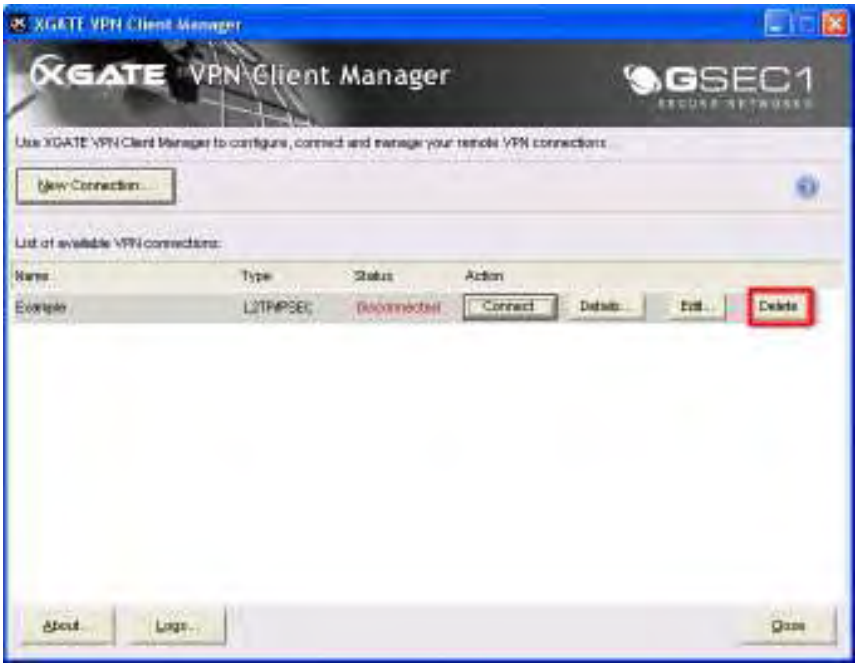
Removing a VPN Connection

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



When the VPN connection's Delete button is pressed, a pop-up window will appear where you must confirm your decision be pressing the Yes button.

This will remove the connection from the XGate VPN Client Manager.

Introduction

Broadband

Broadband is a general term for high-speed Internet access.

XGate supports 3 methods of Broadband Internet connection:

ADSL
If you use a telephone line to connect to the Internet then it is highly likely that you use ADSL.

Cable
If you use a cable modem given to you by a Cable provider, then you use a Cable Internet connection.

Existing Router
If you wish to continue using the features of a router that you already own, in conjunction with XGate.

Introduction

ADSL

What is ADSL?

ADSL is a type of Broadband DSL technology used mostly by home and small business users.

ADSL stands for Asymmetrical Digital Subscriber Line. It is known as asymmetrical because the download speed is significantly higher than the upload speed. As such, ADSL is not the ideal DSL technology for running servers from.

XGate supports 3 types of ADSL standards:

ADSL	-	up to 8Mbit/s download and 1Mbit/s upload speed
ADSL2	-	up to12Mbit/s download and 3.5Mbit/s upload speed
ADSL2+	-	up to 24Mbit/s download and 2.5Mbit/s upload speed

To find out which ADSL standard your Internet connection has, you will need to contact your broadband provider.

ADSL Connection Details

To setup an ADSL connection, the following details are required:

Connection Type
The ADSL standard that your Broadband Provider uses (ADSL, ADSL2, ADSL2+)

Username and Password
The Username and Password you use to connect to the Internet. Some ADSL connections do not require a Username and Password to gain a connection. In this case, tick the My Broadband Connection does not need a Username and Password option.

Country
The country you are connecting from.

Connecting to the Internet using ADSL

1) On the Quick Links menu, click Broadband.

2) Click ADSL Settings button.

3) Type in your Connection Details.
4) Ensure that Use XGate ADSL modem as default Internet Connection is ticked.
5) Press the Connect to Internet button.

Note: to change Connection Details, you will need to disconnect from the Internet.

Using Advanced ADSL Settings

To access the Advanced ADSL settings, click the Advanced Settings button on the ADSL screen.

If your ADSL Internet Connection requires specific settings, you should use the Advanced ADSL settings page. Your Broadband Provider will give you the relevant details needed to connect to the Internet if this is the case.

The following details make up the Advanced ADSL settings page:

Service Name
This is a friendly name to easily identify your Internet connection.

Authentication Type
This tells your ADSL modem which method of authentication you need to communicate with your Broadband Provider.

MRU/MTU
This is the size of the data that is being sent and received through your Internet connection.

Encapsulation Type
Determines the size of each segment that is sent.

VPI/VCI
Determines the route your Internet connection takes.

Internet IP Details

These are the details that your Broadband Provider needs to identify you and get you connected to their servers so you can access the Internet. If you do not have a static IP address, just leave it at the dynamic setting.

DNS Details
This is in the form of an IP address. It allows you to browse the Internet using domain names (i.e. XGate.com). It does this by associating IP addresses of websites with their domain names. If this is not correctly setup, you will have difficulty browsing the web.

Introduction

Cable

What is Cable?

Cable Internet access is often supplied by utilising a cable television infrastructure. As a result, it is often packaged with cable television and phone services.

Cable Connection Details

The following details are required to gain Cable Internet Access:

Automatically get my Connection Details
This option should be ticked if your Cable Provider automatically assigns you an IP Address when you connect to the Internet. This is the most common way to connect to a Cable Internet service

IP Address
This is the address that your cable provider assigns to you so you can be identified and connect to their servers to access the Internet.

Subnet Mask
In general computer networking, this is used to divide networks. In the majority of networks, this should be set to 255.255.255.0.

Gateway
This is the IP Address of the cable provider's server that you wish to connect to

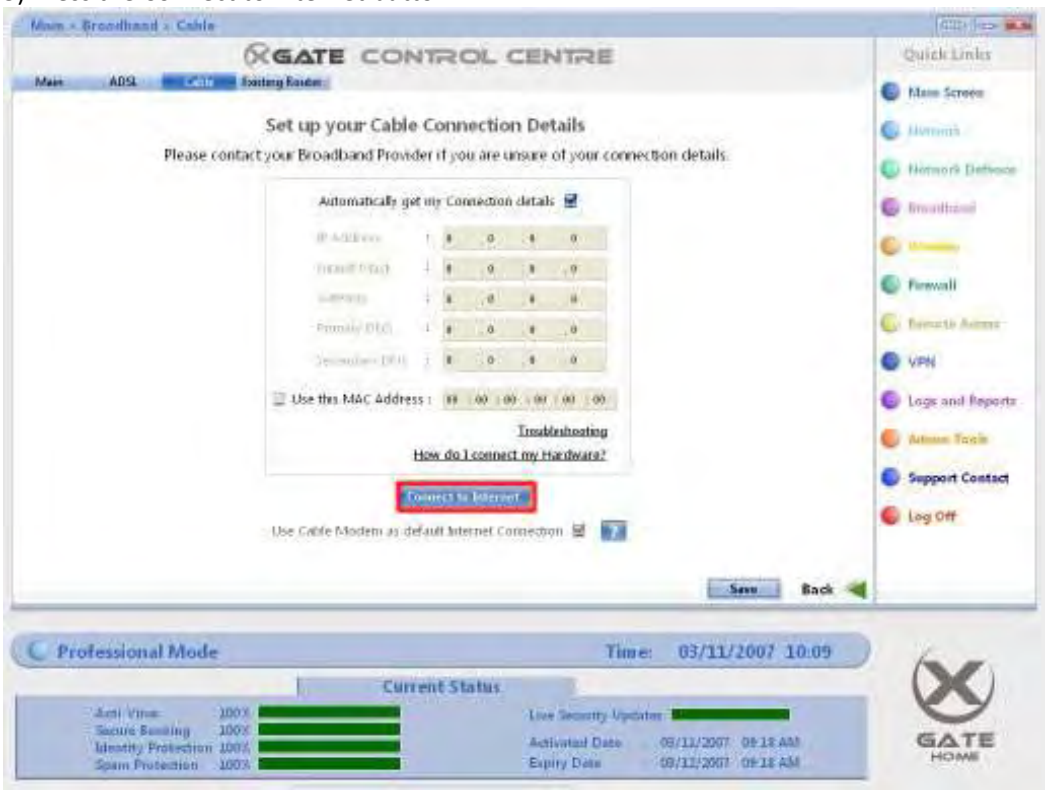
DNS
These are the DNS servers that will allow you to use domain names to browse the web.

Connecting to the Internet using Cable

1) On the Quick Links menu, click Broadband.

2) Click Cable Settings button.

3) Type in your Connection Details.
4) Ensure that Use Cable Modem as default Internet Connection is ticked.
5) Press the Connect to Internet button.



Note: to change Connection Details, you will need to disconnect from the Internet.

Introduction

Existing Router

What is an Existing Router?

It is most likely that the device you previously used to connect to the Internet was a router. Routers differ from standalone modems by connecting networks (typically LAN) together to access the Internet (Via the WAN or ADSL).

Use the Existing Router option if you wish to continue using the features of the router you already own, in conjunction with XGate.

Existing Router Connection Details

The following details are required for Existing Router details:

Automatically get my Connection Details
If your existing router has DHCP enabled, this should be ticked.

IP Address
The IP address of your XGate device.

Subnet Mask
In general computer networking, this is used to divide networks. In the majority of networks, this should be set to 255.255.255.0.

Gateway
This is the IP address of your existing router.

DNS
This points to the device that will allow you to use domain names to browse the web. In most cases, this can be the IP address of your existing router.

Connecting to the Internet using an Existing Router

1) On the Quick Links menu, click Broadband.

2) Click Cable Settings button.

3) Type in your Connection Details.
4) Ensure that Use Existing Router as default Internet Connection is ticked.
5) Press the Connect to Internet button.

Note: to change Connection Details, you will need to disconnect from the Internet.

Introduction

Network

What is a Network?

A computer network consists of two or more computers connected together so they can share data and resources with each other.

Analogy

You can think of computers on a network as houses on a street. Each house has a number to identify it and the same goes for computers. Each computer must be given its own address, which is known as an IP address.

Network Features

From the Network section is where you can set up and view information relevant to your Local Network (LAN).

Within Network you can setup your:

LAN Details
From here it is possible to change the LAN IP Address of your XGate device.

Wireless
Use this to set up and secure your wireless network.

DHCP
Change the range of IP addresses that XGate will distribute to computers on your network.

Static Routing
This is an XGate Pro only feature. This allows network traffic to be directed along a specific path.

Dynamic DNS
Allows you to associate a domain name to the external IP Address of your XGate device. If XGate's external IP address changes then the mapping of the domain name will be updated.

Introduction

LAN Details

What are LAN Details?

From the LAN Details screen, it is possible to set the LAN IP Address details of your XGate device.

Analogy

A standard address comprises of several parts (Name, Street, County/State, Country, Post Code). These parts of an address describe the location and its hierachy. For example, many counties/states make up a country. Similarly, the numbers of an IP Address also describe the hierachy of the network.

In standard addresses, we use commas and new lines to separate each part of relevant data. In IP Addresses dots / full stops are used. Each set of numbers define the address more specifically in contrast to how a normal address would start of very specific (Street) and get more broad with each new section (County/State then Country).

LAN Details

The LAN Details screen is comprised of 3 parts:

LAN IP:	The LAN IP Address of the XGate LAN ports.
Subnet Mask:	The Subnet Mask of the XGate LAN ports
Domain Name:	The Domain Name associated with the XGate LAN IP.

Changing the XGate LAN Details

1) On the Quick Links Menu, click Network.

2) On the LAN Details screen, press the Edit button.

3) Once you have changed the LAN Details to your satisfaction, press the Save button to confirm your changes.

Introduction

Wireless

What is Wireless?

A Wireless Network uses radio waves to communicate information between computers that are not physically connected by wires.

While wireless networks are convenient, they are also a weak link in your network security. It is important to set a good level of security to keep your network protected, as poor wireless security can leave your network open to abuse.

Wireless Details

The XGate Wireless screen shows the following:

My XGate Name (SSID):
This is the name of your XGate Wireless Network.

Wireless Mode:
The method used to transport data wireless. This will also determine the speed of your Wireless Network. Please check the documentation supplied with your wireless adapter to find out which wireless modes are supported.

Channel:
This is the frequency of your wireless network. Change this if you are experiencing interference with other wireless devices.

Broadcast my XGate Details:
When this is switched off, XGate's name (SSID) will not appear when wireless networks are searched for.

XGate Wireless Security:
If this is switched off then your Wireless Network will have no Security (not recommended).

Wireless Access Control:
Once switched on, only computers listed within Wireless Access Control will be able to access the XGate Wireless Network.

Changing my Wireless Network Settings

1) In the Quick Links Menu, click Wireless.

2) Ensure that XGate Wireless is switched on.
3) Press the Customise XGate Wireless button.

4) Amend your Wireless Details.
5) Press the Save button.

Introduction

Wireless Security

What is Wireless Security?

Wireless Security is achieved by using cipher suites to encrypt data before it is sent. This ensures that data can only be decrypted by a computer using the same encryption method and Wireless Network Key.

Analogy

Wireless Security is where you specify your Wireless authentication key which you will use to access your wireless network and prevent others from accessing your network without your permission. The Wireless Authentication Key can be compared to a password or the PIN number you use to access your bank account.

Wireless Security Details

Within XGate Wireless Security, there are 3 Security modes:

WEP

Despite being the oldest and least secure method of wireless security, WEP is also compatible with the widest range of wireless devices. WEP only accepts wireless keys using hexadecimal characters (0-9 and A-F) . It is not advisable to use WEP if your wireless adapter supports higher security standards.

WPA

WPA offers a greater level of Wireless Security than WEP by incorporating TKIP encryption. This added security makes it much more secure than WEP.

WPA2

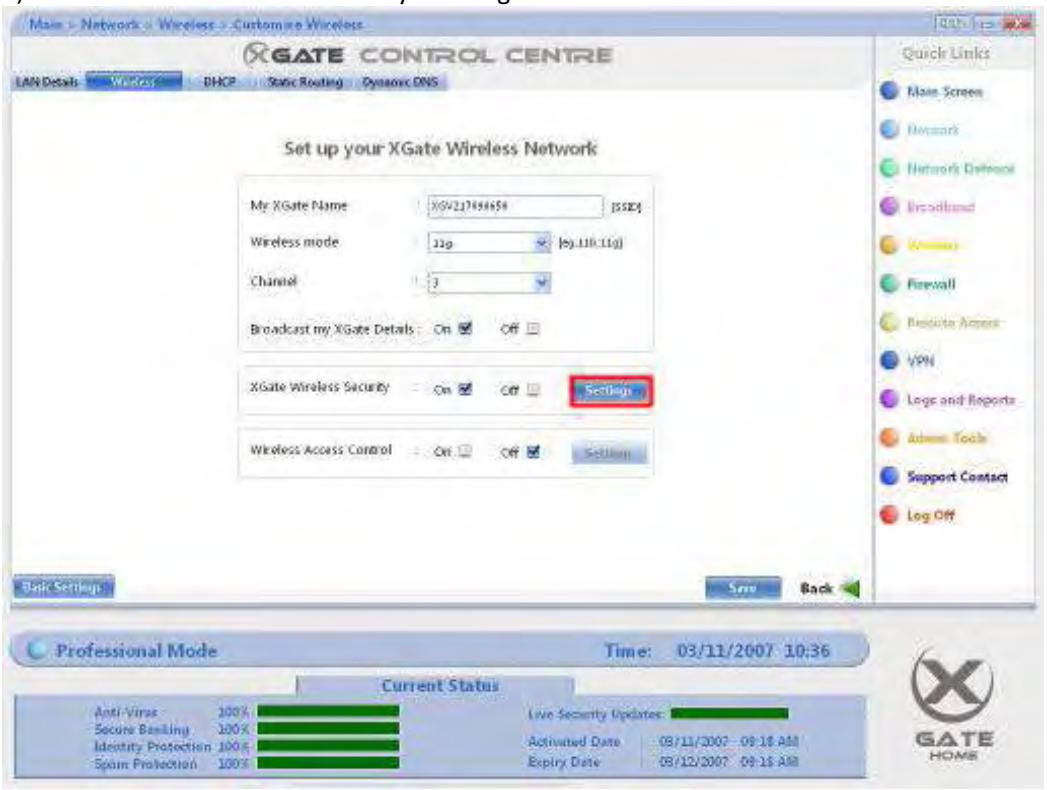
This is the most up to date form of wireless security available in XGate and is an evolution of WPA, as the name suggests. WPA2 is more secure than WPA since it offers a 3-way encryption method. However, since it is the newest, only relatively modern wireless devices are compatible with it. Your wireless adapter will support WAP2 if it was made after March 2006 as it became mandatory to include WPA2 to be Wi-Fi certified after that date.

Changing my Wireless Security Settings

1) In the Quick Links Menu, click Wireless.

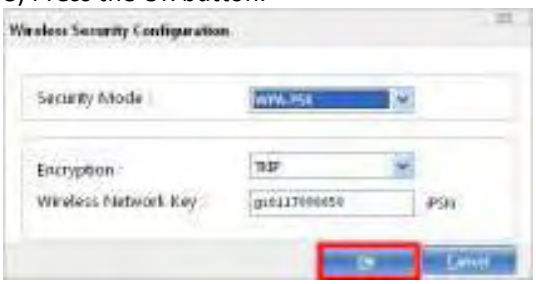
2) Ensure that XGate Wireless is switched on.
3) Press the Customise XGate Wireless button.

4) Ensure that XGate Wireless Security is switched on.
5) Press the XGate Wireless Security - Settings button.

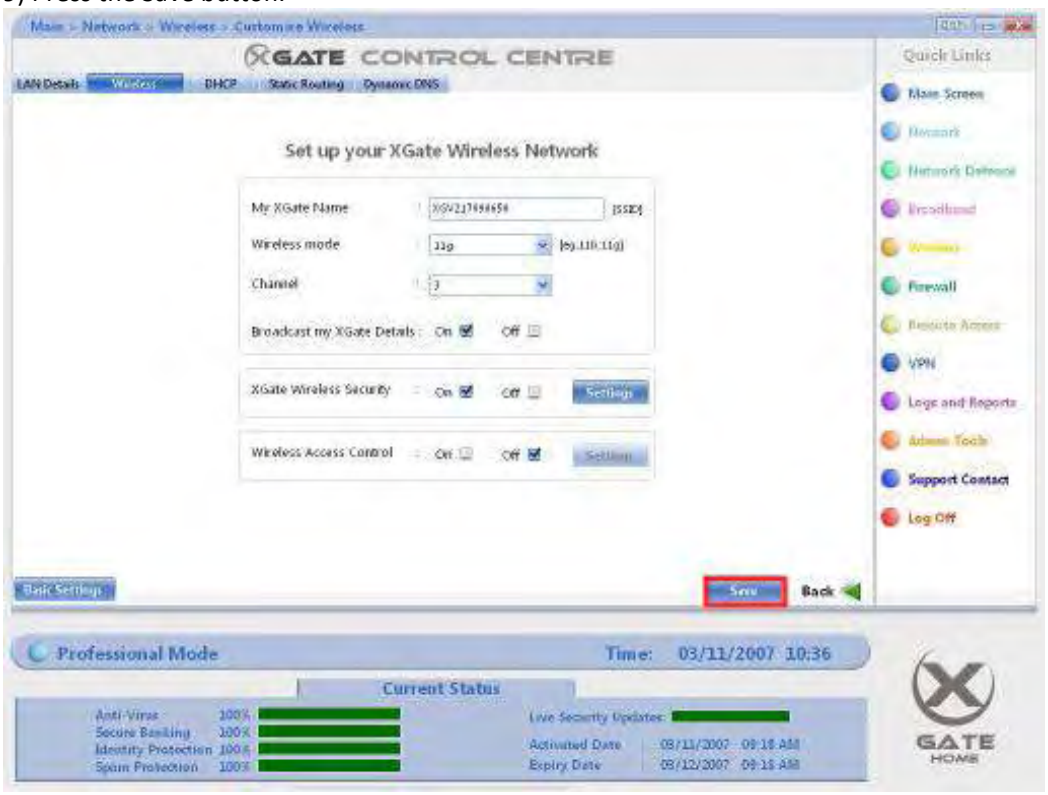


6) Select your Security mode from the Drop Down box.

7) Type in your Wireless Network Key.
8) Press the OK button.



9) Press the Save button.



Introduction

Wireless Access Control

What is Wireless Access Control

Wireless Access Control allows you to further increase your wireless security. By listing your networked computers' MAC Addresses (the computer's unique identifier), XGate will only allow those listed computers access to the Wireless Network.

Analogy

Wireless Access Control is like a guest list to a party. The doormen (The Wireless Access Control module) have a list of names (MAC Addresses) that are allowed into the party (Wireless Network). If the name of the person (the MAC of the computer that is trying to access the network) does not match a name on the doormen's list, they will not be allowed to participate at the party.

How to find your MAC Address

You can find out your computer's MAC address by:
1) Pressing the Start button (or Windows Orb in Vista) in Windows.
2) Pressing Run.
3) Type in "cmd" and press OK (without the quotes).
4) Type in "ipconfig /all" (without the quotes) and press Enter.
5) The MAC Address will be listed as the Physical Address.

Wireless Access Control Details

An entry in the Trusted Wireless Computers list consists of:

Computer Name: A friendly name that will allow you to easily identify your computer.
MAC Address: The computer's unique identifier.

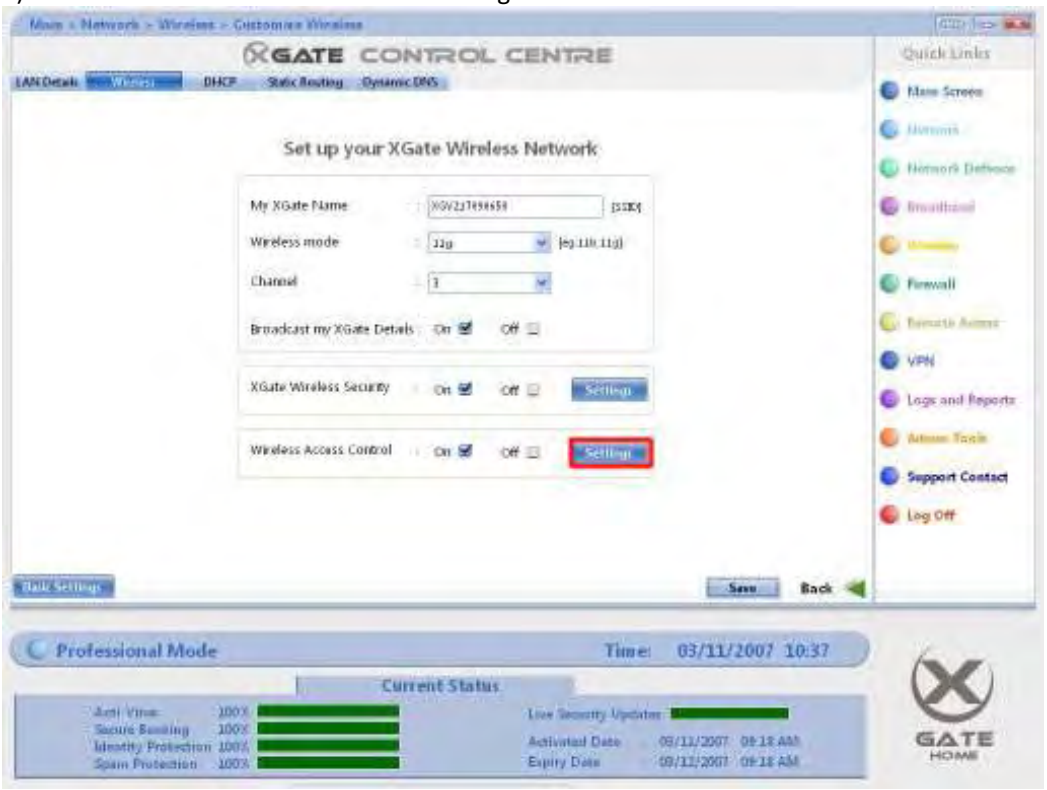
Please note
When you switch on Wireless Access Control, no computers other than the ones listed will be able to connect to the XGate Wireless Network.

