

Proxy Server and Content Filtering Configuration on the US Robotics 9003

The US Robotics 9003 ADSL router incorporates a Proxy Server and Access Control Lists (ACL) to control internet usage. You can use the Proxy server on its own but the ACL (Content Filtering) is designed to work in conjunction with the proxy server.

The proxy server provides username and password access to the internet. This is useful when used on its own to stop unwanted access especially when the USR 9003 is used with a wireless access point. The 9003 provides additional security to the wireless security which by default is not very secure.

The access control lists restrict the internet access by web address, application type (video, audio and pictures). With the proxy server, the ACL's can have specific rules for each user giving precise control.

There are three steps in configuring the Access Control List:

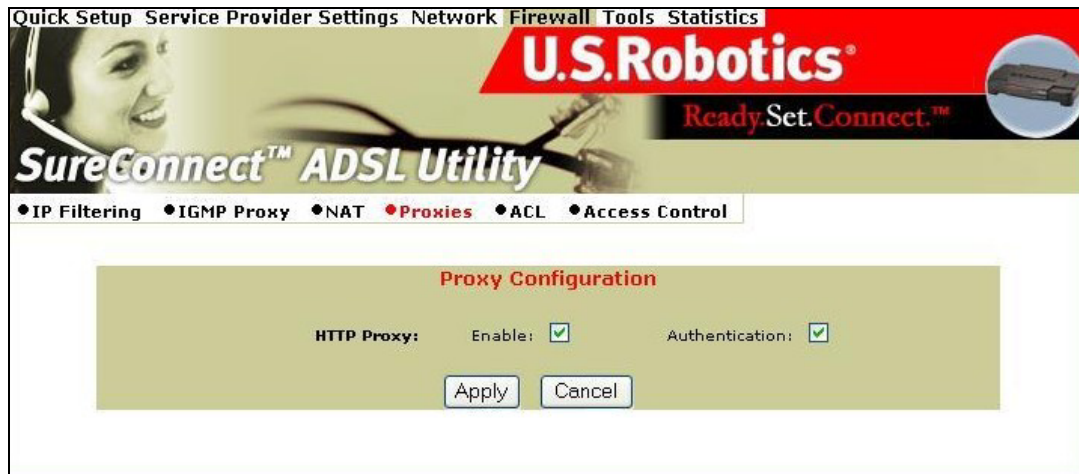
- **Enable the HTTP Proxy**
- **Add a user to the Access Control**
- **Add the rules for that user or all users in the ACL**

Make sure you save the configuration when you are finished or the changes will be lost

Note: You will also need to configure your PC to use the USR 9003 as the proxy server.

Step 1. Enable the HTTP Proxy

From the **Firewall** menu, select **Proxies**. Select **Enable** and **Authentication**. Click on **Apply**.



Note: If Authentication is not selected you will not be able to create rules for each individual. Only rules pertaining to all users will take affect.

If you want to only use Proxy server you can stop here but make sure you configure your PC to use the router as a proxy server.

Step 2. Add a User to the Access Control

Click on the **Access Control** menu and click on **Add**. Enter in the username and password for the user

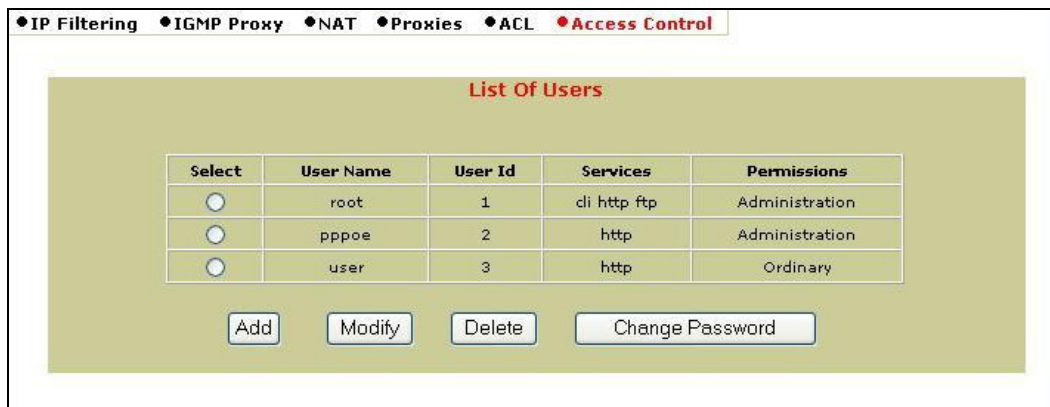


The screenshot shows the 'User Configuration' dialog box within the 'Access Control' menu. The dialog has a title bar with navigation tabs: IP Filtering, IGMP Proxy, NAT, Proxies, ACL, and Access Control (selected). The main area is titled 'User Configuration' and contains the following fields:

- User Name: USER
- Password: [masked with dots]
- Services: CLI (selected), HTTP (highlighted)
- Permissions: Ordinary

At the bottom of the dialog are 'Apply' and 'Cancel' buttons.

