leave a building.

If the security guard is given instructions to allow a person through a door, they can pass. If the instruction is to deny a person of a certain description, they will be told they are not allowed to pass. If the instruction is to reject, the person will be completely ignored.

Firewall Rule Details

Within XGate there are various details that must be provided to have a complete firewall rule. These are:

Name:
This is a friendly name to easily identify the firewall rule.

Direction:
Either set as Internet to PC (Inbound) or PC to Internet (Outbound). In the vast majority of scenarios, this should be set to Internet to PC.

From and To:
This specifies where the traffic is coming from and where it is.

Program:
The list of Programs is derived from the entries within Programs and Applications.

Action:
The Action you wish to perform based on the details provided above.

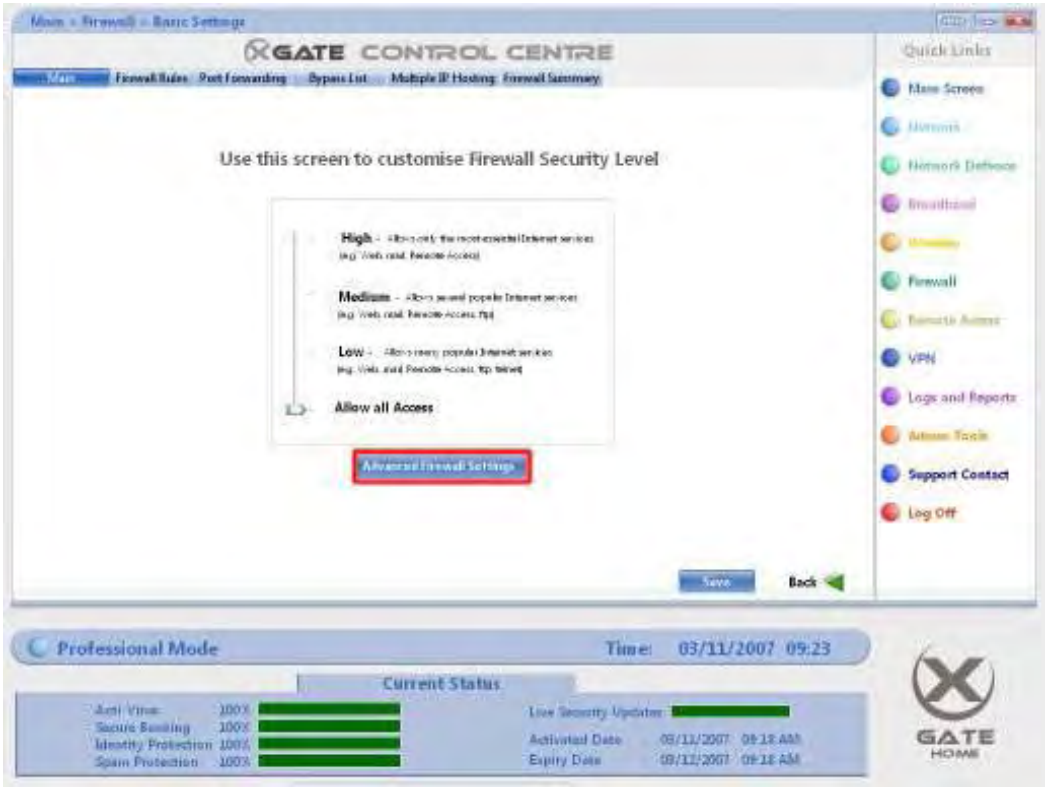
Below is a description of how the Firewall Actions affect traffic.

Allow:
This allows the specified traffic
Deny:
Does not allow the specified traffic and will send a response to the other side, saying that the port is closed.
Reject:
Does not allow the specified traffic, and will not send any response back. Sometimes this is referred to as ‘Stealth’.

Adding a Firewall Rule

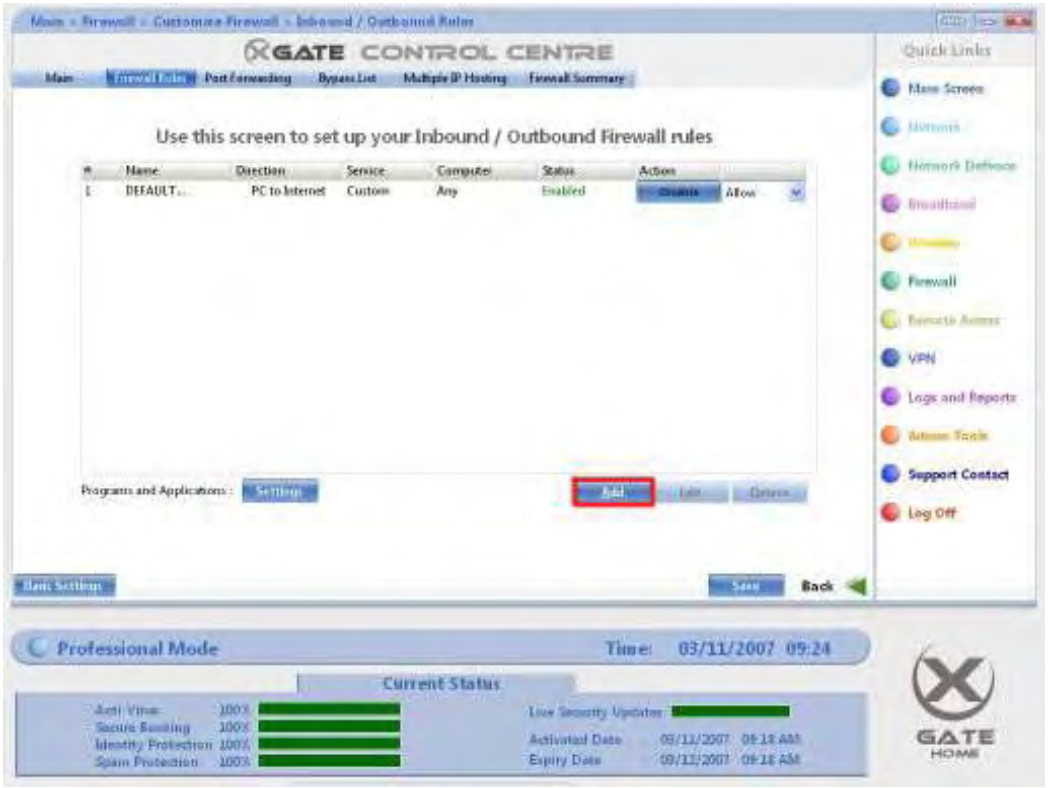
1) Click on Firewall in the Quick Links Menu .

2) Click on Advanced Firewall Settings.



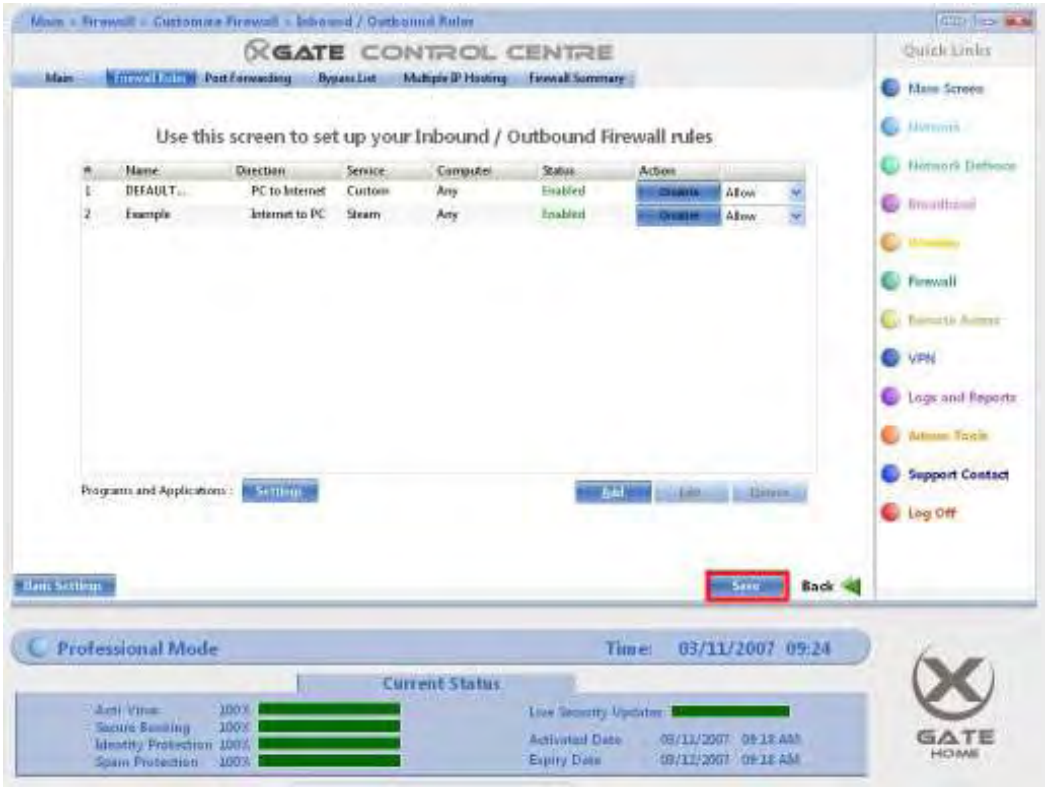
3) Click on the Firewall Rules - Settings button.

4) Click the Add button.



5) Enter your firewall rule details.
6) When you are satisfied with the Firewall Rule details you have provided, press the OK button.

7) Click the Save button to confirm your changes.

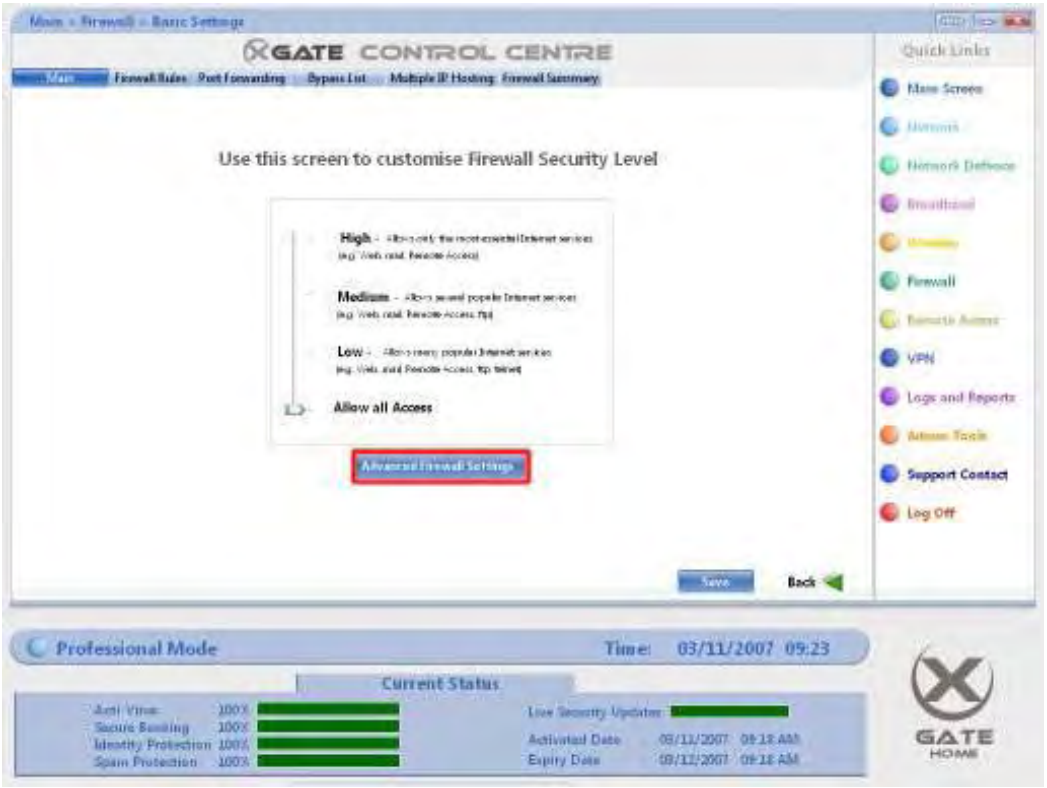


Note: To add your own Program to a Firewall rule, see Adding a Program or Application.

Changing the details of a Firewall Rule

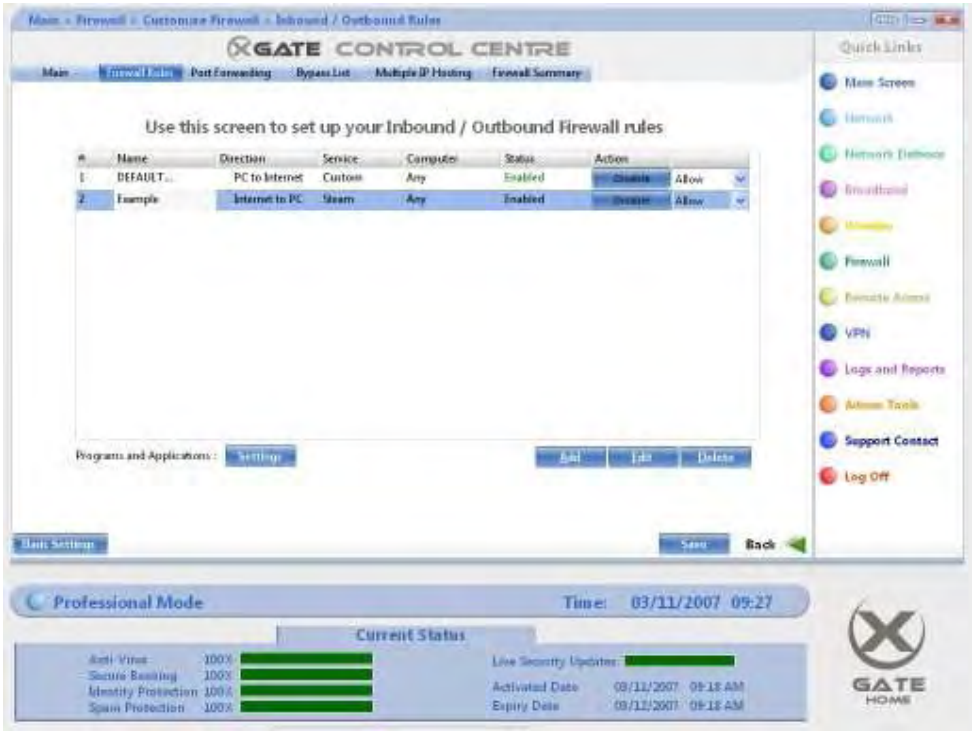
1) Click on Firewall in the Quick Links Menu.

2) Click on Advanced Firewall Settings.

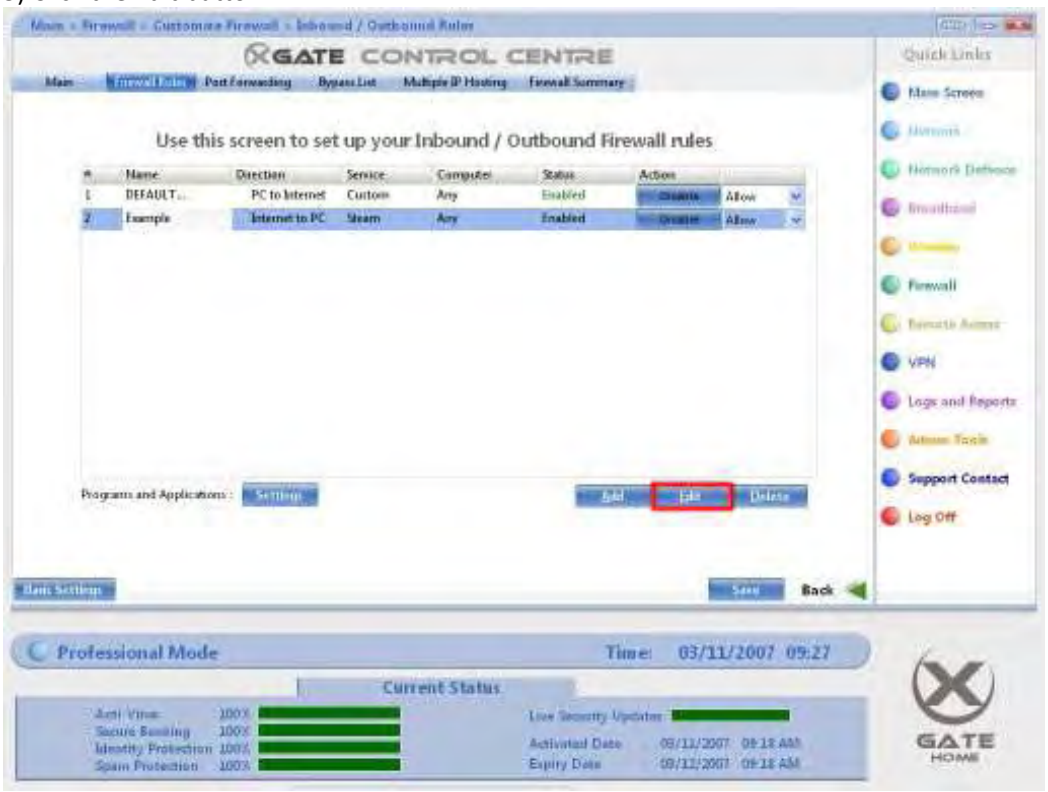


3) Click on the Firewall Rules - Settings button.

4) Select a firewall rule entry by single clicking it. The entry should become highlighted.

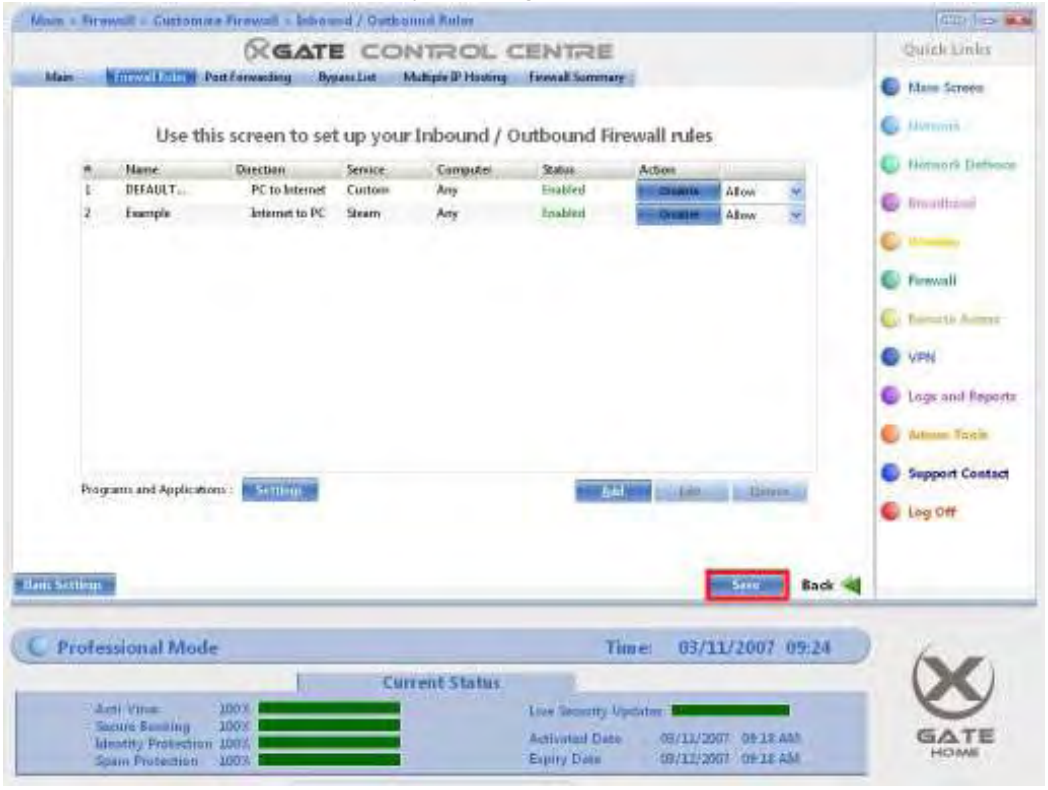


5) Click the Edit button.



6) Change the details of the Firewall Rule .
7) Press the OK button when you are satisfied with your changes.

8) Press the Save button to confirm your changes.

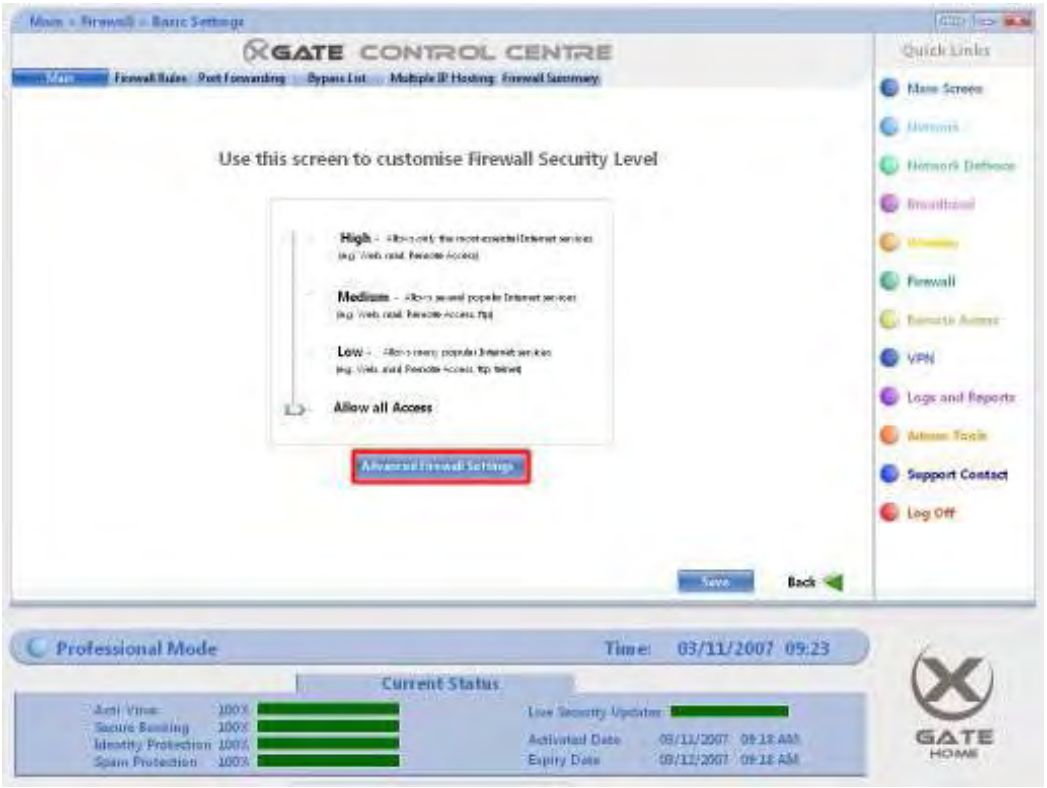


Removing a Firewall Rule

Removing an Inbound / Outbound Firewall rule

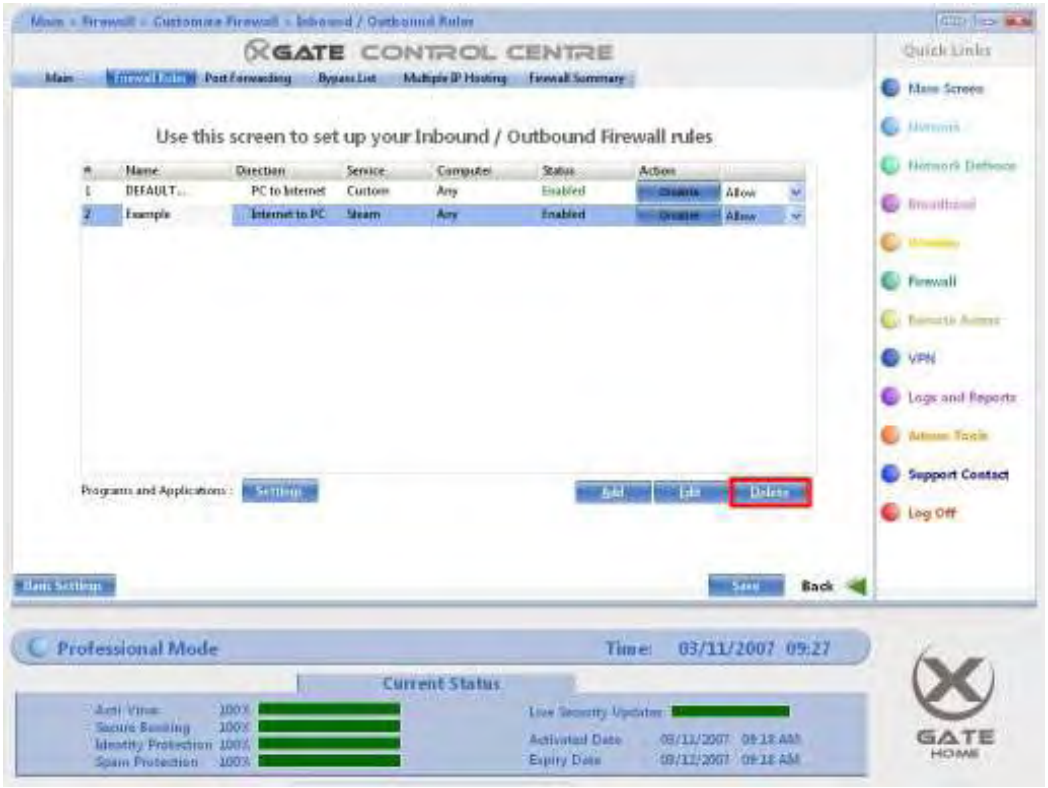
1) Click on Firewall in the Quick Links Menu.

2) Click on Advanced Firewall Settings.

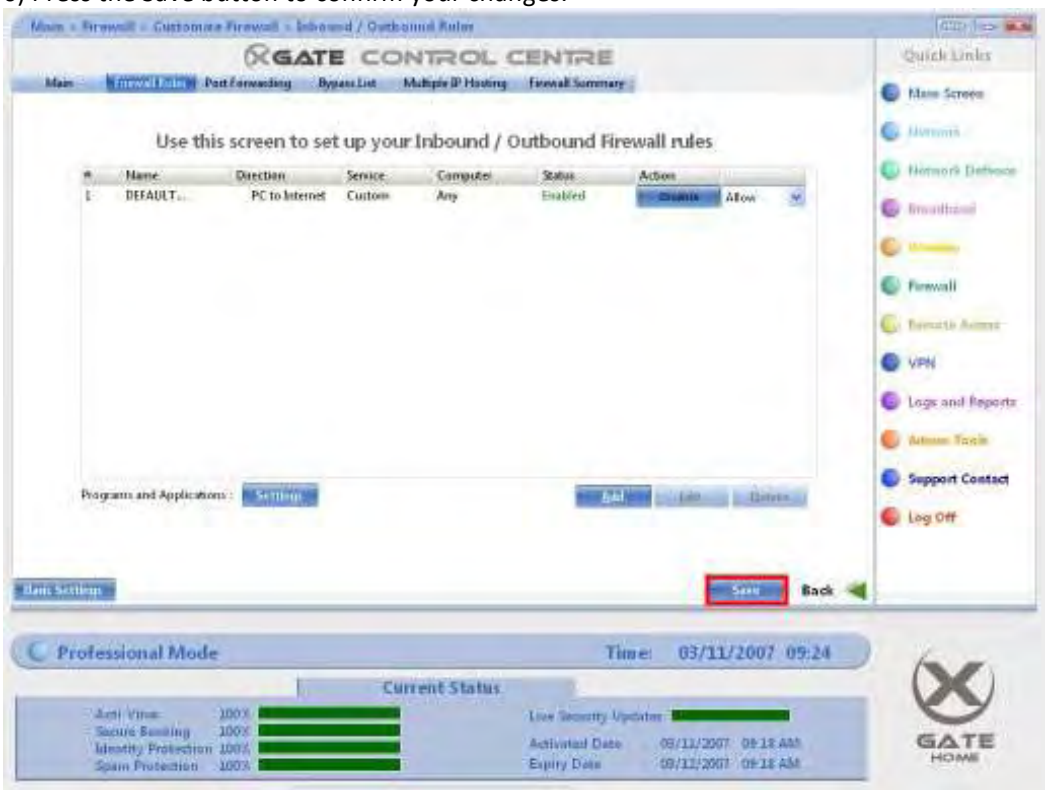


3) Click on the Firewall Rules - Settings button.

4) Select a firewall rule entry by single clicking it. The entry should become highlighted.
5) Click the Delete button. The entry you selected will be removed from the table.



6) Press the Save button to confirm your changes.



Introduction

Programs and Applications

What is a Program / Application?

Within the scope of XGate 2.0, Programs and Applications are made up of a collection of protocols and ports.

When you use a Program or Application that accesses the Internet from your computer, it communicates via the Internet using ports.

