Introduction

Understanding how Web Access Management works is key to having the product work smoothly. This tutorial is intended as a guide for new customers in setting up a new WAM product and as a reference tool for existing customers for later questions. It covers such topics as creating/editing the Forward Table, gathering statistics and how WAM works.

The tutorial as a whole can be used in one of two ways. For libraries new to Teleforms, or for new library staff just beginning to use a Teleforms machine, this tutorial can be followed in a step-by-step manner, using the NEXT PAGE → and ← PREVIOUS PAGE navigation icons. Using the tutorial this way will guide you through all the products functions.

A second way to use the tutorial, particularly suited for a department supervisor primarily interested in a certain task, is to use the menu based approach. Using the menu at the top of the tutorial, you can find the topic you are interested in and go directly there.

PRINT THIS PAGE
close window

Navigation & Requirements

- At the bottom of each page are links to the next and previous pages. We recommend you follow through the tutorial steps using the **Next Page** links.
- At any time you can select from the drop down menus on the navigation bar across the top of each page.
- A menu bar near the top of each page lists each section in the tutorial, with your current location highlighted in red. You can select a different section from the menu bar.
- Within pages there are links to other pages in the tutorial. Use your browser's **Back** button to return to your previous place in the tutorial.
- Links to pages outside the tutorial open in a separate browser window. To return to the tutorial, close the external link window, or click on the tutorial window to make it active.
- **HOT TIP** is used to highlight information that either illustrates or expands a point in the tutorial text.

RECOMMENDED SOFTWARE AND HARDWARE SETTINGS

- Web browser: Netscape Communicator v.4.5 or above; Internet Explorer v.4.5 or above; Mozilla Firefox 1.5 or above

For optimal viewing:

- Web browser: Netscape Communicator v.6.0 or above; Internet Explorer v.5.5 or above
- Monitor setting: 1024 x 768 resolution or higher, with browser window maximized
- Colors: at least 256 or higher

PRINTING

You can print individual tutorial pages and screens from within a Web browser using the '**Print this page**' icon

Customers may also download and print this tutorial as a PDF document. To view and print it you need Adobe Acrobat Reader software which you can download from

DOWNLOADING

Customers who would like to mount this tutorial on a local server for the use of their staff, without having to allow them full access to CSDirect, may download the tutorial as a ZIP file.

After the file has been downloaded and unzipped into the Local directory of choice you will see a list of individual html pages. Double click to open a page called index.html and the tutorial will be accessible. Once it has been downloaded locally, you may choose to open it in a web editor and insert local policies, practices or notes.

Please note that internal links to the Innovative Guide & Reference will result in a "page cannot be found" error message since the tutorial uses a relative addressing system. However, the link reference contains the Reference Guide's page number, which can be searched within the customer Millennium server's own version of the Reference Guide.

Please contact us if you have questions, comments or problems.

PRINT THIS PAGE

close window

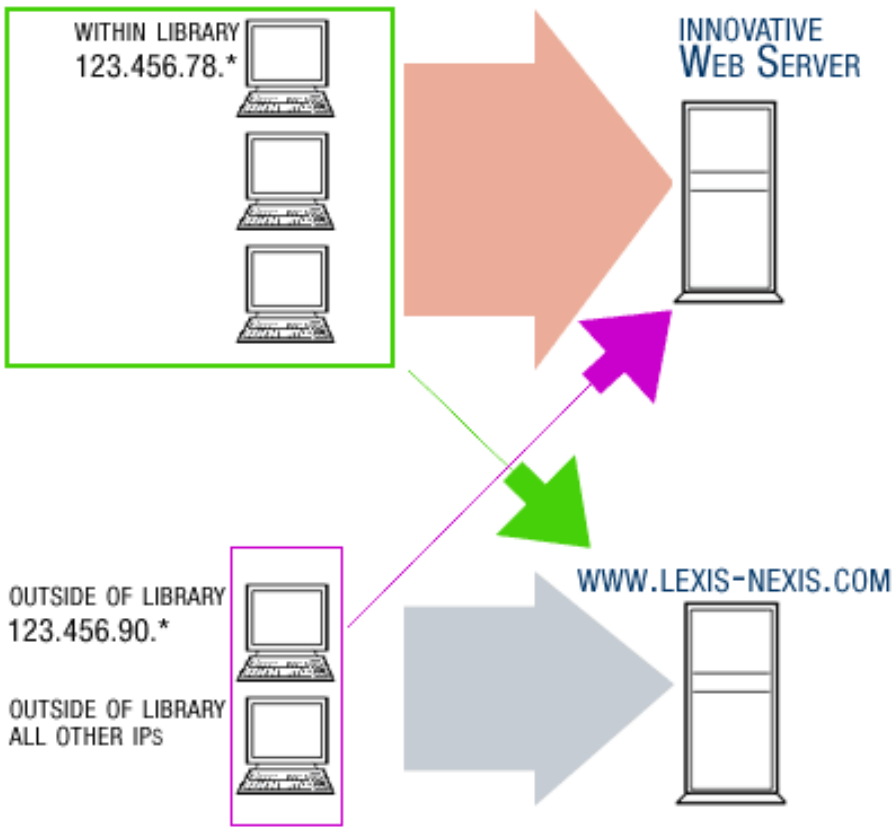
How Web Access Management Works

Web Access Management forwards requests to a remote server by having all requests routed through the Innovative Web server. For example, a library has acquired an account for Lexis-Nexis and wants to offer its patrons a link to this database. This library has set up three logins that are used by the Innovative Web server.

HTTP ACCESS ADMINISTRATION

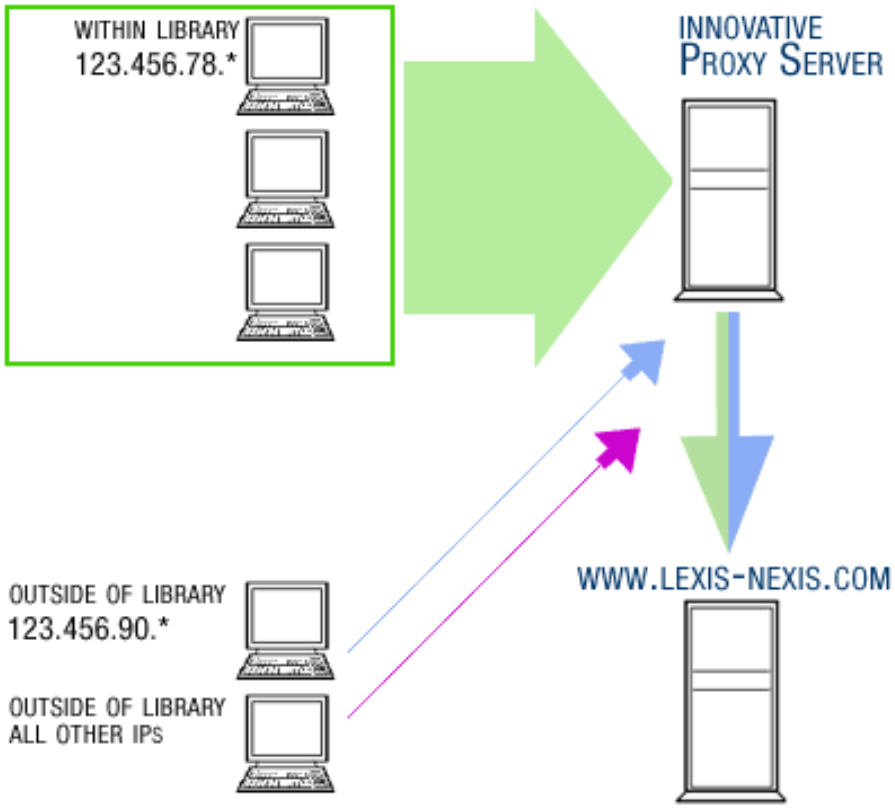
REMOTE HOST	ACCESS?	LOGIN NAME	SERVICE LEVEL
1 > 123.456.78.	Yes	webpac1	4
2 > 123.456.90.	Yes	webpac2	6
3 > all	Yes	webremote	0

The library can insert a direct link to Lexis-Nexis in the Main Menu page or in a MARC 856 field in a bibliographic record. This link will retrieve the initial Lexis-Nexis page for local client browsers. However, the Lexis-Nexis server will not allow access by those client browsers that are not located on campus, because these remote browsers are not considered within the library's account. The diagram below illustrates how client browsers access the Innovative Web Server and Lexis-Nexis when the Web Access Management feature is *not* implemented:



In the diagram above, the **webpac1 (123.456.78.*), webpac2 (123.456.90.*)** , and **webremote (Outside of Library and other IPs)** logins used by the Innovative Web server are represented by the green, blue, and purple arrows, respectively. In addition to accessing the Innovative Web server, the local client browsers could successfully access the Lexis-Nexis server using its actual IP name or address (black arrows), since these logins are recognized by the server as having access through the library's account (i.e., their IP addresses are known to the Lexis-Nexis server). The remote client browsers, however, can see the link to Lexis-Nexis in the library's Main Menu page or a bibliographic record's MARC 856 field, but are not able to access the server (red arrows), because their IP addresses are unknown to the Lexis-Nexis server.

Using **Web Access Management** , the Innovative server acts as an intermediary host and forwards the requests to the remote server as specified in the forwarding table. The remote server never sees the client's IP address since the Innovative server is making the request rather than the client browser. The system then routes the data from the remote server back to the client, as illustrated below:



In the diagram above, all Lexis-Nexis requests made by **webpac1** and **webpac2** logins are forwarded by the Innovative Proxy Server (green and blue arrows). The **webremote** login (purple arrow) is not allowed to access the Lexis-Nexis server. Additionally, the library could specify that patron verification be performed through the web OPAC for the **webpac1** and/or **webpac2** logins.

Because each forwarded request uses the Innovative Proxy Server as the intermediary, the request counts as a Web OPAC login using one of the library's user licenses, unless the library has the unlimited Web OPAC logins feature. However, Web OPAC logins expire after two minutes of inactivity, so their impact on the library's license resources is minimal.

PRINT THIS PAGE
close window

Setup

Web Access Management needs some setup in order to work properly. This setup involves inputting information from your database vendors into a table, configuring Limit Network Access, and setting up patron verification.

- Forward Table
- Two Methods
- Limit Network Access
- Filters
- Patron Verification and Web OPAC
- Multiple IP Support (for libraries that have purchased this)

PRINT THIS PAGE

close window

Forward Table

Web Access Management needs some setup in order to work properly. This setup involves inputting information from your database vendors into a table, configuring Limit Network Access, and setting up patron verification.

The next few pages will describe how to access, setup, and edit the Forward Table.

