Introduction

## Keyword Filter

### What is the Keyword Filter?

The Keyword Filter is another part of the Spam Filter which is used to block or allow e-mails containing specific keywords set by you.

### Keyword Filter Details

Keyword Filter for E-mail

This can be set as the Subject, Message body or Both. This is the field that XGate will search when looking for the specified Keyword.

Custom Keyword

This is the keyword that will be blocked when found in the field specified above.

## Adding a Keyword Filter

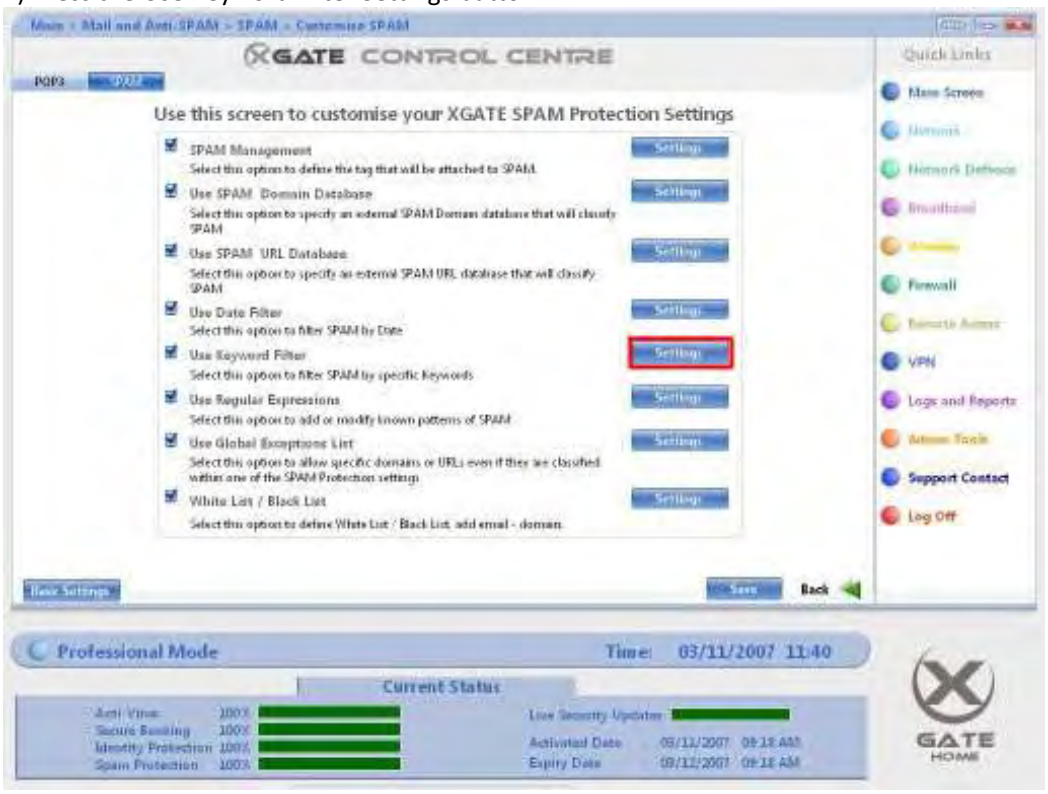
1) Press the Mail and Anti-spam button.


2) Ensure that POP3 has been switched on.
3) Click the Spam Tab.

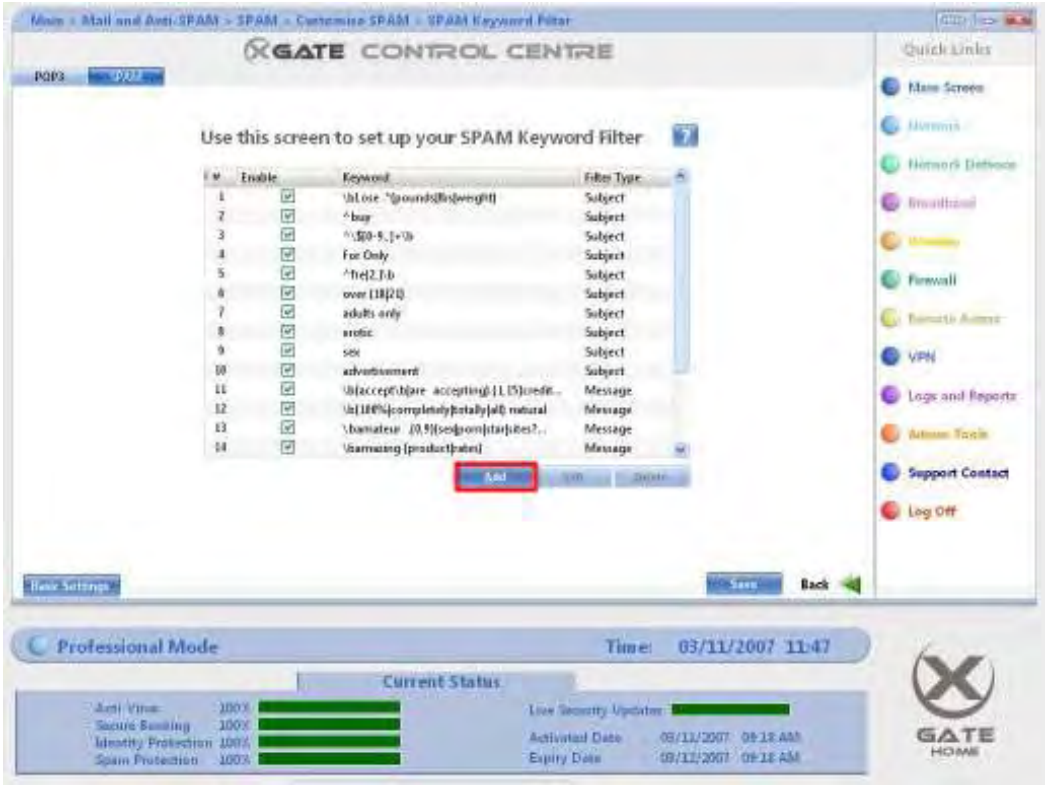

4) Ensure that Spam has been swiched on.
5) Click on Customise SPAM Protection.


3) Ensure that the Use Keyword Filter tick box is ticked.

4) Press the Use Keyword Filter Settings button.

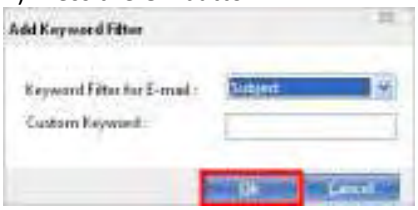



5) Press the Add button.

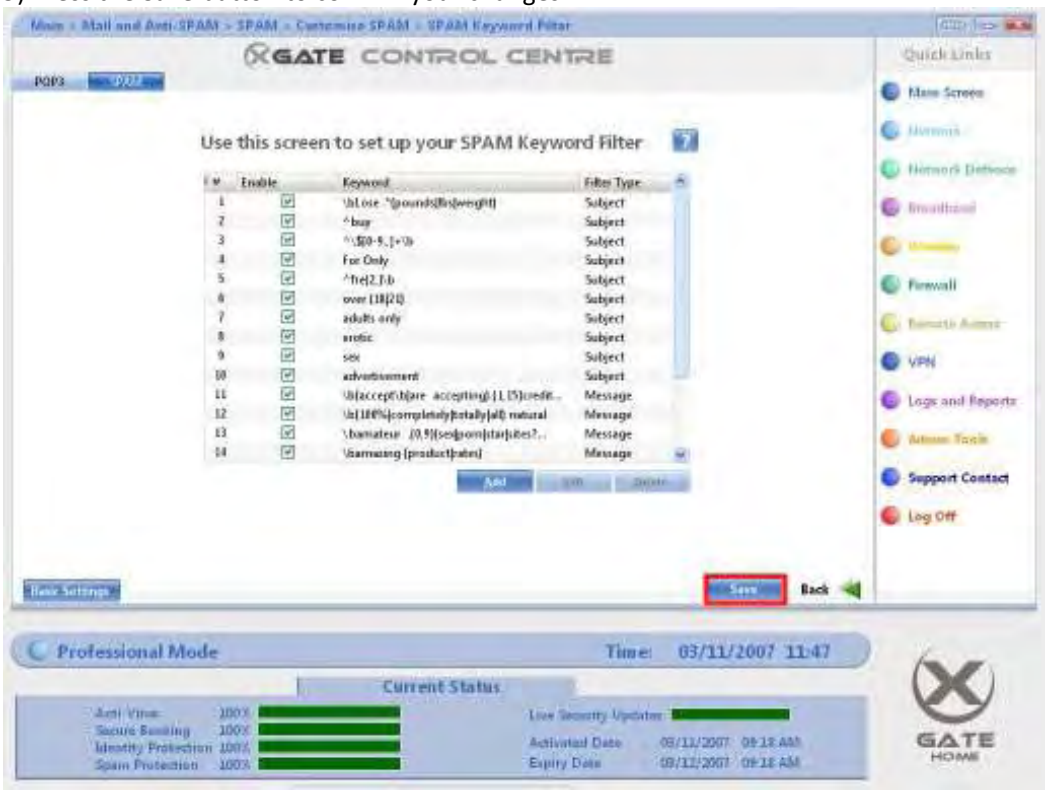



6) Enter your Keyword Filter details

7) Press the OK button.




9) Press the Save button to confirm your changes.



## Changing the details of a Keyword filter

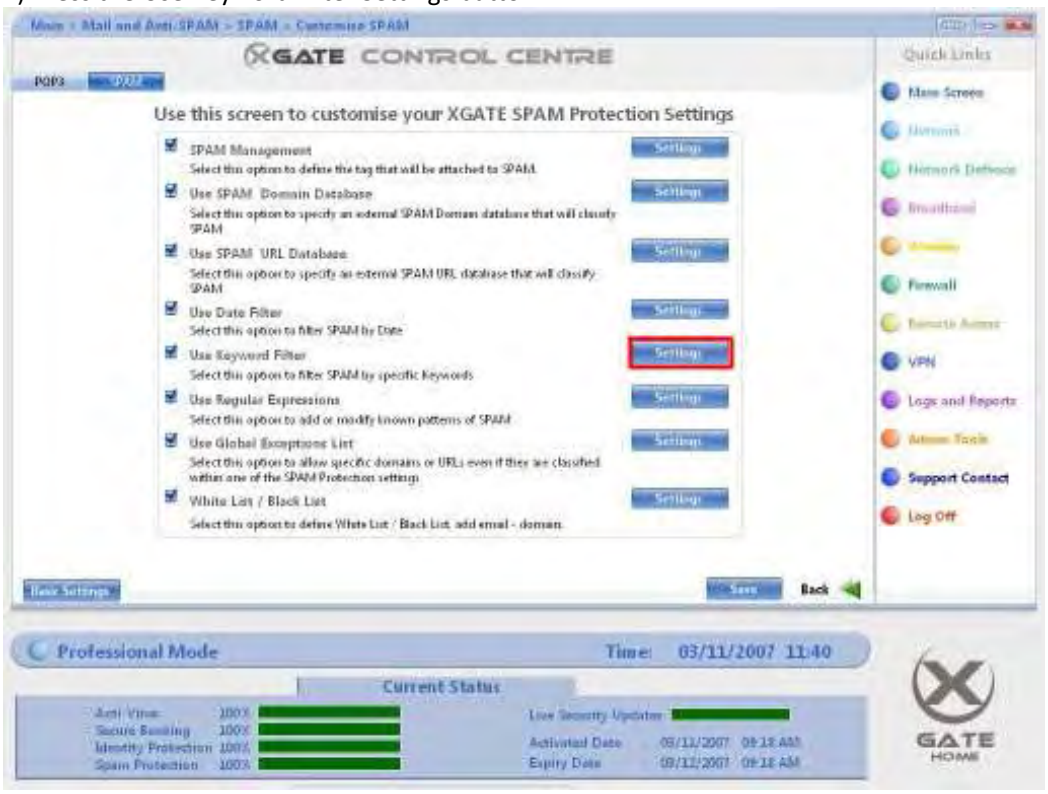
1) Press the Mail and Anti-spam button.


2) Ensure that POP3 has been switched on.
3) Click the Spam Tab.

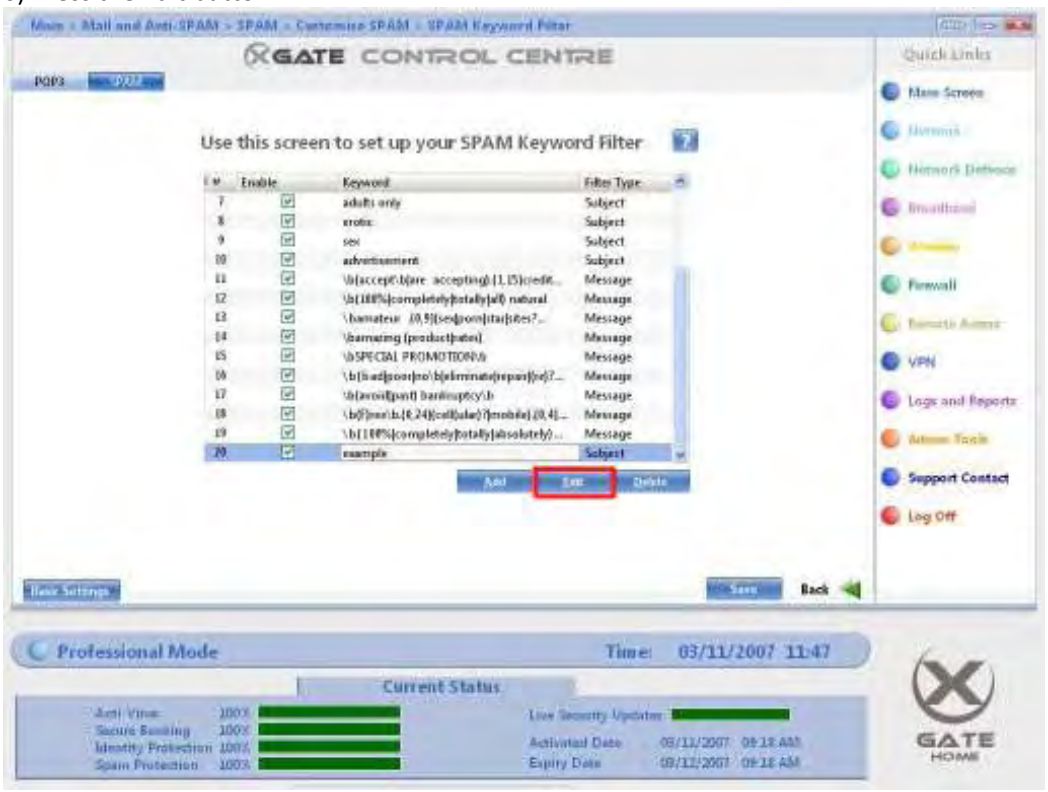

4) Ensure that Spam has been swiched on.
5) Click on Customise SPAM Protection.


3) Ensure that the Use Keyword Filter tick box is ticked.

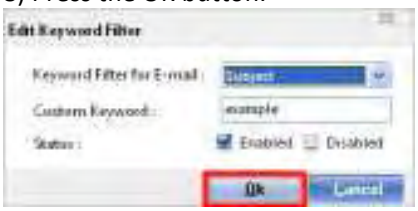
4) Press the Use Keyword Filter Settings button.



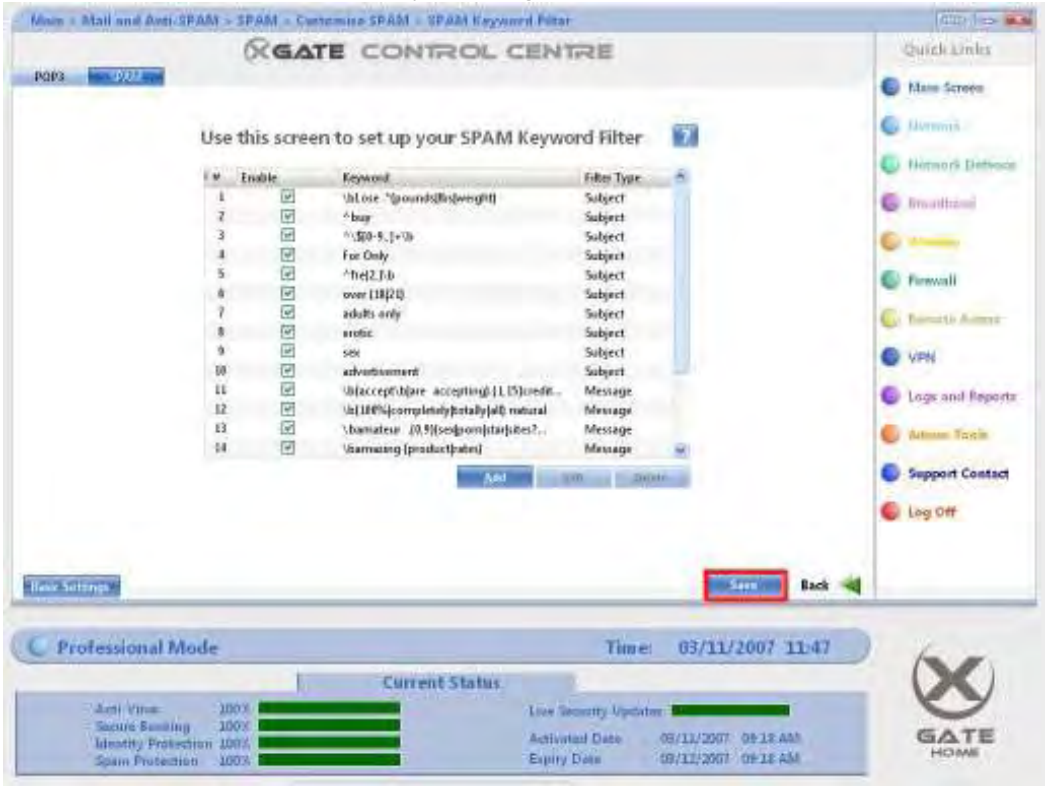

5) Select the entry you wish to edit. This will highlight the entry.
6) Press the Edit button.



7) Amend the details of the Keyword Filter.
8) Press the OK button.




9) Press the Save button to confirm your changes.



**Removing a Keyword Filter**

1) Press the Mail and Anti-spam button.

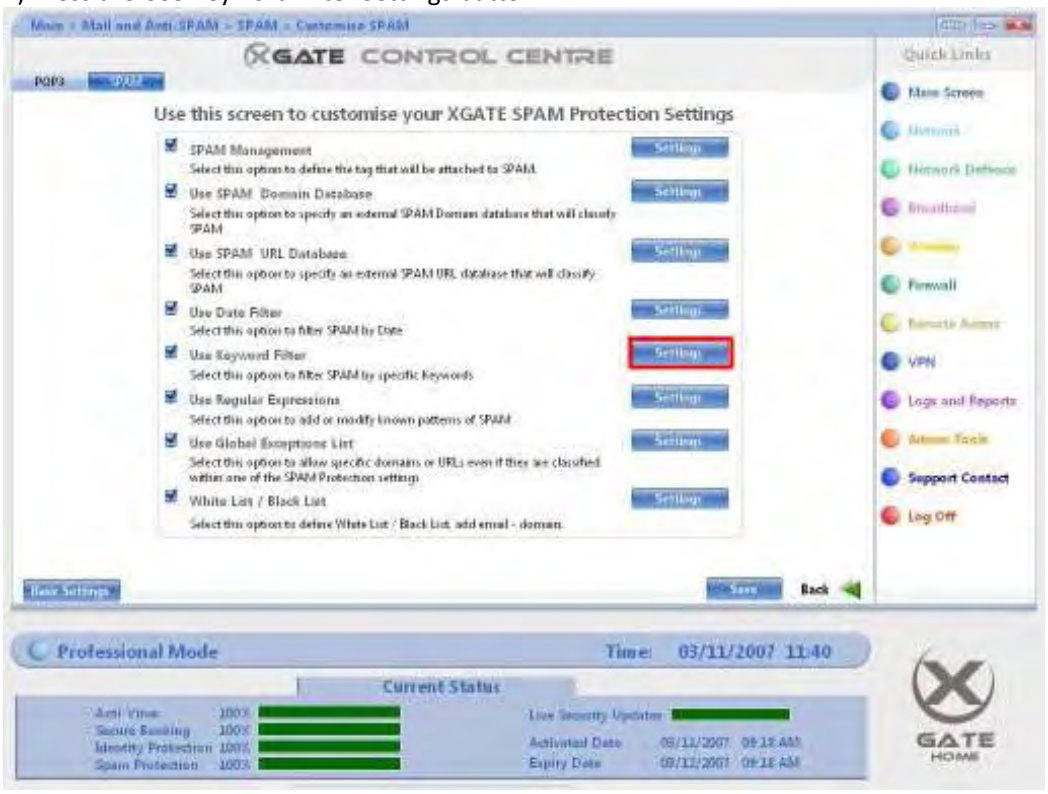

2) Ensure that POP3 has been switched on.

3) Click the Spam Tab.

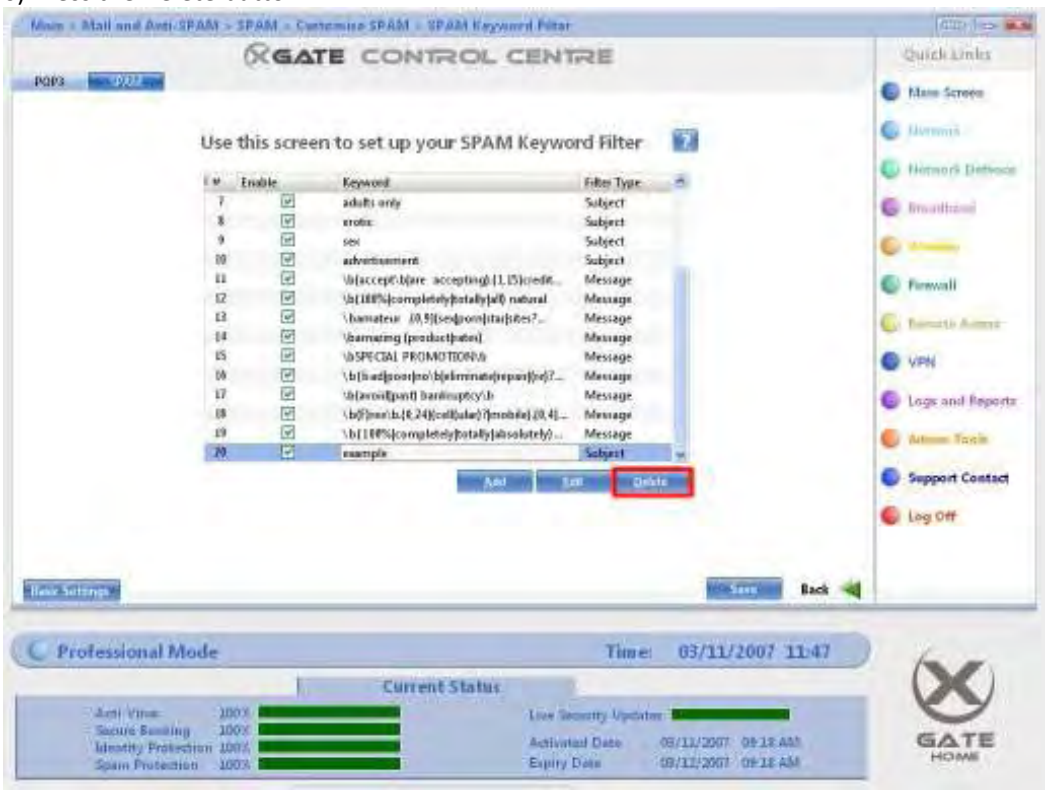

4) Ensure that Spam has been swiched on.
5) Click on Customise SPAM Protection.


3) Ensure that the Use Keyword Filter tick box is ticked.

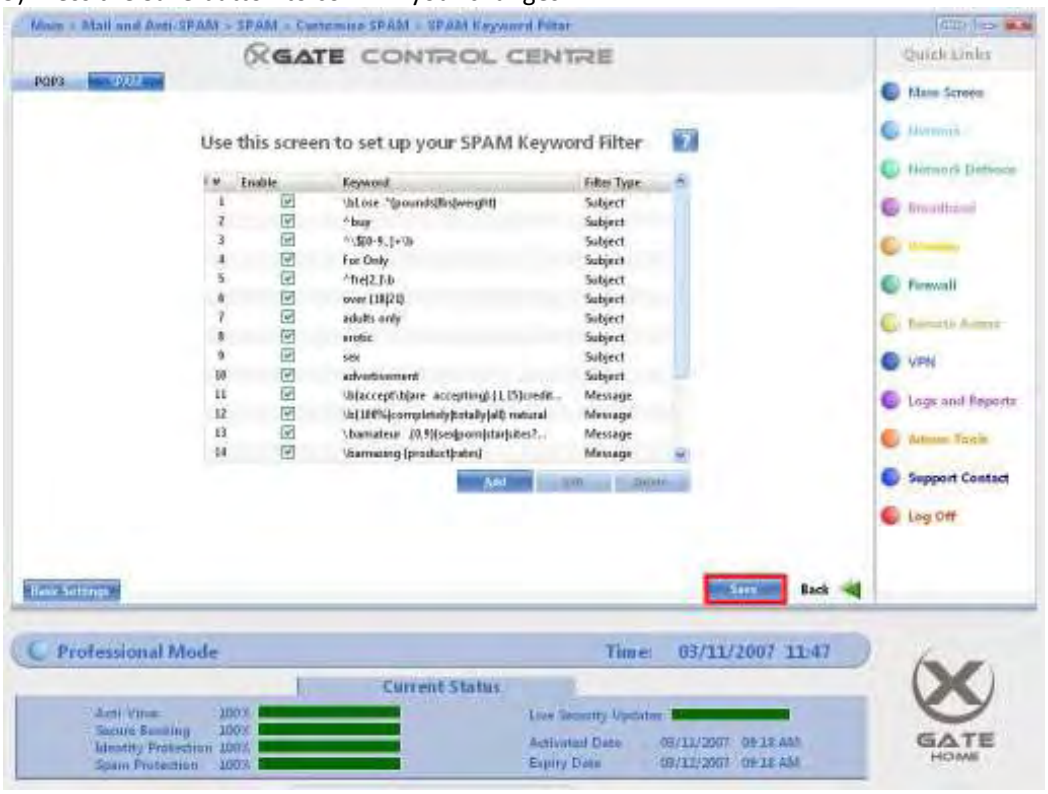
4) Press the Use Keyword Filter Settings button.




5) Select the entry you wish to edit. This will highlight the entry.
6) Press the Delete button.



9) Press the Save button to confirm your changes.



Introduction

## Regular Expressions

### What is a Regular Expression?

A Regular Expression is a sequence of characters that describe a pattern.

Regular expressions can be used in e-mail spam filtering to describe and help detect various forms of spam patterns. Patterns are specified with the use of "wild card characters".

XGate uses the wild card characters: * and ?.

* = used to substitute multiple characters.
? = used to substitute a single character.

For example, if you wish to block the e-mail addresses:
test1@yahoo.com
test2@yahoo.com
test3@yaretoo.com

You would use the following regular expression to cover all these e-mail addresses:
test?@ya*oo.com

### Analogy

Wild Cards derive from card games. A wild card can be designated by its holder to any card they wish. In many card games, Jokers are the wild cards.

In the same way, in XGate, the wild cards that are used are the characters * and ?.

### Regular Expression Details

To enter a regular expression, the following details are necessary:

Select
This can be either an E-mail Address or Domain.

E-mail Address/Domain
This is the e-mail address or domain, with wild card characters.

Action:
Choose whether to allow or block the specified e-mail address or domain regular expression.

## Adding a Regular Expression

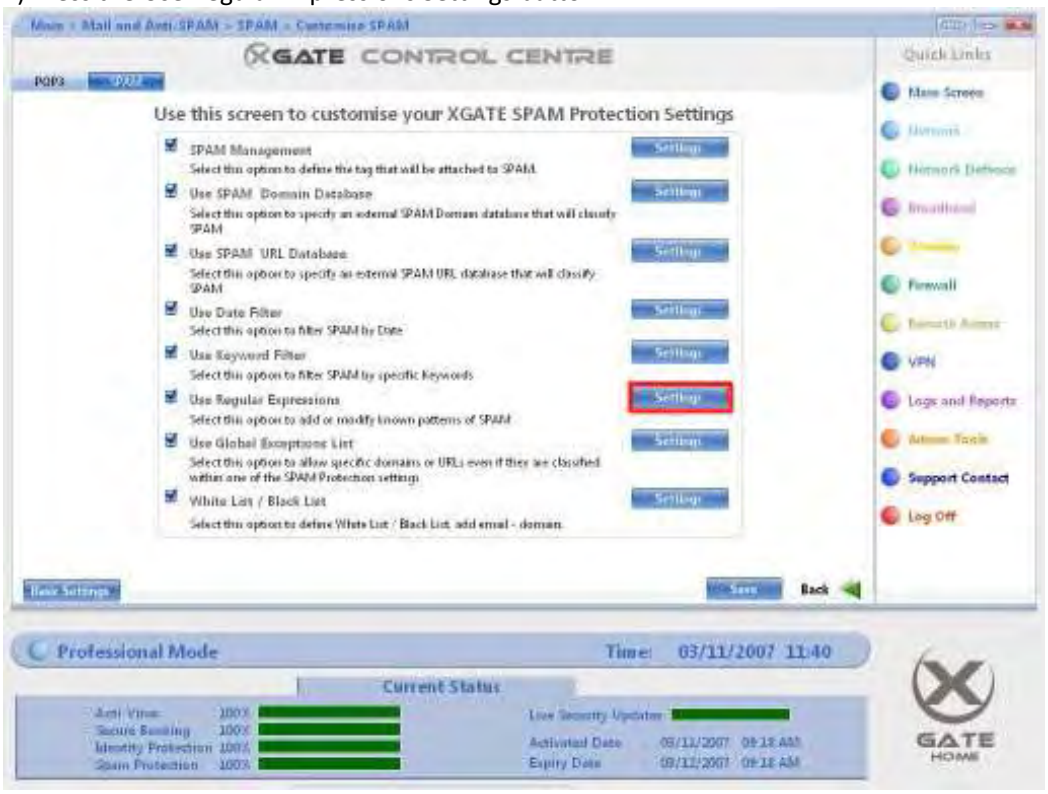
1) Press the Mail and Anti-spam button.


2) Ensure that POP3 has been switched on.
3) Click the Spam Tab.


4) Ensure that Spam has been swiched on.
5) Click on Customise SPAM Protection.


3) Ensure that the Use Regular Expressions tick box is ticked.

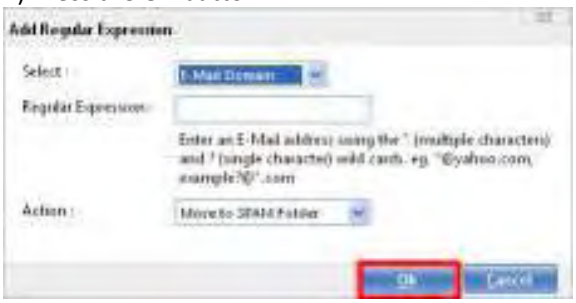
4) Press the Use Regular Expressions Settings button.




5) Press the Add button.


6) Enter your Regular Expression details.

7) Press the OK button.




8) Press the Save button to confirm your changes.

## Changing a Regular Expression

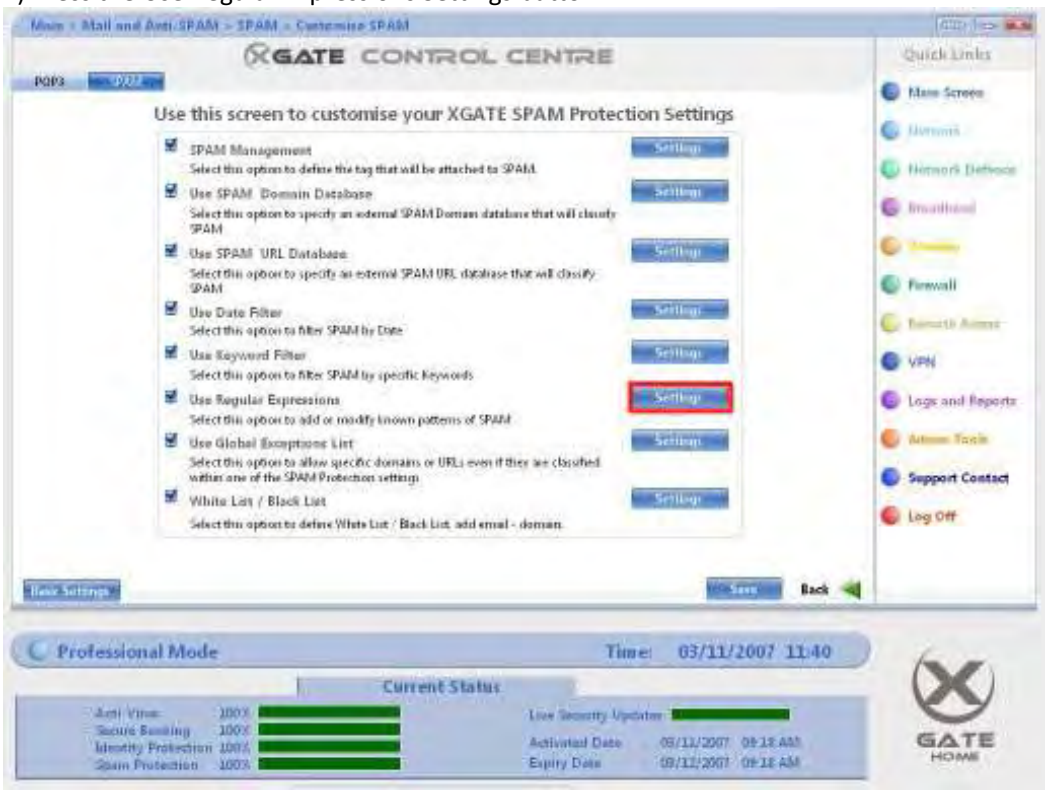
1) Press the Mail and Anti-spam button.


2) Ensure that POP3 has been switched on.
3) Click the Spam Tab.


4) Ensure that Spam has been swiched on.
5) Click on Customise SPAM Protection.

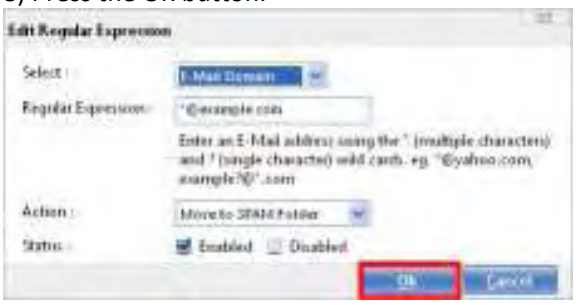

3) Ensure that the Use Regular Expression tick box is ticked.

4) Press the Use Regular Expressions Settings button.




5) Select the entry you wish to edit. This will highlight the entry.
6) Press the Edit button.

7) Amend the details of the Regular Expression.
8) Press the OK button.




9) Press the Save button to confirm your changes.

**Removing a Regular Expression**

1) Press the Mail and Anti-spam button.

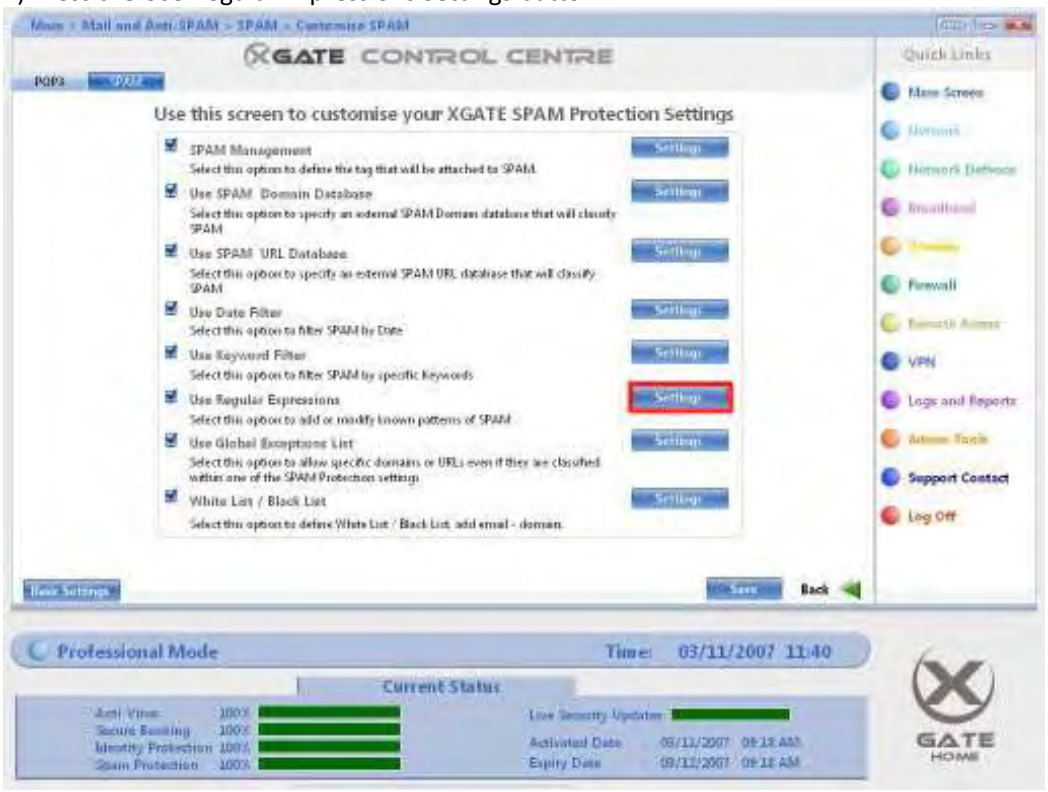

2) Ensure that POP3 has been switched on.