Analogy

A program can be seen as a parcel. This parcel has a label with a door number (the port and protocol). When it is sent in or out of the building (network), the label is examined by a guard (firewall) and sent through the door (port) specified on the parcel label.

By creating Programs and applications in XGate, you can assign them to Inbound / Outbound Firewall rules.

Program and Application Details

Program Name
This is a friendly name to easily identify the program.

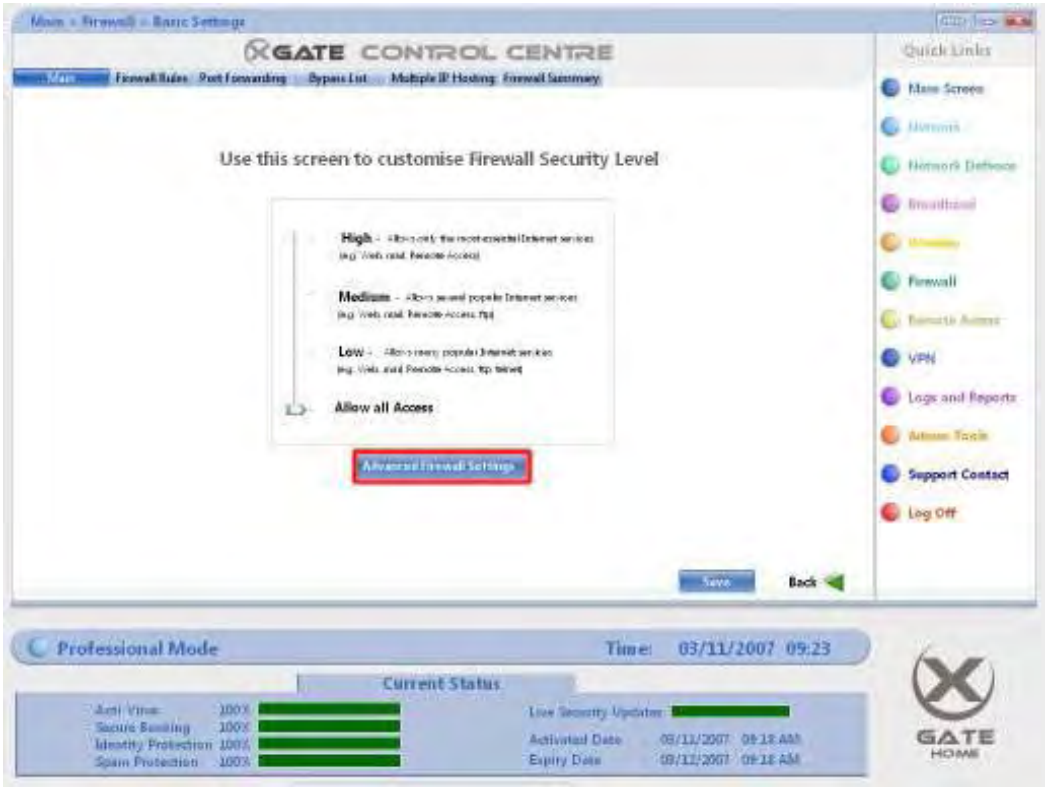
Protocol
TCP is used in the majority of programs. UDP is mostly used in real time programs such as voice communication and games.

Port
You can enter ports and/or port ranges by using commas. E.g. 80, 42000-42800, 42810

Adding a Program or Application

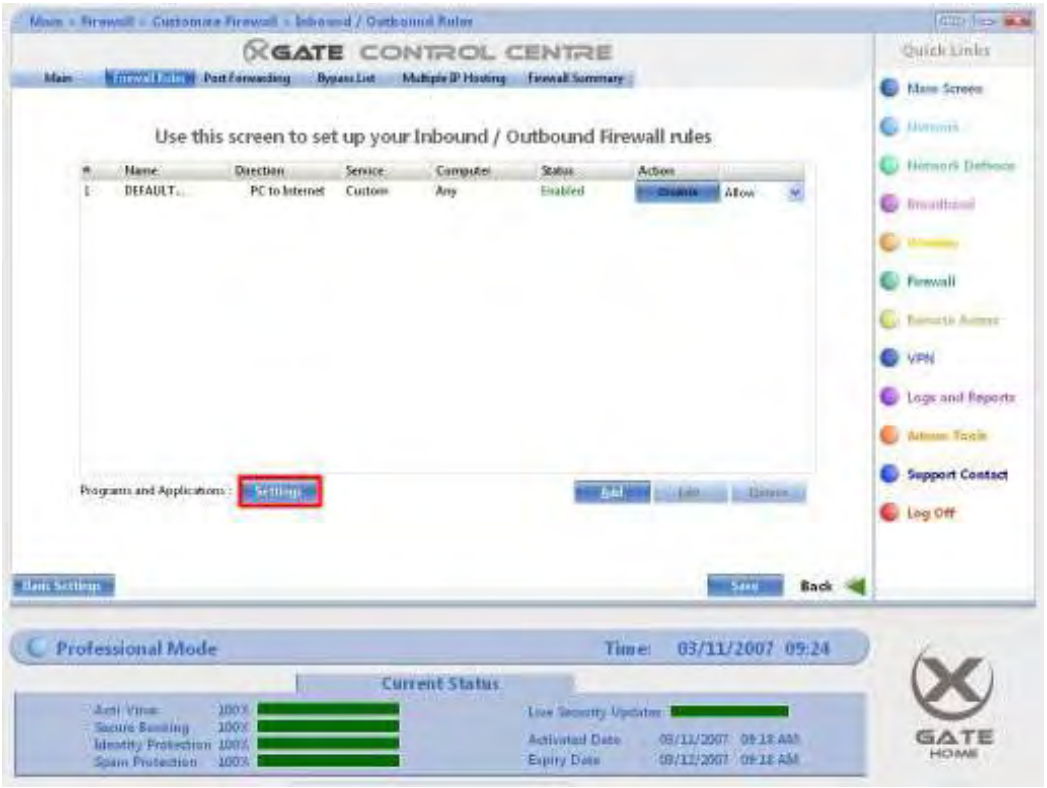
1) Click on Firewall in the Quick Links Menu .

2) Click on the Advanced Firewall Settings button.

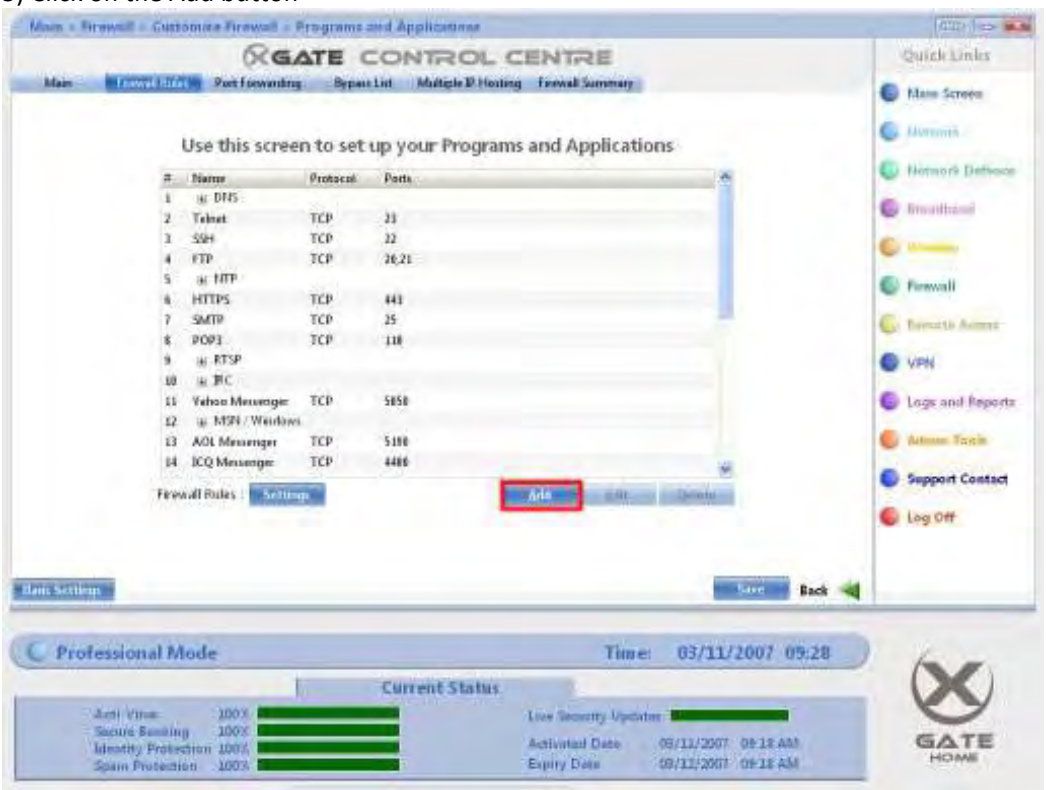


3) Click on the Firewall Rules - Settings button.

4) Click the Programs and Applications - Settings button.



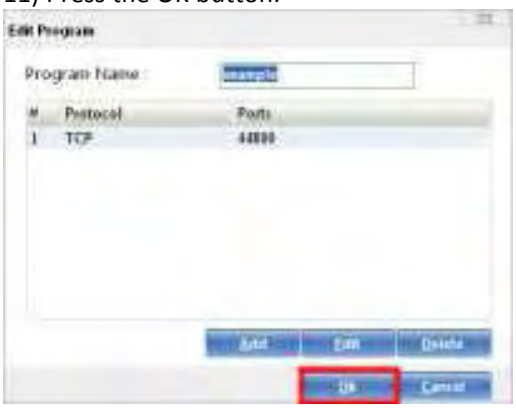
5) Click on the Add button



6) Add a friendly name that will help you easily recognise the collection of ports
7) Press the Add button

8) Select the Protocol.
9) Type in the port or port range.
10) Press the OK button. Repeat steps 7 to 9 until you have added all the ports you need.

11) Press the OK button.



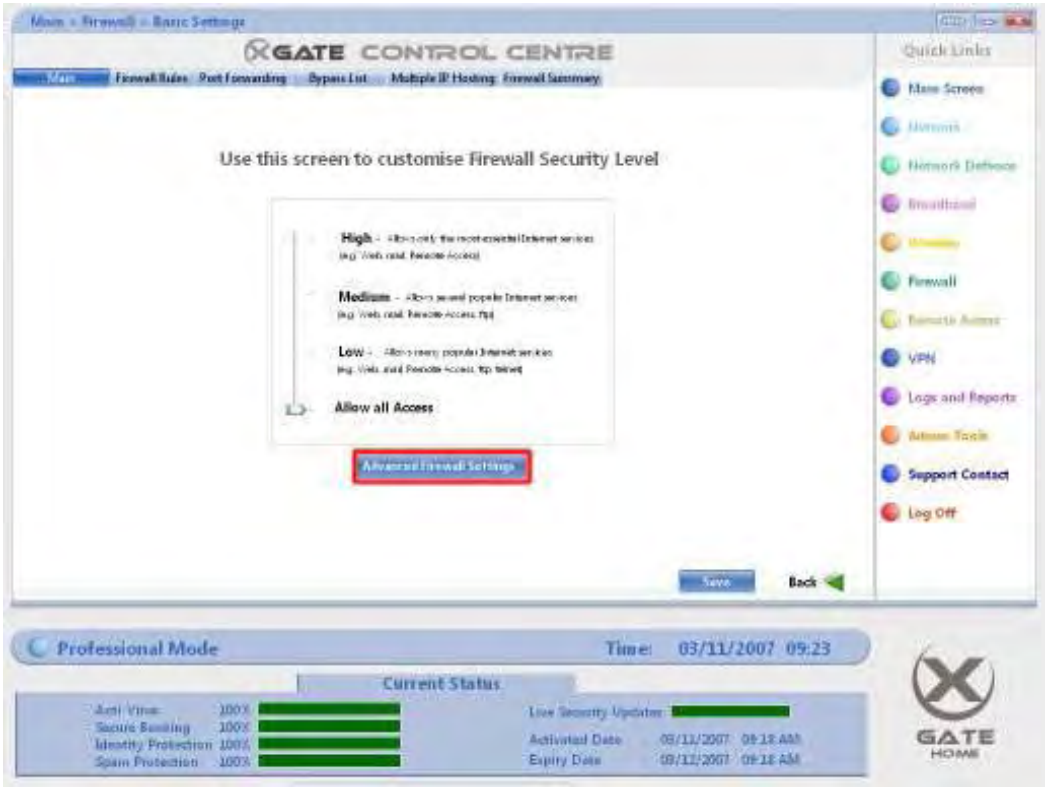
12) Press the Save button.

Now that you have created your own custom Program / Application, you can assign it to Inbound / Outbound rules to have it take effect. For more details on this, go to Adding a Firewall Rule.

Changing the details of a Program or Application

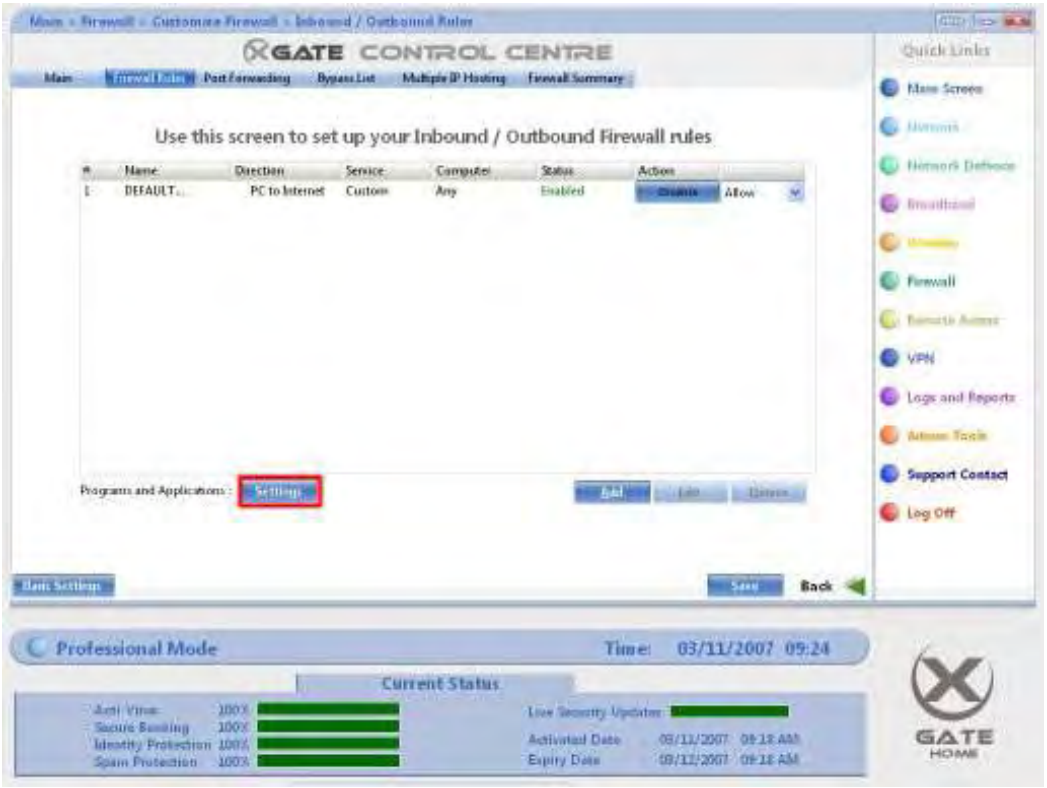
1) Click on Firewall in the Quick Links Menu .

2) Click on the Advanced Firewall Settings button.



3) Click on the Firewall Rules - Settings button.

4) Click the Programs and Applications - Settings button.

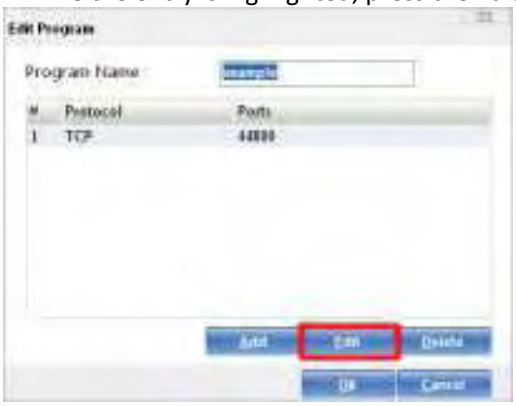


5) Select the entry that you wish to edit by clicking on its name. This will highlight the entry.
6) Press the Edit button.

Adding a set of new ports

See steps 6 to 8 of Adding a Program or Application.

Editing a set of currently existing ports
- Select the entry you wish to edit by single clicking it. This will highlight the entry.
- While the entry is highlighted, press the Edit button.

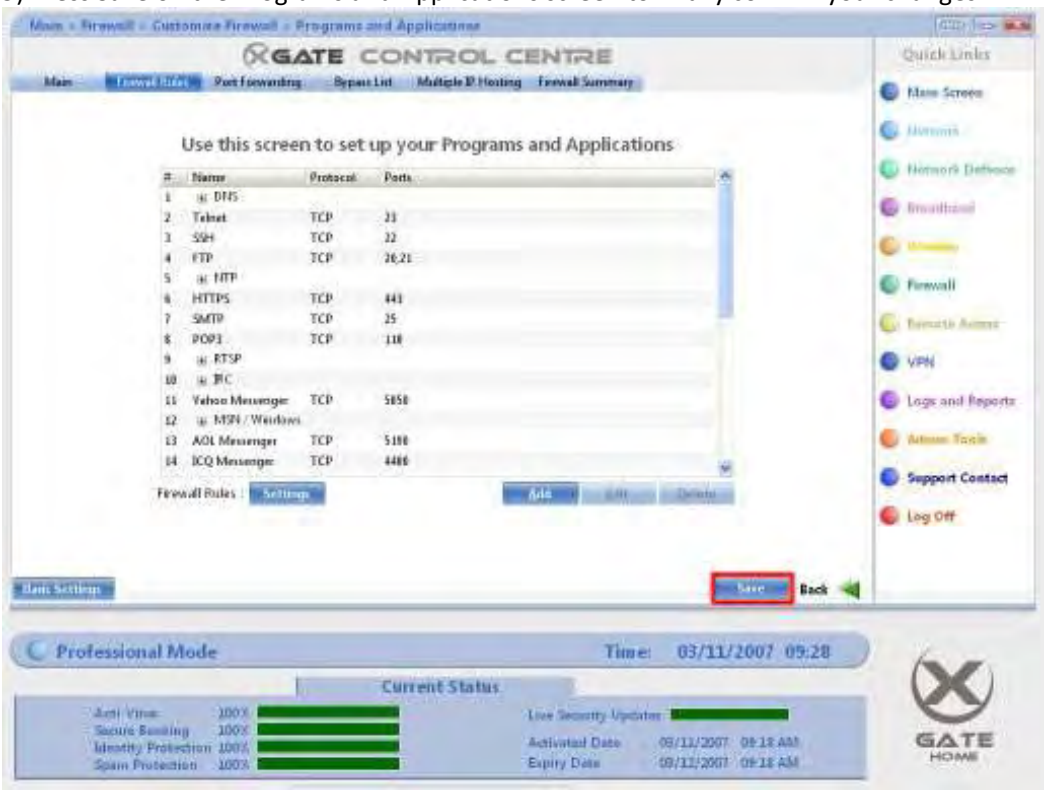


- From the newly opened Edit new Protocol/Port(s) window, you can change the port numbers and protocol.
- Press OK when you are satisfied with your changes.

Removing a set of currently existing ports
- Select the entry you wish to edit by single clicking it. This will highlight the entry.
- While the entry is highlighted, press the Delete button.

8) Once you are satisfied with the changes you have made, press OK on the Edit Program screen.

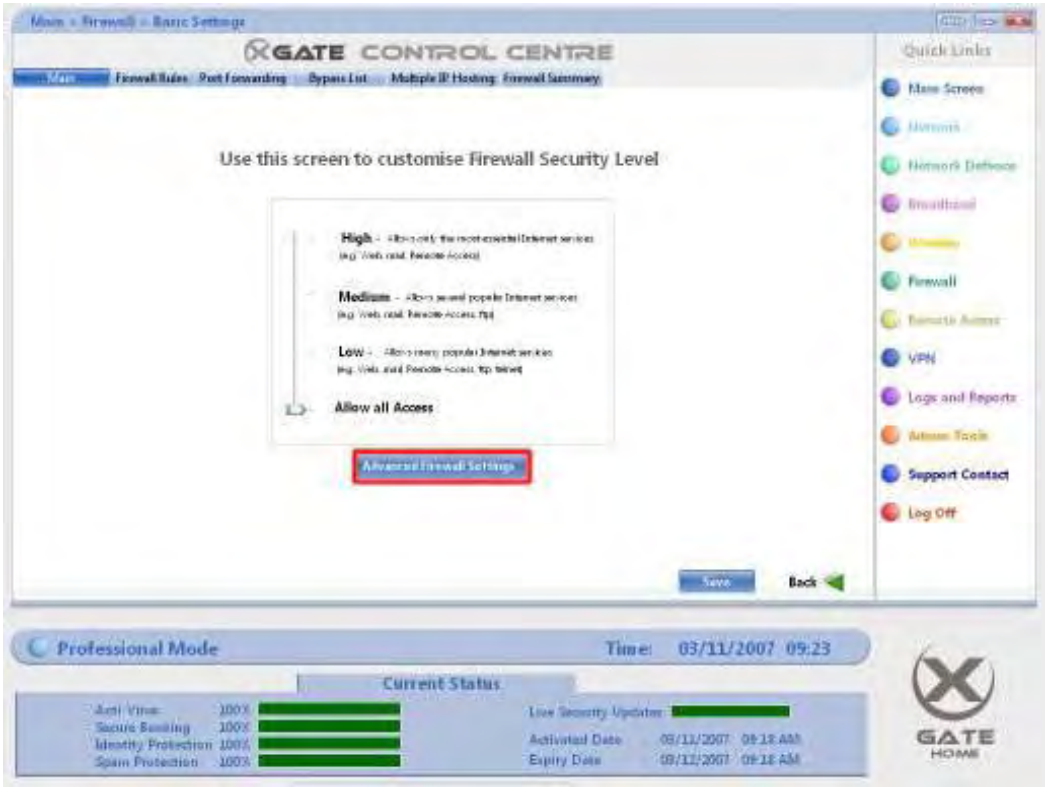
9) Press Save on the Programs and Applications screen to finally confirm your changes.



Removing a Program or Application

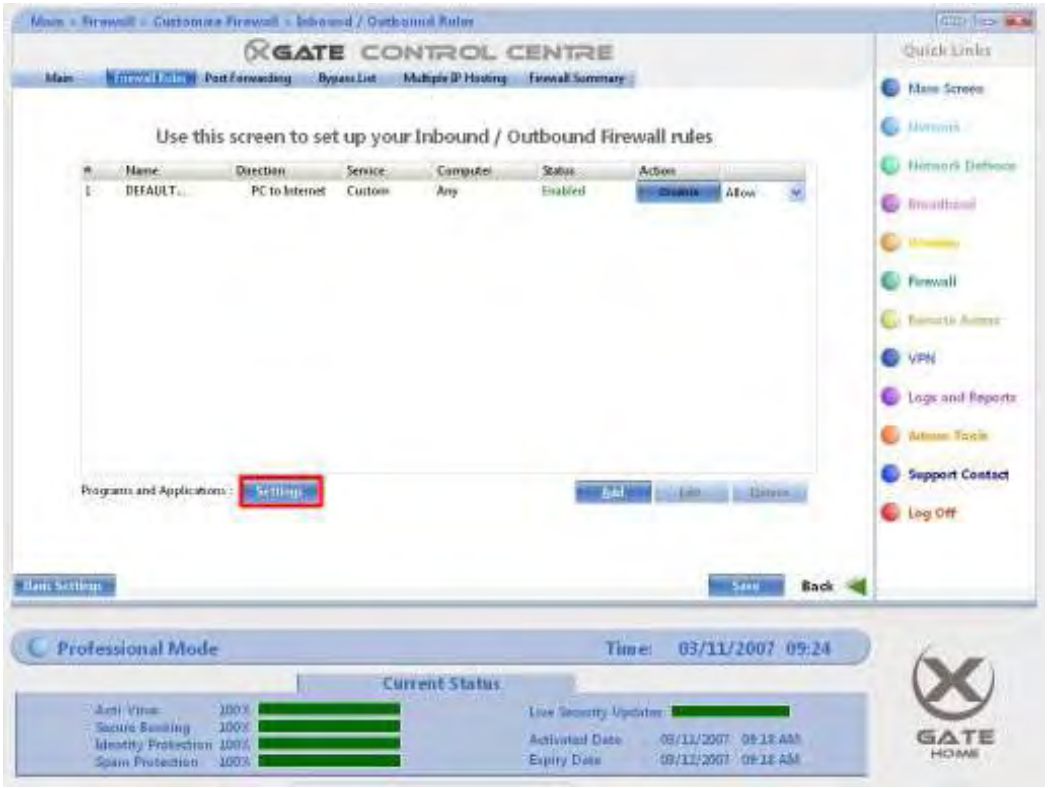
1) Click on Firewall in the Quick Links Menu.

2) Click on the Advanced Firewall Settings button.

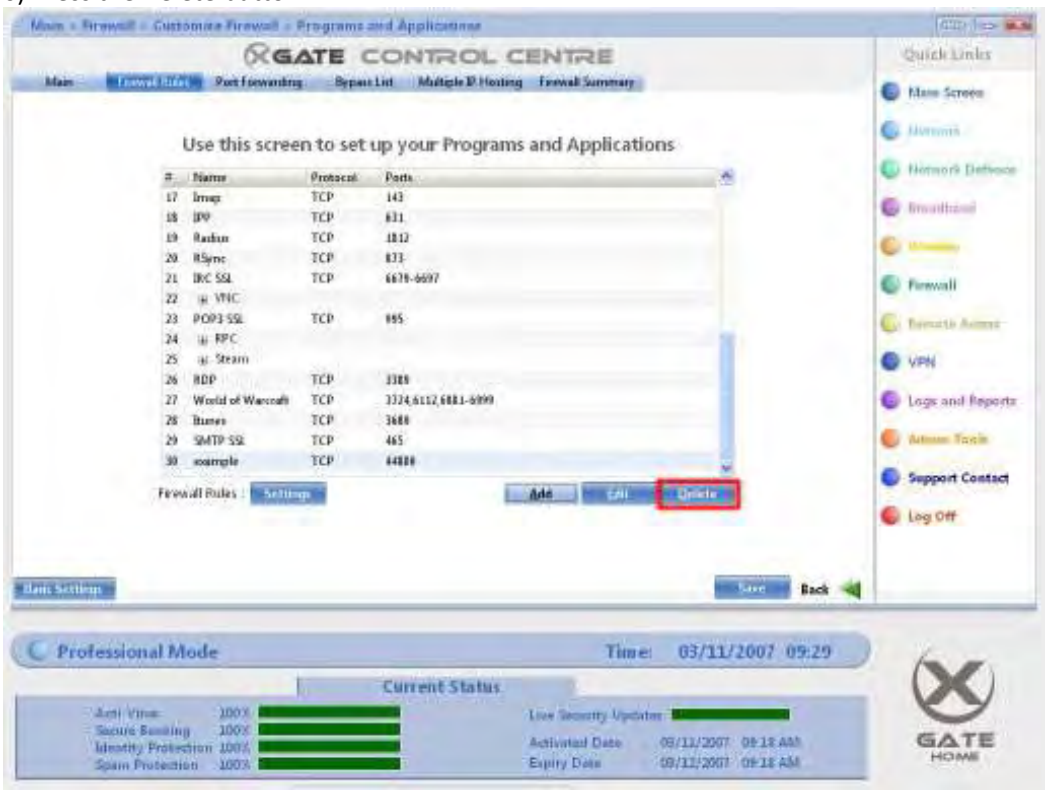


3) Click on the Firewall Rules - Settings button.