- Accessing the Forward Table
- Adding, Appending and Editing and the Forward Table

PRINT THIS PAGE

close window

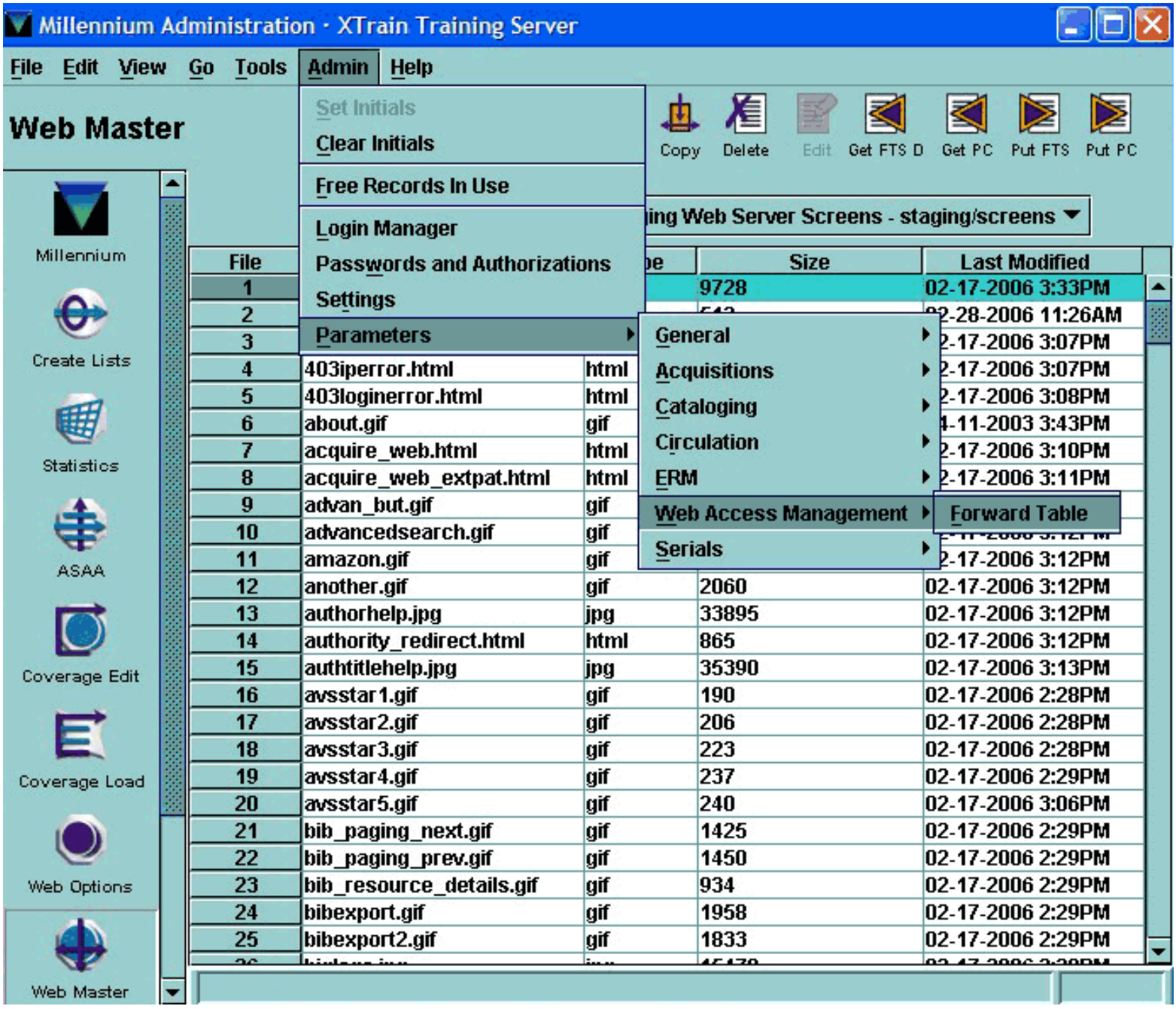
Accessing the Forward Table

In order for the Millennium system to recognize an IP address, you will need to set up the Forward Table.

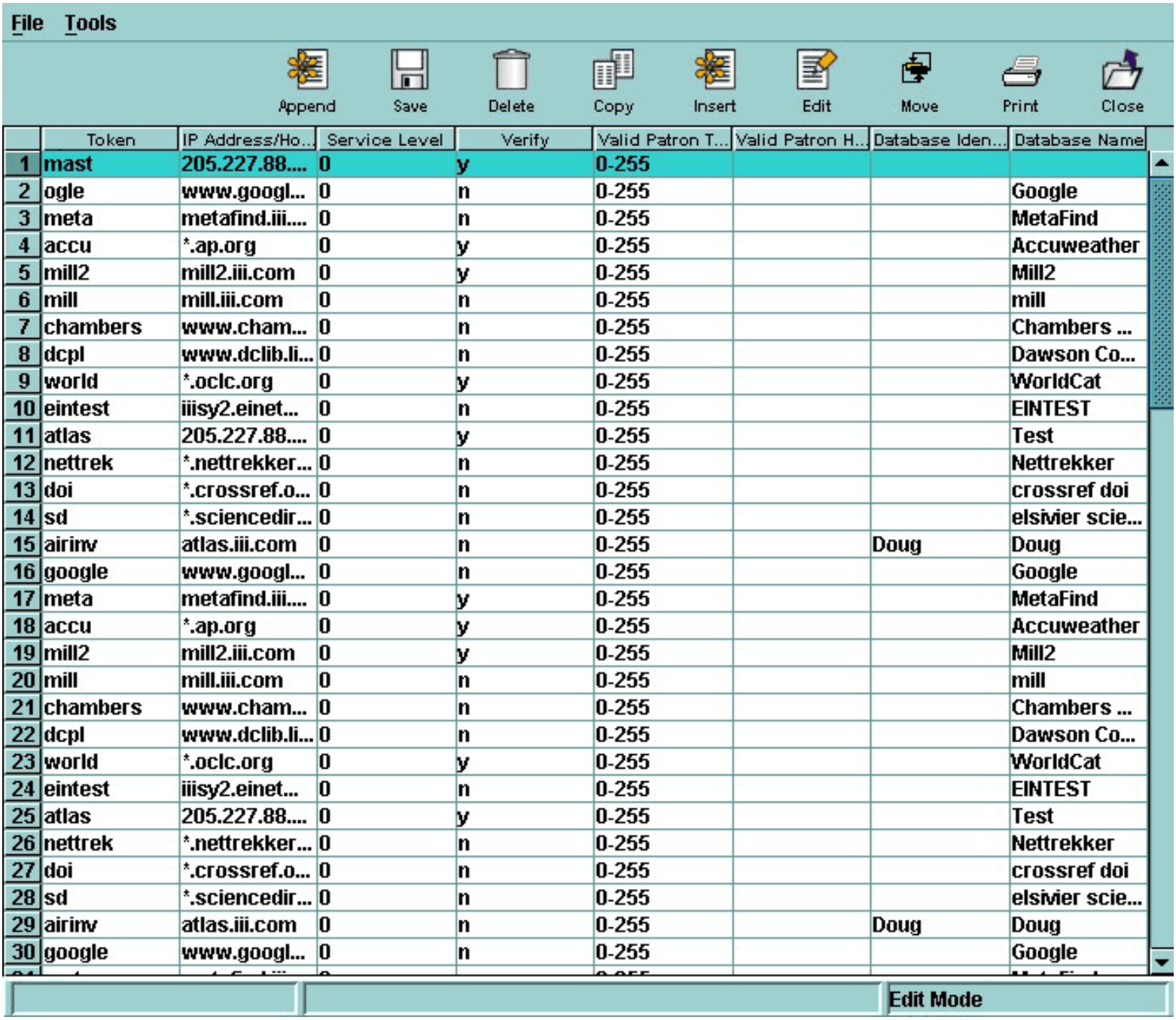
The Forward Table contains details of vendors' IP or server addresses, and methods of authentication: patron verification, login service levels and patron types. The table can include up to 1000 entries. Contact Innovative Interfaces if you need to change this.

To update the Forward Table, you must be authorized for function 696 (Edit the Web Access Management Forward Table). If you are authorized for function 651 (View System Parameters), you can view this file but cannot edit it.

You can access the Forward Table though the Millennium System Administration module. Once logged in there, choose the drop-down menu **Admin | Parameters | Web Access Management | Forward Table** .



You will then see the Forward Table:



	Token	IP Address/Ho...	Service Level	Verify	Valid Patron T...	Valid Patron H...	Database Iden...	Database Name
1	mast	205.227.88....	0	y	0-255			
2	ogle	www.googl...	0	n	0-255			Google
3	meta	metafind.iii....	0	n	0-255			MetaFind
4	accu	*.ap.org	0	y	0-255			Accuweather
5	mill2	mill2.iii.com	0	y	0-255			Mill2
6	mill	mill.iii.com	0	n	0-255			mill
7	chambers	www.cham...	0	n	0-255			Chambers ...
8	dcpl	www.dclib.li...	0	n	0-255			Dawson Co...
9	world	*.oclc.org	0	y	0-255			WorldCat
10	eintest	iiisy2.einet...	0	n	0-255			EINTEST
11	atlas	205.227.88....	0	y	0-255			Test
12	nettrek	*.nettrekker...	0	n	0-255			Nettrekker
13	doi	*.crossref.o...	0	n	0-255			crossref doi
14	sd	*.sciencedir...	0	n	0-255			elsivier scie...
15	airinv	atlas.iii.com	0	n	0-255		Doug	Doug
16	google	www.googl...	0	n	0-255			Google
17	meta	metafind.iii....	0	y	0-255			MetaFind
18	accu	*.ap.org	0	y	0-255			Accuweather
19	mill2	mill2.iii.com	0	y	0-255			Mill2
20	mill	mill.iii.com	0	n	0-255			mill
21	chambers	www.cham...	0	n	0-255			Chambers ...
22	dcpl	www.dclib.li...	0	n	0-255			Dawson Co...
23	world	*.oclc.org	0	y	0-255			WorldCat
24	eintest	iiisy2.einet...	0	n	0-255			EINTEST
25	atlas	205.227.88....	0	y	0-255			Test
26	nettrek	*.nettrekker...	0	n	0-255			Nettrekker
27	doi	*.crossref.o...	0	n	0-255			crossref doi
28	sd	*.sciencedir...	0	n	0-255			elsivier scie...
29	airinv	atlas.iii.com	0	n	0-255		Doug	Doug
30	google	www.googl...	0	n	0-255			Google

You will notice the following buttons

Append - Select this option to add a new entry to the end of the Forward Table. Selecting this button will bring up a dialog box for you to fill out.

Save - To save your changes to the Forward Table, click Save. If you make changes to the Forward Table and do not save those changes, Millennium will prompt you to save before you exit the Forward Table.

Delete - To delete an entry, select the entry and choose Delete. The deletion is not final until you save your changes.

Copy - To add a new resource entry that is similar to one that already exists in the table, you can copy the existing entry and modify the appropriate data elements. The new entry is added to the end of the table.

Insert - To insert a new resource entry, choose Insert. This will bring up a dialog box for you to fill out.

Edit - To edit the elements of an existing entry, select the entry and choose Edit. This will bring up a dialog box for you to edit.

Move - To reorganize the entries, highlight the entry that you want to move and choose Move. The system will then ask for a row number. The entry will be inserted at the selected point, and all succeeding entries will be shifted down one position.

Print - To print the Forward Table, choose Print. You will be prompted to select a printer connected to your computer. Select the printer to use, then choose OK.

