netsweeper

WebAdmin Guide

Manage Filtering with the Netsweeper Policy Server and Client Filter

For Release 2.6.26

EXHIBIT P-22

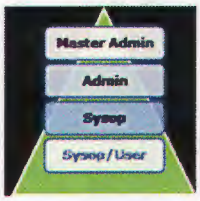
Netsweeper Inc.

104 Dawson Road
Guelph, Ontario N1H 1A7
Canada
Phone: +1 519-826-5222
Fax: +1 519-826-5228

41 Marlowes
Hemel Hempstead, Herts HP1 1LD
United Kingdom
Phone: 01442-355-160

No. 23/35 18th Ave.
Ashok Nagar, Chennai
600 083 India
Phone: 9144-43054005
Fax: 9144-43054006

Netsweeper WebAdmin Guide



About this User Guide

The chart below lists what tasks each user account would probably perform.

Account Holder	Common Tasks
Master Admin	• Manages installation of Netsweeper Policy Server and deployment of the client filters • Monitors and manages the distribution of system resources • Manages the System Tools • Has overall management responsibility for the admins, sysops, and users • Has access to all of the WebAdmin tools.
Admin	• Has no access to the WebAdmin System Tools • Manages one or more groups, with their assigned users and policies • Creates sysop accounts and manages one or more sysops
Sysop	• Has less WebAdmin access than his or her supervising admin • Manages policies, users, and groups only for those groups to which he or she is assigned, under the guidance of an admin. • He or she typically has somewhat limited access to the WebAdmin tools. Sysops can only report on groups and clients assigned to them.
User	• Has very limited WebAdmin access, if at all • May be assigned very limited sysop-like duties, such as the review of reports. Generally, a user can only access his or her own account.

Contacting Technical Support

Netsweeper Inc. is committed to providing exceptional service worldwide. If you require assistance during the installation, configuration, or use of any Netsweeper product, please contact the Netsweeper Technical Support team.

Before you call Technical Support, please have:

- Your Netsweeper product license key
- Physical access to the server hardware used in your content-filtering solution
- Familiarity with your network architecture and server specifications

You can email Support 24 hours a day. Email: support@netsweeper.com. We will respond during regular business hours (8am-5pm Eastern Time), Monday through Friday. You can also telephone Netsweeper Support during regular business hours, Monday through Friday. Telephone the Technical Support Centre nearest your location:

- North America: 1-519-826-5222
- United Kingdom: +44 20 71 93 1044
- India: 9144-43054005

Contents

Introduction to the WebAdmin

The Netsweeper WebAdmin is browser-based software that the Netsweeper *master administrator* (*master admin*), administrators (*admins*) or system operators (*sysops*) use in managing the Netsweeper Internet content-filtering system. The WebAdmin is the dashboard or control centre for your Netsweeper policy server.

This user guide explains how to use the Netsweeper WebAdmin software to create user groups, filtering policies, time segments, logs, and reports for managing your Netsweeper Internet content-filtering solution. It also explains how the master administrator can delegate some tasks to admins and sysops.

Figure 1 WebAdmin, Business Theme

Logging into the WebAdmin

You will access the WebAdmin software a web browsers, such as Internet Explorer, Netscape, Safari, or Firefox.

The address of your Netsweeper policy server has this format:
http://$HOST:8080/webadmin/start/

Instead of **$HOST**, substitute either the host and domain names or the IP address of your Netsweeper policy server.

Your network administrator or a Netsweeper user with *admin* privileges can provide the URL for the Netsweeper policy server, along with your user ID and password. You can save this address as a **Favorite** or **Bookmark** in your browser.

To log in to the WebAdmin software:

1. Use your web browser to navigate to the URL of the WebAdmin/start page for your Netsweeper Policy Server.
2. Type in your username and password.

If you are logging in for the first time, your default username is *admin* and your password is *internet*.

3. After you have logged in, the software will prompt you to change your password. Change it to the password you wrote down in your Installation Checklist.

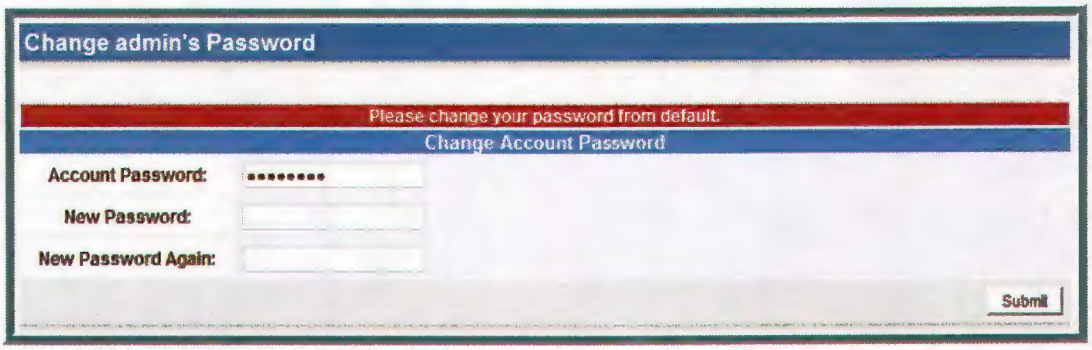


Figure 2 ***Change Admin's Password*** *box displays after first login*

4. Click **Login**.

Overview of the WebAdmin Dashboard

Below are two typical WebAdmin Dashboards. Depending on which Netsweeper product you are using, which theme you have applied, and which user privileges you have, you may not see some of these features or they may display in a somewhat different location.