Adding to the Trusted Wireless Computers List

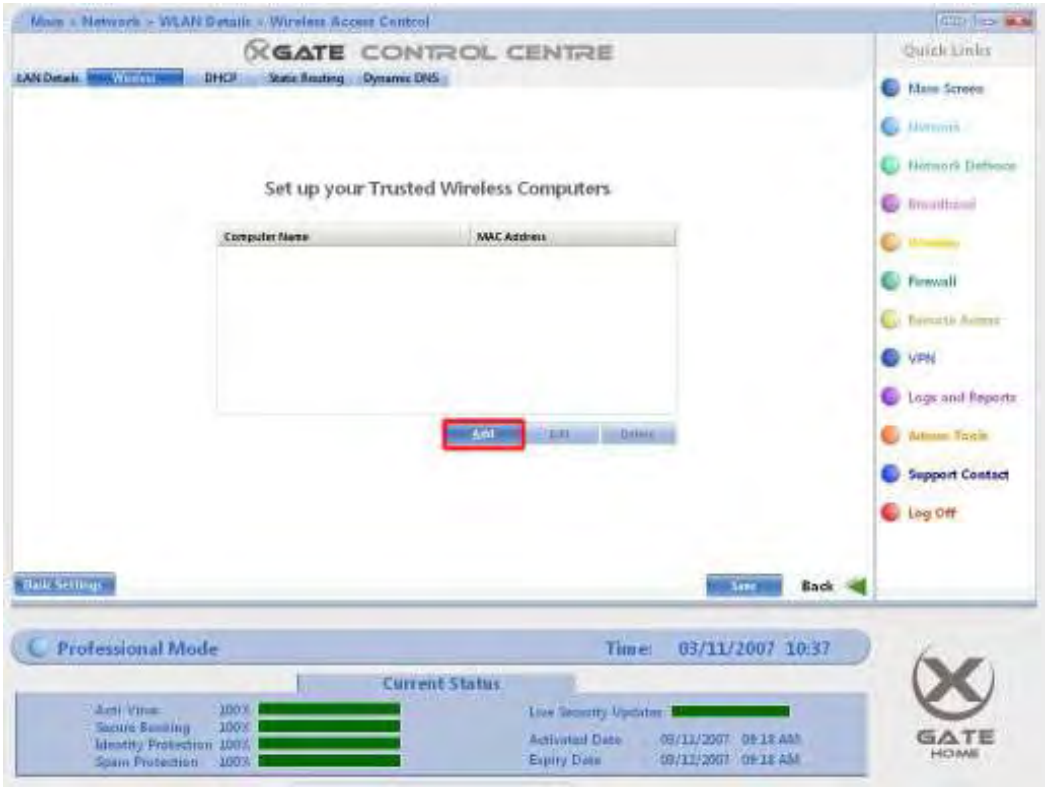
1) In the Quick Links Menu, click Wireless.

2) Ensure that XGate Wireless is switched on.
3) Press the Customise XGate Wireless button.

4) Ensure that Wireless Access Control is switched on.
5) Press the Wireless Access Control - Settings button.

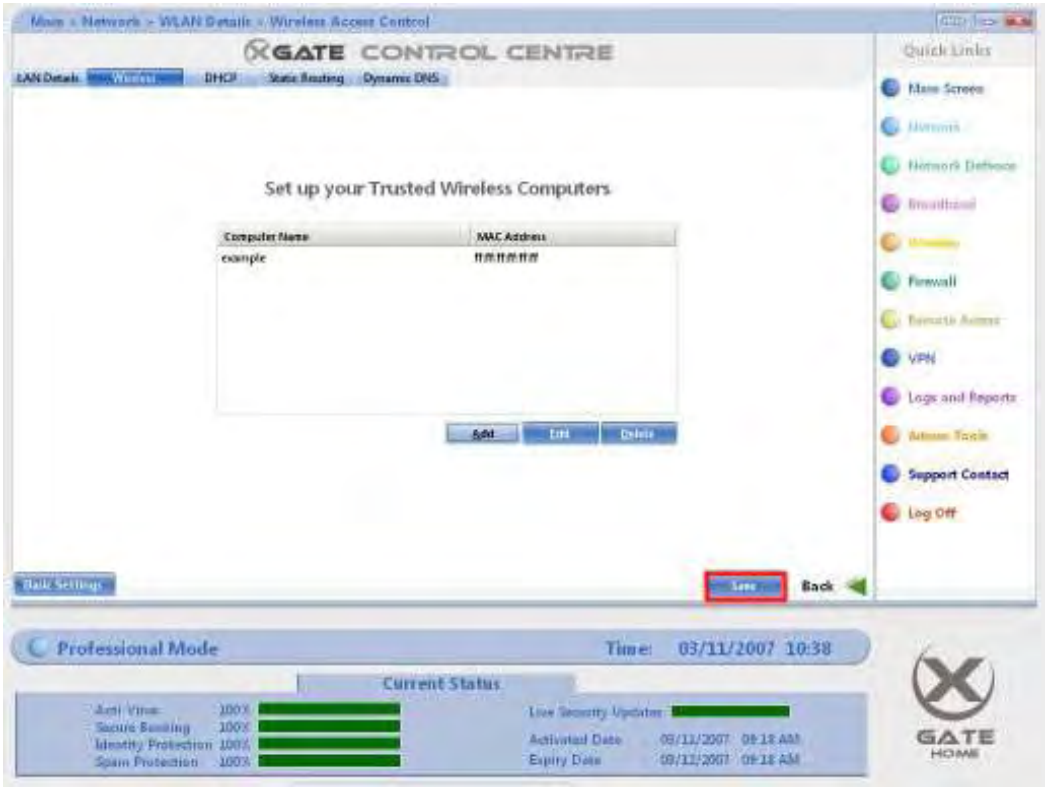


6) Press the Add button.



7) Enter the Computer Name and MAC Address
8) Press the OK button.

9) Press Save to confirm your changes.

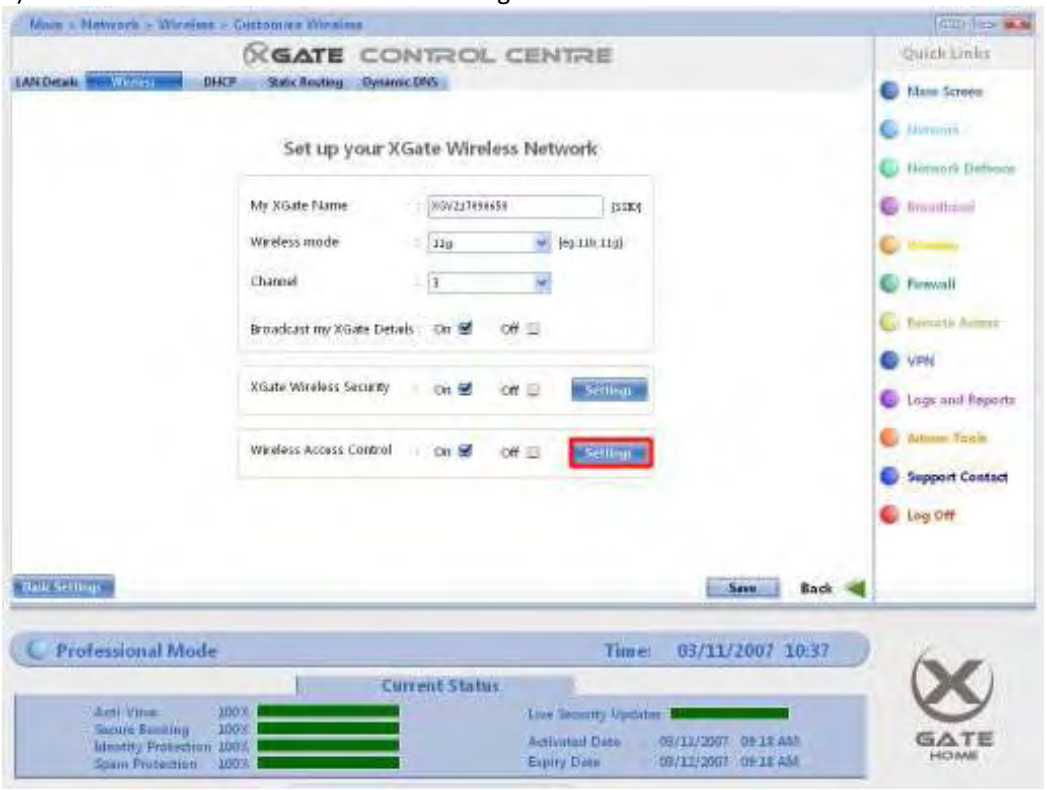

GATE CONTROL CENTRE
Quick Links
Main Screen
Firewall
VPN
Logs and Reports
Support Contact
Log Off
Set up your Trusted Wireless Computers
Computer Name
MAC Address
example
Add
Edit
Delete
Back
Professional Mode
Time: 03/11/2007 10:38
Current Status
Anti Virus 100%
Secure Banking 100%
Identity Protection 100%
Spam Protection 100%
Activated Date 03/11/2007 09:18 AM
Expiry Date 03/11/2007 09:18 AM
GATE
HOME

Changing an entry in the Trusted Wireless Computers list

1) In the Quick Links Menu, click Wireless.

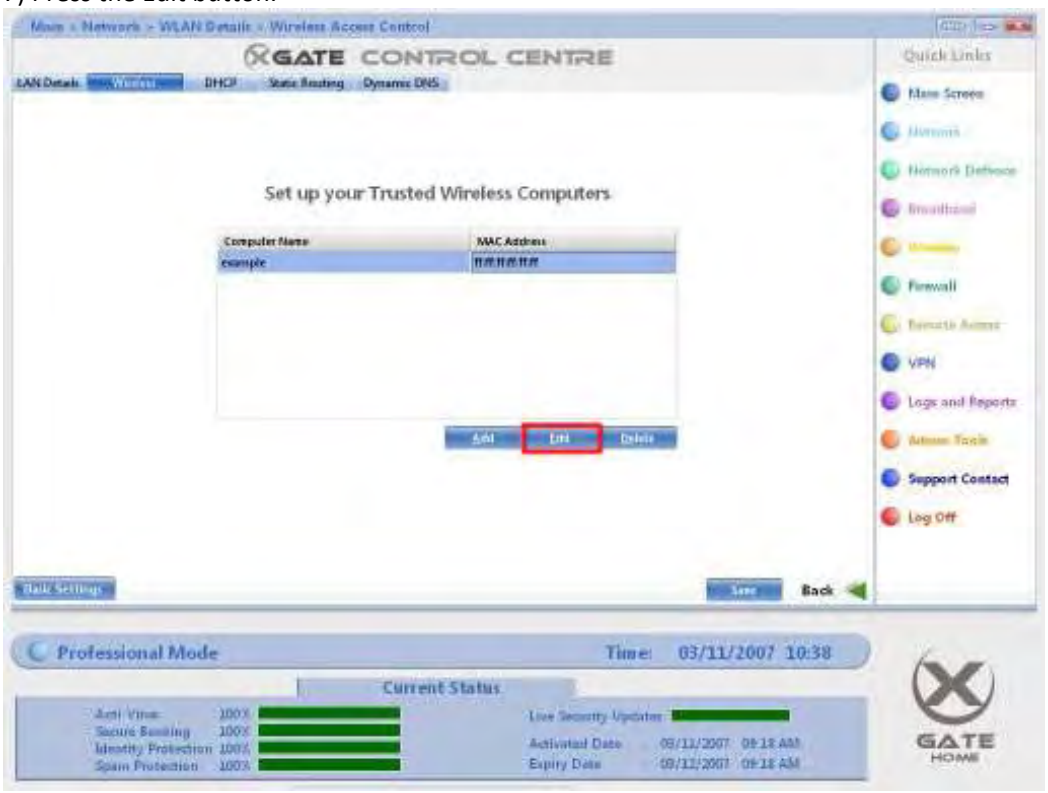
2) Ensure that XGate Wireless is switched on.
3) Press the Customise XGate Wireless button.

4) Ensure that Wireless Access Control is switched on.
5) Press the Wireless Access Control - Settings button.



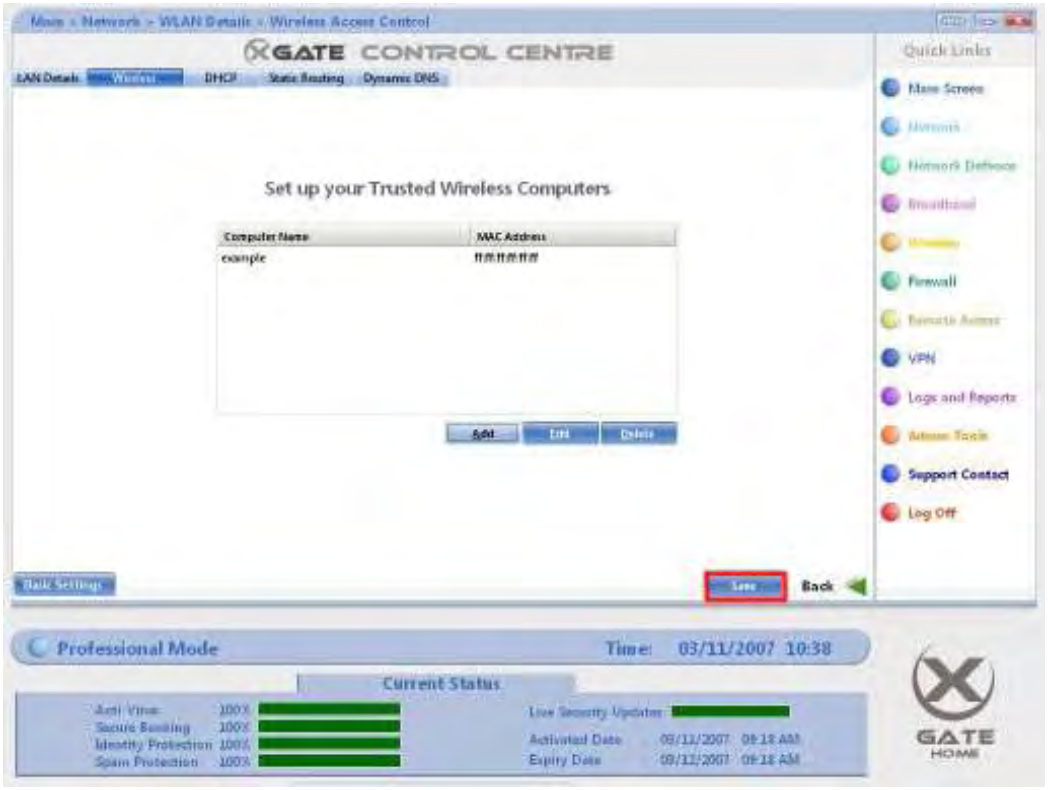
6) Select an entry by clicking it in the Trusted Wireless Computers table. This will highlight

the entry.
7) Press the Edit button.



8) Make the changes you wish to the Computer Name or MAC address
9) Press the OK button.

10) Press the Save button to confirm your changes.

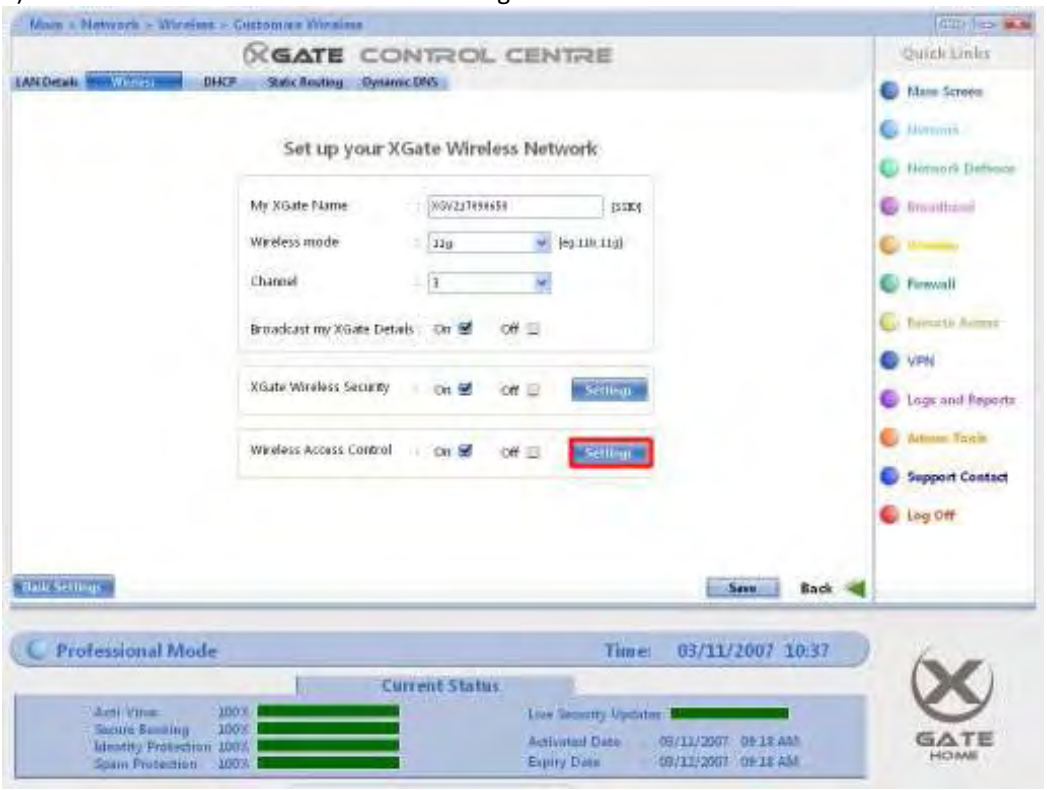

GATE CONTROL CENTRE
Quick Links
Main Screen
Firewall
VPN
Logs and Reports
Support Contact
Log Off
Set up your Trusted Wireless Computers
Computer Name
MAC Address
example
Add
Edit
Delete
Back
Professional Mode
Time: 03/11/2007 10:38
Current Status
Anti Virus 100%
Secure Banking 100%
Identity Protection 100%
Spam Protection 100%
Activated Date 03/11/2007 09:18 AM
Expiry Date 03/11/2007 09:18 AM
GATE
HOME

Removing an entry in the Trusted Wireless Computers list

1) In the Quick Links Menu, click Wireless.

2) Ensure that XGate Wireless is switched on.
3) Press the Customise XGate Wireless button.

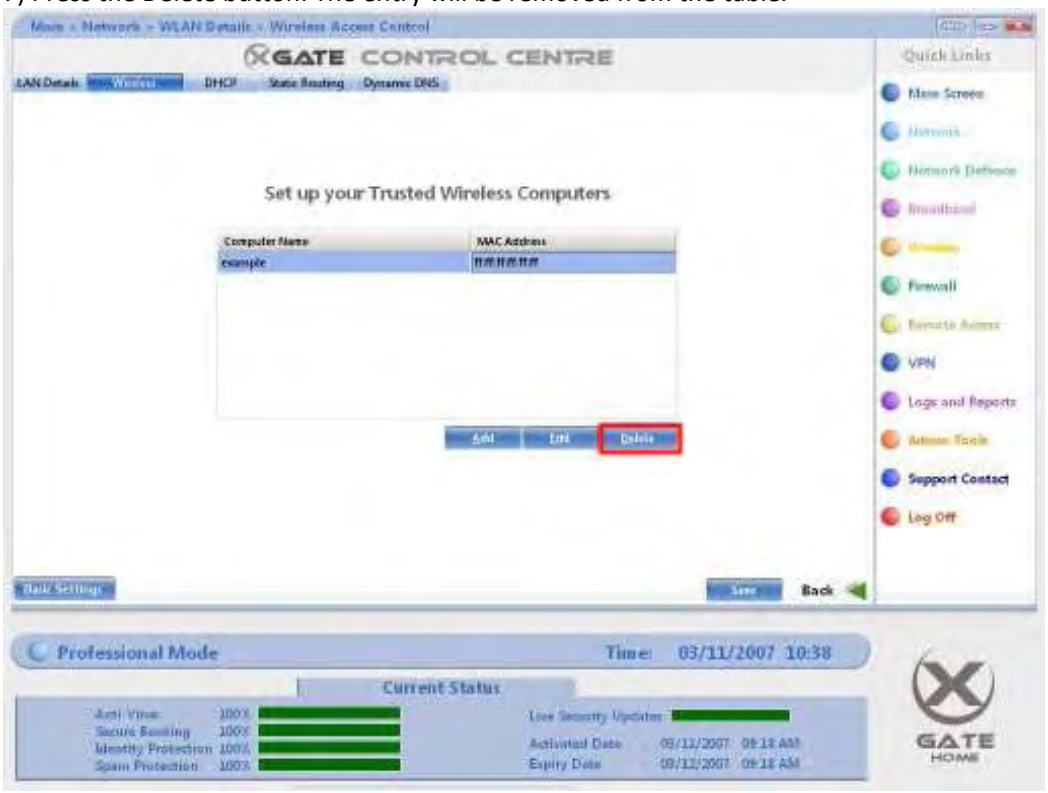
4) Ensure that Wireless Access Control is switched on.
5) Press the Wireless Access Control - Settings button.