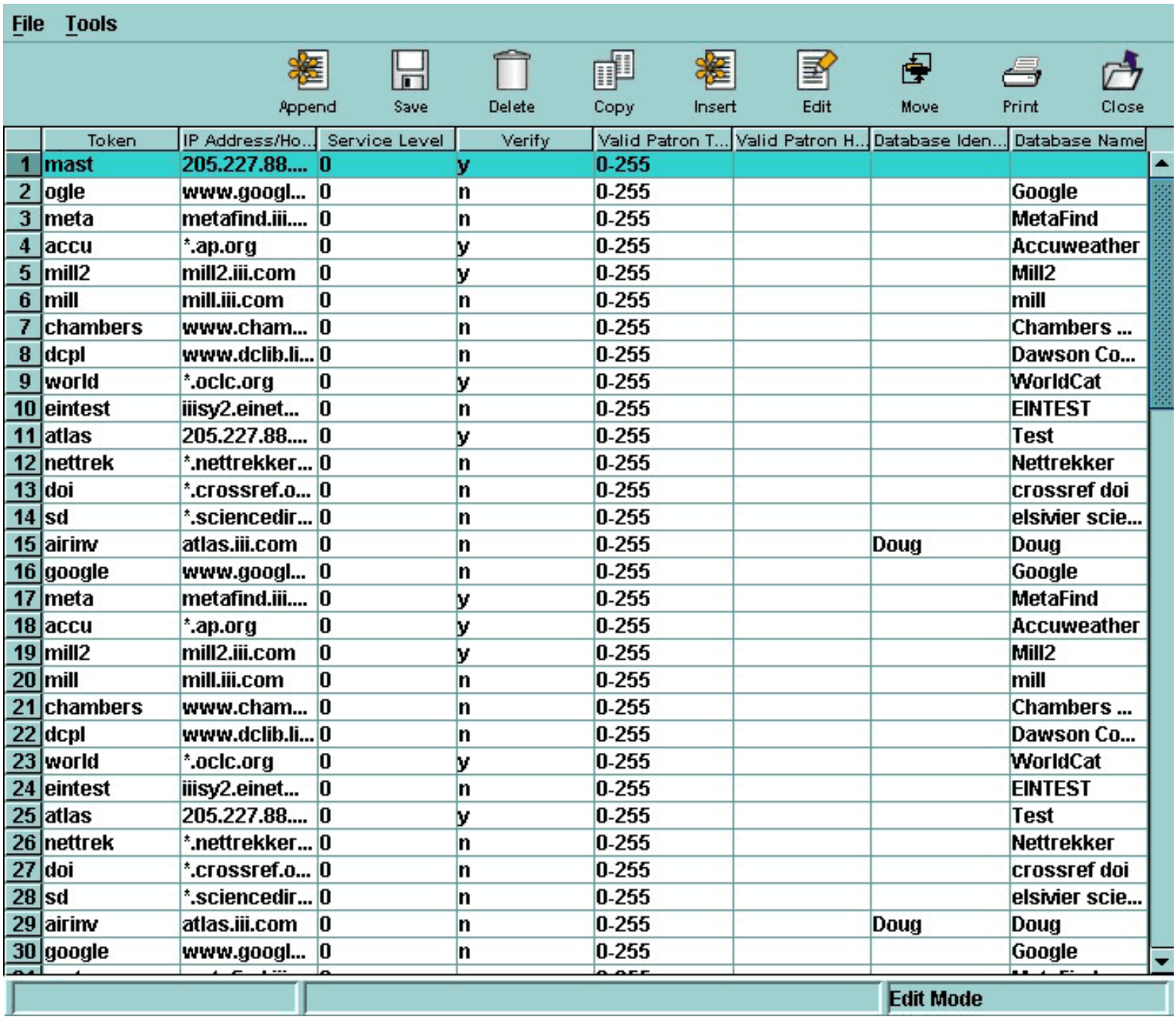
Close - This button closes the Forward Table.

PRINT THIS PAGE

close window

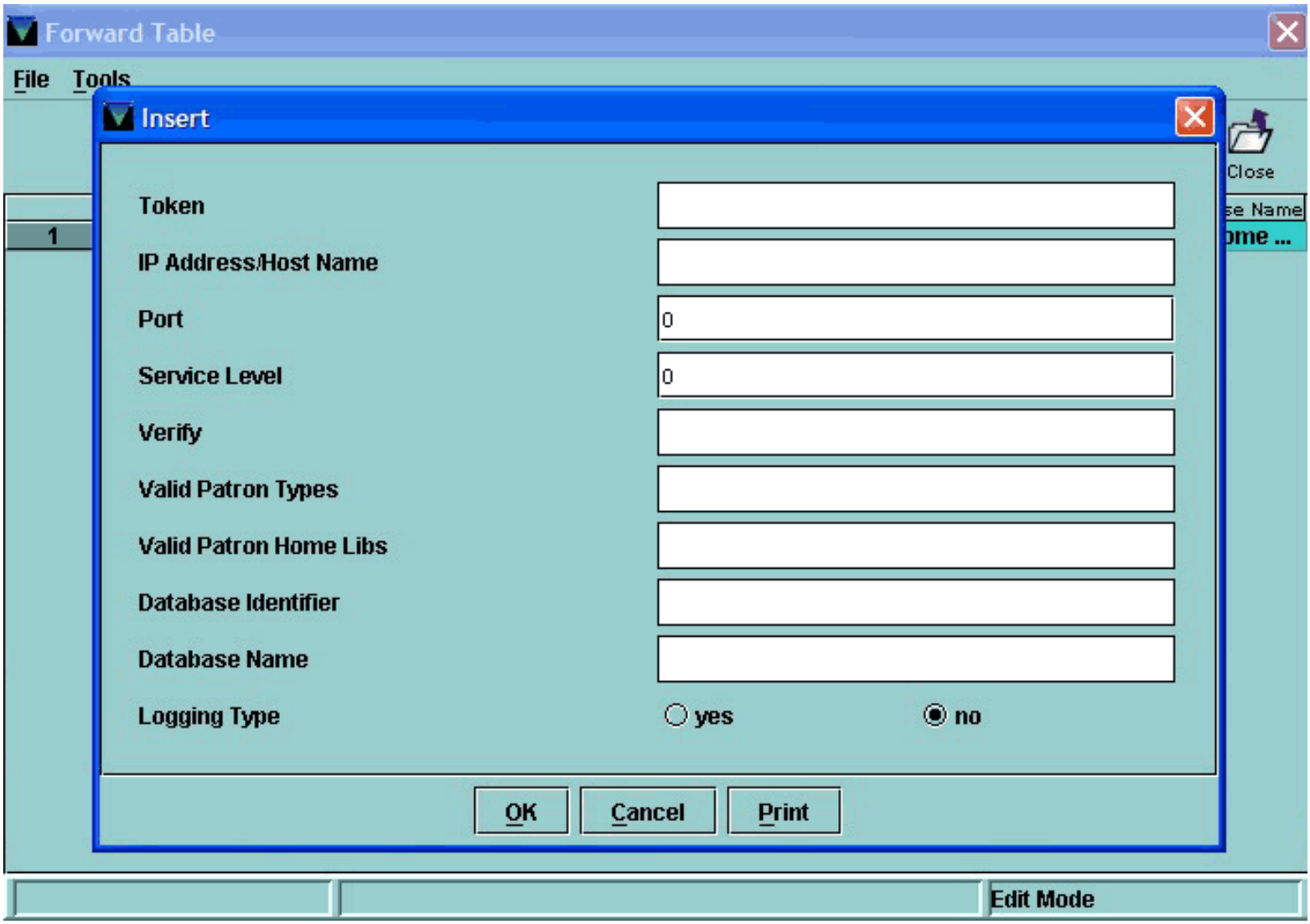
Adding, Appending and Editing the Forward Table

Once you have opened the Forward Table, you can Add an entry, Append an entry or Edit an entry.



	Token	IP Address/Ho...	Service Level	Verify	Valid Patron T...	Valid Patron H...	Database Iden...	Database Name
1	mast	205.227.88....	0	y	0-255			
2	ogle	www.googl...	0	n	0-255			Google
3	meta	metafind.iii....	0	n	0-255			MetaFind
4	accu	*.ap.org	0	y	0-255			Accuweather
5	mill2	mill2.iii.com	0	y	0-255			Mill2
6	mill	mill.iii.com	0	n	0-255			mill
7	chambers	www.cham...	0	n	0-255			Chambers ...
8	dcpl	www.dclib.li...	0	n	0-255			Dawson Co...
9	world	*.oclc.org	0	y	0-255			WorldCat
10	eintest	iiisy2.einet...	0	n	0-255			EINTEST
11	atlas	205.227.88....	0	y	0-255			Test
12	nettrek	*.nettrekker...	0	n	0-255			Nettrekker
13	doi	*.crossref.o...	0	n	0-255			crossref doi
14	sd	*.sciencedir...	0	n	0-255			elsivier scie...
15	airinv	atlas.iii.com	0	n	0-255		Doug	Doug
16	google	www.googl...	0	n	0-255			Google
17	meta	metafind.iii....	0	y	0-255			MetaFind
18	accu	*.ap.org	0	y	0-255			Accuweather
19	mill2	mill2.iii.com	0	y	0-255			Mill2
20	mill	mill.iii.com	0	n	0-255			mill
21	chambers	www.cham...	0	n	0-255			Chambers ...
22	dcpl	www.dclib.li...	0	n	0-255			Dawson Co...
23	world	*.oclc.org	0	y	0-255			WorldCat
24	eintest	iiisy2.einet...	0	n	0-255			EINTEST
25	atlas	205.227.88....	0	y	0-255			Test
26	nettrek	*.nettrekker...	0	n	0-255			Nettrekker
27	doi	*.crossref.o...	0	n	0-255			crossref doi
28	sd	*.sciencedir...	0	n	0-255			elsivier scie...
29	airinv	atlas.iii.com	0	n	0-255		Doug	Doug
30	google	www.googl...	0	n	0-255			Google

Click on the Append, Add or Edit buttons to modify the table. Clicking on one of these buttons will produce a a dialog box that looks like (if you choose edit, the fields may be filled out already):



Fill out or edit the fields as follows:

Token - The token element identifies each entry when reporting Web Access Management usage, such as setting up a statistical filter. Tokens must be unique and contain at least three, but no more than eight, characters. Tokens are case-sensitive (e.g., "forbes" and "Forbes" are considered to be different tokens). *NOTE*: These are not the same "tokens" associated with Web OPAC.

IP Address/Host Name - This is the IP address or host name of the remote server to the database the patron may access. If the host name of the server is used, the Web server must be able to resolve it using a domain name server.

NOTE

The administrators for the remote server must add the IP address of your Innovative server to their own access tables. Make certain to give them this information when setting up forwarding to their server.

If you are using the Innovative Proxy Server to access this remote server, you may include "wildcards" in the host name (e.g., *. **umi.com or 12.2.34.** *). They may be used, for example, to access remote databases or services mounted on more than one physical machine.

Service Level - The minimum Service Level required to access the remote server from the Innovative Web server. This service level is compared to the service level of the login that is using the Innovative Web server, e.g., **webpac, webremote** (for more information on Web OPAC logins, see the Limit Network Access page of this tutorial. If the login's Service Level is less than this value, the login will not be allowed to access the remote server.

For additional information, refer to the Innovative Guide and Reference Manual, Page # 101722: Login Administration

Verify - This element indicates whether Web Access Management performs patronverification (' **y** ') or not (' **n** '). Alternatively, the value of this element can be a Service Level (a number from 0-9); if the login's Service Level is less than the **Verify** value, the Web server requires patron verification; otherwise, verification is not required.