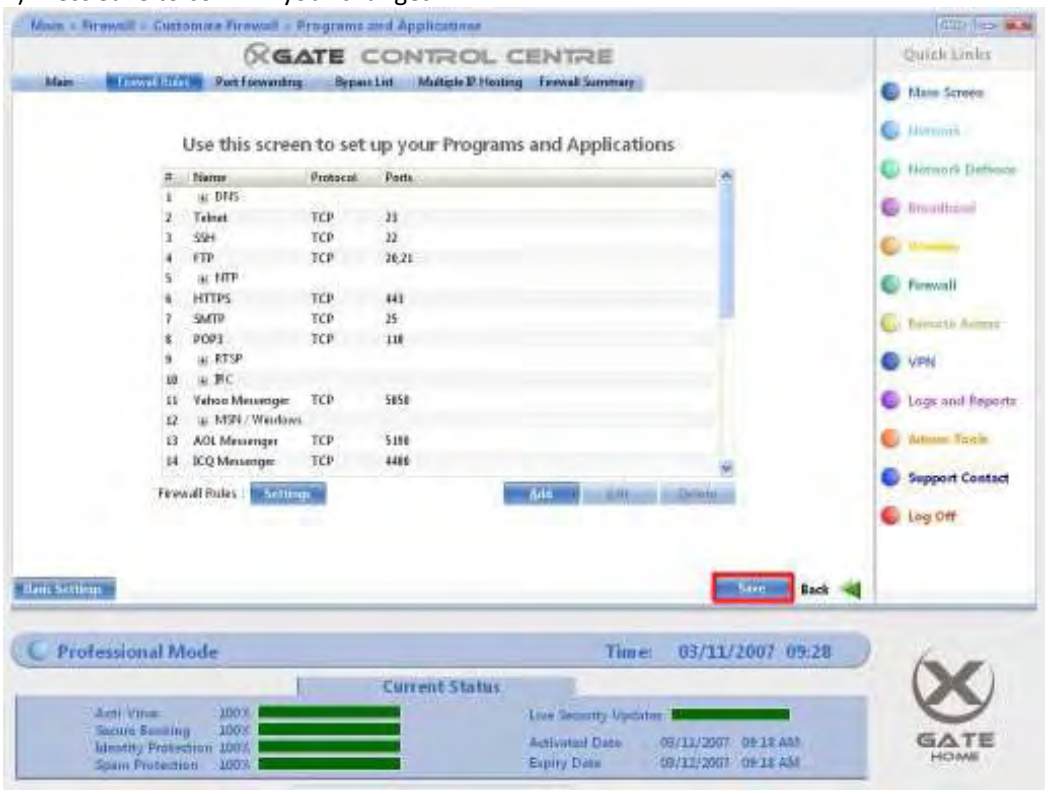
4) Click the Programs and Applications - Settings button.



5) Select the entry that you wish to edit by single clicking on its name. This will highlight the entry.
6) Press the Delete button.



7) Press Save to confirm your changes.



Introduction

Port Forwarding

What is Port Forwarding?

Port Forwarding can also be known as Port Address Translation (PAT). PAT redirects a specified port to a different one.

This may be used, for example, to allow Remote Desktop Protocol (RDP) for more than one external computer. Under normal circumstances, RDP works on only port 3389 and as a result, only one computer can access a computer on the local network at a time. Using Port Forwarding on both the PAT device on the remote side and local side, it is possible to have multiple RDP connections.

Analogy

A Port Forwarding rule is similar to a set of instructions given to a guard (firewall) outside a building (network). When a parcel (data) is sent or received at the building, the guard will look at the parcel and see the name and address (port details). If the name and address match with his instructions, he will direct the parcel to a different door (port).

Port Forwarding Rule Details

Rule Name:
This is a friendly name so you can easily identify the Port Forwarding rule.

Direction:
Either set as Internet to PC (Inbound) or PC to Internet (Outbound). In the majority of scenarios, this should be set to Internet to PC.

Source Port:
This specifies which port the traffic is coming from.

Destination Port:
This specifies which port the traffic is being forwarded to.

From and To:
This specifies the source and destination IP addresses to route the traffic

Action:
The Action you wish to perform based on the details provided above.

Below is a description of how the Port Forwarding Actions affect traffic.

Allow:
This allows the specified traffic.

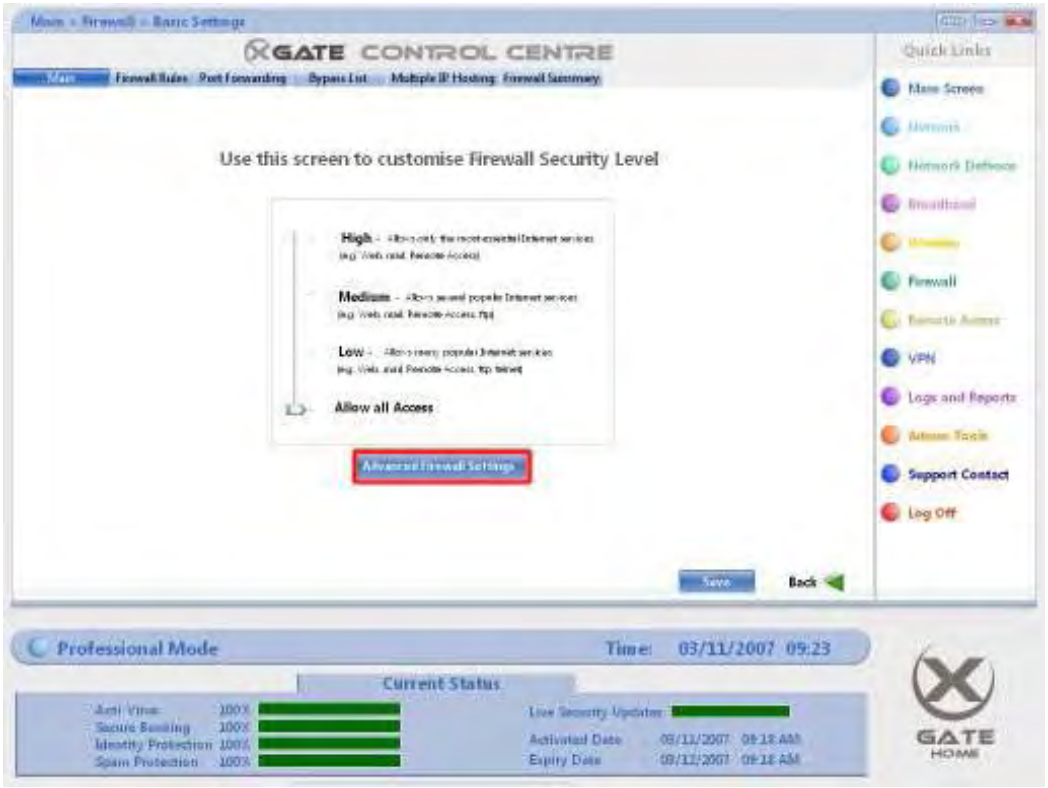
Deny:
Does not allow the specified traffic and will send a response to the other side, saying that the port is closed.

Reject:
Does not allow the specified traffic, and will not send any response back. Sometimes this is referred to as ‘Stealth’.

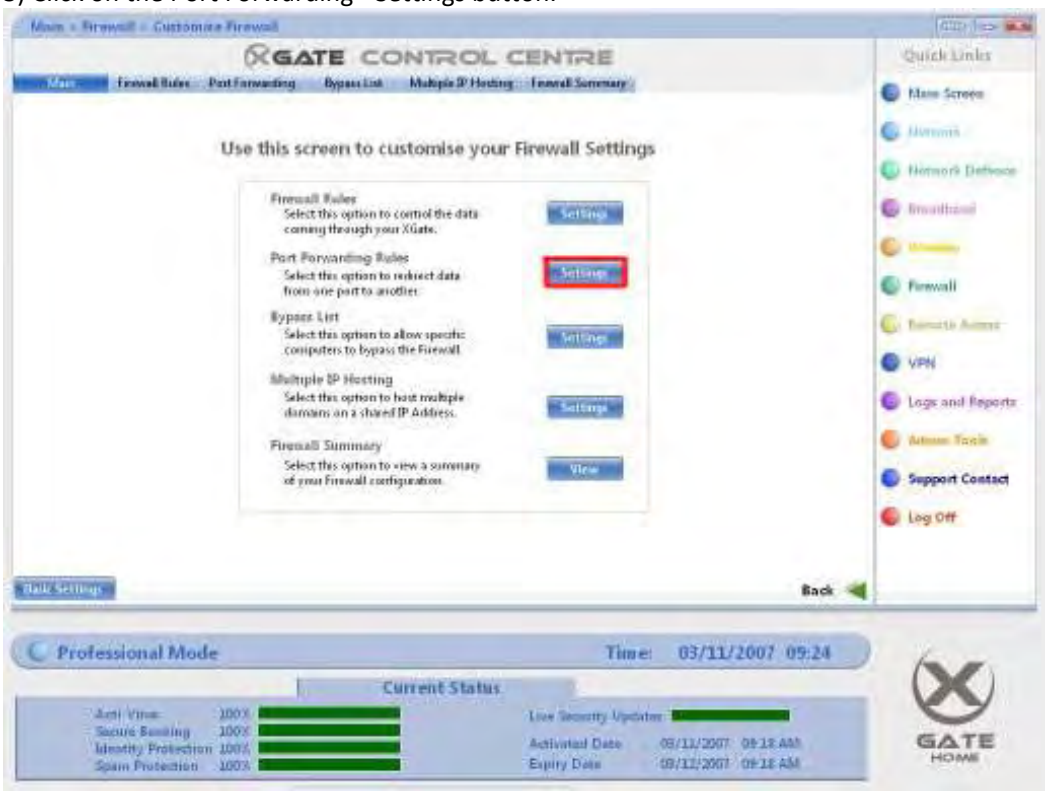
Adding a Port Forwarding Rule

1) Click on Firewall in the Quick Links Menu.

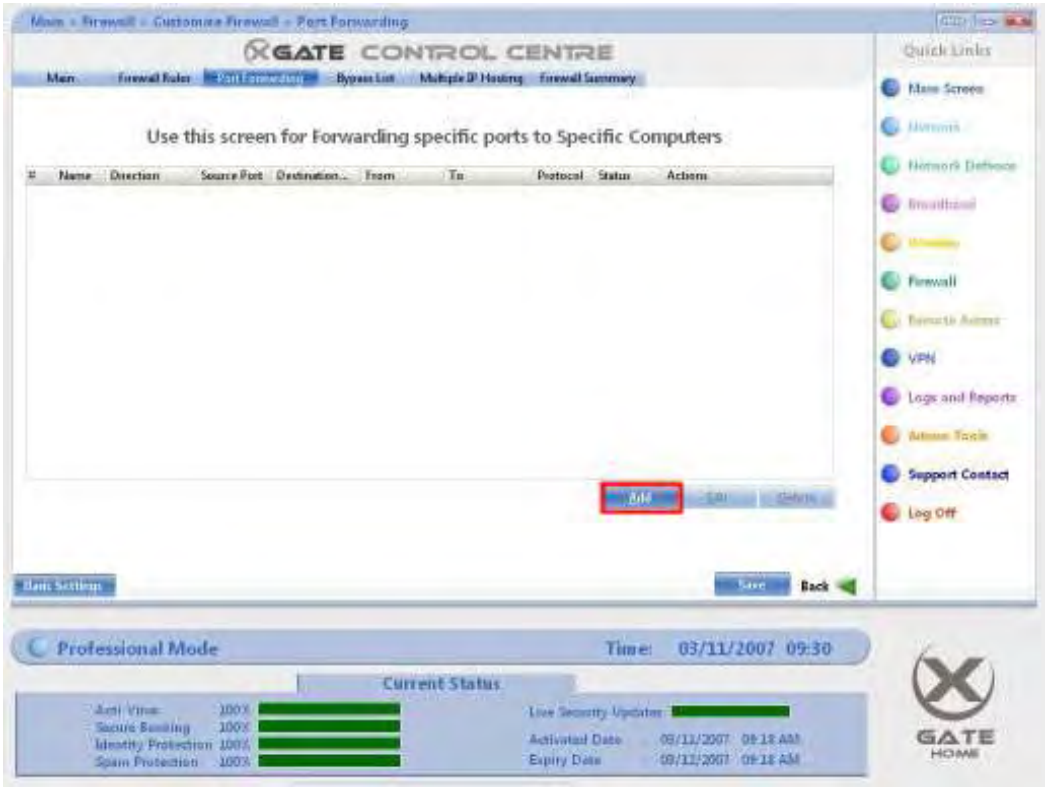
2) Click on the Advanced Firewall Settings button.



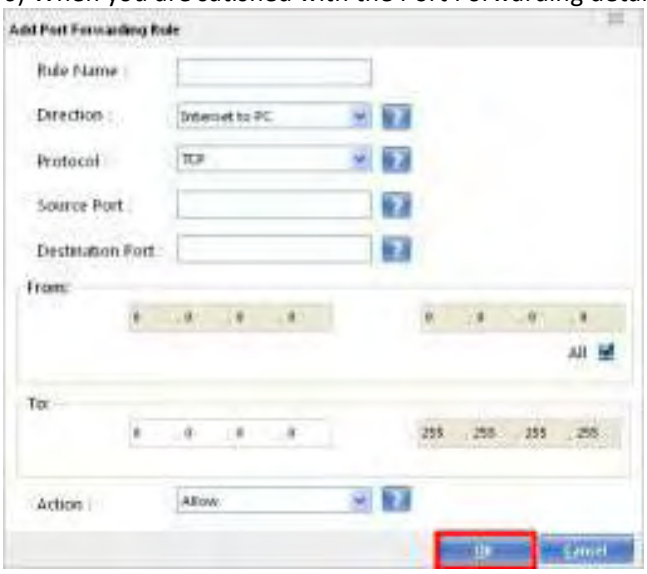
3) Click on the Port Forwarding - Settings button.



4) Click the Add button.



5) Enter your Port Forwarding details.
6) When you are satisfied with the Port Forwarding details, press the OK button.



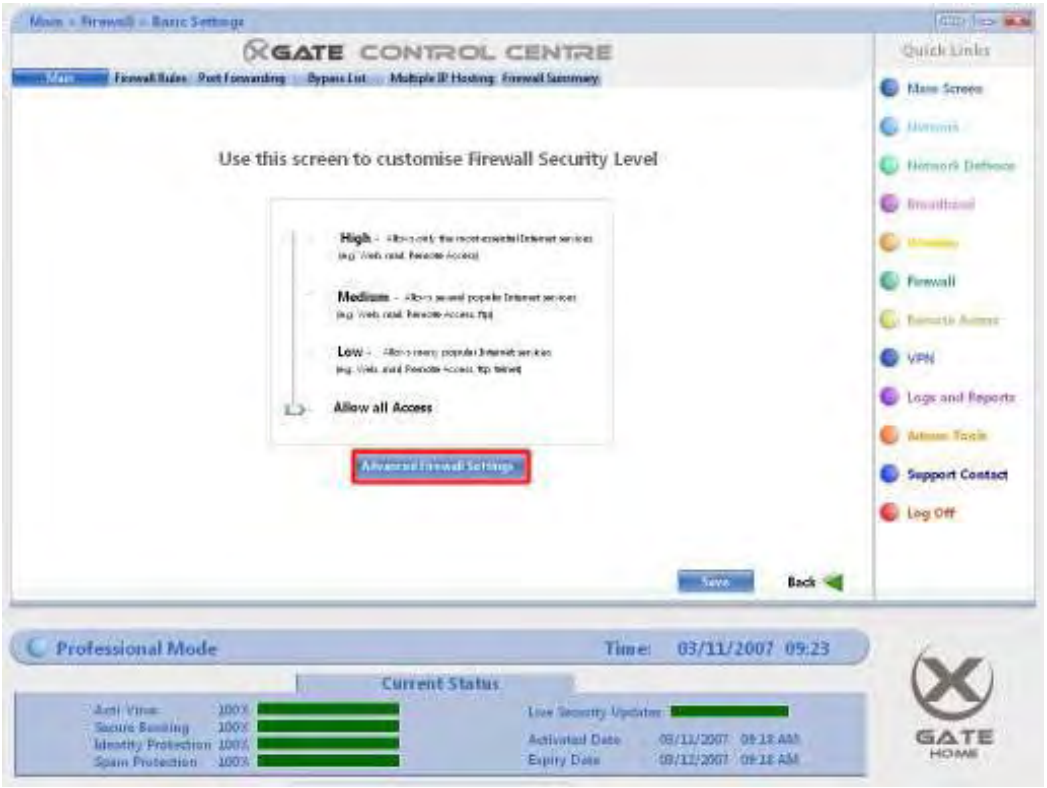
7) Click the Save button on the Port Forwarding Rules.


GATE CONTROL CENTRE
Quick Links
Use this screen for Forwarding specific ports to Specific Computers
Firewall
VPN
Logs and Reports
Support Contact
Log Off
Back
Professional Mode
Time: 03/11/2007 09:31
Current Status
GATE
HOME

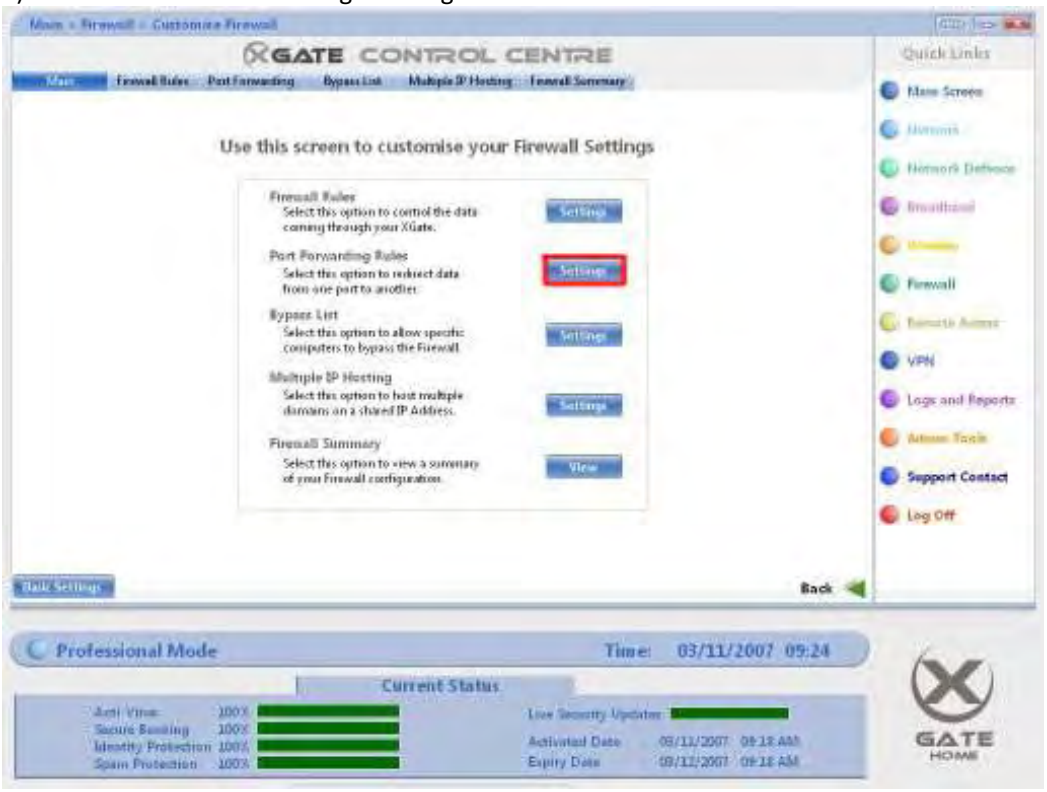
Changing the details of a Port Forwarding Rule

1) Click on Firewall in the Quick Links Menu.

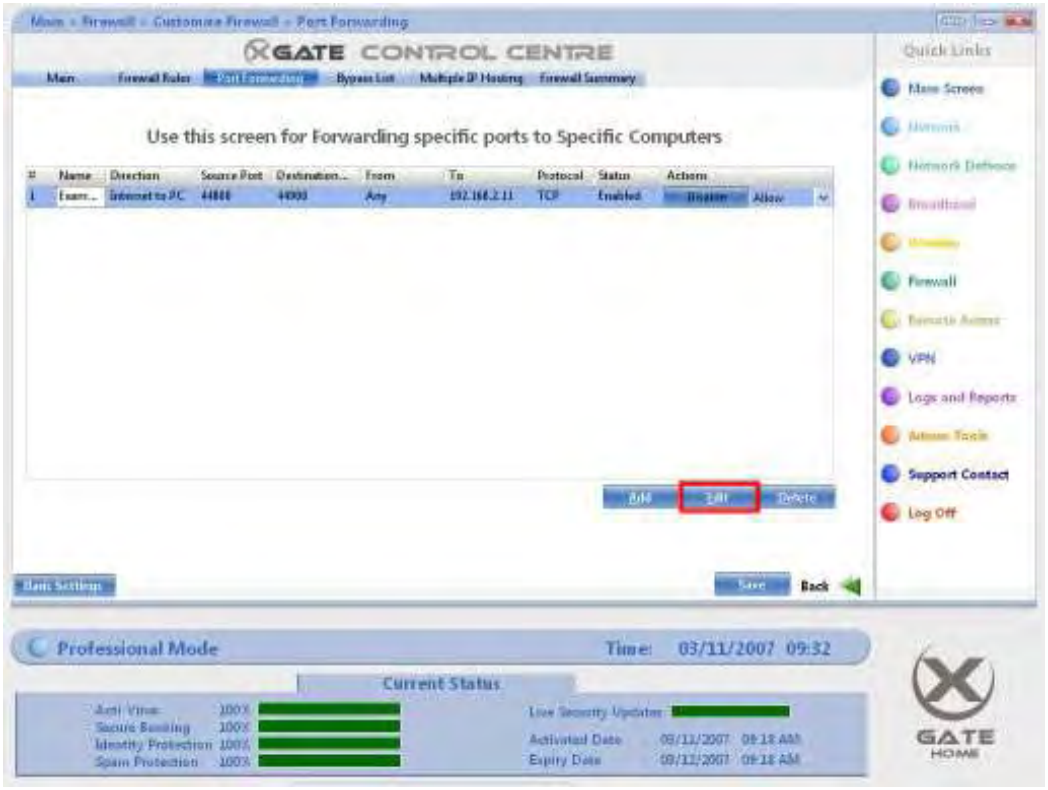
2) Click on the Advanced Firewall Settings button.



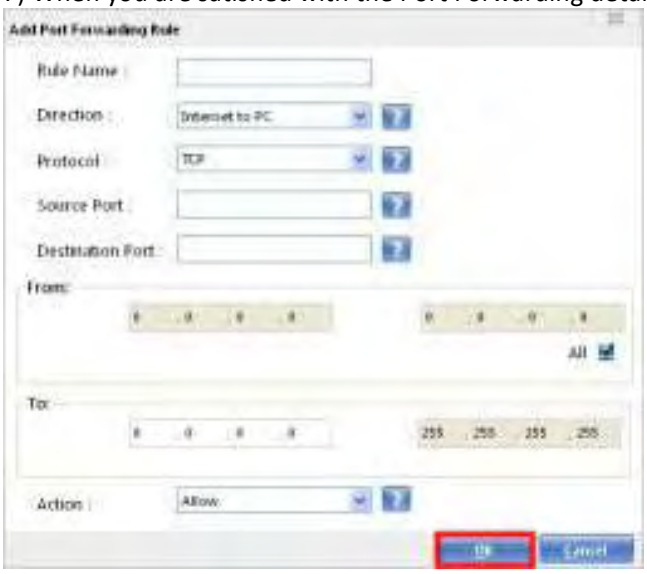
3) Click on the Port Forwarding - Settings button.



4) Select the entry that you wish to edit by clicking on its name. This will highlight the entry.
5) Press the Edit button.



6) Change your Port Forwarding details.
7) When you are satisfied with the Port Forwarding details, press the OK button.



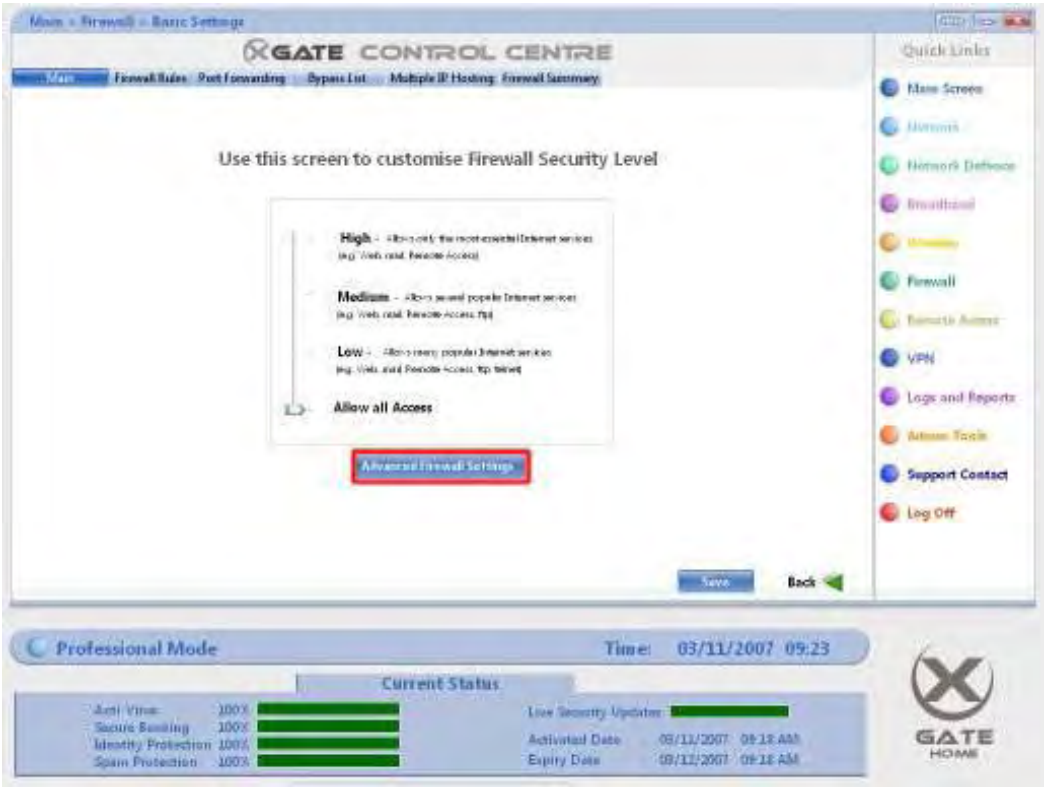
8) Click the Save button on the Port Forwarding Rules screen.


GATE CONTROL CENTRE
Main
Firewall Rules
Port Forwarding
Bypass List
Multiple IP Hosting
Firewall Summary
Use this screen for Forwarding specific ports to Specific Computers
Quick Links
Main Screen
Firewall
VPN
Logs and Reports
Support Contact
Log Off
Save
Back
Professional Mode
Time: 03/11/2007 09:32
Current Status
Anti Virus 100%
Secure Banking 100%
Identity Protection 100%
Spam Protection 100%
GATE HOME

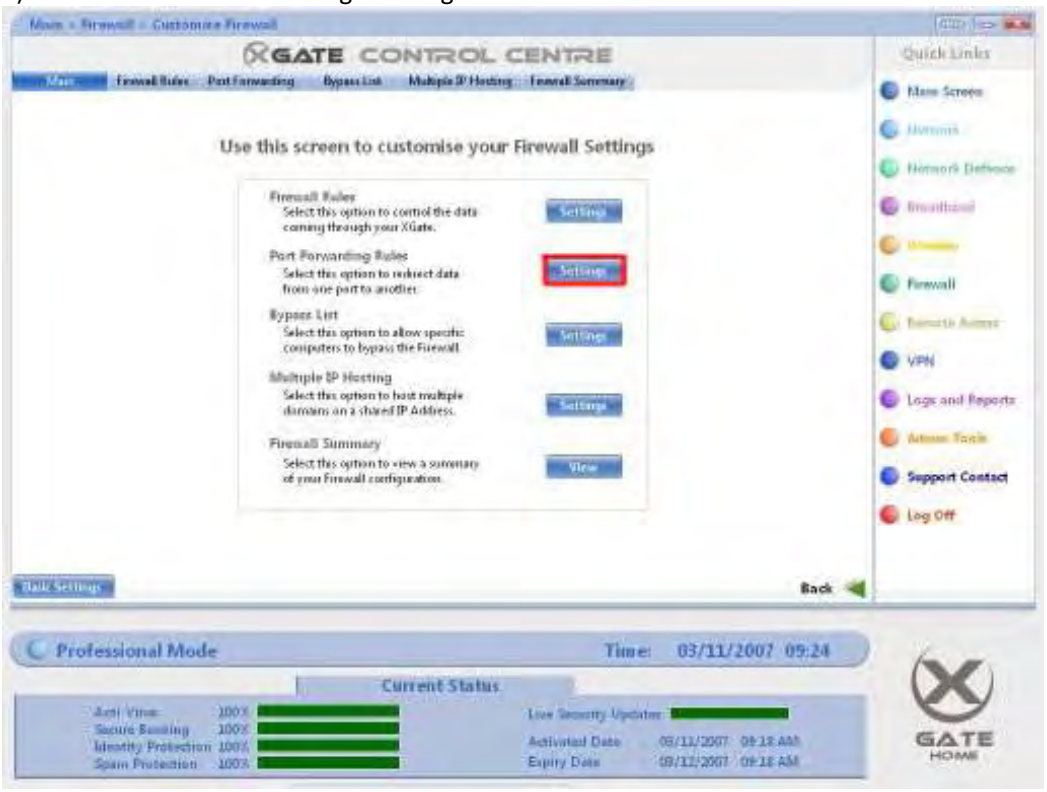
Removing a Port Forwarding Rule

1) Click on Firewall in the Quick Links Menu.

2) Click on the Advanced Firewall Settings button.