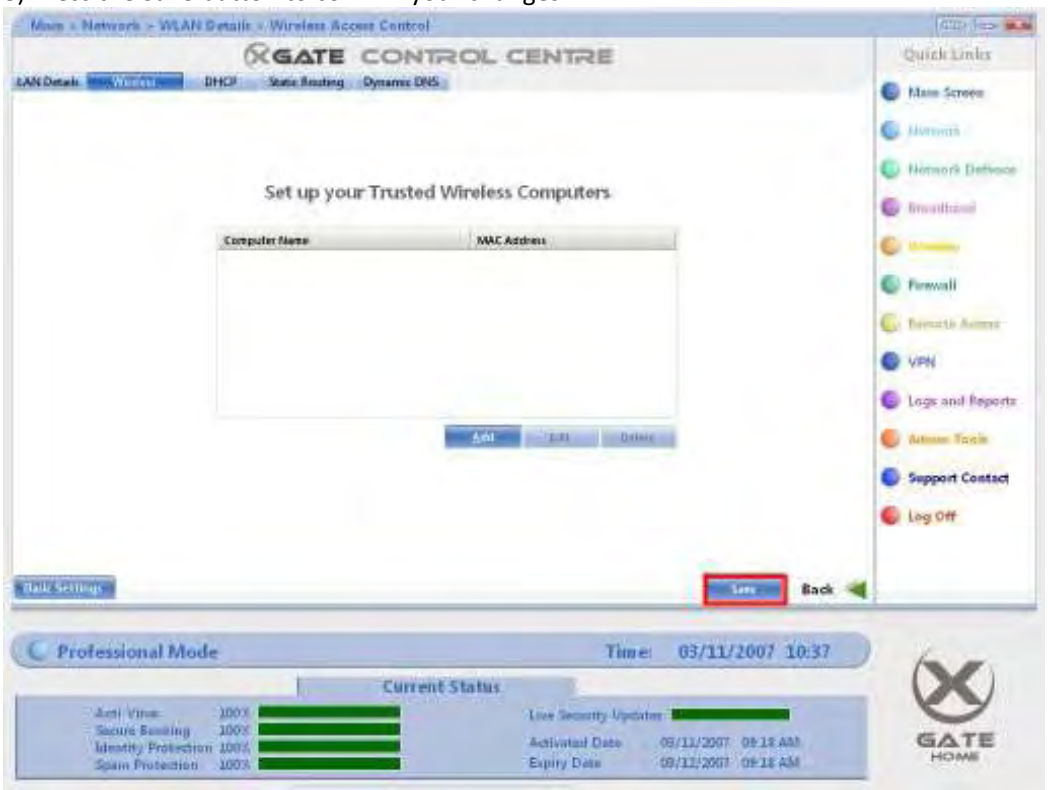
6) Select an entry by clicking it in the Trusted Wireless Computers table. This will highlight

the entry.

7) Press the Delete button. The entry will be removed from the table.



8) Press the Save button to confirm your changes.



Introduction

DHCP Server

What is a DHCP Server?

A DHCP server automates the assignment of IP Addresses and other IP details. The DHCP server holds a bank of IP Addresses. When a computer requests an IP Address, it will assign the computer one from its bank. The DHCP server ensures that each IP Address in use on the network is unique.

Analogy

Obtaining an IP Address from a DHCP server is similar to renting a hotel room. To rent a room (IP address) you must first decide how long you wish to initially stay for. Once a room has been assigned, you can stay there for the entire period of the lease. If you wish to continue living at the house, you can renew before the contract/lease ends. If the owner of the hotel (DHCP Server) rents the room to another person (computer), then they will provide another room for you. If you decide to leave, before your stay expires.

DHCP Server Details

The DHCP Server settings are as follows:
IP Address Range (Start and End IP Address)
This is the range of IP addresses assigned to the DHCP server to be allocated to devices on your network.

IP Address Leases
Lease duration
The lease duration specifies how long the DHCP lease lasts for before it will be renewed. Can be set to expire after 1 to 365 days.

Maximum Number of Leases
This is the maximum number of IP Addresses that the DHCP server will assign at one time.

Changing your DHCP server details

1) In the Quick Links menu, click Network.

2) Press the DHCP tab.

3) Ensure that the DHCP server is switched on.
4) Press the Customise DHCP server button.

5) Change the DHCP details

6)Press the Save button to confirm your changes.

Introduction

DHCP Static Address Reservations

What is a DHCP Static Address Reservation?

Static Address Reservations ensure that a specific computer will always receive the same IP address. This can be useful when using the Firewall or Static Routing in conjunction with the DHCP server.

Analogy

If you were renting a hotel room, DHCP Static Address Reservations would be akin to signing a contract, to ensure that you can rent the same room indefinitely.

Note

Due to the inherent nature of Static Address Reservations, the MAC Address of the computer and the desired IP Address must be specified.

To read more about how to find your computer's MAC address, please refer to the General Troubleshooting section .

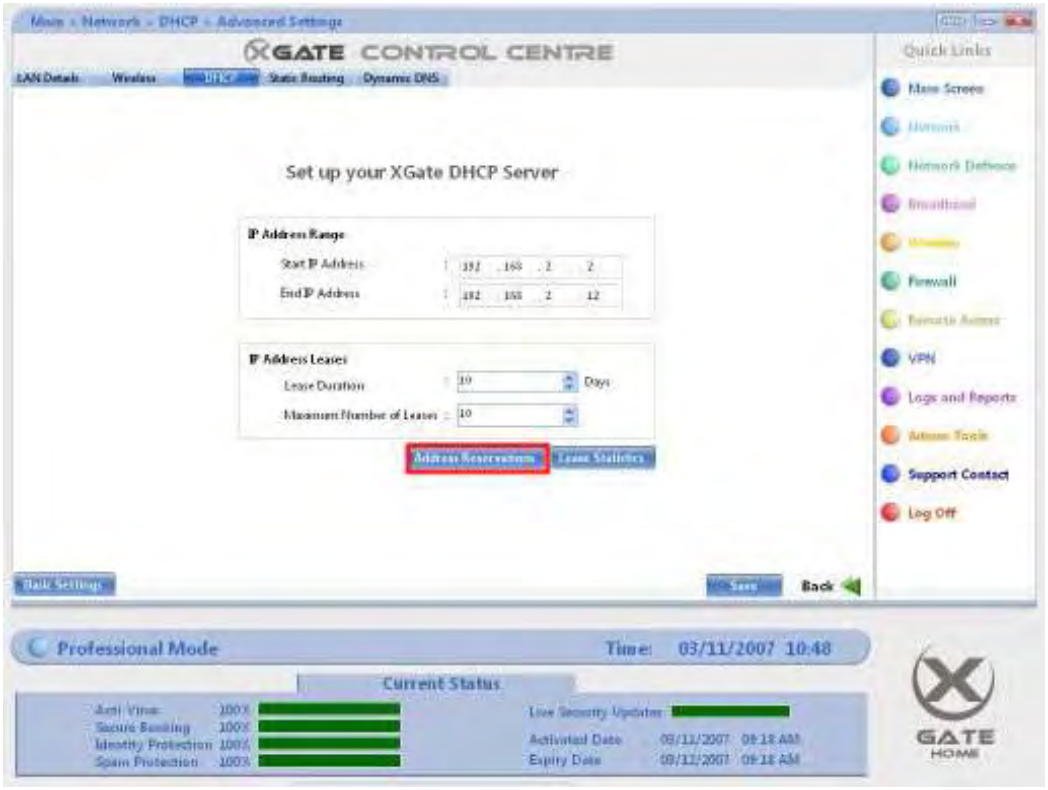
Adding a Static Address reservation

1) In the Quick Links menu, click Network.

2) Press the DHCP tab.

3) Ensure that the DHCP server is switched on.
4) Press the Customise DHCP server button.

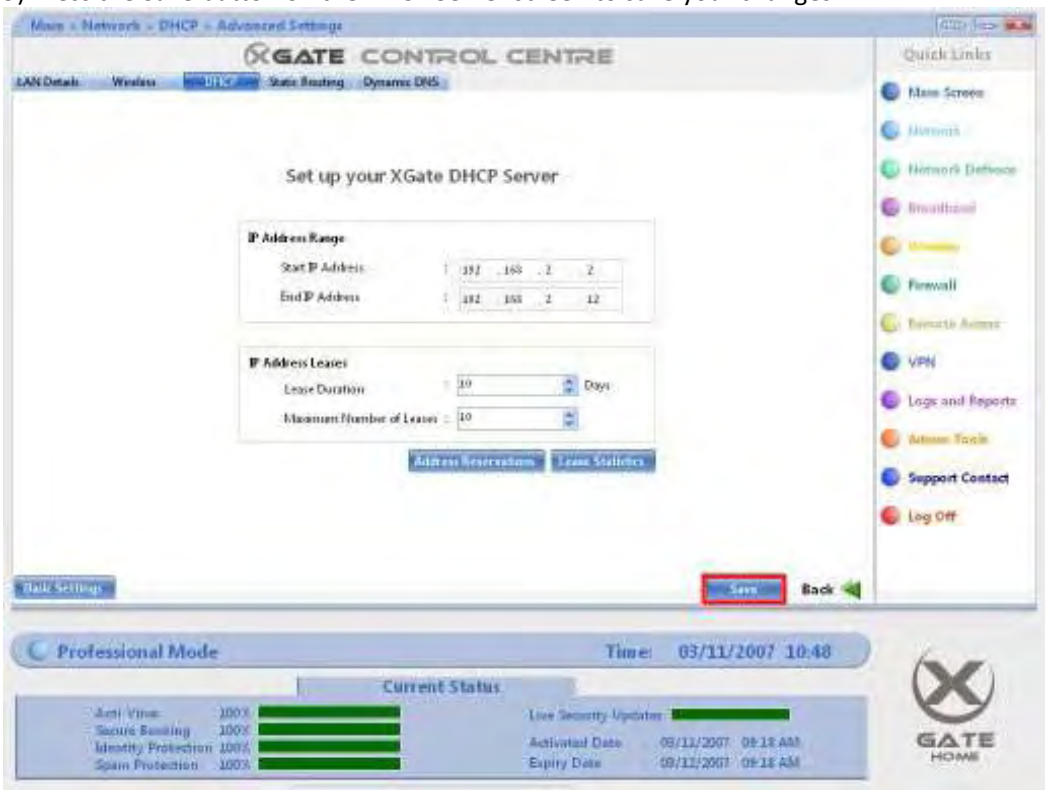
5) Press the Address Reservations button.



6) Enter the MAC Address and Static IP Address.
7) Press the Add button.

8) Press the OK button.

9) Press the Save button on the DHCP Server screen to save your changes.



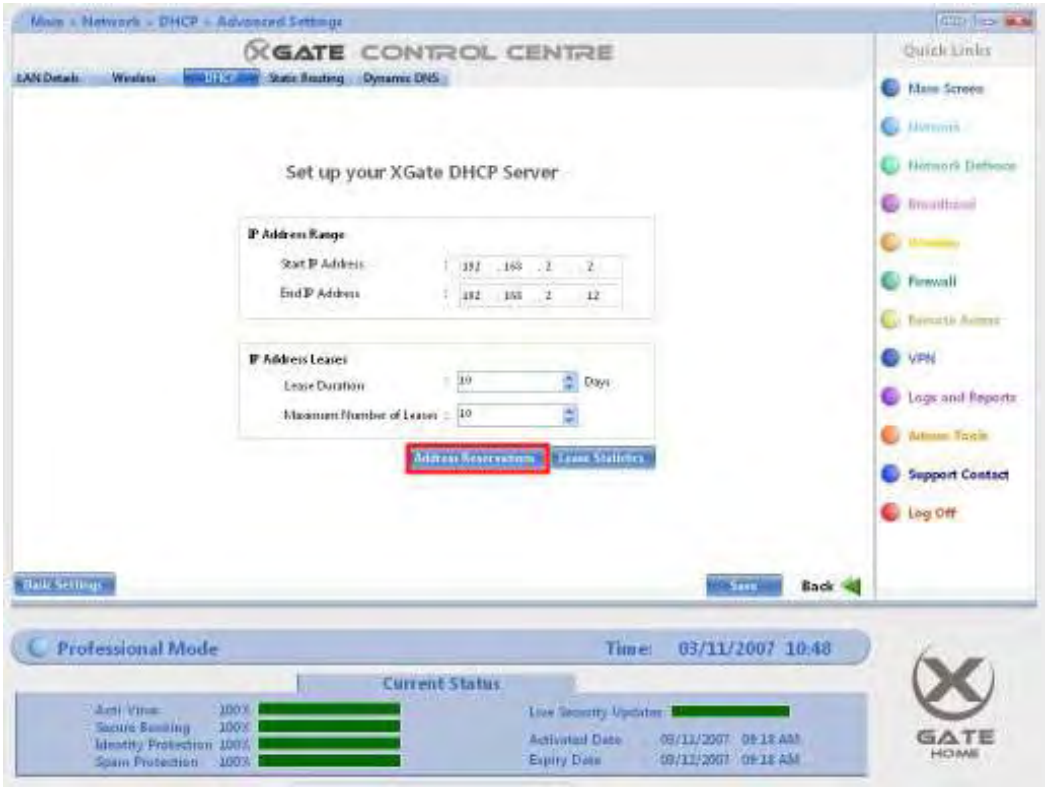
Changing a Static Address Reservation

1) In the Quick Links menu, click Network.

2) Press the DHCP tab.

3) Ensure that the DHCP server is switched on.
4) Press the Customise DHCP server button.

5) Press the Address Reservations button.



6) In the table, select the entry you wish to change by clicking it.
7) Press the Edit button.

8) The details of the Static Address Reservation can be edited using the text boxes at the top of the window.
9) Press the Save button.

10) Press the OK button.

11) Press the Save button to save your changes.


XGATE CONTROL CENTRE
Quick Links
Main Screen
Network Defence
Broadband
Firewall
VPN
Logs and Reports
Support Contact
Log Off
LAN Details
Wireless
Static Routing
Dynamic DNS
Set up your XGate DHCP Server
IP Address Range
Start IP Address
End IP Address
IP Address Leases
Lease Duration
Days
Maximum Number of Leases
Address Reservations
Lease Statistics
Back
Professional Mode
Time: 03/11/2007 10:48
Current Status
Anti-Virus 100%
Secure Banking 100%
Identity Protection 100%
Spam Protection 100%
Live Security Updates
Activated Date 03/11/2007 09:18 AM
Expiry Date 03/11/2007 09:18 AM
GATE
HOME

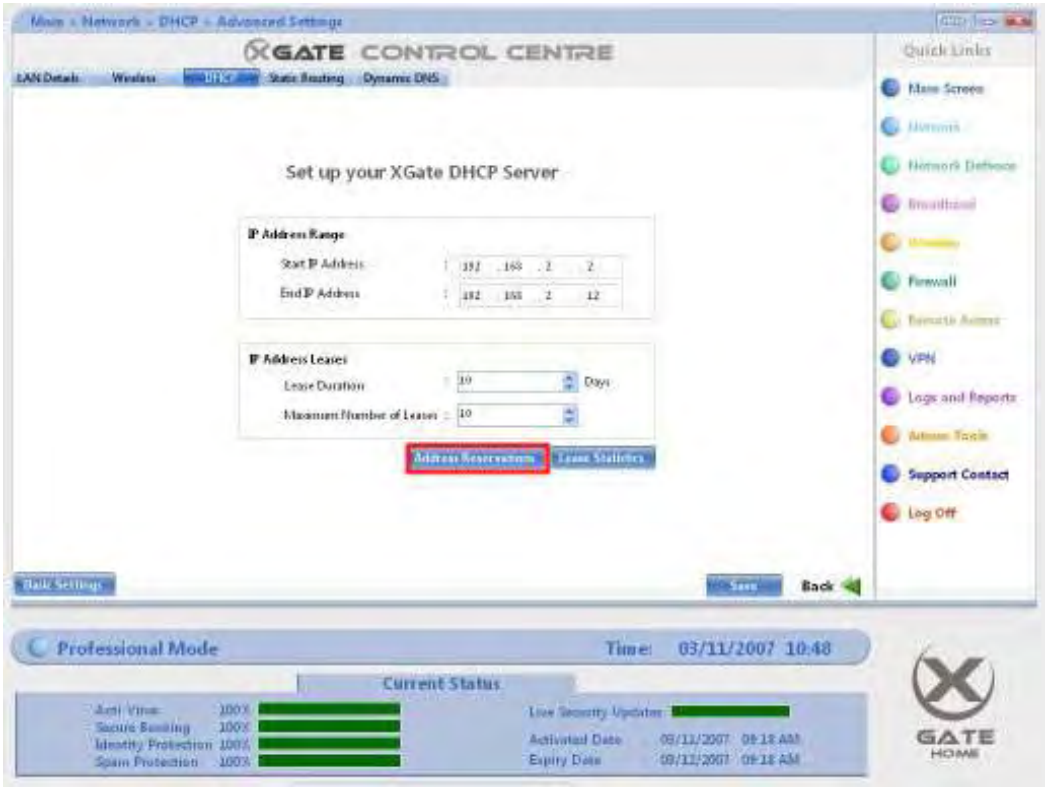
Removing a Static Address Reservation

1) In the Quick Links menu, click Network.

2) Press the DHCP tab.

3) Ensure that the DHCP server is switched on.
4) Press the Customise DHCP server button.

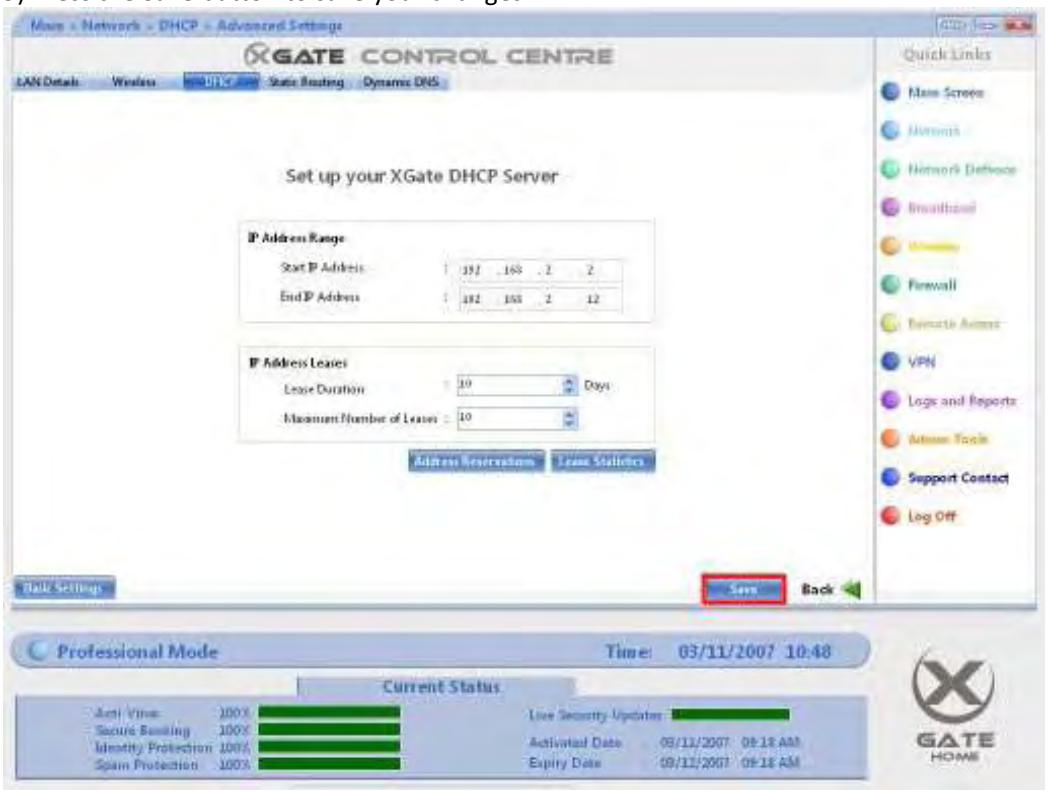
5) Press the Address Reservations button.



6) In the table, select the entry you wish to change by clicking it.
7) Press the Delete button. The entry will be removed from the table.

8) Press the OK button.

9) Press the Save button to save your changes.



Introduction

Static Routing

What is Static Routing?

Static Routing is an advanced networking feature and is only available in XGate Pro.

Static Routes are used for making fixed paths through a network. Unfortunately, if there is a fault somewhere in the route, then the traffic will not re-route as it would normally.

Analogy

Static Routing is similar to planning a journey using a road map. To get from one place to another, there are many routes you can take. Sometimes the most natural route is the one with the shortest distance. However, the shortest route may not always be the fastest route due to speed limits and other factors. As a result, you may want to plan your journey by going via a certain route that is longer but faster.

Static Route Details

When specifying a Static Route, the following details are required:

Route Name
This is a friendly name set by you, so you can easily recognise the static route.

Destination / Network IP
This is the IP address of the computer you wish traffic to be directed to.

Subnet Mask
This is the subnet mask of the computer that you wish traffic to be directed to.

Destination Gateway
The machine that you wish traffic to pass through before reaching the Destination.

Interface
The XGate network port Interface you will be using. This will either be LAN or WAN.

Type
This determines what type of static route you will be setting up. Whether you will be connecting to a host (computer) or a network.

Adding a Static Route

1) On the Quick Links menu, click Network.
2) Press the Static Routing tab.
3) Ensure that Static Routing is switched on.
4) Press the Customise Static Routing button.
5) Press the Add button.
6) Complete all the details of your static route.
7) When you are sure that the details of your static route are correct, press the OK button.
8) On the Advanced Static Routing page, press the Save button.

Changing the details of a Static Route

1) On the Quick Links menu, click Network.
2) Press the Static Routing tab.
3) Ensure that Static Routing is switched on.
4) Press the Customise Static Routing button.
5) Select an entry by single clicking the entry you wish to edit in the static routing table.
6) While the entry is highlighted, press the Edit button.
7) In the Edit Static Route window, amend the static route details to your satisfaction.
8) Press the OK button.
9) Press the Save button to confirm your changes.

Removing a Static Route

1) On the Quick Links menu, click Network.
2) Press the Static Routing tab.
3) Ensure that Static Routing is switched on.
4) Press the Customise Static Routing button.
5) Select an entry by single clicking the entry you wish to remove in the static routing table.
6) Press the Delete button. The entry will be removed from the table.
7) Press the Save button to confirm your changes.

Introduction

Dynamic DNS

What is Dynamic DNS?

Dynamic DNS allows you to associate a dynamic IP address with a domain name.

The large majority of Broadband providers distribute dynamic IP addresses to their customers. This means that your external IP address will change.

Having a dynamic IP address will not affect most people if they are just surfing the web, reading e-mail or using chat programs. However, it is very difficult to run a server using a dynamic IP address.

Some Broadband Providers offer a Static IP Address service meaning that you external (WAN) IP address will never change. However, they often charge extra for this service. On the other hand, some Dynamic DNS services are free.

Dynamic DNS is named because it dynamically changes the association of IP address and Domain name (such as gsec1.com) as your Dynamic IP address changes. As a result, if your IP address changes then the Domain Name will still direct to your computer.

Analogy

An IP Address, in this sense, is like a telephone number; it allows one computer to "call" another. Having a Dynamic IP address is like having a phone that changes numbers from time to time. People would find it difficult to contact you.

Continuing the phone analogy, DNS can be seen to be a phonebook that allows your computer to look up the IP addresses of other computers. When you type in www.gsec1.com your computer uses a DNS server to look up and translate the domain name to the IP address of the gsec1 server.

Dynamic DNS Details

To configure Dynamic DNS, the following details are required:

Account Name
This is a friendly name set by you, to easily identify your Dynamic DNS account.

Service Provider
This is a list of Dynamic DNS providers that are supported by XGate. Before you can configure a Dynamic DNS account in XGate, you will first need to create an account with a Dynamic DNS provider.

User Name
The username you used when signing up to a Dynamic DNS provider

Password
The password you used when signing up to a Dynamic DNS provider.