Valid Patron Types - Enter the range of Patron Type codes that are allowed to access this database. The range can be specified as a single number (e.g., 1), a list of numbers separated by commas (e.g., 1,2,5,15), a range of numbers (e.g., 1-34), or a combination of the two (e.g., 1,3,5-12,34,37,51-63). If you want to allow all patrons to forward requests to this server, enter 0-255.

Valid Patron Home Libs - Your library can restrict access based on the Home Library field in a patron record ("Patron Home Libs"). If your organization does not use the "Patron Home Libs" field, then leave this field blank.

Database Identifier - If a database vendor offers more than one database on a single server, a database identifier will be provided to you by that vendor for each database to which your library subscribes. An example of this is OCLC's First Search, which has access to Eric, PsychInfo, etc. Your library may decide to limit access for each of these databases separately, based on the login's service level or the value of the PTYPE field in the patron's record.

If a Web OPAC user selects the a database link, Web Access Management will use the data in the this field entry to validate the patron's service level and patron type and then forward the connection to the remote server. Similarly, if the user selects another database link, a different entry will be used.

When there are multiple Forward Table entries with the same information in the **IP Addr/Host Name** element, the entry without a database ID must appear after those that do use database IDs. This would mean that the entries for the different databases within First Search (ERIC, PsychInfo, GPO, etc) would go above a generic entry for First Search. This is because Web Access Management reads the Forward Table from the top to the bottom and uses the first entry that matches the URL. An entry with a blank database ID element matches every URL with an ID in this element.

Database Name - The database name can be a maximum of 30 alphanumeric characters and is used to report statistics.

Logging Type - This entry accepts two possible values:

- N - If logging type is 'N', don't log anything for that database
- Y - If logging type is 'Y', apply category filters to each request for that database and do one of the following:
  - If match a filter with category label "X", then don't log that request
  - If match a filter with any category label other than "X", then log with that category label
  - If no match found, then log without any category label

PRINT THIS PAGE
close window

Two Methods

There are two methods to using Web Access Management.

The **proxy method** uses a limited proxy and an automatic proxy configuration file to proxy the user's request on to the vendor server. This method requires browser configuration by the user. The proxy method of Web Access Management works with almost all sites, including those that use JavaScript.

The **proxy rewrite method** uses URL configurations to make the Innovative server act as a proxy server for patron browses. Using this method, the client browser software requires no configuration. Patron browses automatically use the Innovative server as a proxy to external resources.

Your library should decide which method it will use.

The next few pages explain in detail how to set up the two methods.

- Proxy Method
- Proxy Rewrite Method

PRINT THIS PAGE

close window

Proxy Method

The proxy method requires the browser software (Internet Explorer, Netscape, etc) to be configured to use the Innovative server as the proxy host. If your organization chooses to have browsers running in-house forwarded through the Innovative server (rather than reporting the IP addresses of the browsers to the subscription database vendor), your staff should perform this configuration. Your organization should also provide instructions on your Web pages informing those patrons who connect to the in-house Web OPAC from off-site how to do this. These instructions might appear on a separate page that is accessed via a link on the OPAC Menu page or a reference database page. A sample instruction page is provided as part of Web Access Management installation. This page is named **wamproxy.html** and you can view this page at:

http://yourlibraryIP/screens/wamproxy

Have your library's webmaster edit this page and link to it.

TIP : Some libraries have a link somewhere on their page called "Access Library Databases from outside the library" or "How can I access library databases from home?" and link to the wamproxy.html page.

CS Direct also has an FAQ page on the proxy method.

PRINT THIS PAGE
close window

Proxy Rewrite Method

The proxy rewrite method uses URL configurations to make the Millennium server act as a proxy server for patron browses. Using this method, the client browser software (Internet Explorer, Netscape, etc) requires no configuration. Authorized patrons finding a URL to a subscription database in the catalog simply click on the link for access. Please note that if you have records linking to subscription databases, this method requires that all the MARC 856 links will also need to change.

1. Your DNS administrator must make additional entries in the **hosts.db** file (or the equivalent file for your server), so that all addresses that have something preceding your server name get proxied appropriately.

   For example, if your Innovative server is: 123.45.67.89 web.library.edu, you must have an entry resembling:

   *.web.library.edu IN A 123.45.67.89

2. Add the PROXYDNS Web OPAC option to your **WWWOPTIONS** file. Use the following format:

   PROXYDNS=<Innovative server domain name>

   For example:

   PROXYDNS=www.library.edu

   The domain name defined in the PROXYDNS Web OPAC option must match the domain in your hosts.db file and in the links you use in the next step. Remember to restart your Web OPAC processes after editing the WWWOPTIONS file.

3. Create links from your individual pages to databases using the format for the proxy rewrite method.

   http://<port>-<target server>.<Innovative server>/<rest of URL>

Field	Description
<port>	The port number of the resource. If the port number is 80, substitute 0 (zero) for the port number.
<target server>	The address for the target resource.
<Innovative server>	The address of your Innovative server.
<rest of URL>	The rest of the URL for the target resource.

   For example, if your current link is:

   http://galenet.gale.com/a/acp/name/db/bgmi/

   Change the link to:

   http://0-galenet.gale.com.web.library.edu/a/acp/name/db/bgmi/

   Or, if your current link is:

http://search.epnet.com:5670/

Change the link to:

http://5670-search.epnet.com.web.library.edu/

CS Direct also has an FAQ page on the proxy rewrite method.

PRINT THIS PAGE

close window

Limit Network Access

Millennium allows libraries to limit access to the system based on the IP address of the user who is logging in. This can be used to restrict access to reference databases or other computer systems to on-campus library users only. This is often required under the terms of a database vendor's licensing agreement. You may also limit access to the Web OPAC, Millennium servers, and external servers that your library may have acquired.

The library may associate each of its available reference databases with a specific *service level*, a number from 0 to 9 (see also Level of Service in **Gateway Setup**). The library may also associate each of its partners (see INNOPAC Partners in **Optional Features**) with a specific service level. If a login's service level is lower than that for a particular database or partner, INNOPAC will not offer the menu option for that database or partner. For information on how to assign a *service level* to a reference database or INNOPAC Partner, see **Service level for "Y > Search another DB"** in OPAC Options.

When INNOPAC acknowledges a user's login, it checks the IP address of the user's machine (the machine from which the user is logging into the INNOPAC machine), against a list of IP addresses and corresponding service levels which is maintained by the library using the **Limit NETWORK access** function. INNOPAC assigns the user the *service level* that has been determined for his or her IP address.

At a site with reference databases, the system compares the user's service level against the service levels that have been assigned to each individual database. INNOPAC only allows access to those databases whose service level is *less than or equal* to the user's service level.

To set user service levels for the various originating IP addresses, select the Limit NETWORK Access option.

Service Levels in Web Access Management offer an optional method of controlling database vendor access for specified computers within a room, building, branch or campus. You use the service level number in conjunction with a service level set in an HTTP entry in Limit Network Access. The service level acts as a privilege, allowing or denying access to databases.

First you make entries for the IP addresses of computers in HTTP Administration Access. Next you will set corresponding Service Levels in the Web Access Management Forward Table.

Open a Telnet session for your Millennium System:
A > Additional System Functions
A > Alter System Parameters
L > Login names & parameters
N > Limit Network Access
Select HTTP

The HTTP Access Administration screen displays.

Add entries for the IP addresses of computers you want to set up, or use existing IP addresses.

To allow access to a database vendor for specific IP addresses and not require patron verification, set a service level number for the IP addresses in HTTP Access Administration that is **higher than or equal to** the service level for the vendor in the Service Level column in the Web Access Management Forward Table.

To allow access but require patron verification, set a service level in HTTP Access Administration **lower** than the service level specified in the Web Access Management Forward Table.

To **not** allow access to a database vendor for IP addresses, set a service level in HTTP Access Administration that is **lower** than the service level set in the Web Access Management Forward Table.

For example:

IF Service level = 3 in the Web Access Management Table **Service Level** column AND
Service level for IP addresses = 4 in HTTP Access Administration;

THEN Access is allowed for patrons connecting from the specified IP addresses and patron verification is not required.

REMINDER *: Restart the Web and Proxy servers after changing the Web Access Management table.*

For more information on how Service Levels work, please read the FAQ on CSDirect.

PRINT THIS PAGE
close window

Filters

The Web Access Management Statistics Report Filters allow your library to categorize and filter different types of HTTP requests in order to configure your statistics to provide you with the results your organization requires.

Whenever a patron attempts to access resources that requires a proxy, your system can generate a request to that resource and compares that request against your Web Access Management Statistics wam_filter file. Upon purchase, Web Access Management includes a default version of this file, but you can customize the file to better meet your needs.

The wam_filter file is a text file that resides in the **/http/live** directory on your Millennium server (port 80 is your live directory). To edit this file, download it to your local PC using an FTP program such as the one included in the Web Master mode of the Millennium Administration module, then edit it with a text editor of your choice (i.e. Word Pad, Simple Text, etc). After you have made your changes, replace the file using the same FTP method.

Below is an example of a wam_filter file.

```
#Index Number|Category Name|WAM token(s)|Apply to|
Regular Expression
100|images|*|head|image\/.*
#100|X|*|head|image\/.*
101|js script|*|head|application\/x-javascript
102|css*|head|text\/css
103|redirect (302)|*|head|HTTP.*302
104|forbidden (403)|*|head|HTTP.*403
105|page not found (404)|*|head|HTTP.*404
106|bad gateway (502)|*|head|HTTP.*502
107|JSTOR Page View|JSTOR|url|.*\/view\/.*
108|HTML page|*|head|text\/html
109|pdf download|*|head|application\/.*pdf
```

The elements included in the wam_filter file are in the following pipe-delimited format and are described below. Modify only the elements specified.

Index Number|Category Name|WAM token(s)|Apply to|Regular Expression

Index Number - This is a unique number that identifies the filter category. You can repeat the index number if you want to combine several filters into a single category. The filters do not have to appear in numerical order.

Category Name - This is a custom name to categorize the request. Web Access Management compares each patron request against the wam_filter file and categorizes the request using the Category Name of the first successful match. If you do not want to log any requests matching a particular line in the wam_filter, enter single 'X' into this element.

WAM token(s) - A comma-delimited list of tokens used in the Forward Table. The wam_filter is applied to those databases matching the list of tokens.

Use an asterisk (*) to apply the wam_filter to all resources.

Apply to - There are two choices: url and head and they are described below. This element specifies whether the Regular Expression element should match against either the url or the head.

url-matches against the portion of the URL which follows the host:port.

head-matches against the http header of the response from the server.