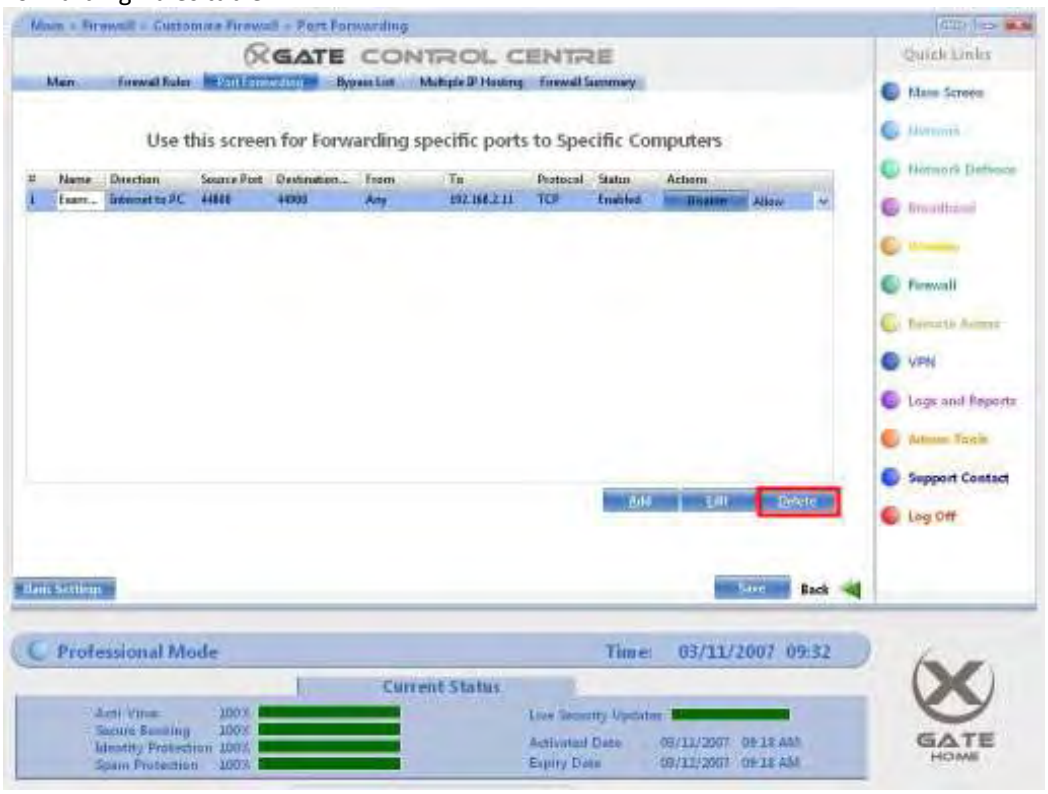


3) Click on the Port Forwarding - Settings button.

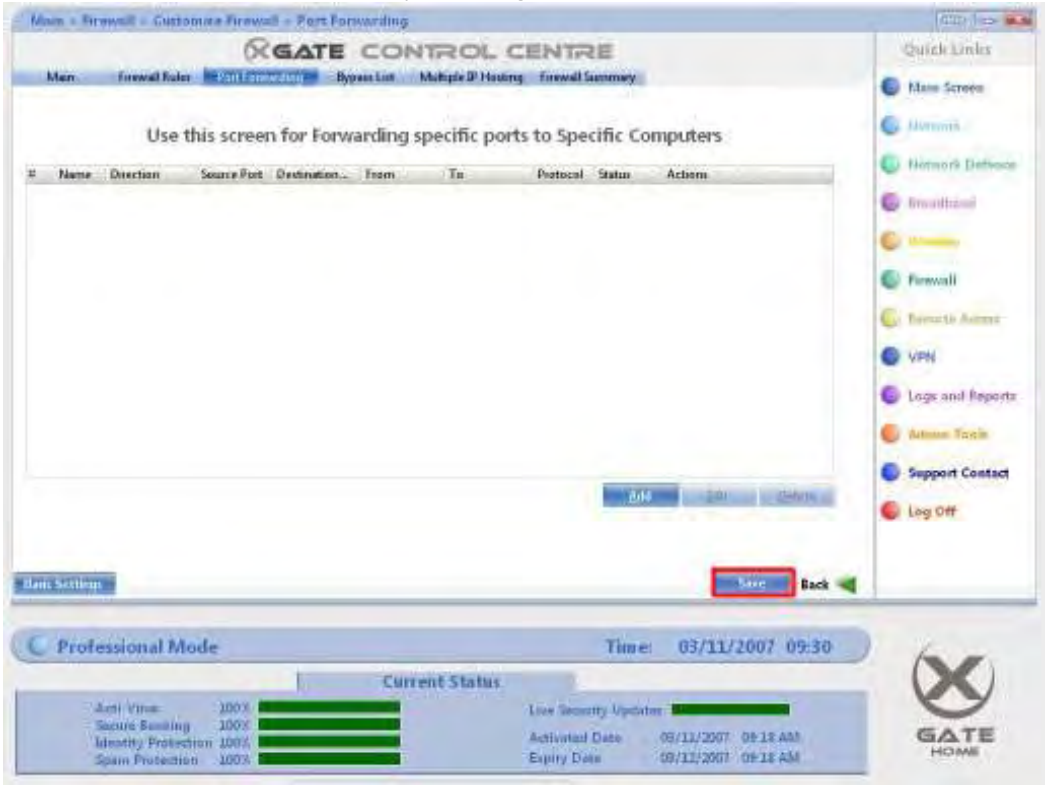


4) Select the entry that you wish to edit by clicking on its name. This will highlight the entry.
5) Press the Delete button. The selected entry will have been removed from the Port

Forwarding Rules table.



6) Click the Save button to confirm your changes.



Introduction

Firewall Bypass List

What is a Bypass List?

The Firewall Bypass List allows selected computers to pass through XGate's Firewall, unaffected by the Firewall Rules.

Analogy

A bypass list is similar to a set of instructions given to a guard (the firewall) outside a building (network). These instructions tell the guard which people (computers) are allowed access to the building without any inspection.

Bypass List Details

A Bypass List entry should contain the following details

Name:
This is a friendly name so you can easily identify a bypass list entry

IP Address:
The IP address of the computer you want to bypass the Firewall.

Subnet Mask:
The Subnet Mask of the computer you want to bypass the Firewall.

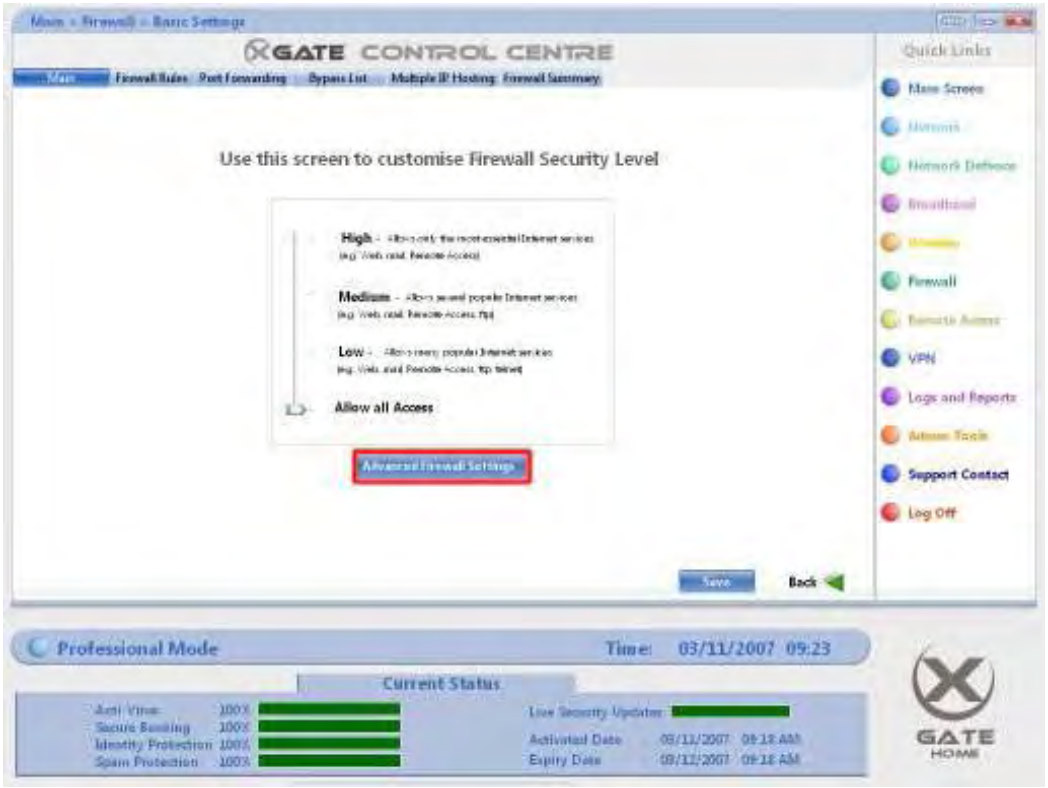
To find out the IP Address and Subnet Mask of a computer please look at “How do I find out a computer’s IP Address and Subnet Mask?” in the FAQs section.

Adding a computer to the Firewall Bypass List

Adding a computer to the Firewall Bypass List

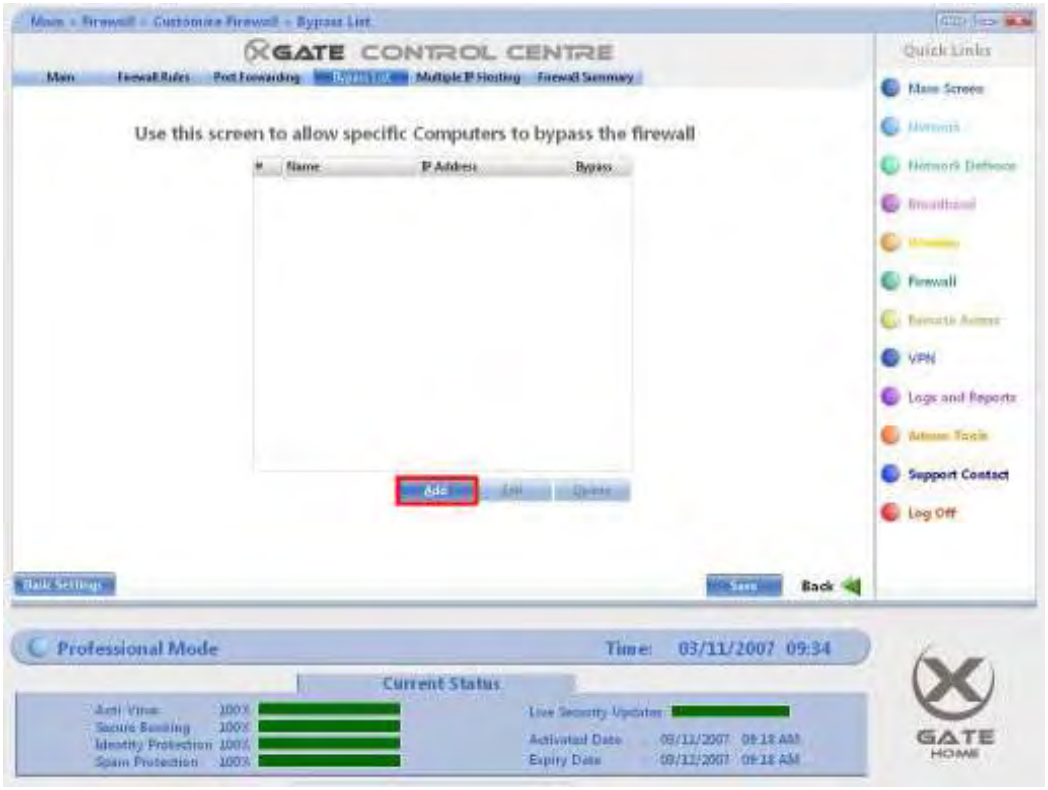
1) Click on Firewall in the Quick Links Menu.

2) Click on Advanced Firewall Settings.



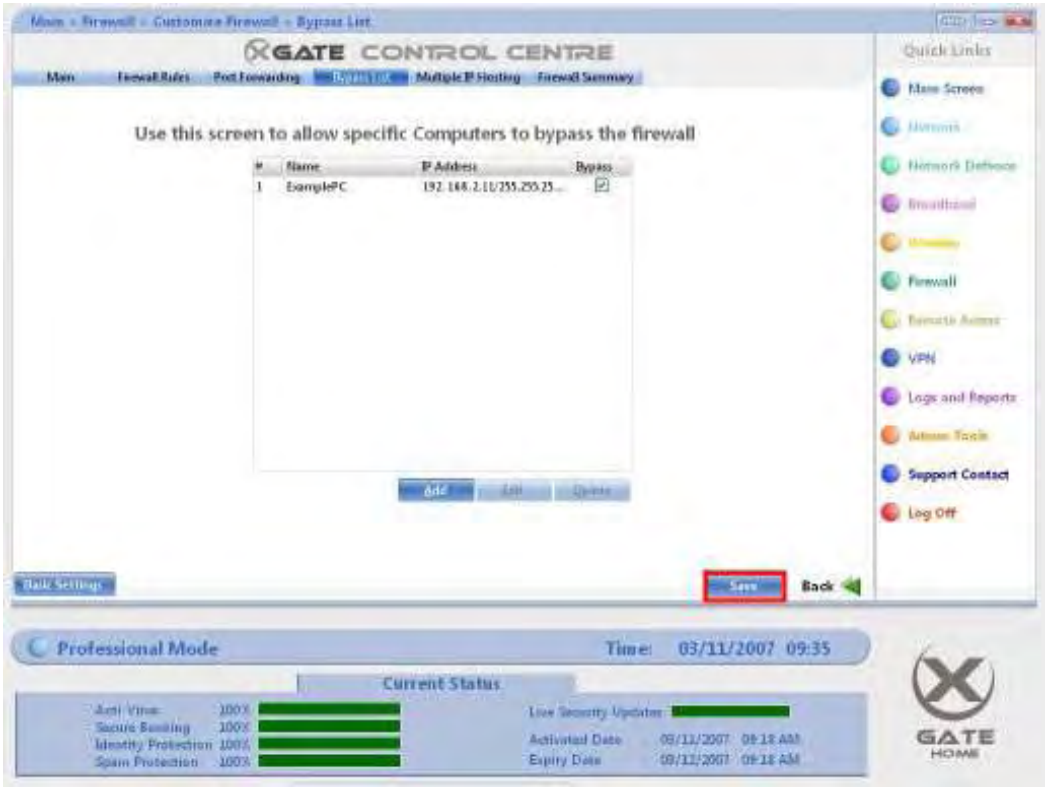
3) Click on the Bypass List - Settings button.

4) Press the Add button.



5) Enter the details of the computer you wish to add to the Bypass list in the text boxes provided.
6) Press the OK button when you have completed the computer's details.

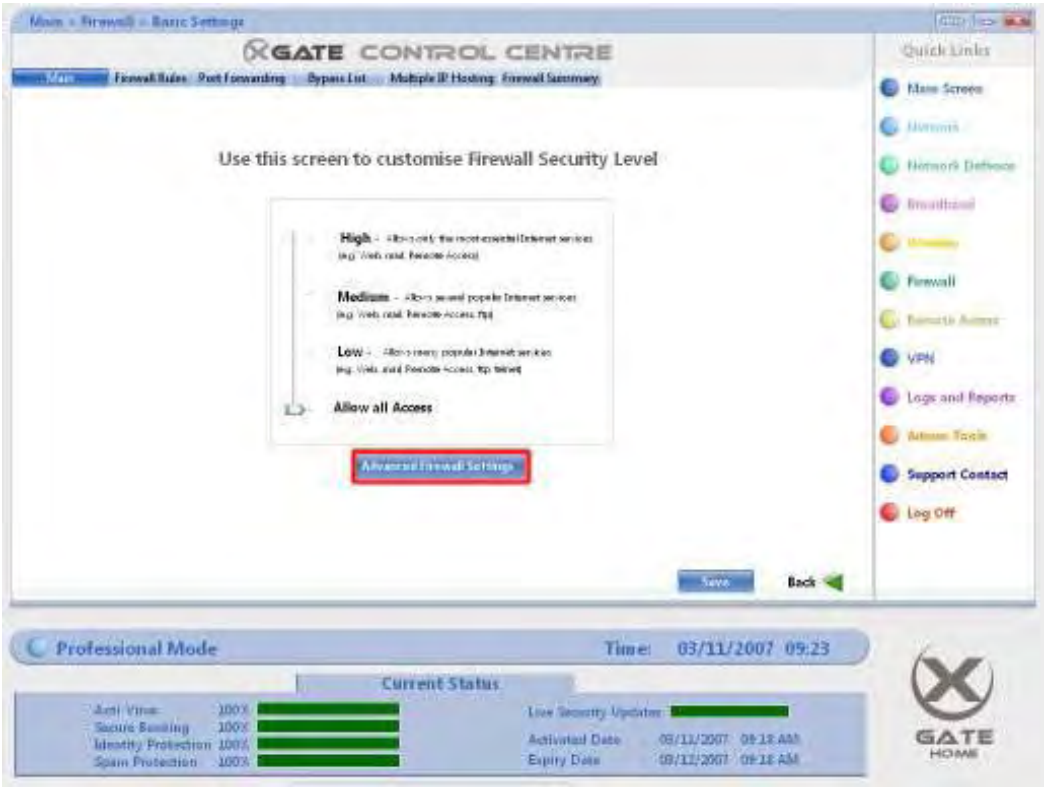
7) Press the Save button.


GATE CONTROL CENTRE
Main
Firewall Rules
Port Forwarding
Multiple IP Hosting
Firewall Summary
Use this screen to allow specific Computers to bypass the firewall
#
Name
IP Address
Bypass
1
ExamplePC
Add
Edit
Delete
Back
Quick Links
Main Screen
Network Defence
Broadband
Firewall
VPN
Logs and Reports
Support Contact
Log Off
Professional Mode
Time: 03/11/2007 09:35
Current Status
Anti-Virus 100%
Secure Banking 100%
Identity Protection 100%
Spam Protection 100%
Activated Date 03/11/2007 09:18 AM
Expiry Date 03/11/2007 09:18 AM
GATE
HOME

Changing the details of a Bypassed Computer

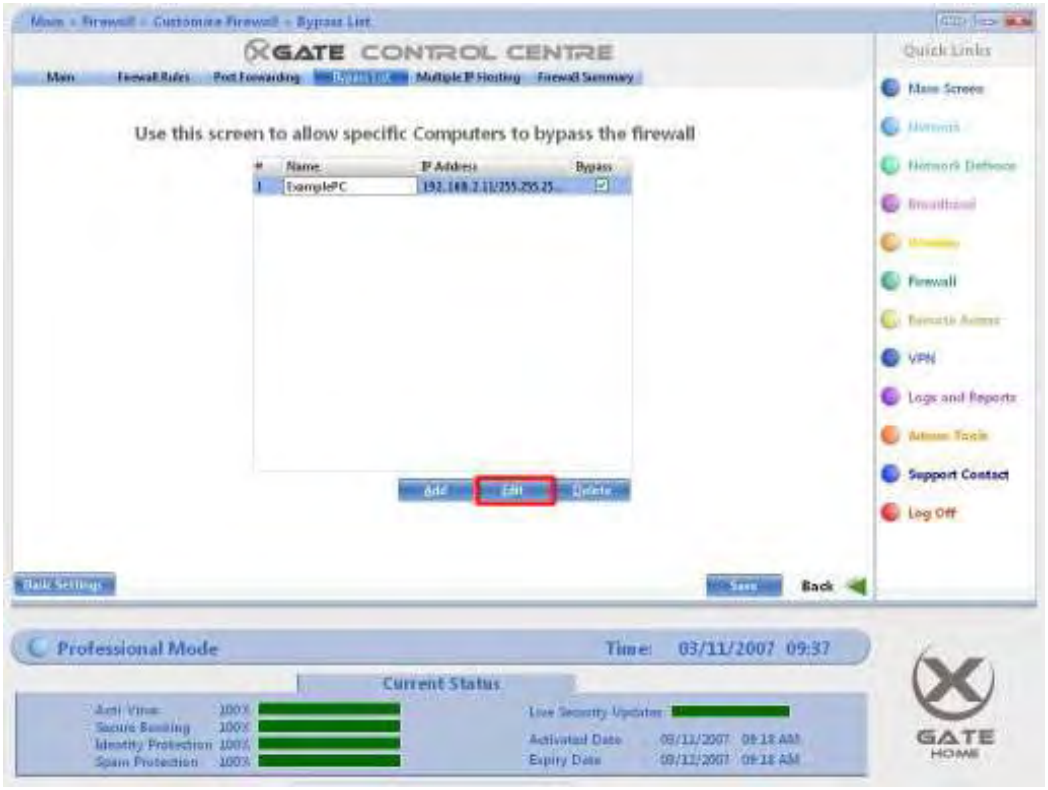
1) Click on Firewall in the Quick Links Menu.

2) Click on Advanced Firewall Settings.



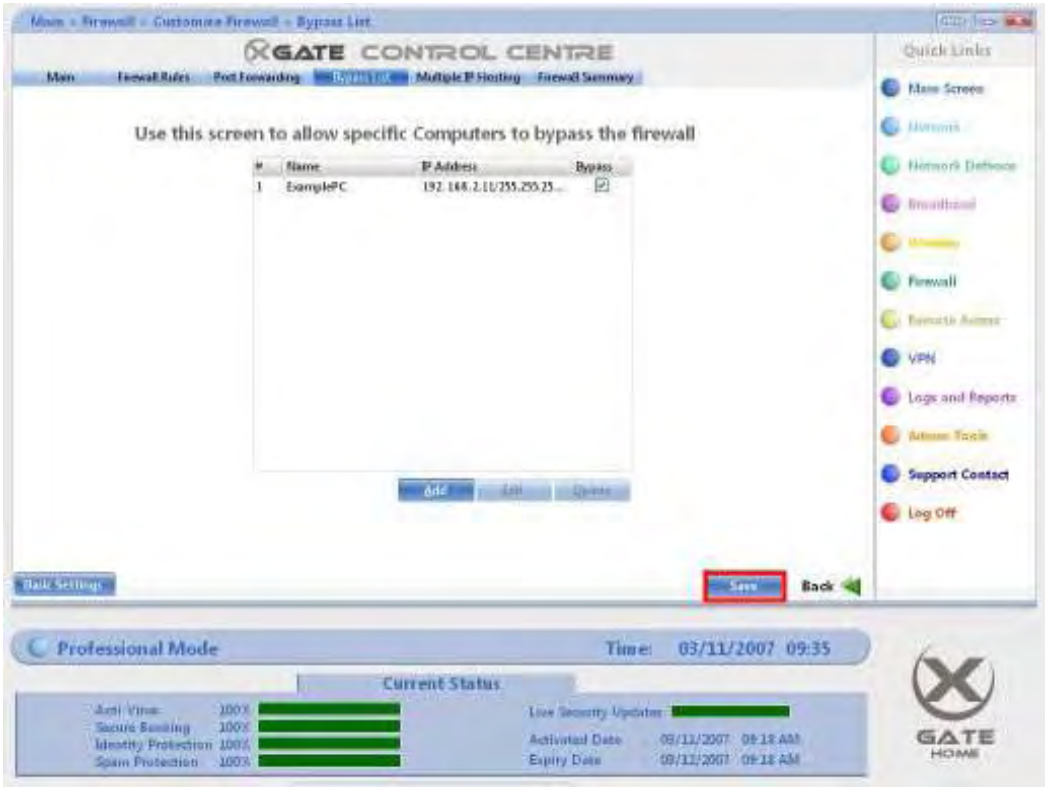
3) Click on the Bypass List - Settings button.

4) Select the entry that you wish to edit by clicking on its name. This will highlight the entry.
5) Press the Edit button.



6) Change the details of the computer.
7) Press the OK button when you have finished changing the computer's details.

8) Press the Save button.

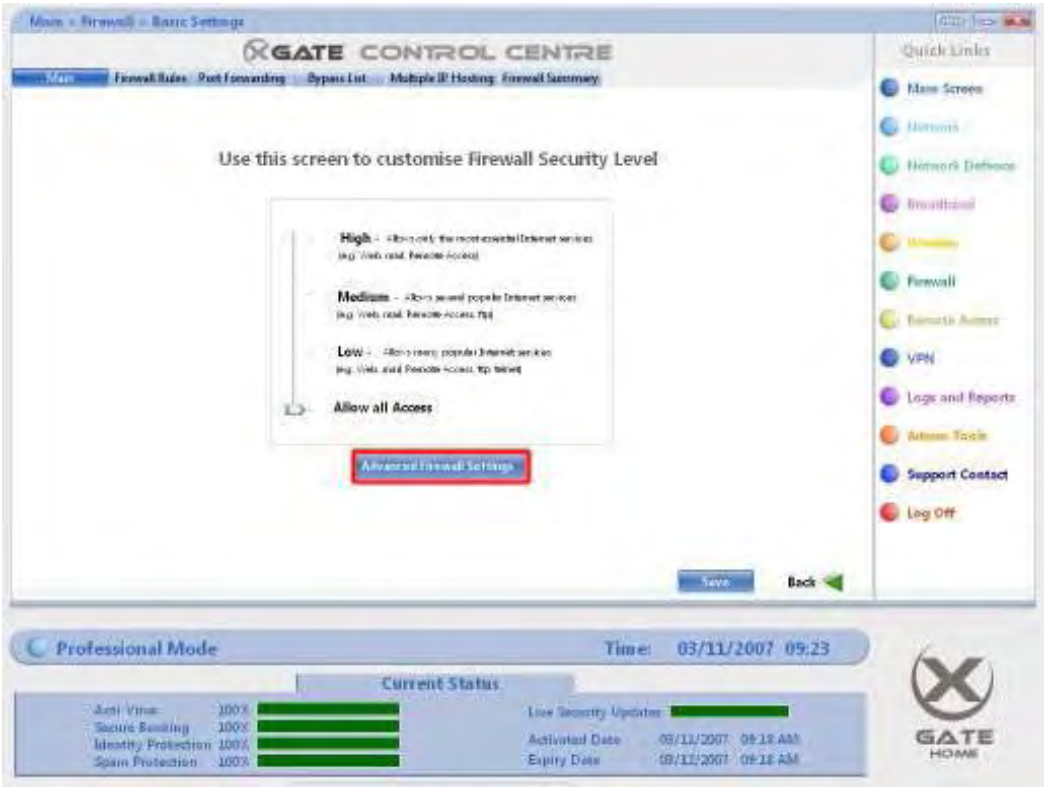

GATE CONTROL CENTRE
Main
Firewall Rules
Port Forwarding
Multiple IP Hosting
Firewall Summary
Use this screen to allow specific Computers to bypass the firewall
#
Name
IP Address
Bypass
1
ExamplePC
Add
Edit
Delete
Back
Quick Links
Main Screen
Network Defence
Broadband
Firewall
VPN
Logs and Reports
Support Contact
Log Off
Professional Mode
Time: 03/11/2007 09:35
Current Status
Anti-Virus 100%
Secure Banking 100%
Identity Protection 100%
Spam Protection 100%
Activated Date 03/11/2007 09:18 AM
Expiry Date 03/11/2007 09:18 AM
GATE
HOME

Removing a computer from the Bypass List

Removing a computer from the Bypass List

1) Click on Firewall in the Quick Links Menu.

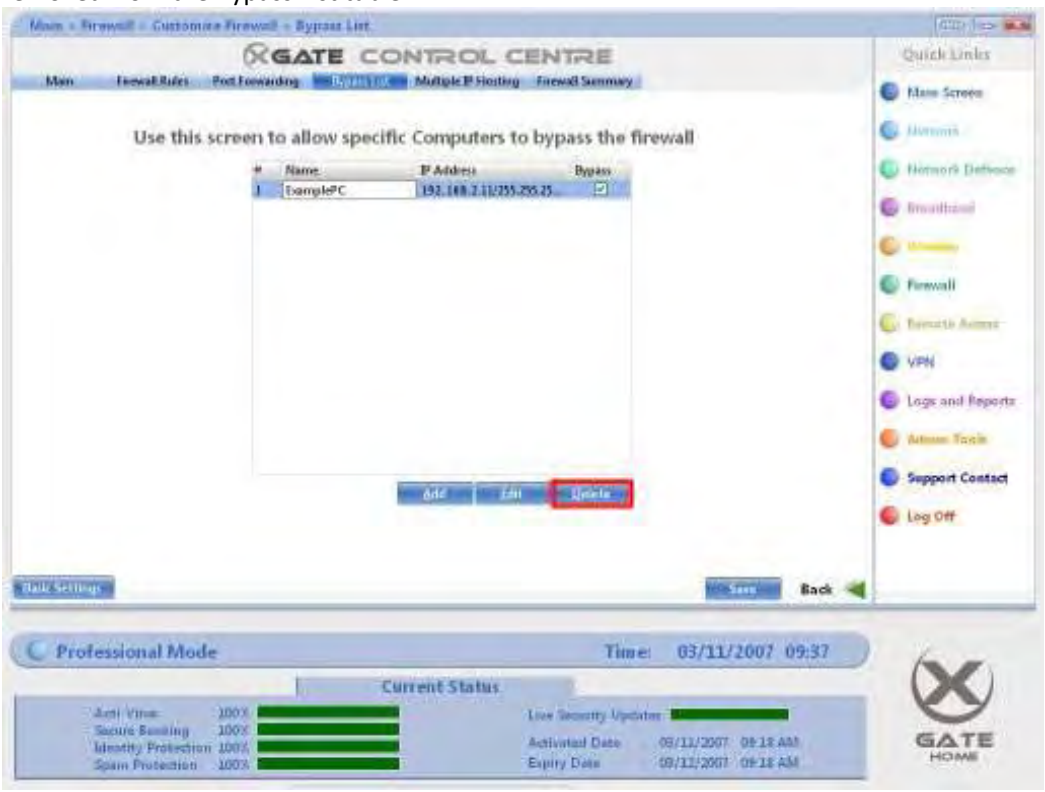
2) Click on Advanced Firewall Settings.