3) Click the Spam Tab.

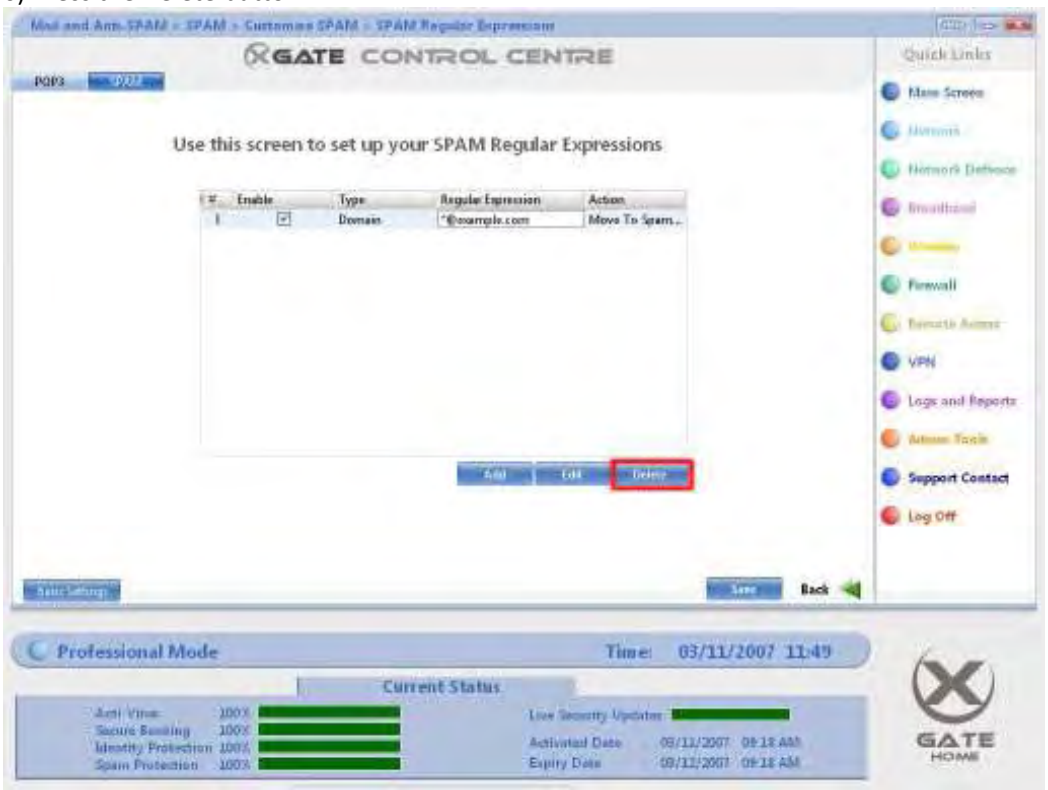

4) Ensure that Spam has been swiched on.
5) Click on Customise SPAM Protection.


3) Ensure that the Use Regular Expression tick box is ticked.

4) Press the Use Regular Expressions Settings button.




5) Select the entry you wish to edit. This will highlight the entry.
6) Press the Delete button.



7) Press the Save button to confirm your changes.

Introduction

## Global Exceptions

### What is a Global Exception?

The Global Exceptions screen allows you to specify e-mail addresses or domains that will be able to bypass the Spam filter on XGate. As such, anything specified in this list will not be filtered

### Global Exception Details

To add a global exception, the following details are required:

Type
This can be set as e-mail address or domain, according to the type you wish to be unaffected by the Anti-Spam filters in XGate.

Domain
The e-mail address or domain that you wish to be unaffected by the Anti-Spam filters in XGate.

## Adding a Global Exception

1) Press the Mail and Anti-spam button.

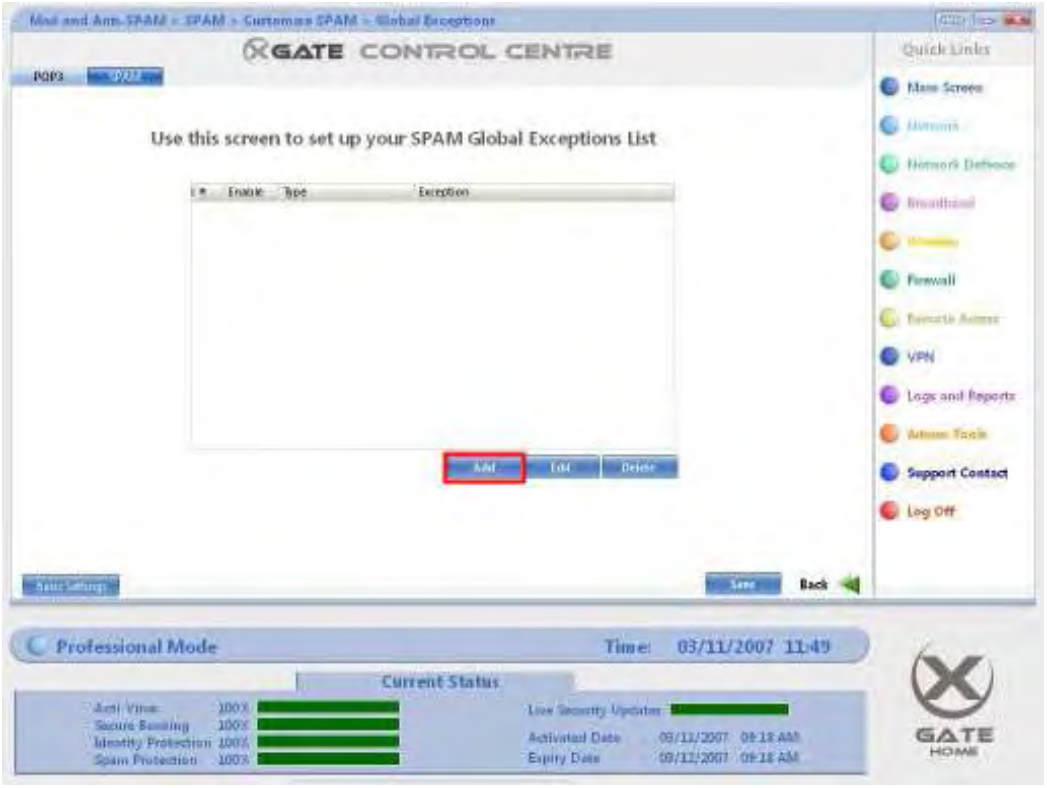

2) Ensure that POP3 has been switched on.
3) Click the Spam Tab.


4) Ensure that Spam has been swiched on.
5) Click on Customise SPAM Protection.


3) Ensure that the Use Global Exceptions tick box is ticked.

4) Press the Use Global Exceptions Settings button.

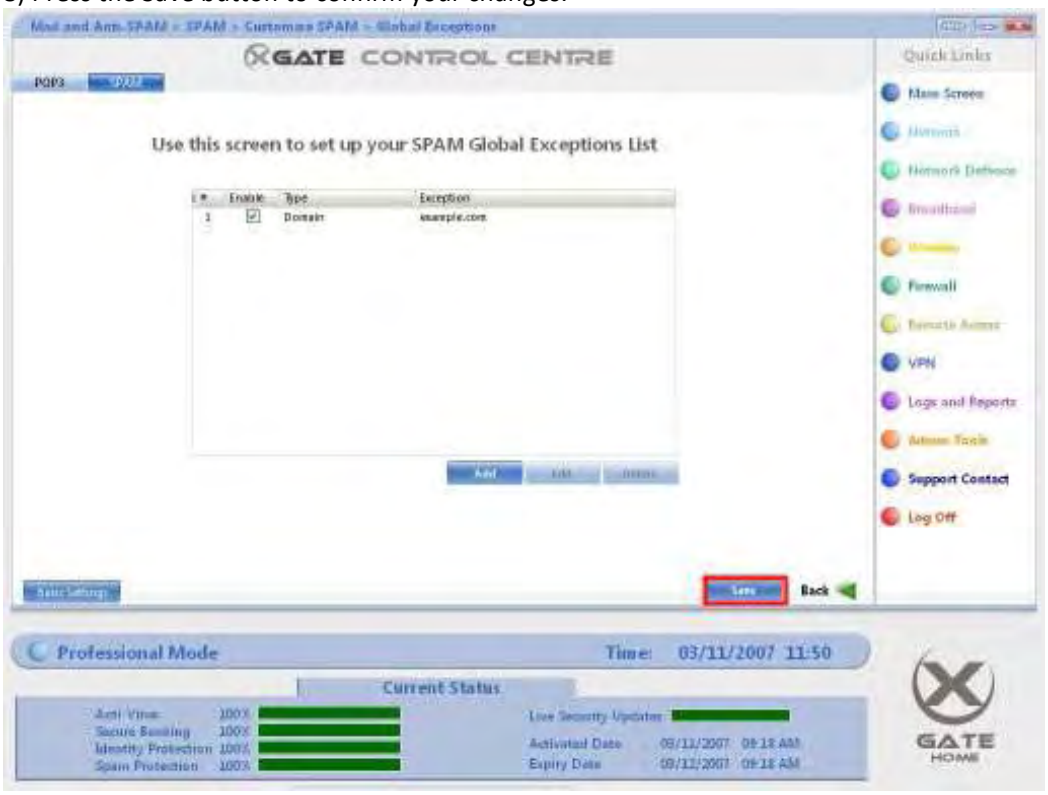

5) Press the Add button.




6) Enter your Global Exception details.

7) Press the OK button.


8) Press the Save button to confirm your changes.



## Changing a Global Exception

1) Press the Mail and Anti-spam button.

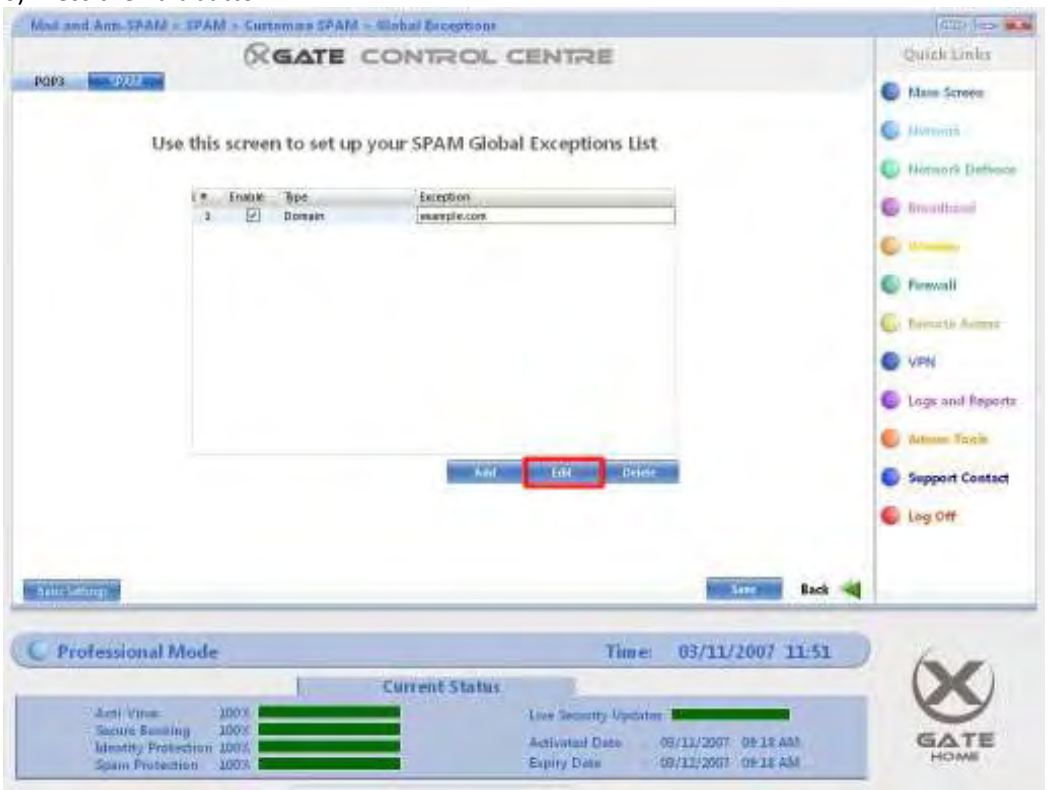

2) Ensure that POP3 has been switched on.
3) Click the Spam Tab.


4) Ensure that Spam has been swiched on.
5) Click on Customise SPAM Protection.

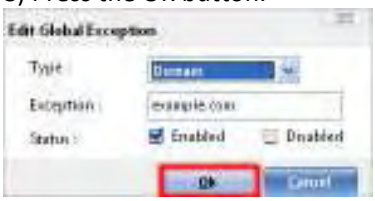

3) Ensure that the Use Global Exceptions tick box is ticked.

4) Press the Use Global Exceptions Settings button.

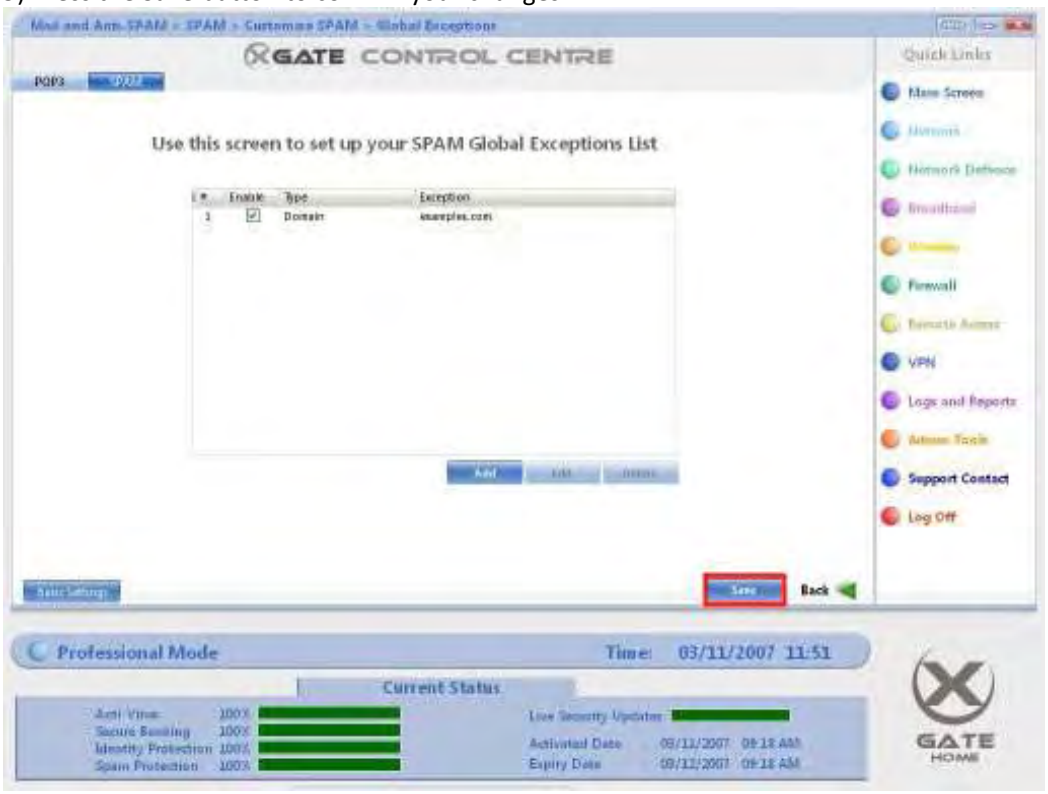

5) Select the entry you wish to edit. This will highlight the entry.
6) Press the Edit button.



7) Amend the details of the Global Exception.
8) Press the OK button.




9) Press the Save button to confirm your changes.



## Removing a Global Exception

1) Press the Mail and Anti-spam button.

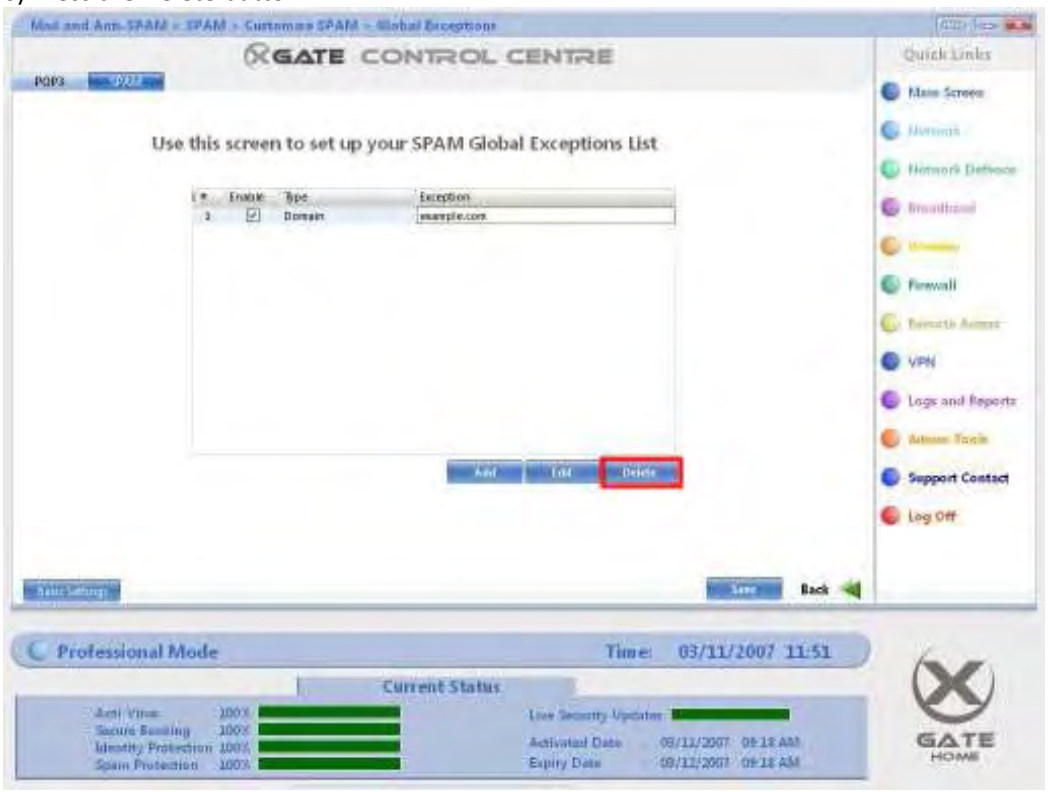

2) Ensure that POP3 has been switched on.
3) Click the Spam Tab.


4) Ensure that Spam has been swiched on.
5) Click on Customise SPAM Protection.

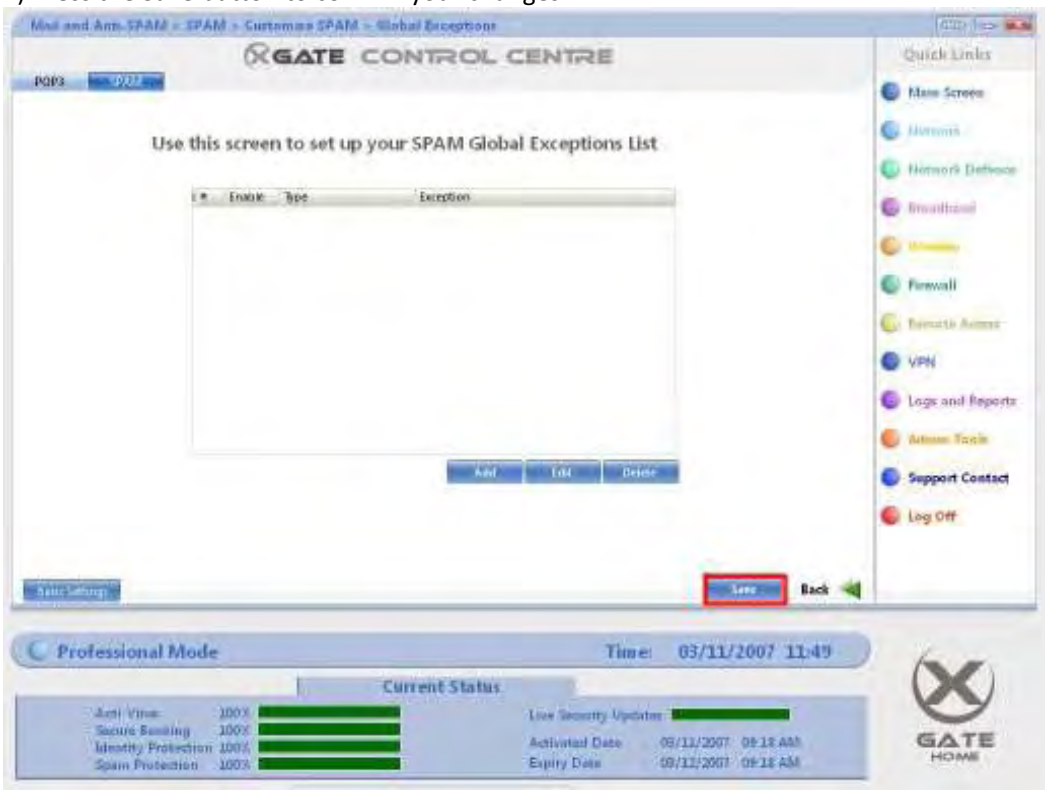

3) Ensure that the Use Global Exceptions tick box is ticked.

4) Press the Use Global Exceptions Settings button.


5) Select the entry you wish to edit. This will highlight the entry.
6) Press the Delete button.



7) Press the Save button to confirm your changes.



Introduction

## White / Black List

### What is the White / Black List?

The White / Black List screen is similar to the Global Exceptions and allows you to commit specific actions to specific e-mail addresses or domains. Where it mainly differs is that all SPAM classifications made by the XGate Anti-SPAM Outlook add-in will be placed in the White / Black List table.

### White / Black List Details

To add a White / Black List entry, the following details are required:

Filter Name
This is a friendly name to easily identify the White / Black List entry.

Domain / E-mail
The e-mail address or domain that you wish to be unaffected by the Anti-Spam filters in XGate.

Action
Allow - This will allow all mail that comes from the specified Domain / E-mail address
Deny - This will block all mail that comes from the specified Domain / E-mail address
Move to SPAM - This move all mail that comes from the specified Domain / E-mail address to the SPAM folder in Outlook.

## Adding a White / Black List entry

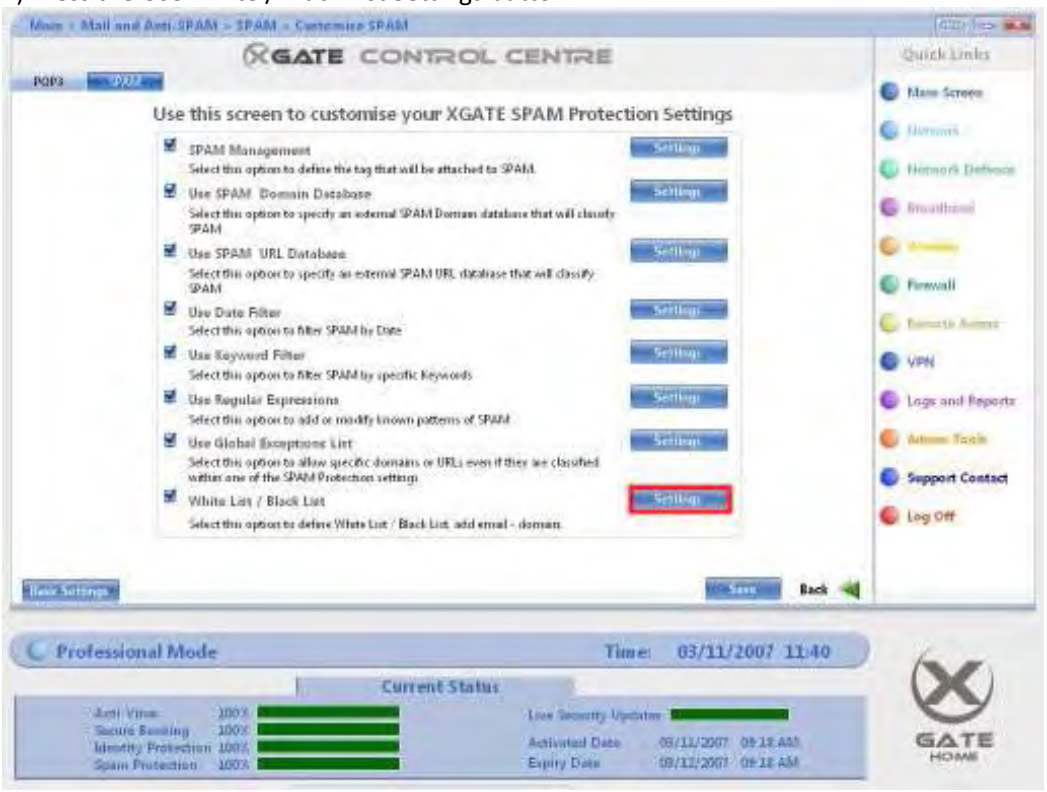
1) Press the Mail and Anti-Spam button.


2) Ensure that POP3 has been switched on.
3) Click the Spam Tab.

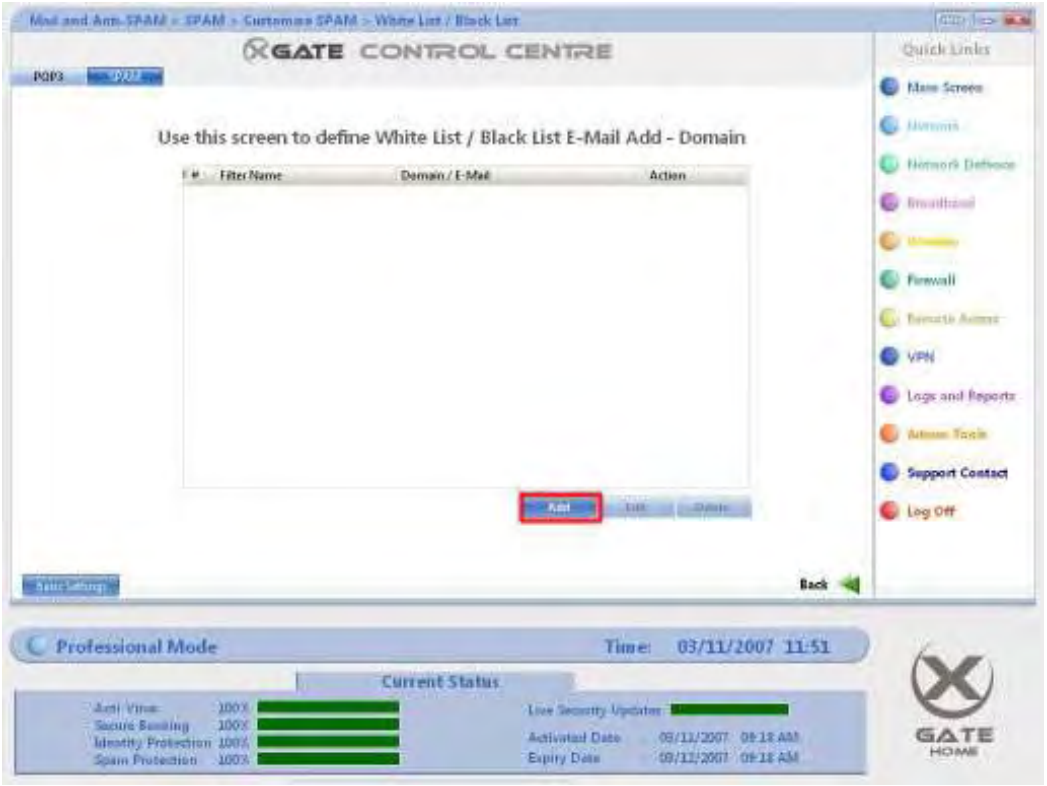

4) Ensure that Spam has been swiched on.
5) Click on Customise SPAM Protection.


3) Ensure that the Use White / Black List tick box is ticked.

4) Press the Use White / Black List Settings button.

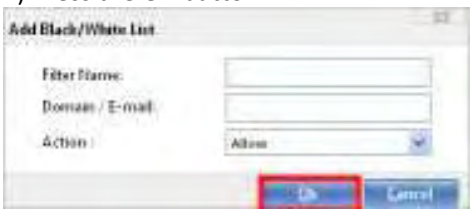



5) Press the Add button.




6) Enter the details of your White / Black List entry.

7) Press the OK button.



Changing a White / Black List entry

## Changing a Global Exception

1) Press the Mail and Anti-spam button.

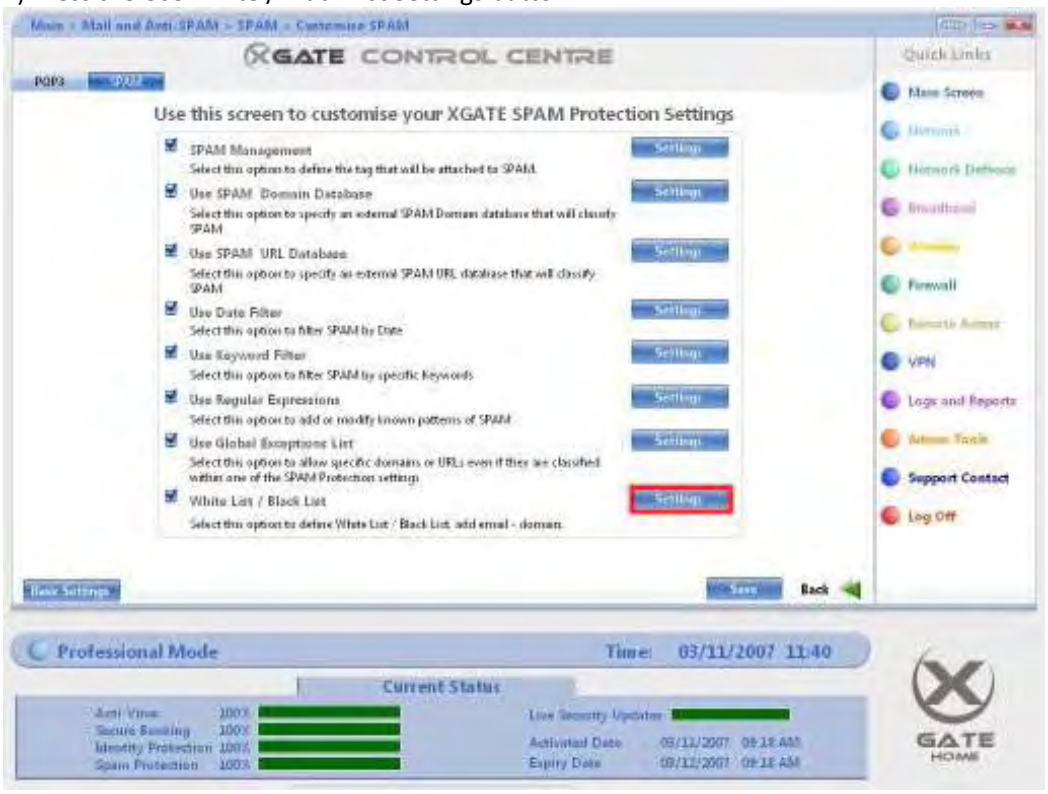

2) Ensure that POP3 has been switched on.

3) Click the Spam Tab.

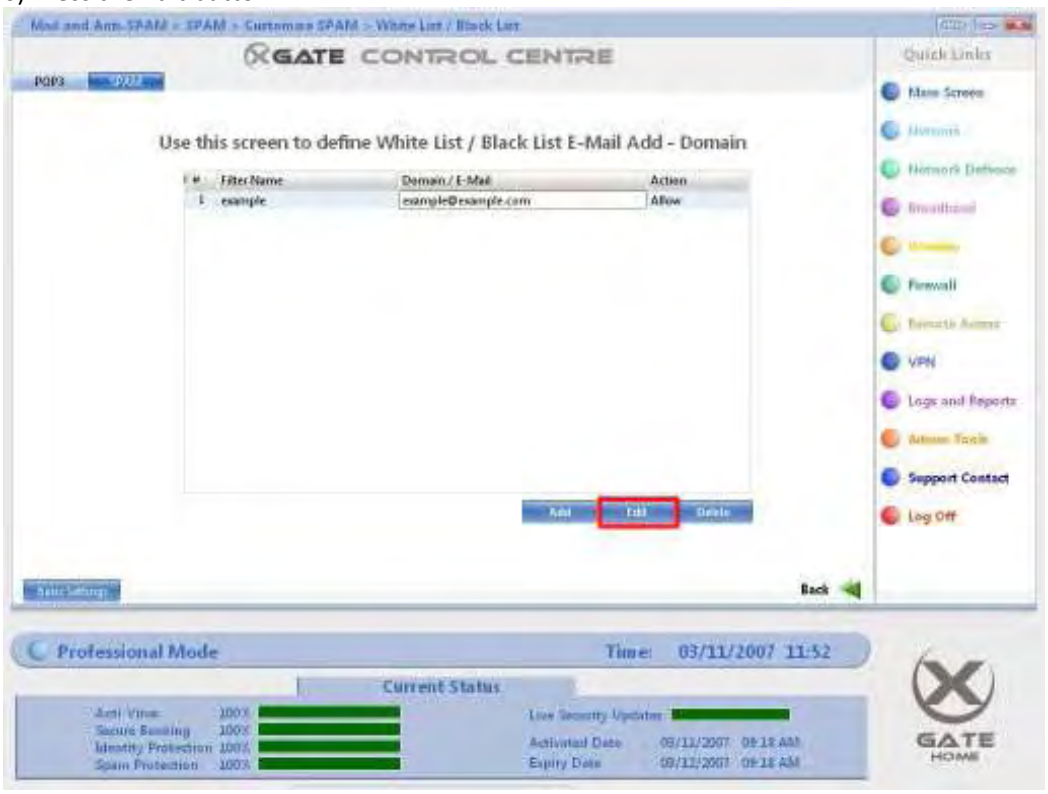

4) Ensure that Spam has been swiched on.
5) Click on Customise SPAM Protection.


3) Ensure that the Use White / Black List tick box is ticked.

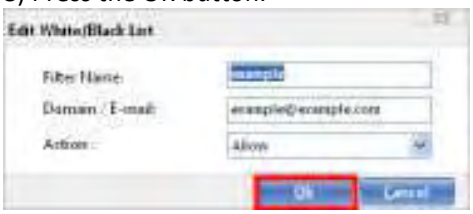
4) Press the Use White / Black List Settings button.




5) Select the entry you wish to edit. This will highlight the entry.
6) Press the Edit button.



7) Amend the details of the White / Black List entry.
8) Press the OK button.



## Removing a White / Black List entry

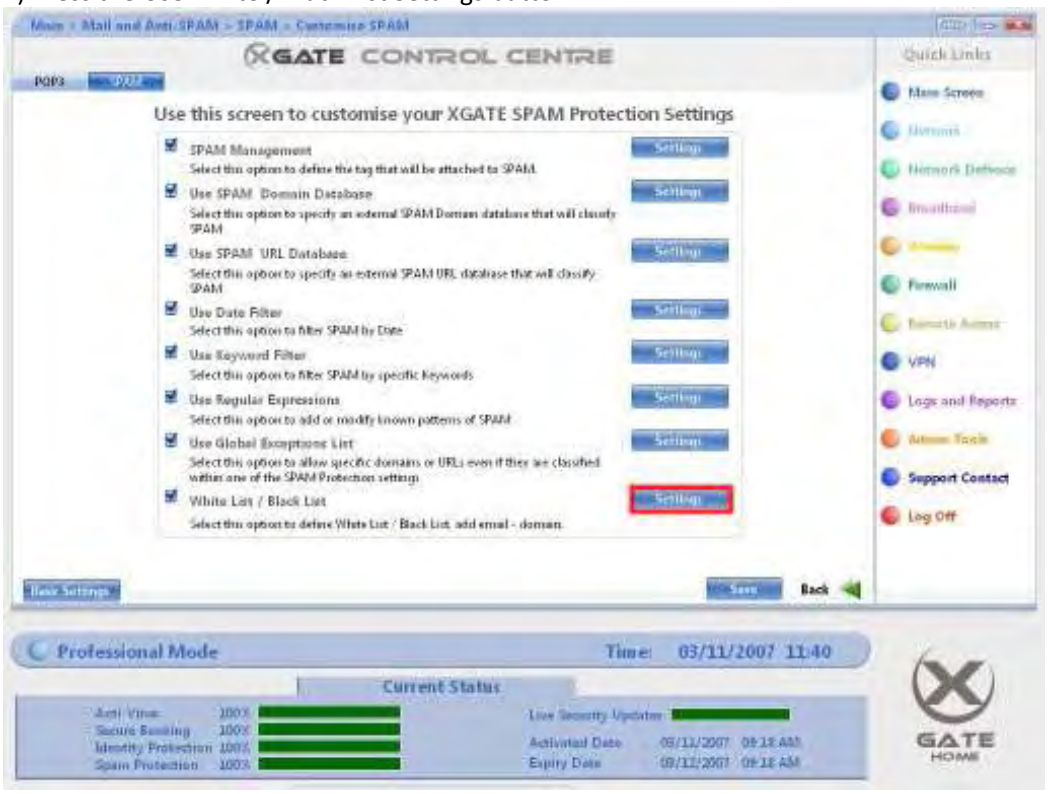
1) Press the Mail and Anti-spam button.


2) Ensure that POP3 has been switched on.
3) Click the Spam Tab.