Regular Expression - A regular expression is required for the filter to work. When using regular expressions, you must escape characters that are part of regular expression syntax such as '.', '/', or '?'. Standard POSIX regular expressions are supported. *Innovative Interfaces does not provide training on regular expressions, however, many libraries find that the regular expressions in the file that comes with WAM suite their needs. However, if you are not familiar with regular expressions, you should read about standard regular expressions before modifying this element.*

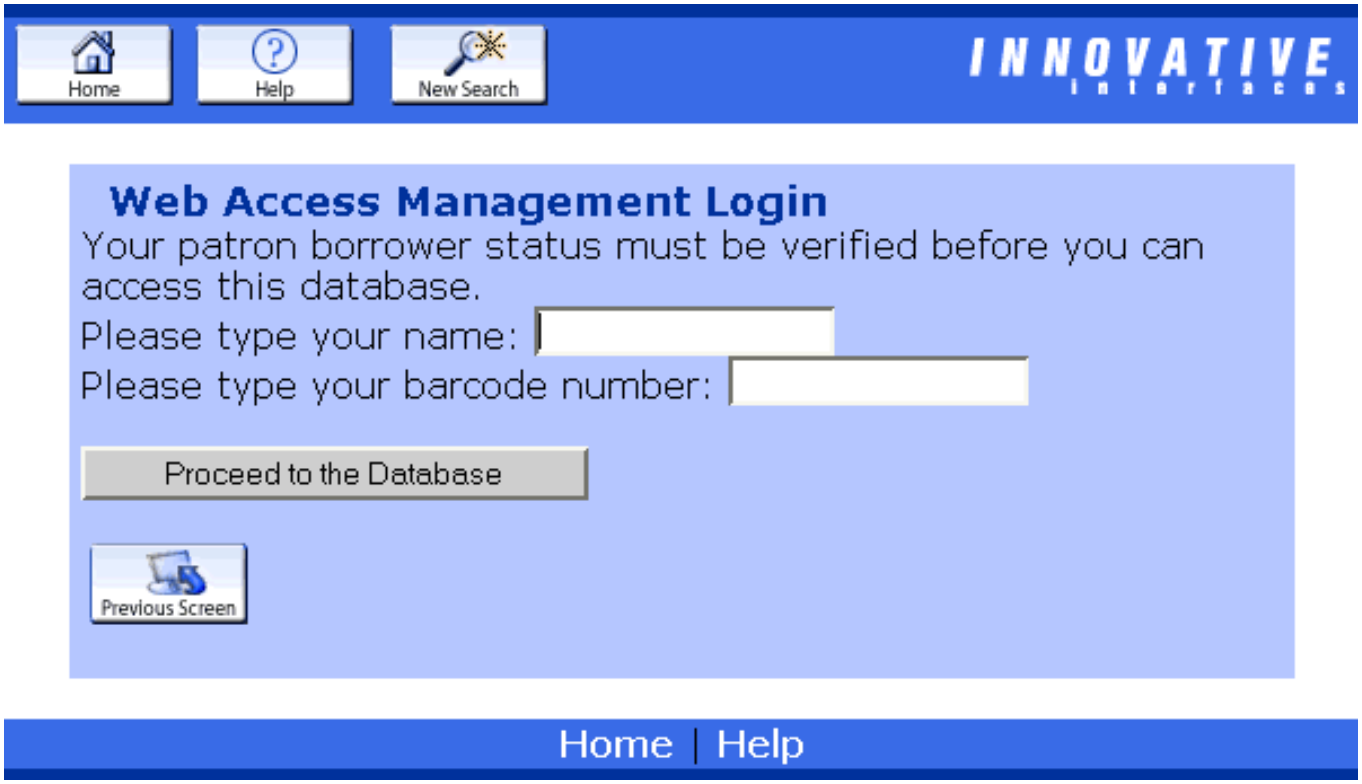
TIP : You can comment out a line with in the wam_filter file. To do this, start the line with ##. This will comment out the line and the line will be ignored.

PRINT THIS PAGE

close window

Patron Verification and Web OPAC

If you specify that patrons need to verify themselves in the Forward Table, your library will need to modify the pverify2_web.html file in the Web OPAC. This file may display as follows:



This page can be modified using the following tokens:

<!--{toplogo}-->	Inserts the and tags that begin an HTML page and displays the HTML defined in the TOPLOGO line in the WWWOPTIONS file. This must be the first line in the pverify2_web.html file.
<FORM>	The start of the HTML form. This tag is required.
<!--{iferrmsg}-->	System checks to see if the form has been submitted properly.
<!--{iferrmsgisPIN}-->	System checks to see if the patron record needs a PIN.
<!--{newpinmsg}-->	Prompts the user to "Please enter a new PIN" if PIN verification is required and the patron record does not have a PIN.
<!--{else}-->	If the <!--{newpinmsg}--> token logic does not apply, the form uses the following token.
<!--{errmsg}-->	Displays various error messages to the user explaining why the patron record cannot be accessed (e.g., "Invalid PIN," "Sorry, cannot locate patron record," "Sorry, name entered does not match name in record," or "Please fill in ALL of the following information").
<!--{xif}-->	Closes the **<!--{iferrmsgisPIN}-->** block.

<!--{xif}-->	Closes the **<!--{iferrmsg}-->** block.
<!--{nameexample}-->	Example for Name; reads the OPAC Option Patron self-identification prompts & examples, "Example for name prompt."
<!--{nameprompt}-->	Prompt for Name; reads the OPAC Option Patron self-identification prompts & examples, "Prompt for name."
<!--{name}-->	Input for Patron Name.
<!--{barcodeexample}-->	Example for barcode; reads the OPAC Option Patron self-identification prompts & examples, "Example for patron ID."
<!--{barcodeprompt}-->	Prompt for barcode; reads the OPAC Option Patron self-identification prompts & examples, "Prompt for patron ID."
<!--{barcode}-->	Input for Patron Barcode or ID Number.
<!--{ifneedspin}-->	System checks if PIN validation is required, and if it is not required, the system proceeds to the **<!--{submit}-->** token.
<!--{iferrmsgisPIN}-->	System checks if patron record does not have a PIN.
<!--{newpinmsg}-->	Prompts the user to "Please enter a new PIN."
<!--{pin1prompt}-->	Prompt for **<!--{pin1}-->** , hard-coded to display "Enter Your PIN."
<!--{pin1}-->	First input for new PIN.
<!--{pin2prompt}-->	Prompt for **<!--{pin2}-->** , hard-coded to display "Enter Your PIN Again."
<!--{pin2}-->	Second input for new PIN.
<!--{else}-->	If PIN is needed and patron record has a PIN, system prompts for PIN input.
<!--{pininstructions}-->	Instructions or examples to the user for **<!--{pin}-->** . Reads the OPAC Option Patron self-identification prompts & examples, "Example for PIN."
<!--{pinprompt}-->	User prompt for **<!--{pin}-->** . Reads OPAC Option Patron self-identification prompts & examples, "Prompt for PIN."
<!--{pin}-->	User input for patron's PIN.
<!--{xif}-->	Closes the **<!--{iferrmsgisPIN}-->** block.
<!--{xif}-->	Closes the **<!--{ifneedspin}-->** block.
</FORM>	Declares the end of form. This tag is required.
<!--{startover}-->	Offers a **Start Over** button which goes to the URL in the PSTARTOVER Web OPAC option.
<!--{botlogo}-->	Displays the HTML defined in the BOTLOGO Web OPAC option. Unlike the token behavior in other Web OPAC custom forms, the **<!--{botlogo}-->** ; token does insert the closing </BODY> and </HTML> tags for the pverify2_web.html form.

For External Patron Verification, the following tokens are used:

<!--{ifextpat}-->	If the External Patron Verification option has an entry for the port serving this file, the system executes the commands in this block.
<!--{extpatid}-->	Inserts the External Patron Verification ID text box.
<!--{extpatpw}-->	Inserts the External Patron Verification password text box.
<!--{xif}-->	Closes the block.

PRINT THIS PAGE

close window

Multiple IP Support

Some libraries purchase support for multiple IP's. If your library did not purchase support for multiple IP's you can skip this section of the tutorial.

Multiple IP's allow the library to specify additional incoming IP's that may have access to the various databases. This could be very useful in a university setting, where the library may have its own IP address that is different from the campus. Having multiple IP support will allow the library to add the campus IP so any computer connected to the campus IP will be recognized as if it were in the library.

You must complete the following steps before you set up Multiple IP Support for Web Access Management:

1. List all incoming IP addresses and incoming patron types for which you want patrons directed to specific vendor databases. For example, you might want to limit access to a medical database to medical students. In this case, you will need a patron type for medical students.
2. Note your system's IP addresses allocated for use by Multiple IP Support for Web Access Management.
3. Associate the correct alternate IP address with an appropriate specific database (e.g., a medical database, a law database), incoming IP addresses, and incoming patron types.
4. Inform your database vendors of the alternate IP addresses that they can expect from your system. They should associate the appropriate databases with the incoming IP address (e.g., the vendor should associate your specified IP address range for medical students with the vendor's medical database).
5. **Software Only Customers** : Customers with a "Software Only" package must configure the system for IP ranges. Review the Software Only Multiple IP Setup section for details.

This next few pages detail setting up multiple IP support. Click on one of the links below to find out more information on that topic.

- Verified and Unverified Patron Table
- Considerations for 'software only' customers (customers that initially only purchased the software, and not the server, from Innovative Interfaces.)

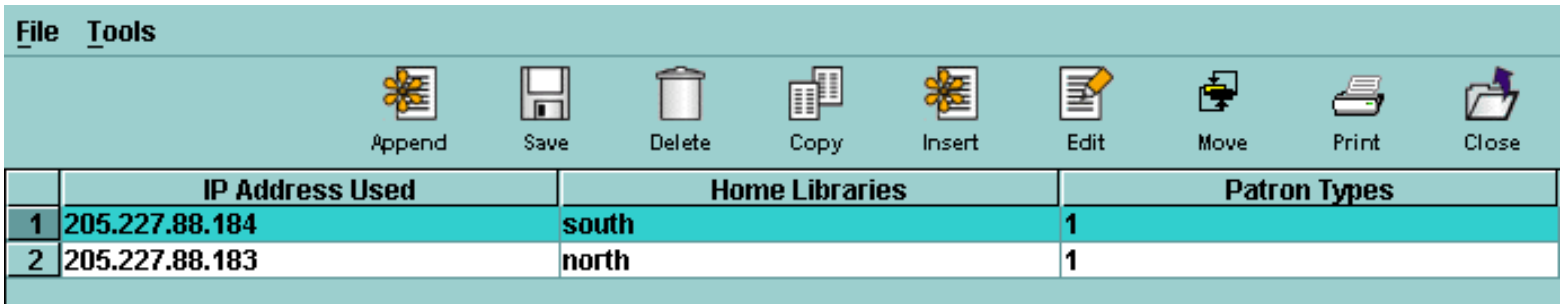
PRINT THIS PAGE

close window

Verified Patron Table

***Please Note**: You must be authorized for function 698 (Edit the Web Access Management Verified Patron Table) to edit the Verified Patron Table. If you are authorized for function 651 (View System Parameters) but not for function 698, you can view this file but cannot edit it. See your Millennium System Administrator for details.*

The Verified Patron table defines the *patron types that must authenticate themselves* before accessing a restricted database (as defined in the Forward Table and the Limit Network Access table) via an alternate IP address set by your organization. Add entries for each incoming patron type, or group of patron types, that will send an alternate IP address to the database vendor. The Verified Patron table looks like:



	IP Address Used	Home Libraries	Patron Types
1	205.227.88.184	south	1
2	205.227.88.183	north	1

The Verified Patron table has three data fields in each entry that need to be filled out.

IP Address Used : This entry is the alternate IP address to be sent to the vendor.

Home Libraries : If your organization does not differentiate between incoming patron types sending the same IP address to the vendor, enter "all" at this prompt. For example, for all patrons of PTYPE 60 to send the same IP address to the vendor, set "Home Libraries" to "all."

TIP : If your organization differentiates between the IP address sent to the vendor by home library and the IP address sent by the patron type, enter the five-character Home Library location code. If the code is shorter than five characters, insert extra spaces at the end to make it five characters long.