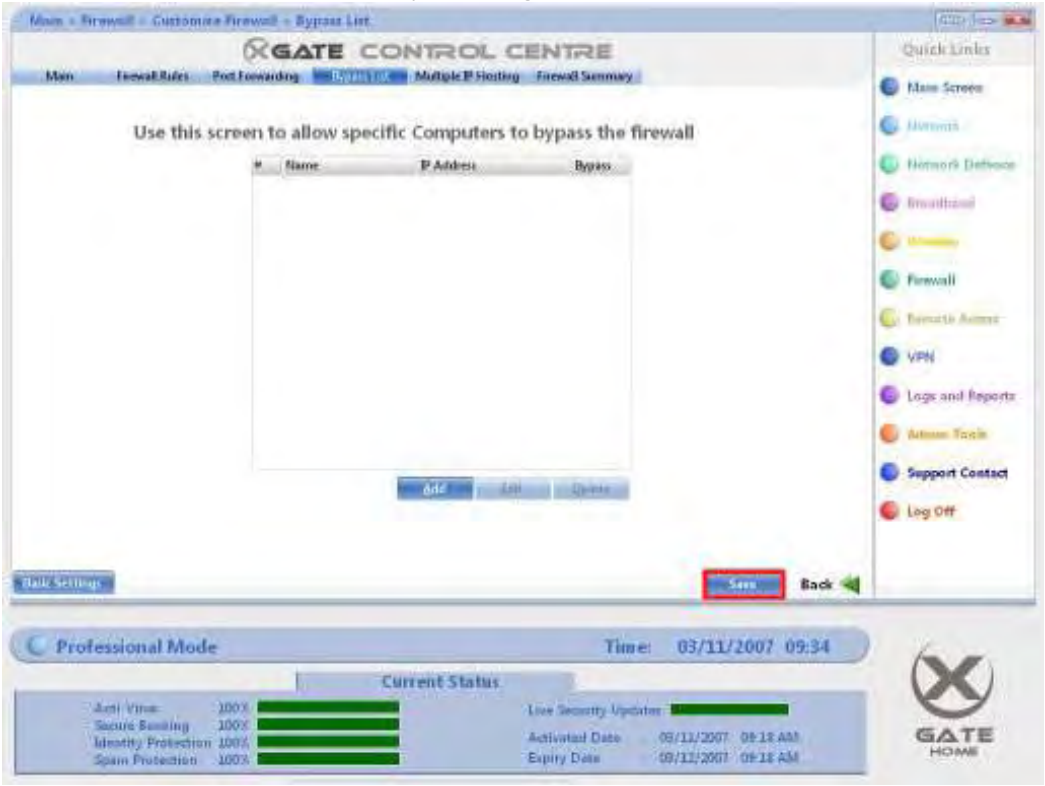
3) Click on the Bypass List - Settings button.

4) Select the entry that you wish to edit by clicking on its name. This will highlight the entry.
5) While the entry is highlighted, press the Delete button. The selected entry will be

removed from the Bypass List table.



6) Press the Save button to confirm your changes.



Introduction

Multiple IP Hosting

What is Multiple IP Hosting?

Multiple IP Hosting allows you to host multiple domains under a shared IP Address. This feature is also known as Virtual Hosting.

This may be useful if you wish to host multiple web services on that computer. For example, you may wish to run two websites from one server.

You can host two types of Virtual hosted servers: Public and Private.

A Public Server is one that is accessible through the Internet while a Private Server is one only accessible through your Local Network. Please note that by configuring and publishing a Private Server, you are giving it public access via the Internet.

Analogy

You could compare the process of Multiple IP addresses as a house (server) which has 2 addresses (IP Addresses). For example, 45 Example Road is the address of the house. However, you decide to split the house into 2 separate flats. One flat will now be 45a Example Road and the other will be 45b Example Road although both are still 45 Example road.

Multiple IP Host Details

To configure a Private Server, you must provide the following details:

Server Name:
This is a friendly name for you to easily identify the Server.

Server Private IP Address:
The current LAN IP address of the Private Server

Mapped Public IP Address:
The new Public Address that you will give to the Private Server.

Mapped Public Subnet:
This is the new public subnet mask that you will give to the Private Server.

To configure a Public Server, you must provide the following details:

Server Name:
This is a friendly name for you to easily identify the Server.

Public IP Address:
Public IP Address that of the Public Server.

Mapped Public Subnet:
This is the subnet mask of the Public Server.

Hosting Multiple Domains on a Shared IP Address

1) Click on Firewall in the Quick Links Menu
2) Click on the Advanced Firewall Settings button.
3) Click on the Multiple IP Hosting - Settings button.
4) Depending on if you wish to set up a Public or Private Server, click the appropriate New Server button.
5) Input the correct details in the provided fields. Press the OK button.
6) Press the Save button.

Changing the details of Multiple IP Hosting entry

1) Click on Firewall in the Quick Links Menu
2) Click on the Advanced Firewall Settings button.
3) Click on the Multiple IP Hosting- Settings button.
4) Press the Edit button of the corresponding Server entry that you wish to change.
5) Change the details of the server entry.
6) Press the OK button when you are satisfied with the changes you have made.
7) Press the Save button.

Removing an entry from the Multiple IP Hosting tables.

Removing an entry from the Multiple IP Hosting tables.

1) Click on Firewall in the Quick Links Menu
2) Click on the Advanced Firewall Settings button.
3) Click on the Multiple IP Hosting - Settings button.
4) Press the Delete button of the corresponding Server entry that you wish to change.
5) Press the Save button to confirm your changes.

Firewall Summary

Firewall Summary

What is a Firewall Summary?
The Firewall Summary page gives you a full overview of your Firewall settings. From this page you can also:

Firewall Summary Features
Save as…
Save the Firewall Summary as a text file (txt), webpage (html) or Comma Separated file (CSV).

E-mail
E-mail the Firewall Summary to a specified E-mail Address.

Print
Print the Firewall Summary so you can view it on paper.

Introduction

Chat Monitoring

What is Chat Monitoring?

Internet chat, also called Instant Messaging (IM), is becoming a part of our everyday lives.

In the home it is used as a way of keeping in touch with friends and family. In the business environment it is a way to keep in touch with clients and staff. The advantage is that it is more immediate than e-mail but cheaper than a phone call.

However, there are potential pitfalls that come with the use of Internet chat programs.

In the home, your children are potentially at risk from:
- Paedophiles.
- Internet bullying.
- Inappropriate conversations such as drugs, sex and suicide methods.

In the business environment, other risks are present, such as:
- Loss of productivity from non-work related conversations
- Legal liability from inappropriate conversations such as at-work bullying and sexual harassment.
- The disclosure of sensitive corporate information.

XGate provides unique Chat Room Monitoring tools, giving you the ability to monitor, block or shut down offensive chat conversations and websites from your mobile phone or email account.

Chat Monitoring Features

Within XGate Chat Monitoring section of the XGate Control Centre, there are a number of features that are accessible.

SMS Balance
This display your current SMS balance (i.e. the number of alerts that can still be sent to your mobile phone).

Alert Settings
From here you can set how you wish to be alerted. This can be either via Mobile Phone Text message or E-mail.

Keyword Monitoring
Select the words and categories that you wish to be alerted about. Once the selected words are used in a chat session, you will be alerted to their use depending on your Alert settings.

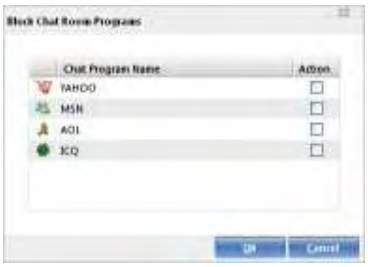
Web Monitor
Select the websites that will trigger an alert once they have been visited.
Please note that Chat Monitoring will only work on computers that have the XGate sensor installed. For more information on installing the XGate Sensor, see the Installing the XGate Sensor page.

SMS Balance

The number of SMS alerts that can be sent to your mobile phone are displayed here.

To view your SMS balance:
1) Press the Chat Room Monitoring button.
2) Press the Customise Chat Room Monitoring button.
3) Press the SMS Balance View button.

Blocking Chat Programs



On the main Chat Monitoring screen, there is the facility to block Chat Programs. The Chat programs that are supported by XGate Chat Monitoring are:

- MSN / Windows Live Messenger.
- Yahoo Messenger.
- AOL Messenger.
- Google Talk.
- ICQ.

To block a chat program, ensure the tick box associated with the program you wish to block is ticked. When a program is blocked from the XGate Control Centre, you will no longer be able to start it. To access the program once again, un-tick the relevant chat program.

In addition, when you block a chat program via Mobile Phone text message or E- mail, the status of the Messenger program will be reflected here.

Alert Settings

This is where you set up how to be alerted by XGate.

XGate can alert you in two ways:

- E-mail Address.
- Mobile Phone Text Message (SMS).

The following details are necessary when setting up alerts:

The method you would like to receive Alerts by:
This is either via E-mail or by Mobile Phone Text Message (SMS).

E-mail Address / Mobile Phone Number:
This is the mobile phone number or e-mail address you wish alerts to be sent to.

Alert me when a chat program is launched tick box:
If this is ticked, you will receive an alert via your chosen method each time a chat program is launched.

Note: Once your SMS credits have run out, your Mobile Service Provider will charge you at a premium rate for each message. Alternatively, you can purchase additional credits at a special rate from the GSEC1 website.

Introduction

Monitor Chat Room

This feature allows you to select which keywords will trigger an alert during chat sessions.

Within this feature are pre-defined words that are grouped into specific categories. These categories are:

Paedophile / Grooming
Sexual
Suicide
Crime/ Violence
Alcohol Tobacco
Drugs
Occult

XGate also provides the facility to add your own Custom Words to be monitored during chat conversations.

The pre-defined and custom words can also be individually enabled and disabled.

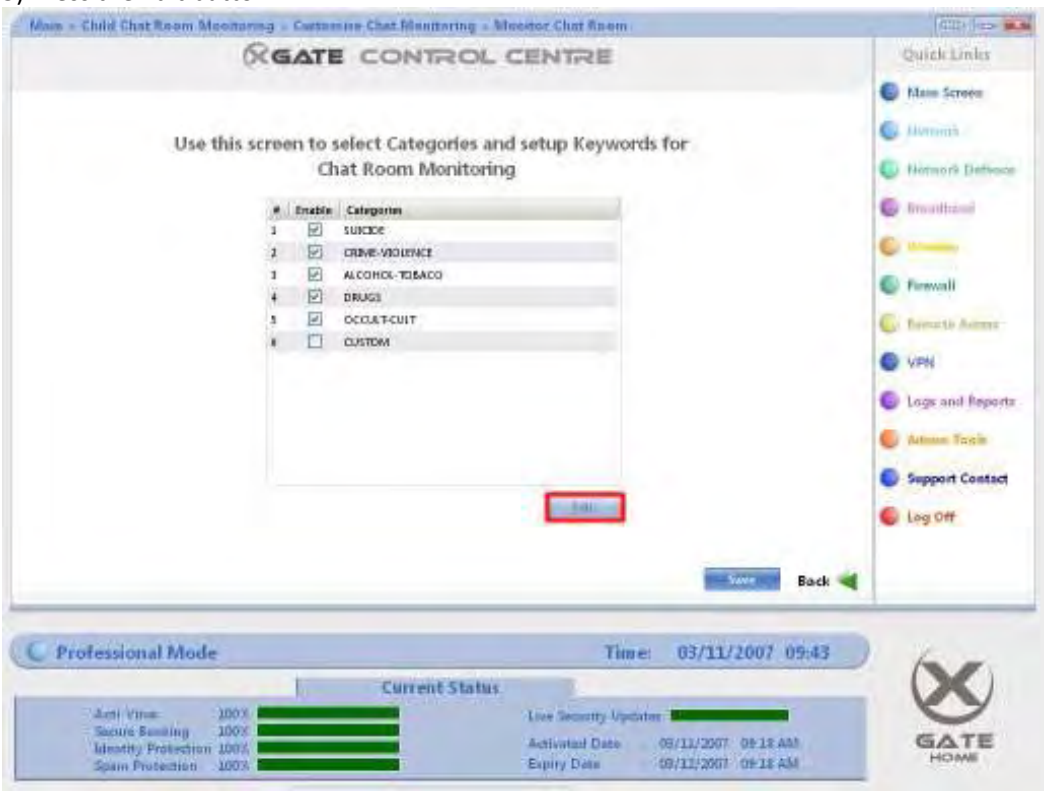
Disabling Monitored Keywords

1) Press the Chat Room Monitoring button.

2) Press the Customise Chat Room Monitoring button.

3) Press the Monitor Chat Room Settings button.
If you wish, you can disable the entire Keyword Monitoring feature by having the tick box on the left un-ticked.

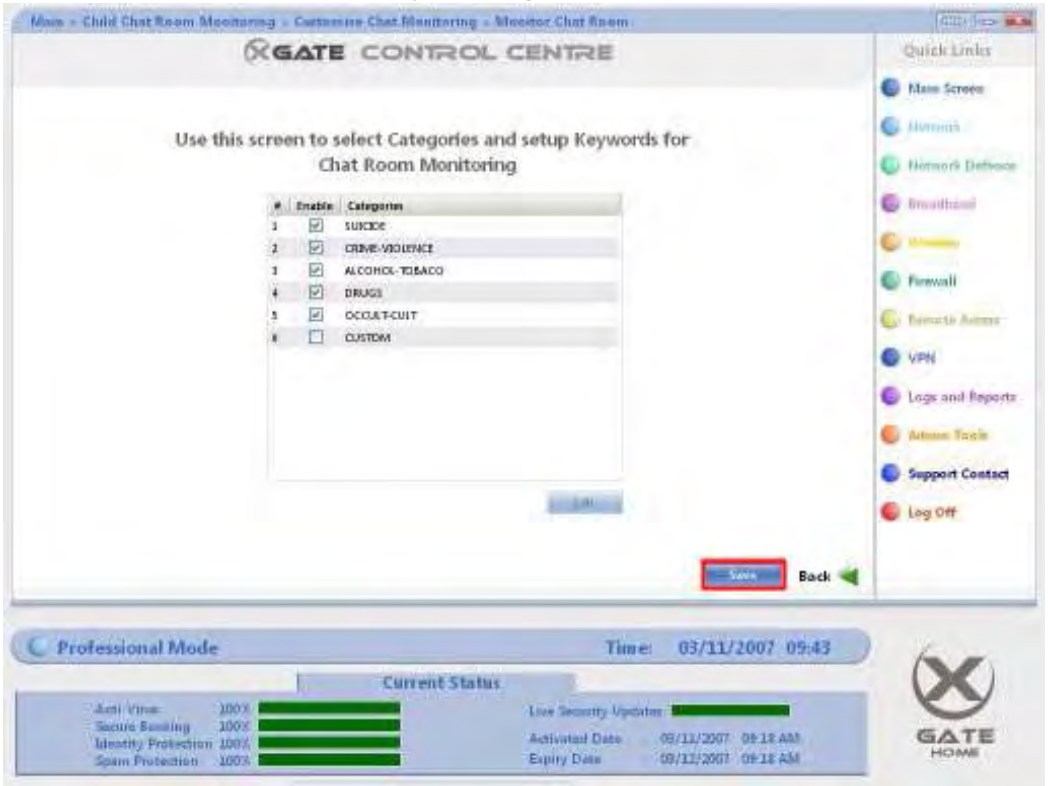
4) Select the category of the keyword you wish to disable by clicking the category name. You can also disable an entire category by un-ticking the appropriate tick box on the left.
5) Press the Edit button.



6) To disable a specific word, un-tick the tick box associated to the word you wish to disable alerts for.

7) Press the OK button to close the Edit Chat Alert Keywords window.

8) Press the Save button to confirm your changes.



Adding Custom Keywords

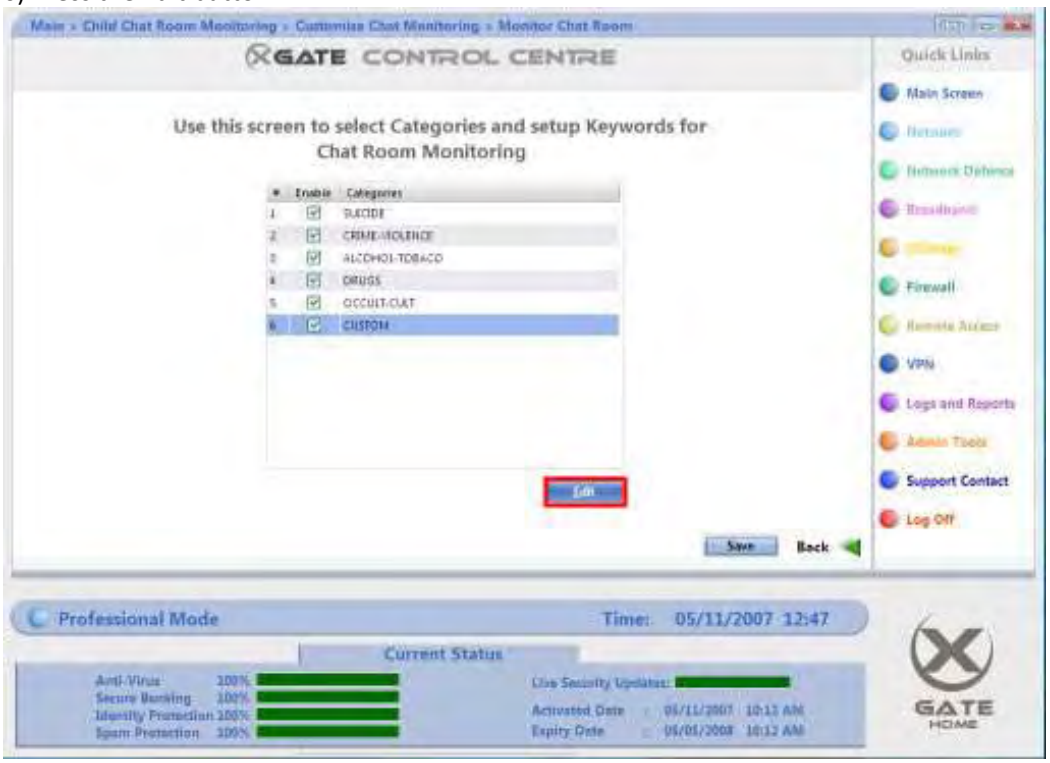
1) Press the Chat Room Monitoring button.

2) Press the Customise Chat Room Monitoring button.

3) Press the Monitor Chat Room Settings button.

4) Ensure the Custom List tick box is ticked.
5) Select the Custom List Category by clicking it in the table.

6) Press the Edit button.

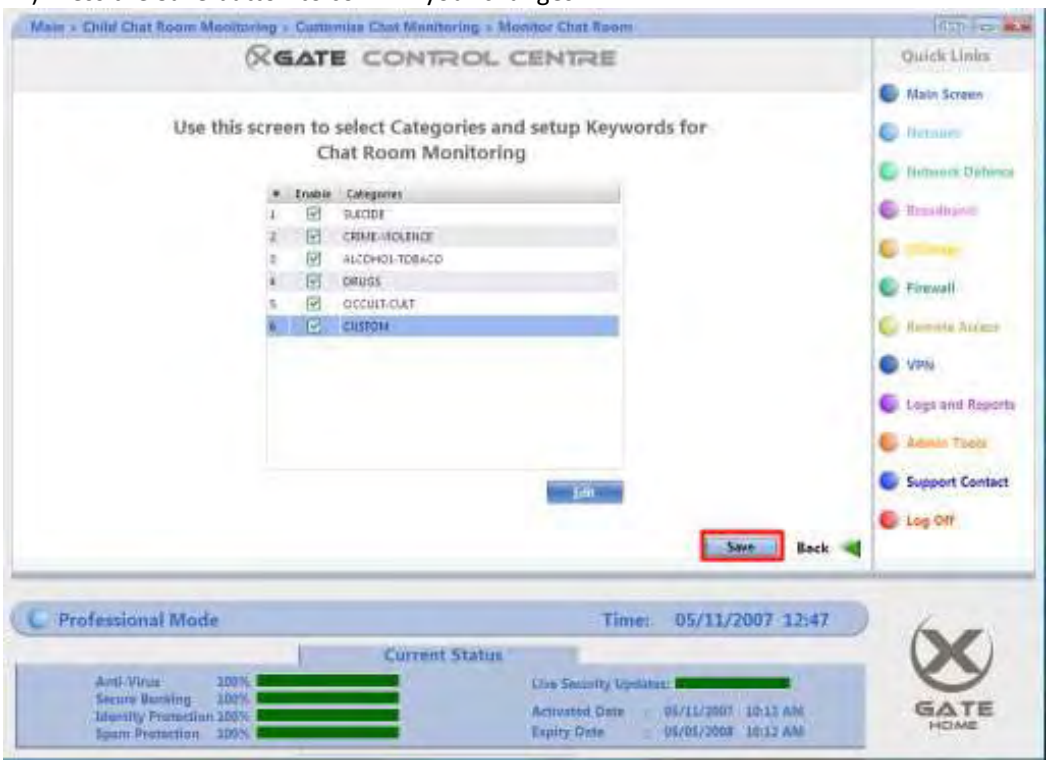


7) Press the Add button.

8) Enter your custom keyword in the Add Custom Word window.
9) Press the OK button.

10) Press the OK button.

11) Press the Save button to confirm your changes.



Changing a Custom Keyword

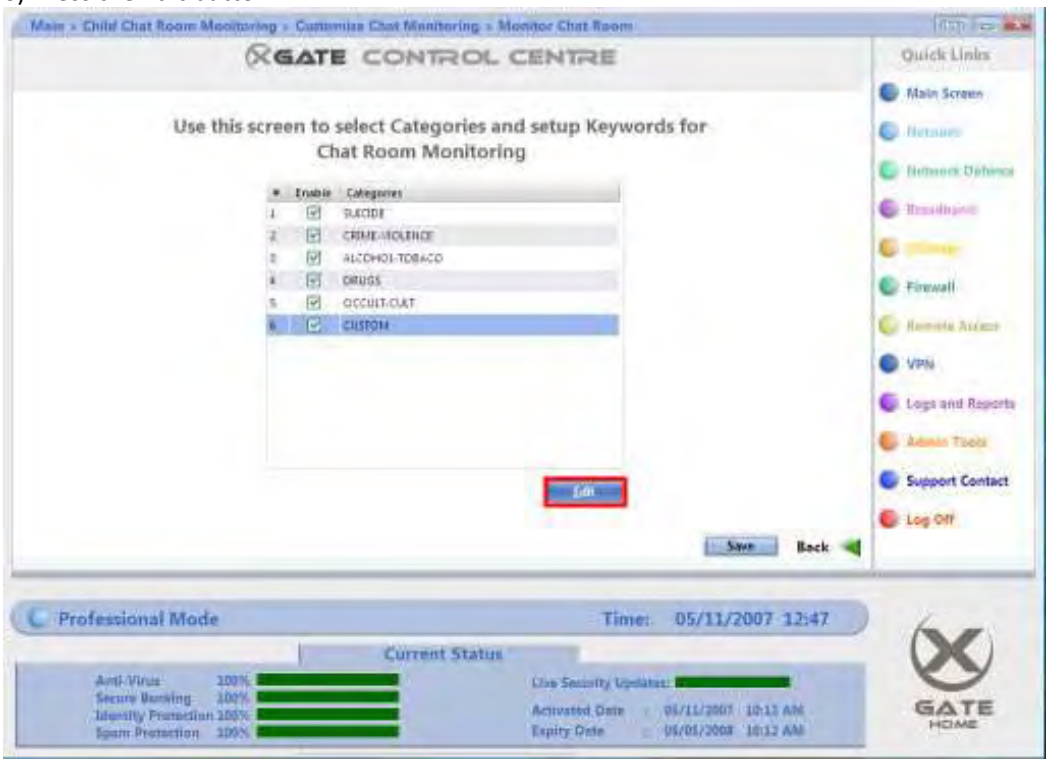
1) Press the Chat Room Monitoring button.

2) Press the Customise Chat Room Monitoring button.

3) Press the Monitor Chat Room Settings button.

4) Ensure the Custom List tick box is ticked.
5) Select the Custom List Category by clicking it in the table.

6) Press the Edit button.

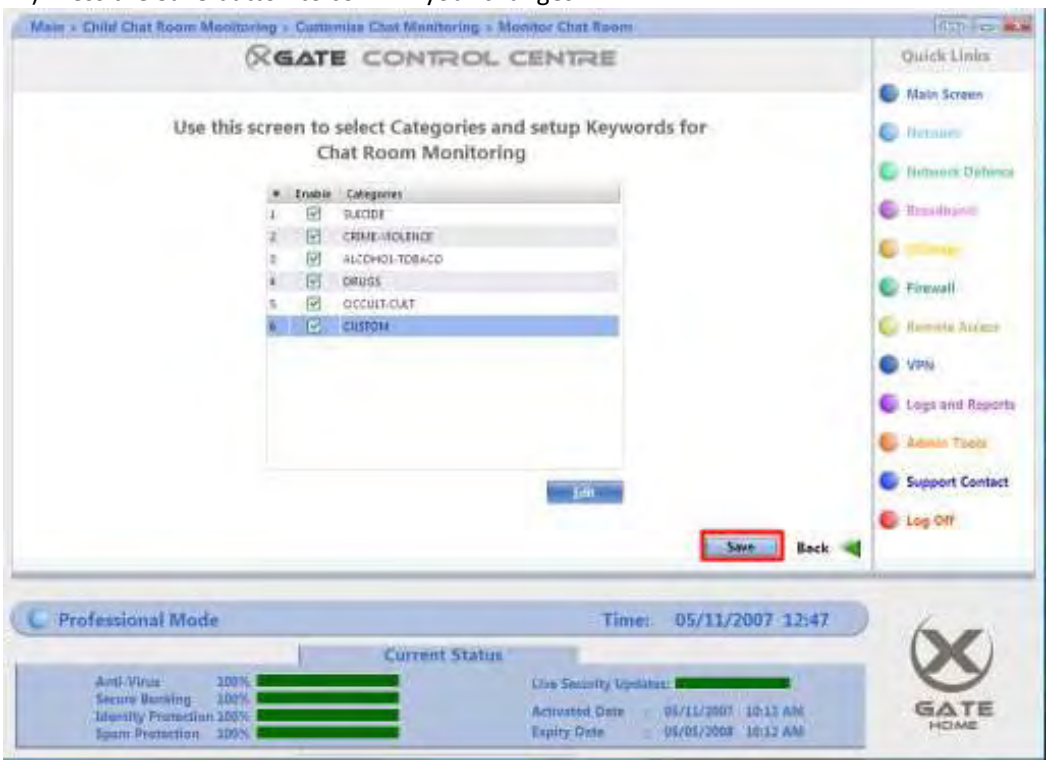


7) Press the Edit button.

8) Edit the custom keyword.
9) Press the OK button.

10) Press the OK button.

11) Press the Save button to confirm your changes.