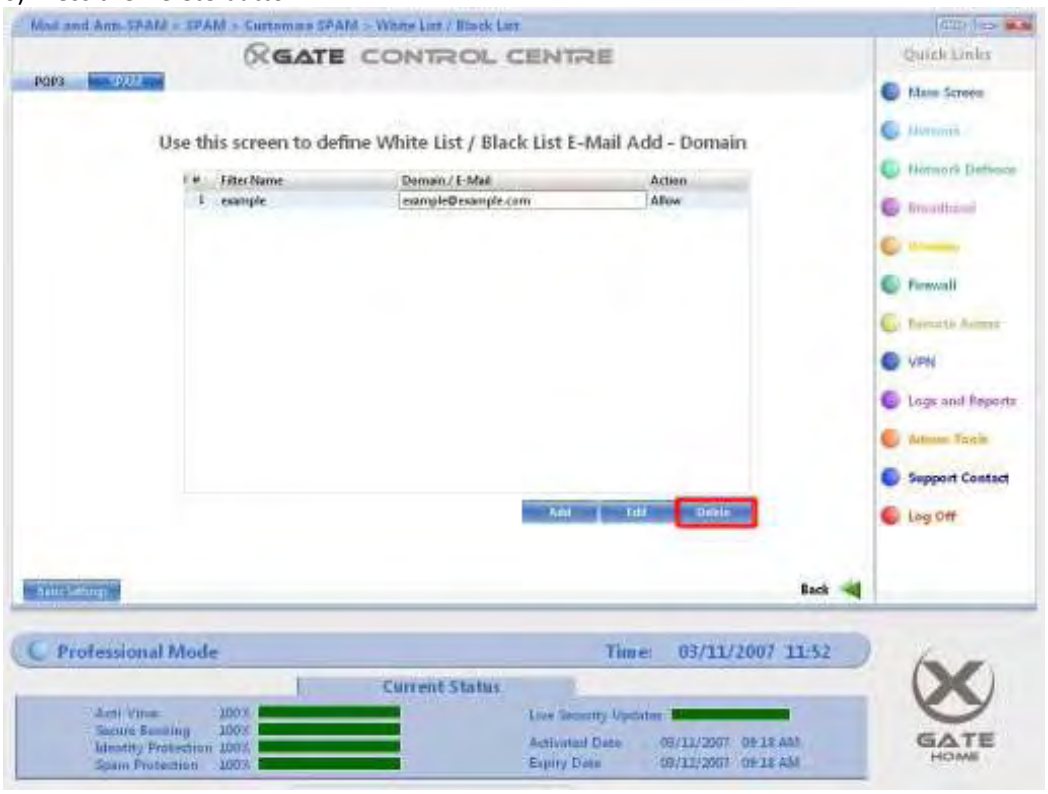

4) Ensure that Spam has been swiched on.
5) Click on Customise SPAM Protection.


3) Ensure that the Use White / Black List tick box is ticked.

4) Press the Use White / Black List Settings button.




5) Select the entry you wish to edit. This will highlight the entry.
6) Press the Delete button.



## Secure Banking

### What is Secure Banking?

Secure Banking ensures that your online banking activities are kept secure.

XGate does this by holding a database of the IP Address details of all major worldwide banks. When you visit a banking website, XGate checks the IP Address of the website with its IP Address it holds in its database and if the two do not match then you will be informed that you may be trying to access a fraudulent website.

XGate Secure Banking also includes Anti-Fraud protection. Using similar technology as Secure Banking, it allows you to shop online and make online transactions without worries. If a site is assumed to be fraudulent, XGate will inform you.

## Setting up Secure Banking

1) Press the Secure Banking button.


2) Ensure that Enable XGate Secure Banking is ticked.

3) Locate your bank(s) in the list and either double click or press the Add button to add that bank to the list of secure banks.

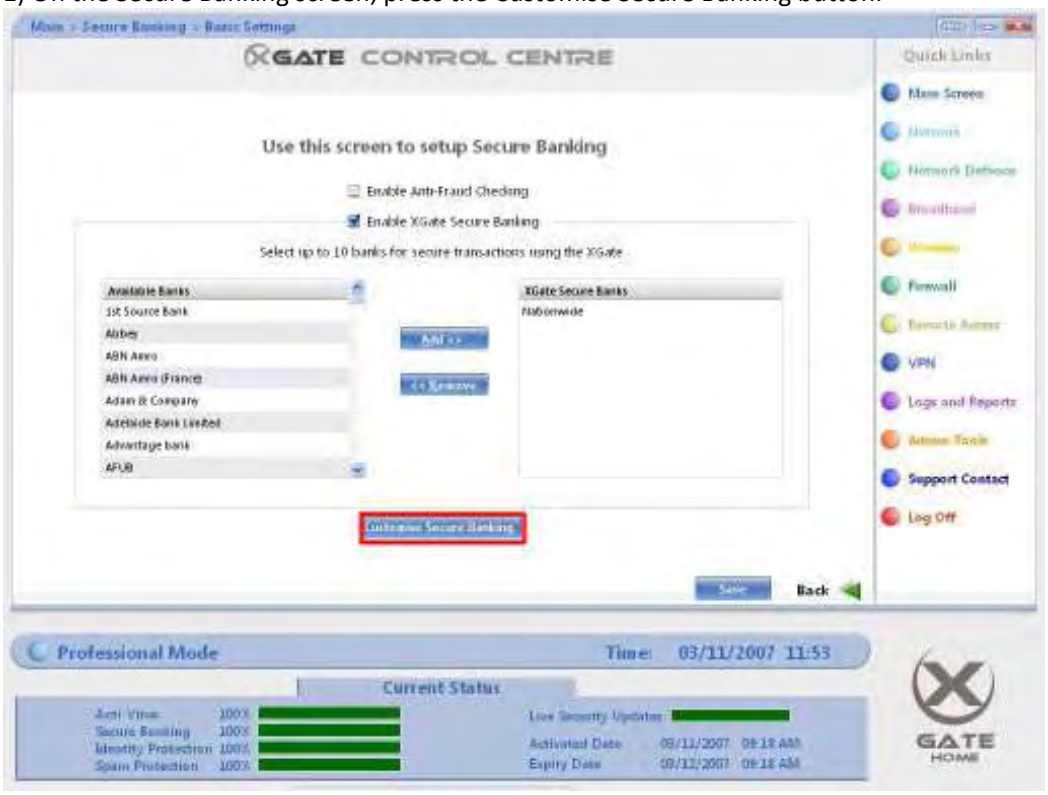

4) Once you are satisfied with the list of selected banks, press the Save button.

## Updating Secure Banking

There are two methods to update XGate Secure Banking: Manually or Automatically.

To switch on automatic updates:

1) On the Secure Banking screen, press the Customise Secure Banking button.

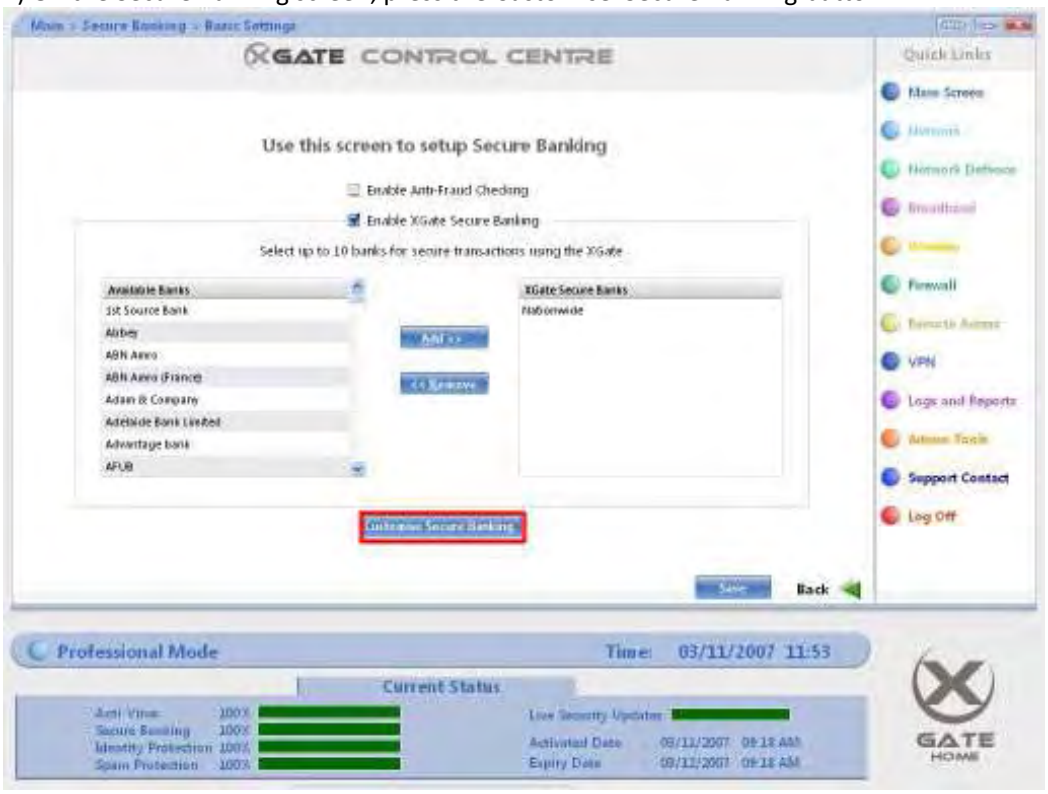



2) Ensure that the tick box adjacent to Automatically Update Secure Banking at… is ticked.


3) Specify the time you would like XGate to check for Secure banking updates in the text box that follows.


To Manually update:

1) On the Secure Banking screen, press the Customise  Secure Banking button.




2) Press the Update Now button.

## Using Secure Banking

1) Open Internet Explorer.
2) Press the XGate Secure Banking button. If no button is present, right click on the top tool bar and make sure that the XGate Secure Banking option is ticked.
3) Select the online bank you wish to go to and press the Go button.

## Gaming

### What is Gaming?

Over recent years, the Computer and Video Games Industry has grown significantly and has become more accepted as a mainstream entertainment medium. The advent of the Internet has also helped increase the growth of the games industry.

As a result, XGate provides the tools for you so you can easily set up a wired Internet connection between your XGate and Game console. You will now be able to have Internet access from your games console painlessly without any complications.

### Gaming Features

Within the XGate Control Centre, there are two features specifically designed for Gaming:

Console Gaming
The Console Gaming screen makes it easy to set up a connection between XGate and your games console.

Virtual Server Hosting
This screen can be used to host a virtual game server. This is primarily used with online PC games.

## Viewing / Changing your Console Gaming settings

1) Press the Gaming button.


2) For the console you wish to see for, press the View button.


3) Change the IP address details if you wish and press OK to close the window.


4) Press the Save button to confirm any changes you have made.


Note: Please ensure that any changes that are made on the Console Gaming screen are reflected in your games console. For more details on how to set up your games console IP Address details, consult your console manufacturer's documentation.

Introduction

## Virtual Server Hosting

### What is Virtual Server Hosting?

Generally, Virtual Server hosting is used for servers so they can host more than one domain name on the same computer. By doing this, there are two methods of communicating with the computer: through its real IP Address and its mapped (or Virtual) IP Address.

This feature can be applied for use as a gaming server. By having a Virtual Game Server, you can manage the resources of your computer easier.

Most games come integrated with their own game server programs. However, when you host a game server and play on that server at the same time, there is a constant battle of resources between the game server and the game engine, which gives you all the graphics and sound. As a result, the performance of both sides can be irregular and inconsistent.

By having a Virtual Server, this battle of computer resources becomes a non-issue and there is a clear separation between the server and game engine.

### Analogy

With Virtual Server Hosting, a computer can be seen to be as a cake. The cake (the computer with the Virtual Server) is divided into separate parts (virtual machines). From here, a person can flavour (user and customise) the cake however they want. One person may wish to have custard or chocolate sauce on their slice of cake. Their slice of cake has been changed to fit their tastes but it has not affected the other slices.

### Virtual Server Hosting details

To set up a Virtual Server, the following details are necessary:

Server Name
This is a friendly name so you can easily identify the Virtual Server.

Server Private IP Address
This is the LAN (Internal) IP address of the computer you wish to host the Virtual Server from.

Mapped Public IP Address
This is WAN (External) IP address that you wish to give to the Virtual Server.

Mapped Public Subnet
This if subnet of the External IP Address that you are giving to the Virtual server.

## Adding a Virtual Server

1) Press the Gaming button.
2) Click the Virtual Server Hosting Tab.
3) Ensure that Virtual Server Hosting is switched on.
4) Press the Customise Virtual Server button.
5) Press the Add button.
6) Add your Virtual Server details.
7) Press the OK button.
8) Press Save to confirm your changes.

## Changing the details of a Virtual Server

1) Press the Gaming button.
2) Click the Virtual Server Hosting Tab.
3) Ensure that Virtual Server Hosting is switched on.
4) Press the Customise Virtual Server button.
5) Click the Virtual Server you wish to edit. This will highlight the entry.
6) Press the Edit button.
7) Change your Virtual Server details.
8) Press the OK button.
9) Press Save to confirm your changes.

## Removing a Virtual Server

1) Press the Gaming button.
2) Click the Virtual Server Hosting Tab.
3) Ensure that Virtual Server Hosting is switched on.
4) Press the Customise Virtual Server button.
5) Click the Virtual Server you wish to remove. This will highlight the entry.
6) Press the Delete button.
7) Press Save to confirm your changes.

Introduction

## VPN Server

### What is a VPN Server?

Using a VPN Server allows you to securely transfer files between one computer network and another via the Internet.

### VPN Policy Types

In the case of XGate, you can either set up a:

Site–to-Site policy
Use this when you wish to create a connection between two networks. Typically, this is between two offices, such as a branch and head office.

Mobile User policy
Use this when you wish to create a connection between a fixed network and a roaming computer. For example, this roaming computer may belong to an employee who travels a lot. It is also recommended that you use L2TP accounts when using a Mobile User policy for additional security and management.

### VPN Policy Details

When configuring a Site-to-Site Policy you need to provide the following details:

Policy Name
This is a friendly name set by you to easily identify your VPN policy.

Policy Type
This should be set to Site-to-Site.

Local IP Address
This is the WAN IP address of the XGate. This should be already filled in.

Local Subnet
These are the Subnet details for your LAN. For example, if you XGate's LAN IP Address is 192.168.2.1 you should enter the details 192.168.2.0 / 255.255.255.0.

Remote IP Address
This is the WAN IP address of the device you wish to establish a VPN connection. with.

Remote Subnet
These are the LAN subnet details of the device you wish to connect to. The device you wish to connect to cannot belong to the same LAN subnet as the XGate device you are using. For example, if your XGate has an IP address of 192.168.2.1, the other device cannot belong to 192.168.2.0 network.

Pre-Shared Key
This is the password of the VPN connection. You will need to enter this on both devices.

Encryption and Authentication Type
This is the type of encryption algorithm that you wish to use. In the majority of cases, the default setting offers adequate security.

When creating a Mobile User policy, the details that need to be provided are slightly different.

Policy Name
This is a friendly name set by you to easily identify your VPN policy.

Policy Type
This should be set to Mobile User.

Local IP Address
This is the WAN IP address of the XGate. This should be already filled in.

Local Subnet
In the majority of cases, this should also be set to the WAN IP address of the XGate. So, if you have a WAN IP address of 195.153.124.111, you should provide the local subnet as: 195.153.124.111 / 255.255.255.255.

Pre-Shared Key
This is the password of the VPN connection. You will need to enter this on both devices.

Encryption and Authentication Type
This is the type of encryption algorithm that you wish to use. In the majority of cases, the default setting offers adequate security.

Within the New Policy screen, Advanced Settings for VPN Policy creation can be reached in the bottom left. Within this screen, the following settings can be edited:

IKE Key Life Time
The IKE key is required to secure the VPN Connection. This specifies the period of time before the key is renewed.

IPSEC Key Life time
This IPSEC key is used for the data transfer. This specifies the period of time before the key is renewed.

Perfect Forward Secrecy
Also known as PFS. This enhances the security of a VPN connection by creating a new key for each data transfer phase. This makes it much harder for an intruder to find out what the keys are and gain access to the system. However, this makes the VPN connection slightly slower to set up as it takes longer to establish the VPN keys.

IP Compression
This compresses the data before encryption so that bandwidth can be used efficiently. Other devices with VPN Servers may not support IP compression so please check your documentation for further information. If you have an XGate or Prodigy device, it is recommended that you enable IP compression.

## Creating a new VPN Policy

1) On the Quick Links menu, click VPN Server.
2) Ensure that the VPN Server is switched on.
3) Press the New Policy button.
4) On the New Policy screen, enter the details of the VPN connection you wish to establish. For options such as Key lifetime, PFS and IP compression press the Advanced Settings button.
5) Press the Save button to confirm your changes.
6) Press the Connect button for the newly created VPN policy.

## Changing the details of a VPN Policy

1) On the Quick Links menu, please click VPN Server.
2) Ensure that the VPN Server is switched on.
3) Press the New Policy button.
4) On the New Policy screen, enter the details of the VPN connection you wish to establish. For options such as Key lifetime, PFS and IP compression press the Advanced Settings button.
5) Press the Save button to confirm your changes.

## Removing a VPN Policy

1) On the Quick Links menu, click VPN Server.
2) Ensure that the VPN Server is switched on.
3) Press the delete button of the VPN policy you wish to remove.

Introduction

## L2TP Settings

### What is L2TP?

L2TP stands Layer 2 Tunnelling Protocol and is used specifically for Mobile VPN connections.

It is highly recommended to use L2TP when using Mobile VPN for security reasons. Also, if you wish to have more than one computer connected to your XGate using your Mobile VPN connection you must set up your L2TP settings.

### Analogy

Using the draw bridge analogy, using L2TP would be similar to covering the bridge (VPN Connection) with a giant pipe or tunnel. It would be impossible to see who is walking across the bridge and impossible to access the bridge outside the start and end points of the bridge.

### L2TP Settings

There are two sections that you need to complete when configuring L2TP: the L2TP server settings and the L2TP user accounts.

The L2TP server settings are made up of the following details:
Server IP address
This will be the LAN IP address of your XGate.

Start IP Address
This is the first IP Address that will be allocated to the Mobile User connecting to XGate.

End IP address
This is the last IP Address that will be allocated to the Mobile User connecting to XGate.

Notes
- Ensure that the start and end IP address must be within the network range of your XGate LAN IP (192.168.2.1 by default).
- Ensure that the range of IP Addresses between the start and end IP address do not overlap with the DHCP Server range otherwise you may have IP address conflicts.

The L2TP User accounts require the following details:
Username
The username the account holder will use when logging in to the VPN server.

Password
The password of the account holder will use when logging in to the VPN server.

## Configuring your L2TP Server settings

1) On the Quick Links menu, click VPN Server.
2) Click the L2TP settings tab.
3) Enter the L2TP Server IP address as the LAN IP address of XGate (192.168.2.1 by default).
4) Enter the L2TP Server Start and End IP address.
5) Press Save to confirm your settings.

## Adding L2TP User Accounts

1) On the L2TP settings screen click the Add button.
2) Enter your L2TP User account details.
3) Press the OK button.
4) Press the Save button to confirm your L2TP user account entry.

Introduction

## Admin Tools

### What are Admin Tools?

Admin tools is a central area to carry out your administration tasks for your XGate device. In computing terms, an administrator is someone who operates and maintains a computer or network.

### What is within Admin Tools?

Admin Tools contains features that are typically used by an administrator. This includes:

Customer Details
This lists the Customer details and the licences they posses.

Licence & Subscription
Purchase and activate new licences and upgrades here.

Support Contact
Displays all the methods of contacting XGate Support.

Remote Access
This allows you to give XGate Support access to your machine if necessary.

Password
Use this screen to change your password or forgotten password question

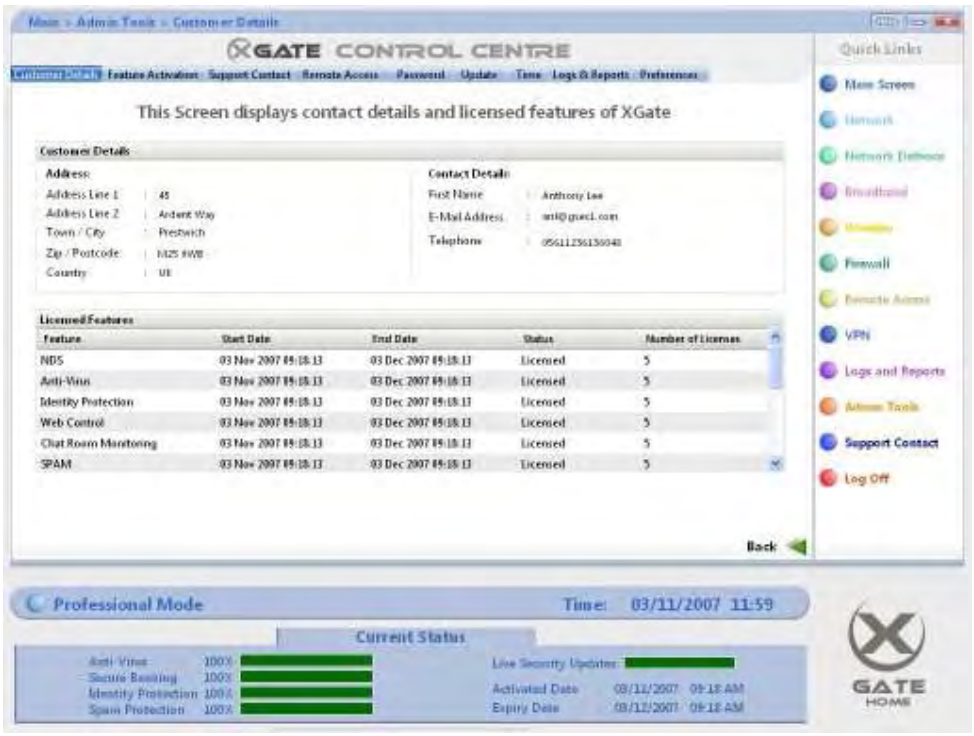
Backup / Restore
This allows you to Backup or Restore your XGate Control Centre settings.

Update
If an update is available, you can upgrade your XGate software from here.

Time
Adjust XGate's time settings from here.

Customer Details

## Customer Details



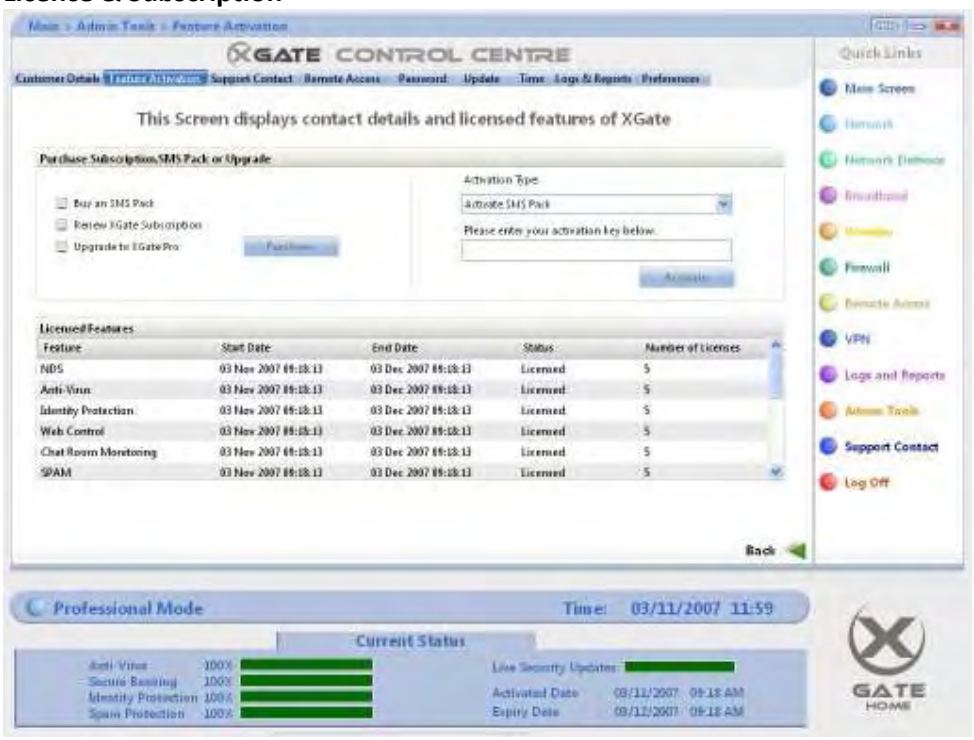

This screen shows 2 items:

- Your customer details which you entered during your XGate Installation
- The XGate features that you have licensed.

When you purchased your XGate, the following features came as standard:
- Anti-Virus
- Identity Protection
- Web Control
- VPN
- Customer Support
- Data Insurance Policy

If you purchased an XGate Pro, then the following features were also provided:
- Static Routing
- VPN Server
- Spam Multiple Domains
- Firewall Multiple IP Hosting

## Licence & Subscription




The Licence & Subscription page allows you to purchase and activate new Licences for your XGate.

To purchase an SMS pack, upgrade or licence renewal:
1) On the Quick Links menu, click Admin Tools.
2) Click the Licence & Subscription tab.
3) Tick the item you wish to purchase (SMS pack, XGate Subscription renewal or XGate Pro Upgrade).
4) Press the Purchase button.

To activate your purchase:
1) Enter your activation key shown on XGate payment website.
2) Press the Activate button.

## Support Contact


This page gives you all the methods of contacting XGate Support. This includes:

1. Call Customer Support
This will provide you with the XGate Support phone number.

2. E-mail Customer Support
This will open your default mail client and give you a message template to send a mail to XGate Support.

3. Visit our Customer Support website
This will open your default web browser and direct you to the XGate Customer Support page.

4. Read our FAQ's
This will open the FAQ's (Frequently Asked Questions) document.

5. XGate Live Support 24/7
This will open your default web browser and direct you to the XGate Live Support 24/7 page.

Also included is general information regarding your XGate. When you contact support, it is likely you will need to tell the XGate Support Engineer this information.

## Remote Access


Remote Access allows XGate Support to remotely log into your computer with your permission. This is used to provide you with the most effective support possible, reducing any possible miscommunication between yourself and the XGate Support Engineer.

**To set up Remote Access:**

1) On the Quick Links menu, click Admin Tools.
2) Click the Remote Access tab.
3) Ensure that Remote Access is switched on.
4) Using the drop down menu, select the PC that the XGate Support Engineer wants access to.
5) Press the Save button to confirm your changes.

Note: After your support call has been closed, please ensure that you switch off Remote Access for security reasons.

Password

## Password


This screen is used for changing your XGate Control Centre login details.

To change your password:
1) On the Quick Links menu, click Admin Tools.
2) Click the Password tab.
3) Enter your Password details.
4) Press Save to confirm your changes.

## Updates

Due to the nature of Internet Security and the constant battle against hackers and malicious programs, XGate is in constant development. As a result, updates will be periodically available to XGate.

Updates include enhancements to security, functionality and usability. As such, it is highly recommended to update your device regularly, when possible.

If an update is available you will see the screen below.


Press the Update Now button to start the update process.

If no update is available then the screen below will be shown.


Main > Admin Tools > Update
XGATE CONTROL CENTRE
Customer Details
Feature Activation
Support Contact
Remote Access
Password
Update
Time
Logs & Reports
Preferences
Use this screen to update to the latest XGate software
Update
There are no updates available. You are currently using the latest version of XGate.
Quick Links
Main Screen
Network
Network Defence
Broadband
Wireless
Firewall
Remote Access
VPN
Logs and Reports
Admin Tools
Support Contact
Log Off
Back
Professional Mode
Time: 03/11/2007 12:00
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 03/12/2007 09:18 AM
GATE
HOME

Introduction

## Time

### What is Time in XGate?

A number of modules within XGate are dependent on Time. This includes features such as the XGate Log Viewer and Time based Web Control. As such, it is important for XGate Time to be correctly set up so these features work correctly.

### Time Server Details

Within XGate there are two ways to set up time:

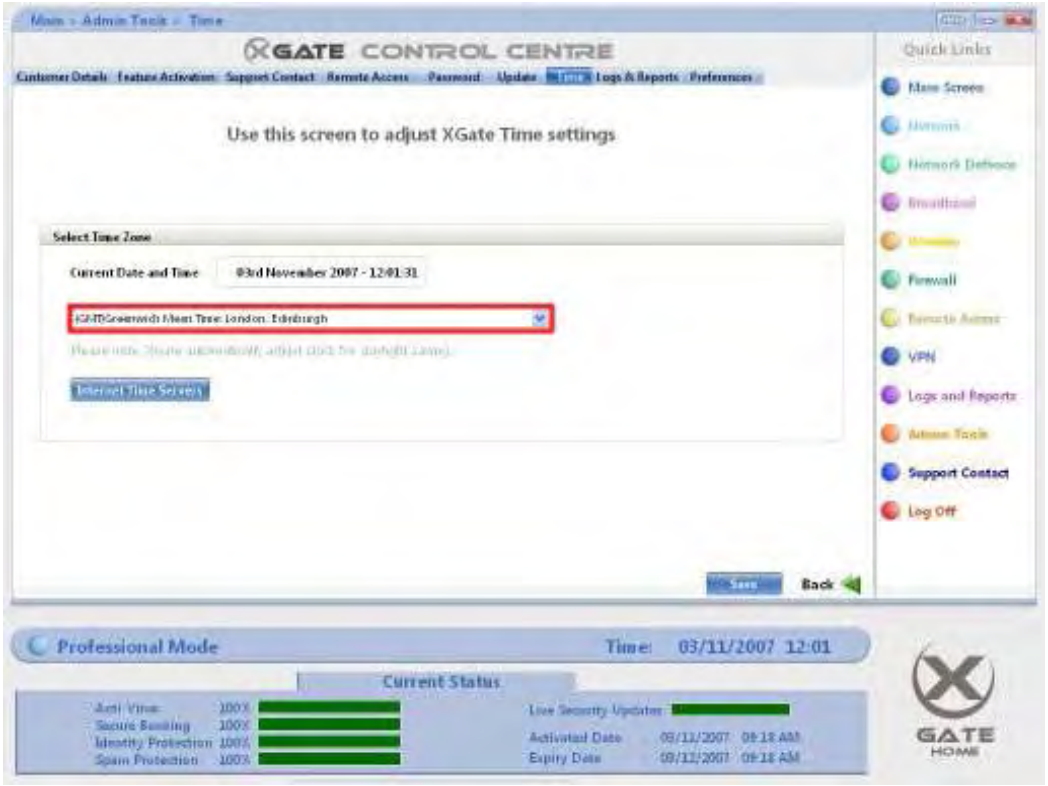
By Time Zone
This is via manually selecting your geographical Time Zone

Using Internet Time Servers
A Time Server is a computer that read time from a reference clock and distributes this time to its clients (in this case, XGate) Commonly, this reference clock is through GPS, which is used by the Atomic clocks on satellites.

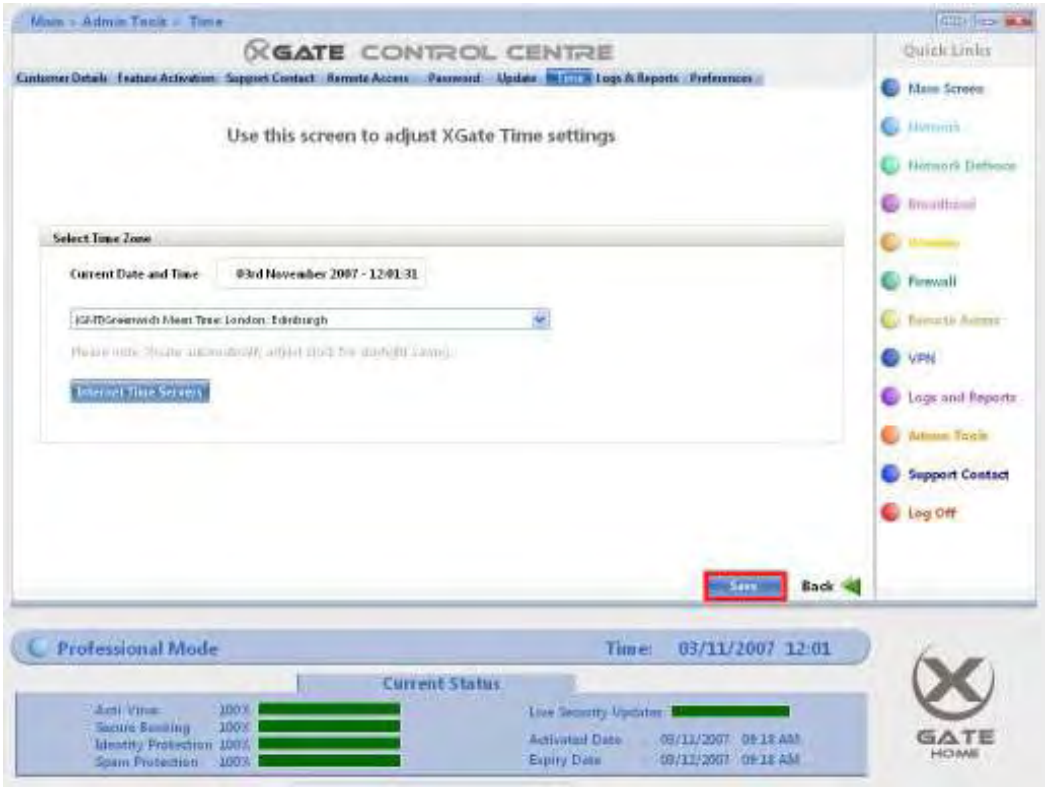
Note: When you press the Synchronise button, your current date and time will be updated to match the Internet Time Server.

## Changing your Time Zone

1) Select the time zone of your geographical region from the Time zone selection drop down menu.



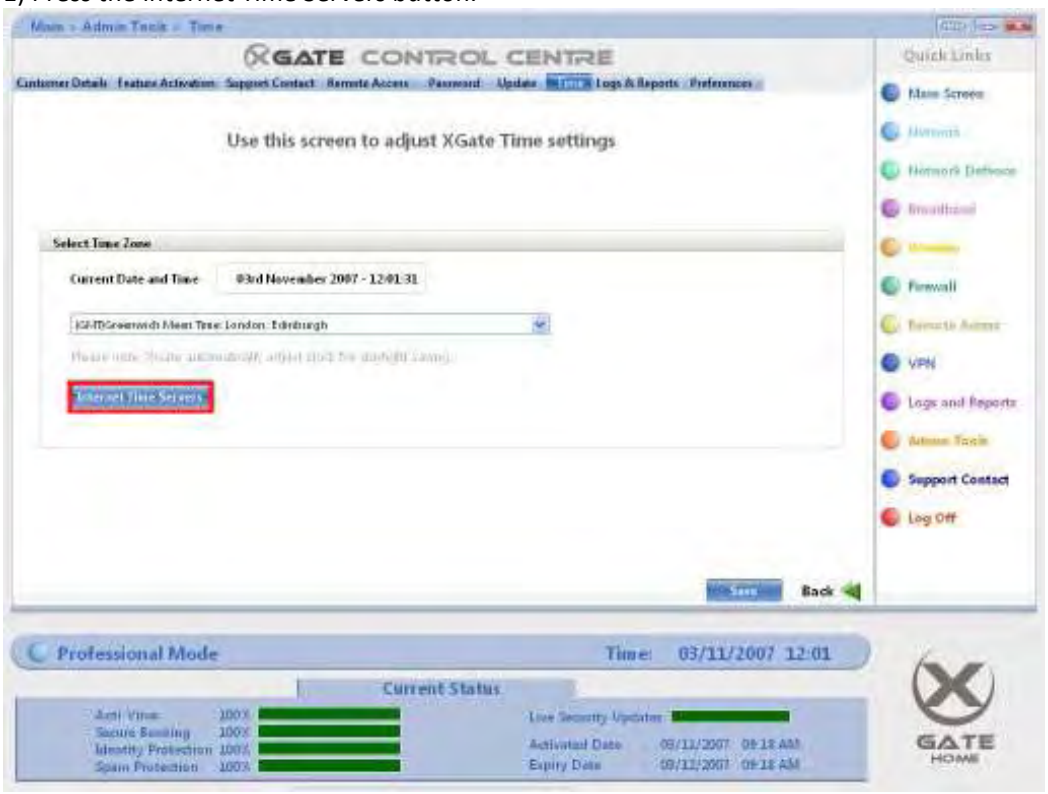

2) Press Save to confirm your changes.