Patron Types : Enter the patron types. Entries can be comma-delimited or in a range, for example, "1-5,10,60". Enter "all" for all patron types. You can use open-ended ranges to include all patron types to the end of the list. For example, "1-5,10,55-" would include patron types 1 through 5, 10, and 55 to the end.

Use the following toolbar options to create entries in or edit the Verified Patron table.

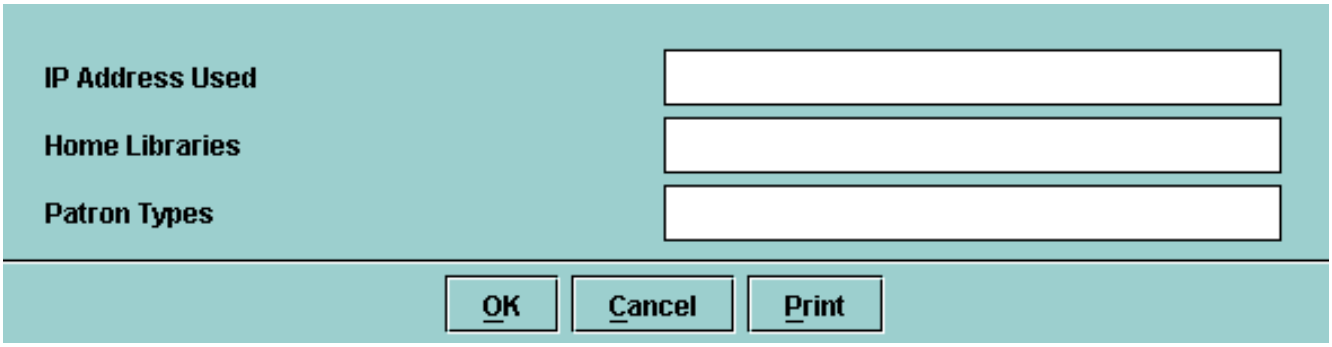
Append : Select this option to add a new entry to the end of the Verified Patron table. The system will prompt you to key each data element for the new entry (see the description of the data elements above).

Save : To save your changes to the Verified Patron table, choose Save. If you make changes to the Verified Patron table and do not save those changes, the system prompts you to save before you exit the Verified Patron table.

Delete: To delete an entry, select the entry and choose Delete. The deletion is not final until you save your changes.

Copy : To add a new entry that is similar to one that already exists in the table, you can copy the existing entry and then modify the appropriate data elements. The new entry is added to the end of the table.

Insert : To insert a new resource entry, choose Insert. At the Insert dialog (shown below), answer the prompts as needed.



Choose OK to save the changes once you are done or choose Cancel to cancel the changes. Choose Print to print the entry you are adding.

Edit : To edit the elements of an existing entry, select the entry and choose Edit. Make your changes in the dialog box that appears, then choose OK to save the changes once you are done or Cancel to cancel the changes. Choose Print to print the entry you are adding.

Move : To reorganize the entries, select the entry that you want to move and choose Move.

Print : To print the Verified Patron table, choose Print. Select the printer to use, then choose OK.

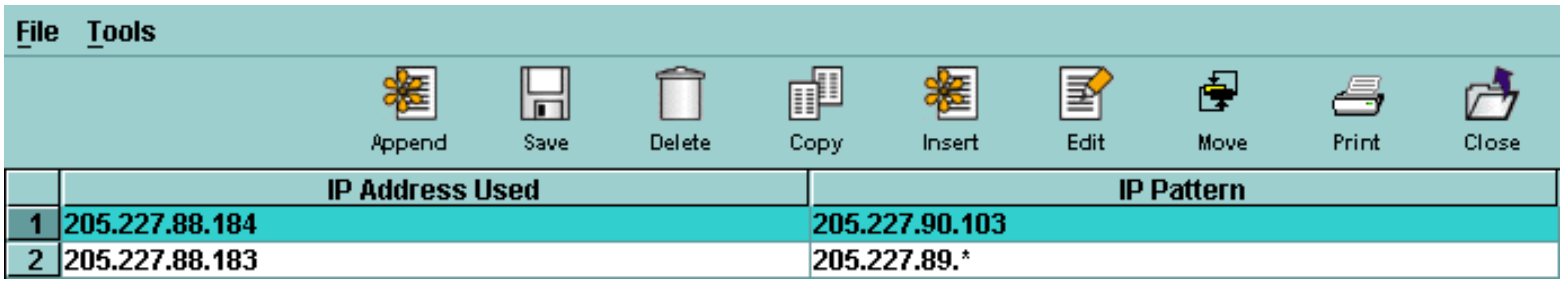
Close : Choose Close to close the Verified Patron table.

PRINT THIS PAGE
close window

Unverified Patron Table

You must be authorized for function 697 (Edit the Web Access Management Unverified Patron Table) if you need to edit the Unverified Patron Table. If you are authorized for function 651 (View System Parameters) but not for function 697, you can view this file but cannot edit it. See your Millennium System Administrator for details.

The Unverified Patron table identifies patrons coming from known or trusted IP addresses *who do not have to authenticate* to access a database (as defined in the Forward Table and the Limit Network Access table). These IP addresses may be for in-library or on-campus computers. Use the Unverified Patron table to set up and maintain entries of known and trusted IP addresses and the associated alternate IP address to use for Multiple IP Support with Web Access Management.



	IP Address Used	IP Pattern
1	205.227.88.184	205.227.90.103
2	205.227.88.183	205.227.89.*

The Unverified Patron table has two data fields that require information. For each entry you add in the Unverified Patron table, you must include:

IP Address Used: This entry is the alternate IP address to be sent to the vendor.

IP Pattern: The incoming, trusted IP address. You can enter IP addresses as single entries, "wildcarded" entries, or in a range with part of the IP string substituted ("globbed"). Unlike the Limit Network Access table, the Unverified Patron table requires decimal places and a range for each decimal place in the IP address (e.g., 123.6.*.*, 123.20.[0-2][05].*). You can have multiple IP patterns for the same IP address.

- Enter wildcarded entries as follows:
  123.234.*.* - This is the entire Class-B network at 123.234.
  123.234.245.* - This is the entire Class-C subnet at 123.234.245.

- Enter globbed entries as follows. You must use opening and closing square brackets ([and]) to successfully glob entries. You can combine globbed entries with wildcarded entries:

  123.456.7.[1-9][0-9] - This is the IP range from 123.456.7.10 to 123.456.7.99. Note that globbed ranges are inclusive. To exclude an IP address in a globbed range, account for the range up to the excluded IP address and then immediately after the excluded IP address. For example:

  123.456.7.[1-6][0-9] - this is the IP range from 123.456.7.10 to 123.456.7.69
  123.456.7.[7-7][0-8] - this is the IP range from 123.456.7.70 to 123.456.7.78
  123.456.7.[8-9][0-9] - this is the IP range from 123.456.7.80 to 123.456.7.99
  The IP 123.456.7.79 is excluded from the example above.

NOTE

Do not use leading zeros for wildcarding and globbing in this table. For example:
123.23.[000-025].* should be 123.23.[0-2][0-5].*
123.23.34.[002-009] should be 123.23.34.[2-9]

TIP : Do **not** enter the main system IP address or any of the alternate IP addresses listed in the "IP Address" prompt.

Use the following toolbar options used to edit the Unverified Patron table.

Append : Select this option to add a new entry to the end of the Unverified Patron table. The system will prompt you to key each data element for the new entry (see the description of the data elements above).

Save : To save your changes to the Unverified Patron table, choose Save. If you make changes to the Unverified Patron table and do not save those changes, the system prompts you to save before you exit the Unverified Patron table.

Delete : To delete an entry, select the entry and choose Delete. The deletion is not final until you save your changes.

Copy : To add a new entry that is similar to one that already exists in the table, you can copy the existing entry and then modify the appropriate data elements. The new entry is added to the end of the table.

Insert : To insert a new entry at the current selection point, choose Insert. On the Insert dialog, answer the prompts as needed. Choose OK once you are done or choose Cancel to cancel the changes. Choose Print to print the entry you are adding.

Edit : To edit the elements of an existing resource entry, select the entry and choose Edit. Modify your entry as needed. Choose OK once you are done or choose Cancel to cancel the changes. Choose Print to print the entry you are editing.

Move : To reorganize the entries, select the entry that you want to move and choose Move. You will then be prompted to enter a enter the row number and choose OK. The entry will be inserted at the selected point, and all succeeding entries will be shifted down one position.

Print : To print the Unverified Patron table, choose Print. Select the printer to use, then choose OK.

Close : Choose Close to close the Unverified Patron table.

PRINT THIS PAGE
close window

Unverified Patron Table

This section of the tutorial explains how to work with WAM and things to keep in mind if you need to make changes.

- Statistics
- Web Bridge
- Meta Find
- Changing Access

PRINT THIS PAGE

close window

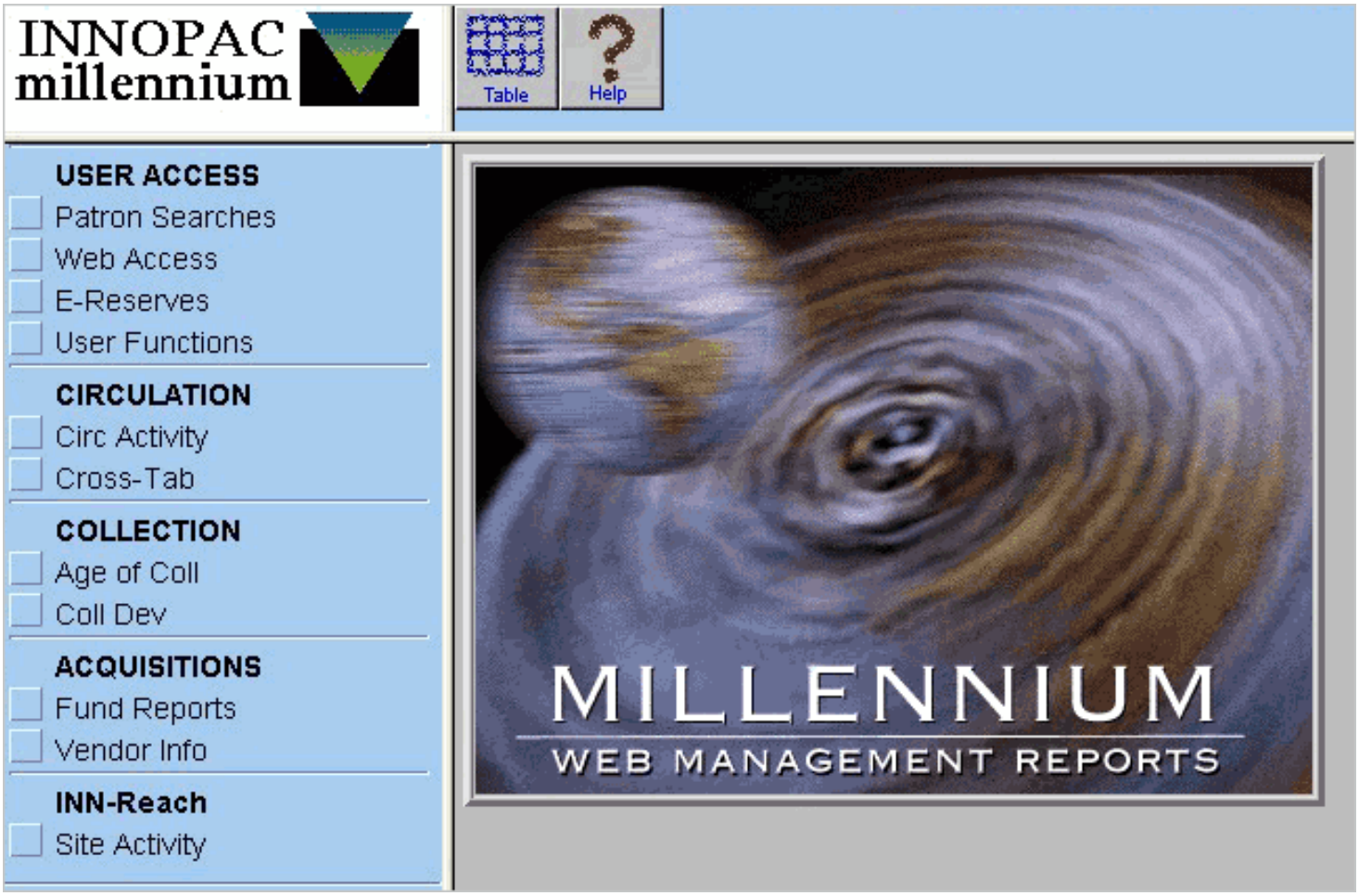
Statistics

Using Web Access Management, you can track usage statistics via Millennium Web Management Reports. Using Filters will allow your library to customize and configure your statistics to provide you with the results your organization requires.

