BT Global Solutions

Y&HGFL

Proxy settings advice

Document Version 1

Table of Contents

1. Introduction 3
   1.1 Purpose and Scope 3
2. Status 3
   2.1 Ownership Details 3
3. Solution Overview 3
   3.1 No local DNS server onsite 3
   3.2 Local DNS server onsite 3
   3.3 Current proxy server settings 4
4. Scenarios Covered 4
   4.1 No on site proxy server and no proxy configured within the users browser. 4
   4.2 No on site proxy server and the proxy server configured within the users browser. 4
   4.3 Proxy server onsite with no upstream config. 4
   4.4 Proxy server onsite with no upstream config and local authentication. 5
   4.5 Onsite proxy server with upstream server set. 5
   4.6 Onsite proxy server with upstream server and authentication set. 5
   4.7 Onsite proxy server with upstream config and local authentication and filtering. 5
5. Proxy Configurations Within The Users Browser 6
   5.1 Standalone PC's onsite 6
   5.2 PC's onsite are members of a domain 8
6. IIS Proxy 2.0 Configuration 13
7. Microsoft ISA Server Configuration 18
8. Trouble Shooting Guide 26
9. Revision History 27

--- end of table of contents ---

Y&HGFL : Proxy Settings Guide

1. INTRODUCTION

1.1 Purpose and Scope

This document has been produced to assist the LEA's within the Y&HGFL that take their ISP services from the Leeds POP (Point of Presence) in Leeds Westgate ATE.

2. STATUS

2.1 Ownership Details

All documents to which this instruction applies shall have their status shown in this section.

Owner	Tim Needham	**Title**	Solution Architect
Tel:	01977 594528	**e-mail**	Tim.needham@bt.com
Security Classification	N/A	**Pilot Review Date**	N/A
Controlled Release	*No*	**Periodic Review Period/Date**	**N/A**

3. SOLUTION OVERVIEW

In this document we will try and document most of the common configuration scenarios and the expected behaviour of the browser in each case.

3.1 No local DNS server onsite

The first point to note is the importance that DNS is configured correctly; if you have no DNS server on your site then all clients should be set to use 10.0.4.21 and 10.0.4.22 as their DNS servers and no others.

This will enable you to use the names we provide for our services. If you choose not to follow this advice then you have problems accessing sites on the internet. Additionally you will have to change the settings when the services we offer have their addresses changed. The whole point of using an address is to prevent you as a user from having unnecessary work.

3.2 Local DNS server onsite

If you have a DNS server locally on your site your clients should be set to use your local DNS server and the DNS server should be configured to forward requests to 10.0.4.21 and 10.0.4.22 and no others. If the options to configure forwarding on your DNS server are greyed out check for a '.' Zone within the list of zones, if this zone exists delete it and restart the DNS service. Full configuration of DNS is beyond the scope of this document.

This will enable you to use the names we provide for our services. If you choose not to follow this advice then you have problems accessing sites on the internet. Additionally you will have to change the settings when the services we offer have their addresses changed. The whole point of using an address is to prevent you as a user from having unnecessary work.

©BT Global Solutions, 2005

3.3 Current proxy server settings

proxy.bty-h.org.uk using port 80 - This challenges for a username and password.

primaryproxy.bty-h.org.uk using port 80 - This provides automatic filtering at a primary level.

secondaryproxy.bty-h.org.uk using port 80 - This provides automatic filtering at a pre 16 level.

shefproxy.bty-h.org.uk using port 80 - This is a duplicate of secondaryproxy and should not be used.

The associated IP addresses for these proxies are to be changed shortly which is why we are emphasizing the use of the names!

4. SCENARIOS COVERED

1. No on site proxy server and no proxy configured within the users browser.
2. No on site proxy server and the proxy server configured within the users browser.
3. Proxy server onsite with no upstream config.
4. Proxy server onsite with no upstream config and local authentication.
5. Onsite proxy server with upstream server set.
6. Onsite proxy server with upstream server and authentication set.
7. Onsite proxy server with upstream config and local authentication and filtering.

4.1 No on site proxy server and no proxy configured within the users browser.

In this scenario when a user opens a browser they will be prompted for a user ID and password. They will not be challenged again for a username or password until there is no internet browsing activity for a period of over a minute. After a minute of inactivity, whether they have kept there browser window open or not, they will be challenged again for a username and password.

4.2 No on site proxy server and the proxy server configured within the users browser.

If the proxy and DNS servers are correctly configured on the users PC (refer sections 5, 6, 7) when they open a browser window they will be challenged for a username and password they should then be able to browse the internet inside this browser window without being challenged again for a userID and password. If the user opens a new browser window from within the current browser window they will not be challenged and should be able to continue browsing. If the user however opens a new instance of IE from either the ‘start menu’ the ‘quick launch bar’ or a shortcut on the desktop they will then be challenged again for a username and password.

4.3 Proxy server onsite with no upstream config.

In this configuration the first user who opens a web browser at the beginning of the day will be prompted for a user name and password, this userID is then cached within the proxy server and all the other users on the network will connect without being challenged, they will all effectively be using the same user ID. If there is a period of greater than a minute of inactivity across all the users on the network then the next user who opens a web browser or clicks on a web link will be challenged for a user ID and password. It will then be this user ID that is cached and used until the timeout occurs again.

©BT Global Solutions, 2005

4.4 Proxy server onsite with no upstream config and local authentication.

If your local proxy server is configured to challenge user for a user ID and password, (for IIS3/Proxy 2.0 ref. section 6, for ISA 2000 server ref. section 7, for ISA 2004 server ref. section 8) then when a user first opens a web browser they will be challenged for a username and password by your local proxy server then they will be challenged for a userID and password by our proxy server. The challenge and response from our proxy server will be cached inside your local proxy and subsequently when then next user on the network opens a web browser they will only be challenged once, by your local proxy server.

This is not an advisable or desirable configuration and if you are seeing multiple authentication requests in this manner check the configuration of your proxy server.

4.5 Onsite proxy server with upstream server set.

If you have configured your proxy server to point to the upstream proxy server in Leeds (ref. Sections 5, 6, 7) it can lead to some unexpected results. When a user opens a web browser they may receive a web page telling them that upstream authentication has failed and the page cannot be displayed. Or they may be challenged for a userID and password. If they are challenged for a userID and password then this configuration will behave in the same manner as 3. Proxy server onsite with no upstream config.

4.6 Onsite proxy server with upstream server and authentication set.

Refer to sections 5, 6, 7 on how to configure this in either IIS3/Proxy 2.0 or Microsoft ISA sever.

In this configuration the users will never be challenged for a userID and password and everyone who uses the network will be authenticated to our proxy server in Leeds using the credentials that have been setup within your local proxy server. All of the web content filtering will be applied at the level of the user account configured within your local proxy server.

4.7 Onsite proxy server with upstream config and local authentication and filtering.

This is a configuration that could be used to give you autonomous control of who has access to the internet and the filtering levels applied.

If you configure you local proxy server with the upstream setting but in the user account field use the proxy pass-through account this would allow all users through with no challenge for a userID and completely unfiltered access to the internet. It would then be possible to add to your proxy server your own content filtering software which would be under your local control; you would also be required to turn on local authentication on your proxy server.

In this configuration all users would be challenged for a username and password by your local proxy server and all content filtering would be provided by your local content filtering system. This configuration would give you full local control over internet access but it would also add a great deal of management and extra support to your local network environment; however it may be a configuration that is appropriate for some installations.