XGATE CONTROL CENTRE
Customer Details
Feature Activation
Support Contact
Remote Access
Password
Update
Logs & Reports
Preferences
Use this screen to adjust XGate Time settings
Select Time Zone
Current Date and Time
03rd November 2007 - 12:01:31
Internet Time Servers
Back
Quick Links
Main Screen
Network Defence
Broadband
Firewall
VPN
Logs and Reports
Support Contact
Log Off
Professional Mode
Time: 03/11/2007 12:01
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

To Add an Internet Time Server

## To Add an Internet Time Server

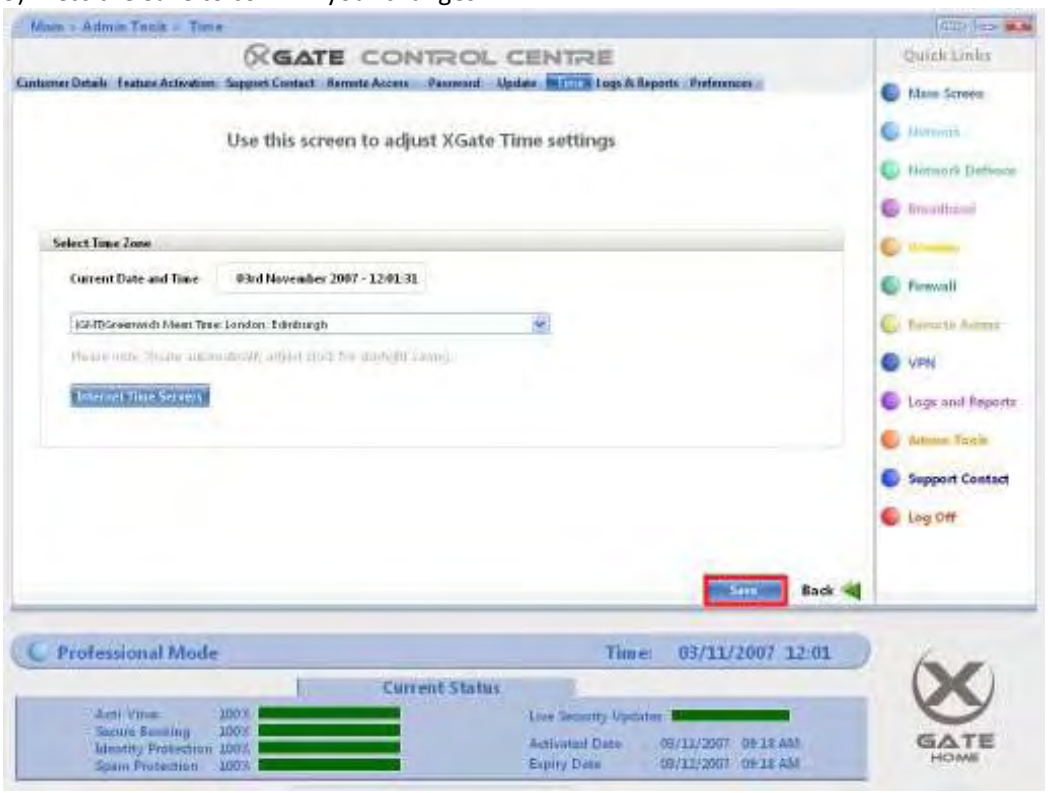
1) Press the Internet Time Servers button.




2) Type in an address of an Internet Time Server.
3) Press the Add button.


4) Press the OK button.

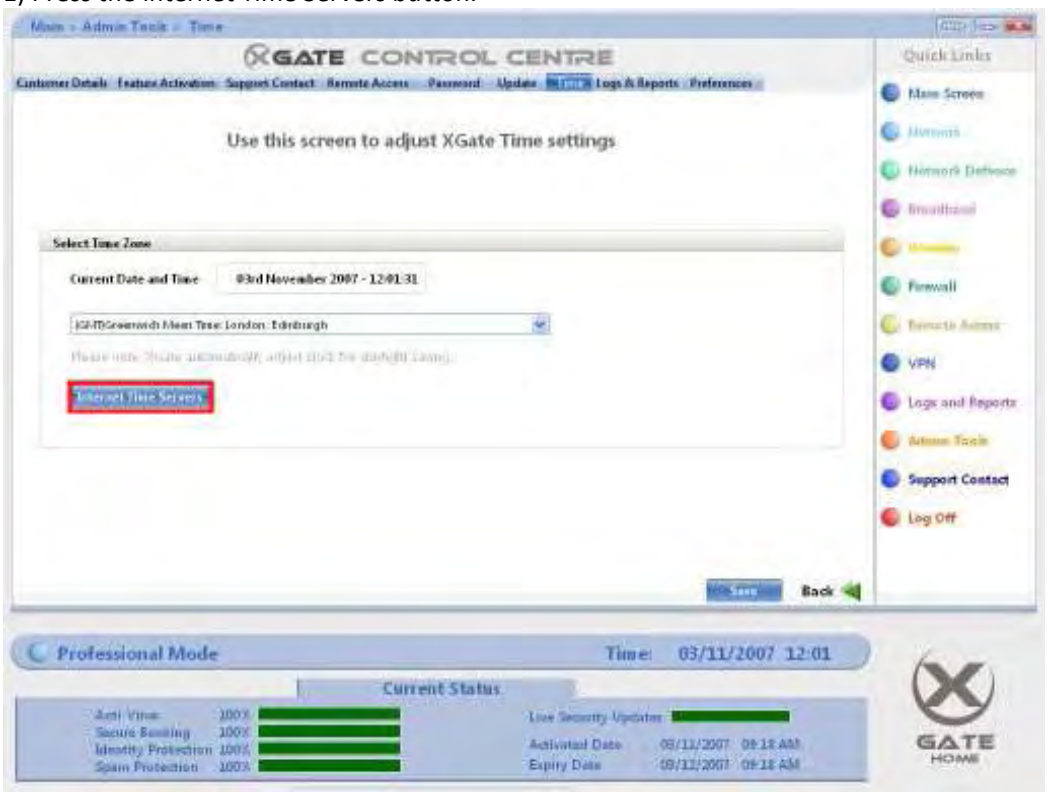

5) Press the Save to confirm your changes.




Note: If you add more than one Time Server, the time will be synchronised to the first working Time Server listed. The other Time Server can be considered as backups.

## Modifying an Internet Time Server Address

1) Press the Internet Time Servers button.



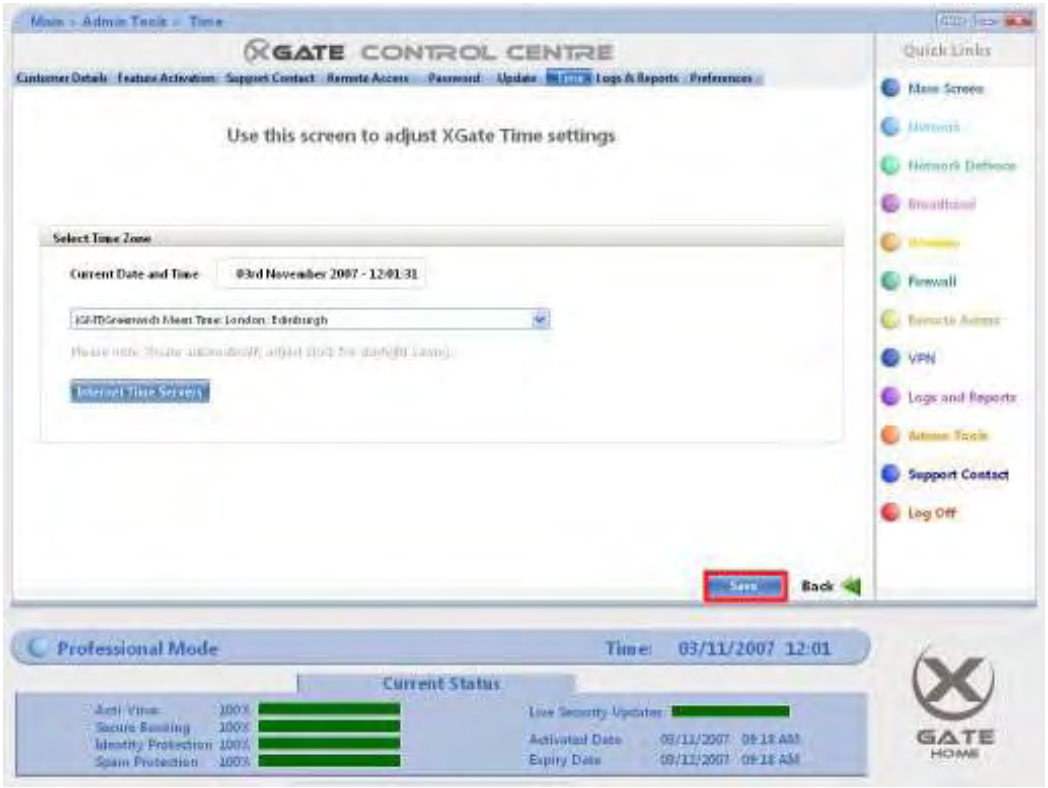

2) Click the Time Server you wish to modify. This will highlight the entry.


3) Press the Edit button.

4) Edit your Time Server Address.
5) Press the Save button.

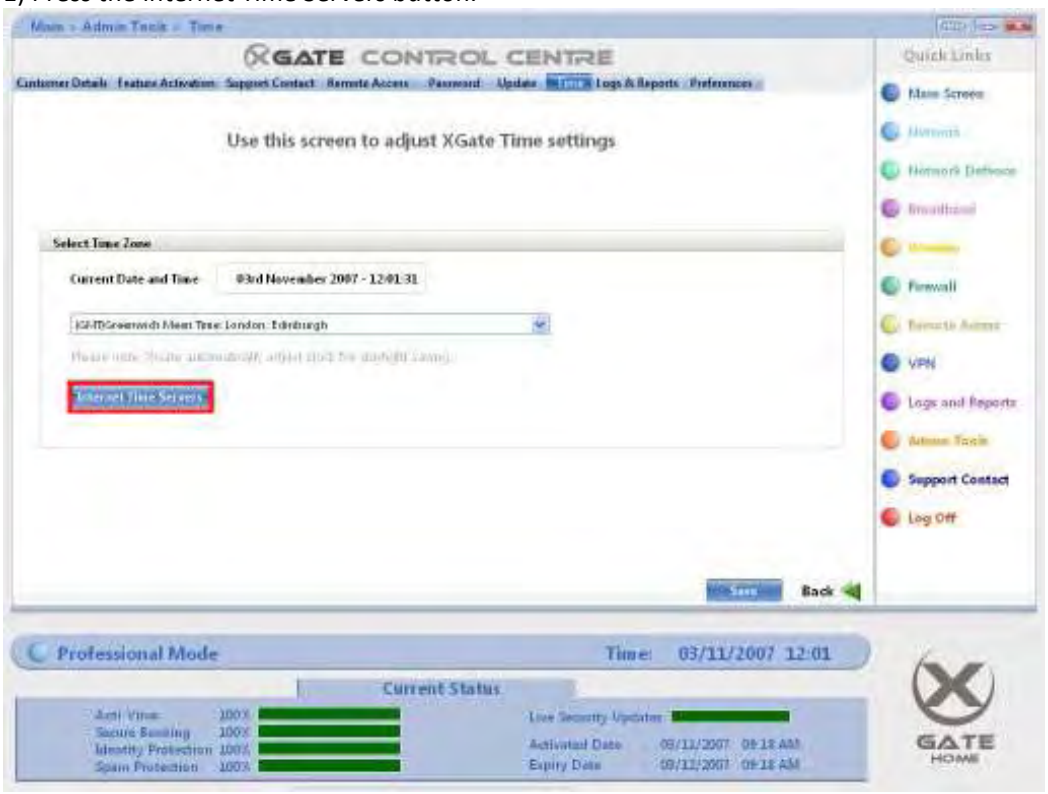
5) Press the OK button.

6) Press the Save to confirm your changes.


XGATE CONTROL CENTRE
Customer Details
Feature Activation
Support Contact
Remote Access
Password
Update
Logs & Reports
Preferences
Use this screen to adjust XGate Time settings
Select Time Zone
Current Date and Time
03rd November 2007 - 12:01:31
Back
Quick Links
Main Screen
Network Defence
Broadband
Firewall
VPN
Logs and Reports
Support Contact
Log Off
Professional Mode
Time: 03/11/2007 12:01
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 an Internet Time Server

1) Press the Internet Time Servers button.

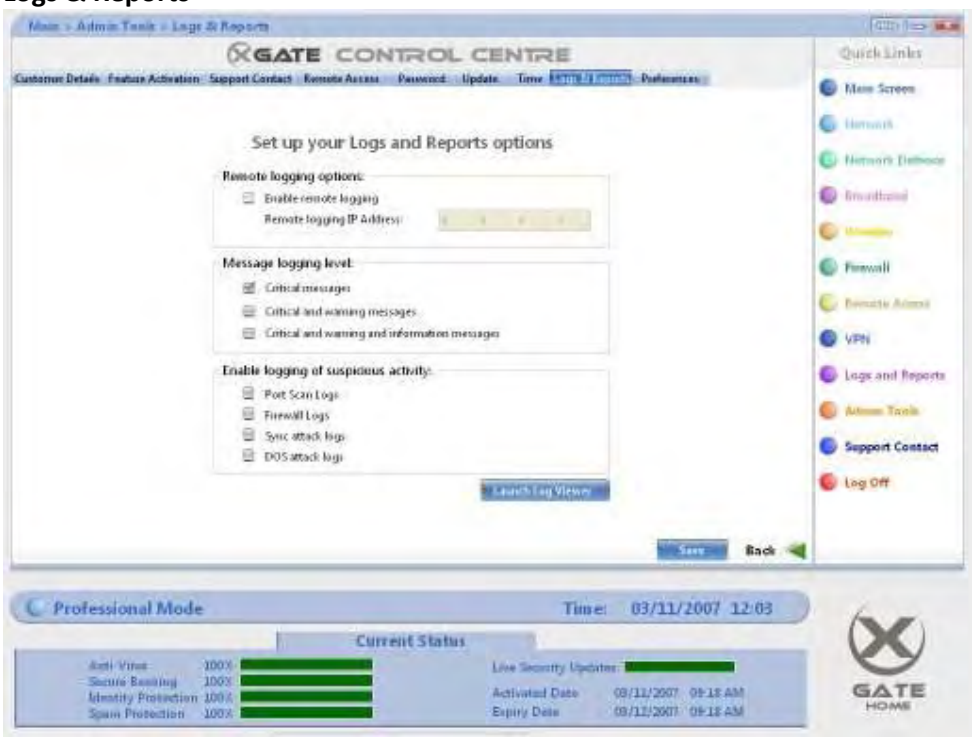



2) Click the Time Server you wish to remove. This will highlight the entry.


3) Press the Delete button.

4) Press the Save to confirm your changes.

**Logs & Reports**




The Logs & Reports screen deals with three parts of setting up the XGate Log Viewer.

Remote Logging
This allows you to direct all the logs to one computer on your network. To set this up, tick the Enable remote logging tick box and specify the IP address of the computer where the logs will be sent.

Message Logging level
This is where you specify the level of logs which will be sent to the specified IP address.

Critical Messages - This option logs only the most important messages. For example, intrusion detections.

Critical and Warning Messages - This option reports all of the warning and critical messages. For example, if a connection to the XGate Control Centre is lost.

Critical, Warning and Information Messages - This reports all messages generated by the XGate 2.0 device, ranging from critical alerts to general information. This includes messages such as web sites visited,.

Logging of Suspicious Activity
This allows you to log specific suspicious activities

Preferences

**Preferences**


This screen allows you to enable and disable two additional features of XGate. These two features are:

Disconnect Automatically from XGate after X minutes of inactivity
If the XGate Control Centre is left idle with no mouse movement for the specified amount of minutes, the control centre will automatically log you out.

Stop sensor installation request
This will disable the sensor installation prompt which appears on the networked computer's web browsers every 24 hours.

## XGate Log Viewer

### What is the Log Viewer?

XGate Log Viewer gives you the flexibility to look at the events taking place within your local network in real time. Alternatively, you can generate reports to track and monitor each computer's Internet and security activity within a specified time period.

### XGate Log Viewer Features

Within the XGate Log Viewer you can generate reports of:

- Websites Viewed
- Chat Activity
- E-mail Activity
- Virus Details
- Spyware Details

## Filtering Real Time Logs

Within the Real Time Logs screen, the following filters are available:

Message Type:
This allows you to filter the Real Time Logs based on the type of message that is displayed. There are eight different types of message:
- Emergency
- Alert
- Critical
- Error
- Warning
- Notice
- Information
- Debug

Modules:
This allows you to filter the Real Time Logs based on the XGate Module the message is from.

Start Date & Time:
Set this option to view XGate Logs recorded after the specified date and time. To set the date and time, click the calendar icon. To remove the date and time, press the eraser icon.

End Date & Time:
Set this option to view all XGate Logs recorded before the specified time and date. To set the date and time, click the calendar icon. To remove the date and time, press the eraser icon.

## Generating and using Reports

1) Click the Reports button. This will automatically navigate you to the Generate screen.
2) Select the computer for which you wish to view the logs. You can do this by clicking the arrow on the right of the drop down box labelled Select Computer and then selecting a computer name.
3) Select the modules you wish to generate a report for. Do this by ticking the boxes of modules you wish to view and un-ticking the ones you do not wish to view.
4) Select the period of logs you wish to retrieve. You may select either a set time period by choosing the top option or a specific range of dates by choosing the bottom option. To configure a specific range of dates, click the Calendar icon right of the text box.
5) When you are satisfied with the settings of the report, click the Generate button.
6) You may now view the logs by selecting the options on the left.

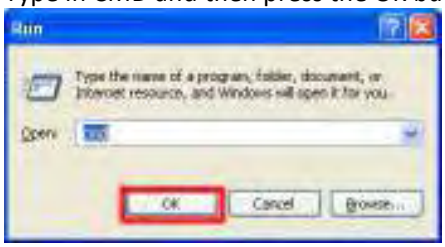
## General Troubleshooting

**1. How do I find out the IP address and MAC address of my computer?**

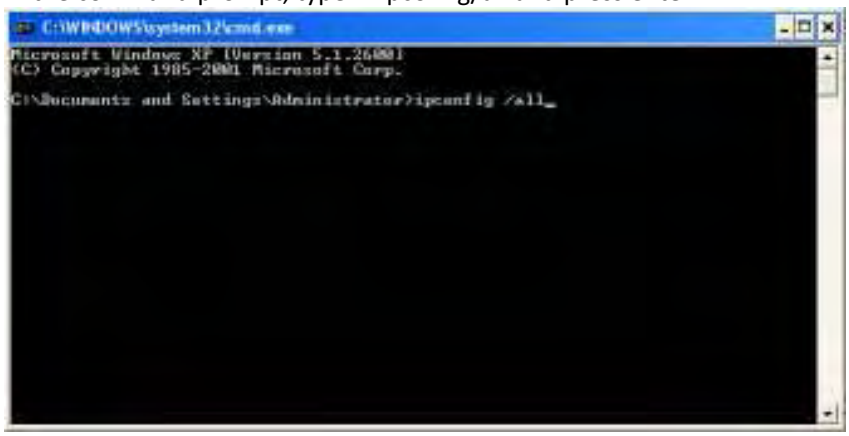
**Finding out an IP and MAC address of a computer**

1) In Windows, press Start.
2) Click Run.

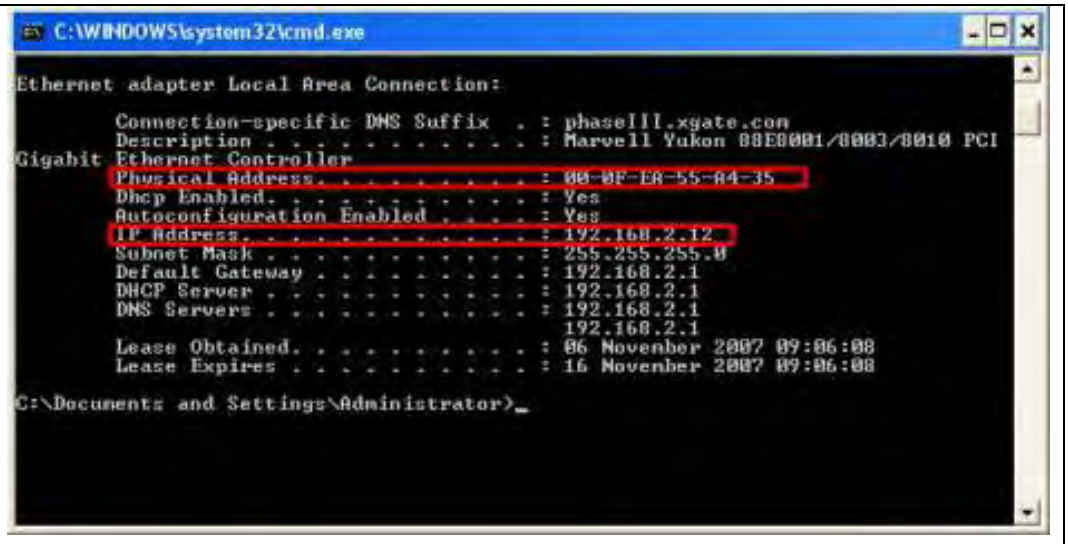

3) Type in CMD and then press the OK button.




4) In the command prompt, type in ipconfig/all and press enter.




5) The IP address and MAC Address (listed as Physical Address) will be displayed here




**2. I cannot connect to the Internet using Cable. What can I do?**

Your Internet Provider may be binding your MAC address to your Internet connection. Due to this, you need to spoof your Cable modem MAC address on the XGate.

**Using your Cable modem MAC address on your XGate**

1) Find the MAC address of your Cable Modem. This typically on the underside of your device.
2) On the Cable screen in the XGate Control Centre, tick the Use this MAC address tick box.


3) Type in the MAC address of your Cable Modem in the Use this MAC address field.


4) Press the Save button.


5) Press the Connect to Internet button.


**3. How can I use XGate Secure Banking and Anti-Fraud with Firefox or Opera?**

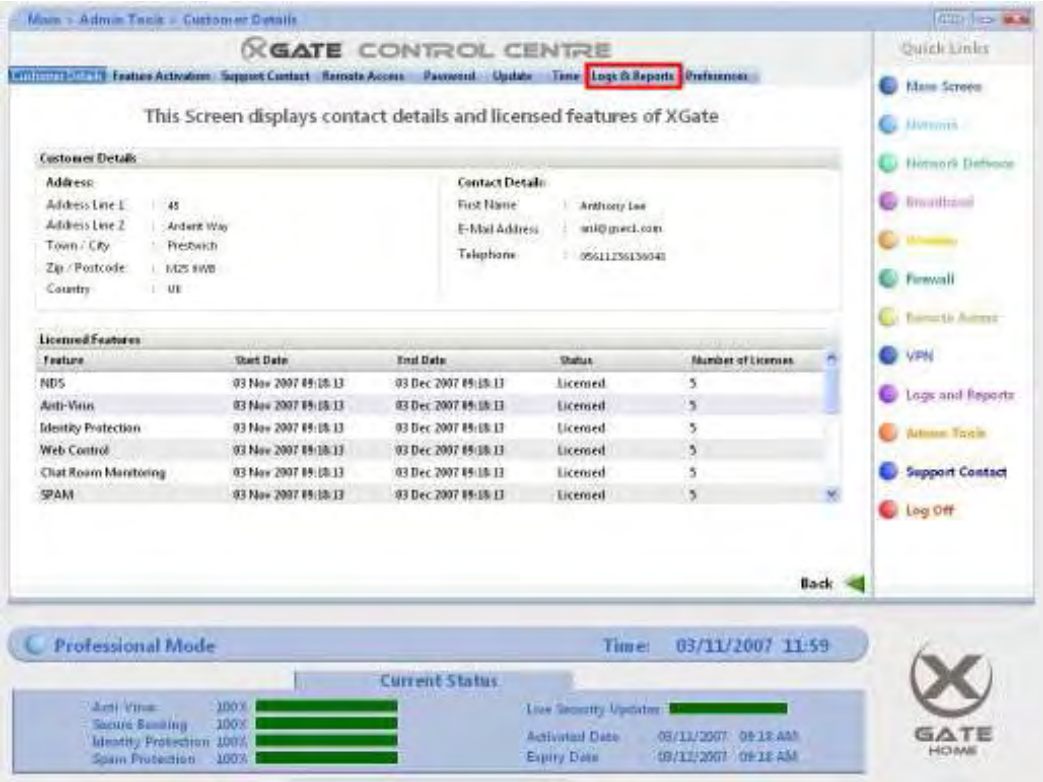
Currently, XGate Secure Banking and Anti-Fraud does not support Firefox or Opera.

**4. How can I view logs using the XGate Log Viewer?**

You may need to enable and set up Remote Logging on the XGate Control Centre. You must also make sure that the XGate Syslog Server (Log Listener) has been started on the computer that you wish to deliver logs to.

| **Enabling and setting up Remote Logging** |
| --- |
| 1) On the main screen, click Admin Tools. |

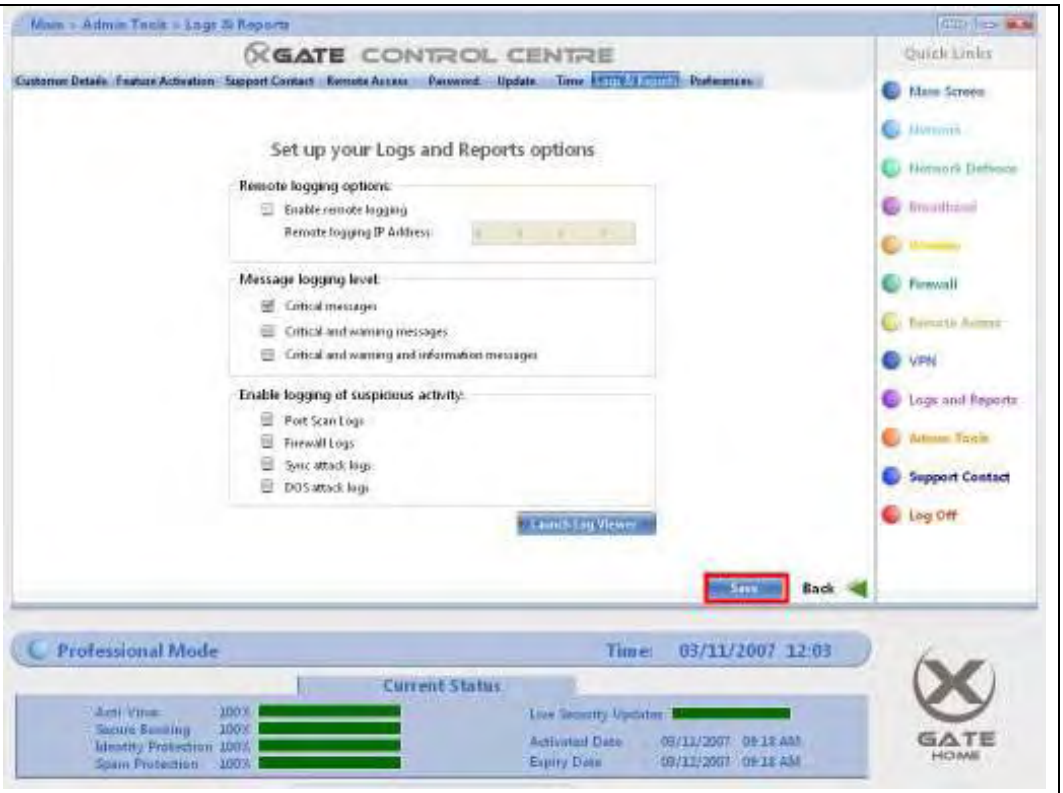

2) Press the Logs & Reports tab.



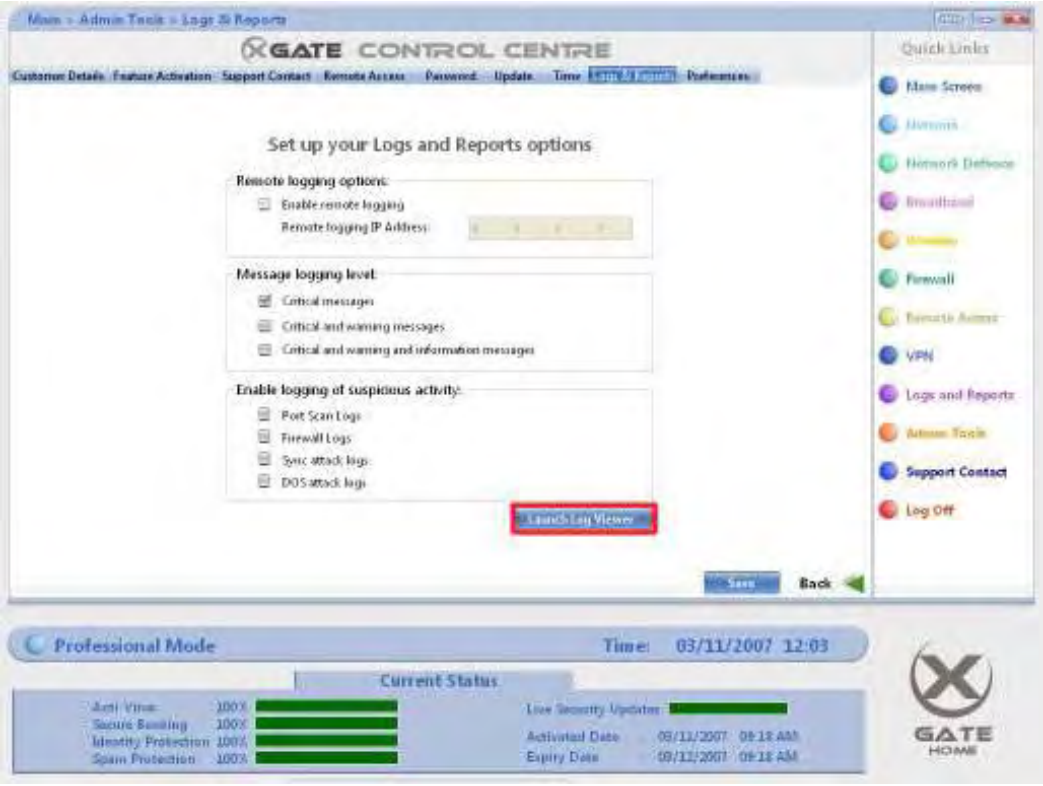

3) Tick the Enable Remote Logging tick box.


4) Type in the IP address of the computer you wish the logs to be sent to.


5) Press the Save button.



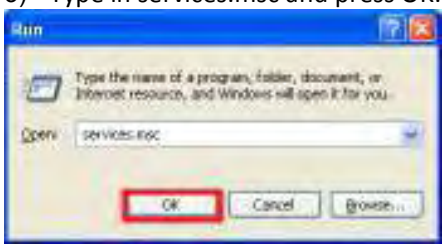

6) Press the Launch Log Viewer button.



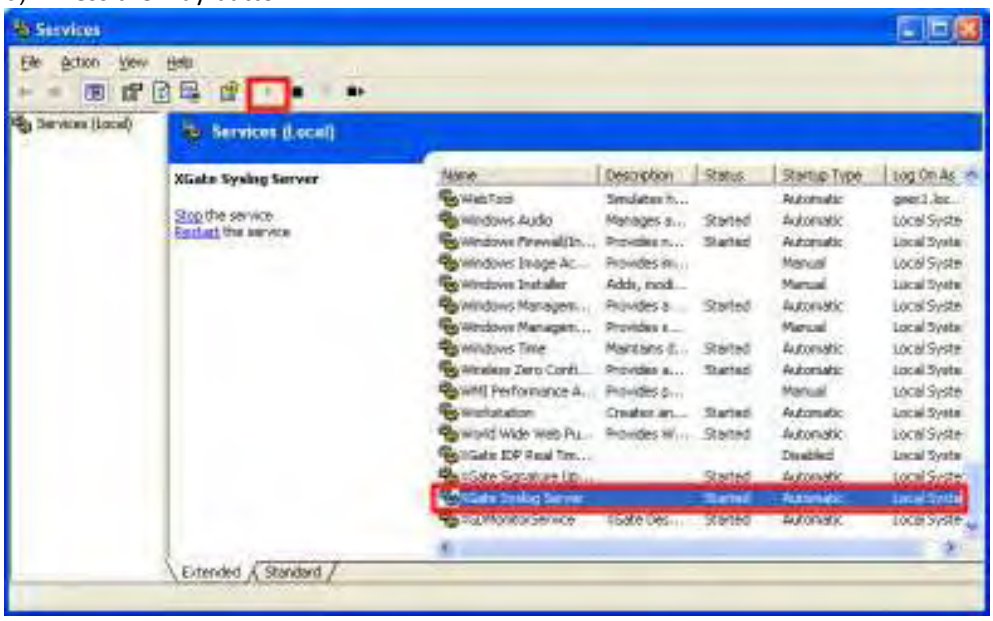
**Starting the XGate Syslog Server**

1) Press the Start button.


2) Click Run.
3) Type in services.msc and press OK.




4) Scroll down to the bottom of the list and select XGate Syslog Server. This will highlight the entry.
5) Press the Play button.



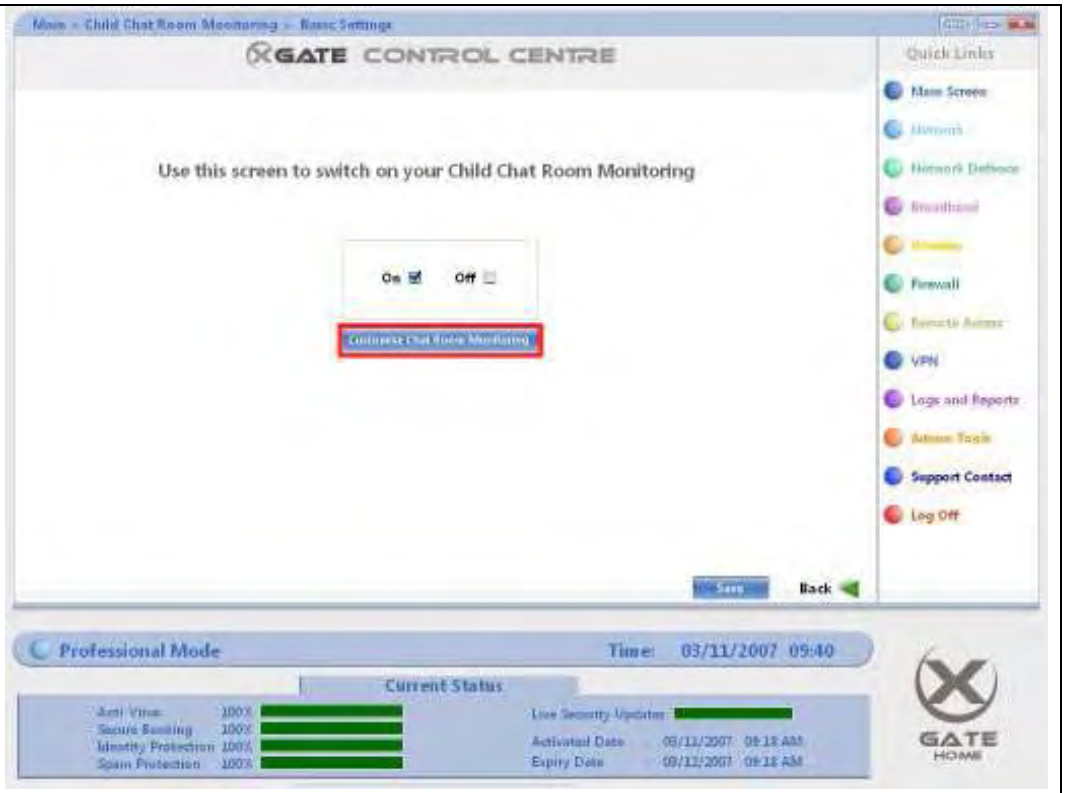
**5. The XGate Sensor will not install on my computer. What can I do?**

Make sure that your computer has the latest service pack for your operating system. For more details, please visit the Microsoft website.

## Chat Monitoring Troubleshooting

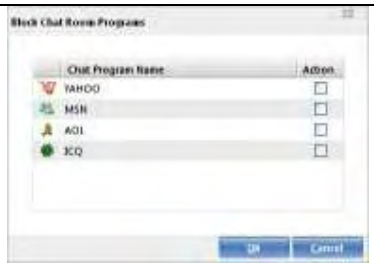
1. **I am not able to open Windows Live Messenger (or another chat application). How can I solve this problem?**
   You may have blocked a chat application via the XGate Control Centre or remotely when replying to an alert.

| **Unblocking a Chat Application** |
| --- |
| 1) On the main screen, press the Child Chat Room Monitoring button.<br>  <br><br>2) Press the Customise Child Chat Room Monitoring button. |




3) Press the Block Chat Applications Settings button.


4) Untick the chat application that is blocked and will not open for you.



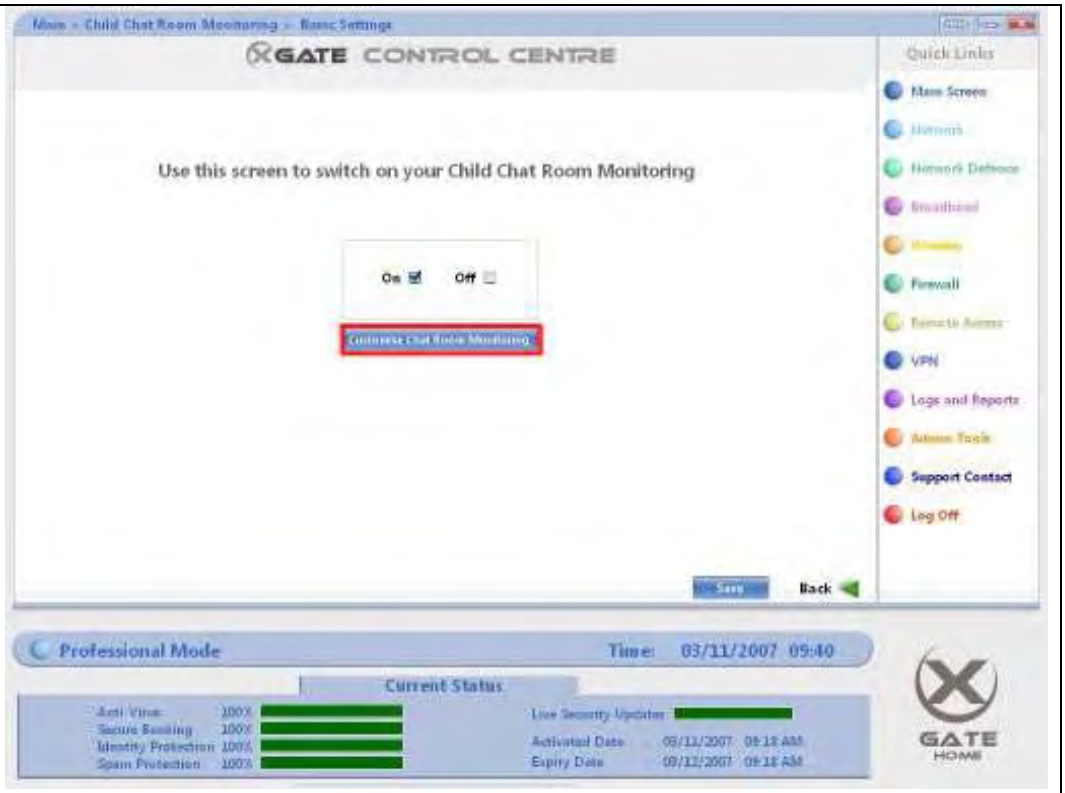

**2. I am no longer receiving Mobile Text Message alerts for Chat Monitoring. What is wrong?**

You may have run out of SMS credits.