You can access web management reports via your web OPAC and add /manage to the end of the address:

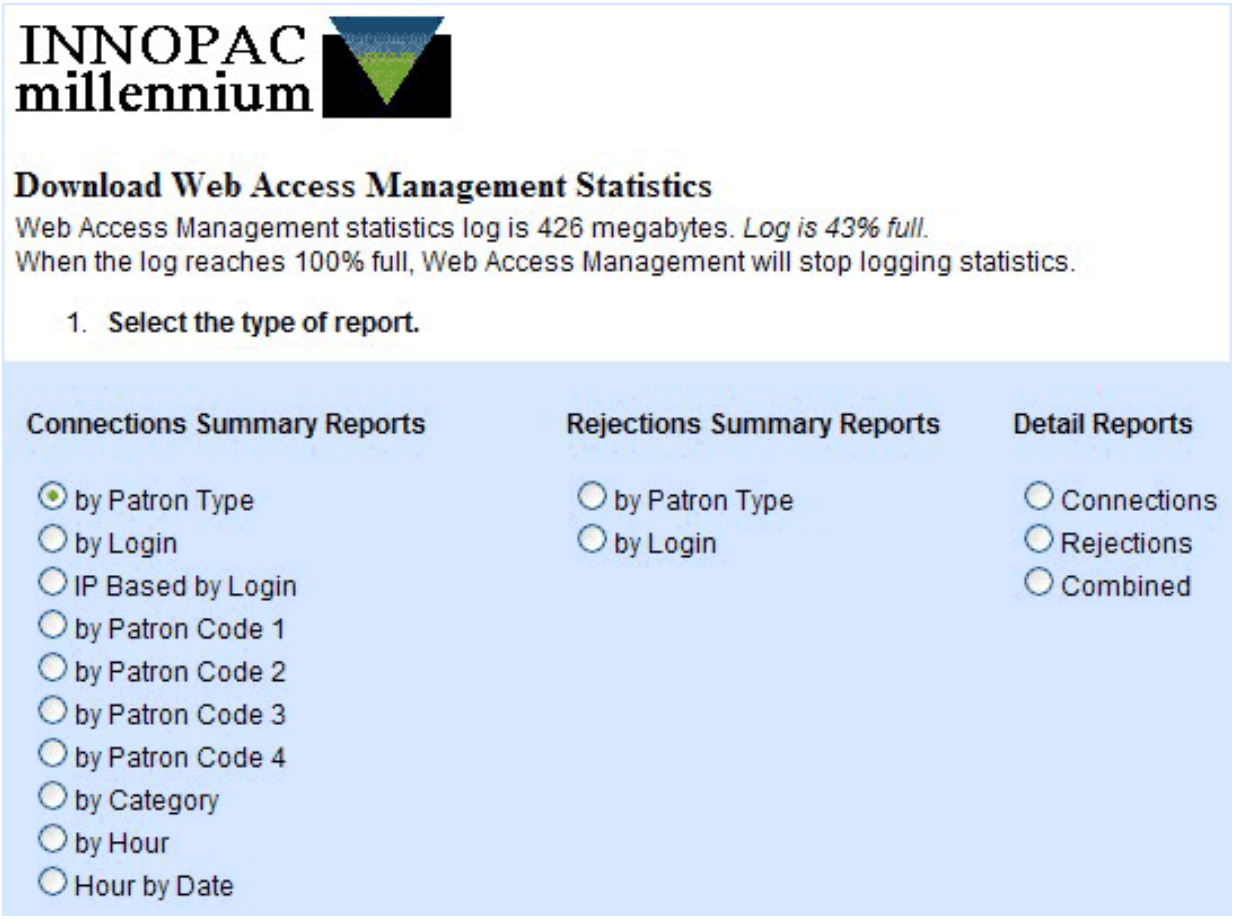
http://yourlibraryOPACIP/manage

You will then see a screen similar to the one below:



Once here, click on Web Access under User Access. You will be prompted to enter your Millennium initials and password.

You will then be taken to a screen where you can specify your criteria for statistics.



Once here, specify the following parameters for your report:

- **Report type** - Select one report type by choosing the appropriate radio button.
- **Resource databases** - You can choose All online resources or a single resource. You also can choose multiple resources by pressing the Ctrl key while choosing resources from the list.
- **Date/time range** - Indicate the date/time range by choosing the appropriate radio button.

If you choose the User Specified date/time option, you must specify a Start date. Then you can choose to enter an End date manually, or have the system determine an end date. When you choose Calculate End Date, the system sets the end date so that the range of records downloaded is as close to 16,000 megabytes as possible (16,000 megabytes is the program limit for Excel spreadsheets).

If you do not specify a start time, you must specify an end time. By default the system uses the first entry in the database as the start time.

Choose one of the following options to generate the report:

- **Download Only** - You are prompted to use the system-generated default report name and save the report file or change the filename and to save the report file to your desktop. The statistics that comprise the report remain on your system for future reporting.
- **Download and Delete** - You are prompted to specify a file name and to save the report file to your desktop. After you save the report file, the system prompts you with a confirmation dialog to delete all statistics for that date range. The confirmation dialog indicates the date and time parameters for these statistics.
- **Delete Only** - The system prompts you with a confirmation dialog to delete all statistics for that date range. The confirmation dialog indicates the date and time parameters for these statistics.

After you download a report, you can view the data in a spreadsheet program (for example, Excel), which enables you to manipulate the data for better analysis.

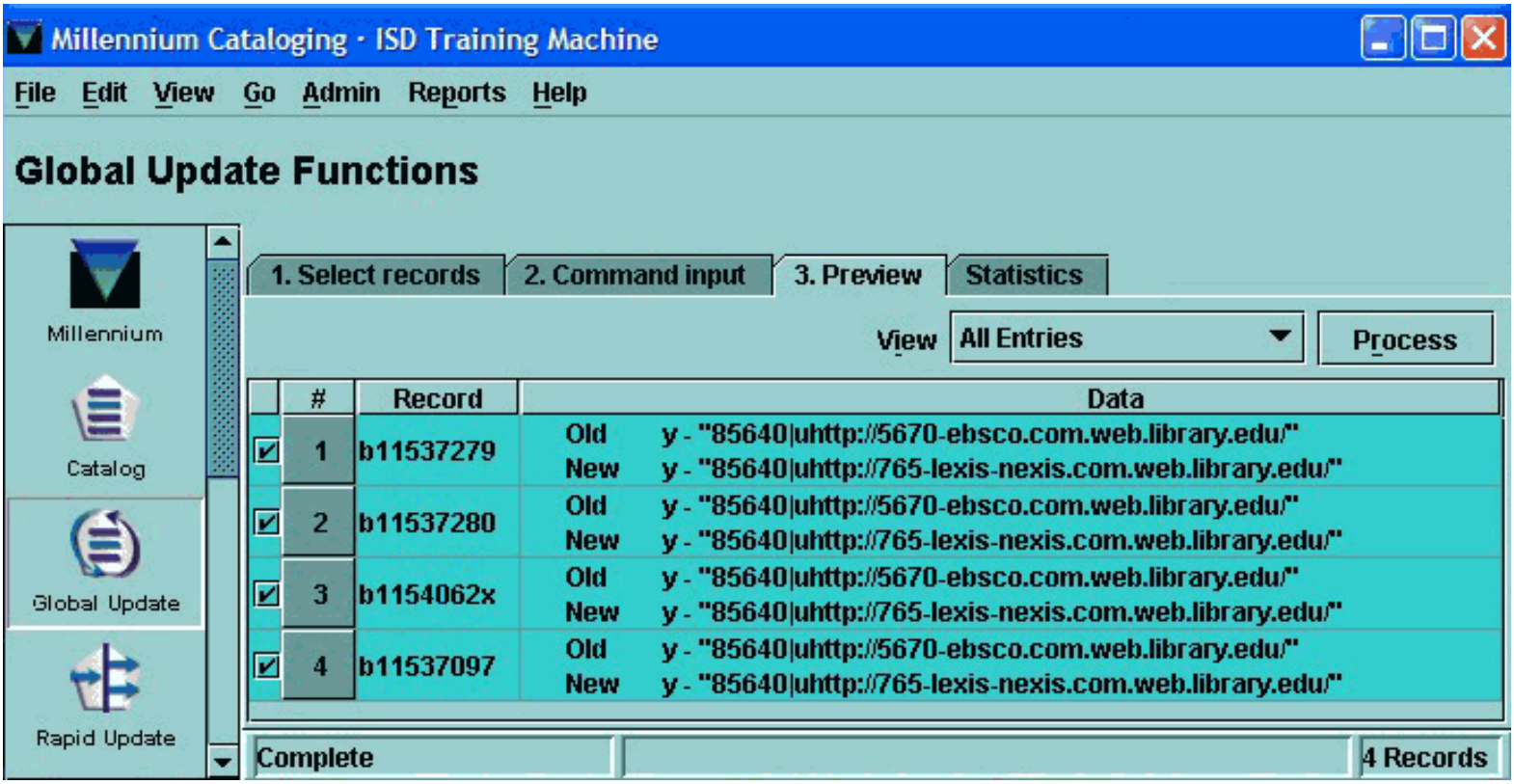
PRINT THIS PAGE

close window

Changing Access

If your library decides to start making changes to access, here are some tips and ideas for workflow to make the transition easier.

Besides changing the Forward Table from the old database vendor to the new database vendor, if you use the Proxy Rewrite Method, you probably need to also do some records maintenance. Use Create Lists to generate a file of records that will need to be changed. After this list is created, use Global Update to update the records. Below is an example for changing access from EBSCO to Lexis-Nexis in the Global Update preview window just before the changes are made.



If your statistics do not have the options that you thought they might, recheck your Filter set-up. Go though each line when you are checking them.

PRINT THIS PAGE
close window

WebBridge

This page of the tutorial is intended to provide some tips on using WebBridge (Product Code 201AMB) and Web Access Management to troubleshoot each other. Libraries that have not purchased WebBridge can skip this page.