Automatically Update every X days
This specifies how often XGate will automatically update the Dynamic DNS with your current IP address.

Retry Updates after X minutes.
This specifies how often XGate will try to update again if your attempt to update the Dynamic DNS with your current IP address fails.

Adding a Dynamic DNS account

1) On the Quick Links menu, click Network.

2) Press the Dynamic DNS tab.

3) Ensure that Dynamic DNS is switched on.
4) Press the Customise Dynamic DNS button.

5) Press the Add button.

6) Complete the details of the account
7) Press the OK button.

8) On the Customise Dynamic DNS screen, press the Save button.

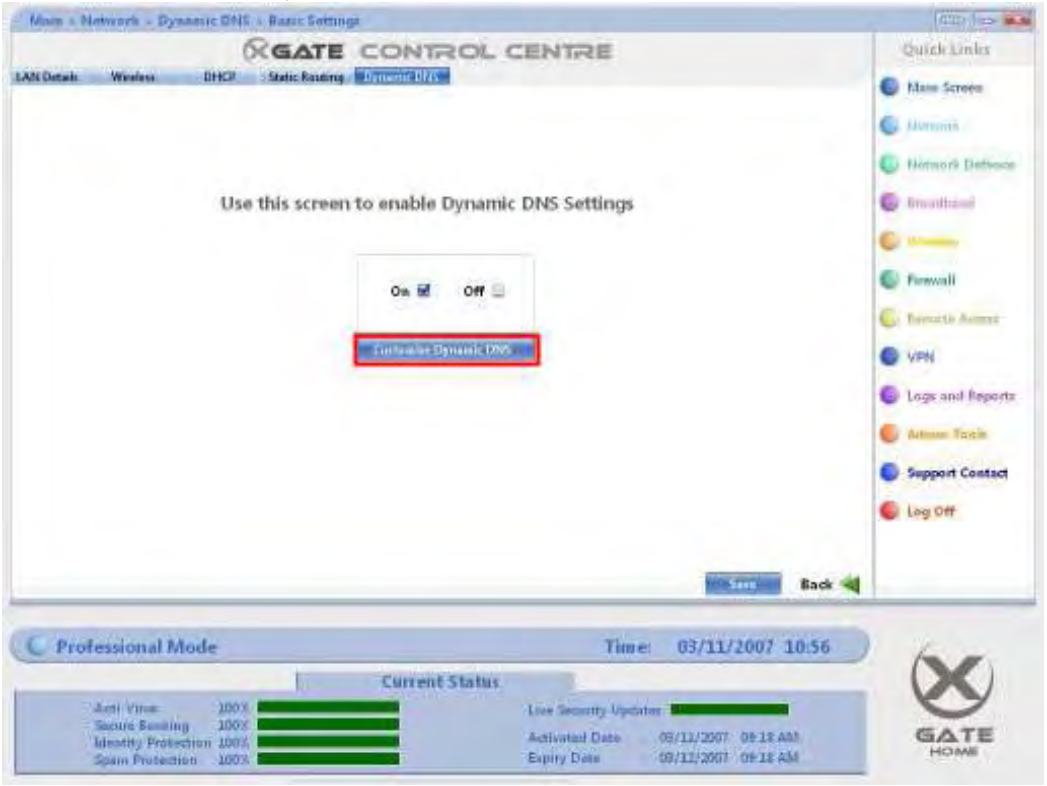

GATE CONTROL CENTRE
LAN Details
Wireless
DHCP
Static Routing
Dynamic DNS
Use this screen to Customise Dynamic DNS settings
Account Name
Service Provider
Status
Action
Enable
Example
www.DynDns.org
Enabled
Update Now
Add
Edit
Delete
Basic Settings
Save
Back
Quick Links
Main Screen
Network Defence
Broadband
Firewall
VPN
Logs and Reports
Support Contact
Log Off
Professional Mode
Time: 03/11/2007 11:02
Current Status
Anti-Virus 100%
Secure Banking 100%
Identity Protection 100%
Spam Protection 100%
Live Security Updates
Activated Date 03/11/2007 09:18 AM
Expiry Date 03/11/2007 09:18 AM
GATE HOME

Changing your Dynamic DNS details

1) On the Quick Links menu, click Network.

2) Press the Dynamic DNS tab.

3) Ensure that Dynamic DNS is switched on.
4) Press the Customise Dynamic DNS button.



5) Select an entry by single clicking the entry you wish to edit in the Dynamic DNS accounts

table.
6) Press the Edit button.

7) Amend the account details to your satisfaction.
8) Press the OK button.

9) Press the Save button to confirm your changes.

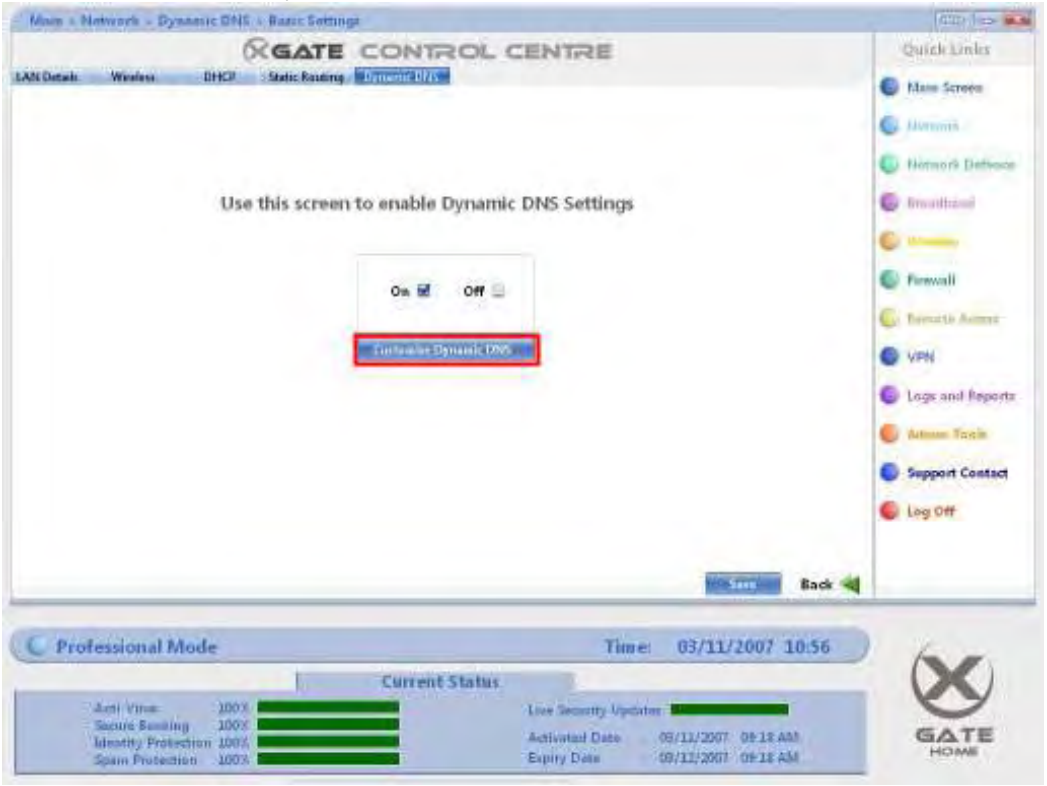

GATE CONTROL CENTRE
LAN Details
Wireless
DHCP
Static Routing
Dynamic DNS
Use this screen to Customise Dynamic DNS settings
Account Name
Service Provider
Status
Action
Enable
Example
www.DynDns.org
Enabled
Update Now
Add
Edit
Delete
Basic Settings
Save
Back
Quick Links
Main Screen
Network Defence
Broadband
Firewall
VPN
Logs and Reports
Support Contact
Log Off
Professional Mode
Time: 03/11/2007 11:02
Current Status
Anti-Virus 100%
Secure Banking 100%
Identity Protection 100%
Spam Protection 100%
Live Security Updates
Activated Date 03/11/2007 09:18 AM
Expiry Date 03/11/2007 09:18 AM
GATE HOME

Removing a Dynamic DNS account

1) On the Quick Links menu, click Network.

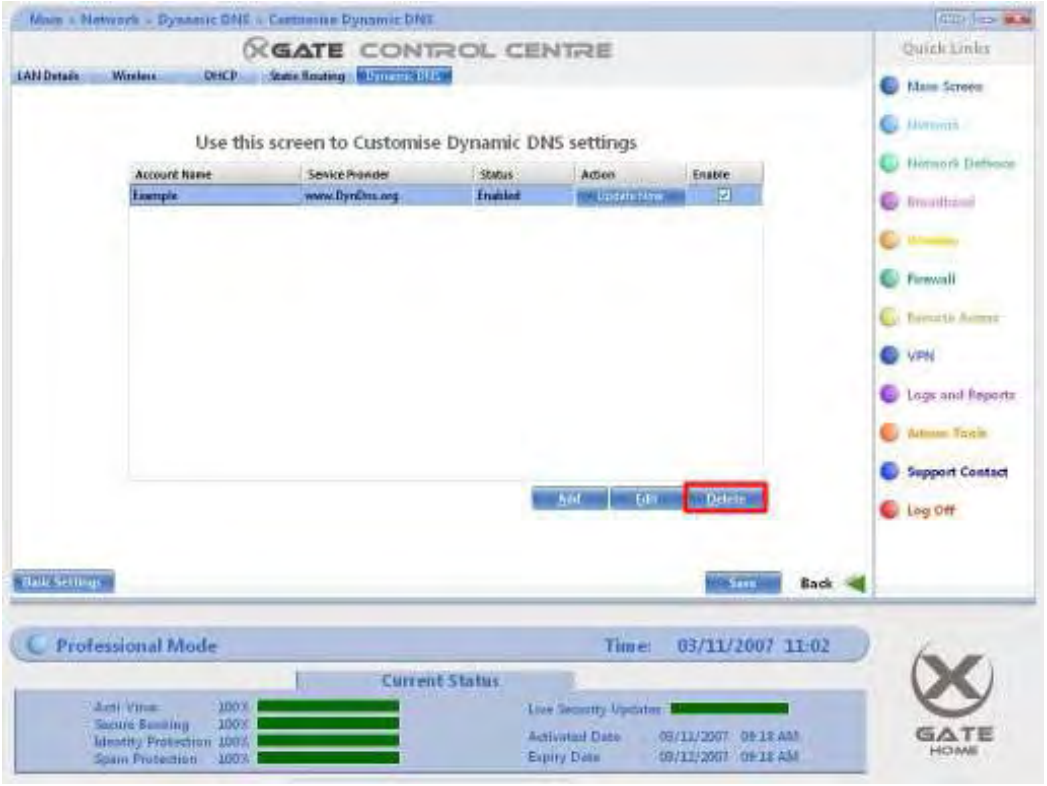
2) Press the Dynamic DNS tab.

3) Ensure that Dynamic DNS is switched on.
4) Press the Customise Dynamic DNS button.

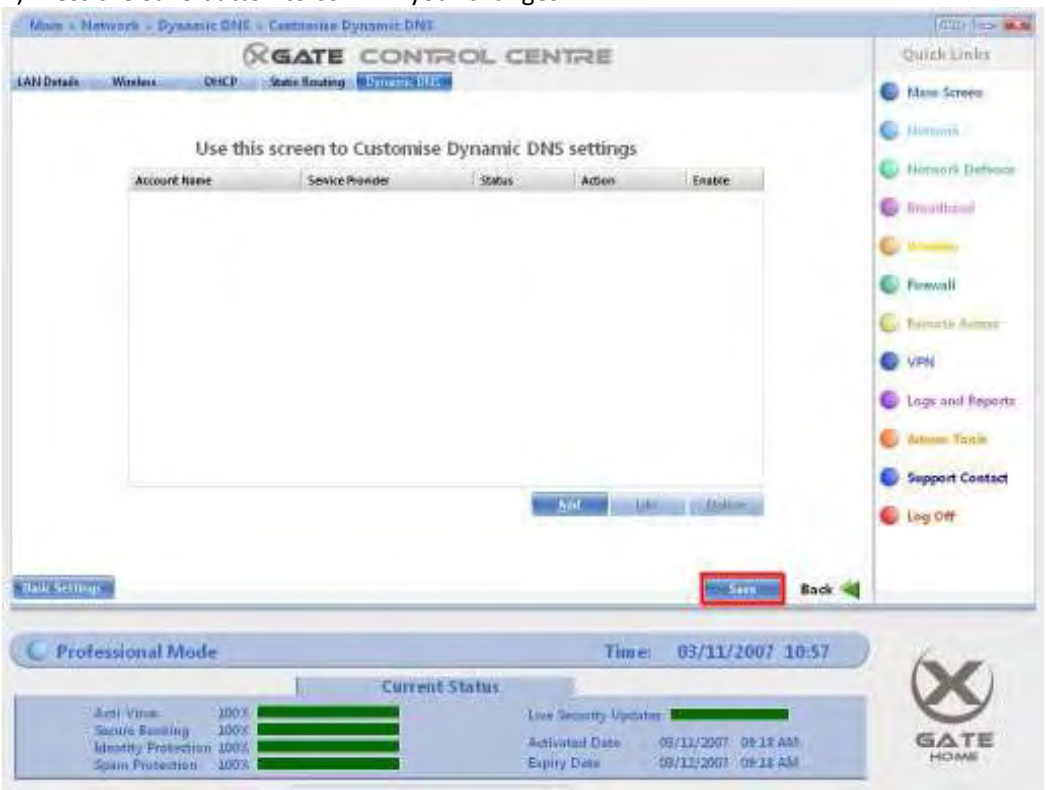


5) Select an entry by single clicking the entry you wish to remove in the Dynamic DNS

accounts table.
6) Press the Delete button.



7) Press the Save button to confirm your changes.



Web Control

What is Web Control?

Surfing the web is a popular use of the Internet. It allows us to be entertained, informed and productive. Yet it can also introduce offensive and inappropriate content into the home or office.

IDC (a global market intelligence firm) stated that 30-40% of Internet Access is for non-business use. Within the business environment, unrestricted web browsing can mean:
- Loss of productivity
- Legal liability when employees access inappropriate content or infringe on copyrighted material.
- Network congestion as valuable bandwidth is used for non-business purposes.

Within the home, dangers are also present as your children are free to access inappropriate material. This inappropriate material can be anything from pornography and drugs to self harm message boards.

With this in mind, XGate includes Web Control, for use within the home or business environment.

The main feature within Web Control is the Web Category Filter, which allows you to control access to different categories of website.

GSEC1 maintains a database of websites on the Internet and groups them into different categories according to their content.

Web Control Details

After installation, XGate will restrict access to the following website categories:

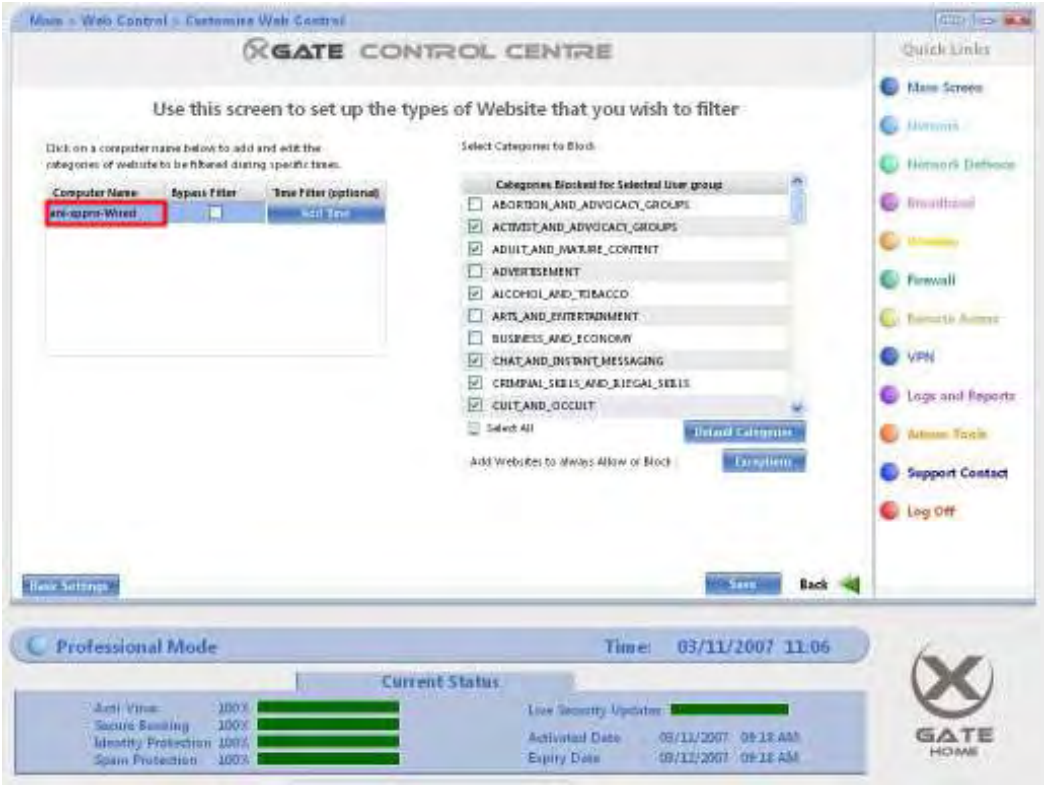
Activist and Advocacy Groups
Adult and Mature Content
Alcohol and Tobacco
Chat and Instant Messaging
Criminal Skills and Illegal Skills
Cult and Occult
Drugs
Gambling
Hacking and Proxy Avoidance Systems
Hate and Racism
Illegal Drugs
Internet Auctions
Nudism
Pay to Surf Site
Personals and Dating
Pornography
Sex Education
Violence
Weapons

Changing the Blocked Web Categories for a computer

1) Click the Web Control button.

2) Ensure that Web Control is switched on.
3) Press the Customise Web Control button.

4) Select the computer who's blocked web categories you wish to change by clicking on its name.



5) Tick a category if you want it to be blocked. Un-tick the category if you want it be allowed.

6) Once you are satisfied with the changes you have made, press the Save button.

Introduction

Time Based Web Category Filtering

What is Time Based Web Category Filtering?

Time Based Web Category Filtering allows you to set specific times and days to block computers from certain web categories.

In a business environment, Time Based Web Category Filtering allows employees to only access certain types of websites at certain times of day. For example, you may want to block Internet Auctions during working hours but allow access to Internet Auction sites during their lunch break.

Time Based Web Category Details

To set up a Time Based Web Category filter, the following details are required:

Start Time

The time that you wish to start blocking selected categories

End Time

The time you wish to stop blocking selected categories

Days

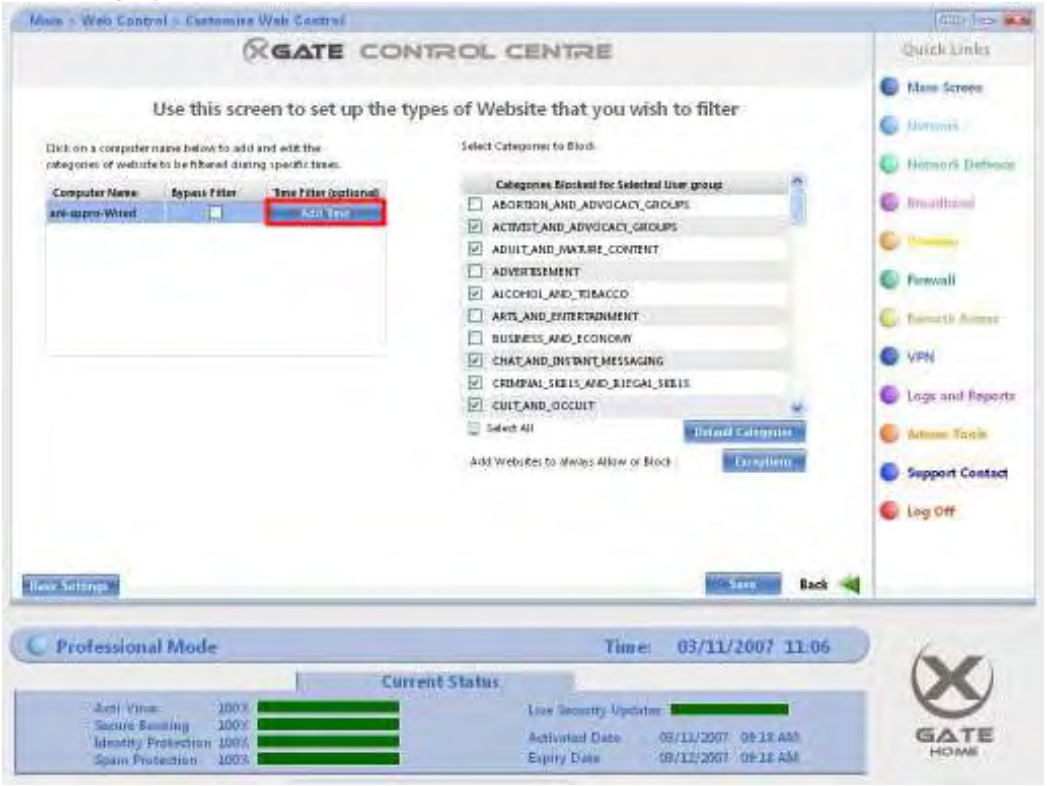
The days the Time Based Web Category filter should be active. If you wish to filter the same categories everyday, ensure that the All tick box is ticked.

Adding a Time Based Web Category Rule

1) Click the Web Control button.

2) Ensure that Web Control is switched on.
3) Press the Customise Web Control button.

4) Click the Add Time button, associated with the computer you wish to add a Time Based Web Category Rule to.



5) Enter the days and time you want the filter to take effect and press the Add button.

6) Select the categories you wish to be blocked for that time period.

7) Press Save to confirm your changes.