Removing a Custom Keyword

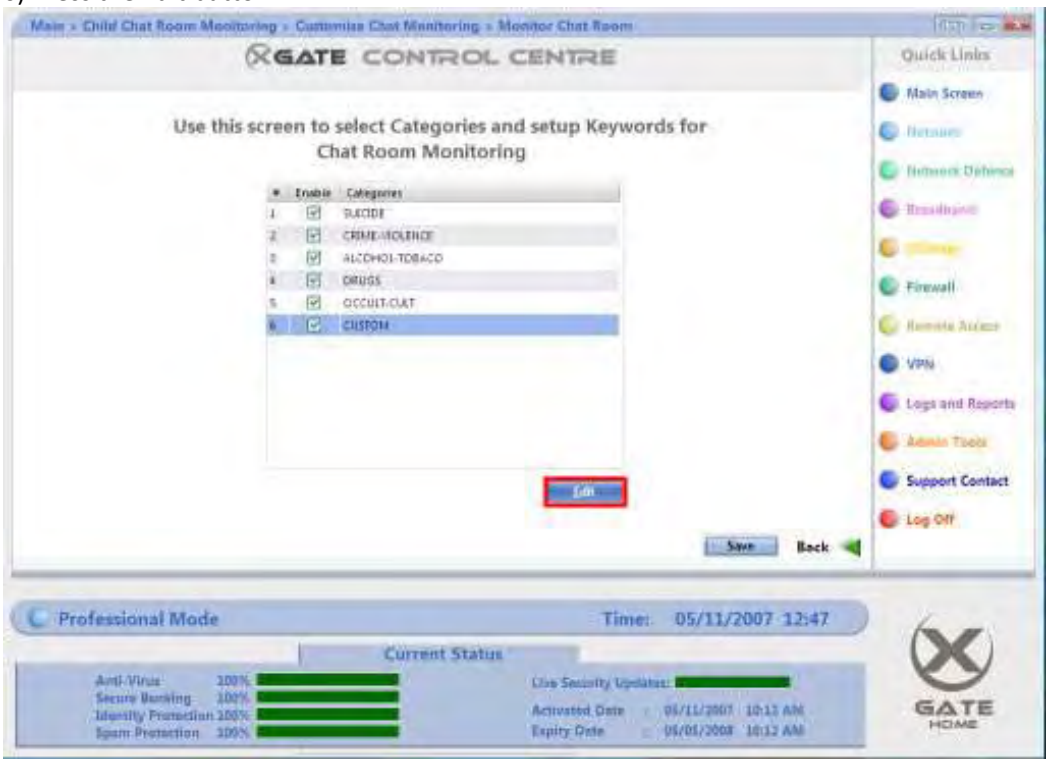
1) Press the Chat Room Monitoring button.

2) Press the Customise Chat Room Monitoring button.

3) Press the Monitor Chat Room Settings button.

4) Ensure the Custom List tick box is ticked.
5) Select the Custom List Category by clicking it in the table.

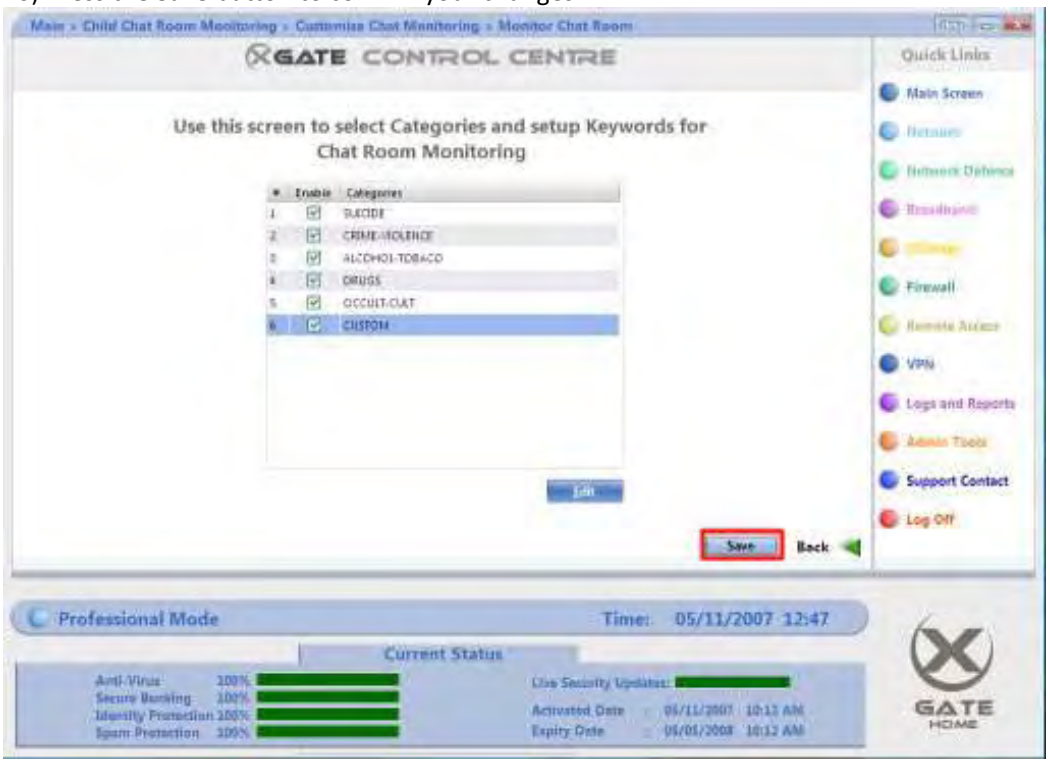
6) Press the Edit button.



7) Click the word you wish to remove. This will highlight the selected entry.
8) Press the Delete button.

9) Press the OK button.

10) Press the Save button to confirm your changes.



Introduction

Monitor Web Activity

Monitor Web Activity allows you to be alerted when a computer on your network accesses a website with a title or address containing specific words

The Web address would be the address you use to access website. For example, www.gsec1.com

In the case of www.gsec1.com, the web page title is: Business Internet Security Intrusion Detection Unified Threat Management Remote Access GSEC1.

To add an entry in to Web Page Title and Address Monitoring, the following details are necessary:

Type
This is either set as Web Address or Web Title.

Address/Title
The Web Address or words in the Website's Title that you wish to be alerted of.

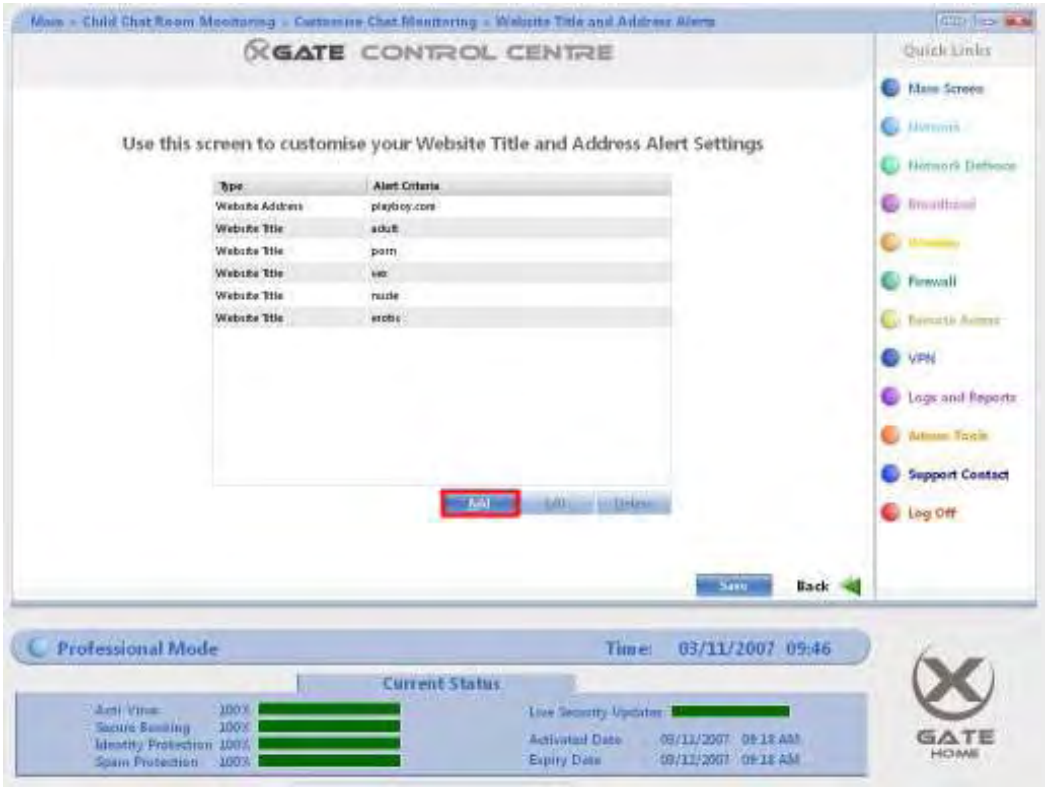
Adding a Web Alert

1) Press the Chat Room Monitoring button.

2) Press the Customise Chat Room Monitoring button.

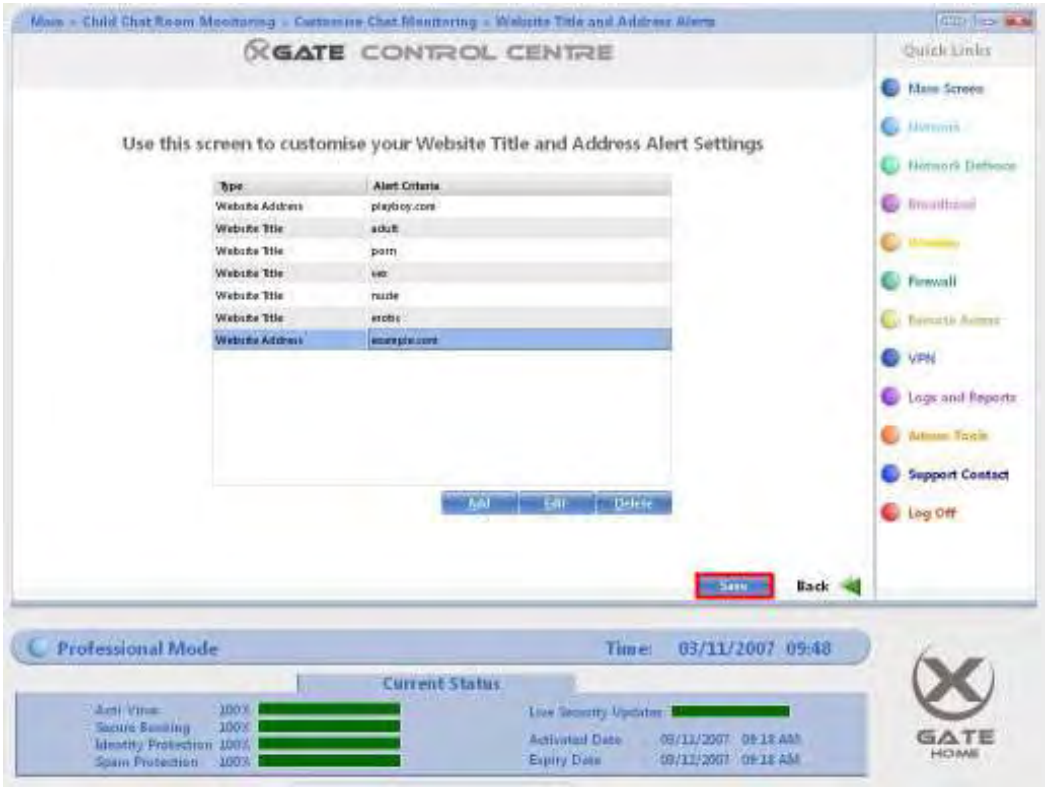
3) Press the Monitor Web Activity Settings button.

4) Press the Add button.



5) Enter your Web Alert details.
6) Press the OK button.

7) Press the Save button to confirm your changes.


Main > Child Chat Room Monitoring > Customise Chat Monitoring > Website Title and Address Alerts
GATE CONTROL CENTRE
Quick Links
Main Screen
Network Defence
Firewall
VPN
Logs and Reports
Support Contact
Log Off
Use this screen to customise your Website Title and Address Alert Settings
Type
Alert Criteria
Website Address
playboy.com
Website Title
adult
Website Title
porn
Website Title
sex
Website Title
nude
Website Title
erotic
Website Address
Add
Edit
Delete
Save
Back
Professional Mode
Time: 03/11/2007 09:48
Current Status
Anti-Virus 100%
Secure Banking 100%
Identity Protection 100%
Spam Protection 100%
Live Security Updates
Activated Date 03/11/2007 09:18 AM
Expiry Date 03/11/2007 09:18 AM
GATE HOME

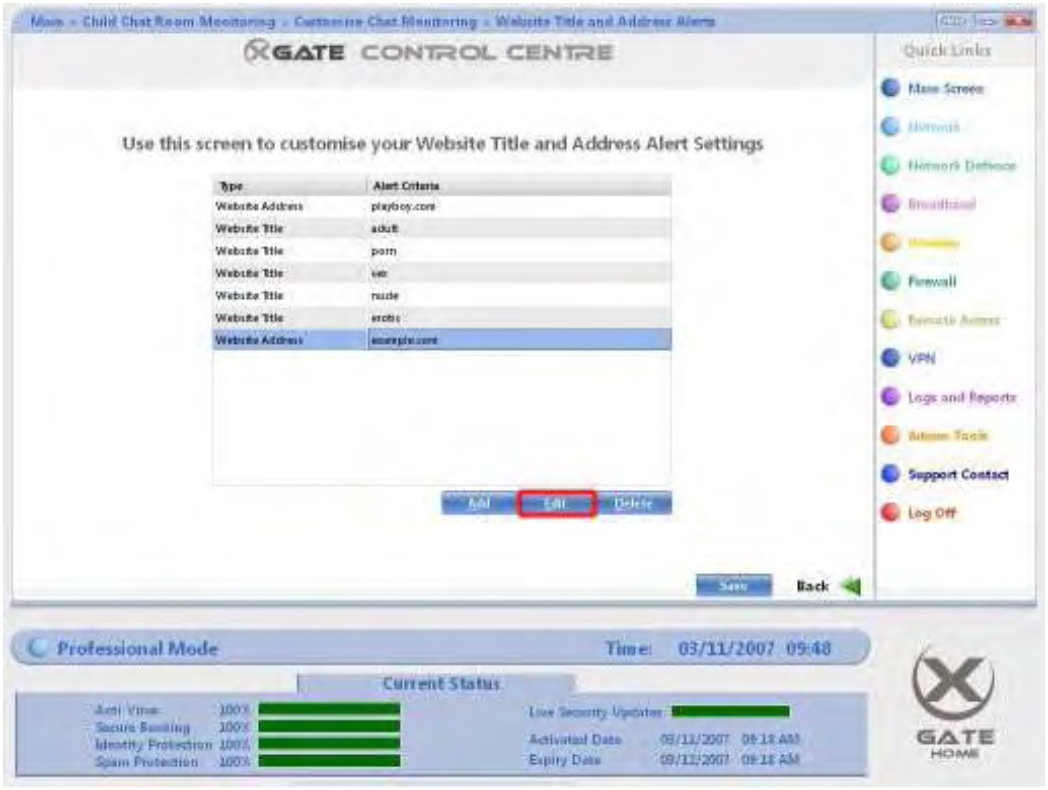
Changing a Web Alert's details

1) Press the Chat Room Monitoring button.

2) Press the Customise Chat Room Monitoring button.

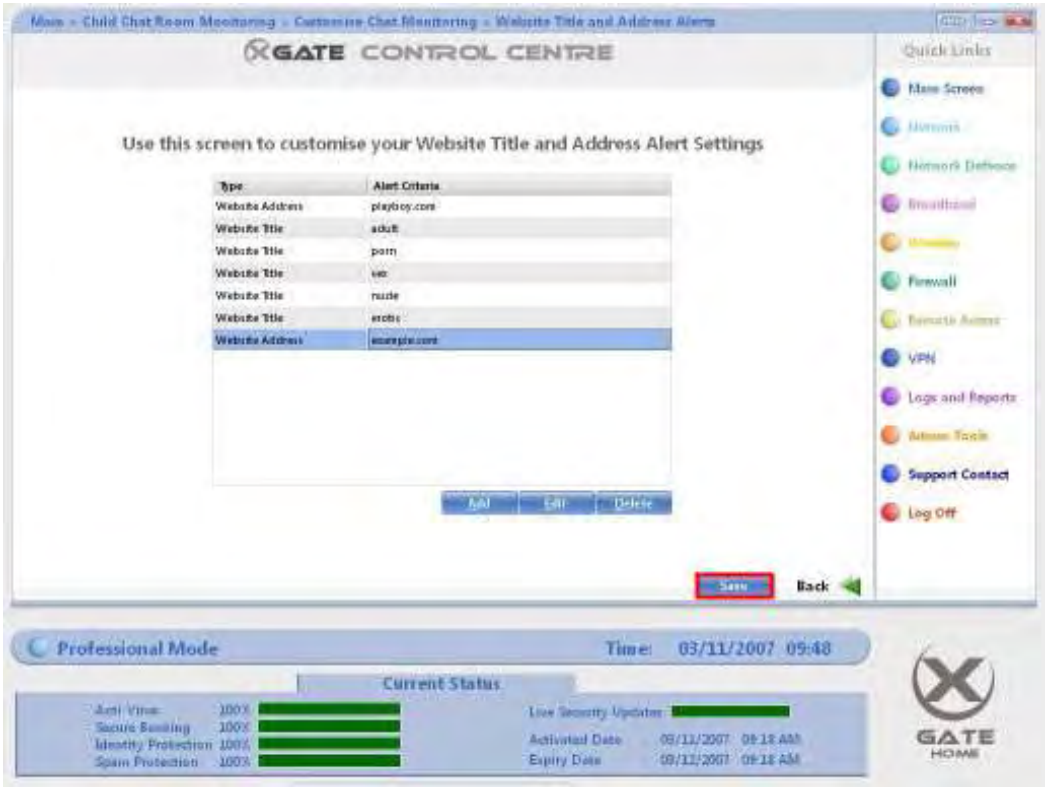
3) Press the Monitor Web Activity Settings button.

4) Click the entry you wish to edit. This will highlight the entry.
5) Press the Edit button.



6) Change your Web Alert details.
7) Press the OK button.

8) Press the Save button to confirm your changes.


Main > Child Chat Room Monitoring > Customise Chat Monitoring > Website Title and Address Alerts
GATE CONTROL CENTRE
Quick Links
Main Screen
Network Defence
Firewall
VPN
Logs and Reports
Support Contact
Log Off
Use this screen to customise your Website Title and Address Alert Settings
Type
Alert Criteria
Website Address
playboy.com
Website Title
adult
Website Title
porn
Website Title
sex
Website Title
nude
Website Title
erotic
Website Address
Add
Edit
Delete
Save
Back
Professional Mode
Time: 03/11/2007 09:48
Current Status
Anti-Virus 100%
Secure Banking 100%
Identity Protection 100%
Spam Protection 100%
Live Security Updates
Activated Date 03/11/2007 09:18 AM
Expiry Date 03/11/2007 09:18 AM
GATE HOME

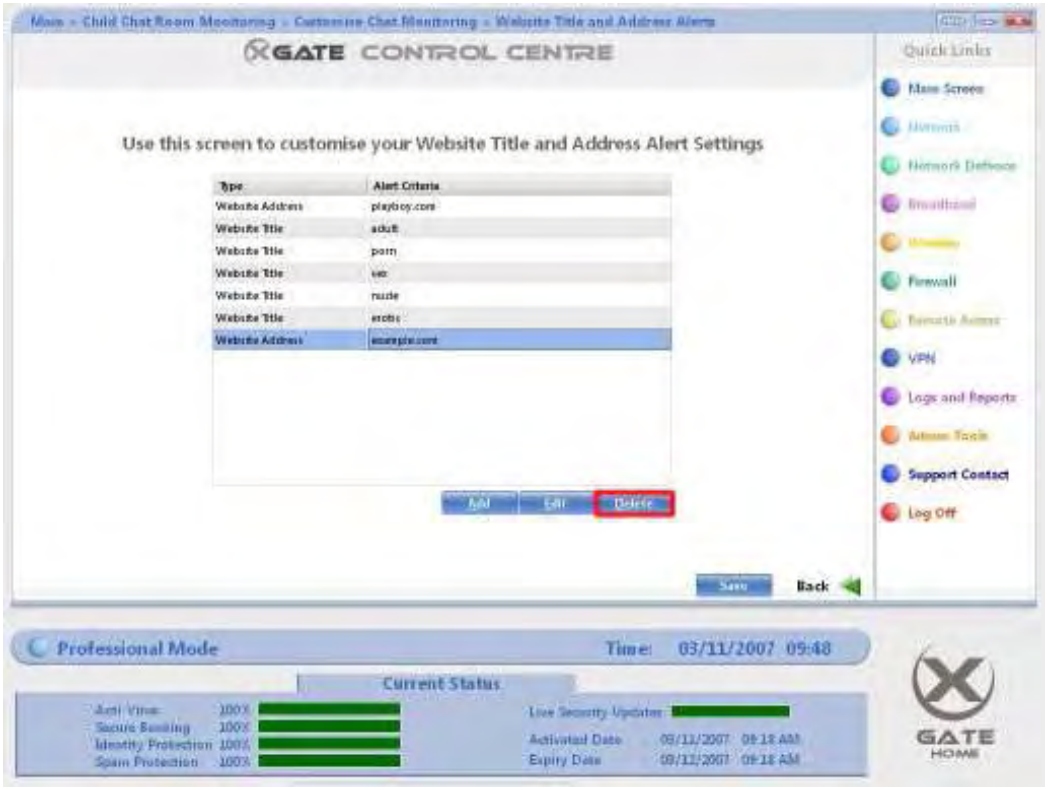
Removing a Web Alert

1) Press the Chat Room Monitoring button.

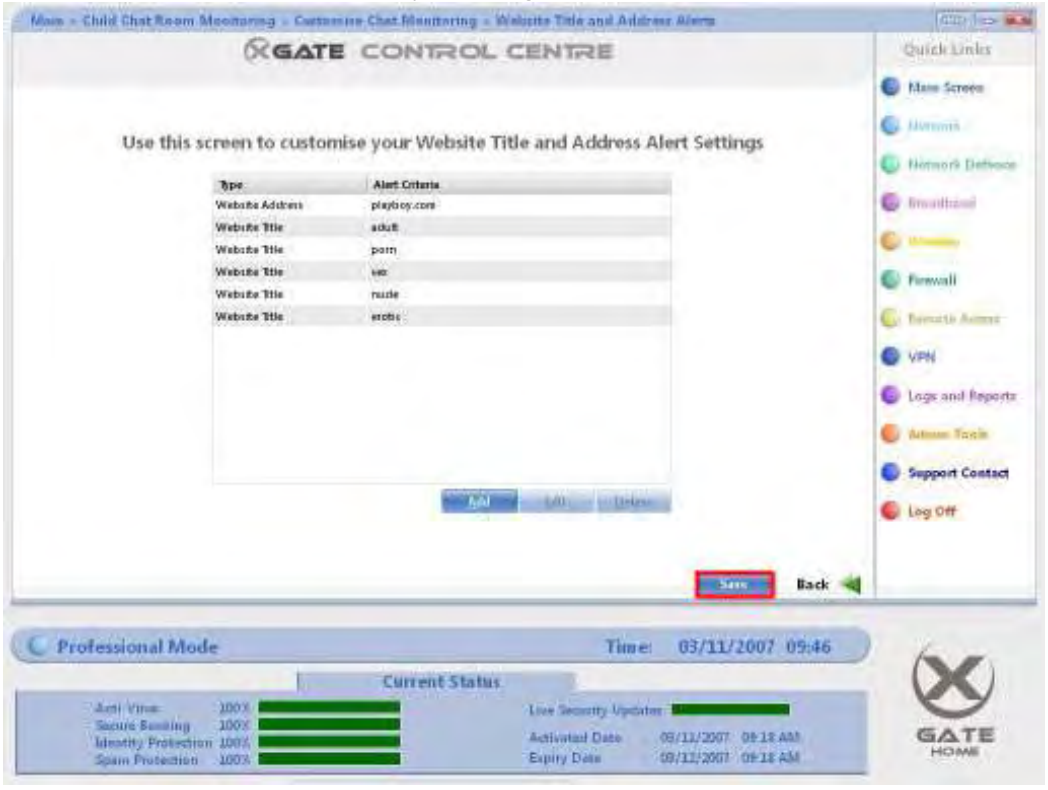
2) Press the Customise Chat Room Monitoring button.

3) Press the Monitor Web Activity Settings button.

4) Click the entry you wish to edit. This will highlight the entry.
5) Press the Delete button.



6) Press the Save button to confirm your changes.



Introduction

Network Defence

What is Network Defence?

Network Defence encompasses all functions related to scanning and protecting the computers on your network from malicious programs and applications such as Viruses, Spyware and Malware. This is achieved by the use of triple engine Virus and Identity Protection scans.

Network Defence is used in conjunction with the XGate Sensor. To take full advantage of XGate 2.0's security, please install the XGate sensor on the machines that you wish to protect within your network. For more details on how to do this, please see the to Installing the XGate Sensor page.

Analogy

Network Defence can be imagined as the defence headquarters of your Network. From here you can see an overview of your network's defence status and manage any potential threats from viruses and spyware.

Network Defence Features

Within the Network Defence module are the following features:
Network Defence System:
Scan any PC with the sensor installed from here.

Advanced Settings:
Set up and manage your Anti-Virus and Identity Protection settings.

Quarantine List:
Set up computers to be automatically or manual quarantined from the Internet.

Scan Schedule:
Schedule when you wish Anti-Virus and Identity Protection scans to be started on all computers with the sensor installed on your network.

Control rights:
Allow users control of specific modules within the XGate sensor.

Network Defence Status

Network Defence System

What is the Network Defence System?
The Network Defence System allows you to run scans from the XGate Control Centre on any computer within your local network that has the XGate Sensor installed. This feature also displays an overview of your network's sensor deployment status and scan history.

Network Defence System Properties
When scanning computers on your network from the Network Defence System screen, there are a number of different scan options available.

Scan Type
Full Scan:
This will set up the Anti-Virus and Identity Protection to scan all the files on a computer
Fast Scan:
This set up the Anti-Virus and Identity Protection to scan just the main system files on the computer.

Number of Engines
Single Engine:
Scans the selected computer with a single scan engine
Dual Engine:
Scans the selected computer with both scan engines.

Scan Modules
Anti-Virus:
Scans the selected computer for Viruses

Identity Protection:
Scans the selected computer for Spyware.
All Modules:
Scans the selected computer for Viruses and Spyware

To scan a single computer, click the associated Scan button.

To scan all the computers on the network with the XGate sensor installed, press the Scan All button in bottom right.

Advanced Settings

What are Advanced Settings?
Advanced Settings allows for customisation of XGate Anti-Virus and Identity Protection settings.

Advanced Settings
Below is a description of the Advanced Settings screen.

Enable/Disable
On: Switches the module on.
Off: Switches the module off.

Customise
Enable Gateway Scanning:
This scans all traffic that goes through the XGate for Viruses. This ensures that Viruses are blocked by the XGate device before they can reach your computer.

Enable Real Time Scanning:
This scans all data being processed on your computers within your network. This means that all malicious software should be picked up before they have a chance to run and damage your computer.

Scan each computer when
It is switched on:
All computers with the XGate Sensor installed will be scanned as they are switched on.

Response options

Log and remove:

This option will log the details of malicious files in the XGate Log Viewer and attempt to delete it from the computer.

Log and quarantine:

This option will log the details of the malicious files in the XGate Log Viewer and quarantine them in a protected folder to ensure it does not damage your computer.

Log but take no action:

This option will log the details of malicious files in the XGate Log Viewer but take no action. It is not recommended to use this option as malicious Virus or Spyware files will be left on your computer and could infect your network.

Quarantine List

Quarantine List

What is the Quarantine List?
The Quarantine List is a central management area for computers with suspected malicious activity.

Quarantine List Properties
From this screen you can:
- View the quarantine status of computers within your network.
- Scan computers within your network.
- Block and unblock computers within your network.
- Set computers to automatically quarantine if a threat has been detected.
- See the Sensor deployment status of each computer within your network.

Introduction

Scheduled Scans

What is a Scheduled Scan?

From the Scheduled Scan screen, it is possible to view and edit the times when XGate will scan computers on your network for Viruses and/or Spyware.

The Scheduled Scans screen comes with 3 default scans. These are daily scans set to occur at 10am, 1pm and 5pm. It is recommended that to set up scans to run during times that your computer(s) will be switched on but are not being intensively used.

Analogy

Scheduled scans can be thought of similarly to setting your video recorder to record television programmes from your Television at a certain time and date.

Scheduled Scan Details

The following details must be configured to set up a scheduled scan.

Time:
The time the scheduled scan will start.