**Checking your SMS balance**

1) On the main screen, press the Child Chat Room Monitoring button.


2) Press the Customise Child Chat Room Monitoring button.



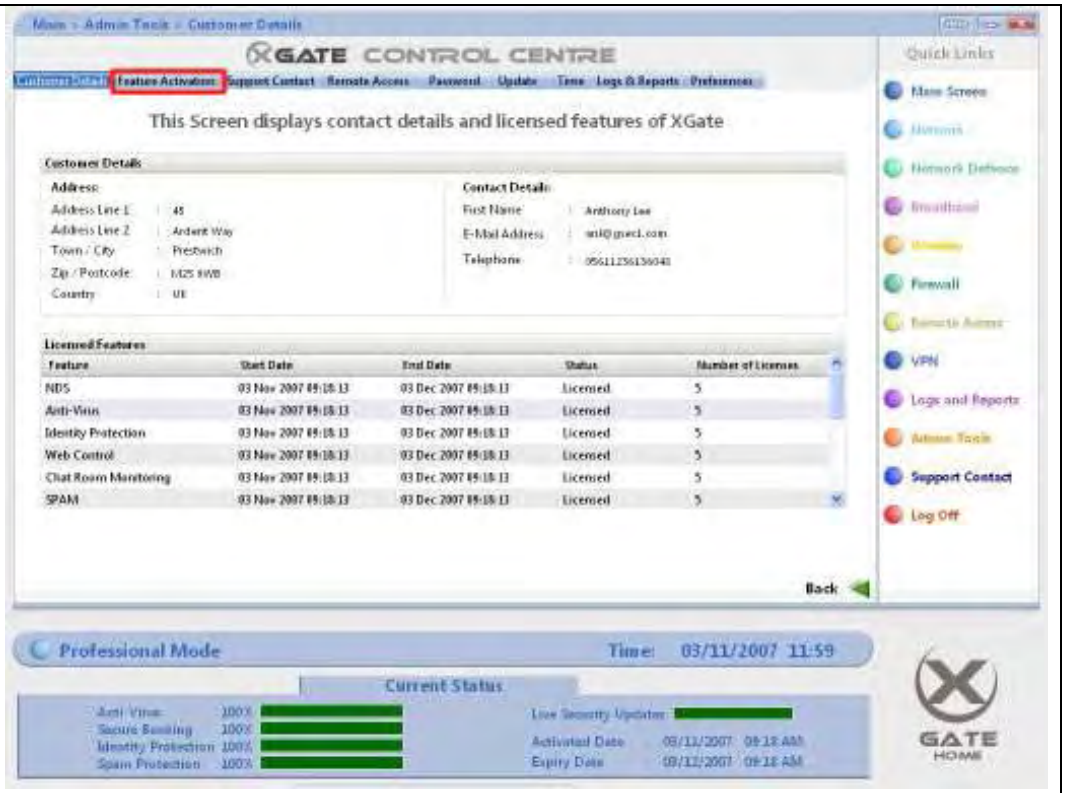

3) Press the SMS Balance View button.

If you wish to continue using Mobile Text Message alerts, you will need to purchase an SMS pack.

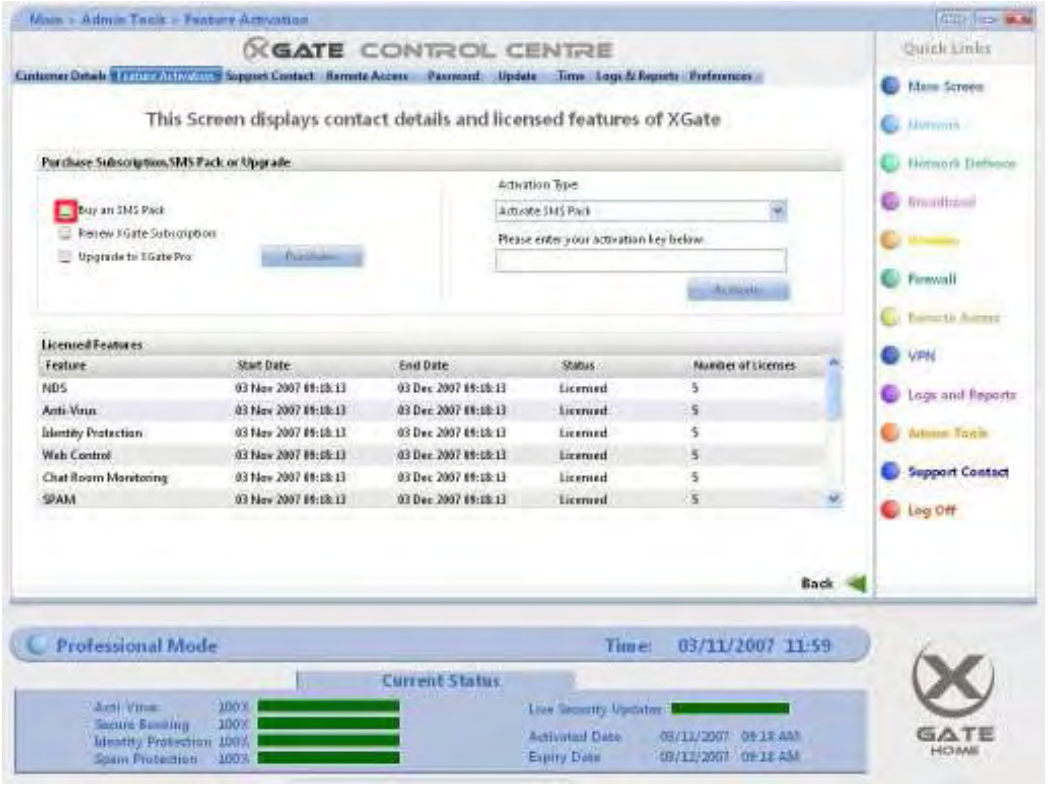
**Buying an SMS pack**

1) On the main screen, press Admin Tools.

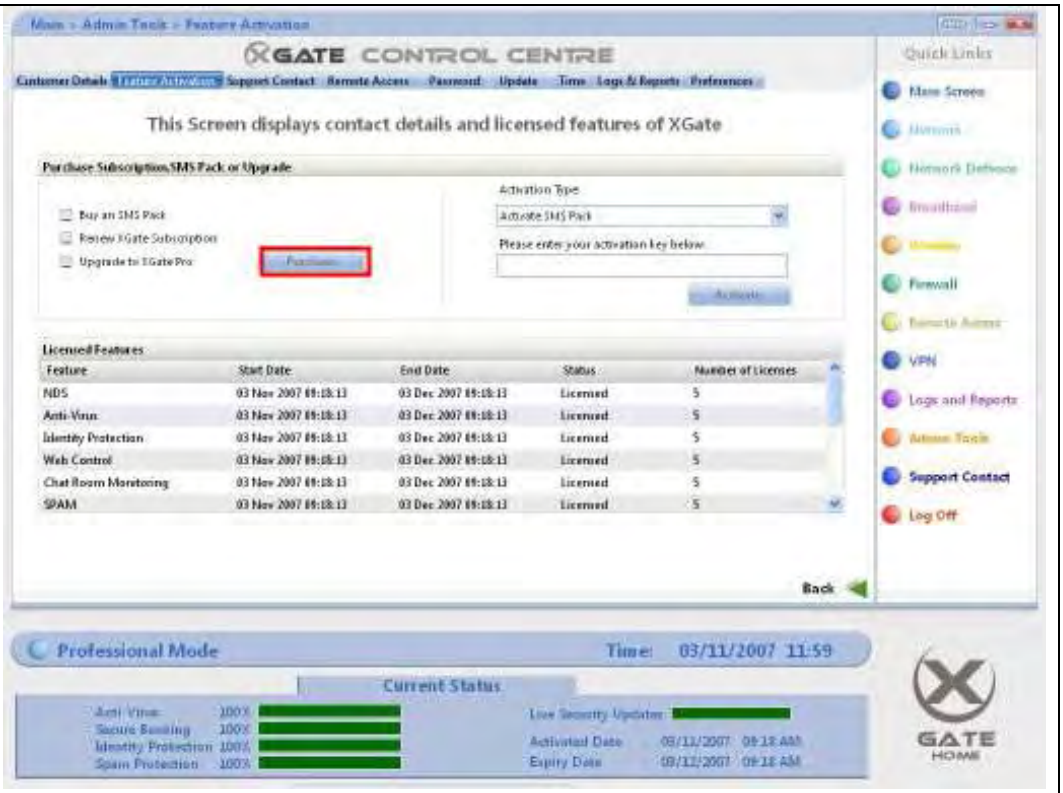

2) Press the Feature Activation tab.




3) Select Purchase an SMS pack.




4) Press the Purchase button.




5) Follow the instructions on the XGate Payment Gateway website.

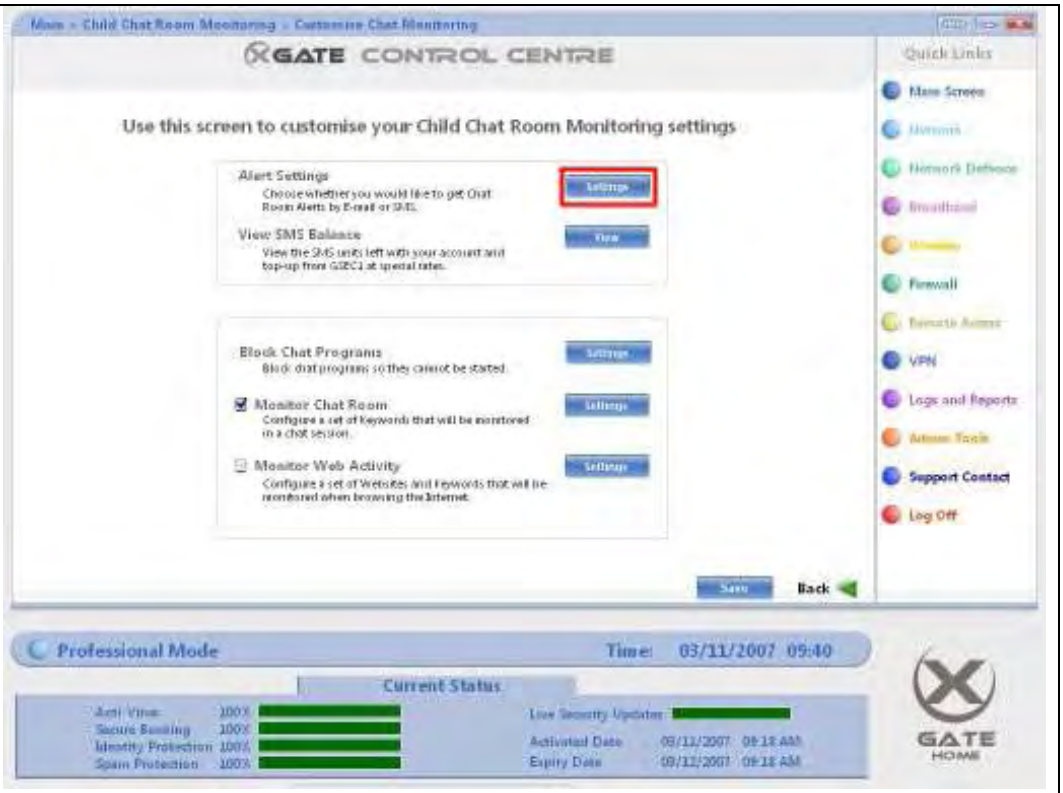
**3. I am receiving an alert every time someone opens a chat application. How do I turn this feature off?**

You may have accidentally turned this feature on in the XGate Control Centre

| **Turning off Chat Application start up alerts** |
|---|
| 1. On the main screen, press the Child Chat Room Monitoring button. |


2. Press the Customise Child Chat Room Monitoring button.


3. Press the Alert Settings button




4. Untick the Alert me when a Chat Application has been started tick box.


5. Press OK.


6. Press Save.


**4. How do I get the Web Monitoring alerts to work with Firefox or Opera?**

Currently, XGate Web Monitoring does not support Firefox and Opera.

## Mail & Anti-SPAM Troubleshooting

> **Important Note**: Please note that the Anti-SPAM feature will work only if the POP3 proxy is switched ON.

### 1. How do I receive e-mails using the XGate POP3 Server?

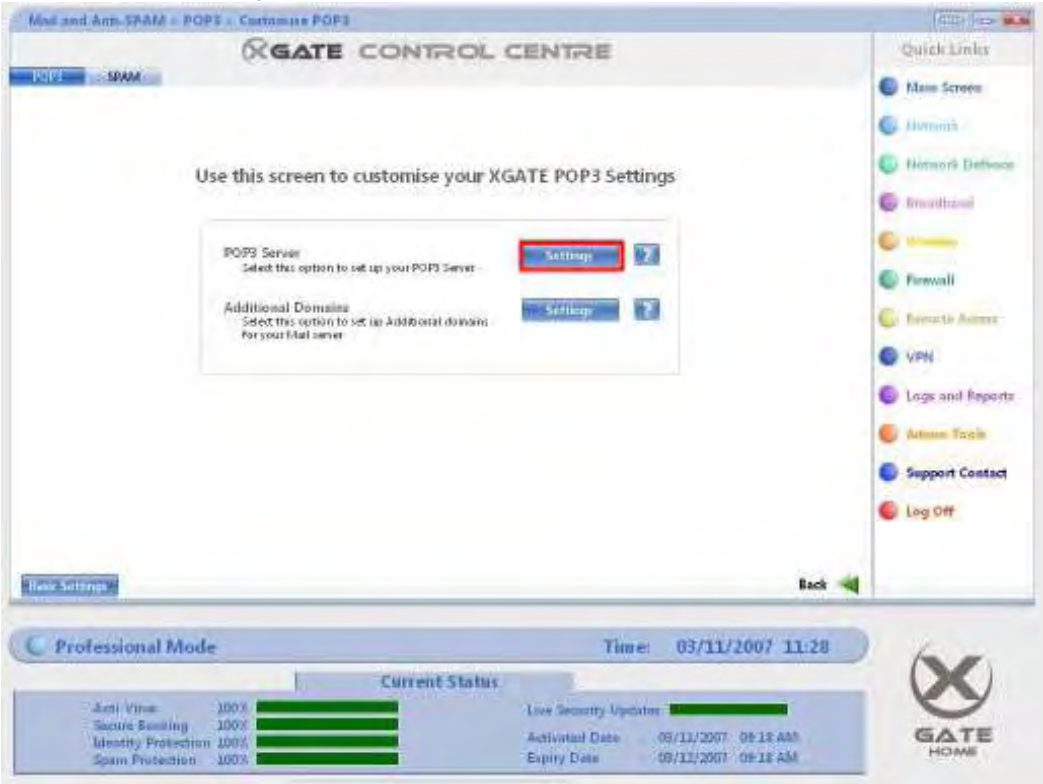
When you receive e-mails using the XGate POP3 Server, the e-mails are subject to SPAM filters. This ensures that the unwanted SPAM e-mails are segregated.

To configure your POP3 servers:

1. On the main screen, go to ***Mail and Anti Spam***
2. Select the "**On**" check box and press the Save button.

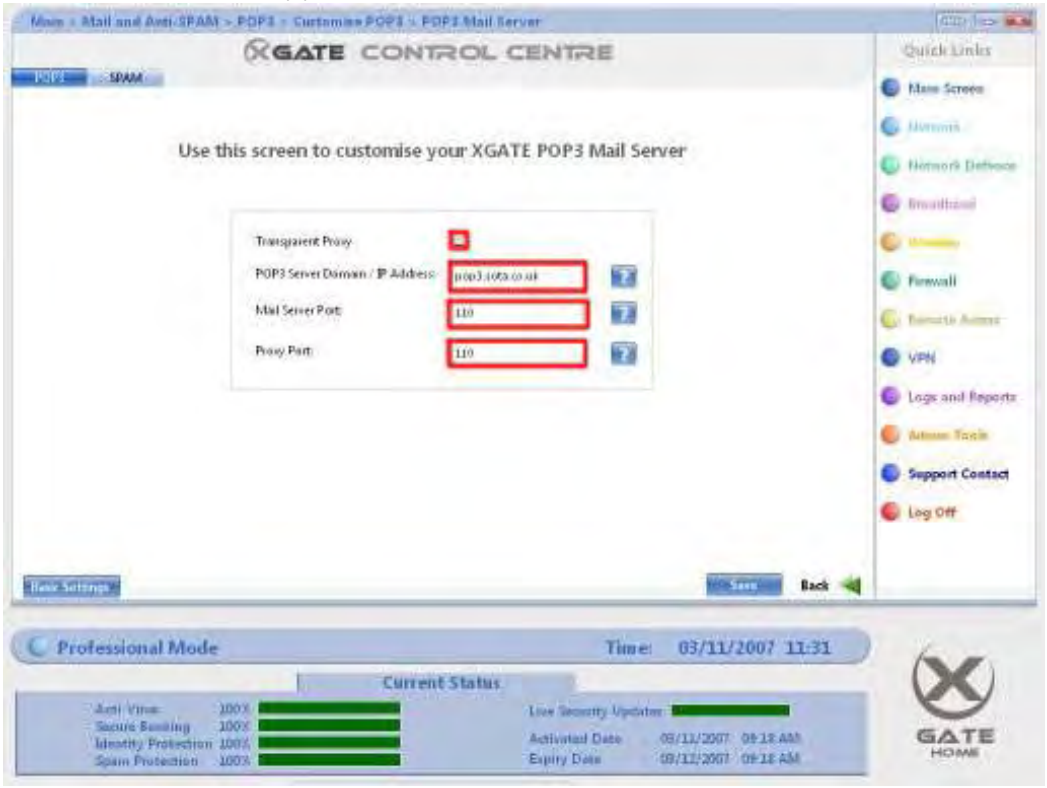

3. Click on the **Customise POP3 Settings** button.


4. Click on the **Settings** button for the POP3 Server.

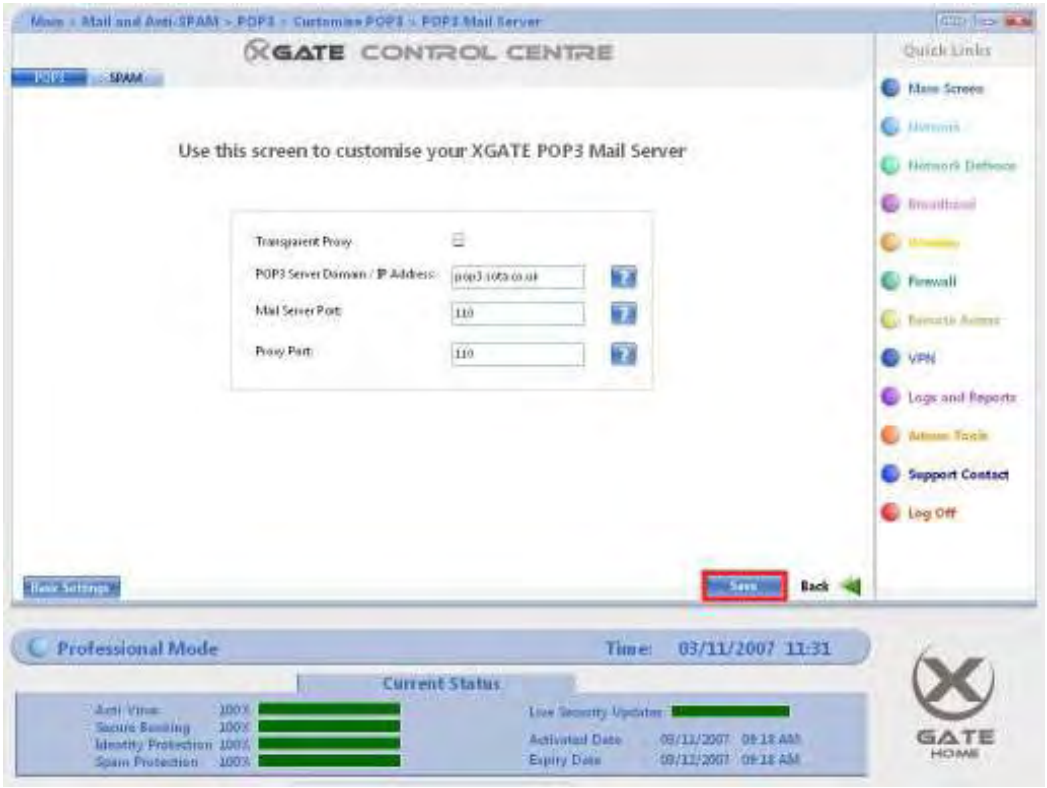



For example, if your e-mail address reads like john@mycompany.com then enter the details as follows:

1. Tick the “Transparent Proxy” check box.
2. In the POP3 Server Domain / IP Address Field, enter **mycompany.com**.
3. In the Mail Server Port field, leave the default value **110**, unless your ISP has provided any other port number for your mail server.
4. Leave the POP3 Proxy port with the default value (110).




5. Press the Save button to save the changes made.




6. You can now start to receive e-mails to your mail client.

## 2. I have a second e-mail account on a different e-mail server. How do I receive e-mails from that account?

To receive e-mails from your second account on another e-mail server, follow the instructions below:

1. On the main screen, go to ***Mail and Anti Spam***
2. Select the "**On**" check box and press the Save button.
3. Click on the **Settings** button for the **Additional Domains**
4. In the Additional Mail Domains screen, click the **Add** button

For example, if your second e-mail address is john@sota.co.uk then enter the details as follows:

1. In the Server Name field, enter a user friendly name for the mail server (**Sota Account** for example).
2. In the Server Domain / IP Address Field, enter ***sota.co.uk***
3. Press the OK button.

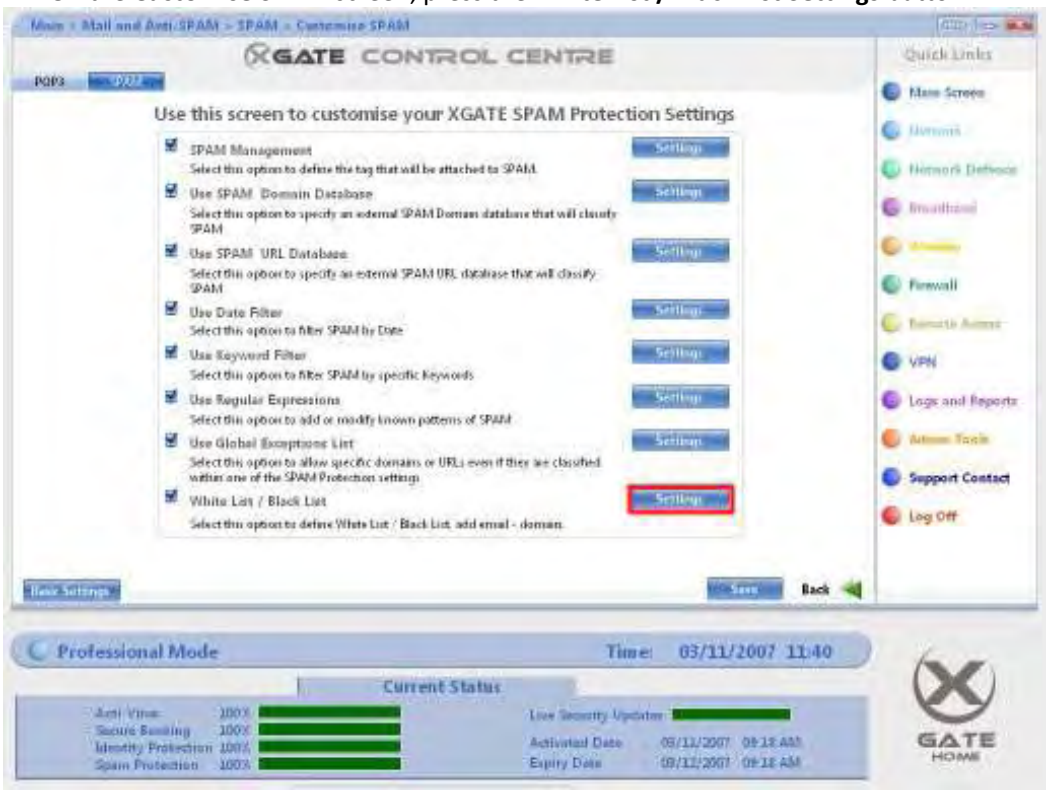
Press the Save button to save the changes made. Now you can configure your e-mail client to receive e-mails from the second account.

**Important Note**: Please note that XGate does not support POP3 accounts that require SSL authentication. As a result, you may not be able to configure XGate to receive e-mails from popular web based e-mail providers like **GMAIL** or **Yahoo**.

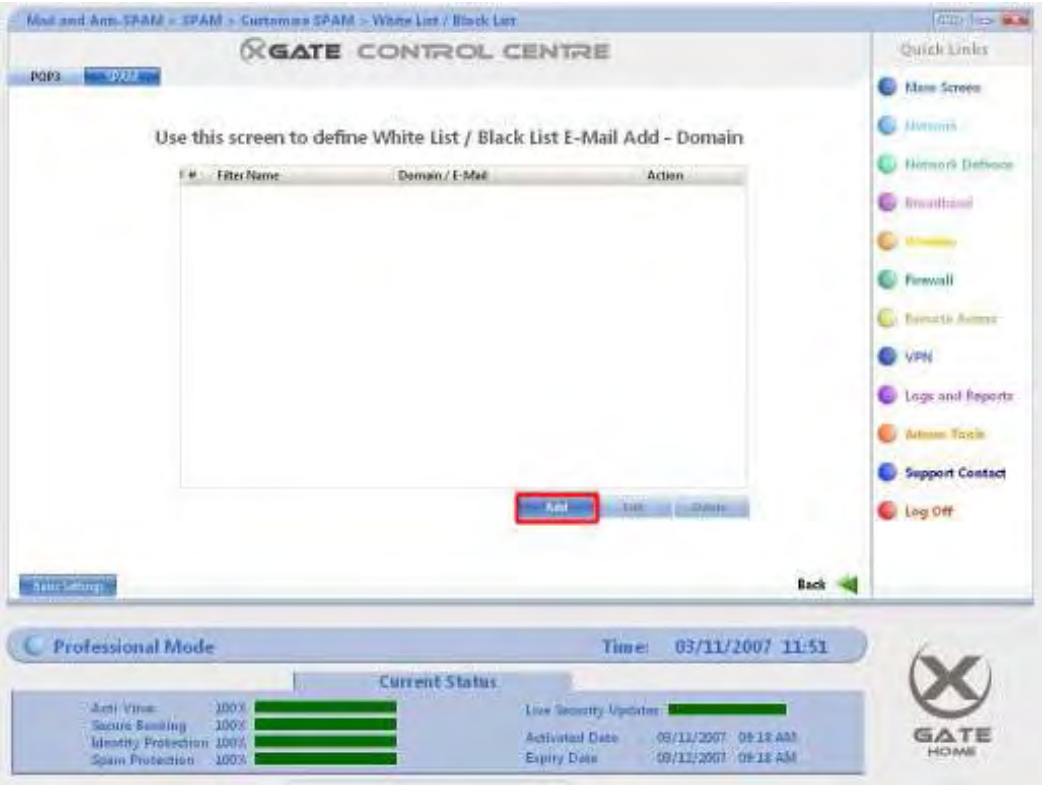
**3. A lot of SPAM e-mails are still not being classified as SPAM. How do I remedy this?**

XGate provides you several ways to filter SPAM e-mails. Also it is pre-configured to filter the most common SPAM e-mails. However, in the case where you need to explicitly mark e-mails from a specific person or domain as SPAM, you can use the Black List feature.

| **Use Black list – Method 1** |
| --- |
| The best way to add an e-mail address to the black list is to use the Classify feature of the ***XGate Outlook Add-in***. After the installation of XGate Sensor, an Add-in is attached to your Microsoft Outlook E-mail client. This has three buttons, one of which is "Classify".<br><br>Use the following procedure to add an e-mail address to the black list:<br><br>1. Select the e-mail which you consider as a SPAM<br>2. Press the Classify button in the Add-in.<br><br>The e-mail address that has sent that e-mail is added to the Black list and all the e-mails received from that e-mail address will be tagged as SPAM and moved to the SPAM folder, automatically. |

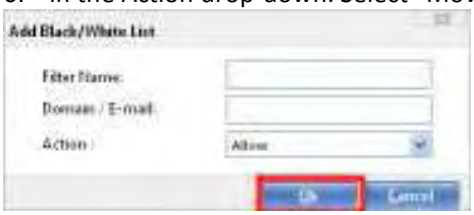
| **Use Black list – Method 2** |
| --- |
| Another way is to manually configure the black list in the XGate Control Centre. Use the following procedure to configure the black list:<br><br>1. On the **Customise SPAM** screen, press the **White List / Black List Settings** button<br>  <br> |

2. Press the **Add** button.




For example, if you want to filter e-mails from the address spammer@spam-domain.com then enter the following details:

1. In the Filter Name field, enter an user-friendly name. For example “Spammer”
2. In the Domain / E-mail field, enter the e-mail address. For example spammer@spam-domain.com
3. In the Action drop-down. Select “Move to SPAM Folder” and press the OK button.




Any e-mail received from this e-mail address in the future, will be marked as SPAM and it will be moved to the SPAM folder in your Microsoft Outlook.

Using this method, you can mark e-mails from an entire domain as SPAM. Just enter the domain name in the Domain / E-mail field.

**4. E-mails received from known persons are tagged as SPAM. How do I prevent this?**

You can use the either of the following methods, to prevent wanted e-mails getting tagged as SPAM.

**Use White list – Method 1**

The best way to add an e-mail address to the white list is to use the **De-classify** feature of the ***XGate Outlook Add-in***. After the installation of XGate Sensor, an Add-in is attached to your Microsoft Outlook E-mail client. This has three buttons, one of which is “De-classify”.

Use the following procedure to add an e-mail address to the white list:

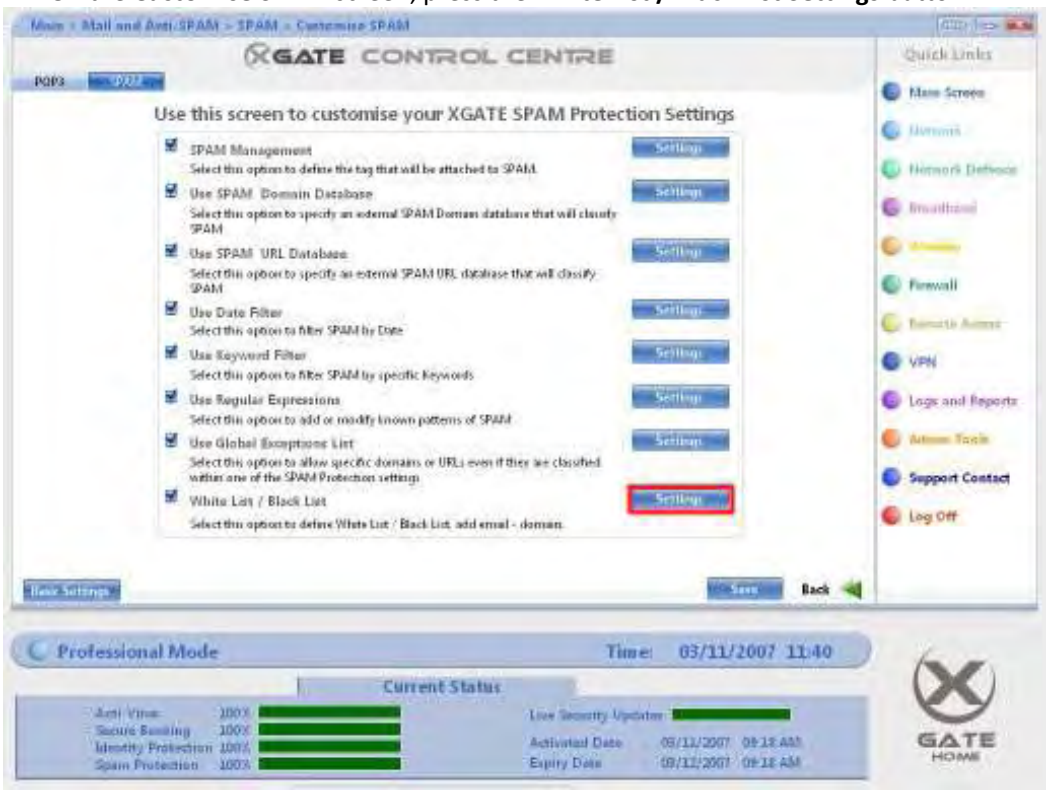
1. In Microsoft Outlook, go to the SPAM Folder.
2. Select the e-mail which you consider as a good mail.
3. Press the De-classify button in the Add-in.

The selected e-mail address is added to the white list automatically and all the e-mails received from that e-mail address will not be subject to any SPAM filters.

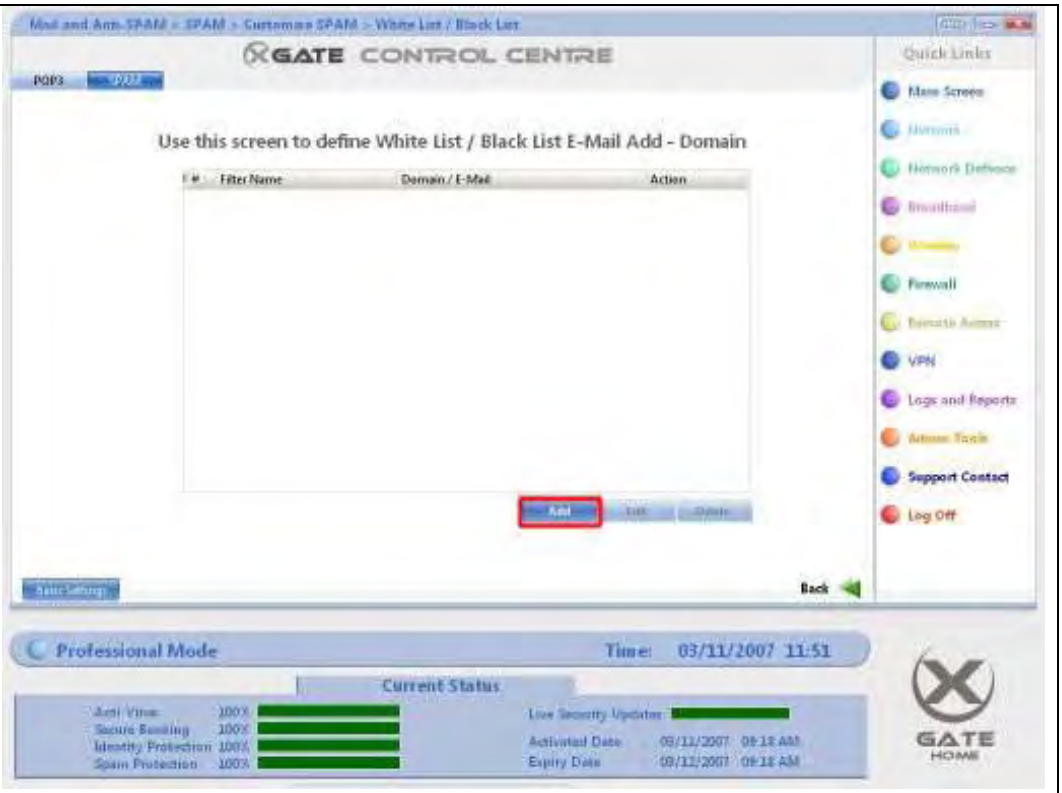
**Use white list – Method 2**

Another way is to manually configure the white list in the XGate Control Centre.
Use the following procedure to configure the white list:

1. On the **Customise SPAM** screen, press the **White List / Black List Settings** button.

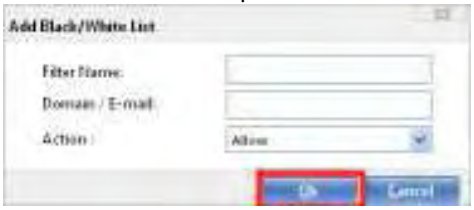



2. Click the Add button.




For example, if you want to filter e-mails from the address friend@friend-domain.com then enter the following details:

1. In the Filter Name field, enter an user-friendly name. For example “My Friend”
2. In the Domain / E-mail field, enter the e-mail address. For example friend@friend-domain.com
3. In the Action drop-down. Select “Allow” and press the OK button.




Any e-mail received from this e-mail address in the future, will not be subject to any SPAM filters.

Using this method, you can mark e-mails from an entire domain as SPAM. Just enter the domain name in the Domain / E-mail field.

**5. Is it possible to change the SPAM tag that is added to the SPAM E-mails?**

The subject of any E-mail that is filtered using the SPAM filter will be prefixed with a tag for identification purposes. By default the name of the tag is “XGATE SPAM”.