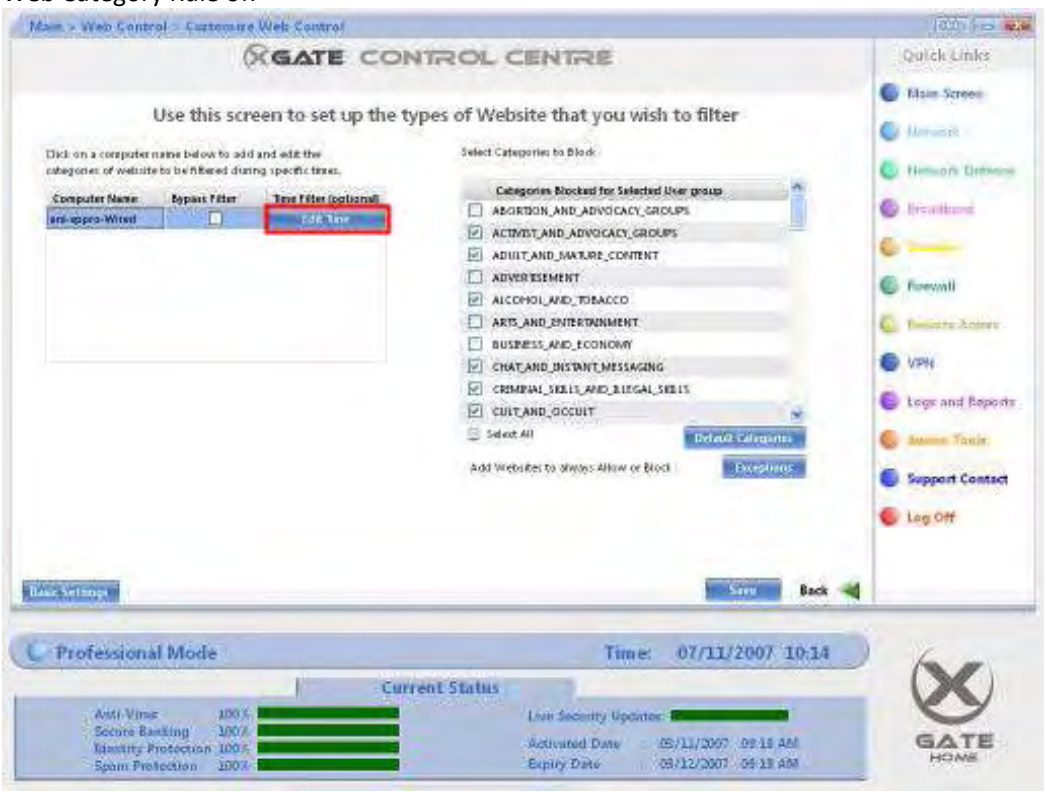
8) Repeat steps 5 to 7 if you wish to set up more than one time period for that computer.

Editing a Time Based Web Category Rule

1) Click the Web Control button.

2) Ensure that Web Control is switched on.
3) Press the Customise Web Control button

4) Click the Edit Time button associated with the computer you wish to edit the Time Based Web Category Rule of.



5) On the Time Based Web Control screen, select the time you wish to edit by single clicking

it. The details will be populated in top left of the screen.

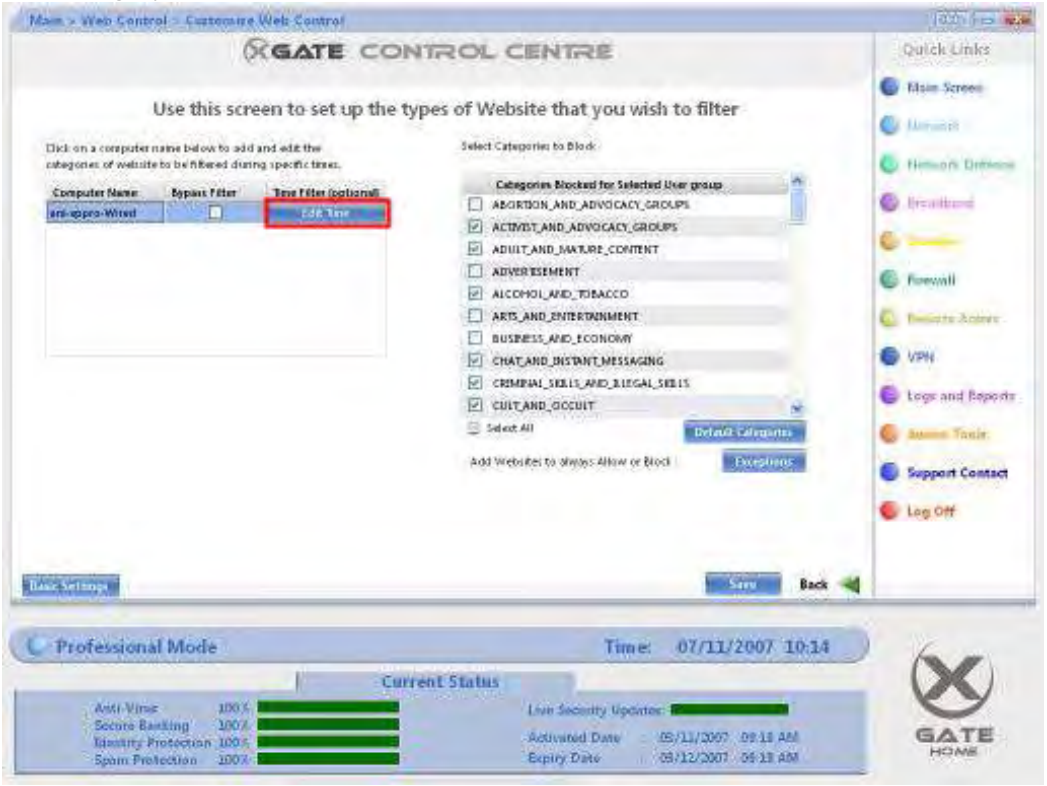
6) Edit the time and category details of the rule.
7) Press the save button to confirm your changes.

Deleting a Time Based Web Category Rule

1) Click the Web Control button.

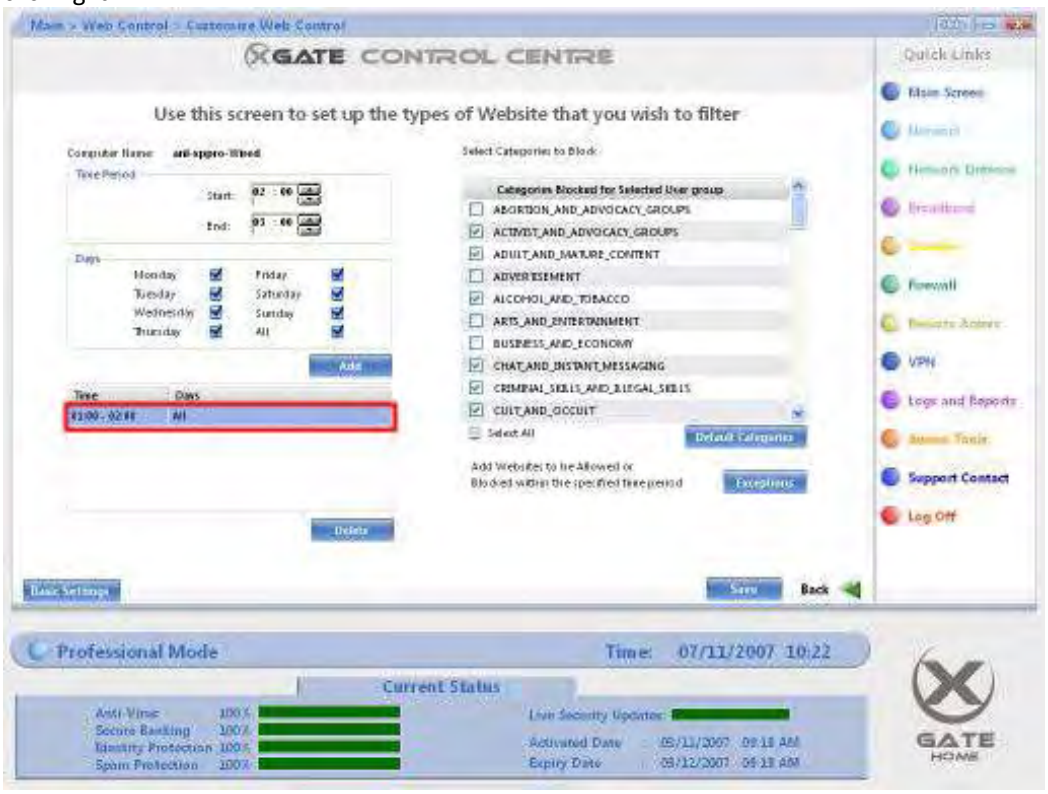
2) Ensure that Web Control is switched on.
3) Press the Customise Web Control button

4) Click the Edit Time button associated with the computer you wish to edit the Time Based Web Category Rule of.



5) On the Time Based Web Control screen, select the time you wish to delete by single

clicking it.



6) Press the Delete button.

Introduction

Web Category Exceptions List

What are Web Category Exceptions?

The Web Category Exceptions List allows you to block or allow access to individual websites. For example, if the Web Category Filter has been set to block Technology websites, but you would still wish to allow access to www.gsec1.com you can use the Exceptions List to achieve this.

Both Exception Lists used within the Web Category Filter and the Time Based Web Category Filter work on the same principle.

Please note that the Web Category Exceptions list only accepts domain names (i.e. www.gsec1.com) and not full web addresses (i.e. http://www.gsec1.com/contacts/contact.php)

Web Category Exception Details

To add a Web Category Exceptions list entry, the following information must be provided:

Website Address:
The address of the Website that you wish to allow or block.

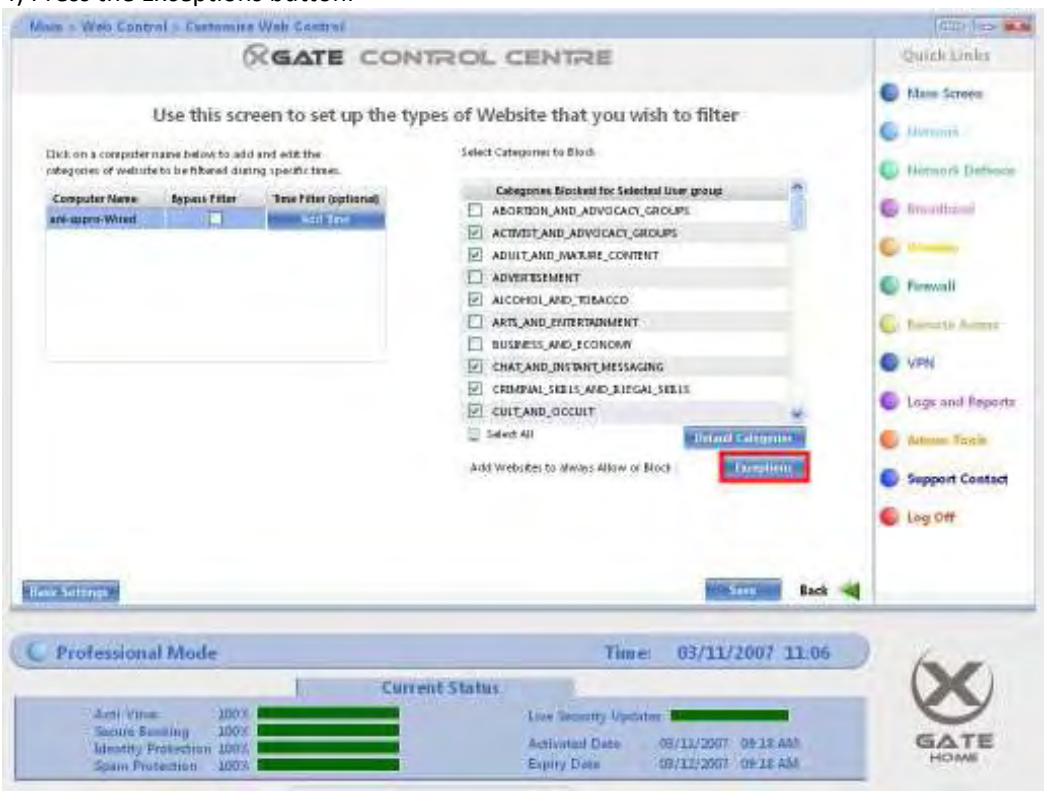
Action:
Whether you wish to Allow or Block the specified Website.

Adding an Exception in Web Control

1) Click the Web Control button.

2) Ensure that Web Control is switched on.
3) Press the Customise Web Control button.

4) Press the Exceptions button.



5) Enter the Website address and action of the exception.
6) Press the OK button.

7) Press the Save button to confirm your changes.

Within Time Based Web Category Filtering

1) Click the Web Control button.

2) Ensure that Web Control is switched on.
3) Press the Customise Web Control button.

4) Click the Edit Time button, associated with the computer you added a Time Based Web

Category Rule to.

5) Press the Exceptions button.

6) Enter the Website address and action of the exception.

7) Press the OK button.

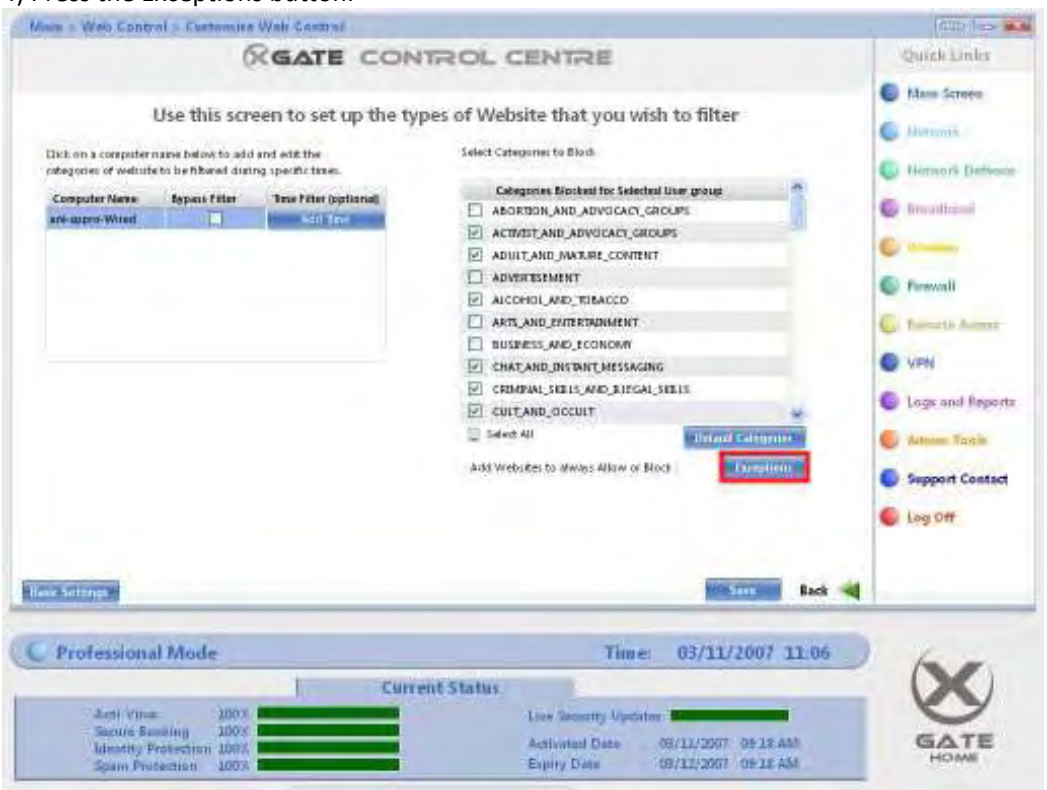
8) Press the Save button to confirm your changes.

Changing a Web Control Exception in Web Control

1) Click the Web Control button.

2) Ensure that Web Control is switched on.
3) Press the Customise Web Control button.

4) Press the Exceptions button.



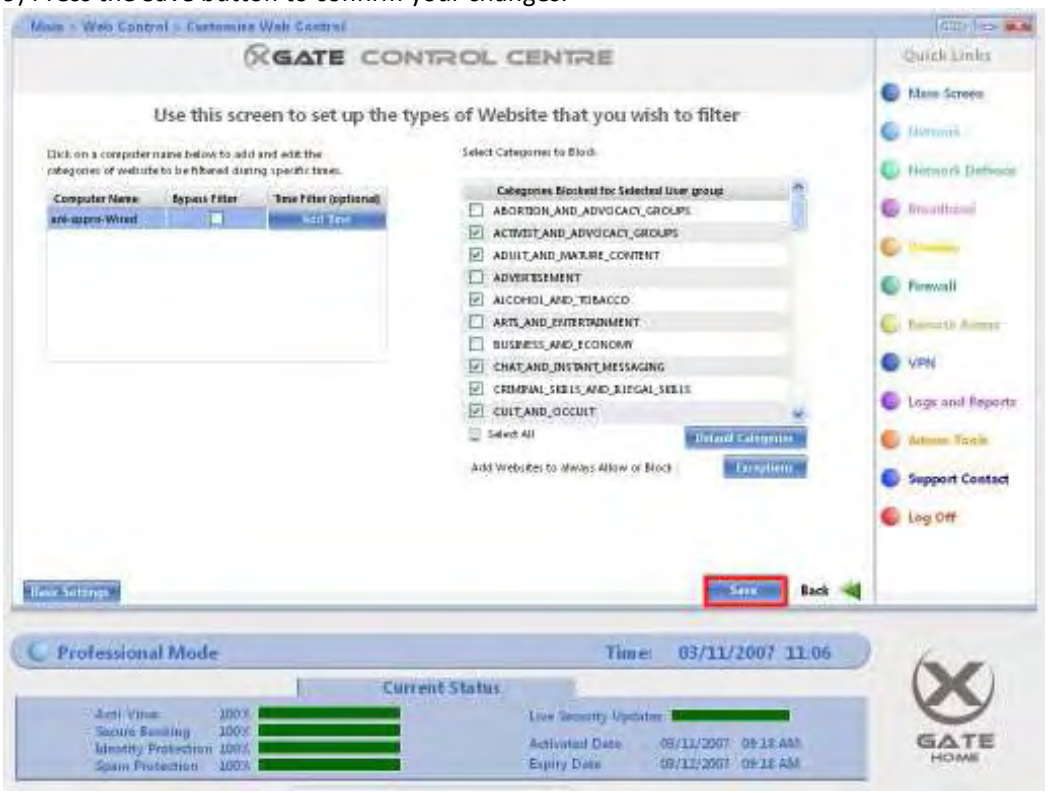
5) Click the entry you wish to edit. This will highlight the entry.

6) Press the Edit button.

7) Edit the details to your satisfaction.
8) Press the Save button.

8) Press the OK button.

9) Press the Save button to confirm your changes.



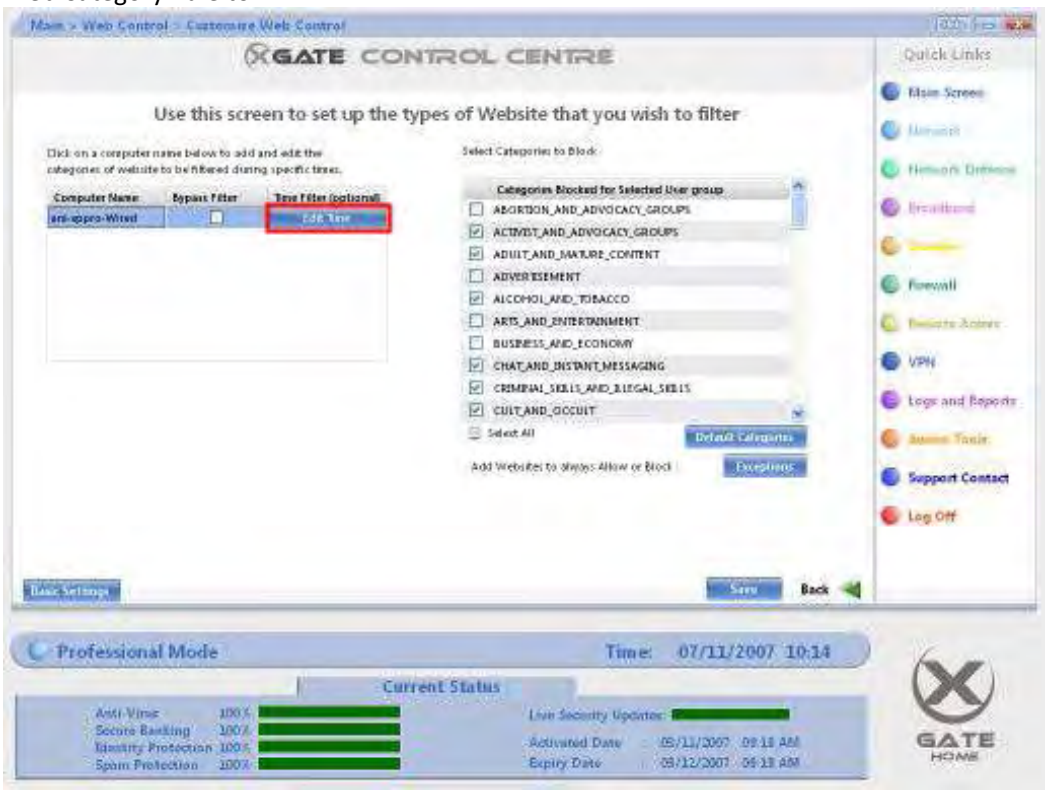
Changing a Web Control Exception within Time Based Web Category Filtering

1) Click the Web Control button.

2) Ensure that Web Control is switched on.
3) Press the Customise Web Control button.

4) Click the Edit Time button, associated with the computer you wish to add a Time Based

Web Category Rule to.



5) Press the Exceptions button.

6) Click the entry you wish to edit. This will highlight the entry.

7) Press the Edit button.

8) Edit the details to your satisfaction
9) Press the Save button.

10) Press the OK button.

11) Press the Save button to confirm your changes.

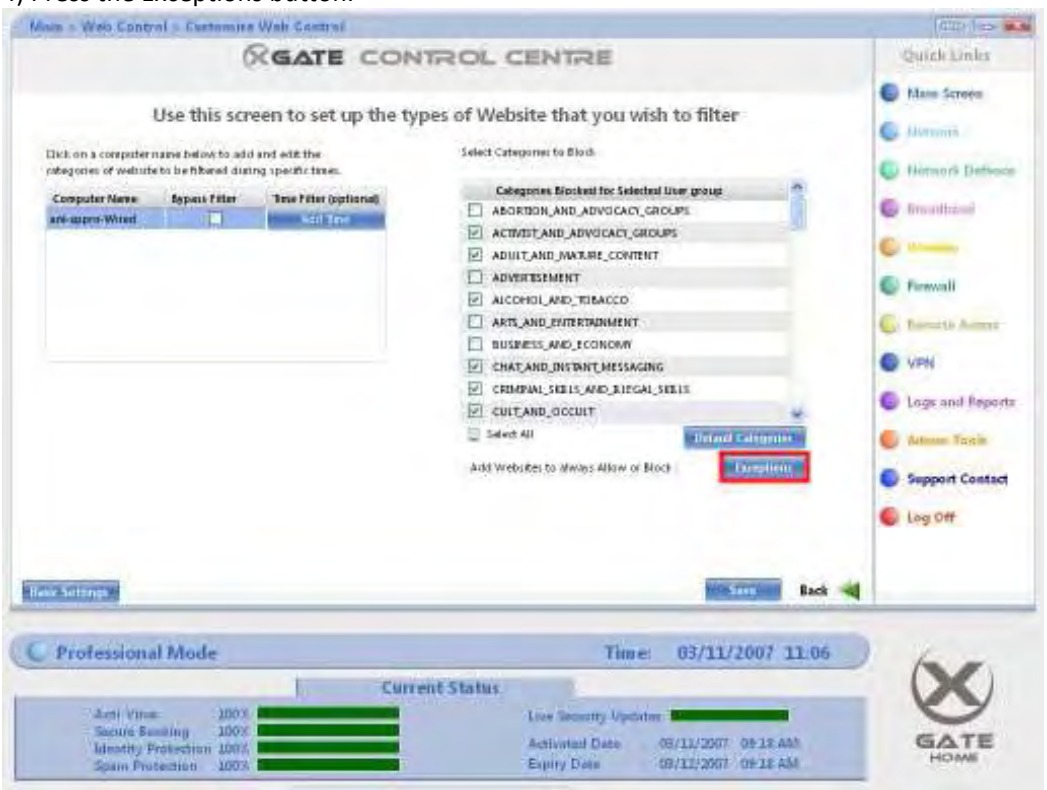
Removing a Web Control Exception in Web Control

1) Click the Web Control button.