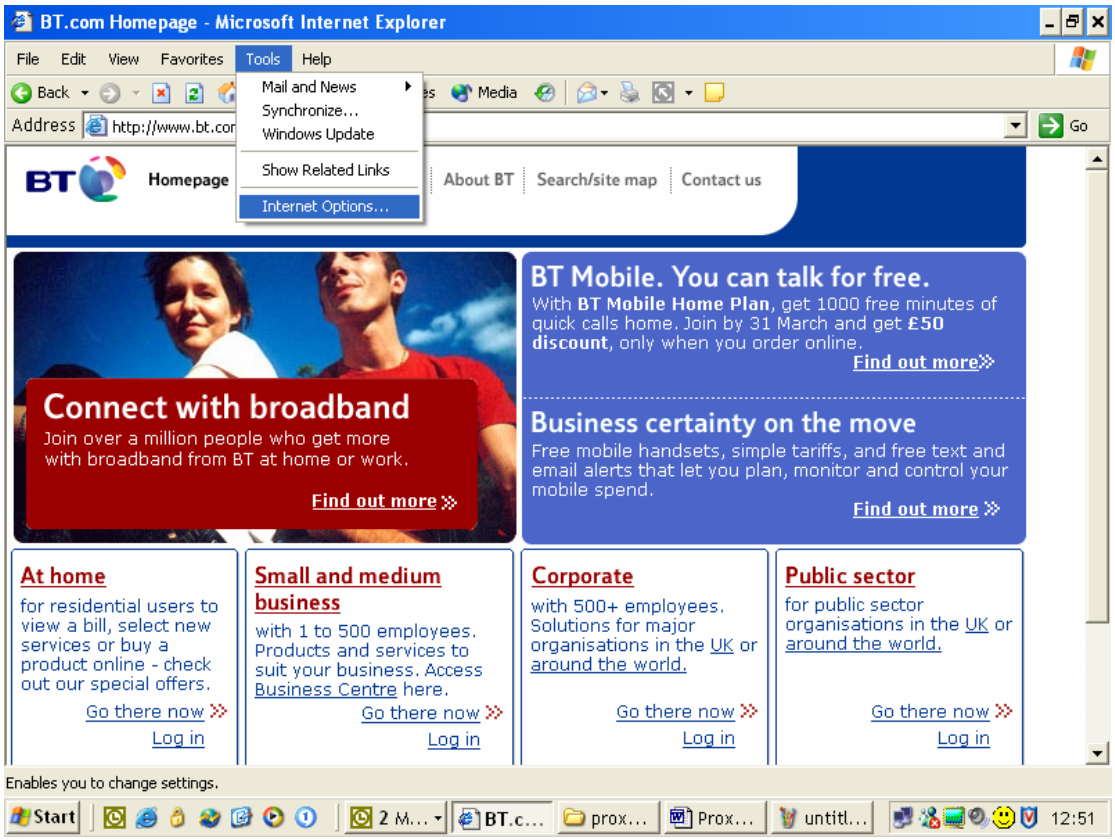
©BT Global Solutions, 2005

5. PROXY CONFIGURATIONS WITHIN THE USERS BROWSER

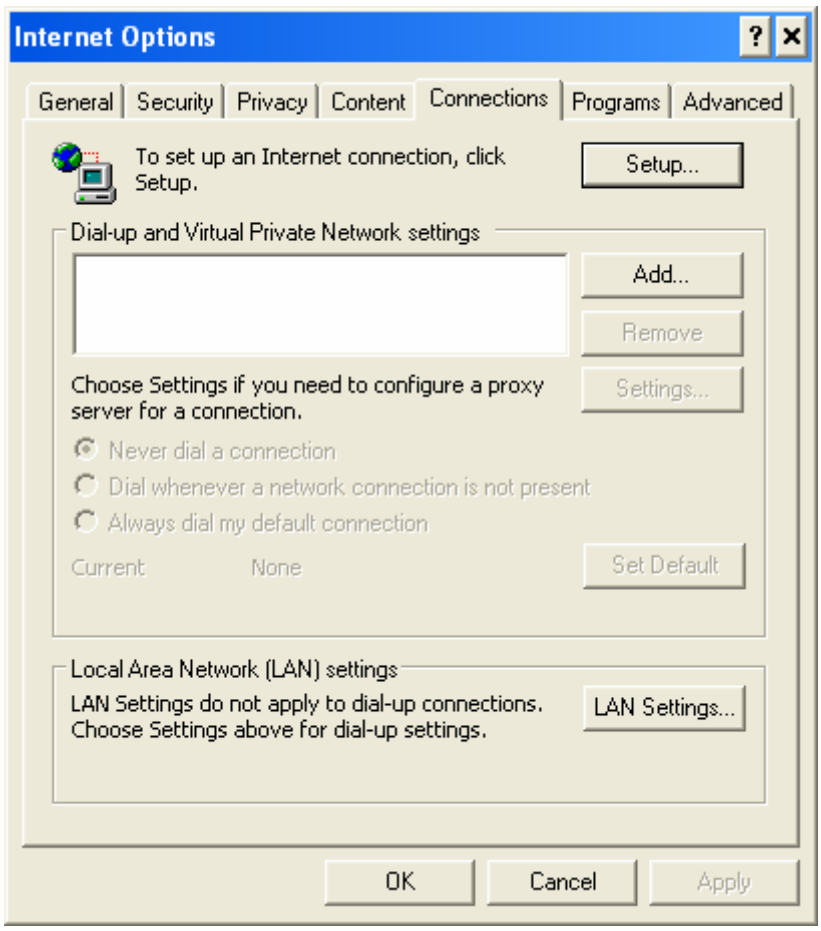
5.1 Standalone PC's onsite

If all of the user PC's on your network are configured in a stand-alone manner i.e. not part of a Windows 2000 domain, then this configuration change will have to be manually made on each of the users PC's.

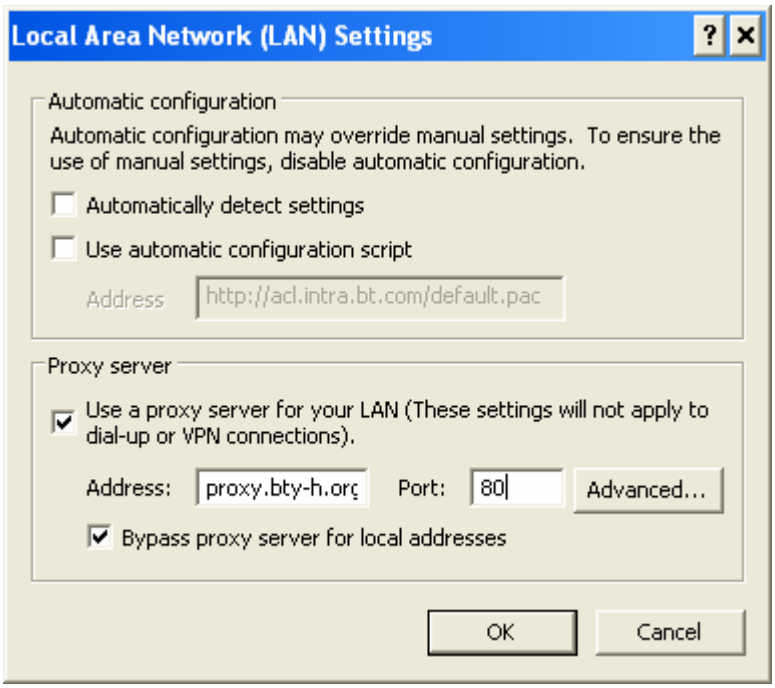
Open the Web browser on the PC, this document assumes that Internet Explorer is being used, however the process is very similar for Netscape and other web browsers. Go to the tools menu:



Click on the Internet options menu item and select the ‘Connections’ tab:



Now click on the LAN settings button:



Untick 'Automatically detect settings' and 'Use automatic configuration script', tick 'Use a proxy server for your LAN'. In the address field type in proxy.bty-h.org.uk and in the port field 80, if you have a local proxy server, in the address field fill in the name or the IP address of your proxy server.

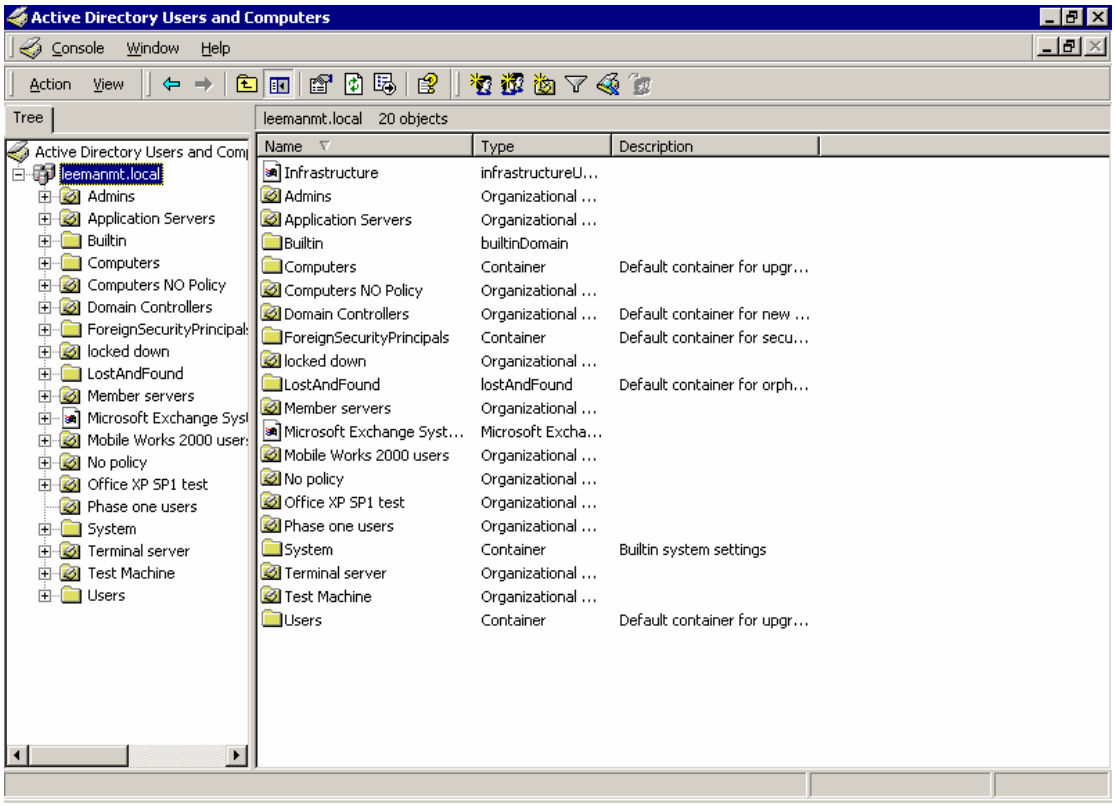
Tick the 'Bypass proxy server for local addresses' tick box and click 'OK'.

