



EAU
education and microtechnology unit

**Using the 'Prefect' Internet
Proxy Server
Management Tools**

The Prefect Management system is installed on Sandwell LEA Internet Proxy servers. To use it you require a correctly configured computer with Netscape Navigator or Microsoft Internet Explorer 3.02 or better.

The proxy server configuration and the management tools were developed by Keith Chandler, EMU and Roy Barnard, Sandwell MBC IT Division.

Contents	Page
Ethical Internet Access	4
Starting the Management system	5
The Access list	6
The Allow and Deny lists	7
Adding users	8
Using the Access log to modify the Allow/deny lists	9
Backing up and restoring your lists	10
Miscellaneous other functions	11

Ethical Internet Access

The Prefect Management system is installed on your Linux Proxy server controlling access to the Internet. Access to web resources is restricted by three data files, allow.txt, deny.txt and userpass.txt. These files, which contain website names, are used as the “rules” governing whether or not a user can load a web resource. This is achieved in the following way:

- Anyone can have any resource from a website listed in the allow list
- No one can have anything from a website listed in the deny list
- Users requiring resources from websites that are not in the allow or deny lists must supply a valid username and password.

The management system allows you to modify these files, and to view where users are obtaining their Internet resources. Websites can be added to allow and deny lists, users and passwords can be set up to give staff fuller access to the web.

It must be noted, however, that the Internet is a volatile system with new areas being added and changed every day. To attempt to keep up is an immense job. It is recommended therefore that the technological approach to access restriction should be complemented by a pastoral system, where:

- students and parents sign up to an acceptable use policy before they are allowed to access the Internet,
- students are made aware (possibly by creating an example) that they are being closely monitored.

Other issues to be considered include email services, many of which allow advertisements, and for “opportunistic” contacts that may lead to bullying or worse. Only a small number provide security and monitoring systems that are essential for student access.

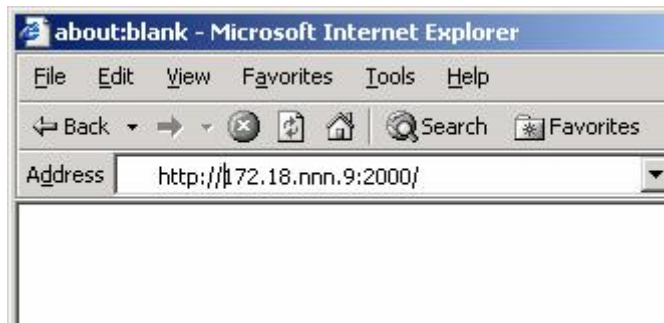
Readers should consult EMU or the Advisory Service for help with developing an Acceptable Internet Use policy. Model use policies can be found at the following websites:

- www.acitt.org.uk/aup.html
- www.bcs.org.uk/iap.html
- www.naace.org.uk
- www.becta.org.uk

Starting the Prefect Management System

Load Internet Explorer, then in the address bar enter your proxy server's ip address: this will be 172.18.n.9 (phone EMU if you don't know n should be)

Click on any "click here to continue" buttons that you are offered.



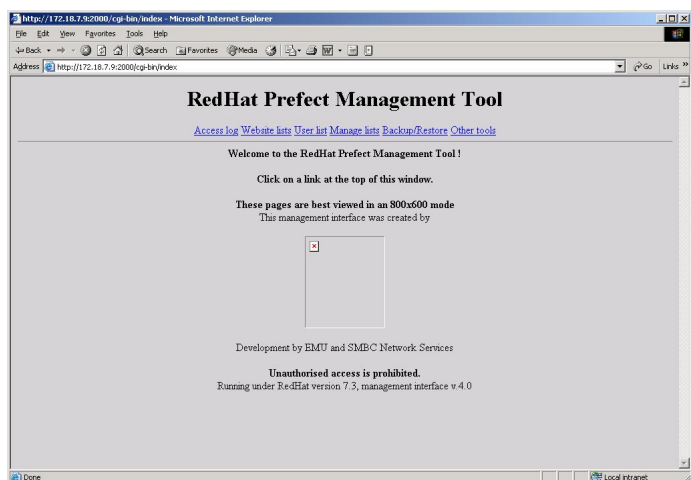
The authentication dialogue for the management system is different to the authentication for web pages: the resource name (see example) says Prefect_Management: this helps you to see what you are logging on to.

The user name for the Management system is **manager**. You will have been told the password, and will be able to change this later.



Having authenticated yourself, you will be presented with the management system home page, as shown.