2) Ensure that Web Control is switched on.

3) Press the Customise Web Control button.

4) Press the Exceptions button.



5) Within the Exceptions window, click the entry you wish to delete. This will highlight the entry.

6) Press the Delete button.

7) Press the OK button.

8) Press the Save button to confirm your changes.

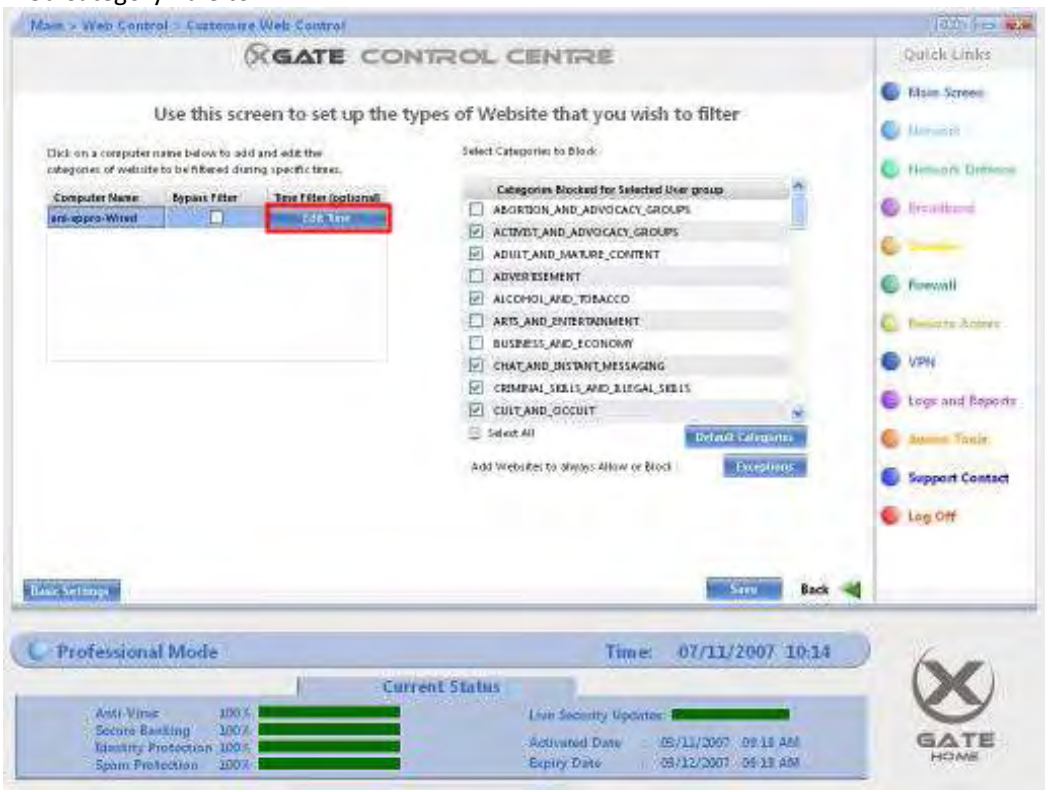
Removing a Web Control Exception within Time Based Web Category Filtering

1) Click the Web Control button.

2) Ensure that Web Control is switched on.

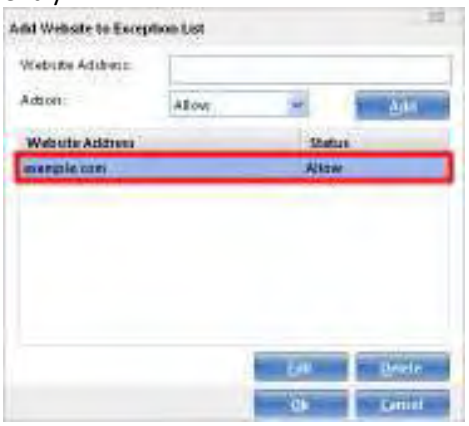
3) Press the Customise Web Control button.

4) Click the Edit Time button, associated with the computer you wish to add a Time Based Web Category Rule to.



5) Press the Exceptions button.

6) Within the Exceptions window, click the entry you wish to edit. This will highlight the entry.



7) Press the Delete button.

8) Press the OK button.

9) Press the Save button to confirm your changes.

Mail and Anti-Spam

What is Mail and Anti-Spam?

Just like ‘snail mail', electronic mail is susceptible to abuse by senders of unwanted junk or ‘spam’ mail.

XGate helps prevent this torrent of unwanted mail by using Anti-Spam technology, which incorporates various filters and databases to prevent spam mail from entering your mail client’s inbox.

To help with classification of spam mails, XGate communicates with your POP3 e- mail server. The POP3 server is where your incoming e-mail is stored.

> **Important Note**:
> Only Microsoft Outlook (2000, 2002, 2003, 2007) is fully supported by XGate Anti-SPAM.

Mail and Anti-Spam Features

There are two main features within Mail and Anti-Spam:

POP3
Setting up POP3 ensures that all incoming mail passes through the XGate. This allows XGate to filter and control incoming mail.

SPAM
This is where you can set up how XGate will scan your mail for Spam.

Introduction

POP3

What is POP3?

POP3 stands for Post Office Protocol 3 and is the primary method of retrieving mail from the Internet on to your computer's mail client.

Analogy

POP3 is similar to how you would obtain your real life/snail mail. When someone sends you a mail, it is sent to their closest post sorting office (their mail server). The sorting office then looks at the mail and sends it to the address that is specified. The mail is directed to your local post office (your mail server). The mail can now be picked up from your letter box (mail client).

POP3 Features

Within POP3, you can set up the following:

POP3 Server
This is where you can set up XGate to deliver incoming mail to your mail client.

Additional Domain
This allows you to set up additional domains for your POP3 mail server

Address Filter
This allows you to block mail from specific e-mail addresses or domains.

Introduction

POP3 Server

What is a POP3 Server?

The definition of a Proxy is something that acts on behalf of something else. The XGate device acts on the behalf of your computers when communicating with your Mail server. When XGate receives mail, it will then forward it to the appropriate computer's mail client.

POP3 Server Details

Transparent Proxy

A Transparent Proxy can also be referred to as a "Forceful Proxy". This is because a transparent proxy forces each computer's mail client to go through the XGate POP3 Server/Proxy. As such, this feature can be useful if you do not wish to set up each individual mail client on your network to go through the XGate.

POP3 Server Domain / IP Address

This is the POP3 server. To find out what your POP3 Server domain or IP Address is, check your Microsoft Mail Client. For more information please see the troubleshooting section.

Mail Server Port

This is the server port of the POP3 Server. Typically this should be 110. For more information please check the troubleshooting section.

Proxy Port

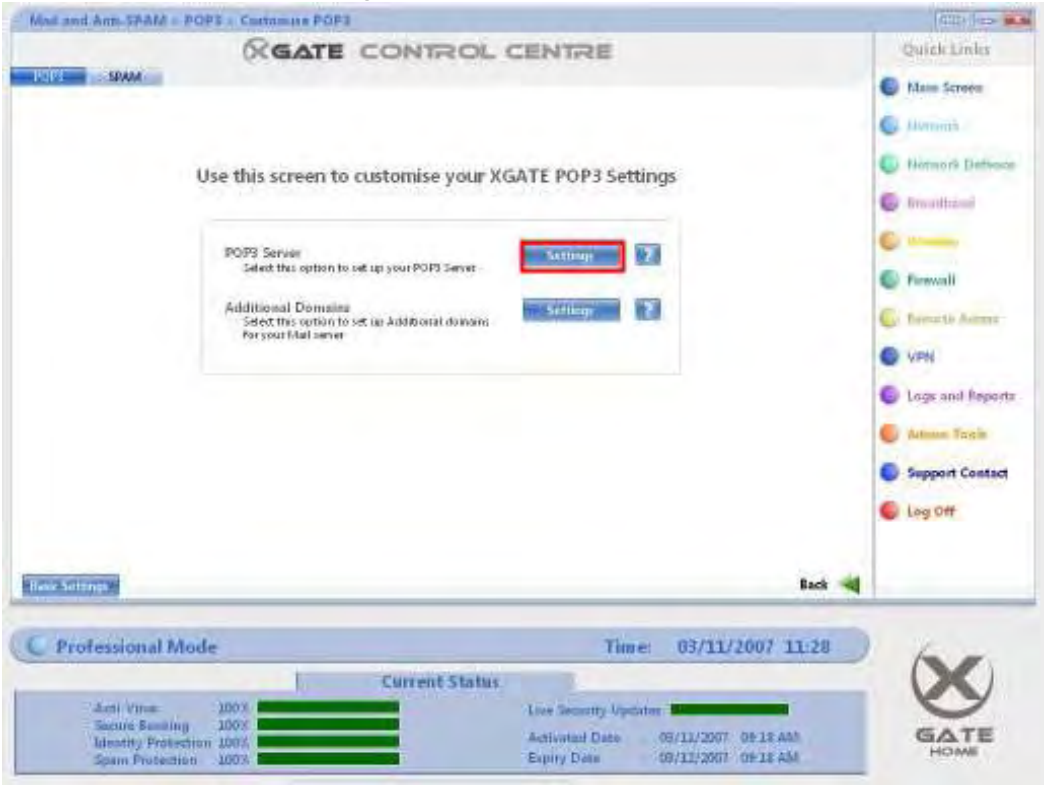
This is the port of the XGate POP3 Proxy. In most cases, it should be the same as the Mail Server Port.

Changing the POP3 Server settings

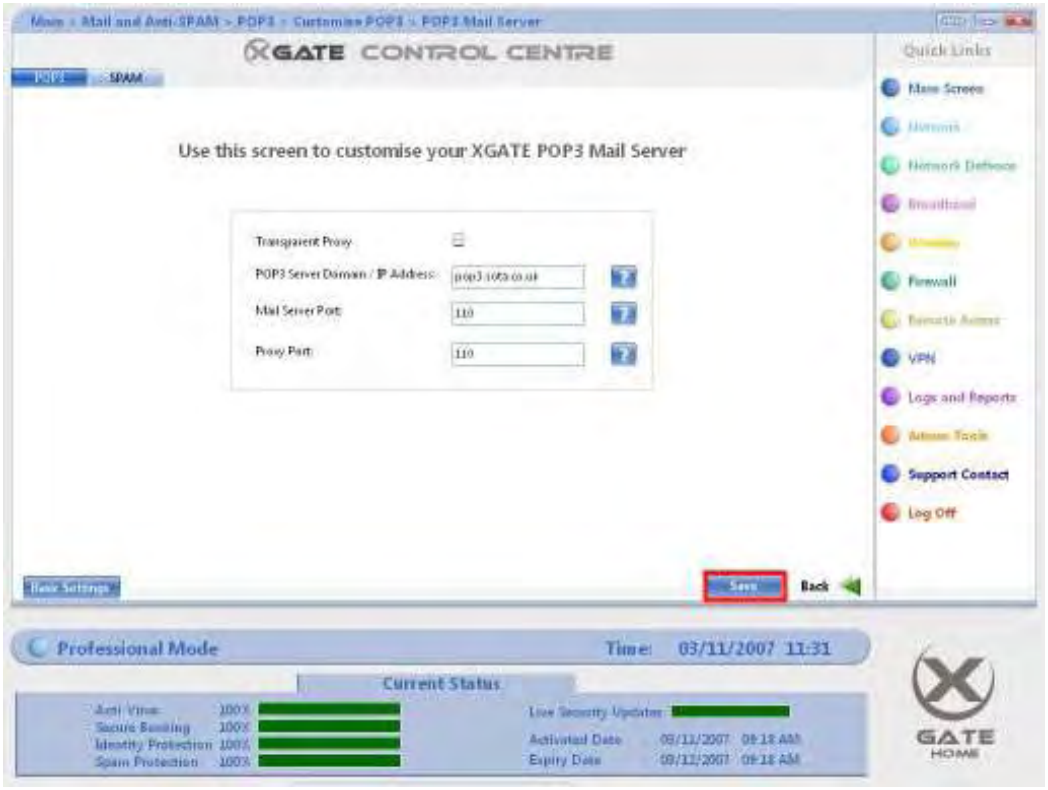
1) Press the Anti-Spam and Mail button.

2) Ensure that the POP3 Server is switched on.
3) Press the Customise POP3 Settings button.

4) Click the POP3 Server - Settings button.



5) Make the appropriate changes you wish.
6) Press the Save button to confirm your changes.


XGATE CONTROL CENTRE
Quick Links
Use this screen to customise your XGATE POP3 Mail Server
Transparent Proxy
POP3 Server Domain / IP Address:
Mail Server Port:
Proxy Port:
Back
Professional Mode
Time: 03/11/2007 11:31
Current Status
Anti-Virus 100%
Secure Banking 100%
Identity Protection 100%
Spam Protection 100%
Activated Date
Expiry Date

Introduction

Additional Domain

What is an Additional Domain?

Additional Domains allow you to associate multiple domain names to the same POP3 server specified within XGate.

Additional Domain Details

To set up an Additional Domain, the following details are necessary:

Server Name
A friendly name so you can easily identify the entry.

Server Domain/IP Address
The Domain name or IP address which you wish to associate with your current POP3 server.

Adding an Additional Domain

1) Press the Anti-Spam and Mail button.
2) Ensure that the POP3 Server is switched on.
3) Press the Customise POP3 Settings button.
4) Click the Additional Domain Settings button.
5) Press the Add button.
6) Enter the details of your Additional Domain.
7) Press the OK button.
8) Press the Save button to confirm your entry.

Changing the details of an Additional Domain

1) Press the Anti-Spam and Mail button.
2) Ensure that the POP3 Server is switched on.
3) Press the Customise POP3 Settings button.
4) Click the Additional Domain Settings button.
5) Select the entry you wish to edit by clicking it. This will highlight your selected entry.
6) Press the Edit button.
7) Change the details of your Additional Domain.
8) Press the OK button
9) Press the Save button to confirm your changes.

Removing an Additional Domain

1) Press the Anti-Spam and Mail button.
2) Ensure that the POP3 Server is switched on.
3) Press the Customise POP3 Settings button.
4) Click the Additional Domain Settings button.
5) Select the entry you wish to edit by clicking it. This will highlight your selected entry.
6) Press the Delete button.
7) Press the OK button.
8) Press the Save button to confirm your changes.

Introduction

SPAM

What is SPAM?

The term SPAM is used to describe unsolicited and generally unwanted E-mail, usually relating to advertising.

XGate creates a Spam folder to separate and store e-mail identified as junk. It is recommended that you check this folder on a fairly regular basis to ensure that no genuine mails are being directed to the folder in error during XGate's Spam 'learning phase'.

Please note that you can only configure Spam when POP3 is switched on and correctly configured. This is due to Spam being reliant on the POP3 server/proxy to view and monitor the mails being passed through XGate to your computer.

Analogy

Spam can be likened as the electronic form of the junk mail you receive in your post box, advertising takeaways, double glazing and credit cards.

SPAM Features

Within Anti-Spam you can access many Spam prevention methods, such as:

Spam Domain Database
This contains the external Spam domain databases that will classify Spam and place it in your mail client's Spam folder.

Spam URL Database
This contains the external Spam URL databases that will classify Spam and place it in your mail client's Spam folder.

Date Filter
This option allows you to filter Spam by the date it was sent.

Keyword Filter
This allows you to classify mail containing specific words as Spam

Regular Expressions
Regular Expressions allows you to specify Spam patterns which, when detected, will classify mails as Spam.

Global Exceptions List
This is the list of exceptions for the Spam feature. It will allow you to specify the domains or e-mail addresses which will be allowed to bypass the Spam classification.

SPAM Management
What is SPAM Management?

This window allows you to change the XGate SPAM tag.

When a mail is deemed to be SPAM by XGate, it appends the SPAM tag to the e-mail subject.

For example, if we set the SPAM tag to “[XG SPAM] “ and we receive an e-mail with a subject of “Example”, then the e-mail will come as “[XG SPAM] Example”.

Introduction

Spam Domain Database

What is a SPAM Domain Database?

Spam Domain Databases, also called DNS blacklists, are online databases, which hold information on known and verified sources of Spam.

Spammers tend to fake the e-mail addresses which they send Spam from. As such, Spam Domain Databases aim to list the IP Addresses of the servers where Spam originates.

SPAM Domain Database Details

To enter a Spam Domain Database, only the URL of the Spam Domain Database needs to be entered.

Adding a Spam Domain Database

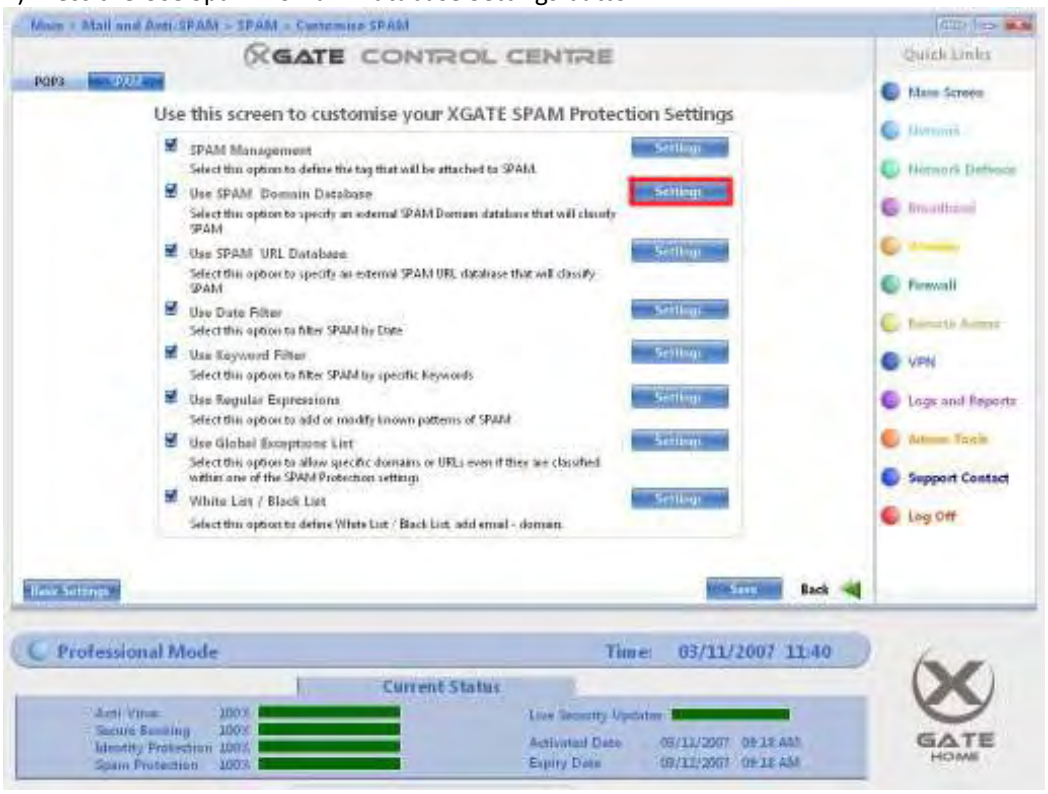
1) Press the Mail and Anti-spam button.

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

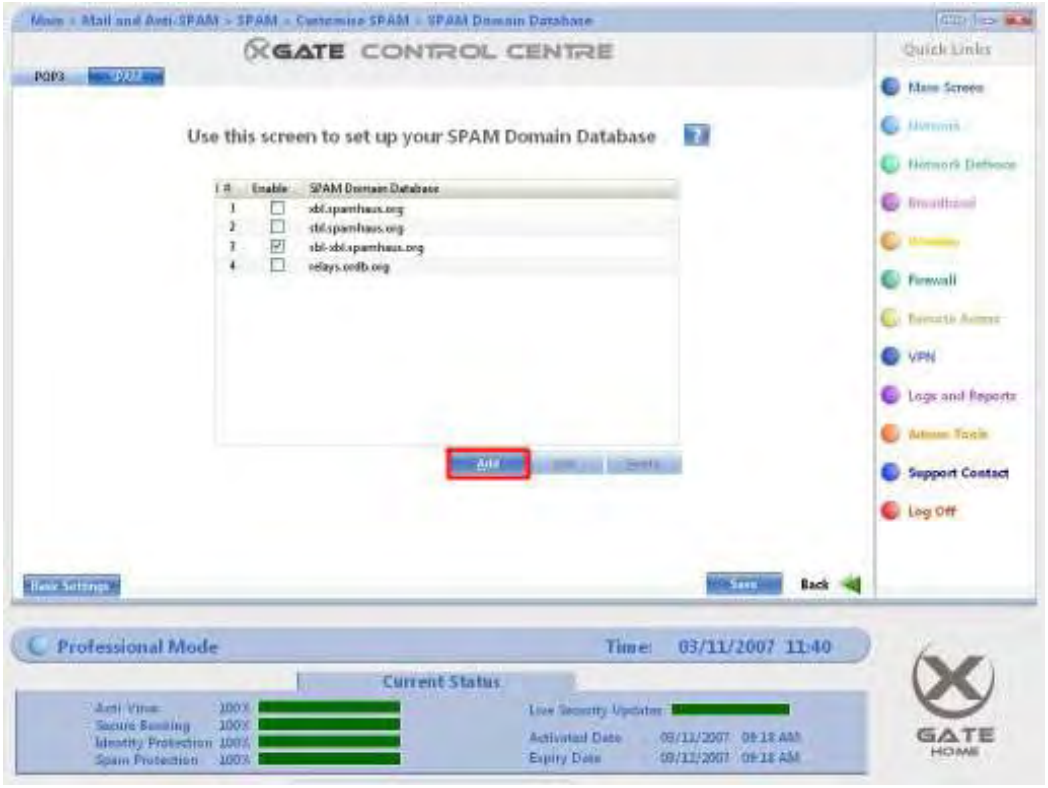
4) Ensure that Spam has been swiched on.
5) Click on Customise SPAM Protection.

6) Ensure that the Use Spam Domain Database tick box is ticked.

7) Press the Use Spam Domain Database Settings button.

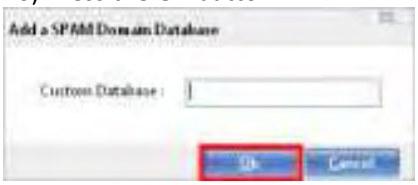


8) Press the Add button.