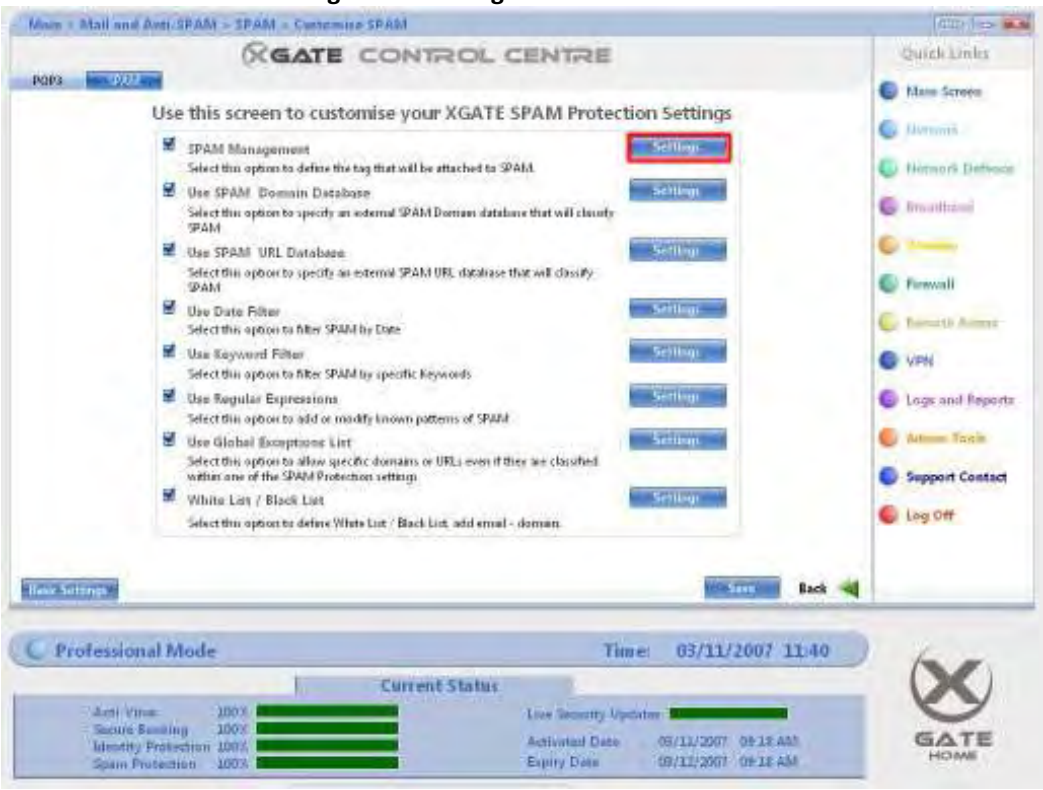
To change this tag:

1. On the main screen, click the **Mail and Anti SPAM** button


2. Click the **SPAM** tab

3. Click on the **Customise SPAM** button


4. Click on the **SPAM Management Settings** button




5. In the Define SPAM Tag field, enter a tag of your wish.

6. Press OK to save the changes.


After this point, any e-mail that is tagged as SPAM will be tagged with the changed text.

**6. How do I disable the SPAM filter?**

1. On the main screen, click the **Mail and Anti SPAM** button


2. Click the **SPAM** tab


3. Tick the OFF checkbox.


4. Press Save to the save the changes.


Please note that if you disable the SPAM filter:

- The SPAM mails will not be tagged.
- SPAM Mails will not be moved to the SPAM folder.

**7. I have enabled the SPAM filter. But I can see SPAM tagged e-mails in my Inbox. They are not moving to the SPAM Folder. What is wrong?**

This could happen when you receive bulk of e-mails from you server, say around 50 e-mails at a time.

Press the ***Update SPAM Manually*** button in the SPAM Add-in. This will move the SPAM tagged e-mails to the SPAM Folder.

**8. I cannot receive mail using my Outlook mail client from Google or Yahoo mail. What is going wrong?**

Google and Yahoo mail use SSL to deliver mail to your mail client. SSL prevents inspection of incoming mail and as a result XGate cannot filter your mail for spam.

To workaround this issue please follow FAQ 9.

**9. I have multiple POP3 e-mail accounts and followed your instructions on how receive e-mails using the XGate POP3 Server. Now I can only receive mails from one account. What do I do?**

This is due to the transparent proxy. It is forcing all requests to receive mail to be directed at only one of your mail providers.

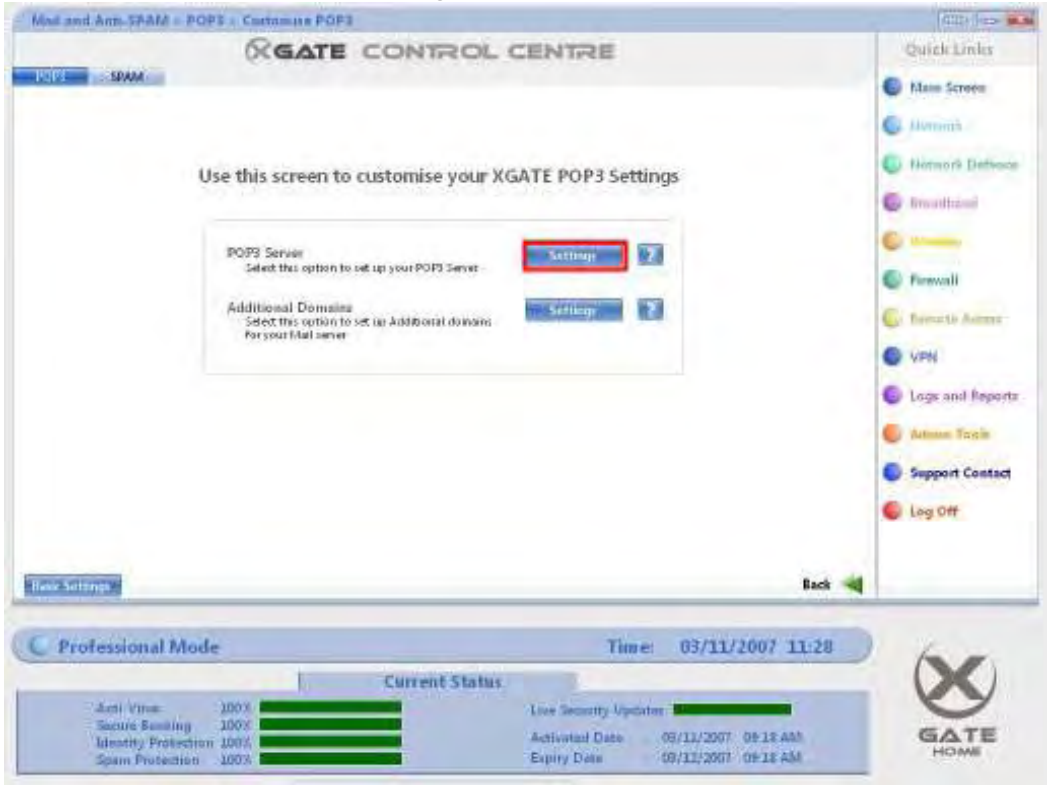
There are two steps to remedy this issue:

Step 1: Turning off the transparent proxy:

1. On the main screen, go to ***Mail and Anti Spam***

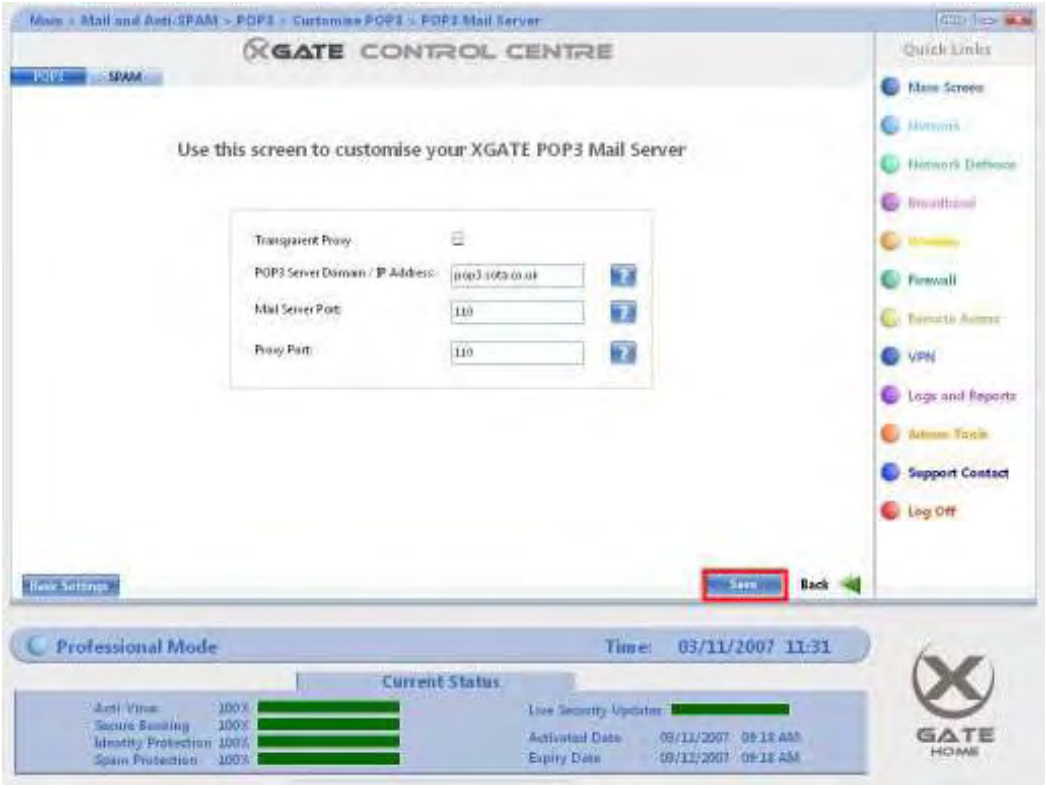

2. Select the "**On**" check box and press the Save button.


3. Click on the **Customise POP3 Settings** button.




4. Untick Transparent Proxy.

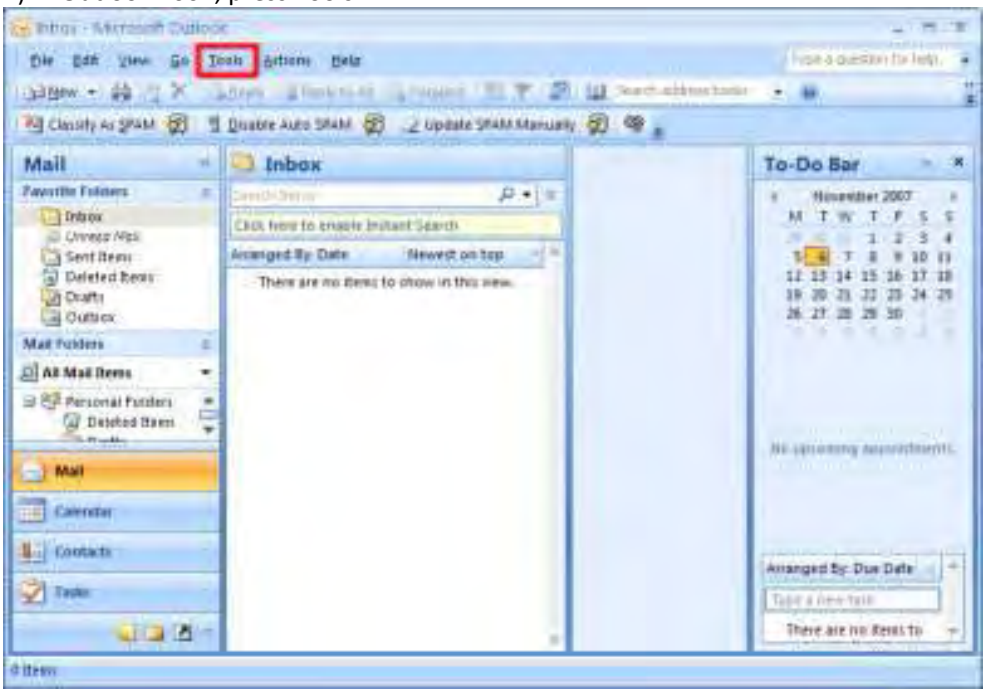

5. Press the Save button




Step 2: Configuring your mail accounts in Outlook

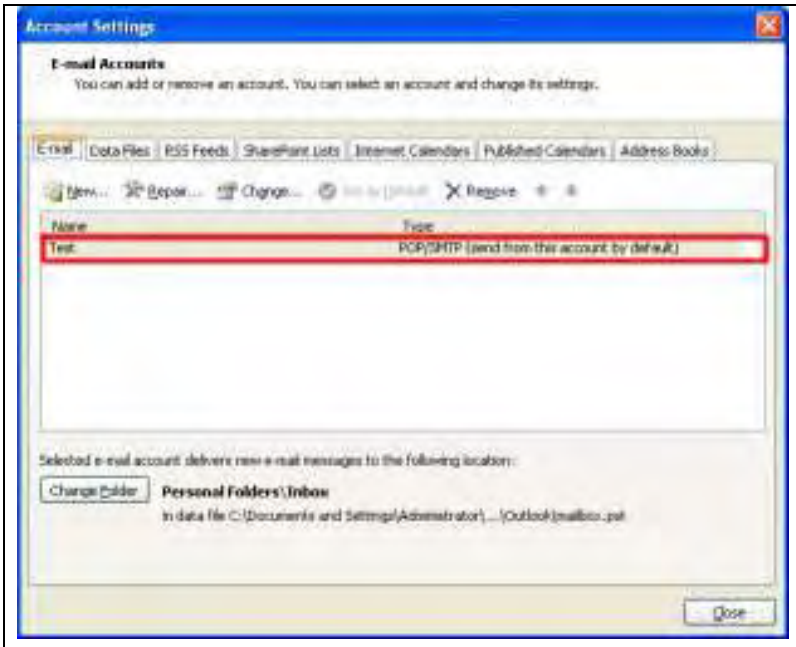
**Scenario 1: Outlook 2007**

1) In Outlook 2007, press Tools.




2) Press Account Settings…

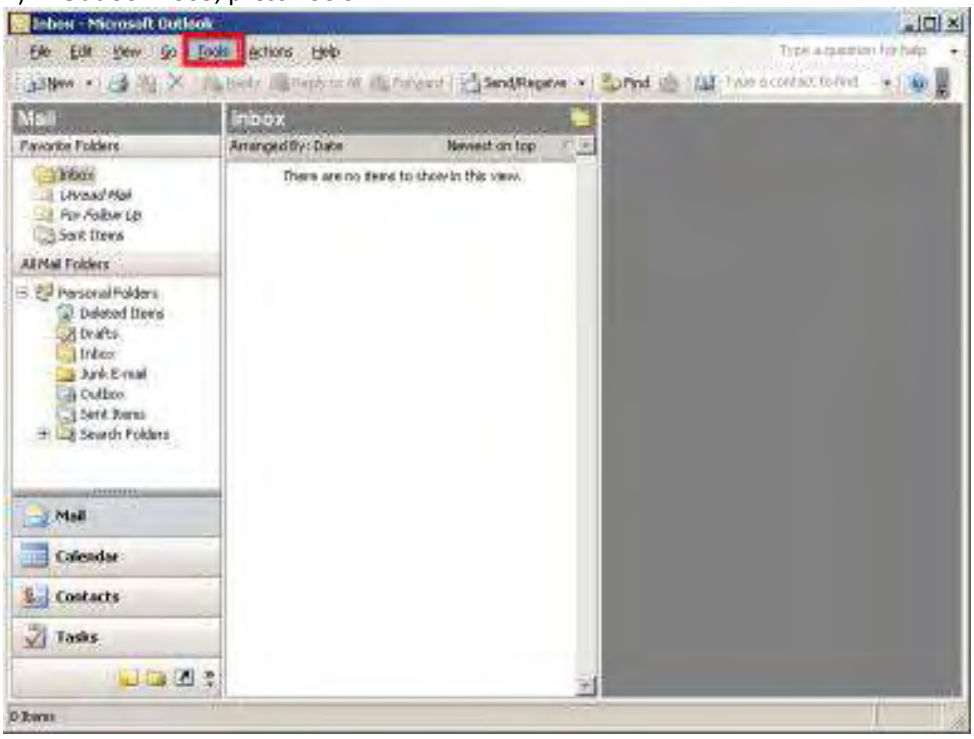

3) Double click on one of the mail accounts that is not going to be filtered for SPAM.



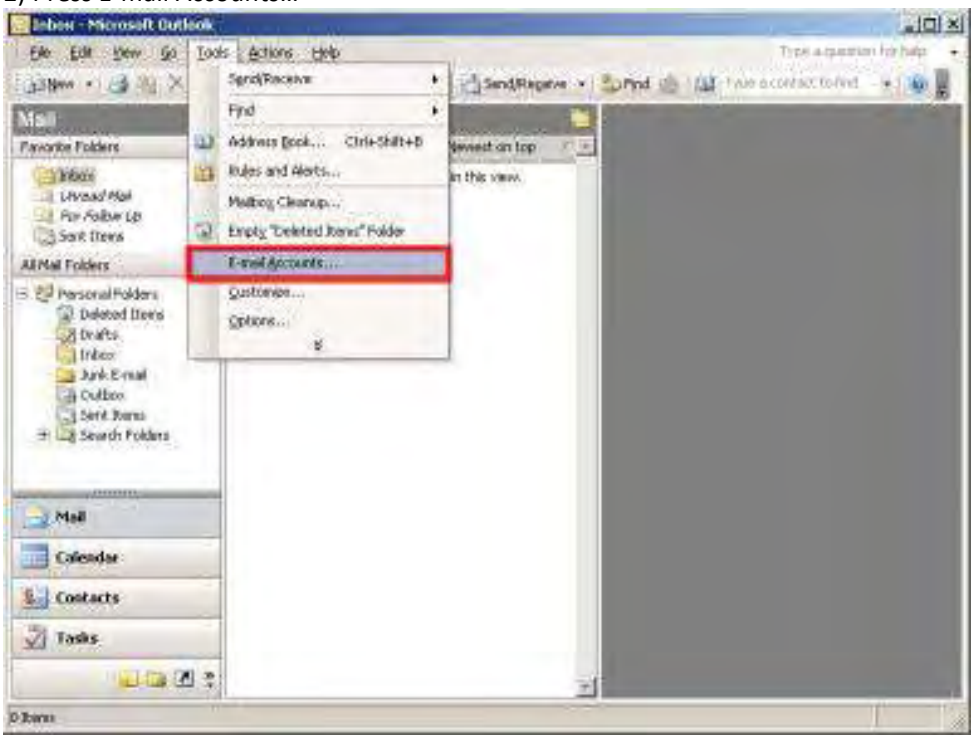

4) On Incoming mail server, type in the LAN IP Address of your XGate (by default this is 192.168.2.1)

**Scenario 2: Outlook 2003**

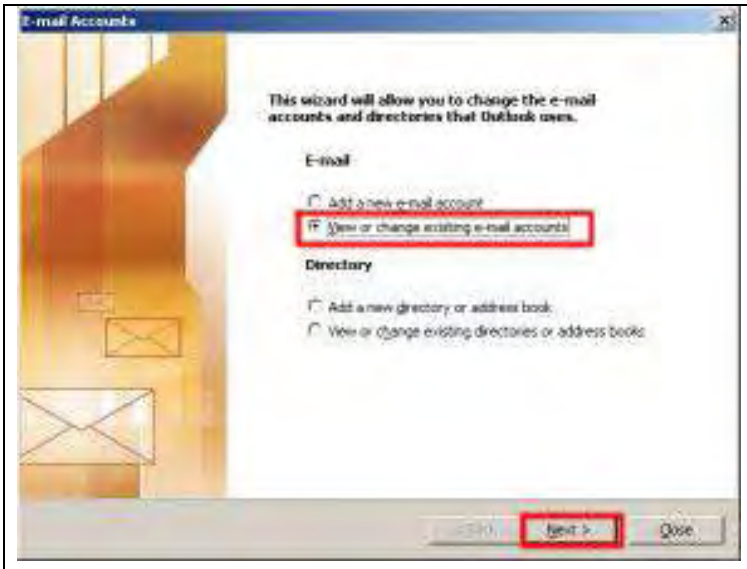
1) In Outlook 2003, press Tools.



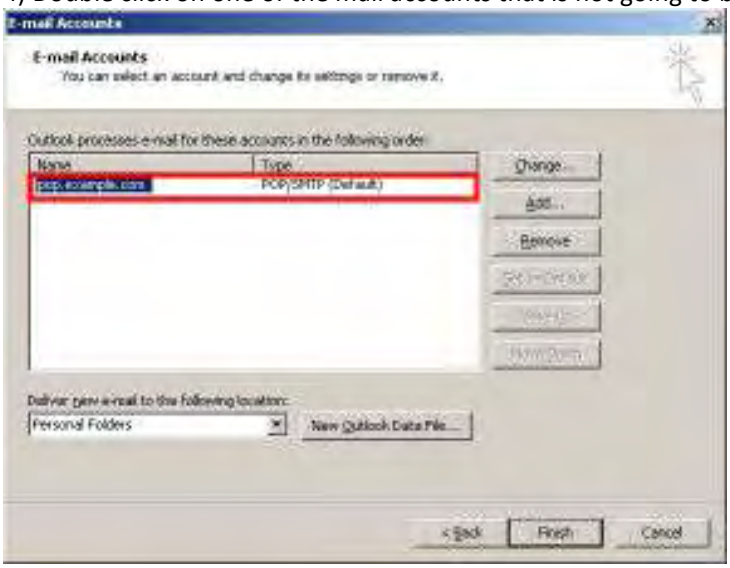

2) Press E-mail Accounts…




3) Select View or change existing e-mail accounts then press Next.



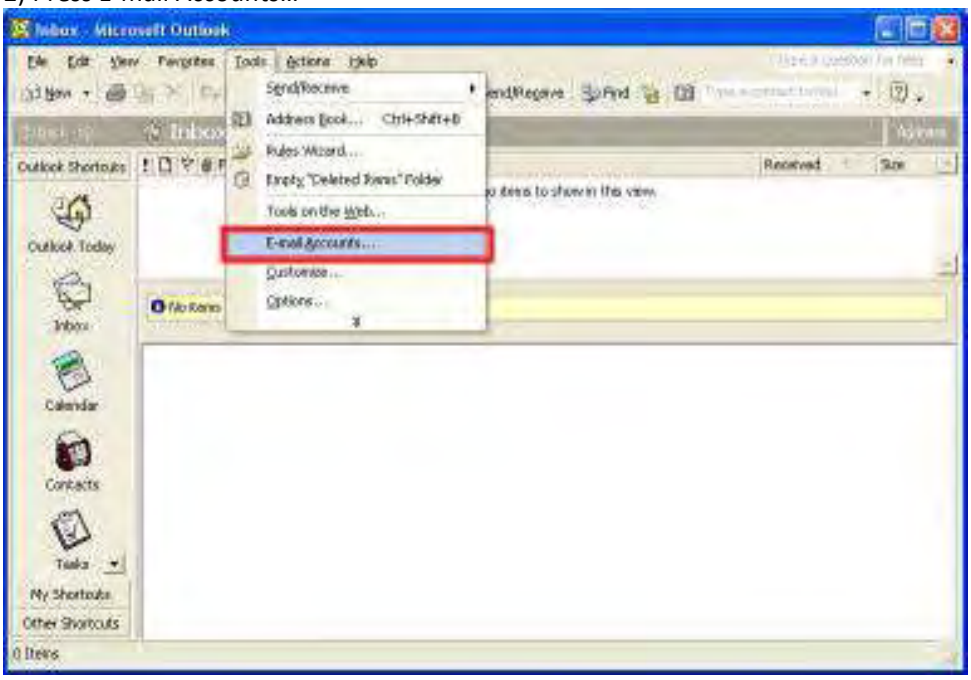

4) Double click on one of the mail accounts that is not going to be filtered for SPAM.



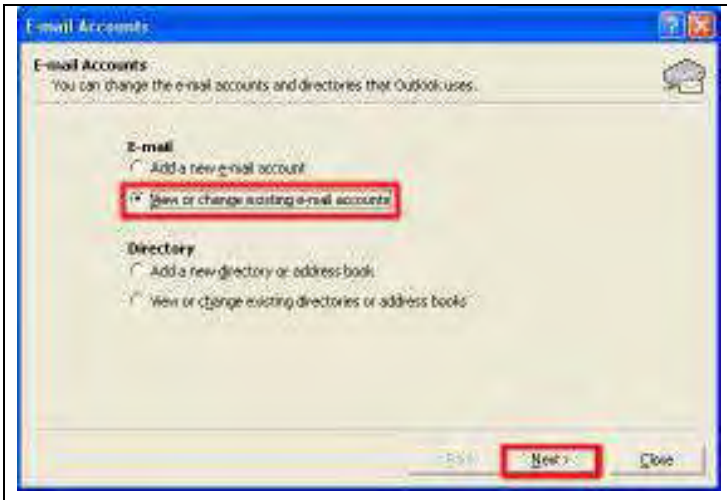

5) On Incoming mail server (POP3), type in the LAN IP Address of your XGate (by default this is 192.168.2.1)


| **Scenario 3: Outlook 2002/XP** |
| --- |
| 1) In Outlook 2002/XP, press Tools. |

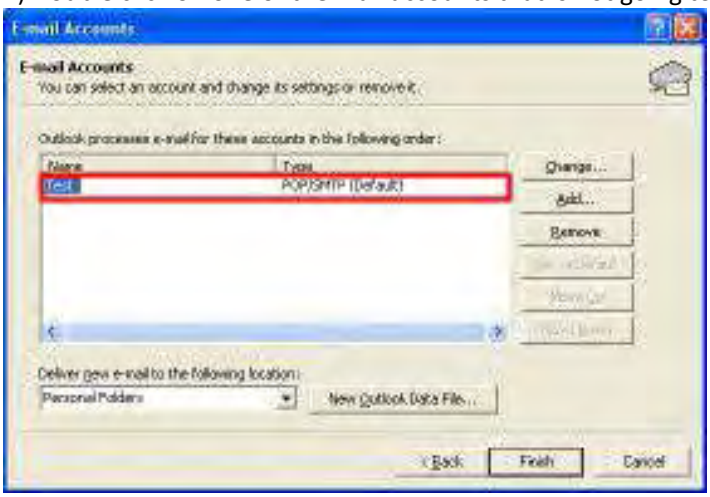

2) Press E-mail Accounts…



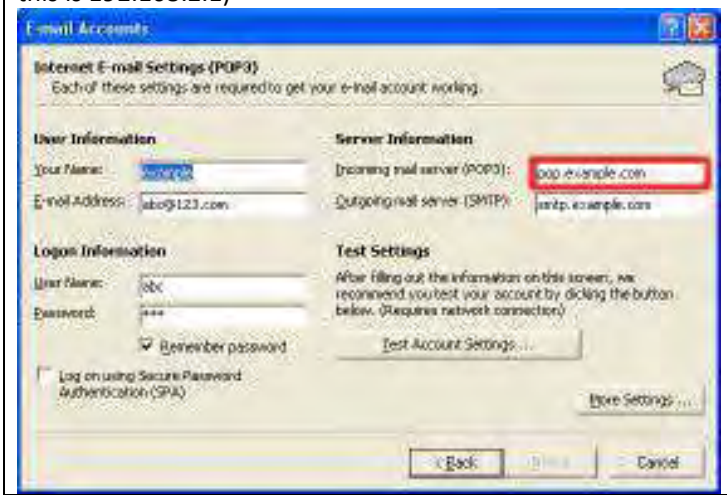

3) Select View or change existing e-mail accounts then press Next.



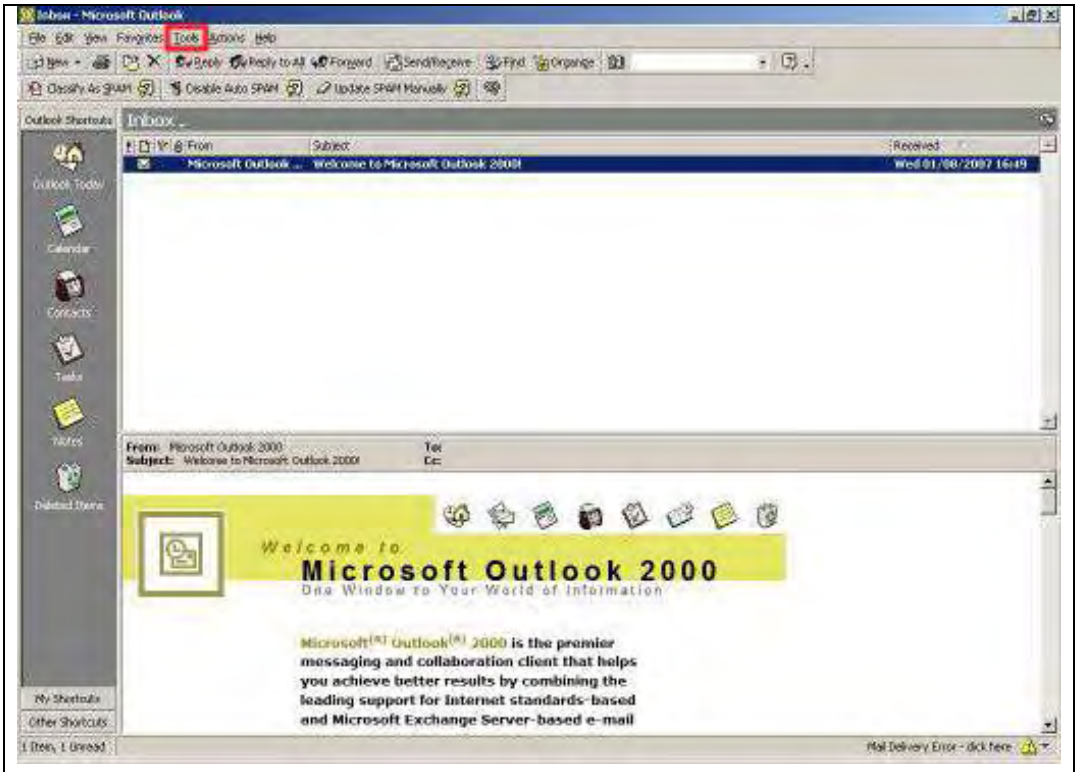

4) Double click on one of the mail accounts that is not going to be filtered for SPAM.



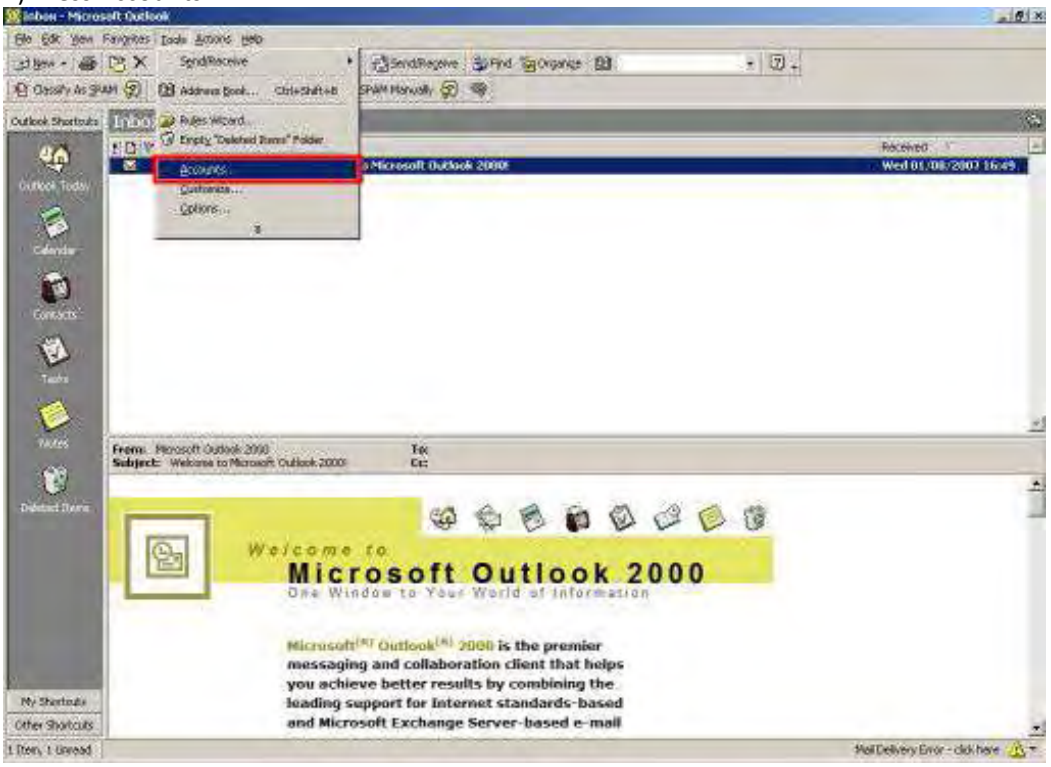

5) On Incoming mail server (POP3), type in the LAN IP Address of your XGate (by default this is 192.168.2.1)



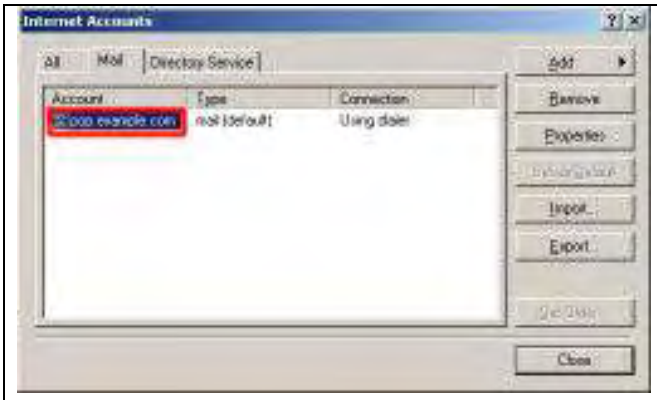

| **Scenario 4: Outlook 2000** |
| --- |
| 1) In Outlook 2000, press Tools. |




2) Press Accounts…




3) Double click on one of the mail accounts that is not going to be filtered for SPAM.




4) Click on the Servers tab.


5) On Incoming mail server (POP3), type in the LAN IP Address of your XGate (by default this is 192.168.2.1)


If you do this for each of the mail accounts that are not specified in the XGate Control Centre

– POP3 Server screen, you should be able to receive mail.

## Web Control Troubleshooting

**Important Note**:

1. The Web Control features works on the basis of categories. Websites are Categorised based on their content. You can control the access to these websites by simply enabling or disabling the categories.
2. You can use Exceptions to allow a specific website even though it is falling under a blocked category.
3. The customisation of Web Control module is applicable only to the computers where XGate sensor is installed. The ***Customise Web Control*** screen will not display computers that do not have sensors.
4. Any computer that does not have the Sensor will be governed by the Default Categories selected in factory settings. You cannot change this selection.

**1. Immediately after installing XGate in my network, some of the websites I visit regularly are blocked. How do I access them?**

XGate is pre-configured to block websites that are classified under a set of categories. These are selected by default.

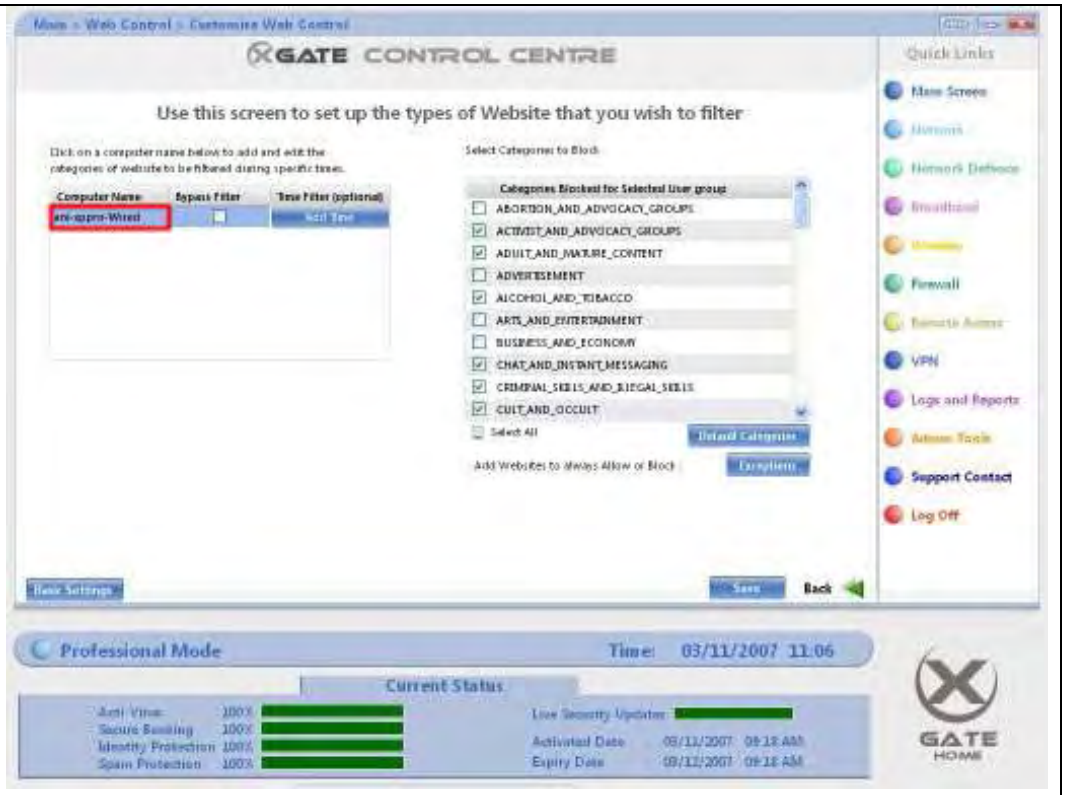
To get access to the blocked site, follow the steps below:

- On the main screen, press the **Web Control** button.

- Click on the **Customise Web control** button.