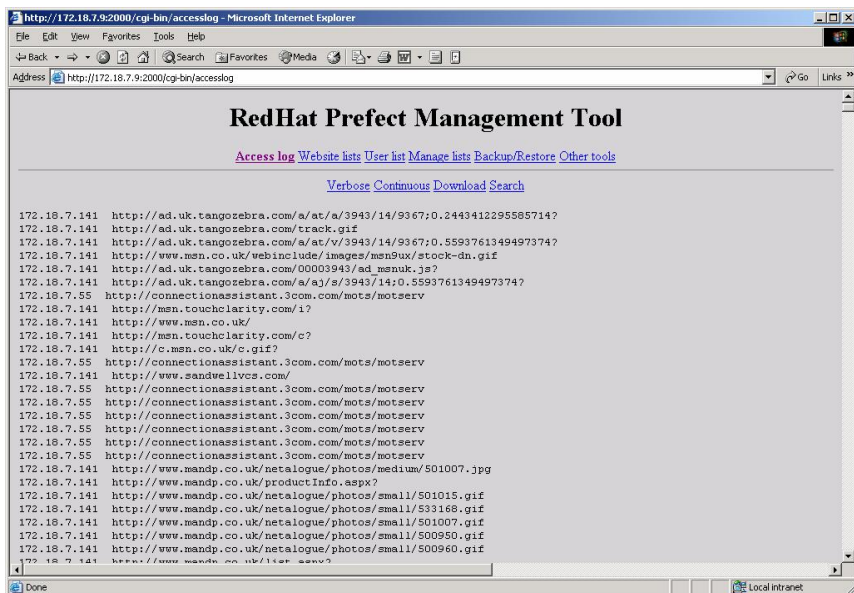
You can now access the tools using the menus across the top of the screen, and the menus on the sub pages.



The Access List

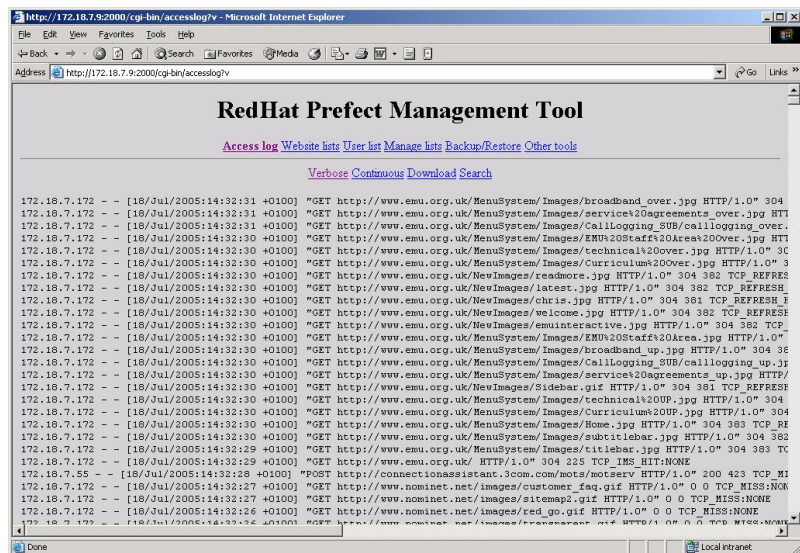
The access list is obtained from the Access log button on the toolbar down the left side of the screen.

The access log tells you what pages have been accessed, and by which computers, and at what time. From this it should be possible to determine who was looking on the web for what, and if necessary, steps could be taken to counsel the individual concerned...



The access log has two other views:

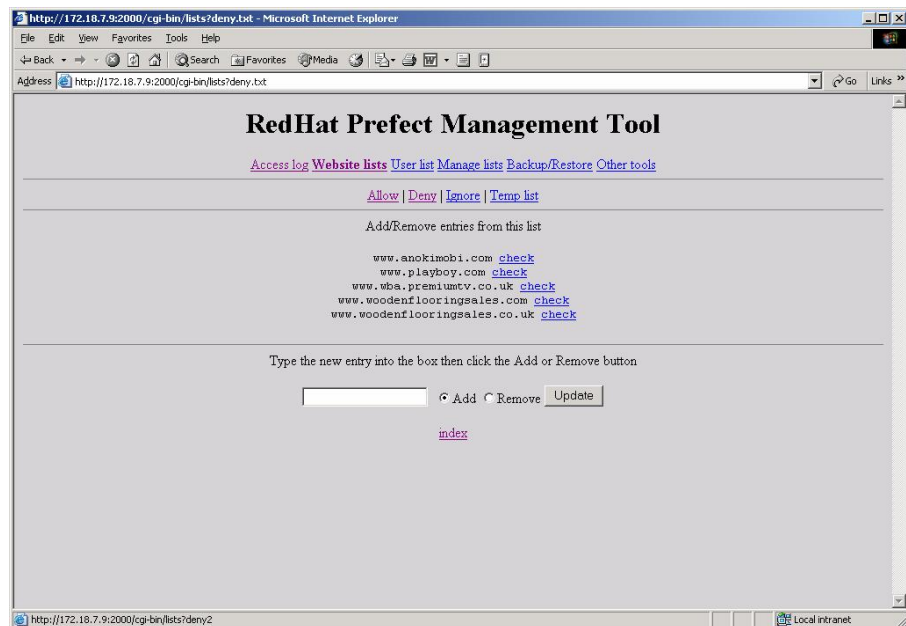
- continuous view, useful if you leave the log running (on a secure system) and keep an eye on it during the day.
- verbose view, giving workstation, logged on user, date and time the resource was requested.



The access log can get very long very quickly. You may need to archive the log rather than deleting it so that you can refer back to any previous misdemeanours. Click the Download log file button at the top of the screen.

The Allow and Deny lists

The allow and deny lists govern what Internet resources can be accessed by users of your network.



Adding websites is achieved by typing the website name (eg **www.bbc.co.uk**) into the box at the bottom of the page, clicking the add button and clicking on Update list.

There are also options for deleting pages from the lists.

Note that only **website names** (not page names or resource names) should be put into the allow and deny lists: so **www.bbc.co.uk** is acceptable, but **www.bbc.co.uk/education** is not.

IP addresses of servers can also be placed in the allow and deny lists. These will take the form **123.45.67.89**.

Parent domains will block child domains (eg smile.com and www.smile.com) by entering .smile.com as the domain. (Note the leading full stop)

Updates that you make to the allow and deny lists may not be implemented until the service is next restarted. Turn to page 11 to see how to do this.

Adding Users

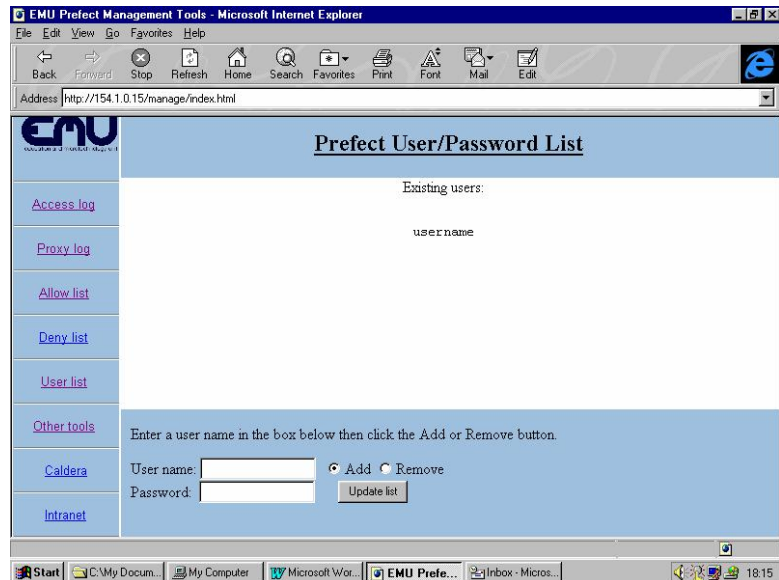
Full Internet access is achieved by password authentication. It is recommended that this be reserved for staff users. The security of the system is achieved by restricting student access to the websites in the allow list.

New staff usernames and passwords can easily be added. Type in the user name and password for your new user, and click on the update list button. The username and password that you use only works on the Internet proxy list: it does not need to match any other passwords that you use, nor does it change with them.

If users lose their password, you can reset them by adding the user again, ie type in their details. The system will replace the existing user details with those entered.

Note that any update will not be activated until the proxy server is next rebooted.