Click on **Apply** when finished and the user you added should now in the list.



The screenshot shows the 'List Of Users' table within the 'Access Control' menu. The table has a title bar with navigation tabs: IP Filtering, IGMP Proxy, NAT, Proxies, ACL, and Access Control (selected). The main area is titled 'List Of Users' and contains the following table:

Select	User Name	User Id	Services	Permissions
<input type="radio"/>	root	1	cli http ftp	Administration
<input type="radio"/>	pppoe	2	http	Administration
<input type="radio"/>	user	3	http	Ordinary

Below the table are 'Add', 'Modify', 'Delete', and 'Change Password' buttons.

The pppoe user is there by default and can be removed.

Step 3. Add the Rules for that user or all users in the ACL

Example 1. Deny a User Access to a Website

This example uses a keyword for denying a user access to a website. Using Keywords are easier than specifying a web address as it blocks all websites including sub sites containing that keyword. I.e. if you specified "xtra" as a website to block www.xtra.co.nz, "xtrmail.co.nz" will also be blocked. It would also block sites that you may want to allow through like www.extra.com. In those cases you will need to create an additional ACL with a lower priority to allow those websites through.

This method is useful for parents want to deny children access to any explicit sites.

Select **ACL** and Click on **Add**. Only options selected will apply in the ACL

Access List Configuration

Proxy Parameters

Port: HTTP Priority: 10000

User Name: user Destination Address:

Application Type: applicationall Domain Name: xtra

Source IP Range From: To:

Life Time

Day From: SUN 00 00 Day To: SAT 23 59

Action: Deny

Apply Cancel

When finished, click on **Apply** and the rule will now be in the list

ACL List

Select	Application	Priority	User Name	Src IP Range		Dest IP Address
	Domain	Mime	Date		Action	
				From	To	
				Time From	Time To	
<input type="radio"/>	HTTP_PROXY	10000	user	None	None	None
	xtra	None		None	None	Deny

Add Delete

Example 2. Deny Video Access for All Users

Select **ACL** and Click on **Add**.

Access List Configuration

Proxy Parameters

Port: HTTP Priority: 10000

User Name: Destination Address:

Application Type: videoall Domain Name:

Source IP Range From: To:

Life Time

Day From: SUN 00 00 Day To: SAT 23 59

Action: Deny

Apply Cancel

When finished, click on **Apply** and the rule will now be in the list

ACL List

Select	Application	Priority	User Name	Src IP Range		Dest IP Address
	Domain	Mime		From	To	
<input type="radio"/>	HTTP_PROXY	10000	None	None	None	None
	None		video;	None	None	Deny

Example 3. Allowing a User to have Audio Access on Websites in the Weekends Only while Denying All Other Users

Select **ACL** and Click on **Add**.

IP Filtering
 IGMP Proxy
 NAT
 Proxies
 ACL
 Access Control

Access List Configuration

Proxy Parameters

Port: HTTP Priority: 10000

User Name: user
 Destination Address:

Application Type: audioall
 Domain Name:

Source IP Range From: To:

Life Time

Day From: SAT 00:00 Day To: SUN 23:59

Action: Allow

Click on **Apply** and Click on **Add** to add the second ACL

IP Filtering
 IGMP Proxy
 NAT
 Proxies
 ACL
 Access Control

Access List Configuration

Proxy Parameters

Port: HTTP Priority: 10001

User Name:
 Destination Address:

Application Type: audioall
 Domain Name:

Source IP Range From: To:

Life Time

Day From: SUN 00:00 Day To: SAT 23:59

Action: Deny

When finished, click on **Apply** and the rules will now be in the list

ACL List

Select	Application	Priority	User Name	Src IP Range		Dest IP Address
				From	To	
	Domain	Mime	Date		Action	
<input type="radio"/>	HTTP_PROXY	10000	user	None	None	None
	None	audio;	sat(00:00)	sun(23:59)		Allow
<input type="radio"/>	HTTP_PROXY	10001	None	None	None	None
	None	audio;	None	None		Deny

Note: When using an ACL that has a time associated with it, you will need to make sure the 9003 clock has been set. To do this, go to Tools menu and select Date and Time.

Configuring Your PC to use the 9003 as a Proxy Server

Click on **Start** and then **Settings** and select **Control Panel**. Double click on **Internet Options** and select the **Connection** Tab. Click on the **LAN Setting** Button and enter in the details below.

Local Area Network (LAN) Settings

Automatic configuration
Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

Automatically detect settings
 Use automatic configuration script

Address:

Proxy server
 Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

Address: Port:

Bypass proxy server for local addresses

Keep Clicking on **OK** to Exit.