For example, www.ebay.com is blocked under a category INTERNET_AUCTIONS then there are two possible solutions:

| **1. Allow the INTERNET_AUCTION category:** |
| --- |
| 1. In the left hand side, select the Computer for which you wish to allow the website. |



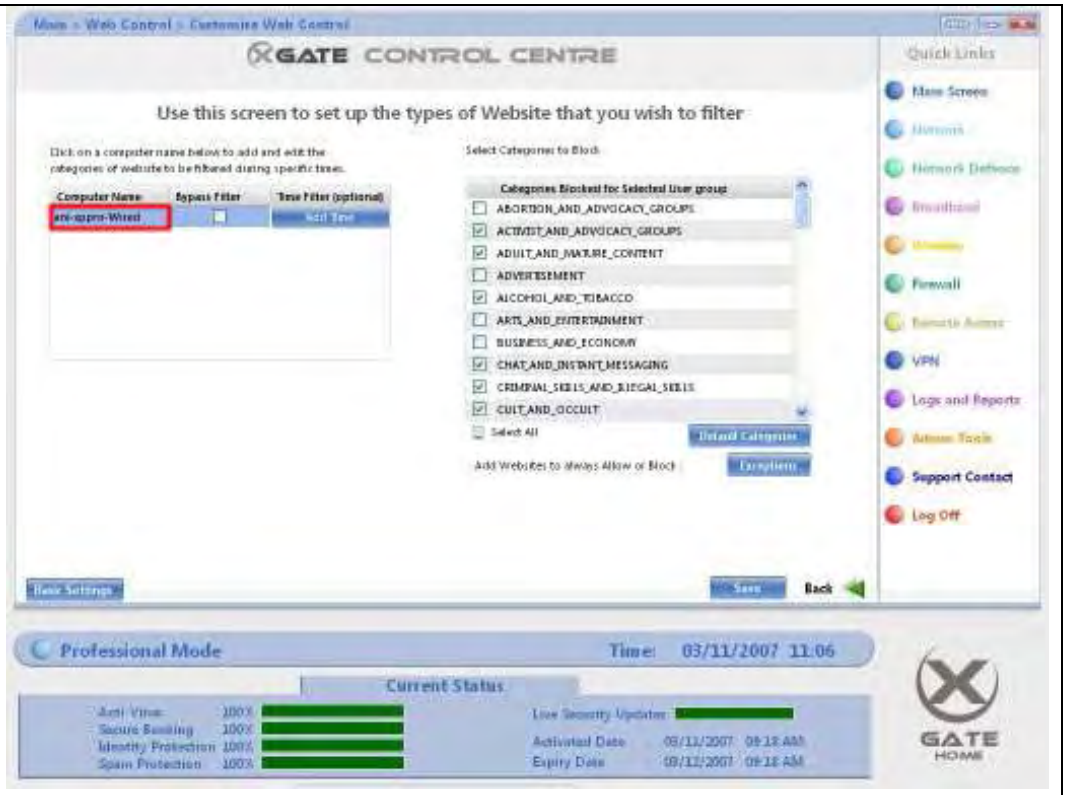

2. In the right hand side, scroll to find the category INTERNET_AUCTION and clear the checkbox selection.


3. Press the Save button.

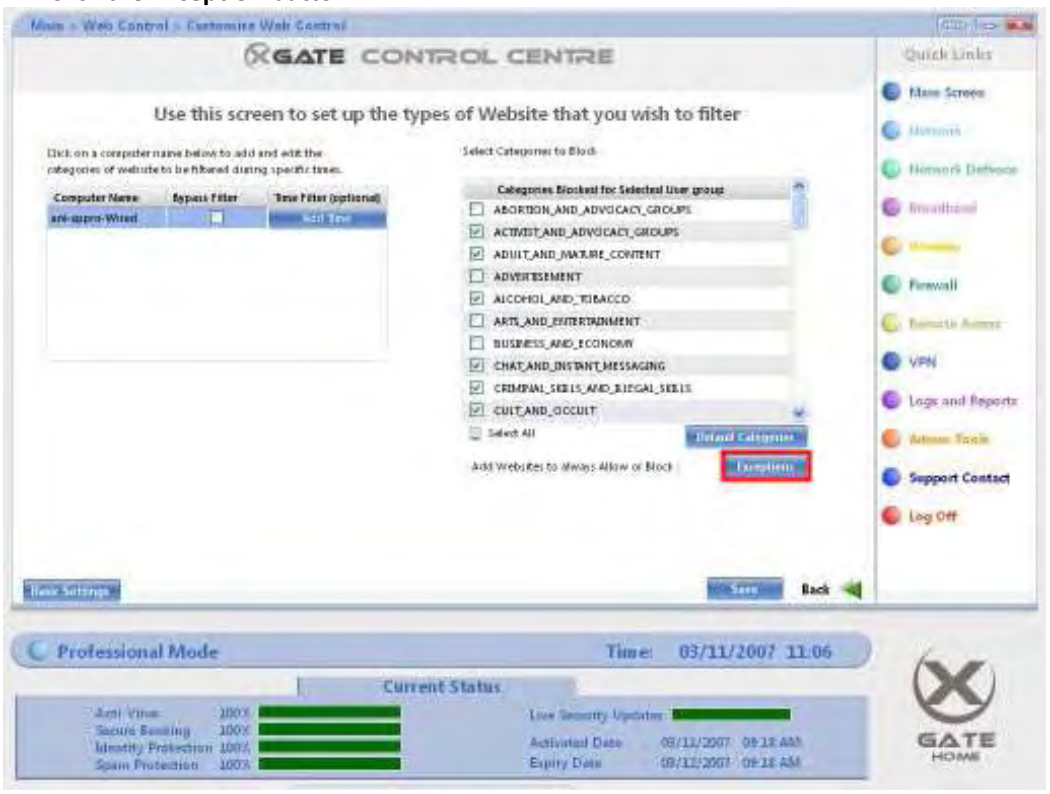

However, please note that all the websites categorized under INTERNET_AUCTION will be accessible.

**2. Add the website to the Exception List**

1. In the left hand side, select the computer for which you wish to allow the website.




2. Click the **Exception** button**.**

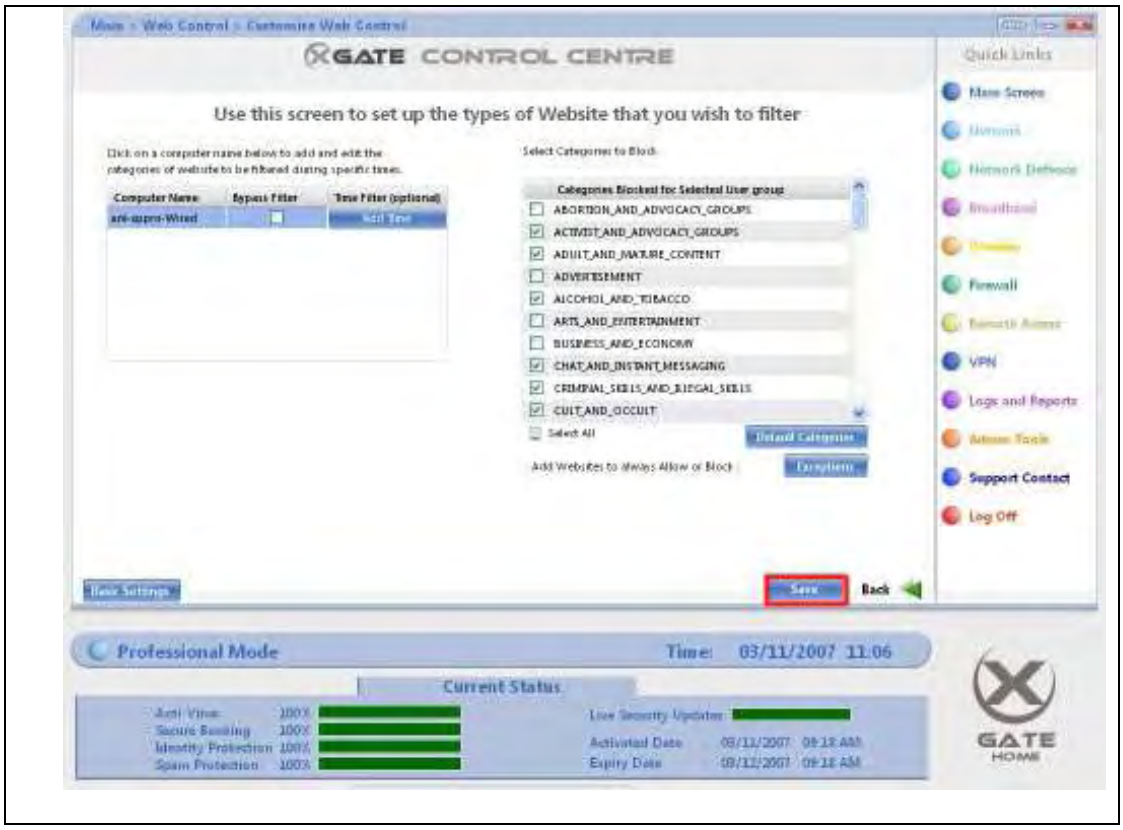



3. In the **Website Address** field, type www.ebay.com. Do not enter the http:// qualifier.
4. In the **Action** Field, select Allow.

5. Press the **Add** button.


6. Press the **OK** button.


7. Press the **Save** button.




**2. I want to block access to a specific site but I do not know which category it belongs to. How do I block it?**

When you want to block access to a specific website and you do not know about the category it belongs to, follow the steps below:

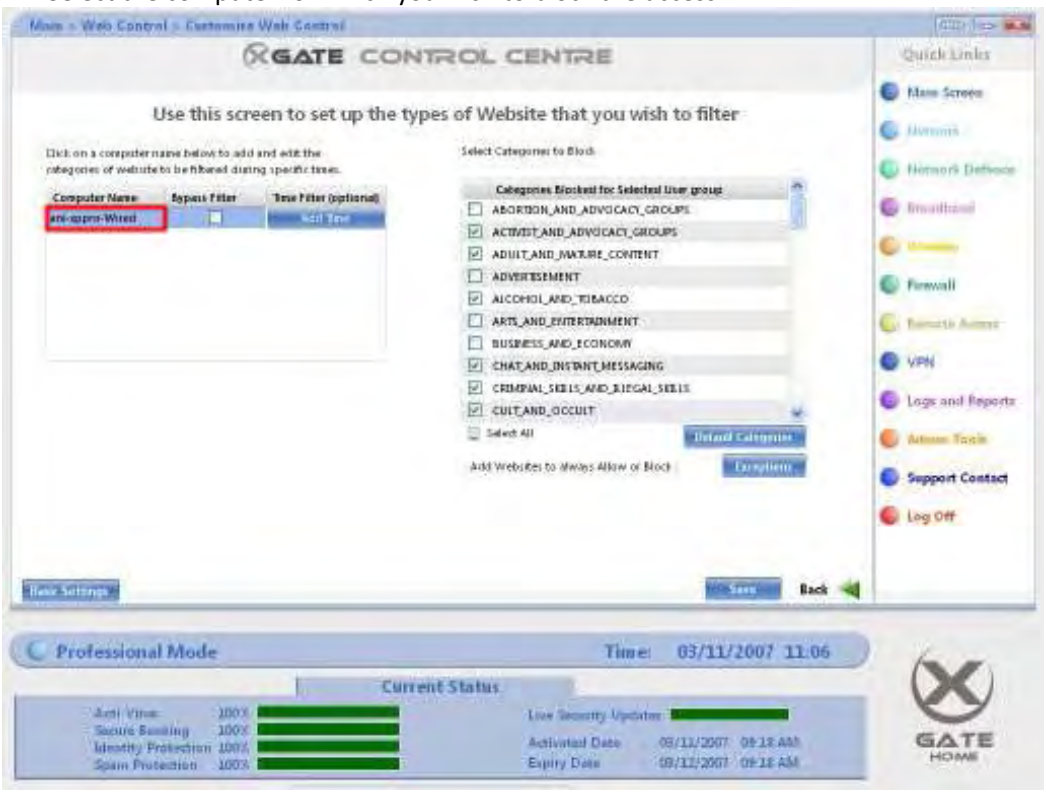
1) On the main screen, press the **Web Control** button.


2) Click on the **Customise Web control** button.


For example, you want to block the access to the website www.casinoonline.com.

**Add the website to the Exception**

1. Select the computer for which you wish to block the access.




2. Click the **Exception** button.

3. In the **Website Address** field, type www.casinoonline.com
4. In the **Action** Field, select Block.
5. Press the **Add** button


6. Press the **OK** button.


7. Press the **Save** button.


The selected computer will not be able to access the website www.casinoonline.com.

3. **I do not want my employees to watch sports sites during office hours. How do I do that?**

You can use Time Based Filter to block / allow access to websites on specific time periods in a day.

1) On the main screen, press the **Web Control** button.


2) Click on the **Customise Web control** button.

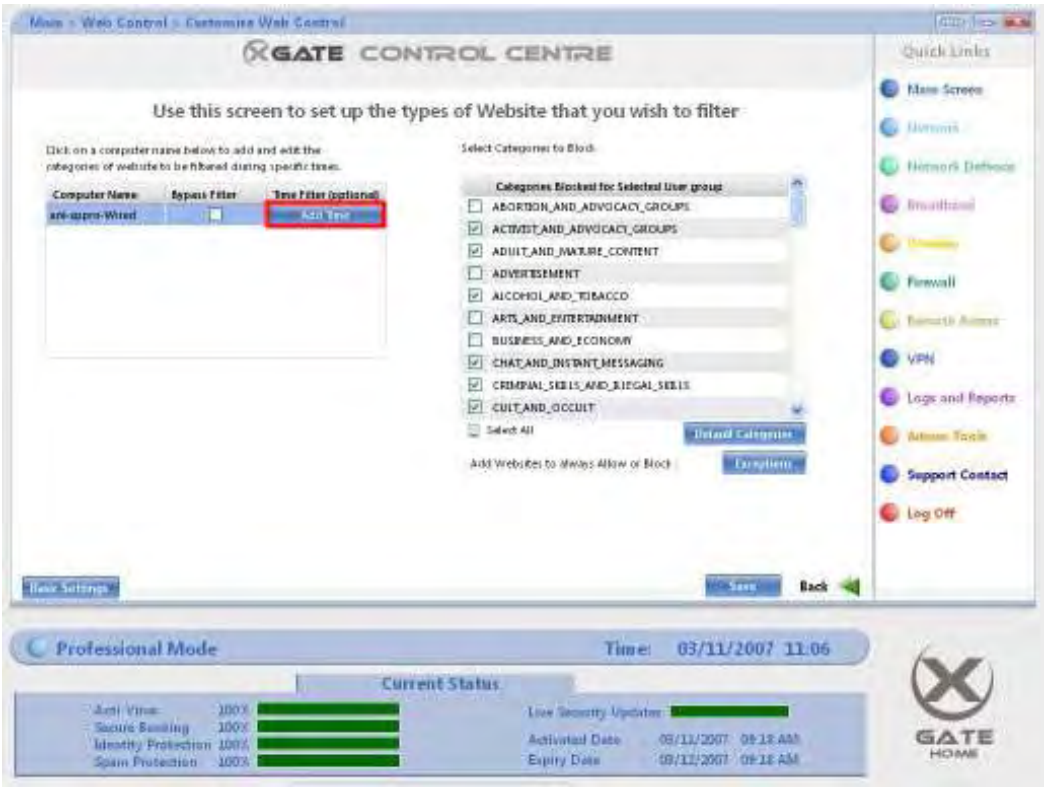
For Example, follow the steps below to block a particular website, *www.espn.go.com,* during office hours and allow it during lunch hour [1.00 PM to 2.00 PM].

| **Block the website first** |
| --- |
| Follow the steps in the FAQ 2 and block the website www.espn.go.com |

**Allow the website in the lunch hour**

Using the following procedure, allow access to www.espn.go.com during the lunch hour:

1. Click the **Add Time** button of the computer which you wish to grant access during the lunch hour.




2. In the Time Period section enter 13.00 for the **Start** field.
3. Enter 14.00 for the End field.
4. In the Days section, select the **All** Checkbox.
5. Press the **Add** button.


6. The time 13:00 – 14:00 will be added to the grid.
7. Select the added time period (13:00 – 14:00).
8. Click the **Exception** button in the right hand side**.**

9. In the **Website Address** field, type www.espn.go.com
10. In the **Action** Field, select Allow.
11. Press the **Add** button.


12. Press the **Ok** button.


13. Press the **Save** button.


**Important Note**:

- If you wish to accomplish the same for all the computers, you have to repeat the procedure for all the computers.
- You cannot define overlapping time periods for a given day. For example, you cannot define 13:00 – 14:00 and 13:30 – 15:00 on Monday. However, you can do that on different days.

**4. I want my computer to get access to all the websites at any time. What should I do?**

Follow the steps below to give access to all the websites for a specific computer:

1) On the main screen, press the **Web Control** button.


2) Click on the **Customise Web control** button.


3) Select the **Bypass Filter** Checkbox for the computer that you wish to give access to all websites.


4) Press the **Save** button.


**Important Note:**
If your Computer is not listed then ensure that the Sensor is installed on it.

## Wireless Troubleshooting

### 1. How do I connect my Computer/ Laptop to the XGate Wireless Network?

Your XGate device is wireless ready. This means that all the necessary data is pre-configured for you. Knowing the **Wireless Network Key** (a password), you will be able to connect to the XGate wireless network from your Laptop / Computer.

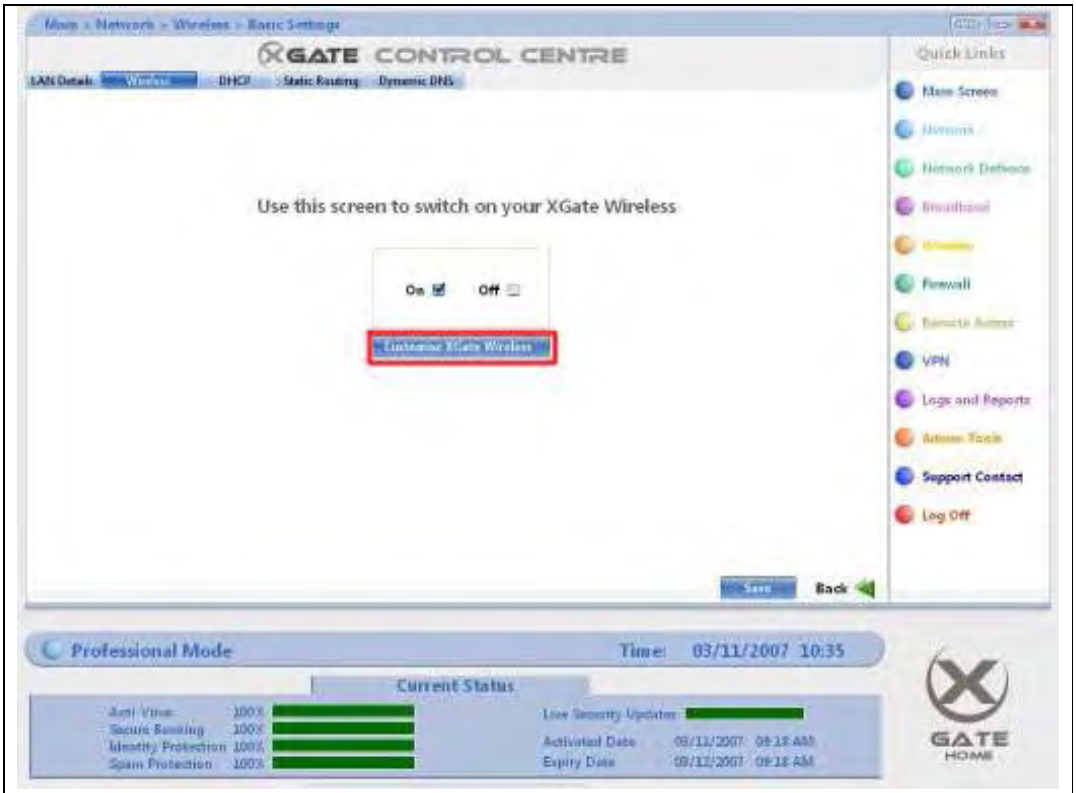
You can find your **Wireless Network Key** by looking underneath your wall mountable base stand.

However, in order to ensure maximum security, we recommend that you change the default Wireless Network Key. To change the default Wireless Network Key, follow the steps below:

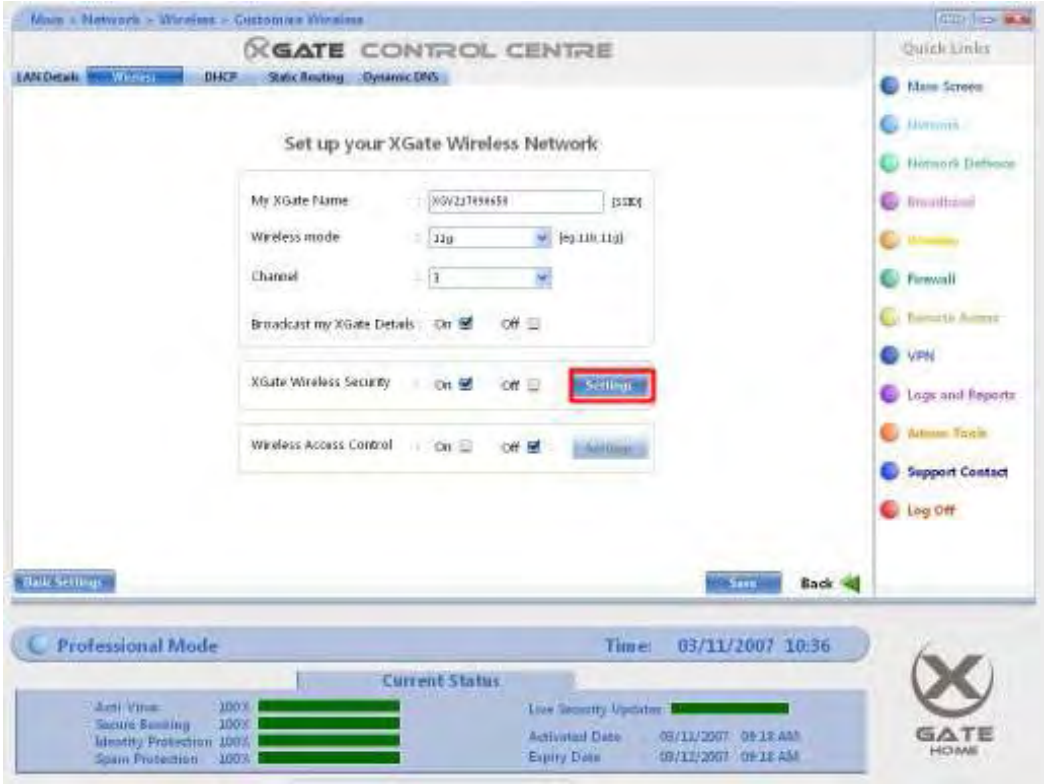
**Changing the default Network Key:**

1. On the main screen, click ***Wireless*** in the quick links section.


2. Click the **Customise Wireless Settings** button.



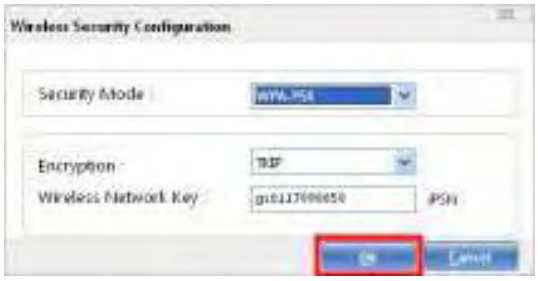

3. Change the name of the **My XGate Name** to friendly name, if you prefer.
4. Click the **Settings** button in the ***XGate Wireless Security*** section.



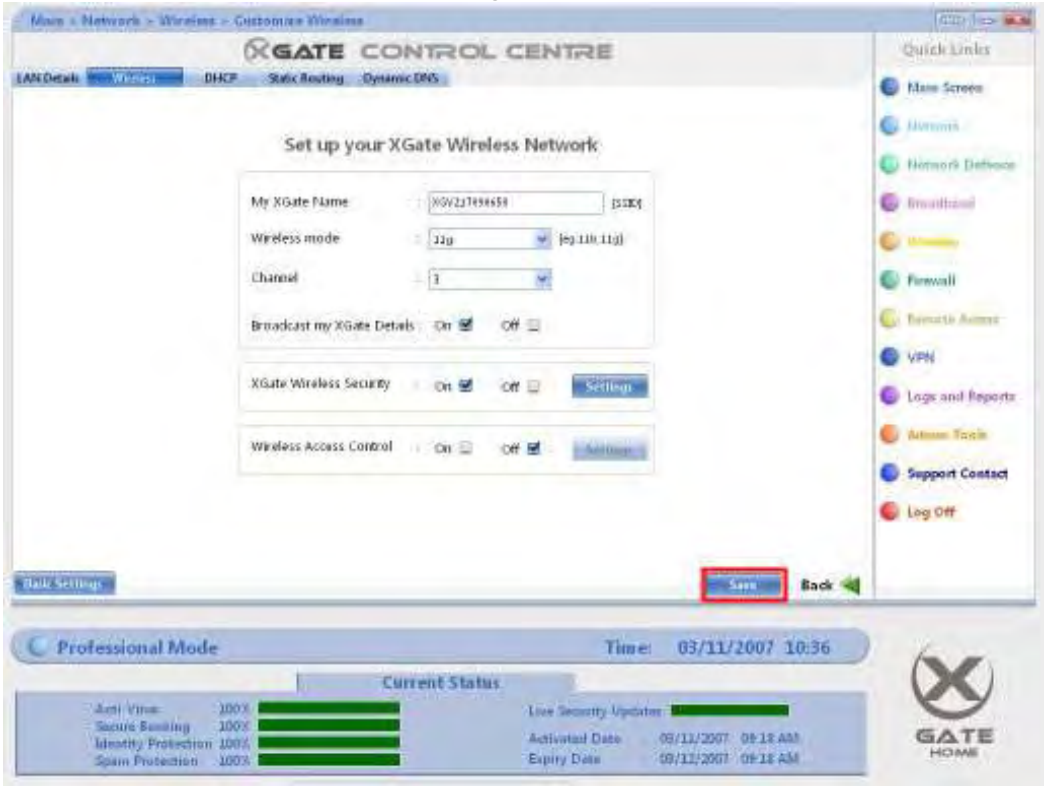

5. Change the default value of the ***Wireless Network Key*** field to a value of your choice.

Please note that a Wireless Network Key should have minimum 12 characters.

6. Press **OK** button to close the window.



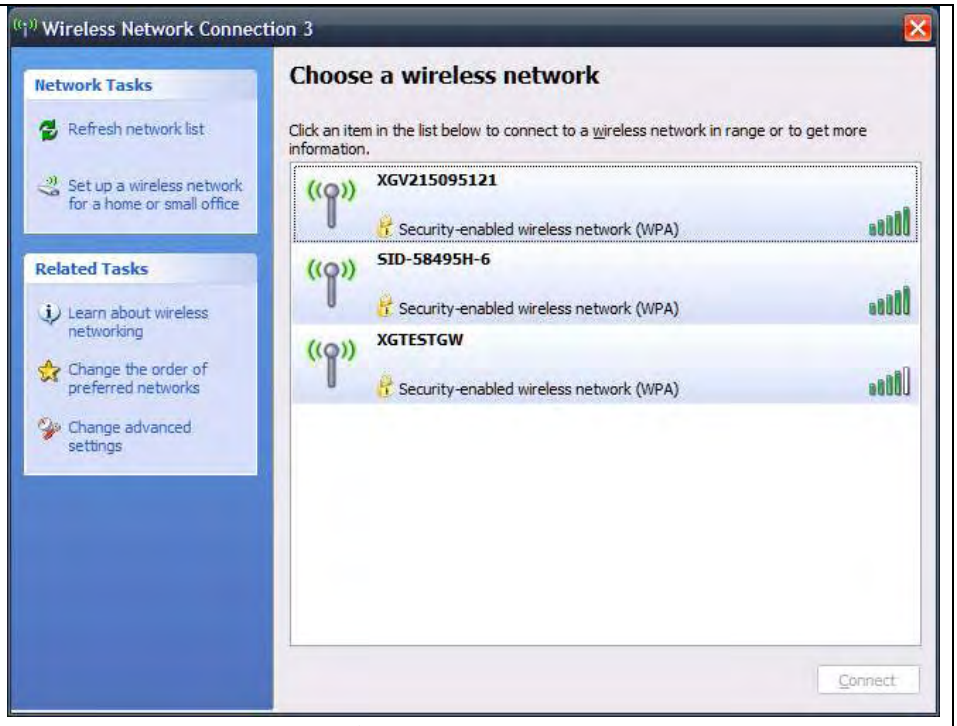

7. Press the **Save** button to save the changes.



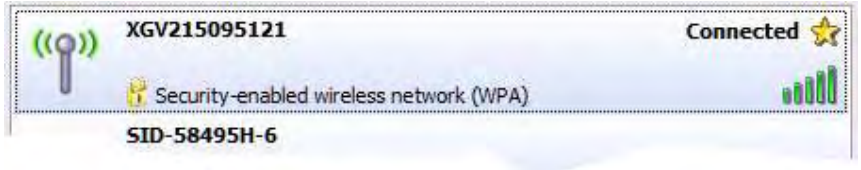

**Connecting your Laptop / Computer to the XGate Wireless Network:**

**Note**: The following instructions are specific to the **Windows XP** Operating System. For working with any other Operating System / Product, please refer the Online Help of the respective Operating System / Product.

| **Connect to XGate Wireless Network from your Laptop / Computer (XP)** |
|---|
| 1. In your system tray, look for the following icon.<br>2.  <br>3. Right Click on the icon and select the ***View available Wireless Networks*** menu.<br>4. Windows will provide you a list of Wireless Network in your Range. |

5. 

6. Select the XGate Device name from the list and click Connect.
7. You will be prompted to enter a Wireless Network Key.
8. 

9. Enter the **Wireless Network Key** and Click Connect.
10. If the connection is successful, it will be displayed as shown below:
11. 


**Important Note**: Please ensure that the signal strength (shown as vertical bars in green colour) is high. (All the bars are visible). If you have trouble in getting full signal strength, please refer to the question 4.

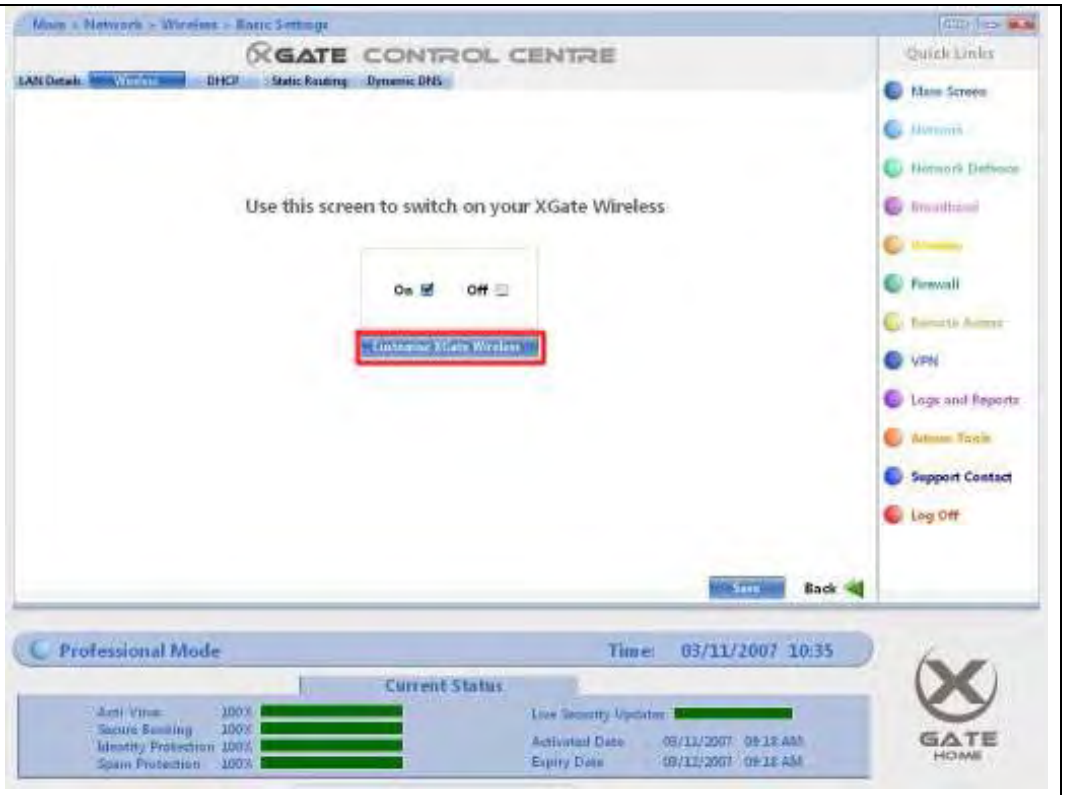
**2. I am able to see the XGate Wireless Network but I am not able to connect to it with my Laptop. What could be the problem?**

Follow the instructions given below and try to connect again.

1. Ensure that you have given the correct Wireless Network Key while connecting to the Device.

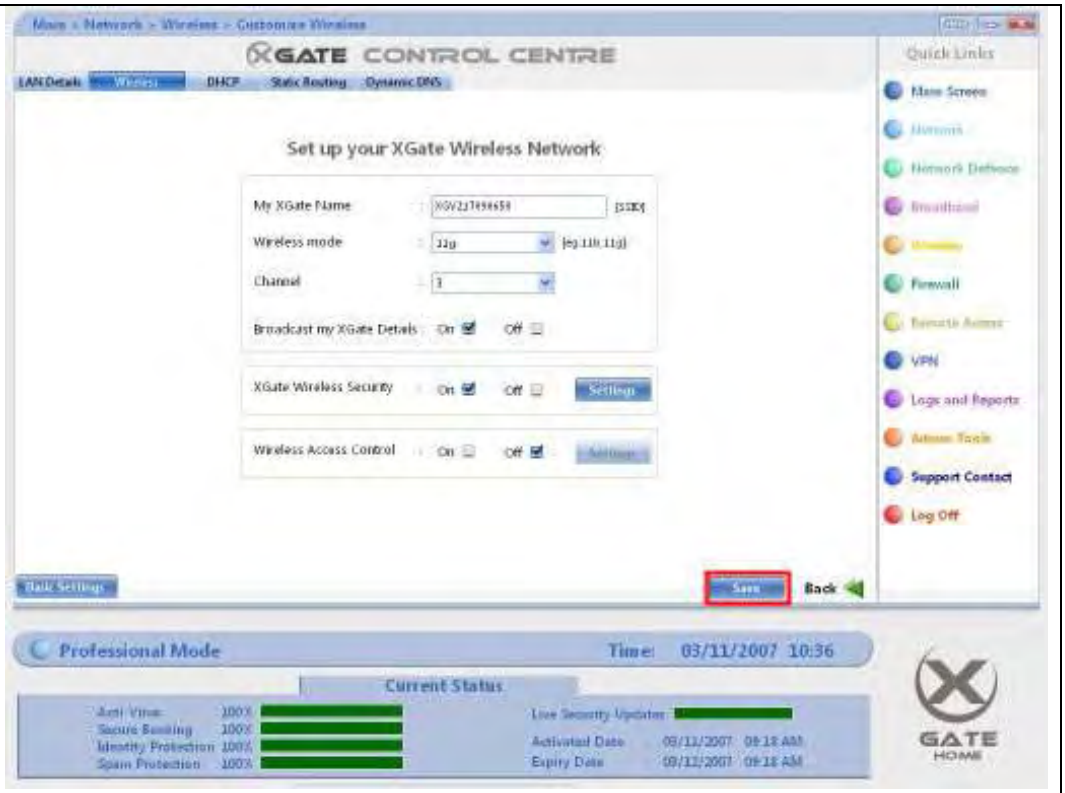
2. Ensure that **Wireless Access Control** option in XGate is switched **OFF**. To switch of, follow the steps below:
   - On the main screen, click ***Wireless*** in the quick links section.


   - Click on the **Customise Wireless Settings** button




- Select the OFF checkbox corresponding to **Wireless Access Control.**

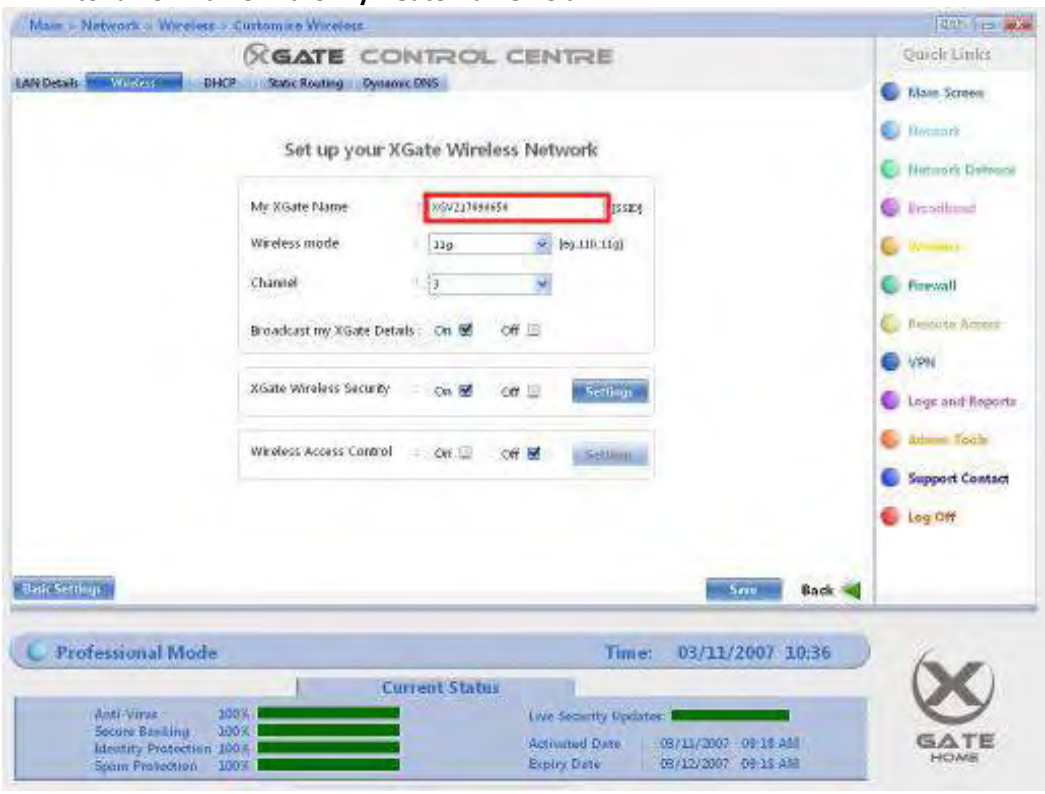

- Press the **Save** button.