Before proceeding, make sure you have ruled out the common issues for not connecting: can you access another www link (www.iii.com, csdirect.iii.com, www.google.com) through your browser; is your machine plugged securely into the wall; can the problem be replicated on another machine.

If linking does not work with WebBridge, try the link in the address bar. If it does not work, check your address and contact your vendor in order to rule out a mistyped address or down vender server. IP authentication can come into the equation, either in LNA or on the vendors' server, if you are using a PC within the correct IP range.

If the address is correct, and the vender server is functioning, check your syntax if using the Proxy Rewrite Method and in the WebBridge table.

If you are asked to authenticate, check your Forward Table. Specifically check the IP address, Service Level, Verify and Verify Patron Type. These could be out of sequence with what library is intending.

PRINT THIS PAGE

close window

MetaFind

Innovative Interfaces' MetaFind (Product Code 201AMF) uses Web Access Management to access external electronic resources. If your library has not purchased MetaFind, you can skip this section.

MetaFind is currently hosted by Innovative on a server located at our headquarters in Emeryville, California, USA. You can access MetaFind directly by using the link provided to your organization by Innovative.

A MetaFind link in your record may look something like:

http://metafind.iii.com/muse/servlet/MusePeer?action=logon&userID=<Innovative Supplied ID>&userPwd=<Innovative Supplied Password>

Innovative requires remote access to each restricted or licensed resource you request to profile for your MetaFind and Innovative recommends using the Web Access Management Proxy Rewrite Method for this purpose.

Innovative Interfaces also recommends that the libraries use service levels for authentication. However, libraries can also use ssl certification. For this, we recommend that you use a wildcard ssl cert with our Proxy Rewrite Method, and we also recommend that the name of the ssl cert, wildcard or not, match the name of the DNS that you use to rewrite their links.

Enter each resource in your Forward Table and provide Innovative with the rewritten URLs for each licensed resource.

The following is an example of a Metafind link using Proxy Rewrite Method:

http://0-metafind.iii.com.www.yourorganization.org/muse/servlet/MusePeer?action=logon&userID=<Innovative Supplied ID>&userPwd=<Innovative Supplied Password>

For example, you can assign a Service Level of 3 to patron types accessing MetaFind from within your organization's authorized IP range and then enter metafind.iii.com in your Forward Table. You can specify that users with a Service Level of 3 or higher will be allowed access without being prompted. When users connect to MetaFind via WAM, the Innovative server checks the Service Level associated with the incoming patrons. Patrons with a Service Level of 3 or higher are passed through to MetaFind. Other patrons (for example, coming from an unknown IP and assigned a Service Level of 0) will have to authenticate themselves before getting through. Patrons without a valid Innovative Patron Record will not be able to get through.

Also, make sure you add generic entries be added to the Forward Table. An example of this is below.

search.epnet.com = *.epnet.com

PRINT THIS PAGE
close window

Solutions

This section of the tutorial is intended to provide you with information on troubleshooting issues that may arise, and an FAQ page.

- Troubleshooting
- FAQ
- Consideration for Different Servers

PRINT THIS PAGE
close window

Troubleshooting

Below are some suggested areas to check if you are having issues connecting to your database vendors.

Proxy rewrite method is not working; error message indicates web site not found, cannot display this page, or hostname not resolving:

When you create a wildcard entry for your library's DNS make sure you use the proper IP address of your Innovative server, not an alias. Use only the IP address. For example, your DNS wildcard entry should look like this:

*.web.library.edu IN A 123.456.78

If you have changed the IP address originally set up for your server, you must advise Innovative.

When you create the URL for a database entry on your Web page, make sure that the URL is the same as the entry for the database in the Forward Table, and the exact port number is entered if it is not 80.

Database vendor connections are very slow, or error messages indicates that the IP address is not valid and a login is required:

Check that the vendor IP address or domain name in the Web Access Management table is correct.

Many vendors have variations in the domain name IP address. To overcome this, use the asterisk wildcard in the domain name:

e.g. *.oclc.org

An error message indicates that the server won't act as a proxy, or you are not authorized to view a page:

The patron may be not allowed to access a database because his or her Ptype is not included in entry in the Web Access Management table or the Forward Table. Re-check these two tables for inconsistencies.

In addition to the above solutions, some possible reasons why you cannot connect to database vendors set up in the Forward Table, or do not see a patron verification screen, are as follows:

1. Check that the vendor IP address in the Forward Table is correct. It should contain only the vendor's server IP address or domain name, e.g. **www.eb.org.** Do not include subdirectories or login information after the server IP address. Add those details to the database vendor HTML link on your Web OPAC.
2. If you used the asterisk wildcard in a vendor's IP address make sure that it acts only as a wildcard to replace the server part of the IP address, e.g. **www.oclc.org** is replaced by ***.oclc.org.** Do not add an extra element into the IP address.
3. If you have added a Database Identifier (DB ID) for a specific database from a vendor, you must also make an entry for the vendor without a DB ID. The general vendor entry must be below specifc database entries in the table. Add the same DB ID to the HTML link for the database vendor on your Web OPAC.
4. Remove the Database Identifier (DB ID) if you do not need it. This optional value is used only if you want to provide separate access to a specific database, or need usage statistics by database.
5. Make sure that the vendor has the IP address of your Millennium catalog server.
6. If you made changes to entries in the table, also refresh the proxy configuration file by closing and reopening your Web browser.

PRINT THIS PAGE

close window

FAQ

Innovative Interfaces maintains a list of frequently asked questions for Web Access Management. This list is located on CSDirect at: http://csdirect.iii.com/faq/#wam.

This page is updated on a regular basis with the most recent updates shaded. Questions are also being added on a regular basis.

PRINT THIS PAGE

close window

Considerations for Different Servers

Organizations with the "Software Only" package (did not buy a server from Innovative Interfaces) are responsible for their own system configuration for IP ranges. Setup instructions vary depending on the supported operating system. Chose your operating system from the list below to access specific instructions.

- HP Alphas (also known as DEC Alphas or Compaq Alphas)
- HP-UX
- Sun/Solaris
- IBM/AIX

PRINT THIS PAGE
close window

HP Alphas

Log in as superuser and edit the /etc/rc.config file as follows:

1. Set NUM_NETCONFIG="<total number of IP addresses>". For example:
   NUM_NETCONFIG="4"
2. For each alternative IP address that your organization will use for Web Access Management multiple IP routing, there must be a NETDEV_<number>= and an IFCONFIG_<number>= line. For example:

```
NUM_NETCONFIG="4"
NETDEV_0="tu0"
NETDEV_1="tu0"
NETDEV_2="tu0"
NETDEV_3="tu0"
IFCONFIG_0="12.34.56.71 netmask 255.255.255.0"
IFCONFIG_1="12.34.56.72 netmask 255.255.255.0"
IFCONFIG_2="12.34.56.73 netmask 255.255.255.0"
IFCONFIG_3="12.34.56.74 netmask 255.255.255.0"
```

NOTE

- Each IP address must be within the same subset (e.g., 12.34.56.7 in the example above).
- The order of the IFCONFIG_<number> lines is specific, depending on OS version.
  - Alpha 4.0D and 4.0F require that the main system IP be the first IFCONFIG_<number> entry (e.g., IFCONFIG_0=12.34.56.71)
  - Alpha 5.1A requires that the main system IP be the last IFCONFIG_<number> entry (e.g., IFCONFIG_8=12.34.56.71 for 9 entries).
- The entry for the NETDEV_<number>= is the name of the device. For example, the device name might be "tu0".

3. Save and quit.
4. Make the changes active by entering the following command on the command line:
   /usr/sbin/rcinet restart

To test the setup, telnet to each IP address entered in the /etc/rc.config file.

PRINT THIS PAGE
close window

HP - UX

1. Log in as superuser and edit the /etc/rc.config.d/netconf file.

   The file contents will resemble the following:

```
INTERFACE_NAME[0]=<device name>
IP_ADDRESS[0]=<IP address>
SUBNET_MASK[0]=
BROADCAST_ADDRESS[0]=""
LANCONFIG_ARGS[0]="ether"
DHCP_ENABLE[0]=0
```

   For each alternate IP address your organization will use for Web Access Management multiple IP routing, the file must include each of the above lines. For example:

```
INTERFACE_NAME[0]=lan0
INTERFACE_NAME[1]=lan0
INTERFACE_NAME[2]=lan0
IP_ADDRESS[0]=12.34.56.71
IP_ADDRESS[1]=12.34.56.72
IP_ADDRESS[2]=12.34.56.73
SUBNET_MASK[0]=255.255.255.0
SUBNET_MASK[1]=255.255.255.0
SUBNET_MASK[2]=255.255.255.0
BROADCAST_ADDRESS[0]=""
BROADCAST_ADDRESS[1]=""
BROADCAST_ADDRESS[2]=""
LANCONFIG_ARGS[0]="ether"
LANCONFIG_ARGS[1]="ether"
LANCONFIG_ARGS[2]="ether"
DHCP_ENABLE[0]=0
DHCP_ENABLE[1]=0
DHCP_ENABLE[2]=0
```

2. Save and quit the file.
3. Run **ifconfig <device> :1 <IP address>** on the command line. For example: ifconfig hme0:1 12.34.56.71

   To test the setup, telnet to each IP address entered in the /etc/rc.config.d/netconf file.

PRINT THIS PAGE

close window

Sun / Solaris

For organizations using Sun or Solaris, use the following procedure for each IP address that your organization is using with Multiple IP Support for Web Access Management.

1. Log in as superuser and edit the /etc/hostname.<device>:<alias number> file where <device> is the name of the device. Create a file for each system IP address alias.

   Add a hostname alias. For example:

   vi /etc/hostname.hme0:1

   Add:

   alias1

   Save and quit.

2. While logged in as superuser, edit the /etc/hosts file and add an IP address and alias for every IP entry intended for proxy rewrite. For example:

   12.34.56.71 alias1
   12.34.56.72 alias2 ...

   Save and quit.

3. Run **ifconfig <device> plumb** on the command line. For example:

   ifconfig hme0 plumb

4. Run **ifconfig** again to configure each new aliases with the IP addresses. Use this command structure:

   ifconfig <device>:<alias number> <IP address> up. For example:

   ifconfig hme0:1 12.34.56.71 up

To test the setup, telnet to each IP address entered in the /etc/hosts file.

PRINT THIS PAGE
close window

IBM / AIX

For organizations using IBM/AIX, use the following procedure for each IP address that your organization is using with Multiple IP Support for Web Access Management.

1. On the command line, run the following command to set the system alias:

   ifconfig <device> alias <IP address>

   where <device> is the device name and <IP address> is the alternate IP address.
   For example:

   ifconfig en0 alias 12.34.56.71

2. Log in as superuser and edit the /etc/rc.local file to add the alias information.

   Add the following:

   ifconfig <device> alias <IP address>

   where <device> is the device name and <IP address> is the IP address.
   For example:

   ifconfig en0 alias 12.34.56.71

3. Save your changes and quit the /etc/rc.local file.
4. Edit the /etc/inittab and add the line to boot the /etc/rc.local file when the system starts.
   For example:

   rclocal:2:once:/etc/rc.local > /dev/console 2 > 81

   Save and quit.

To test the setup, telnet to each IP address entered in the /etc/rc.local file.

PRINT THIS PAGE
close window