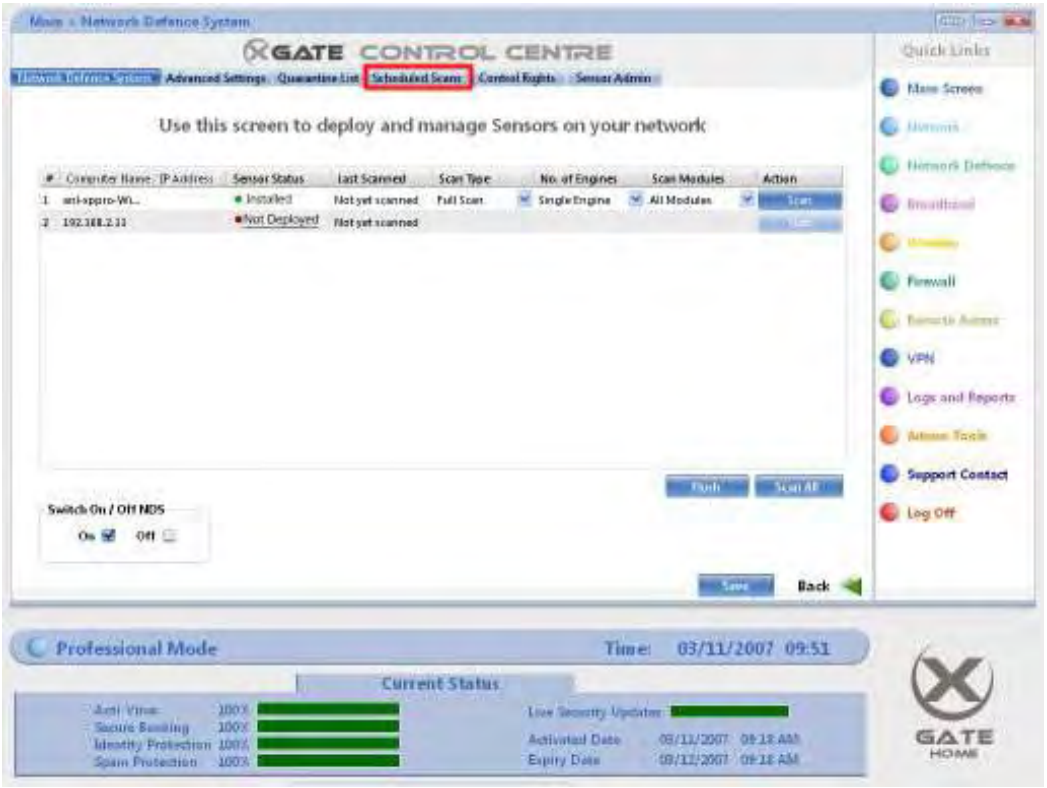
Type
Full Scan:
This sets up the Anti-Virus and Identity Protection to scan all the files on a computer.
Fast Scan:
This sets up the Anti-Virus and Identity Protection to scan just the main system files on the computer.
Single Engine:
Scans the selected computer using a single scan engine.
Dual Engine:
Scans the selected computer using both scan engines.

Modules
Anti-Virus:
Scans the selected computer for Viruses.
Identity Protection:
Scans the selected computer for Spyware.
All Modules:
Scans the selected computer for Viruses and Spyware
Days:
The days that the scan will run.

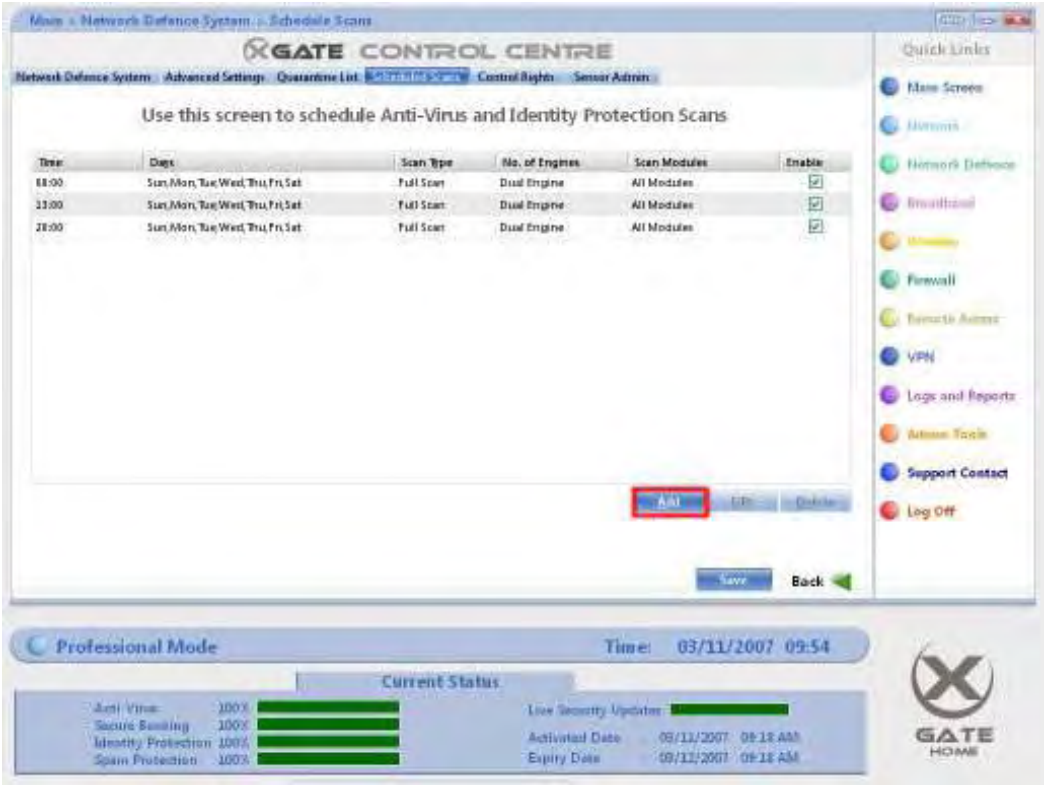
Adding Scheduled Scans

1) Click on Network Defence in the Quick Links Menu.

2) Click on the Scheduled Scans tab.

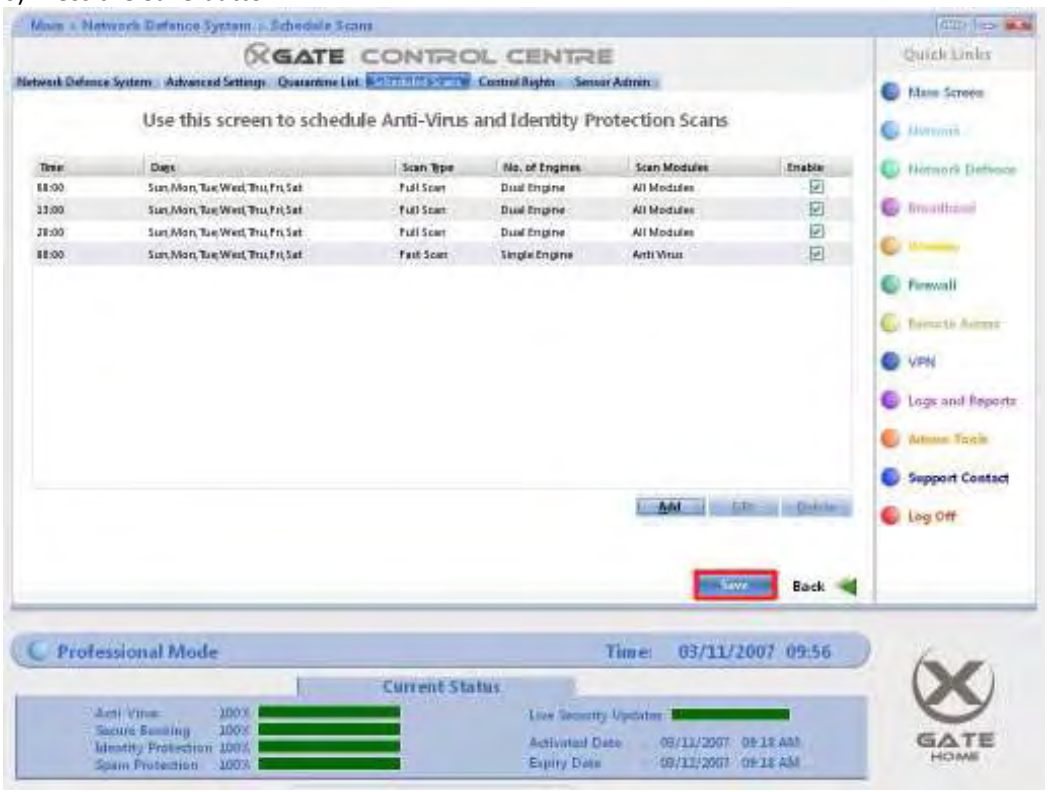


3) Click on the Add button.



4) Set the details for your new scheduled scan.
5) Press the OK button.

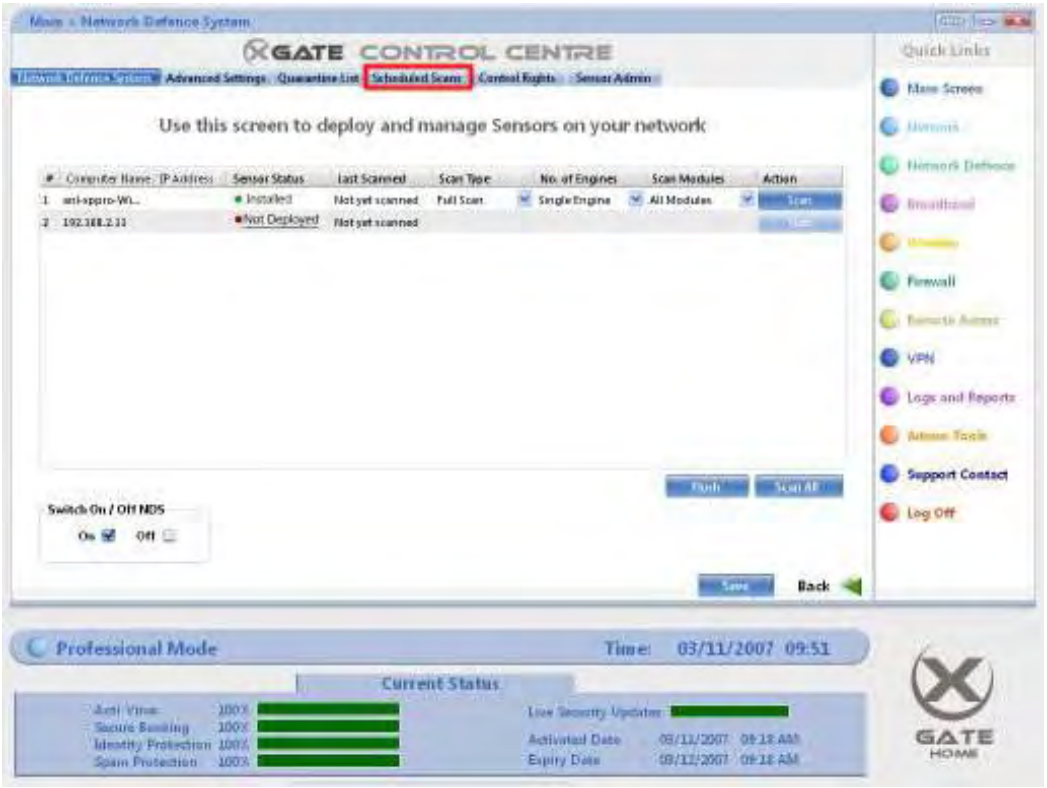
6) Press the Save button.



Changing a Scheduled Scan

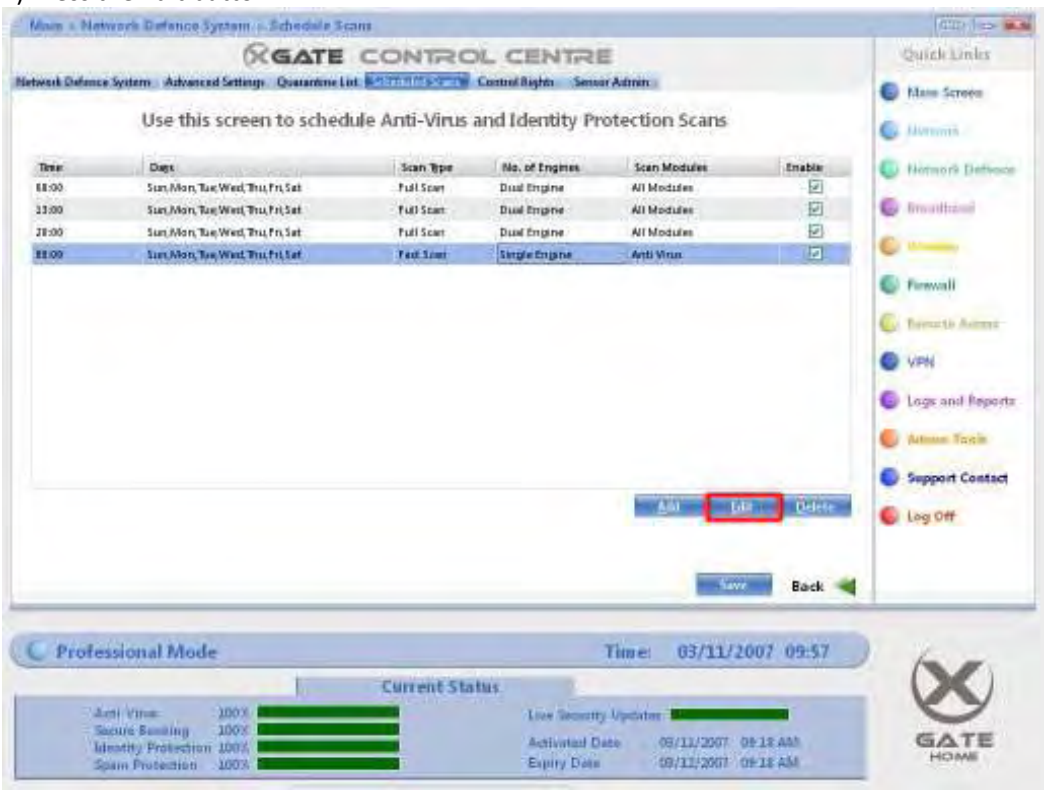
1) Click on Network Defence in the Quick Links Menu.

2) Click on the Scheduled Scans tab.



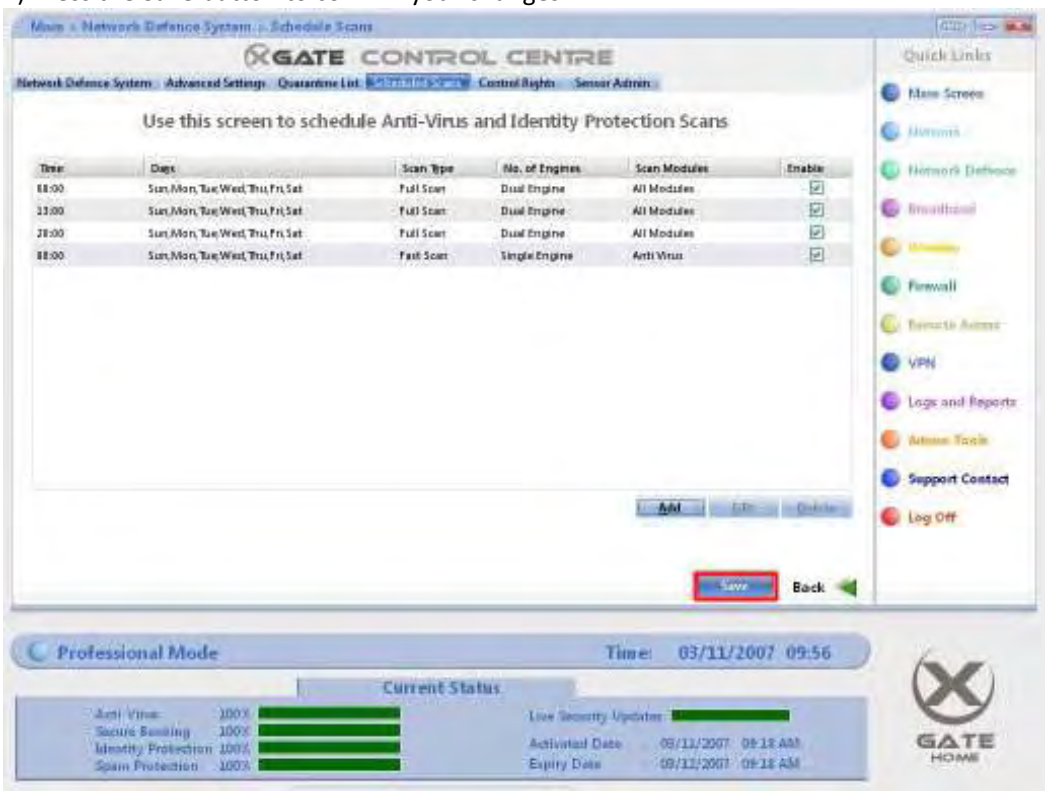
3) Select an entry by single clicking it in the table. This will highlight the Scheduled Scan entry.

4) Press the Edit button.



5) Amend the details as you see fit.
6) Press the OK button.

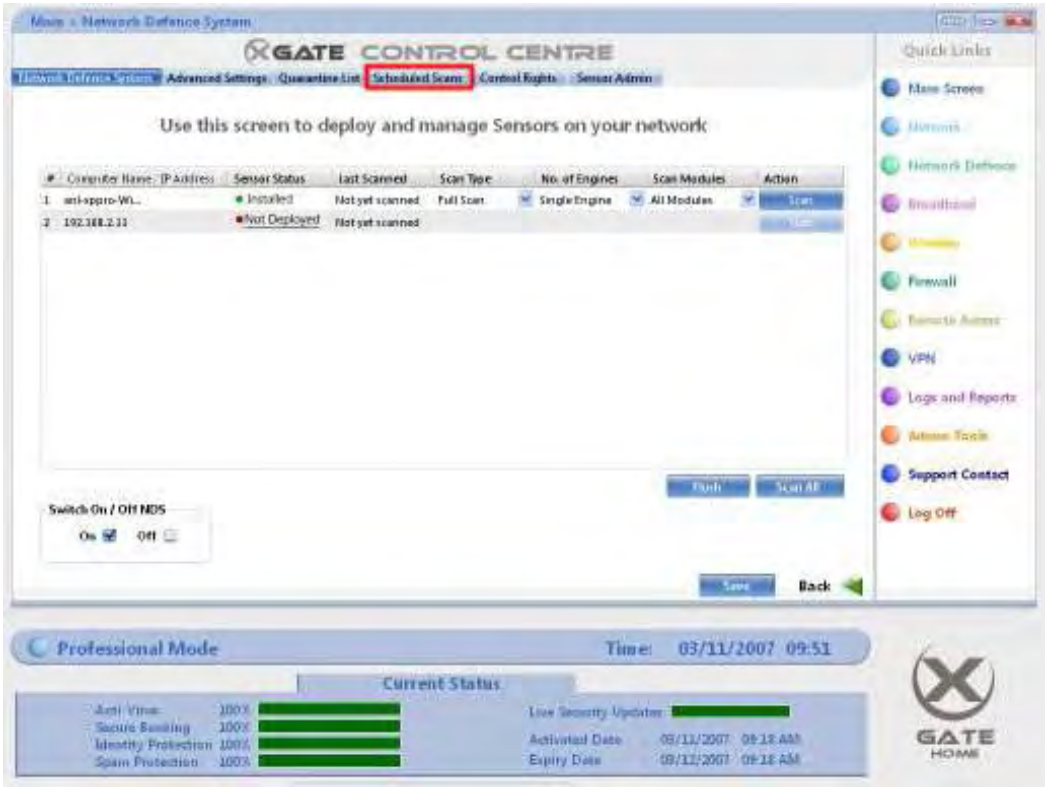
7) Press the Save button to confirm your changes.



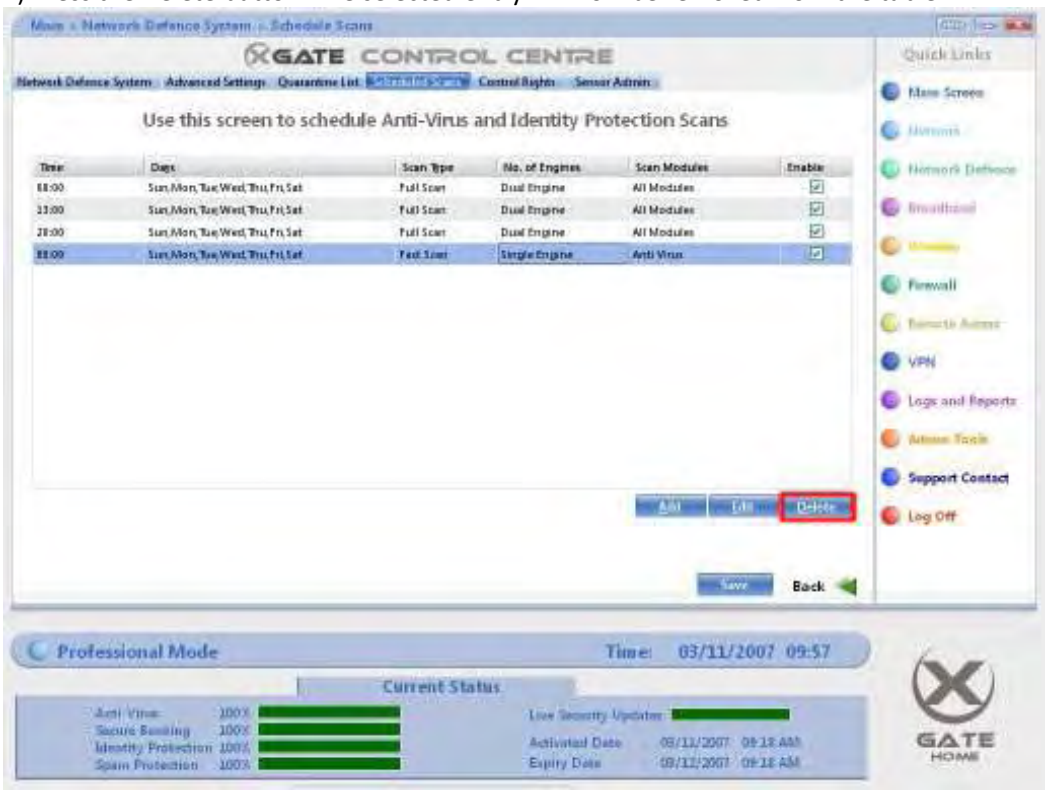
Removing a Scheduled Scan

1) Click on Network Defence in the Quick Links Menu.

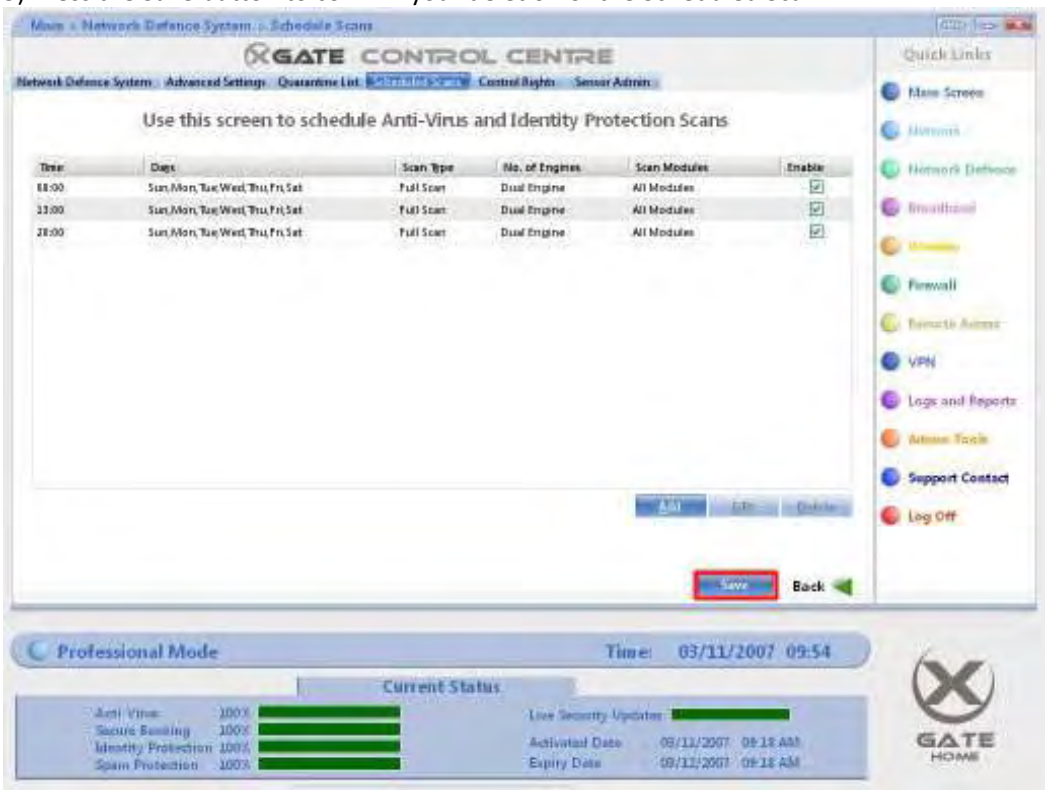
2) Click on the Scheduled Scans tab.



3) Select an entry by single clicking it in the table. This will highlight the Scheduled Scan entry.
4) Press the Delete button. The selected entry will now be removed from the table.

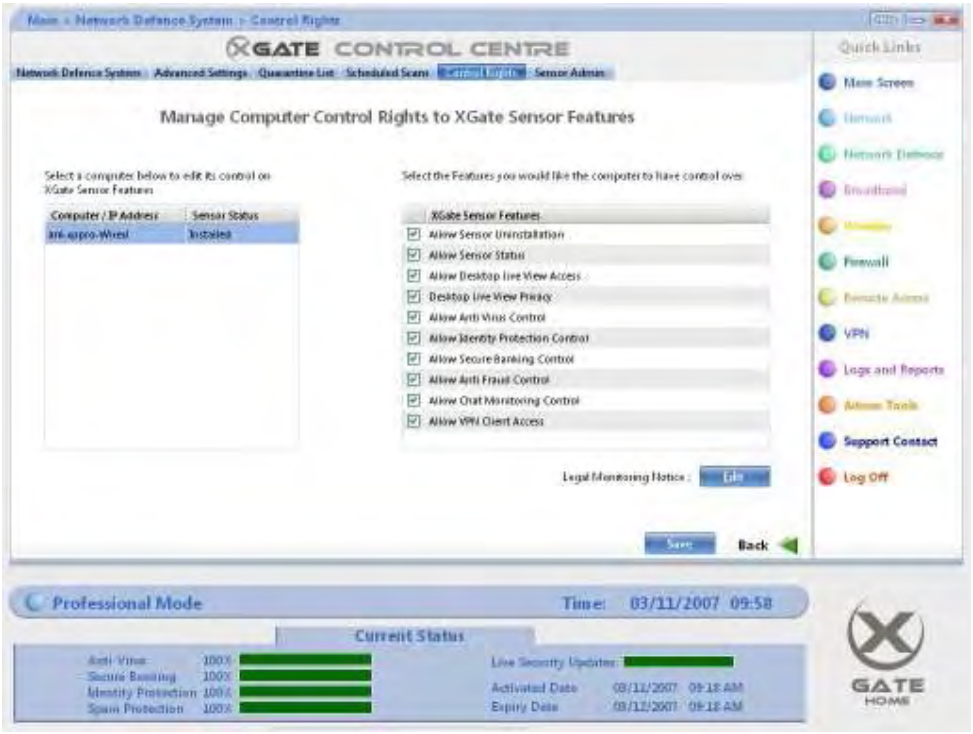


5) Press the Save button to confirm your deletion of the Scheduled Scan.



Introduction

Control Rights



What are Control Rights?
Control Rights offer the ability to assign certain rights and privileges to specific computers on your network.

The Control Rights screen is split up in to two tables:
- Allow user rights to uninstall Sensors.
- Allow user control of Modules.

Control Right Properties
Within these tables, there are options for:

Allow Sensor Uninstallation:
By ticking this option, you allow the specified user to uninstall the XGate Sensor from their computer.

Allow Desktop Live View Access:
By ticking this option, the Desktop Live View option will appear on the XGate Sensor menu. This menu is accessible by right clicking the XGate sensor icon in the windows system tray. For more details on Desktop Live View please see the Desktop Live View section.

Desktop Live View Privacy
By ticking this option, the selected computer's desktop will not appear within the Desktop Live View application.

Allow VPN Client access

By ticking this option, the VPN Client option will appear on the XGate Sensor menu. This menu is accessible by right clicking the XGate sensor icon in the windows system tray.

Allow Anti-Virus Control
This allows the user to configure the Anti-Virus settings and conduct their own scans for the selected computer.

Allow Identity Protection Control
This allows the user to configure the Identity Protection settings and conduct their own scans for the selected computer.

Allow Anti-Fraud Control
This allows the user to enable or disable the Anti-Fraud feature for the selected computer.

Allow Secure Banking Control
This allows the user to enable or disable the Secure Banking feature for the selected computer.

Allow Chat Monitoring Control
This allows the user to enable or disable the Chat Monitoring feature for the selected computer.