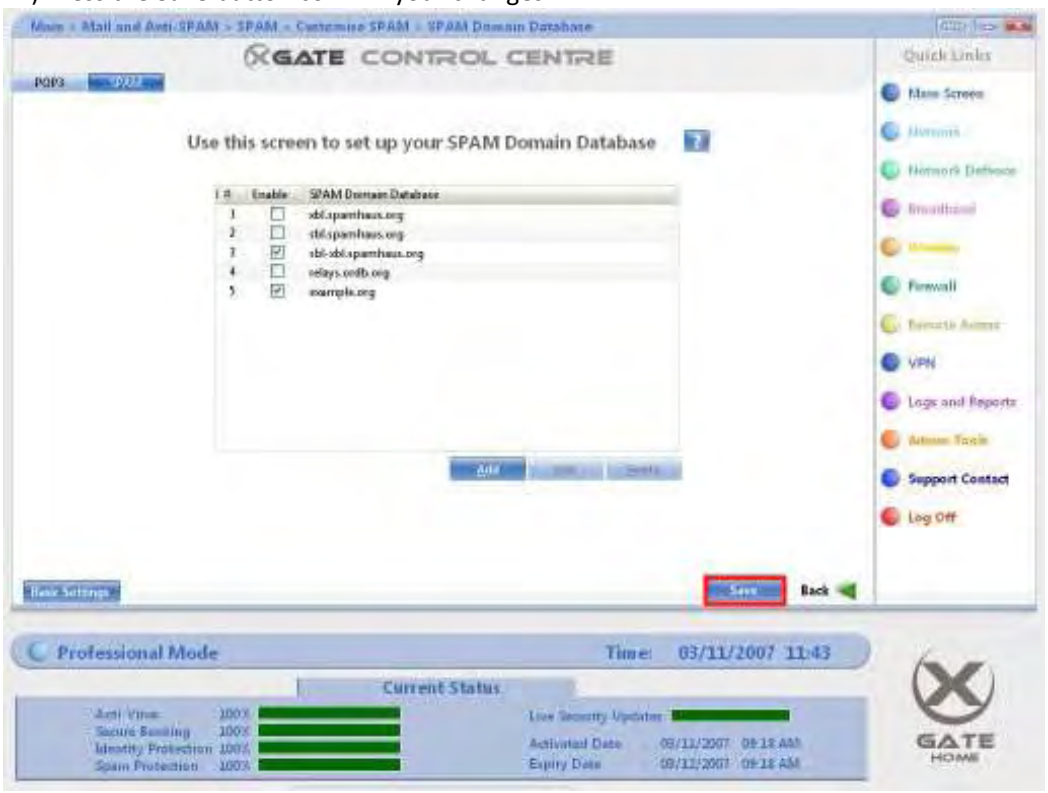


9) Type in the url of the Spam Domain Database you wish to enter.

10) Press the OK button.



11) Press the Save button confirm your changes.



Changing a Spam Remote Database

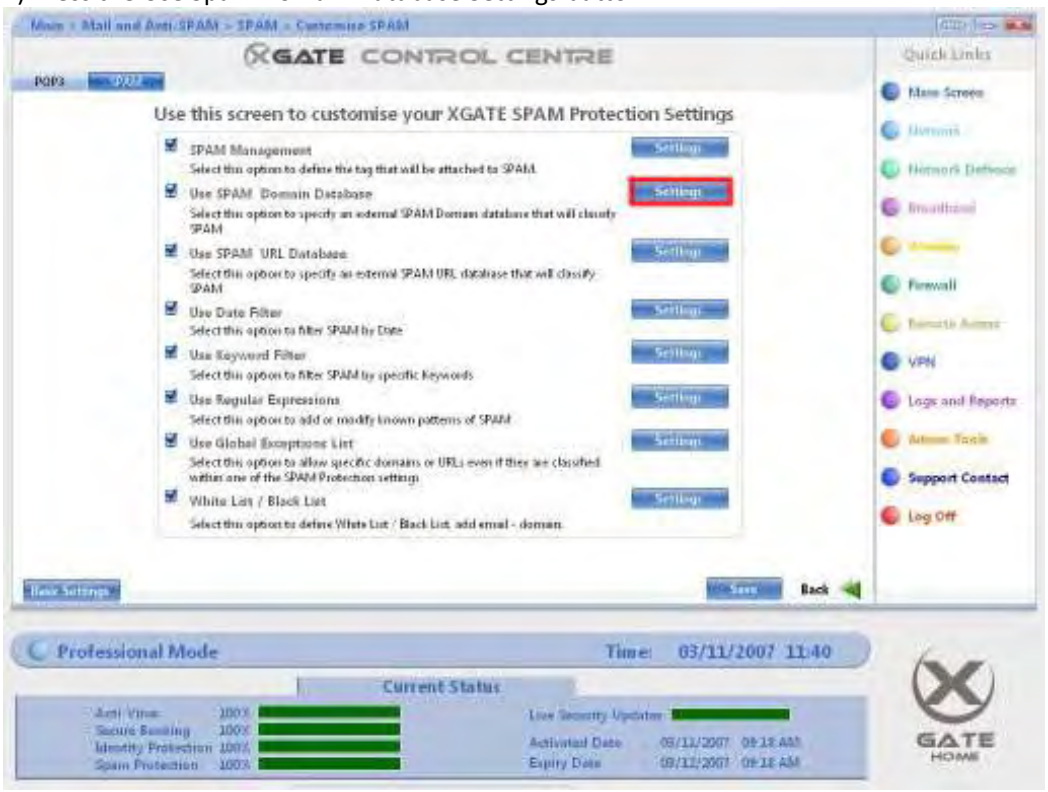
1) Press the Mail and Anti-spam button.

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

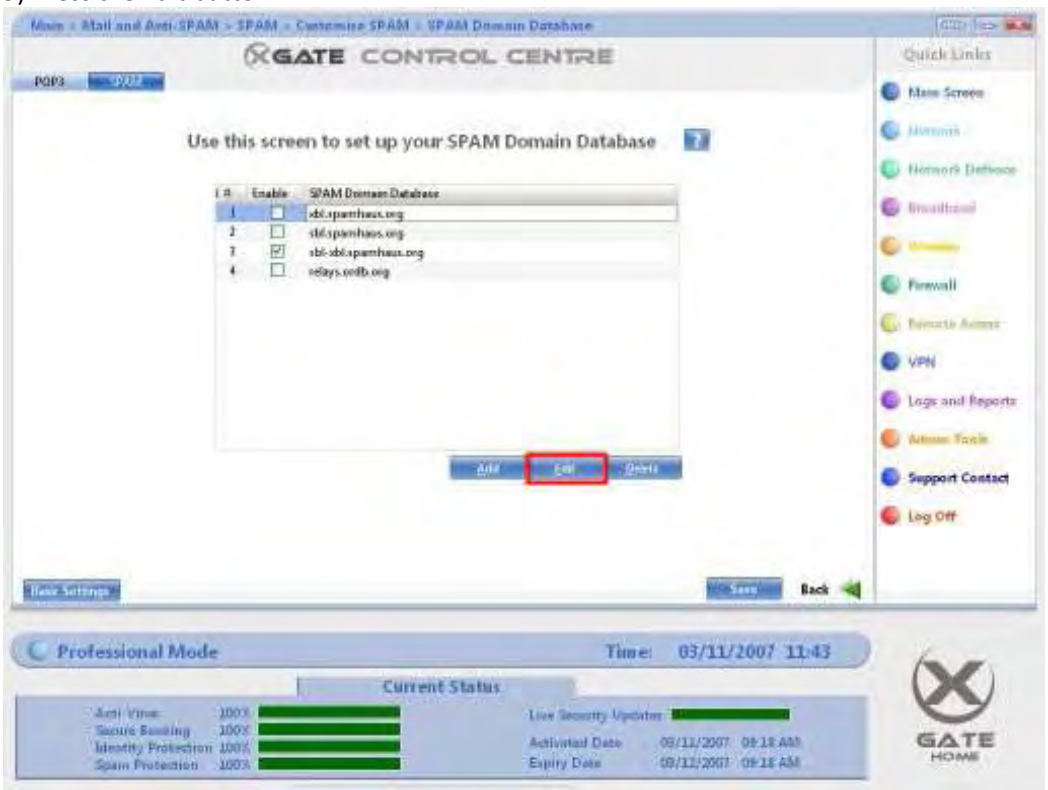
4) Ensure that Spam has been swiched on.
5) Click on Customise SPAM Protection.

6) Ensure that the Use Spam Domain Database tick box is ticked.

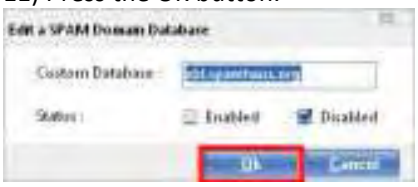
7) Press the Use Spam Domain Database Settings button.



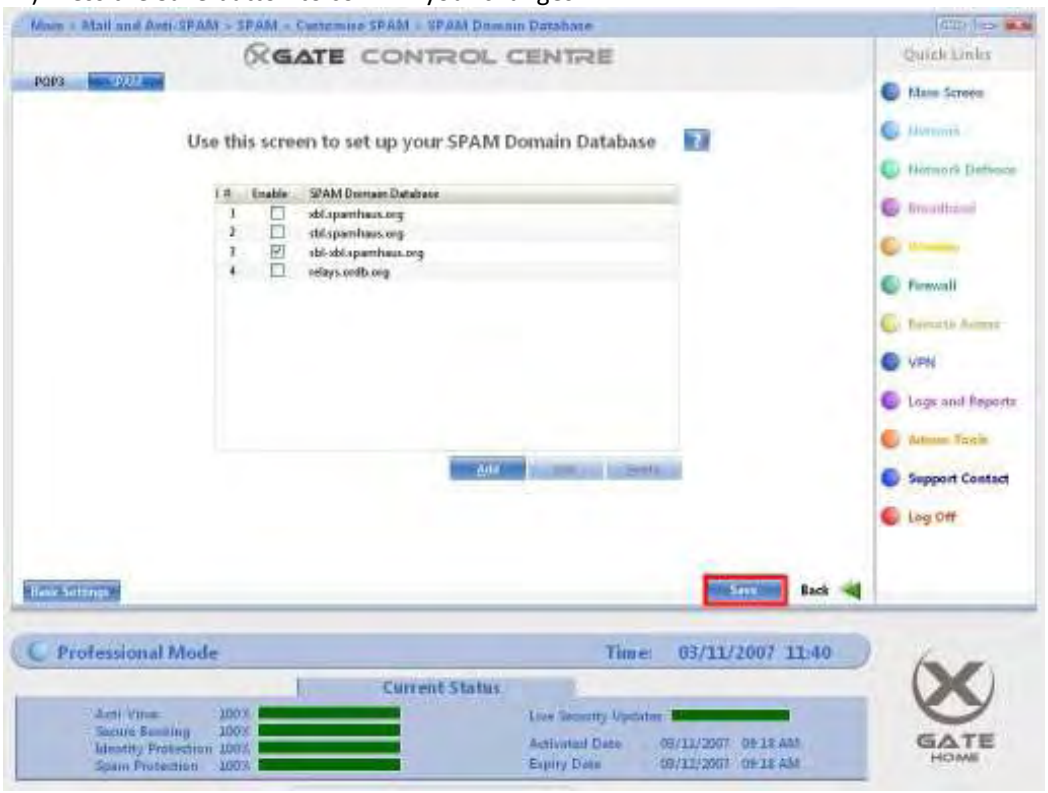
8) Select the entry you wish to edit. This will highlight the entry.
9) Press the Edit button.



10) Amend the URL of the Spam Domain Database.
11) Press the OK button.



12) Press the Save button to confirm your changes.



Removing a Spam Domain Database

1) Press the Mail and Anti-spam button.

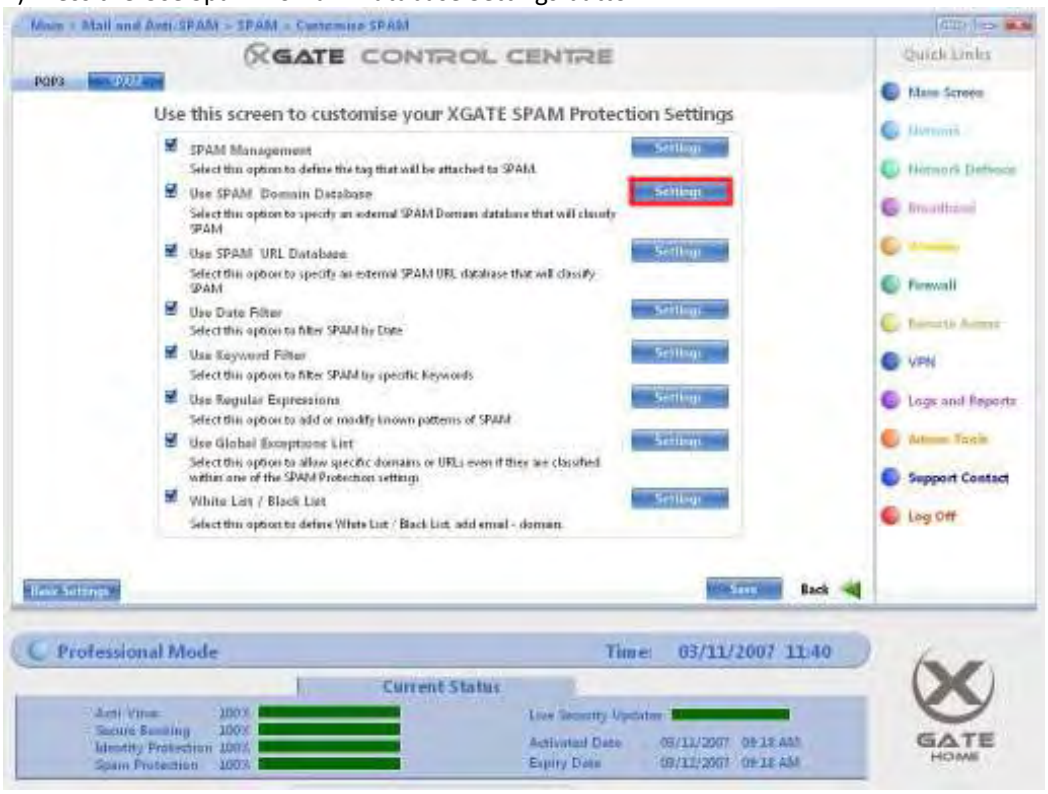
2) Ensure that POP3 has been switched on.

3) Click the Spam Tab.

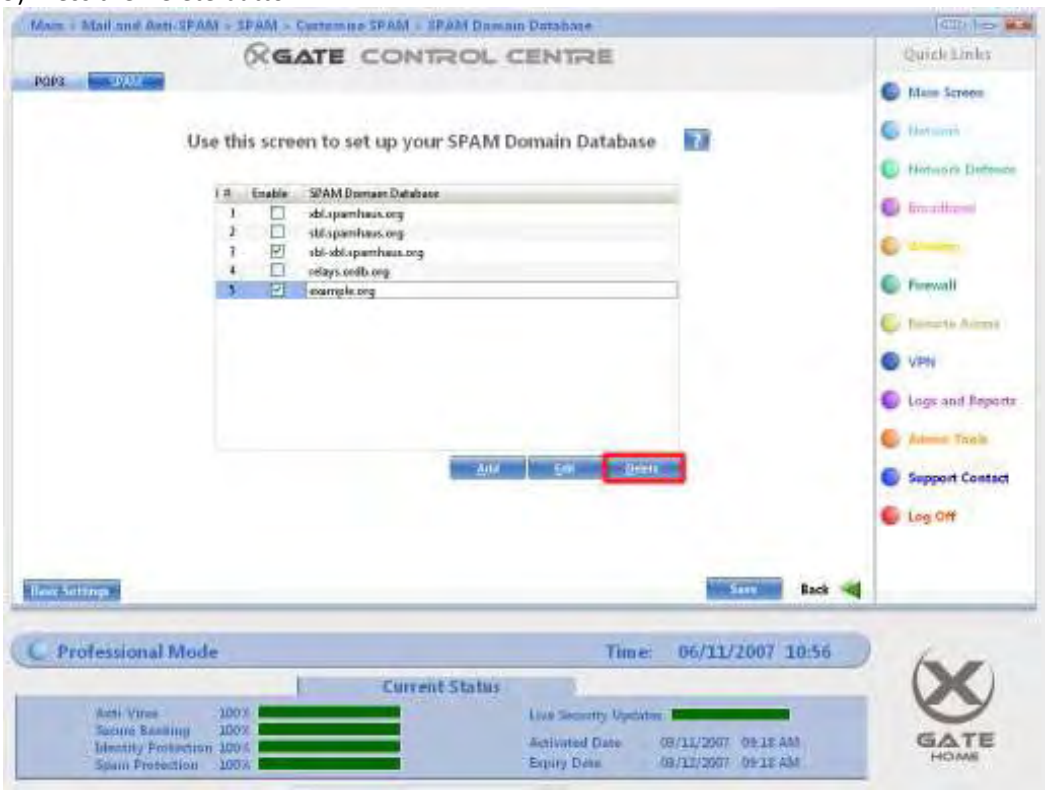
4) Ensure that Spam has been swiched on.
5) Click on Customise SPAM Protection.

6) Ensure that the Use Spam Domain Database tick box is ticked.

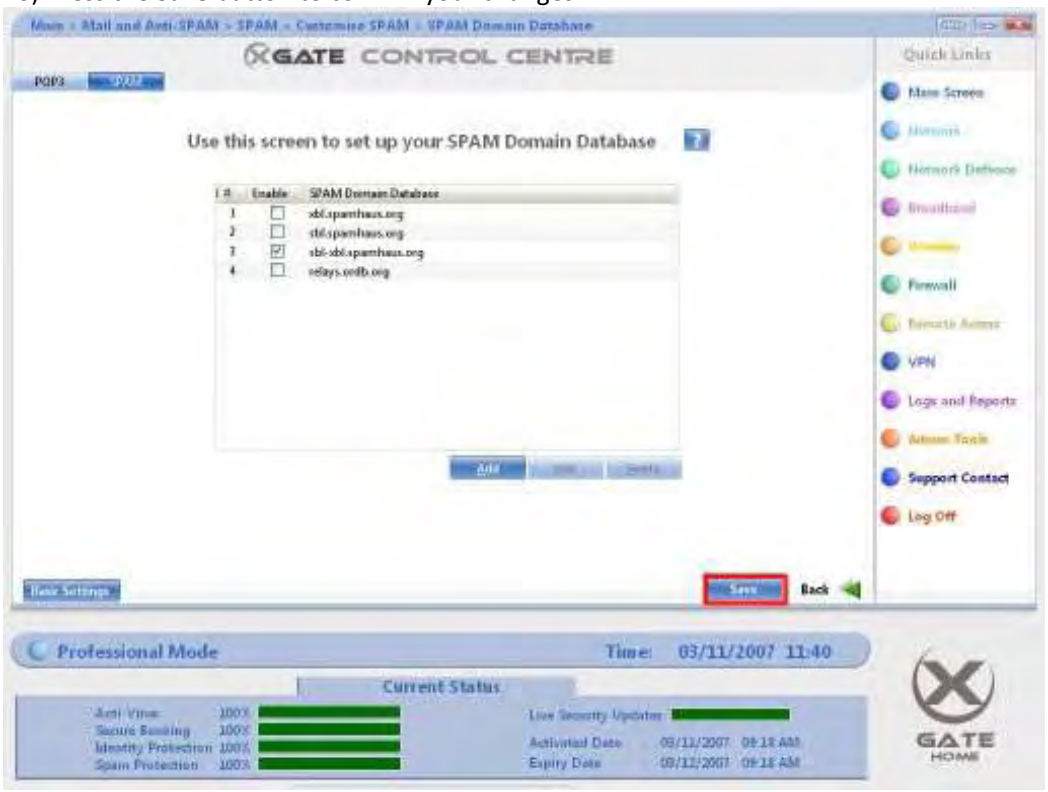
7) Press the Use Spam Domain Database Settings button.



8) Select the entry you wish to edit. This will highlight the entry.
9) Press the Delete button.



10) Press the Save button to confirm your changes.



Introduction

Spam URL Database

What is a Spam URL Database?

Spam URL databases differs from Spam domain Databases in one key area. Unlike Spam domain databases, URL databases detect Spam based on the web addresses in the message body of the e-mail.

In the context of e-mail, a message body is the main core of the e-mail where the message itself lies.

Used in conjunction with Spam Domain Databases, Spam URL databases can be effective against Spam e-mails.

Spam URL Database Details

To enter a Spam URL database, only the URL of the Spam URL database needs to be entered.

Adding a Spam URL Database

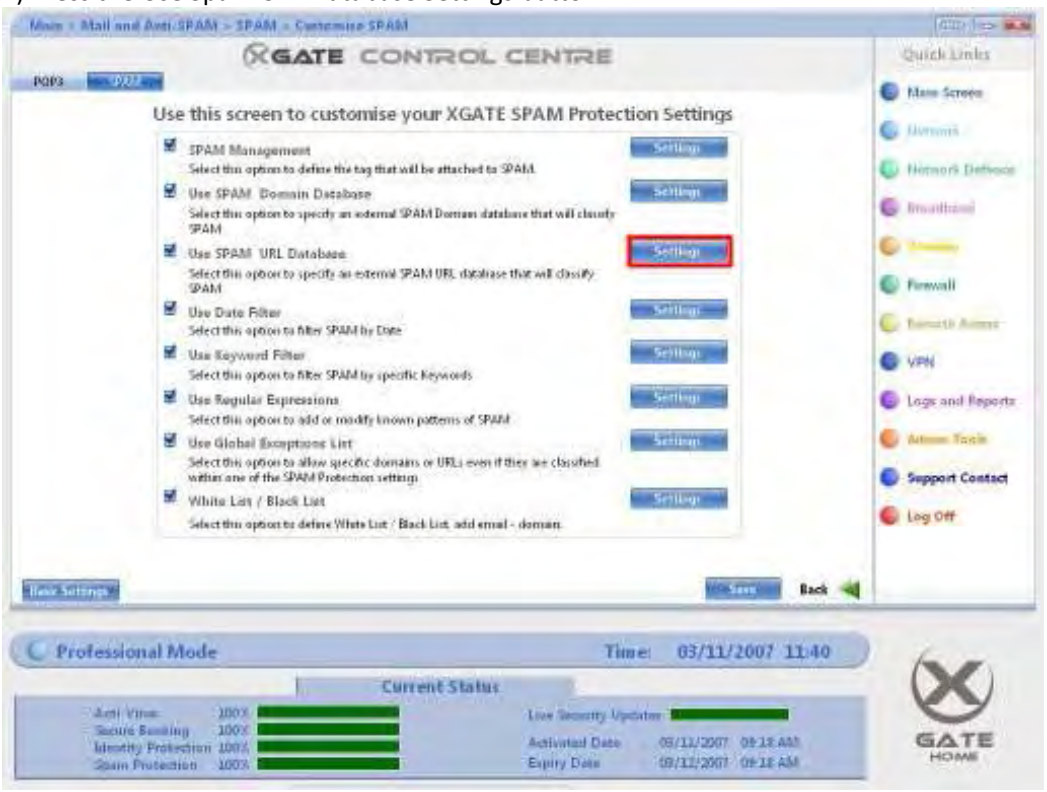
1) Press the Mail and Anti-spam button.