5.2 PC's onsite are members of a domain

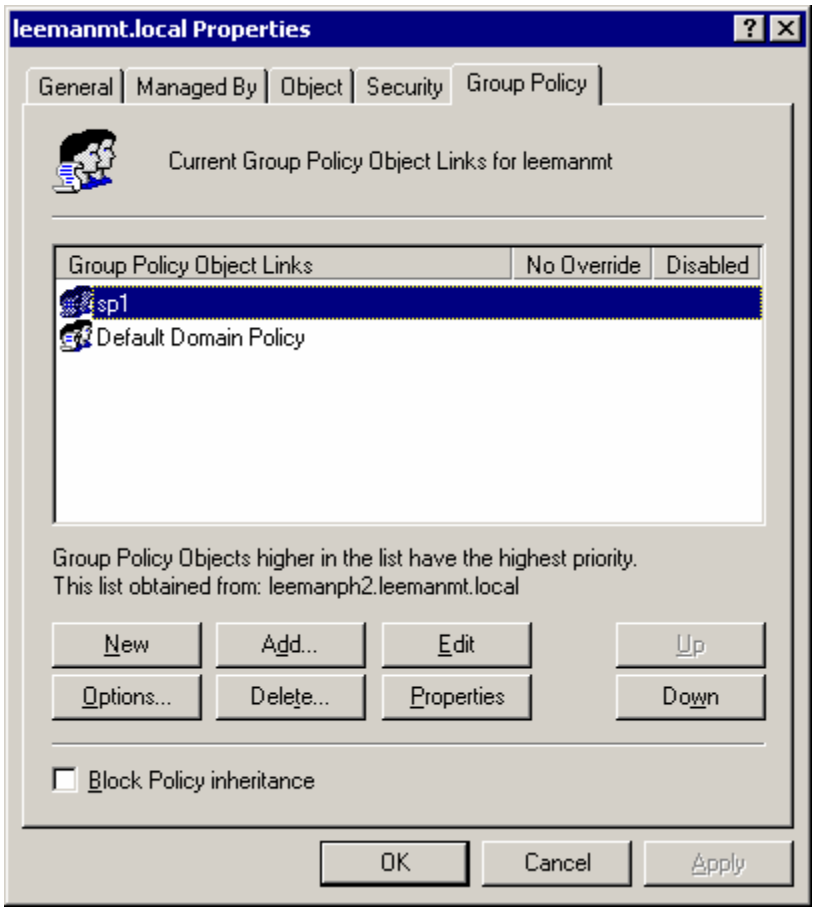
If all of the PC's in your network are part of a Windows 2000 domain the change can be made to all of the users PC's centrally using Windows 2000 group policy.

Open Active Directory users and Computer from the Administrative Tools menu:

©BT Global Solutions, 2005

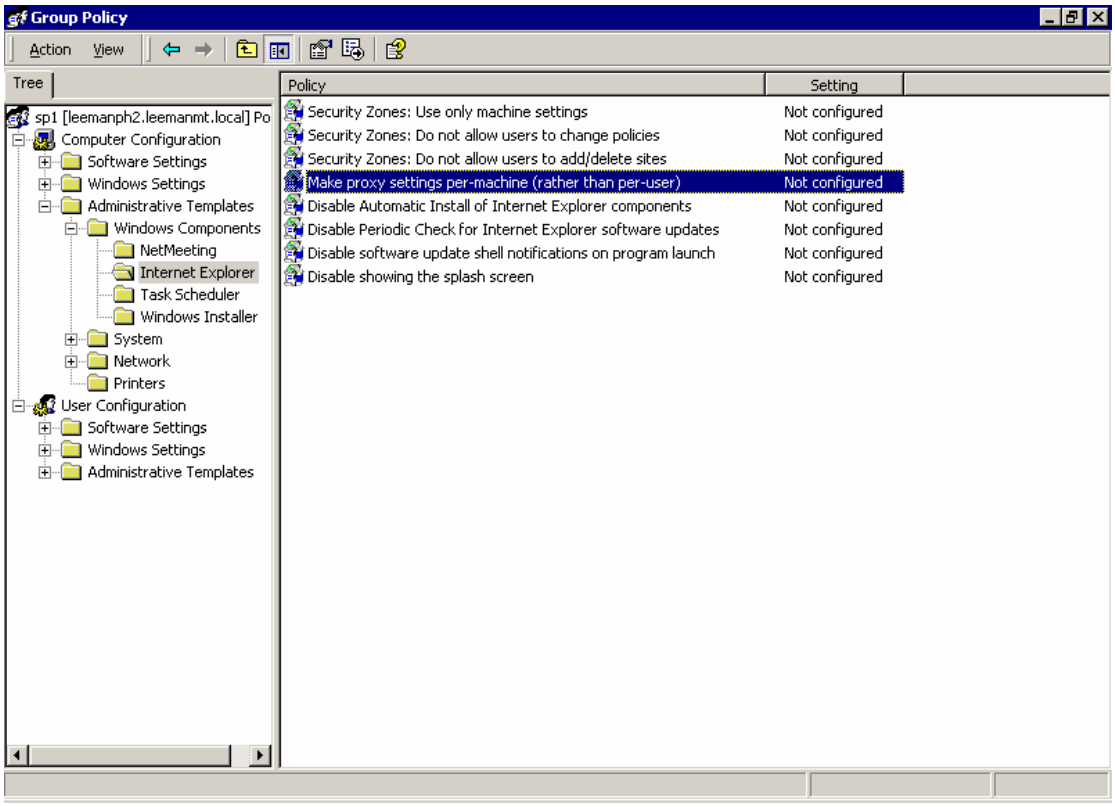

Active Directory Users and Computers
Console Window Help
Action View
Tree
leemanmt.local 20 objects
Active Directory Users and Comp
leemanmt.local
Admins
Application Servers
Builtin
Computers
Computers NO Policy
Domain Controllers
ForeignSecurityPrincipal
locked down
LostAndFound
Member servers
Microsoft Exchange Syst
Mobile Works 2000 user
No policy
Office XP SP1 test
Phase one users
System
Terminal server
Test Machine
Users
Name
Type
Description
Infrastructure infrastructureU...
Admins Organizational ...
Application Servers Organizational ...
Builtin builtinDomain
Computers Container Default container for upgr...
Computers NO Policy Organizational ...
Domain Controllers Organizational ... Default container for new ...
ForeignSecurityPrincipals Container Default container for secu...
locked down Organizational ...
LostAndFound lostAndFound Default container for orph...
Member servers Organizational ...
Microsoft Exchange Syst... Microsoft Excha...
Mobile Works 2000 users Organizational ...
No policy Organizational ...
Office XP SP1 test Organizational ...
Phase one users Organizational ...
System Container Builtin system settings
Terminal server Organizational ...
Test Machine Organizational ...
Users Container Default container for upgr...

Right click on your domain at the top of the right hand window and select properties, now select the 'Group policy' tab:

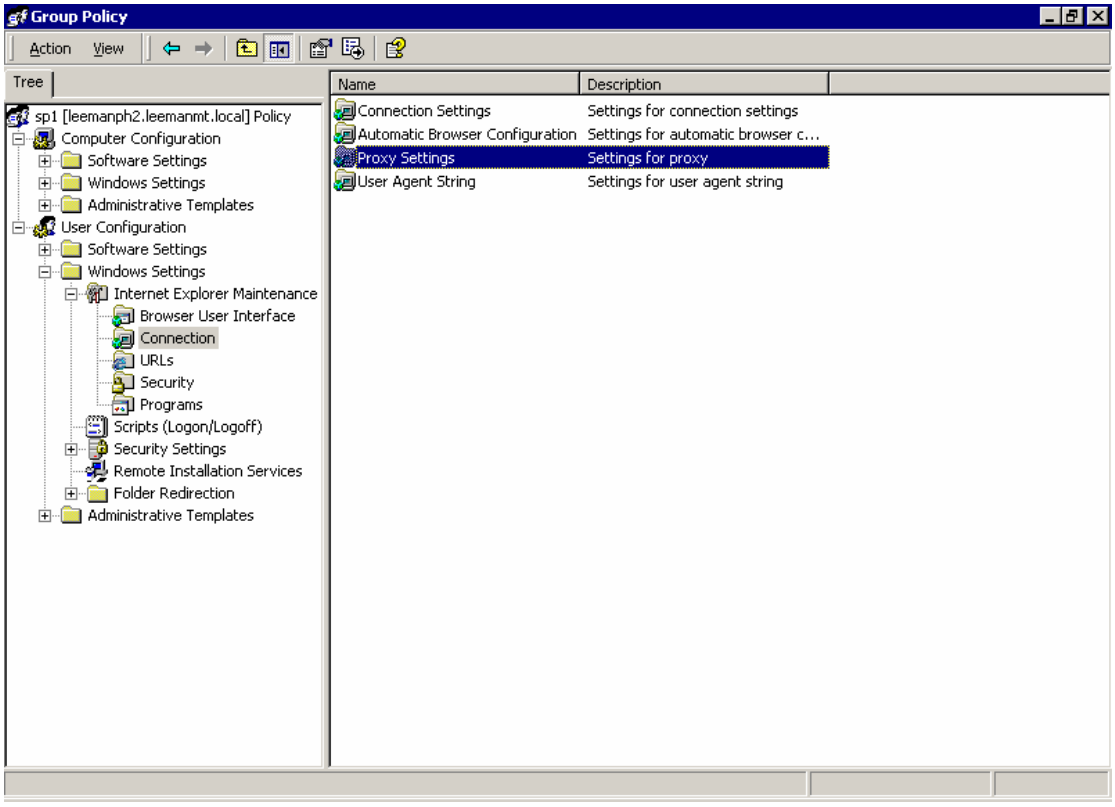


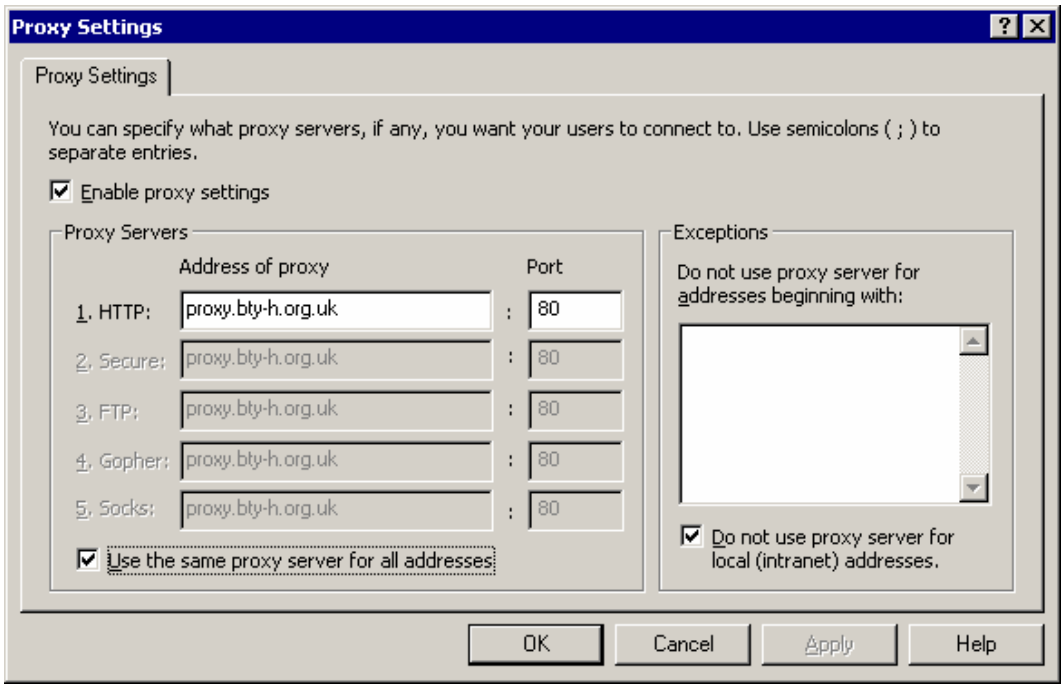
Select the 'Default Domain Policy' and click edit.