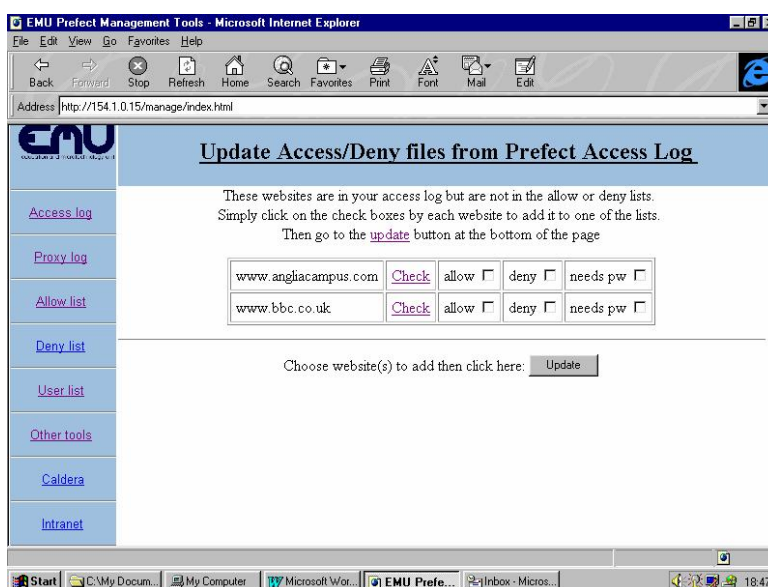
More important note: once authenticated, the system assumes that the user is authenticated for all subsequent requests: the user has full Internet access to everything except the deny list. If staff get into the habit of typing in their user name and password to help a student to view a (legitimate) website, and then move on to work with another user, that student is able to browse without being challenged. The session will only be closed when all open Internet Explorer windows are closed. Staff should be advised to watch over any authenticated workstations until the session is closed. Staff should never divulge their username and password to any students.



Using the Access log to modify the Allow/deny lists

While your users have been browsing, the websites they have visited are being compiled into the access log. This can then be compared against the allow and deny lists to give a list of websites that people need to go to, but have to authenticate themselves for. There are buttons on the allow list, deny list and access log pages to link the access log, allow and deny lists for ease of updating.

Choose Manage lists on the toolbar, or follow the Allow/deny sites link from the Access log page, or the Modify from access log buttons from the allow and deny pages.

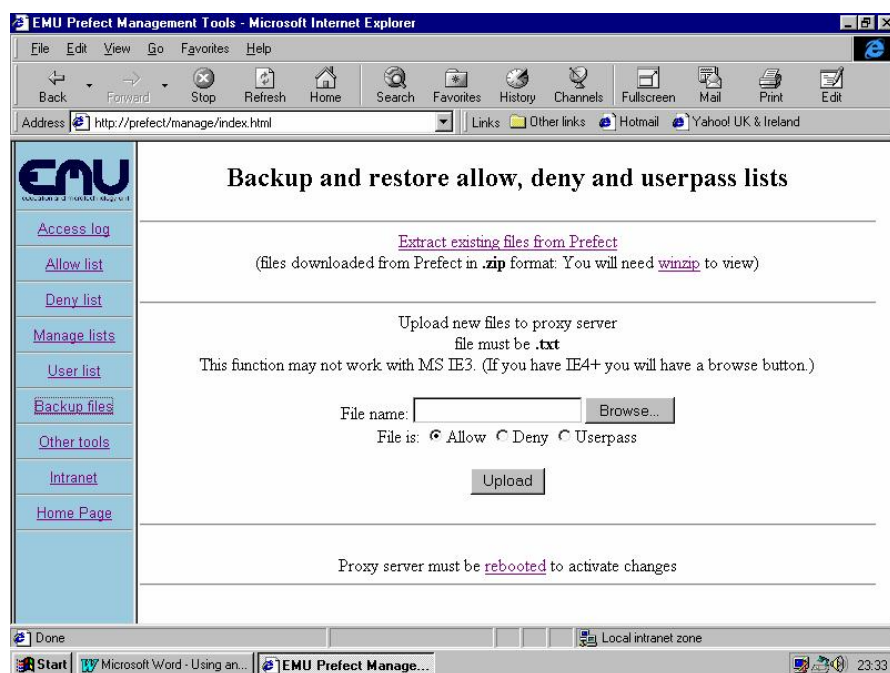


To allow the website, click the allow button. To deny access, click deny. There may be some websites that you want staff to be able to access, but not students. Click the needs pw button for these sites.

When you have finished, click the update button. Note that updates will not be implemented until the proxy server is next rebooted.

Important note: Some websites (such as Geocities.com) contain valid educational material, but also have areas of inappropriate material. It may be sensible to leave such websites in the third category where access requires a password., and obtain their resources only as a supervised activity. Alternatively, a blanket deny stops the risk of students “hacking” their way to such sites.