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

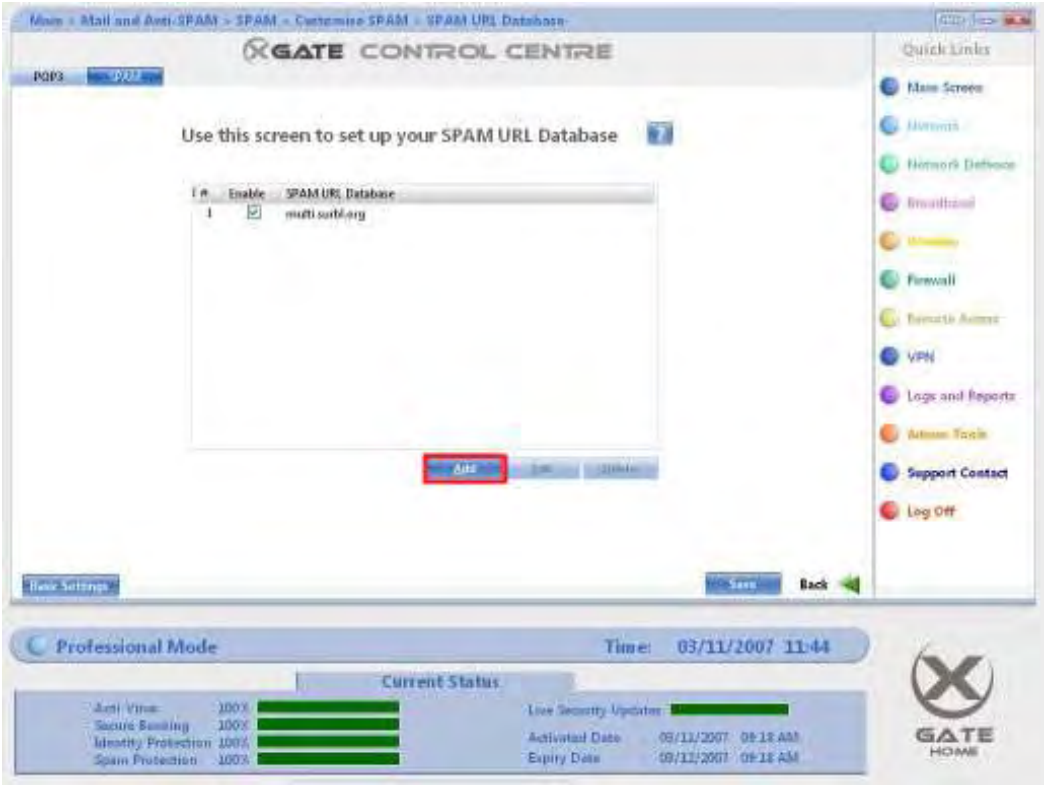
4) Ensure that Spam has been swiched on.
5) Click on Customise SPAM Protection.

3) Ensure that the Use Spam URL Database tick box is ticked.

4) Press the Use Spam URL Database Settings button.



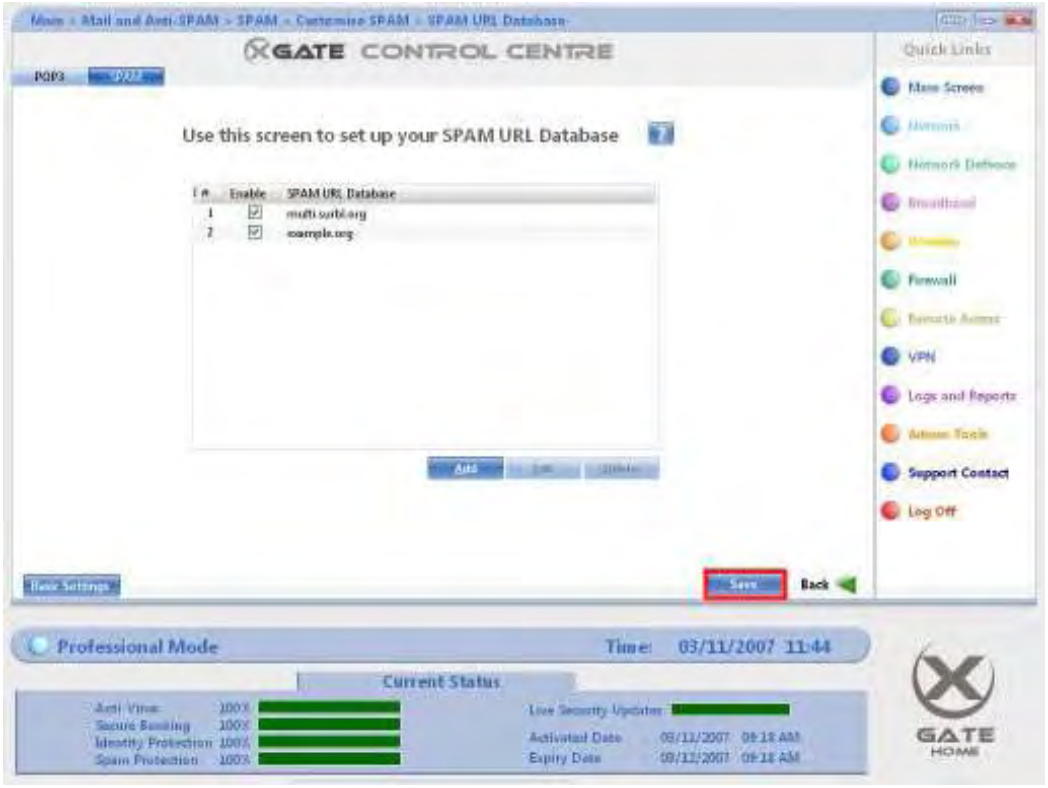
5) Press the Add button.



6) Type in the URL of the Spam URL database you wish to enter.

7) Press the OK button.

8) Press the Save button confirm your changes.



Editing a Spam URL database

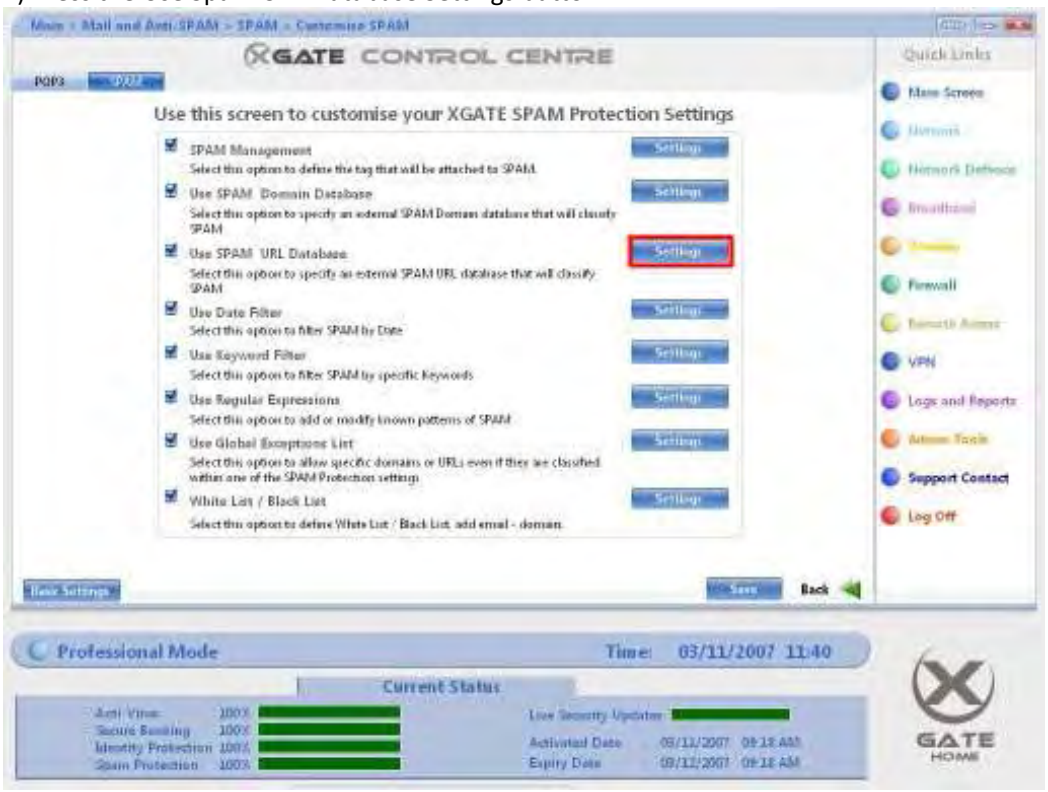
1) Press the Mail and Anti-spam button.

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

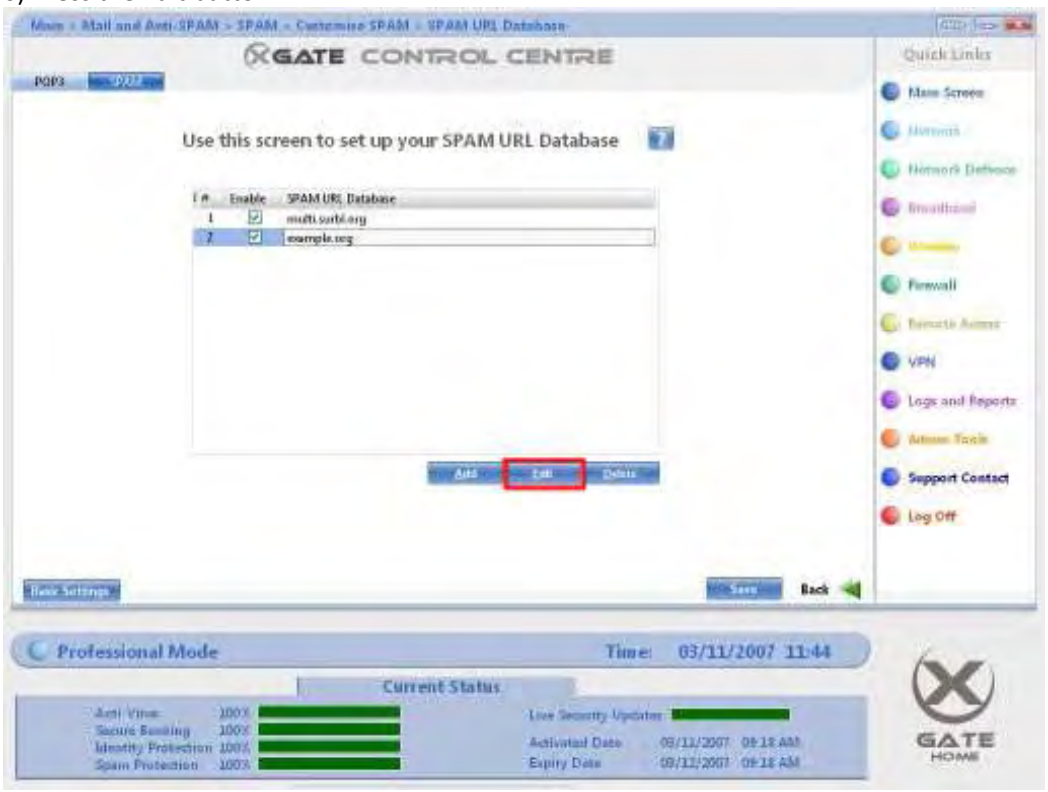
4) Ensure that Spam has been swiched on.
5) Click on Customise SPAM Protection.

3) Ensure that the Use Spam Domain URL tick box is ticked.

4) Press the Use Spam URL Database Settings button.

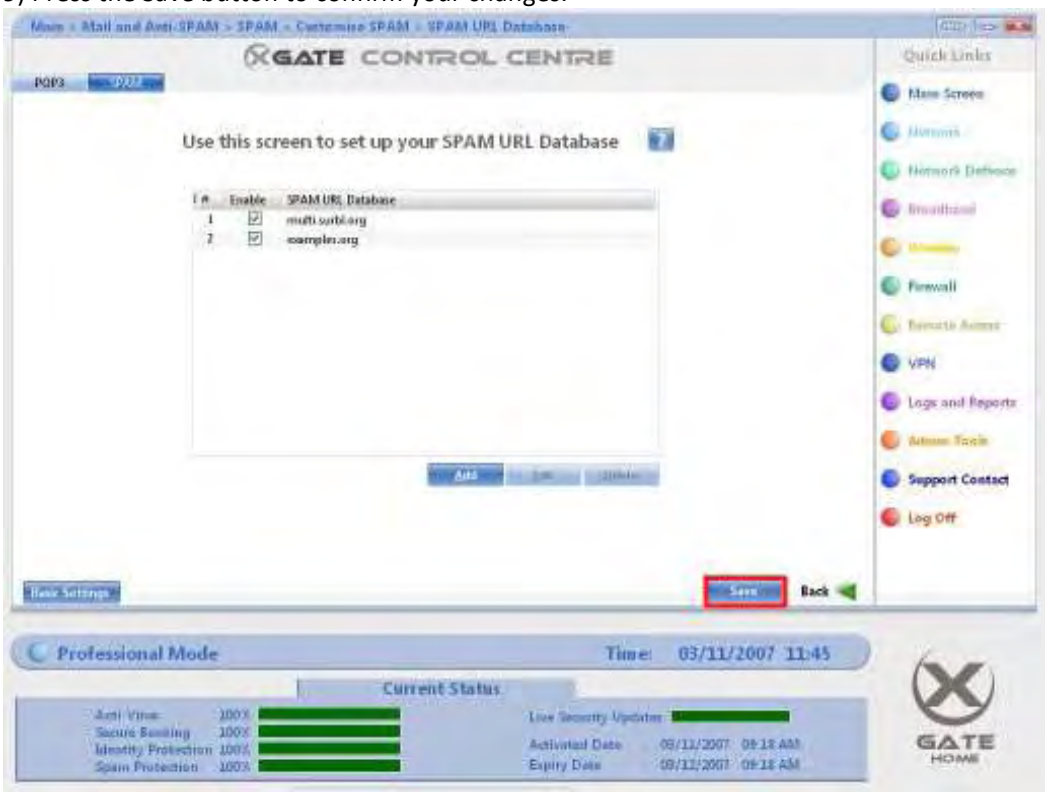


5) Select the entry you wish to edit. This will highlight the entry.
6) Press the Edit button.



7) Amend the URL of the Spam URL Database.
8) Press the OK button.

9) Press the Save button to confirm your changes.



Removing a Spam URL database

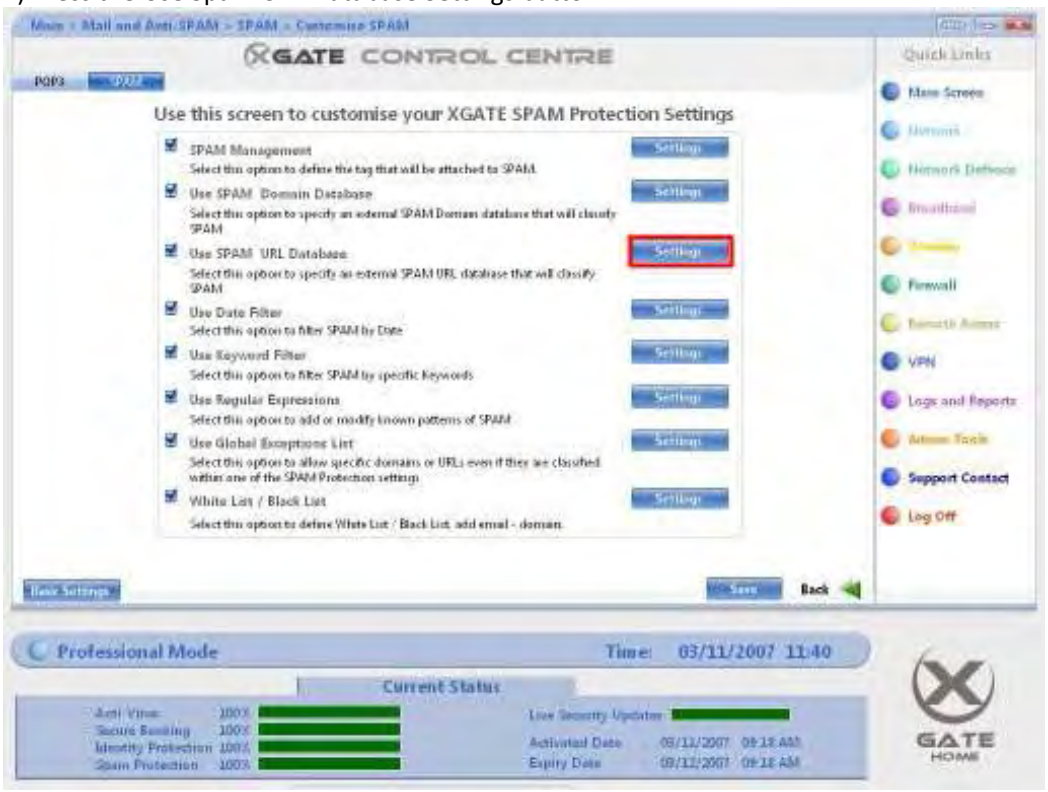
1) Press the Mail and Anti-spam button.

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

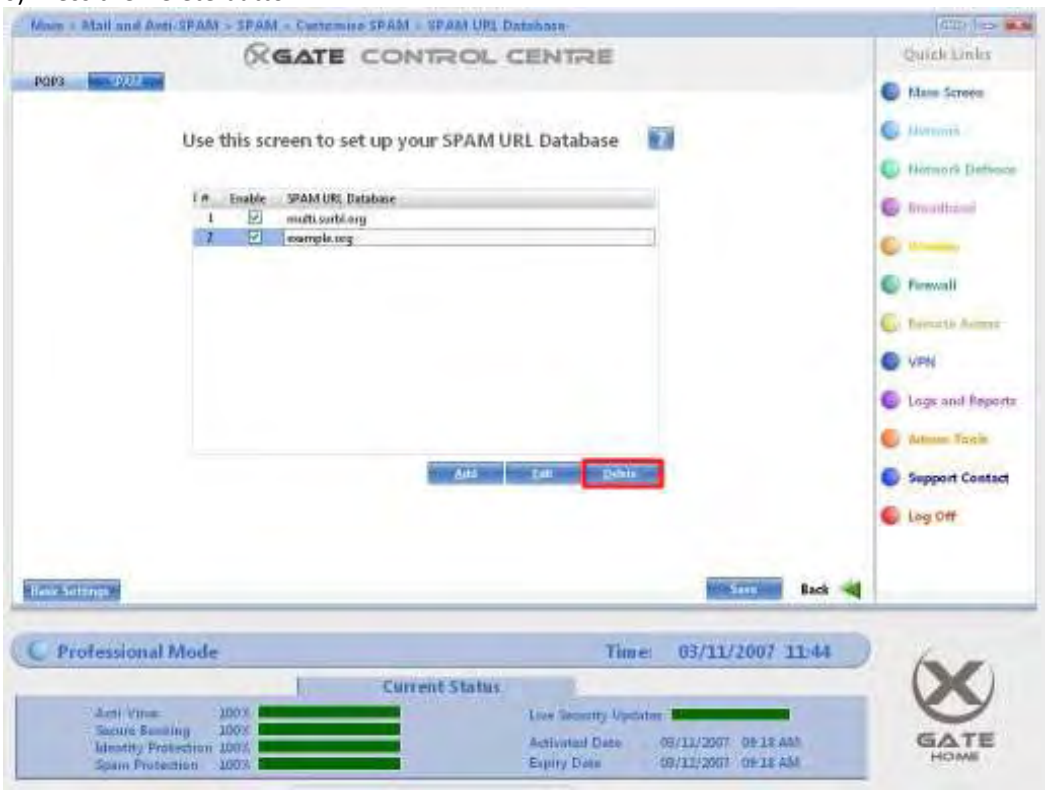
4) Ensure that Spam has been swiched on.
5) Click on Customise SPAM Protection.

3) Ensure that the Use Spam Domain URL tick box is ticked.

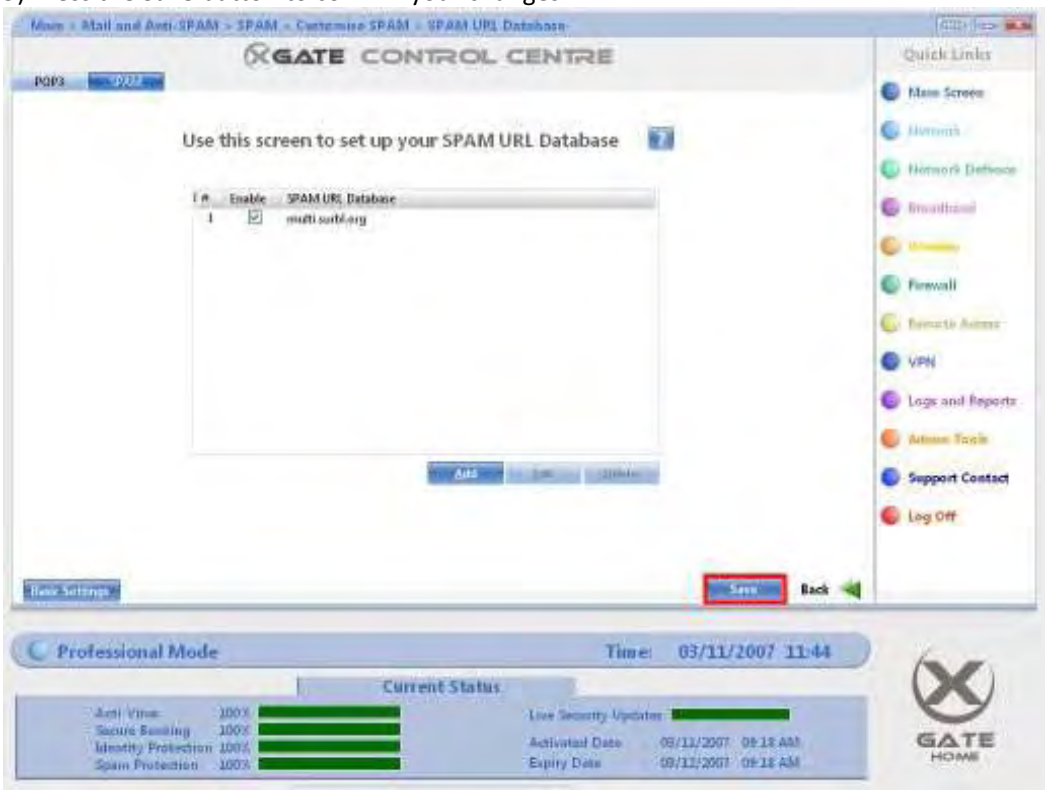
4) Press the Use Spam URL Database Settings button.



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

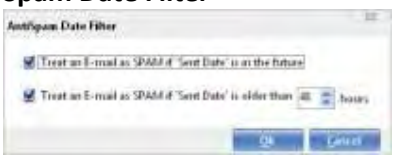


9) Press the Save button to confirm your changes.



Date Filter

Spam Date Filter



What is the Spam Date Filter?
The Spam Date Filter allows XGate to classify e-mails as Spam if the date of the e- mail seems irregular.

For example, if the date of an e-mail is sent in the future it can be seen as Spam.

Spam Date Filter Properties
Within the Spam Date Filter you can set the following date filters:

Treat an e-mail as SPAM if ‘Sent Date’ is in the future.

Treat an e-mail as SPAM if ‘Sent Date’ is older than X hours.
(You can set the amount of hours .)