Expand the 'Computer Configuration', 'Administrative Templates', 'Windows Components' and select 'Internet Explorer' in the left-hand window. Now double click on the 'Make proxy setting per machine' option in the right hand window and set the option to 'Enable'.



Now in the left-hand pane expand ‘User Configuration’, ‘Windows Settings’, ‘Internet Explorer Maintenance’ and select ‘Connection’. Now double click ‘Proxy Settings’ in the right-hand window.





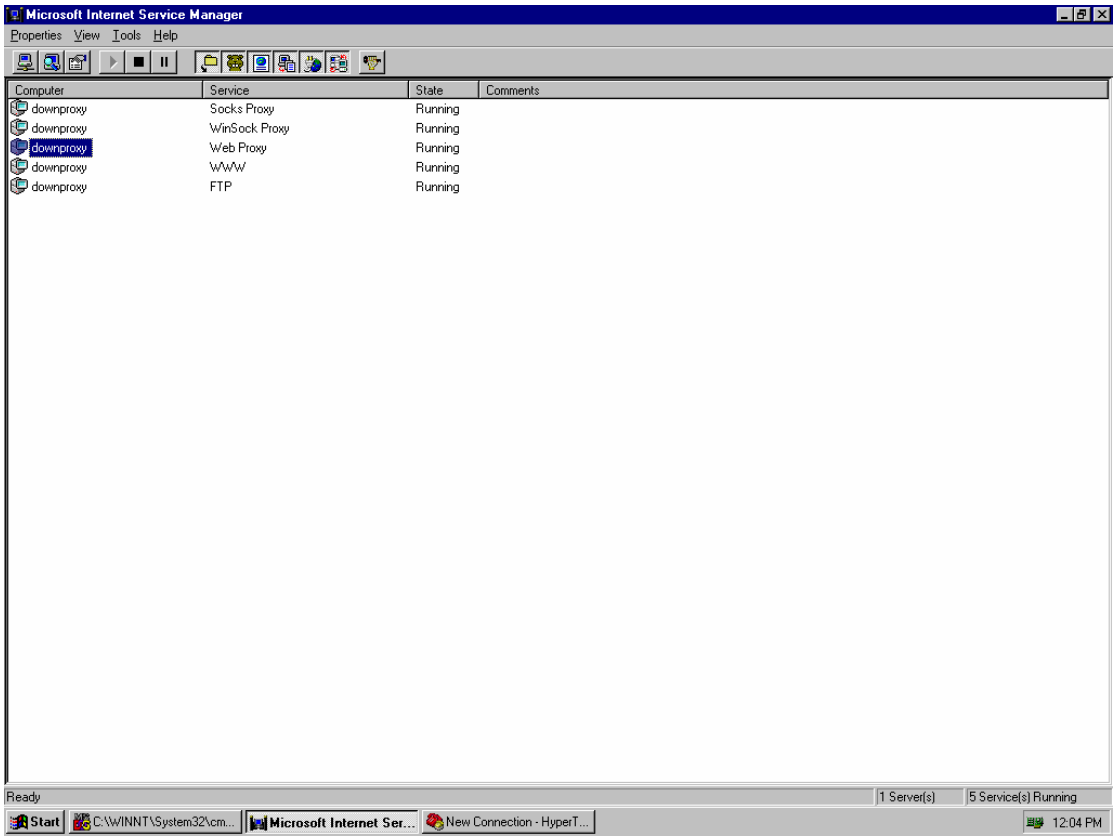
Tick the 'enable proxy settings' box in line 1. type in proxy.bty-h.org.uk or the name of your local proxy server, fill in the port 80 for the Leeds proxy server, tick the 'Use the same proxy sever for all addresses' and click 'OK'. Close the group policy window and the Active directory users and computers window. This new policy will be implemented when the users PC's are rebooted.

©BT Global Solutions, 2005

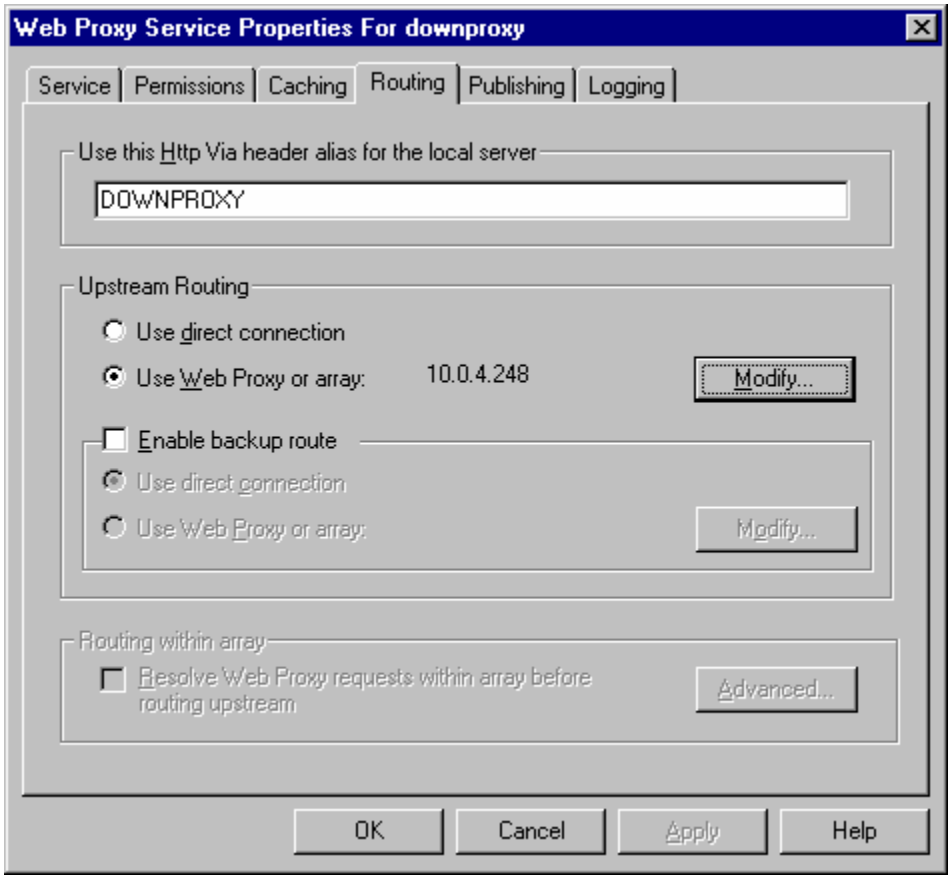
6. IIS PROXY 2.0 CONFIGURATION

Configuring Upstream Proxy with a user account

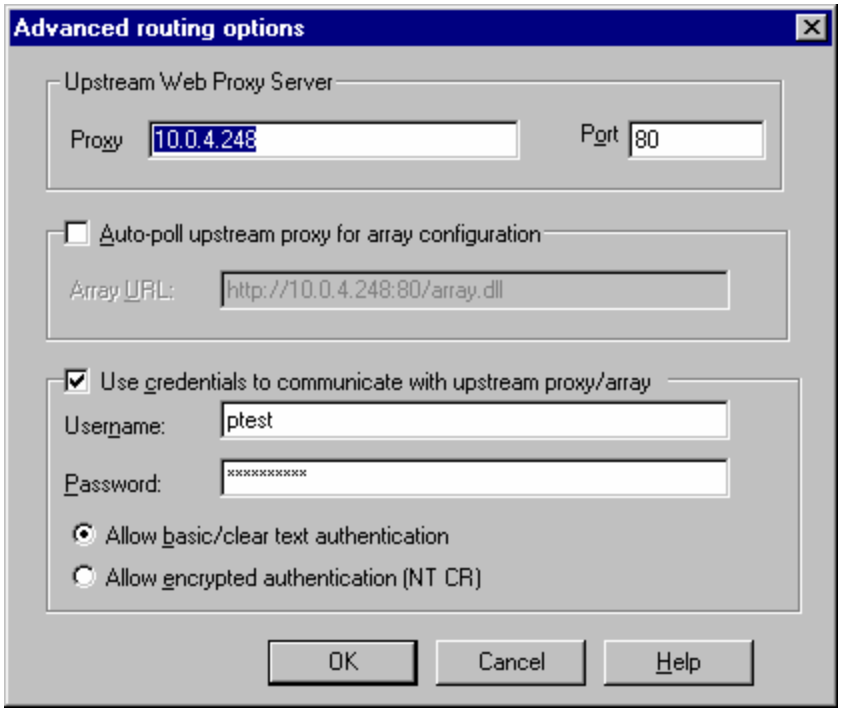
Open the IIS3 management console:



Double click on the Web Proxy Icon for your server to open the general configuration page, now select the routing tab:



Select the radio button ‘Use Web Proxy or array’ and click the ‘Modify’ button:



In the Proxy field enter proxy.bty-h.org.uk and port 80. Ensure the 'Auto-poll upstream proxy' check box is unticked.