Backing up and restoring your lists

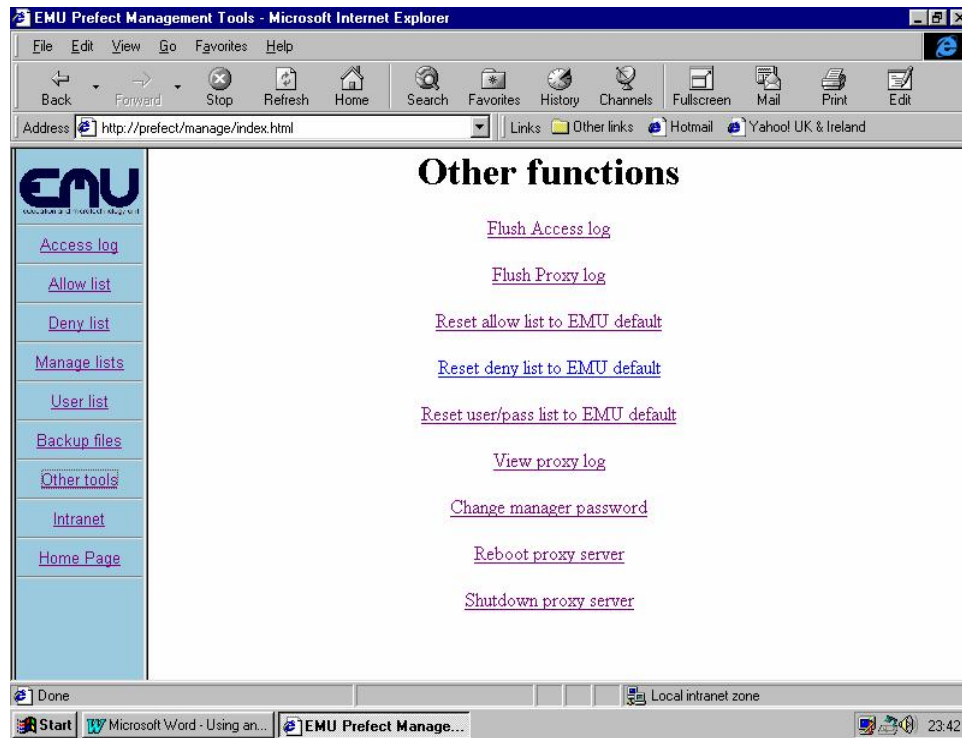


Backing up involves taking a copy of your files from the proxy server to another computer. The management system allows this, and compresses the files into a .zip file to make transport easier.

If you want to view the contents of the .zip file you will need an unzip program such as winzip. There is an evaluation copy of winzip on the download page if you need it.

Uploading (the opposite of backing up) can only be carried out if you have IE3.02 with upload support, or IE4 or IE5 (or Netscape Navigator). Earlier copies of MS IE do not have the required code to allow file uploading. To upload a stored or modified file onto your system, first locate the file, then click the browse button on the backup/restore page, allowing you to browse for the file. Uploaded files need to be named allow.txt, deny.txt or userpass.txt. All other names will be rejected. As an added precaution you must check the appropriate radio button (allow, deny, userpass) to confirm what is being uploaded. This should prevent deny lists being uploaded as allow lists and so on.

Other functions



- Flush access log: after prompting for confirmation, the access log is cleared (you did back it up, didn't you?) The proxy server reboots immediately to ensure that it isn't running without an access log.
- Flush proxy log: the proxy log is a tool for Keith and Roy to use.
- Reset allow/deny/password lists: these links allow you to restore your system in the event of a catastrophic loss of data in the middle of an editing session. It is sensible to back up your data sets before starting to edit them.
- View proxy log: the proxy log is a very boring tool for Keith and Roy to use.
- Change manager password: this is the Prefect_Management password that you used on page 5. You can change the password, but currently not the username. Try to keep both secret.
- Reboot proxy server: (favourite tool of the couch potato) a link to use if the server needs rebooting, eg after editing the allow or deny lists, without having to get up out of that comfortable armchair and walk over to the proxy server keyboard.
- Shutdown proxy server: essential if the server has to go off at any time. On older machines you will also need to turn it off after a minute or two. You should never turn the proxy server off without first clicking the shutdown link.

Education and Microtechnology Unit

Department of Education and Community Services
Sandwell Metropolitan Borough Council

Training and Development Centre

Popes Lane

Oldbury

West Midlands

B69 4PJ

Tel: 0121 544 2001

Fax: 0121 511 1022