3. Ensure that you do not have another Wireless Network with the same name as your XGate and you do not select that network while connecting. If required, please change the XGate Wireless Network name. To do that:
    - On the main screen, click ***Wireless*** in the quick links section.

- Click on the **Customise Wireless Settings** button


- Enter a new name in the **My XGate Name** field**.**



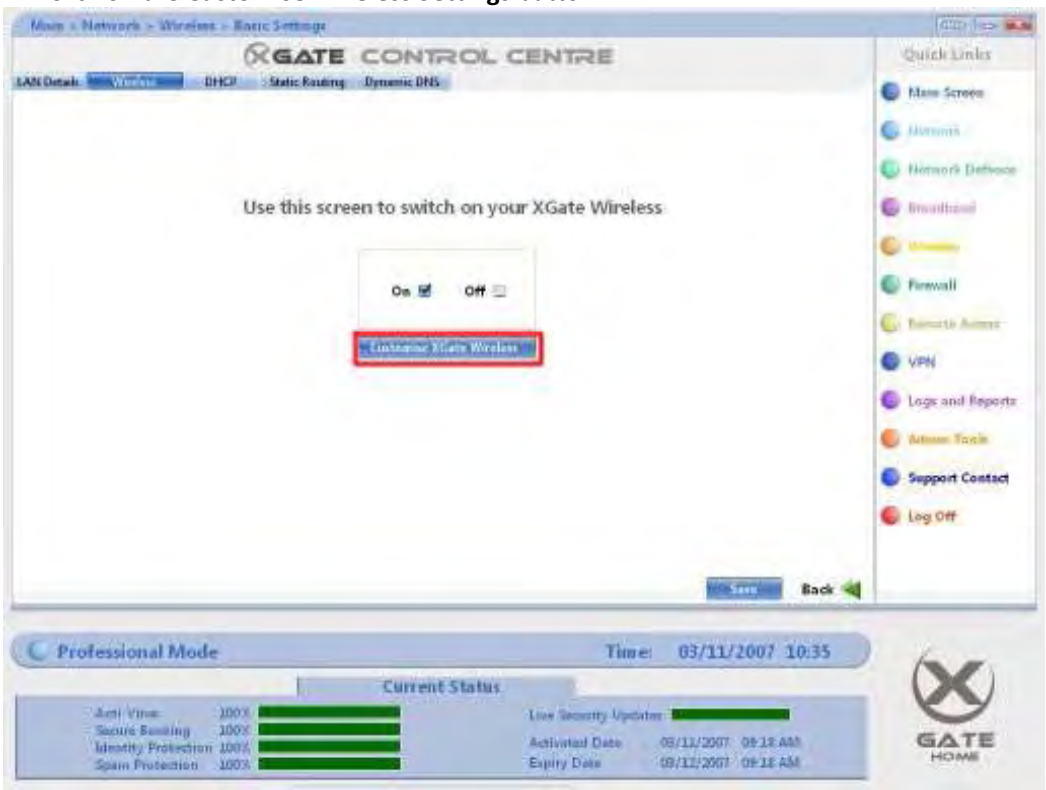
- Press the **Save** button.


**3. My Laptop does not detect the XGate Wireless Network. What could be the problem?**

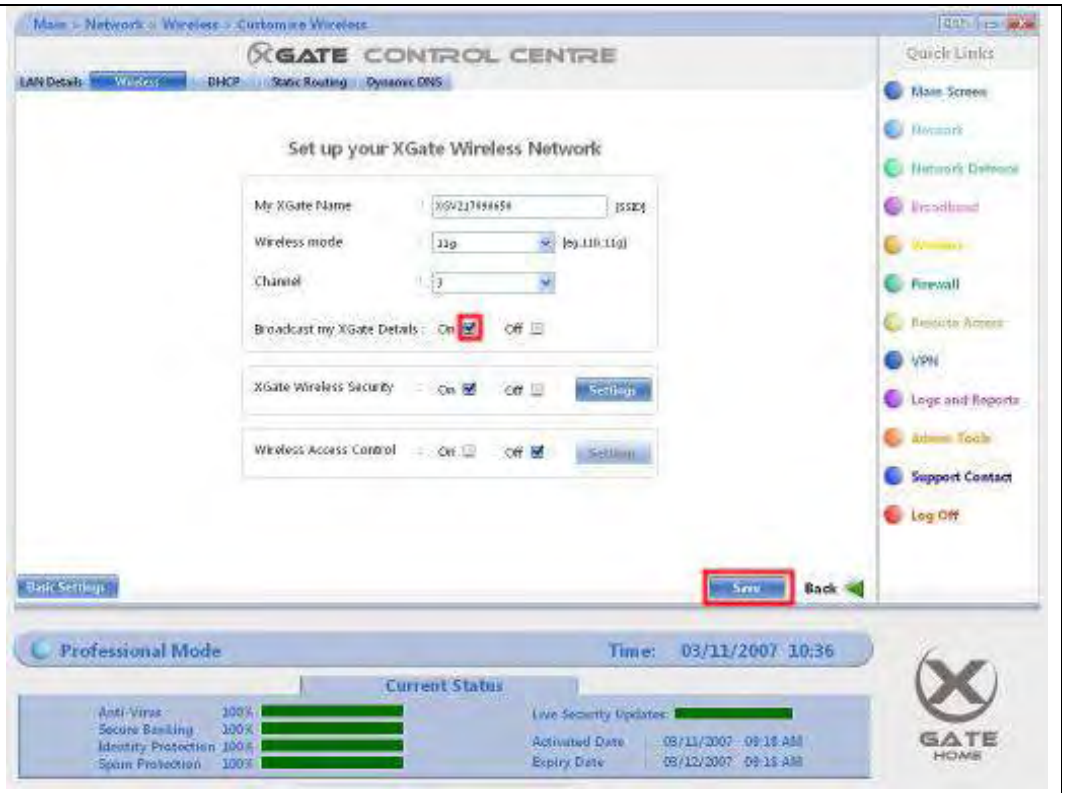
If your Laptop does not detect the XGate Wireless Network try any one of the following suggestions and try again.

1. Ensure that your Wireless Adapter is switched on. Check the side or front of your laptop for a switch.
2. Ensure that XGate wireless is switched on. On the main screen, click ***Wireless*** in the quick links section.
3. Ensure that the **Broadcast My XGate Details** Option in XGate Wireless Security is Switched ON. To do that, follow the procedure below:
    - On the main screen, click ***Wireless*** in the quick links section.


- Click on the **Customise Wireless Settings** button




- Select the **ON** checkbox corresponding to the **Broadcast My XGate Details.**
- Press the Save button**.**




4. Wireless Networks are always limited by their coverage distance. XGate can cover a range of 300 meters from the Device. Ensure that your Laptop is well within this range.

5. If you use a Wireless Adapter, please ensure that it is plugged-in properly in the slot.

**4. I have connected to the XGate Wireless LAN. However Browsing is very slow. What could be the problem?**

If you experience slow browsing when you connected via the Wireless Network, try any one of the following suggestions. It could improve the browsing speed.

1. XGate can support up to 300 meters radius range. Ensure that you locate yourself well within this range.
2. Poor signal strength may cause slow network traffic. Ensure that you get good signal strength. To know the signal strength, follow the steps below:
   - In your system tray, look for the following icon.
   - 

   - Right Click on the icon and select the ***View available Wireless Networks*** menu.
   - Windows will list the Wireless Networks in your Range.

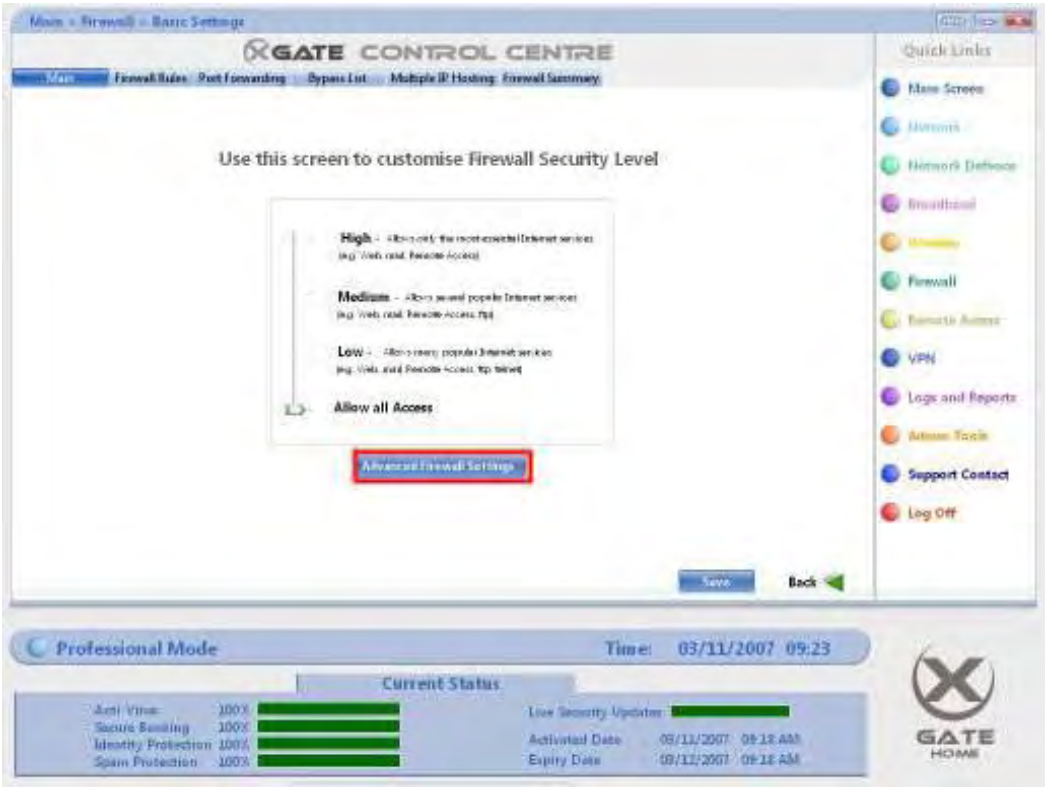

- Ensure that the XGate Wireless Network has the full signal strength. All the 5 green vertical bars indicate that the signal strength is good.

3. Ensure that thick concrete walls do not separate you from the XGate device. This could be a reason for a slow wireless network.
4. Ensure that any ***Radio Frequency*** devices (***Wireless Speakers, Microwave Owen, and Cordless Phones***) are not causing any interference with the XGate Device. You may relocate these devices and try again.
5. If you are not able to relocate the devices, you may change the XGate device's channel, which will reduce the chances of interference. To change the channel on which XGate works, please refer the **FAQ 5**.

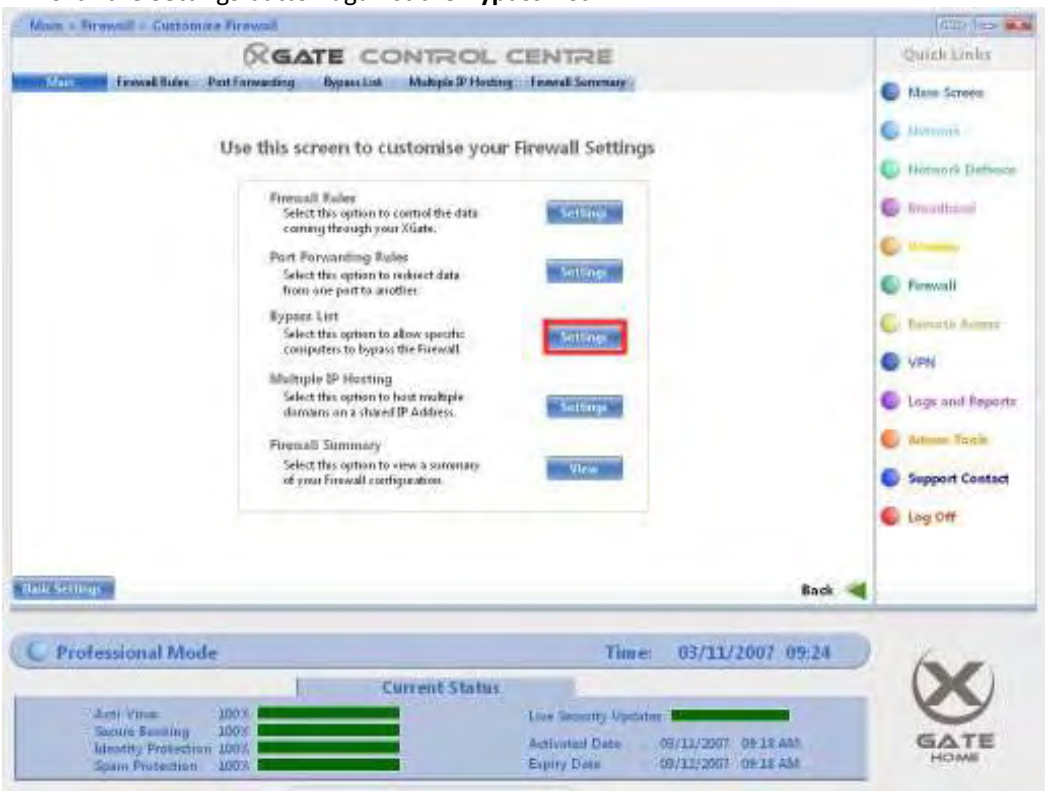
If none of the above solves your problem, you can resort to the following solution temporarily. However it is highly recommended not to use this option permanently.

- Click the **Firewall** Quick Link.

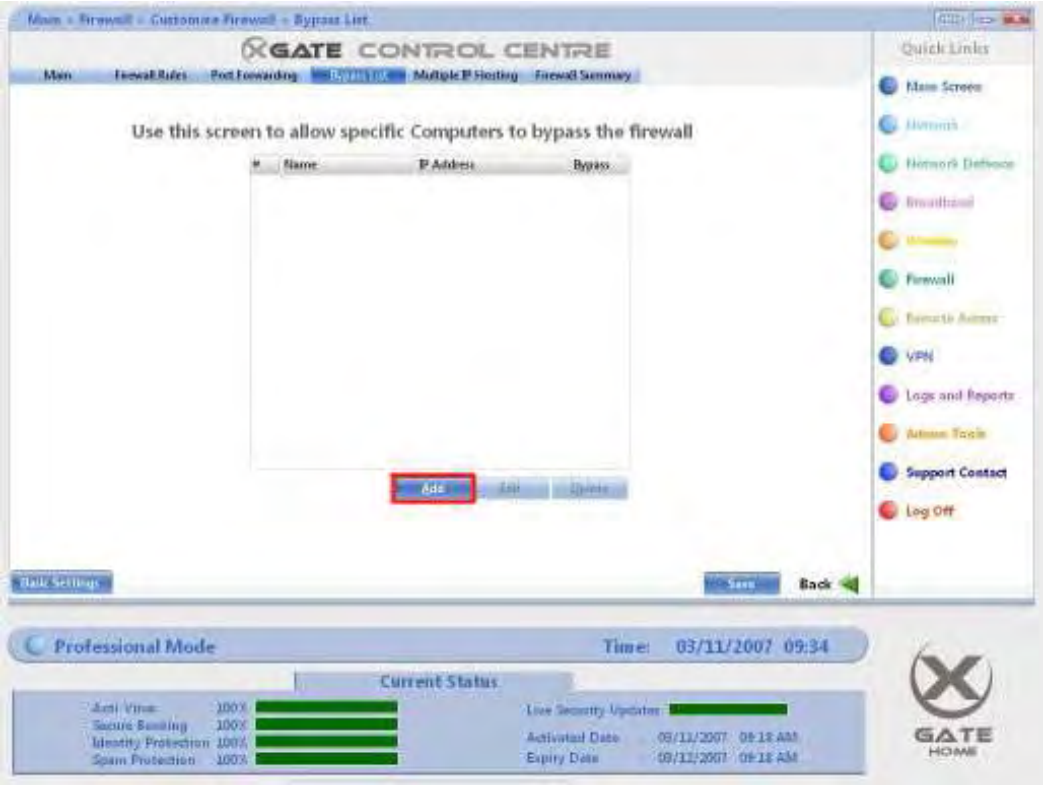

- Click the **Advanced Firewall Settings** button.




- Click the Settings button against the **Bypass List**




- Click the Add button.




- Enter a User Friendly name of the Computer in the **Computer Name** field.
- Enter the IP Address of the Computer in the **IP Address** field.
- Click the OK button to Save.


**5. My XGate Device interferes with other Radio Frequency devices in my place. How do I configure XGate to reduce the interference?**

Most equipment that use Radio Frequency for wireless communication use channel number 3 as their default channel. This could cause problems when they are operated simultaneously.

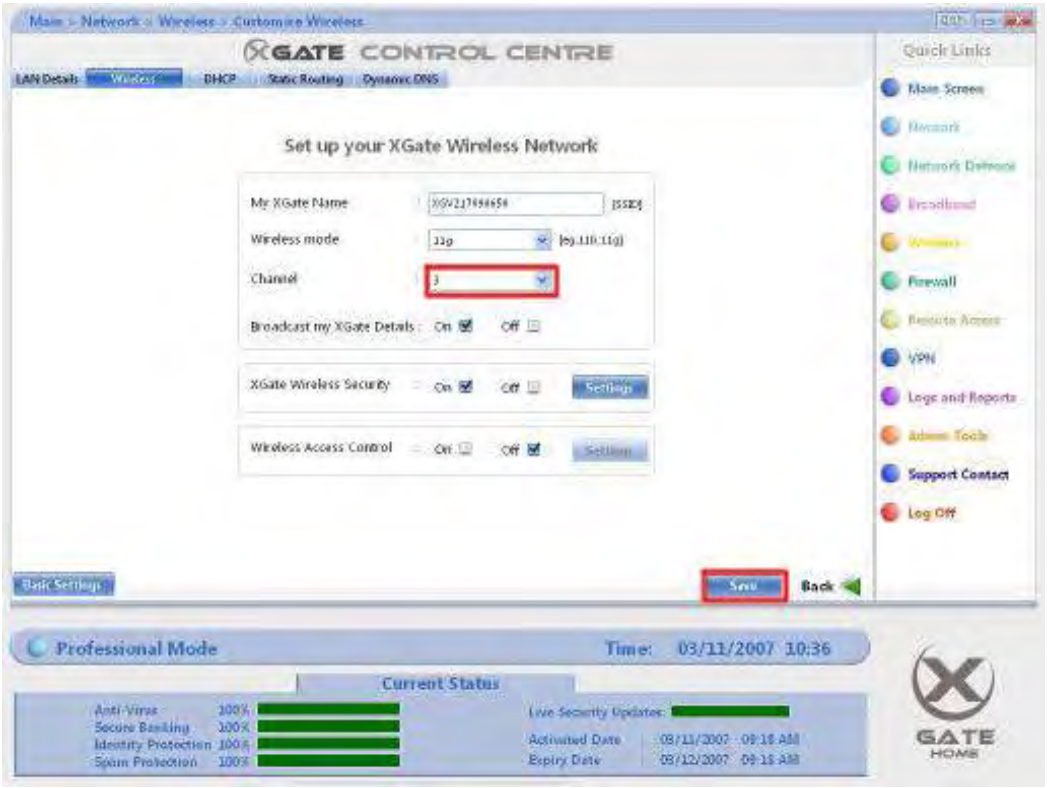
If your XGate device develops any issue with any other equipment near by, you can change the channel that XGate operates on. This can avoid interference with other devices.

To change the channel, follow the below steps:

- Click the **Wireless** Quick Link.


- Click the **Customise XGate Wireless** button.


- In the **Channel** field, select a desired channel from the drop-down.
- Press the **Save** button.

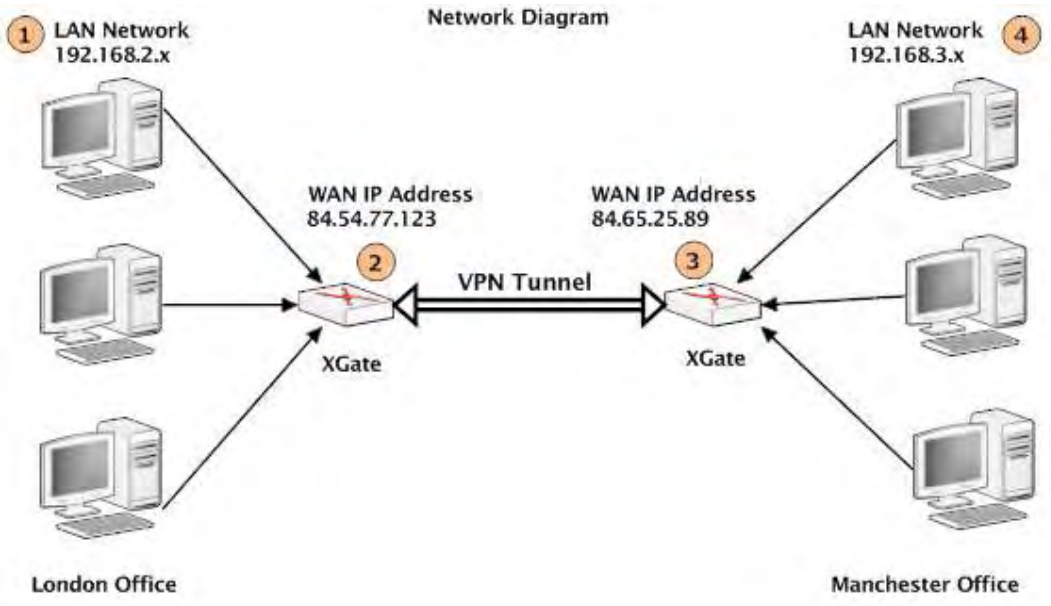

Main > Network > Wireless > Customize Wireless
XGATE CONTROL CENTRE
LAN Details
Wireless
DHCP
Static Routing
Dynamic DNS
Set up your XGate Wireless Network
My XGate Name
Wireless mode
11g
(b,g,11b,11g)
Channel
3
Broadcast my XGate Details :
On
Off
XGate Wireless Security
Settings
Wireless Access Control
Basic Settings
Save
Back
Quick Links
Main Screen
Network
Network Defence
Broadband
Wireless
Firewall
Remote Access
VPN
Logs and Reports
Admin Tools
Support Contact
Log Off
Professional Mode
Time: 03/11/2007 10:36
Current Status
Anti-Virus 100%
Secure Banking 100%
Identity Protection 100%
Spam Protection 100%
Live Security Updates:
Activated Date 08/11/2007 09:16 AM
Expiry Date 08/12/2007 09:16 AM
GATE
HOME

## VPN Troubleshooting

1. **How do I connect my Branch Office Networks using XGate VPN Service?**

> **Important Note**: The following procedure applies when you have a XGate Device at your head office and branch offices. For details on how to connect using other devices please read FAQ 3.

We will take a scenario where the head office is located in London and the Branch office is located in Manchester. The following diagram gives the necessary information to configure the VPN between the two offices.




These are the following details required to establish a VPN Connection:

| | London Office | Manchester Office |
|---|---|---|
| LAN Network | IP Address: 192.168.2.1<br>Subnet : 255.255.255.0<br>**Marked as 1** | IP Address: 192.168.3.1<br>Subnet: 255.255.255.0<br>**Marked as 4** |
| Public WAN IP Address | 84.54.77.123<br>**Marked as 2** | 84.65.25.89<br>**Marked as 3** |

To configure the VPN in the **London** office:

- On the Main screen, click VPN
- On the VPN Manager screen, click the **New Policy** Button.
- Enter the details below:

| Field | Value |
|---|---|
| Policy Name | Manchester |
| Policy Type | Site-to-Site |
| Remote IP Address | 84.65.25.89 |

| | |
|---|---|
| Remote Subnet | 192.168.3.1 / 255.255.255.0 |
| Pre-shared Key | connect-to-me (This is an example; you can have any other string as a shared secret.) |
| Encryption and Authentication Type | 3DES-MD5 |

- Press the **Save** button.
- The VPN Policy will be listed in the Define Policy section of the VPN Screen.
- Press the **Start** button.

Now configure the VPN Policy in the **Manchester** Office:

- On the Main screen, click VPN Server
- On the VPN Manager screen, click the **New Policy** Button.
- Enter the details below:

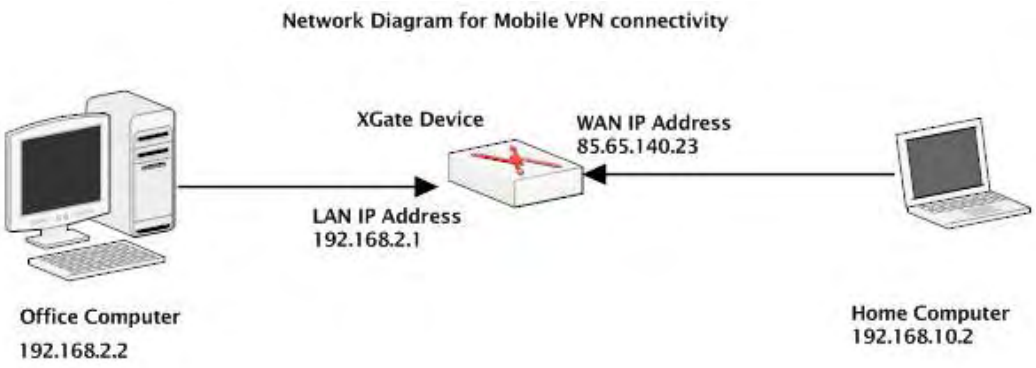
| Field | Value |
|---|---|
| Policy Name | London |
| Policy Type | Site-to-Site |
| Remote IP Address | 84.54.77.123 |
| Remote Subnet | 192.168.2.1 / 255.255.255.0 |
| Pre-shared Key | connect-to-me (This is an example; you can have any other string as a shared secret.) |
| Encryption and Authentication Type | 3DES-MD5 |

- Press the **Save** button.
- The VPN Policy will be listed in the Define Policy section of the VPN Screen.
- Press the Start button.

Now the VPN connection will be established between London office and the Manchester office.

2. **How do I connect to my office network when I am roaming with my Laptop?**

XGate VPN feature supports mobile VPN connections with the **XGate VPN Client Manager** software. This software is installed when the XGate Sensor is installed on your computer (Laptop). You can also use third-party Mobile VPN connectivity software like SafeNet VPN Client. However, the procedure described below is only for the XGate VPN Client Manager Software.




The first step in configuring Mobile VPN connectivity is to create Mobile User accounts. To configure the Mobile User Accounts (L2TP settings):

**A. Mobile User configuration (L2TP Settings)**

8. On the main screen, click VPN
9. Press the L2TP Settings tab.
10. In the Server IP Address field, enter 192.168.2.1.
11. In the Start IP Address Field, enter 192.168.2.4.
12. In the End IP Address Field, enter 192.168.2.5.
13. Click the **Add** button to open the User Accounts window.
14. In the User Name field, enter the name that will be used to identify you (e.g. Fred).
15. In the Password field, enter the password. (e.g. password).
16. Re-enter the password for confirmation.
17. Press OK to save.
18. Press the **Save** button.

This account will be used in the XGate VPN Client Manager software.

The second step is to create a Mobile VPN Policy.

**B. Create a Mobile VPN Policy**

1. On the main screen, click VPN
2. Click **New Policy** Button.
3. In the **Policy Name** field, enter a name that will be used to identify the VPN Connection (i.e. Fred Home VPN)
4. In the **Policy Type** field, select Mobile.
5. In the **Pre-shared Key** Field, enter 'connect-to-me'.
6. Press the **Save** button.

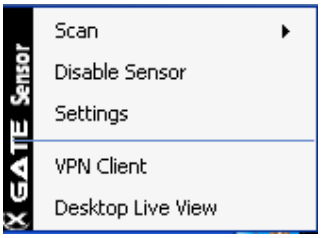
Now we are ready to access the Office network remotely from the Home computer.

**C. Connecting from the Home using the XGate VPN Client Manager.**

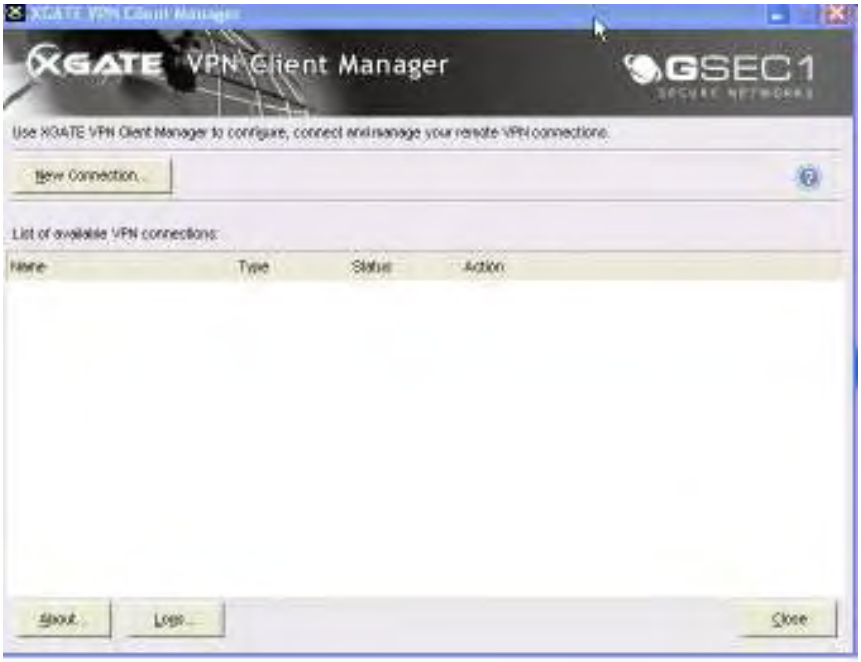
In your Home Computer:

1. Right-click on the XGate Sensor icon in the Task Bar.


2. In the context menu, select **VPN Client**.




3. XGate VPN Client manager application will be launched.




4. Click the **New Connection** button.


5. In the Connection Name field, enter **Mobile VPN**.
6. In the Connection type field, select L2TP/IPSEC.
7. In the Remote Host Name/ IP Address Field, enter the WAN IP Address of the XGate Device, i.e. 85.65.140.23 (Refer the illustration)
8. In the User Name field enter the user name entered in step A, i.e., 'Fred'
9. In the Password field enter the password entered in Step A, i.e., 'password'
10. In the Shared Secret field, enter the Shared Secret vale entered in Step B, i.e., 'connect-to-me'.
11. Click the OK button to save the changes.

The connection is added to the main screen. Under the **Action** column, click the **Connect** button. This will create the VPN connection between your computer and your office network

3. **My branch office does not have a XGate device. It has another vendor's device that supports VPN. Will I be able to connect my branch office using VPN?**
The XGate VPN Server is capable of connecting to various vendor's VPN devices. The example given below lists the steps necessary to connect the XGate device with a **NETGEAR ADSL Firewall Router DG834**.

**Important Note**: Please note that different devices may require slight changes and tunings in their configuration to make them work. Contact the user manual of the respective device

For example, we will take the same scenario described in FAQ 1.

The London office has a XGate device. The Manchester Office has a NETGEAR device.

To configure the XGate VPN in the **London** office:

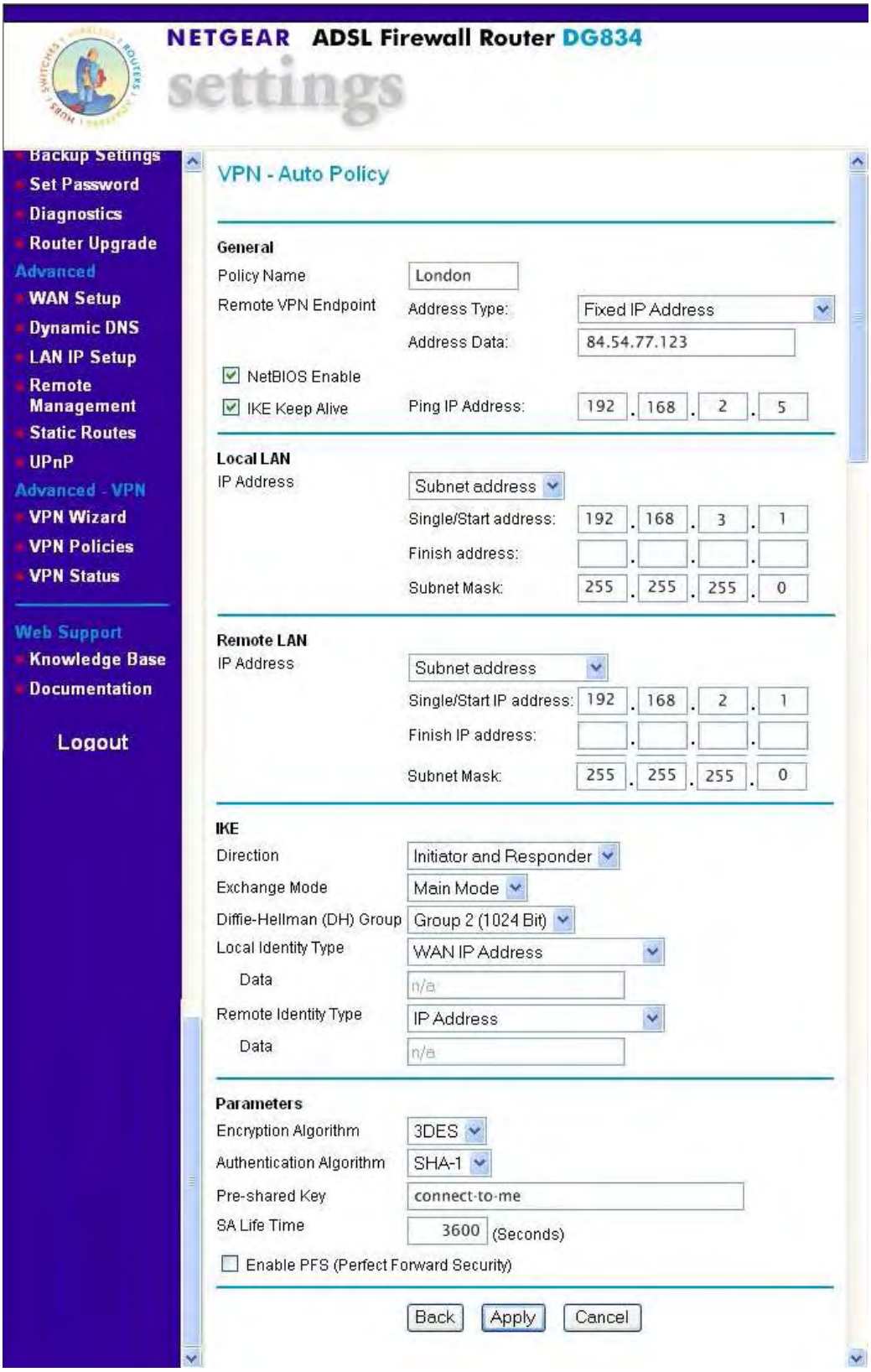
- On the main screen, click VPN
- Click **New Policy** Button.
- Use the following table to enter the details

| Field Name | Value |
|---|---|
| Policy Name | Manchester |
| Policy Type | Site-to-Site |
| Remote IP Address | 84.65.25.89 |
| Remote Subnet | 192.168.3.1 / 255.255.255.0 |
| Pre-Shared Key | connect-to-me (This is an example; you can have something else as the pre-shared key.) |
| Encryption and Authentication Type | 3DES-SHA1 |

- Press the **Save** button.
- The VPN Policy will be listed in the Define Policy section of the VPN Screen.
- Press the **Start** button.

To configure the NETGEAR VPN in the Manchester Office:

- Logon to the NETGEAR configuration pages using the browser.
- Select the Advanced – VPN > VPN Policies section.
- It should look like the screen below:




Use the details below to configure the Netgear:

| Section | Field Name | Value |
|---|---|---|

| | | |
|---|---|---|
| **General** | | |
| | Policy Name | London |
| | Address Type | Fixed IP Address |
| | Address Data | 84.54.77.123<br>(WAN IP Address assigned to the London Office XGate device) |
| | NetBIOS Enabled | Selected |
| | IKE Keep Alive | Selected |
| | Ping IP Address | 192.168.2.5<br>(This could be any computer's IP Address in the remote network) |
| **Local LAN** | | |
| | IP Address | Subnet Address<br>(Select from the Combo box) |
| | Single / Start Address | 192.168.3.1 |
| | Finish Address | Nil |
| | Subnet Mask | 255.255.255.0 |
| **Remote LAN** | | |
| | IP Address | Subnet Address<br>(Select from the Combo box) |
| | Single / Start Address | 192.168.2.1 |
| | Finish Address | Nil |
| | Subnet Mask | 255.255.255.0 |
| **IKE** | | |
| In this section, you need not change any of the default values. | | |
| **Parameters** | | |
| | Encryption Algorithm | 3DES |
| | Authentication Algorithm | SHA-1 |
| | Pre-Shared Key | Connect-to-me<br>(This is same as configured in the London Office) |
| | SA Life Time | 3600 |

After enter these settings, click the **Apply** button in the bottom. The VPN connection will be established. You can verify the status of the connection by selecting **VPN Status** on the left.