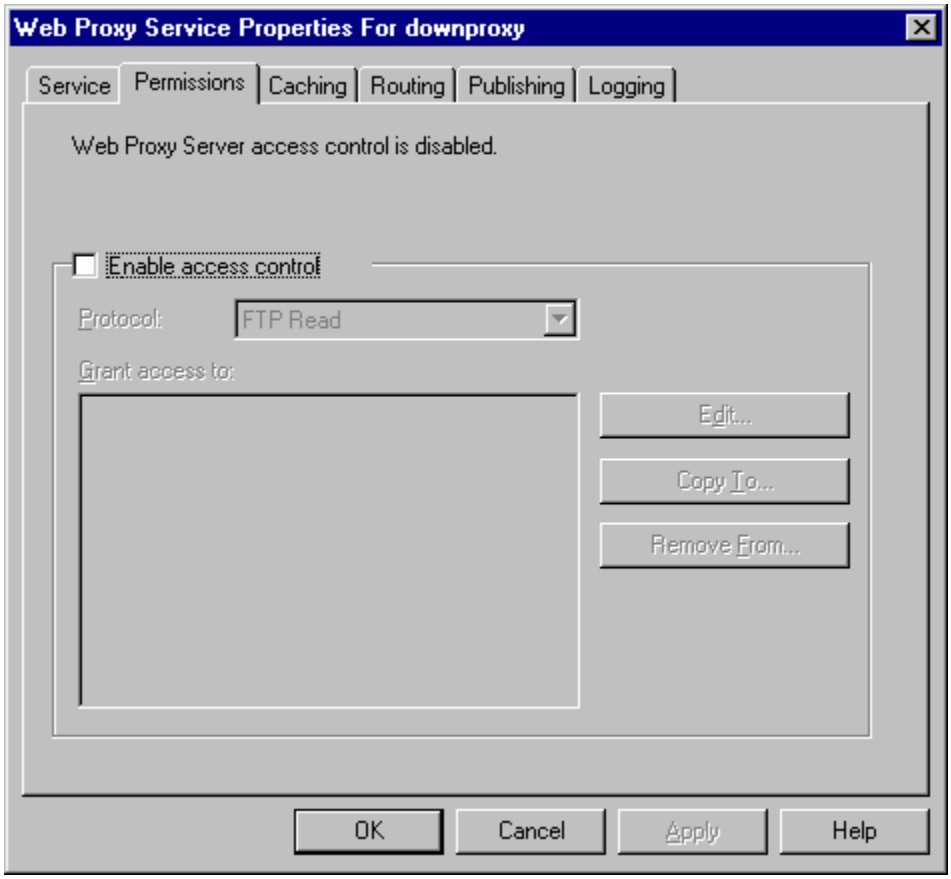
Tick the 'Use credentials to communicate with an upstream proxy' check box. Fill in an appropriate username and password in the fields remember that this is the user account all of your users will be passed to the content filtering system with, so ensure it is at a level you are happy with all of your users being filtered at.

Select the 'Allow basic or clear text' radio button and then click ok.

All of your users should now be able to browse the internet without being challenged for a username and password.

Configuring / Checking the local authentication setting of the proxy server

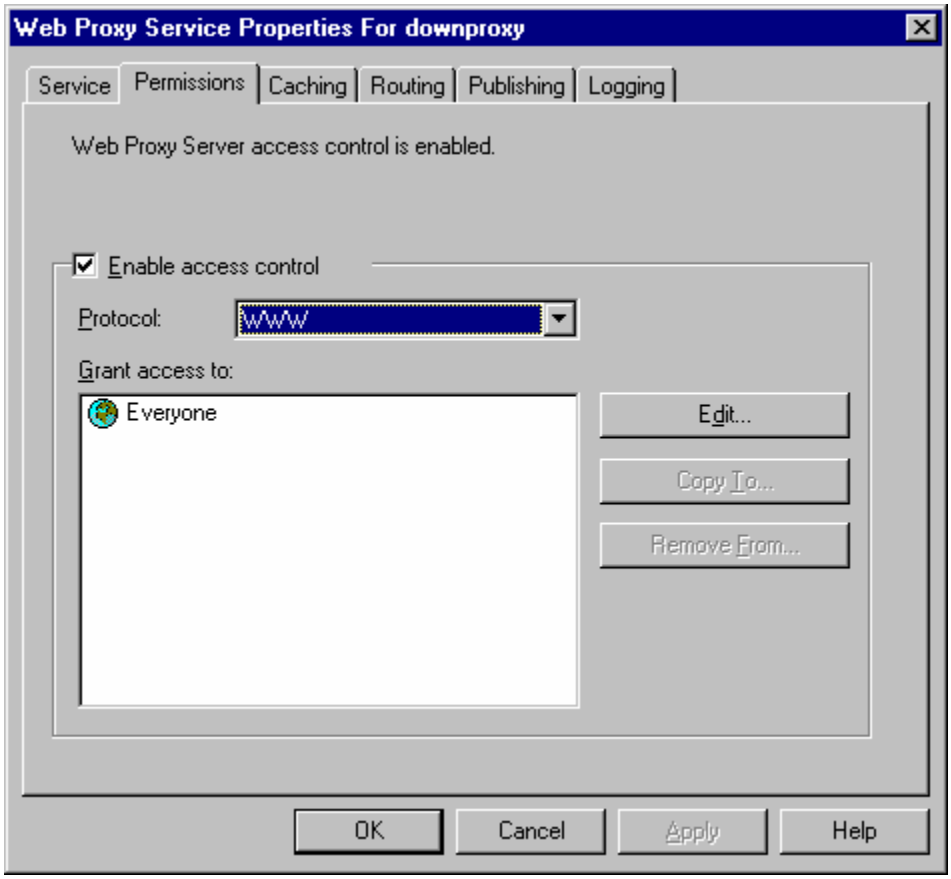
Open the IIS3 management console and double click on the Web Proxy Icon for your server to open the general configuration page and select the 'permissions' tab:



If you do not want your proxy server to challenge users for a password ensure that the 'Enable access control' tick box is unchecked.

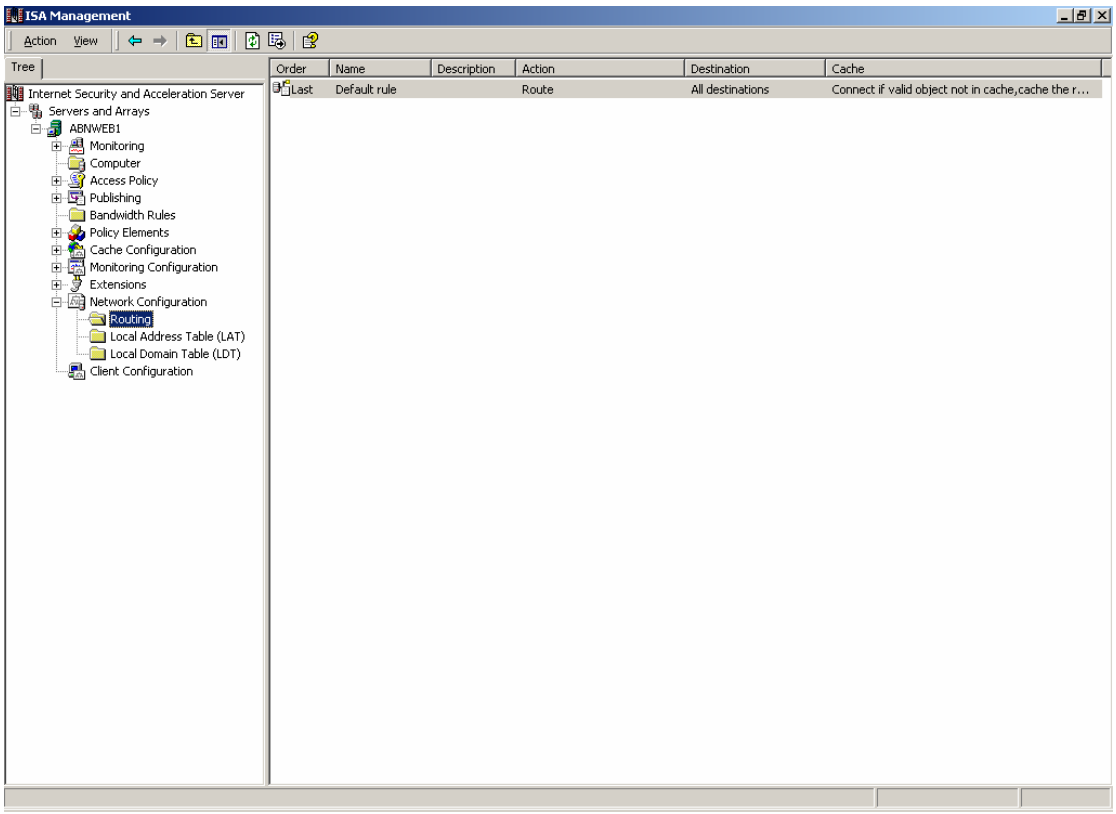
If you want your local proxy server to challenge users ensure the tick box is selected, you can then select a protocol and select the user accounts or groups that you want to grant permissions to have access:

©BT Global Solutions, 2005

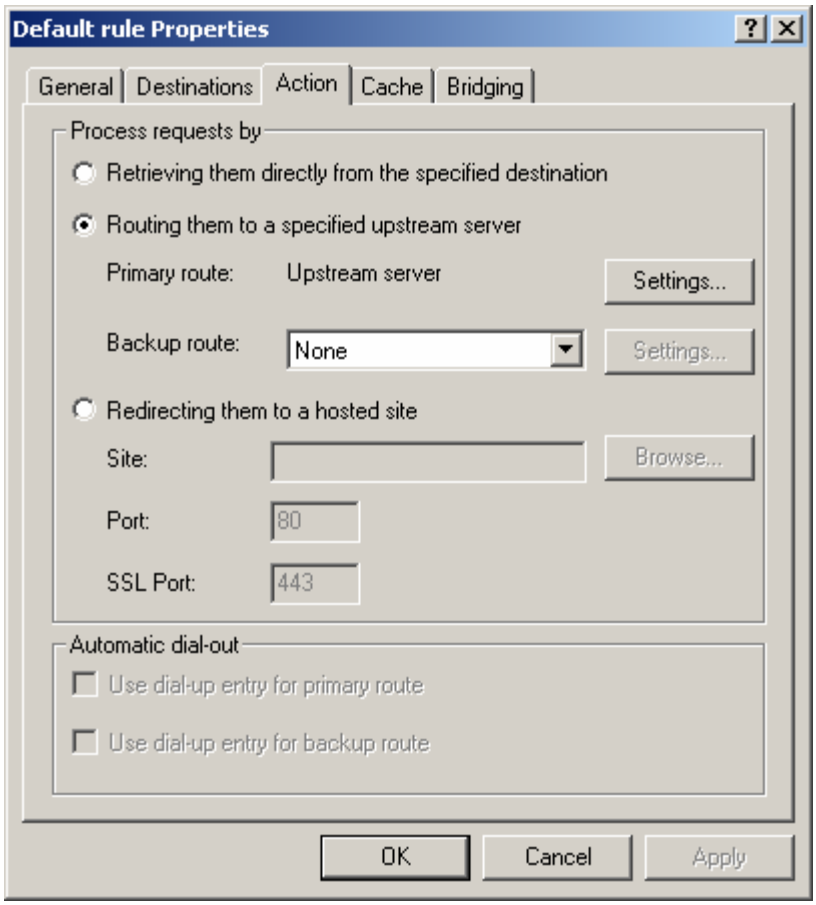

Web Proxy Service Properties For downproxy
Service
Permissions
Caching
Routing
Publishing
Logging
Web Proxy Server access control is enabled.
Enable access control
Protocol:
WWW
Grant access to:
Everyone
Edit...
Copy To...
Remove From...
OK
Cancel
Apply
Help

7. MICROSOFT ISA SERVER 2000 CONFIGURATION

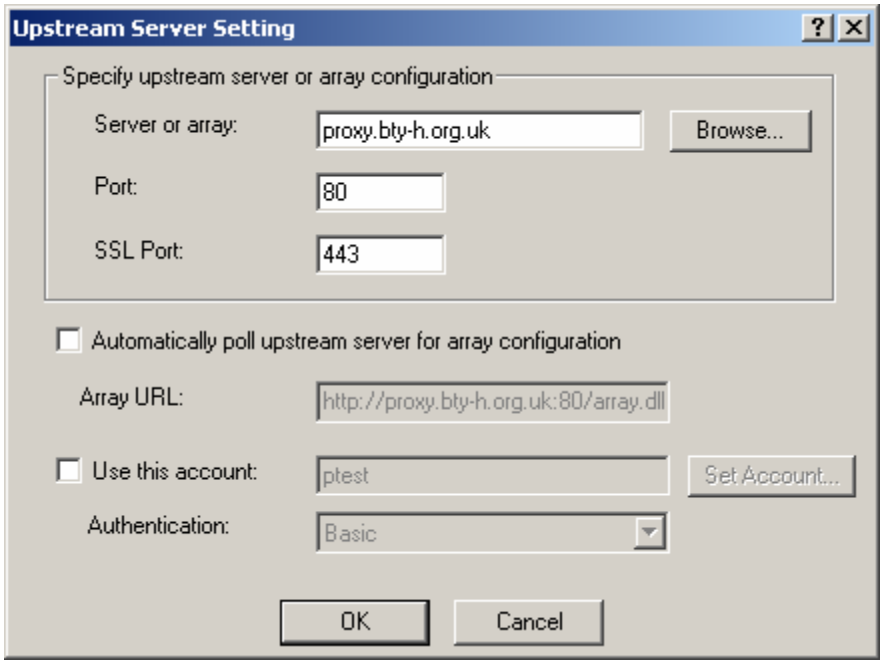
Open the ISA management console and under your proxy server expand the 'Network configuration' section and select the 'Routing' folder. There should only be a single rule visible in the right-hand window, double click it:



On the dialog box that opens select the ‘Action’ tab:

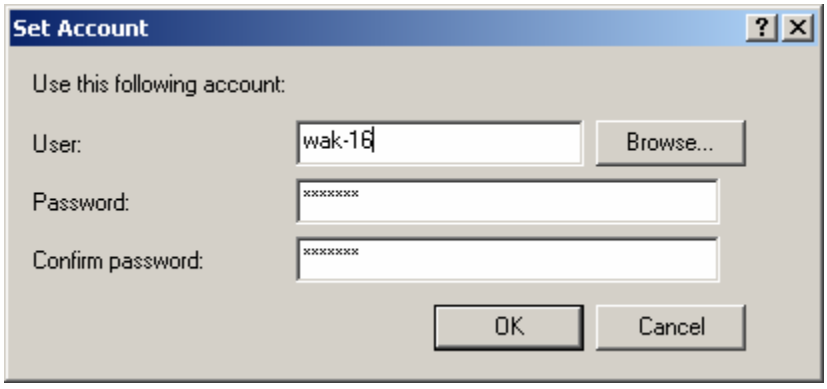


Select the ‘Routing them to a specified upstream server’ radio button and then click the settings button:



In the 'Server' field enter proxy.bty-h.org.uk the port is 80 and the SSL port is 443.

Tick the 'Use this account' check box and click the 'Set Account' button:



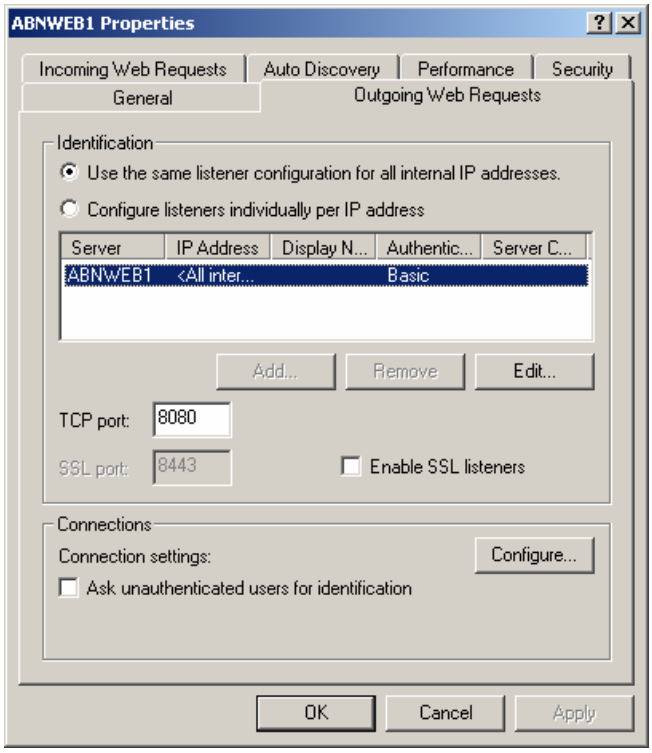
Fill in an appropriate username and password in the fields remember that this is the user account all of your users will be passed to the content filtering system with, so ensure it is at a level you are happy with all of your users being filtered at. Click 'OK' and on the previous window ensure that the 'Authentication' drop down is set to 'Basic'.

All of your users should now be able to browse the internet without being challenged for a username and password.

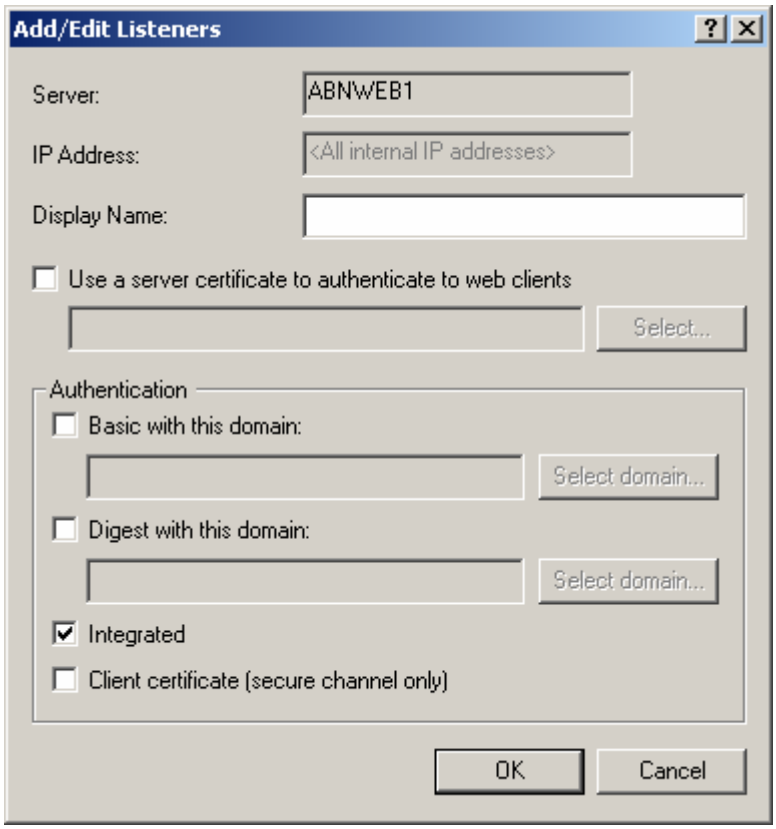
Configuring / Checking the local authentication setting of the proxy server

This section will vary depending whether your ISA server is Active Directory integrated with your domain, or if it's a stand alone ISA server.