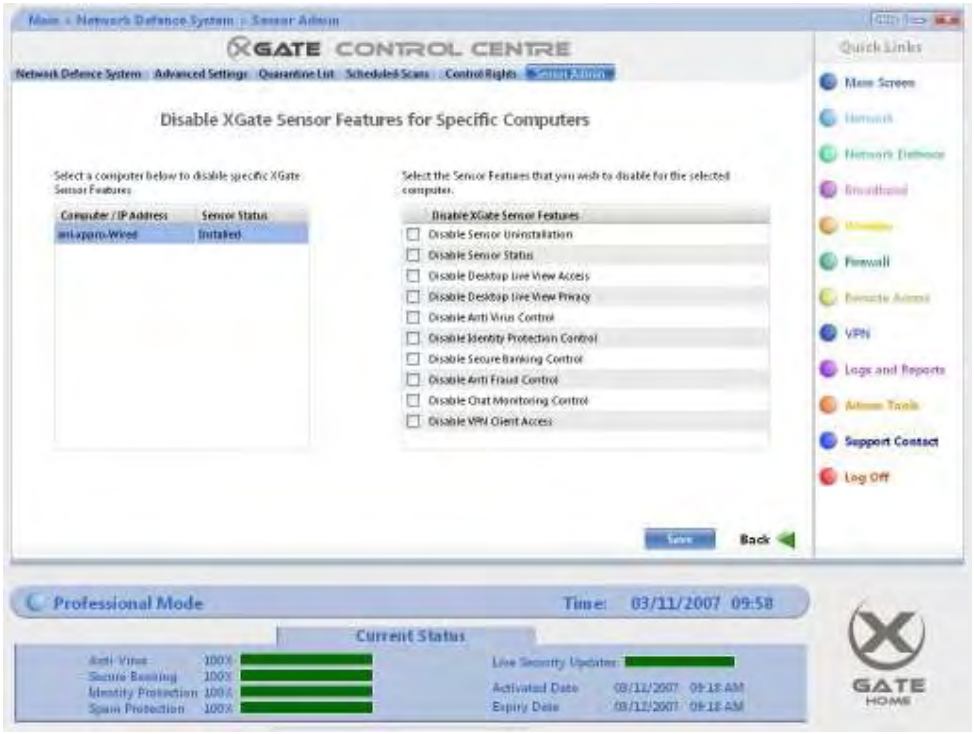
What is a Legal Monitoring Notice?

Due to the nature of Desktop Live View, it is legally required for a business to notify all network users that they are being monitored. For this reason, a Legal Monitoring Notice is provided for XGate.

The Legal Monitoring Notice is a message that appears every time a user logs on to their computer that is connected to the XGate. Along with the message, a file can be attached for the user to view. This file can be an electronic copy of your company's terms and conditions or working practices.

Sensor Admin

Sensor Admin



What is Sensor Admin?
Sensor Admin allows you to remotely disable XGate Sensor features from the XGate Control Centre for specific computers.

Control Right Properties
Within these tables, there are options to:

Disable Anti-Virus
Disable Identity Protection
Disable Anti-Fraud
Disable Secure Banking
Disable VPN Client
Disable Chat Monitoring
Disable Desktop Live Viewer
Disable Desktop Live View Client

Introduction

XGate Sensor

What is the XGate Sensor?

The XGate Sensor looks for suspicious patterns of data (e.g. from Viruses and Spyware) on all the computers behind XGate to ensure your computer's health. The Sensor provides the main mode of communication between the computers on your network.

Installing the XGate Sensor allows you to use:
- Anti Virus
- Identity Protection
- Anti Fraud
- Secure Banking
- VPN Client
- Chat Monitoring
- Desktop Live View

The features listed above are only available to a computer connected to XGate with the XGate Sensor installed.

As such, it is highly recommended to install the XGate sensor on computers to ensure the safety of your internal network.

Remote Security Sensor

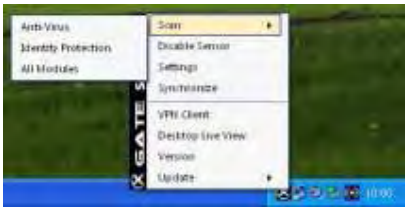
The XGate Sensor will work beyond your home network. For example, if you install the XGate Sensor on a portable laptop, you will be protected from viruses and spyware no matter where you are.

Installing the XGate Sensor

1) Insert the XGate Installation CD into your computer's CD / DVD drive.
2) Click XGate Sensor on the Installation Options screen.
3) Follow the instructions on screen.

Running a Scan

1) On your Windows Desktop, right click the XGate Sensor icon.



2) Move your mouse cursor to Scan and the options to start an Anti-Virus, Identity Protection or All Modules scan will appear. Click the type of scan you wish to complete.
3) The Sensor Scan will start and a notification message will appear in the bottom right.

By default, the sensor scan window will be minimised in the Windows task bar. If you wish to view the sensor scan window, click the application listed in the Windows task bar.

The sensor scan window gives you the option to pause or cancel the scan at any time.

Configuring a Scan

1) On your Windows Taskbar, right click the XGate Sensor icon.
2) Click Settings

The following options are available:

Manual Scan Options
Enable Anti-Virus
Enables or disables Anti-Virus scans from your current computer.

Enable Identity Protection
Enables or disables Identity Protection scans from your current computer.

Scan Type.
This can be set as:

Fast Scan-	Will only scan vital system files.
Full Scan -	Will scan all files on the computer.

Number of Engines
This determines the number of Anti-Virus and Identity Protection engines that will be used to scan for viruses. As each engine has different definitions of Viruses and Spyware, the greater number of engines, the less chance a Virus may infect your computers.

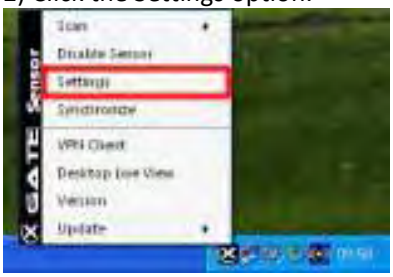
Scan Display Mode
Maximised Window
When a Scan is started, the Sensor Scan Window will be appear on the desktop. This will catch your attention but may distract you if you are using your computer at the time.

Minimised in Taskbar
When a Scan is stated, the Sensor Scan window will be minimised in the taskbar. This means that you will not be disrupted by the scanning window if you are currently using the computer. (e.g. watching a movie). To see the scanning window, click on XGate Scanning in the task bar.

Hidden
If this option is selected then the scanning window will be hidden from view when a scan is running. To view the scanning window, click the XGate Sensor icon in the task bar and select View Scan.

Enabling and Disabling Modules

1) On your Windows Desktop, right click the XGate Sensor icon.
2) Click the Settings option.



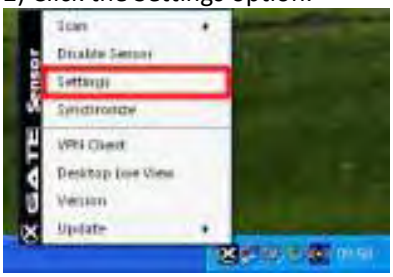
3) Click the Module Options tab. You can disable the modules here by un-ticking the appropriate tick boxes.

Note: If some of the modules are greyed out, this is due to the settings within Network Defence Control Rights. For more information see the Network Defence Control Rights section.

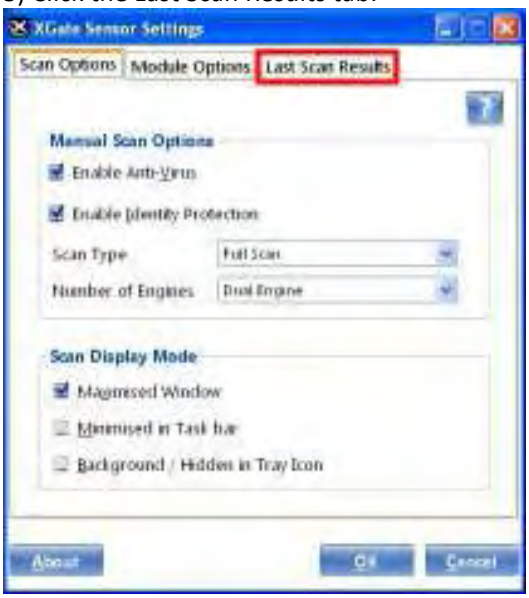
Viewing your Last Scan Results

Viewing your Last Scan Results

1) On your Windows Desktop, right click the XGate Sensor icon.
2) Click the Settings option.



3) Click the Last Scan Results tab.



Desktop Live View

What is Desktop Live View?

Desktop Live View gives real-time views of all connected desktops for monitoring and reporting purposes.

To have access to Desktop Live View, the XGate Sensor must be installed on the machine. For more details, please see the XGate Sensor section.

Also be aware that the other computers in your network must have the XGate sensor installed if you wish to see them within the Desktop Live View program.

Analogy

A good real life comparison with Desktop Live View is the use of CCTV (Closed-circuit television). CCTV allows you to observe and monitor events where the cameras are in place. In the case of XGate, your cameras are the XGate Sensor.

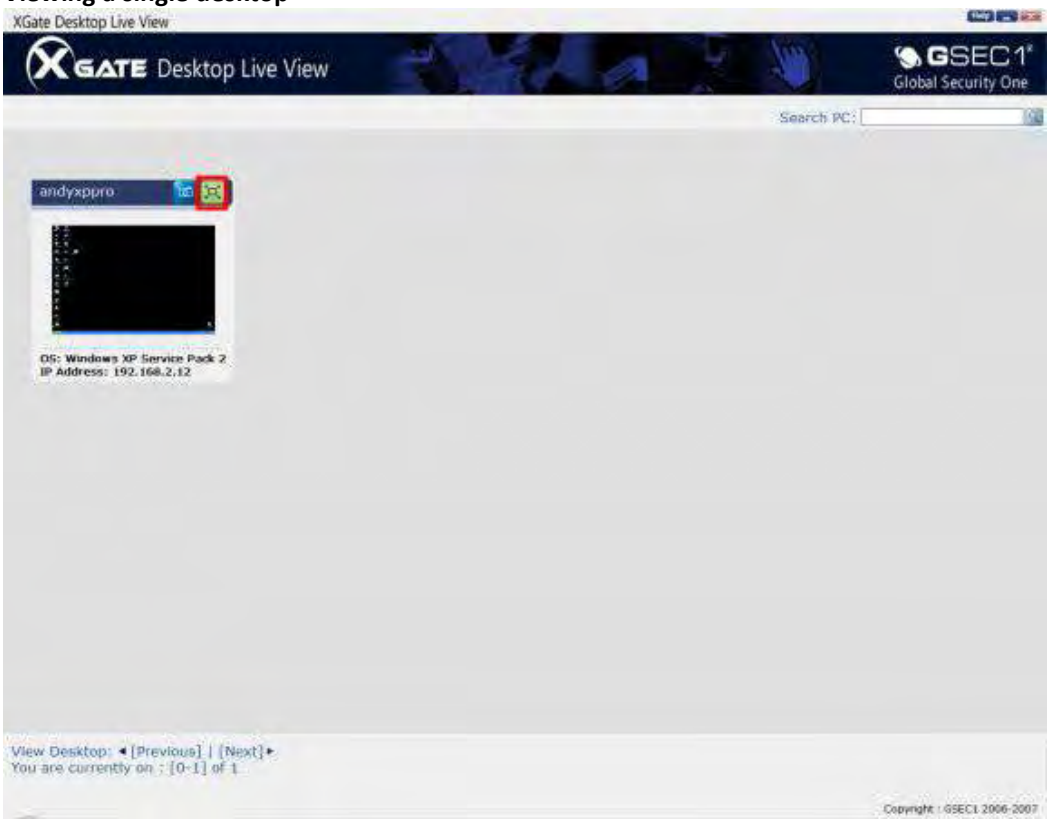
Starting Desktop Live View

To start the Desktop Live View program:
1) On your system tray, right click the XGate Sensor Icon. This will bring up a menu.
2) Left click Desktop Live View. This will open the Desktop Live View program.

Using Desktop Live View

Within Desktop Live View, there are a number of actions you can achieve. This page lists each of those actions and the method to perform them.

Viewing a single desktop

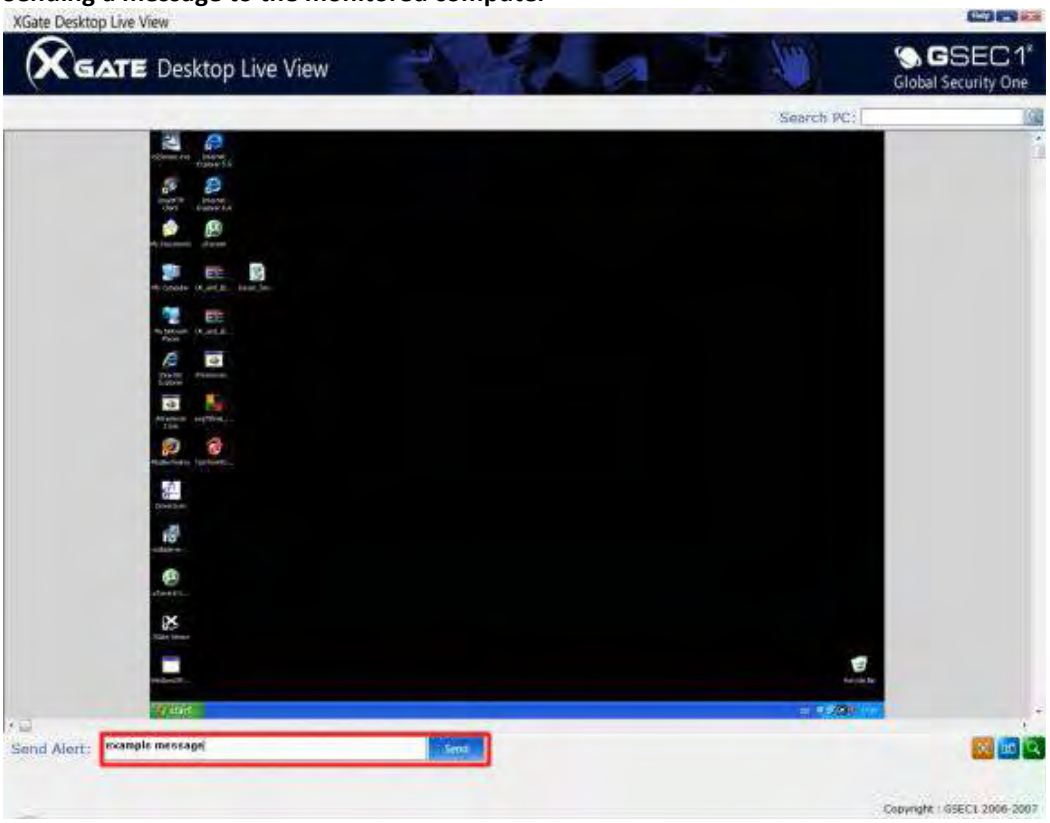


To view a full screen single desktop, double click on the screen you wish to view. Alternatively, you can press the associated green maximise button of the screen you wish to view.

Taking a screenshot of a desktop

Press the blue camera button to take a screenshot of a desktop. You can find the screenshots in the \bin\images folder of the XGate installation directory, on the computer where you are using Desktop Live View.

Sending a message to the monitored computer



To send a message, maximise a desktop then type in a message in the text at the bottom of

the screen and press Enter.

Introduction

VPN Client

What is the VPN Client?

XGate VPN Client Manager allows you to create a secure connection between computers over the Internet. Two connection methods are supported in the XGate VPN Client Manager:

- PPTP
- L2TP / IPSec

PPTP enables remote uses to access corporate networks securely across the Microsoft Windows platform. PPTP is widely used for remote access because it is easy to configure and does not require any additional software.

PPTP supports authentication, encryption and packet filtering. PPTP authentication uses PPP-based protocols such as EAP, CHAP and PAP.

L2TP technology enables remote users to access corporate networks securely. It is more secure than PPTP and uses Internet Key Exchange (IKE) and Internet Protocol Security (IPSec) tunnelling protocols to create and manage a secure connection.

The XGate VPN Client Manager allows you to:

- Negotiate tunnelling parameters like addresses, algorithms and lifetime, pre- shared key etc.
- Authentication of users by usernames and passwords.
- Establishment of user access rights and tunnels based on the parameters provided.
- Management of security keys for encryption and decryption.
- Allows L2TP/IPsec clients to negotiate and use the Diffie-Hellman Group 2048 protocol.
- Authentication, encryption and decryption of data through the tunnel.

For example, to use a remote PC to read e-mail from your company's network you need to connect to the Internet. You then start the VPN Client and establish a secure connection through the Internet to your company's private network. When you open your e-mail, the VPN server will use IPSec to encrypt the e-mail message. It then transmits the message through the secure tunnel to GSEC1's VPN Client which will decrypt the message so you can read it on your remote PC. If you reply to the e- mail message, the VPN Client uses IPSec to decrypt and return the message to the private network.

When setting up a VPN connection, the following details are required:

Connection Name
A name you define to easily identify the VPN Connection.

Connection Type
Either L2TP / IPsec or PPTP.

Remote Host Name or IP Address
The Host Name / IP Address of the Remote VPN Server.

Username

Username used for logging on to the VPN Server.

Password
Password for logging on to the VPN Server.

Shared Secret
This is the key for authentication, which applies only for L2TP / IPSec connections. This field is not available for PPTP connections.

The Advanced button allows you to enable the following additional settings.
Enable Packet Compression
This will enable the packet compression for this connection. This option is only available for L2TP / IPSec connections.

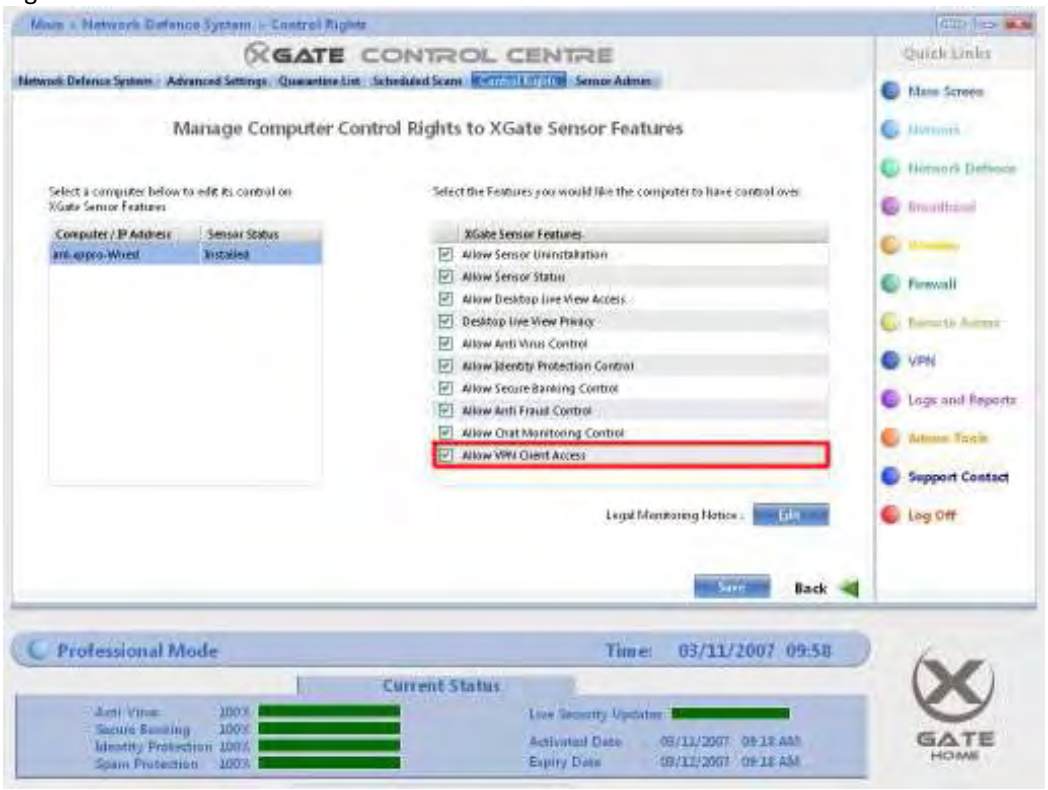
Enable Remote Gateway
This will configure the default gateway of the VPN Client machine as the remote VPN Server. Un-checking this tick box will restore the VPN Client machine's default gateway.

By enabling the remote gateway you will be restricted to one active VPN Connection.

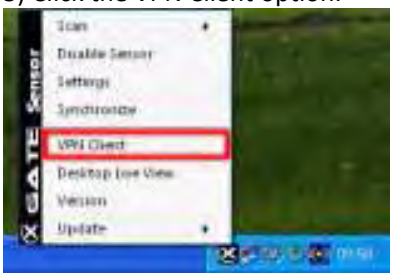
Create a new VPN Connection

Creating a new VPN Connection

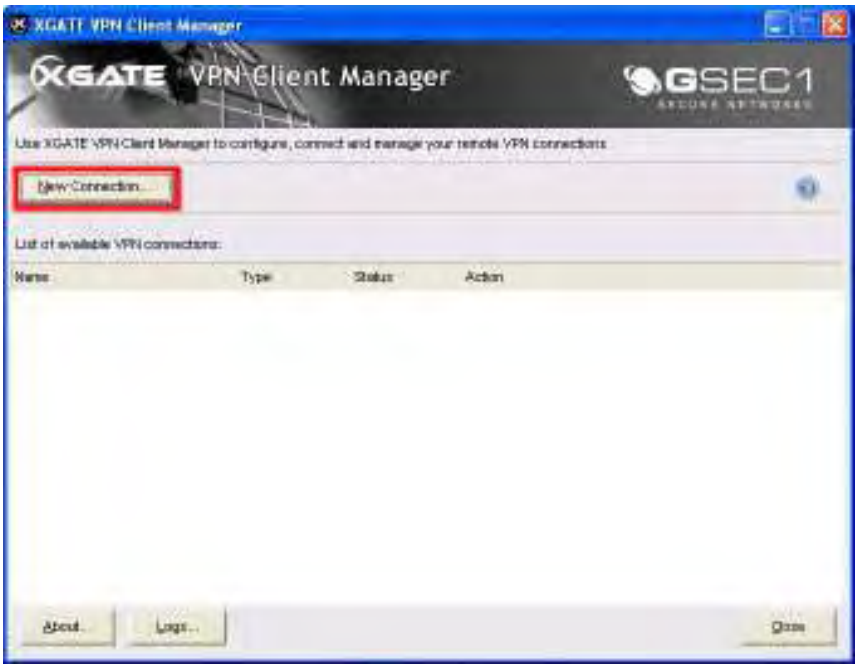
1) Ensure that the VPN client is enabled for the computer in Network Defence Control Rights.



2) On your Windows Desktop, right click the XGate Sensor icon.
3) Click the VPN Client option.

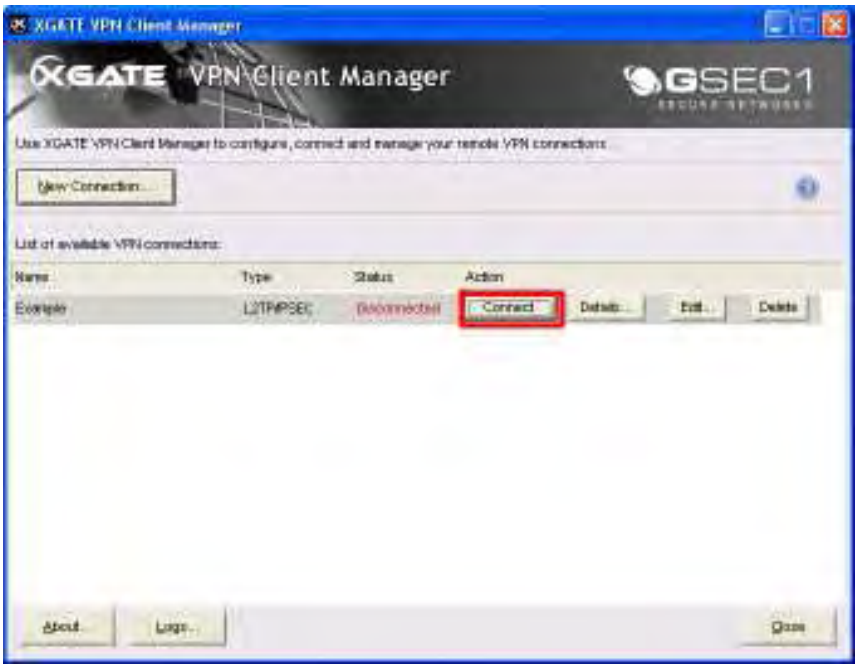


4) Press the New Connection… button.



5) Complete your connection details in the New Connection window.
6) Press OK to confirm your entry.

Connecting or Disconnecting a VPN Connection



When the Connection Status is disconnected, pressing the Connect button will attempt to establish the connection to the Remote Server.

If duplicate entries are found, an error message will be displayed, as shown below.

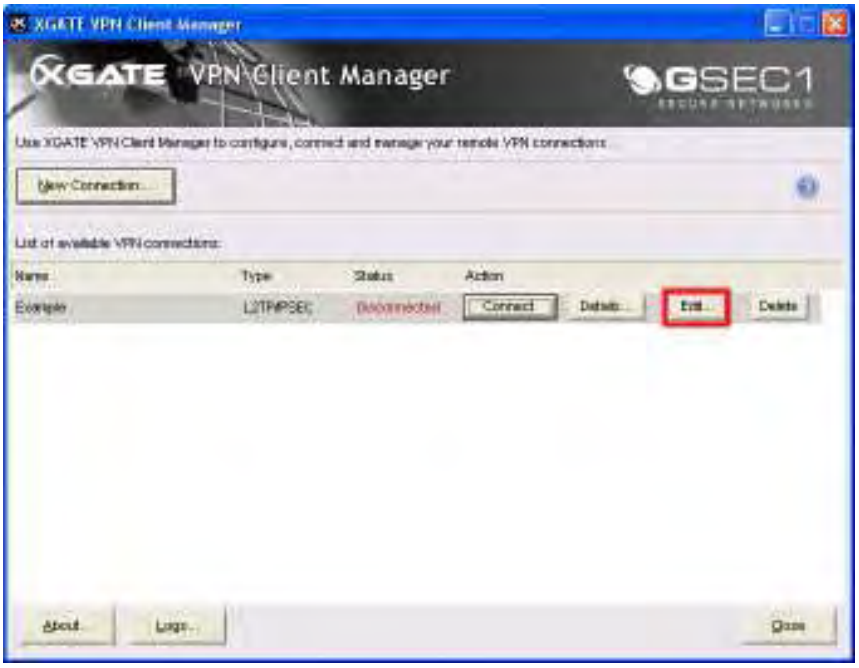
While attempting to connect, the process window will display all stages of the connection process.

When the connection has been successfully established, the Status of the connection will change to Connected and the Connect button will be shown as Disconnect.

If the Disconnect button is pressed it will disconnect that specific VPN connection.. A prompt will appear to you, asking to confirm your decision. If you select Yes, the VPN Client will disconnect from the VPN Server.

Changing the details of a VPN Connection

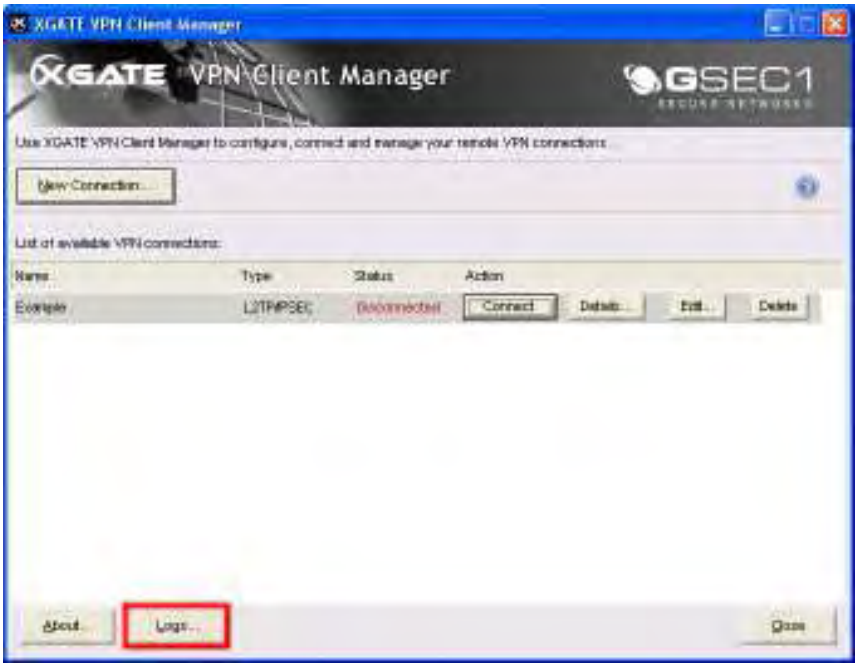
A VPN Connection can only be edited if its connection status is shown as Disconnected.



To edit a VPN connection, press the Edit button relating to it.

Using the XGate VPN Client Manager Logs

You can access the VPN Client Manager Logs by clicking the Logs button.



The following describes all the actions that can be carried out:

Clear Logs button
This allows you to clear the logs in the Log Viewer window.

Pause button
This will stop updating the logs so you can go through the logs available in the log viewer window without being distracted.

Save logs button
This will prompt a save window. This allows you to save the currently displayed logs to a file.

Copy Logs button
This allows you to copy the currently displayed logs on to your computer's clipboard. This allows you to paste the logs to a word document for example.