Open the main ISA management console and right click on your server at the top of the left-hand window. The dialog box that opens is the same in both cases, select the 'Outgoing web requests tab':



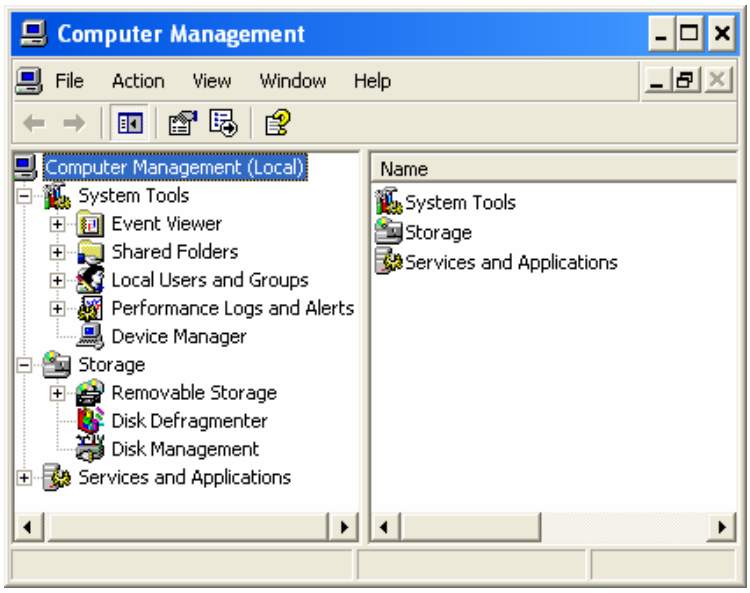
Inside the window select the 'Listener' and click 'edit':



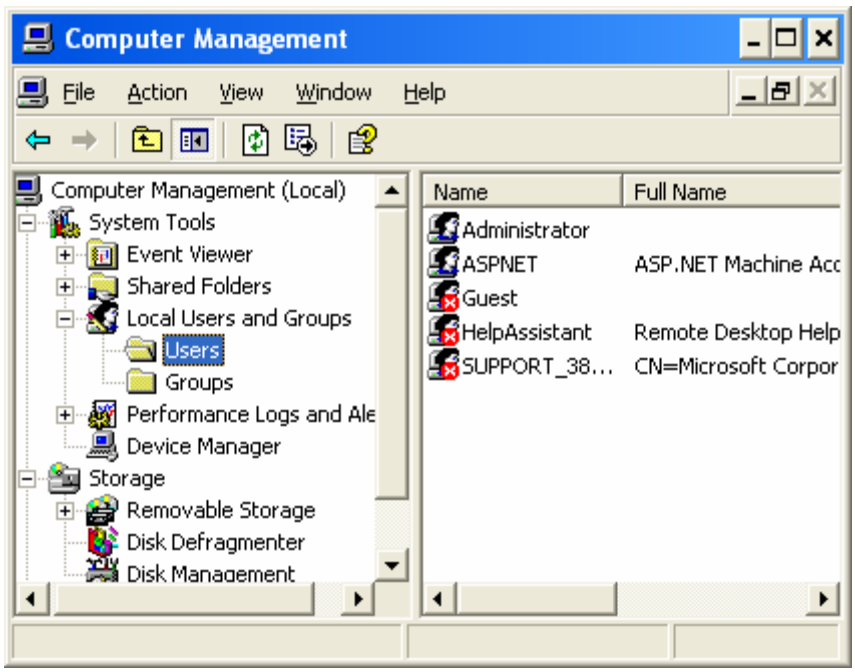
The default setting for ISA server is 'Integrated', this means the ISA server will try and authenticate the user using the username and password they logged onto their Windows desktop with. If your ISA server is part of a domain and all of your users PC's are part of the same domain you should not have any problems. If your ISA

server is configured as a stand alone server you may need to make a slight change if you do not want your users to be challenged by your local proxy.

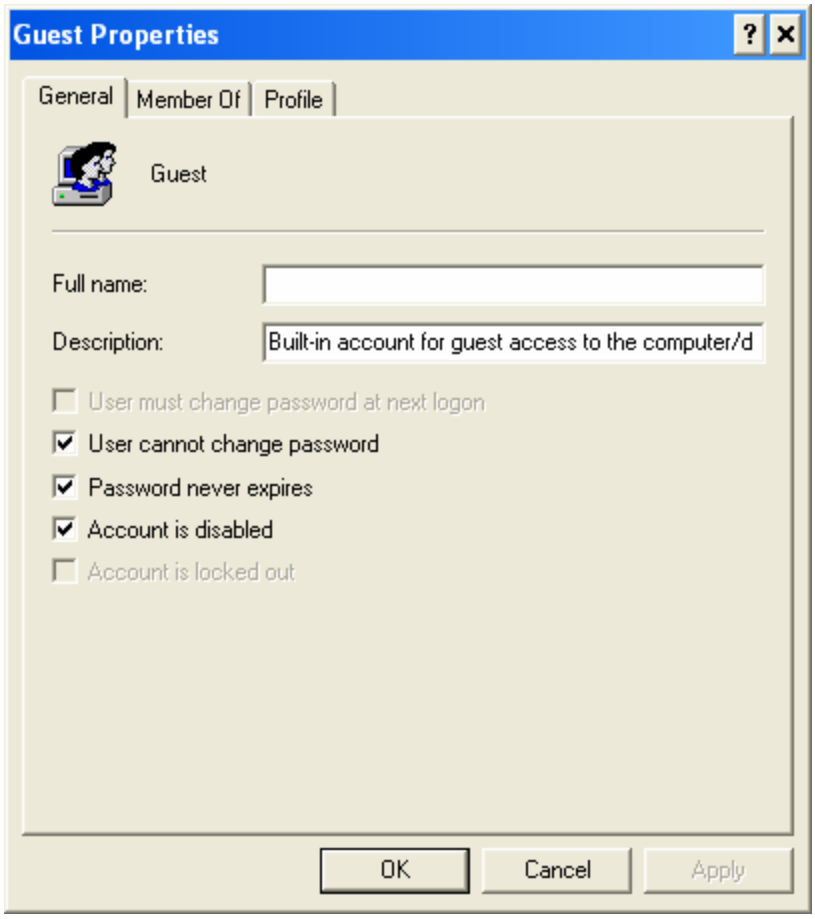
If you are being challenged for authentication by your local ISA server and it is a stand alone server open the computer management console, you can find this inside the 'Administrative tools' menu:



In the left-hand window expand the 'Local Users and groups' section and select the user's folder:



In the right-hand window there should be a guest account with a red cross on it. Right click on the 'Guest' user and select properties:



Untick the 'Account is disabled' tick box and select 'OK'. For security reasons we now need to rename this account and reset it's password. Right click on the guest user and select rename, enter a new name for the account which is meaningful to you. Right-click on the user again and select 'Set password', again set a password that is complex but you can remember or in this case you could take a note of it and keep this in a safe place.

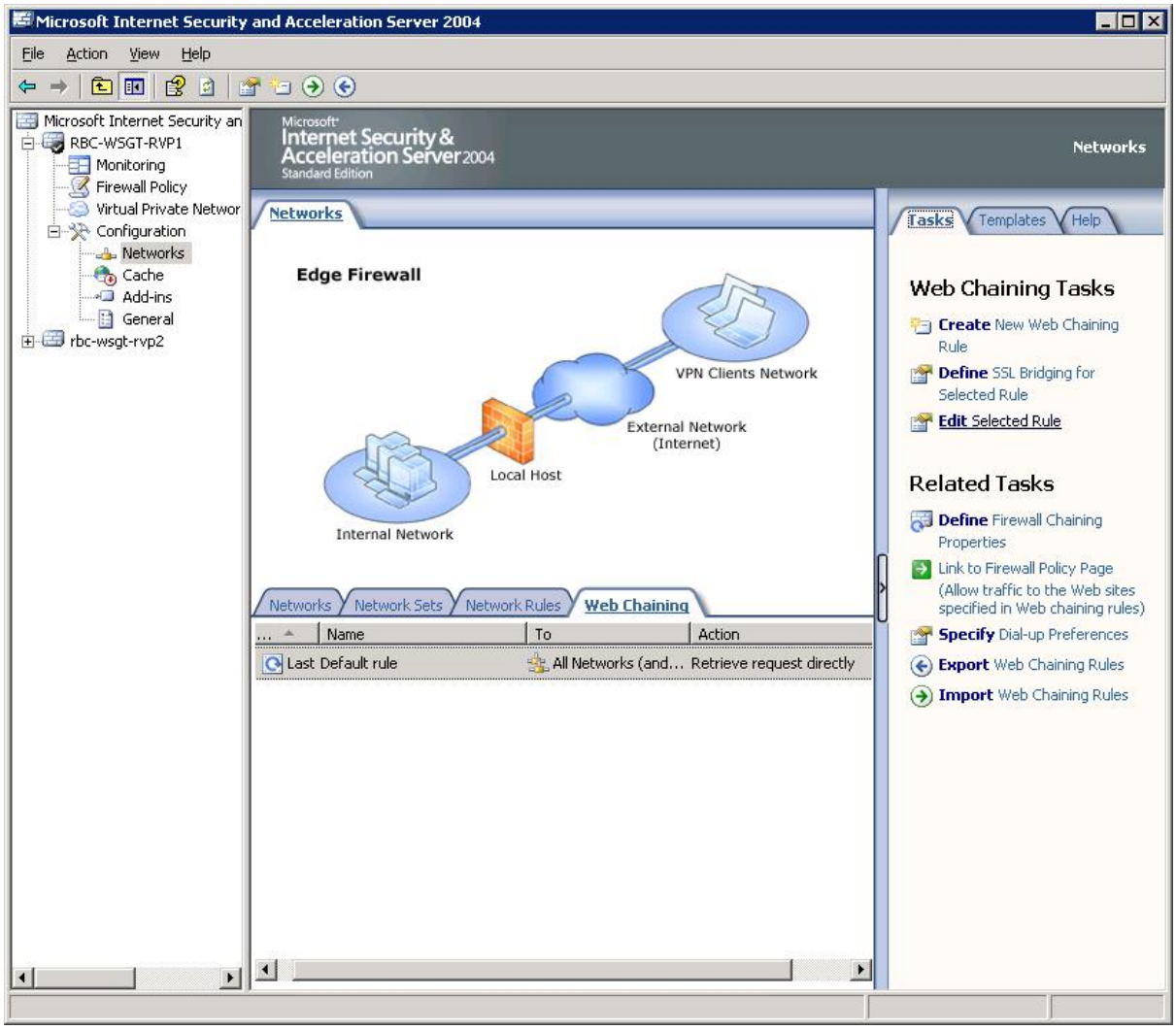
Once these steps have been taken your users should no longer be challenged by your local proxy server.

If your ISA server is a member of a Domain and your users PC's are not part of the domain, open the main ISA server management console and right on the Enterprise policy at the top of the right-hand window and select properties. On the security tab click add browse through the list to find the 'Domain guest's' group and add it to the list, you may also need to enable and rename the guest user account as detailed above.

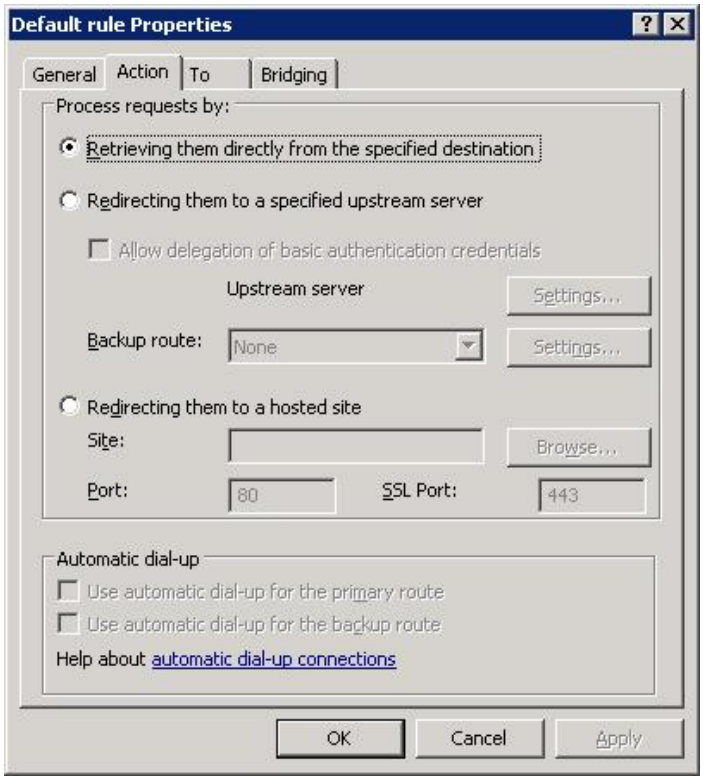
©BT Global Solutions, 2005

8. MICROSOFT ISA SERVER 2004 CONFIGURATION

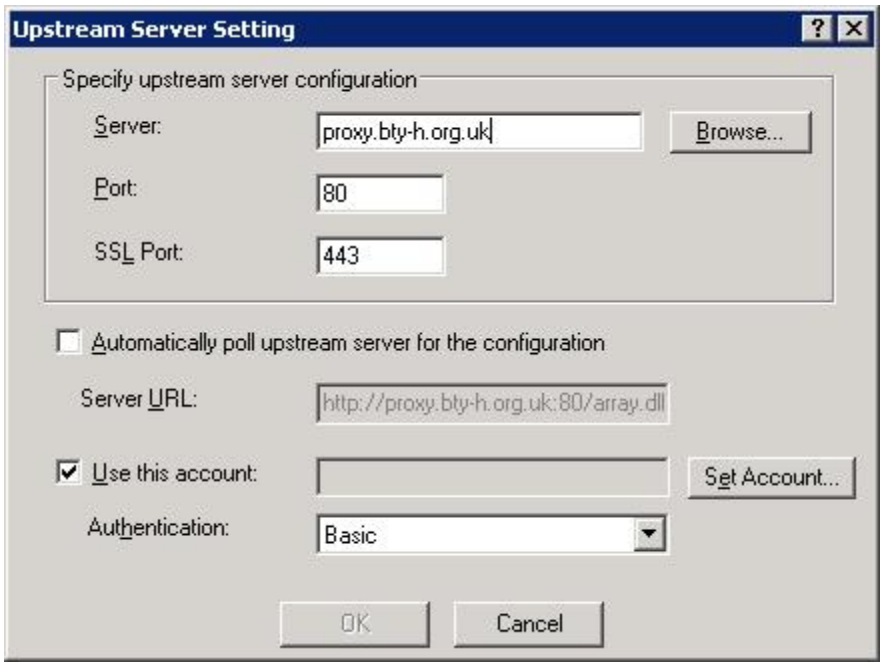
Open the ISA management console and under your proxy server expand the 'Configuration' section and select the 'Networks' folder. In the right hand window click on the "Web Chaining" tab.There should only be a single rule visible in the right-hand window:



Edit this rule, and click on the "Action" tab.

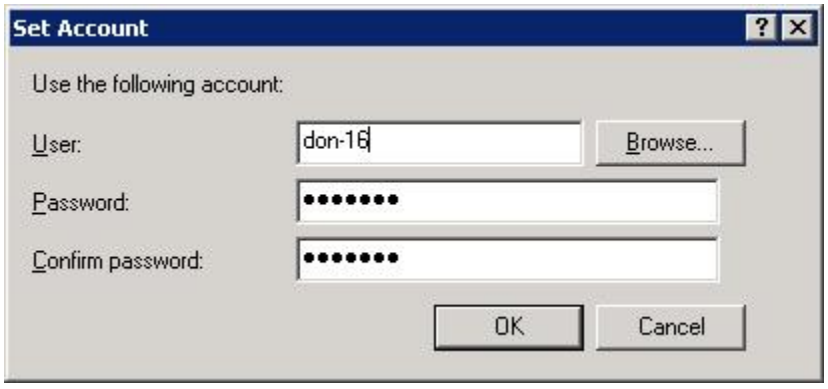


Click the radio button next to “redirect to an upstream server”. Ensure “allow delegation” box is NOT ticked, click on the “settings” button for the upstream server.



Enter the details proxy.bty-h.org.uk on port 80. Click on use this account and select basic authentication from the drop down choice. Click on the “Set account” button.

©BT Global Solutions, 2005



Enter the user account you wish to use, to give the level of Websense filtering required.

Click OK three times to close all the windows and action the changes.

9. TROUBLE SHOOTING GUIDE

The first step is to decide which of the above scenario's your network fit's into. Follow the above guidelines and see if the expected results match your actual results.

If you have followed the guidelines and are still experiencing unexpected results we then need to test network connectivity and DNS.

The first round of tests should be carried out on your proxy server, it is assumed that your proxy server has two network interface cards one of which is connected to the same network as all your client PC's and the other network interface is connected to the network provided by the service. This interface should be using an IP address inside the range that has been assigned to you i.e. 10.32.x.x. If this is not the case it can add further complication to the problem, to carry out these tests you need to be at a PC that is using one of the allocated IP address and connected to the network provided by the service.

1. First open a command prompt and enter the command:

Ping 10.0.1.254

You should see a reply from this address go to step 2, if not check all of your connections check the router that has been provided to you to ensure it is powered up, if there are no obvious problems call the help desk to report a fault.

2. Now enter this command:

Ping www.bty-h.org.uk

You should see this reply with an address of 10.0.4.15 go to step 3, if you see no response or a response of 'Unknown host' at the command prompt type 'ipconfig /all' check the IP addresses listed for your DNS servers unless you have a local DNS server these should be 10.0.4.21 and 10.0.4.22 and only these. If you do not see these or there are other addresses listed open the properties of your network card and add these two entries and remove any others now try this test again. If you now see a response go to step 3 if not call the help desk and report a fault.

If you have a local DNS server then for the moment change your network properties as described above, remove the address of your DNS server and add 10.0.4.21 and 10.0.4.22 and repeat the above test, if you now receive a response there is a change that needs to be made to your local DNS server this change is described at the beginning of this document. If you've made these changes and still see no response then call the help desk to report a fault.

©BT Global Solutions, 2005

3. If you have passed the above two tests you should now be able to test the whole solution from one of the client PC's on your network. Open a web page and see if the response is as you expect it. If not, check that your client can ping your local proxy server. In addition check the DNS settings on the client PC. If you are using an automated proxy setting then open a web page to http://update.bty-h.org.uk which is located in the POP at Leeds. If this page is displayed then try a page on the internet. If the page is not displayed, try using one of the other proxy settings to see if that server has failed. If at this stage you are still having problems please call the help desk to report a fault giving as much information about the configuration of your local network as possible.

10. REVISION HISTORY

Date	Version	Description	Author
26/09/2005	1	Updated with proxy details and ISA 2004	I George
23/02/2004	0	Proxy Guide	T Needham

--- end of document ---