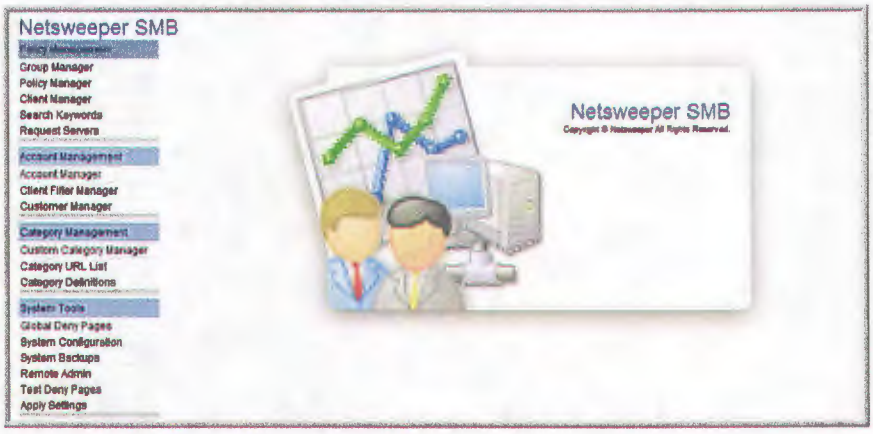


Figure 3 WebAdmin Dashboard, SMB Theme

Figure 4 WebAdmin Dashboard, School Theme

Note *Instructions in this guide assume that you are using one of these user Themes (interfaces): Business, School, and SMB. Some of the other Themes are no longer in common use, and we would recommend that you avoid using them.*

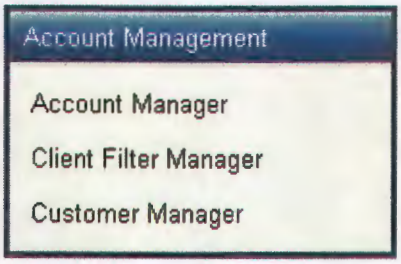
Table 1 Elements of the WebAdmin Dashboard

Dashboard Object	Function
Policy Management Account Management Category Management System Tools Monitoring Reports Logs URL Tools Your Account *Menu bar*	When you click one of these nine tool buttons, the menu options for that tool set will display as a dropdown list. Some of the interface **Themes** display all 44 of the tool buttons at once instead of as part of nine tool sets. Others show the menus in a frame on the left side of the page. You must use the scroll bar to display the menu you want to select. In each of these cases, you will click a tool button to open the page for that tool.
Reports Status WebAdmin Log *Quick Links bar*	*The **Quick Links** bar allows quick access to three areas of the WebAdmin: **Reports**, **Status**, and **WebAdmin Log**. Just click the link to view the appropriate page.*

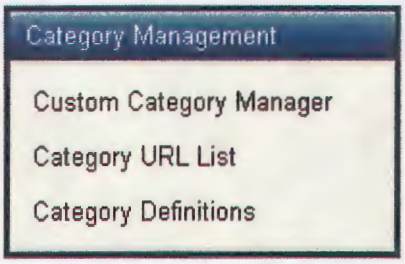
Dashboard Object	Function
admin | Home | Apply Settings | Logout *Task bar*	The WebAdmin task bar, located at the top right corner of the page, has three buttons: **Home**, **Apply Settings**, and **Logout**. • Click **Home** to display the WebAdmin home page. • Click **Apply Settings** to have the WebAdmin apply changes you have made to the various settings. • Click **Logout** to log out of the WebAdmin.
 *Splash screen*	The splash screen is strictly a design element. However, when you click an option on either the Menu Bar or the Quick Links bar, the page for that tool or option displays in this general area.
© 2008 Netsweeper INC. SUPPORT *Link to Netsweeper Technical Support*	*Click SUPPORT at the bottom of each WebAdmin page to go to the Netsweeper Support website.*

Overview of the WebAdmin Tool Menus

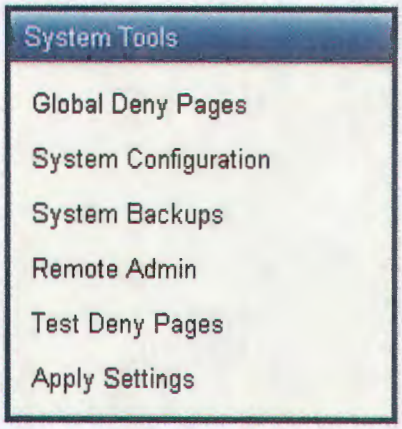
See Managing Policies.



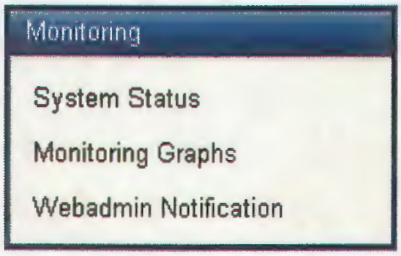
See Managing Accounts.



See Managing Categories.

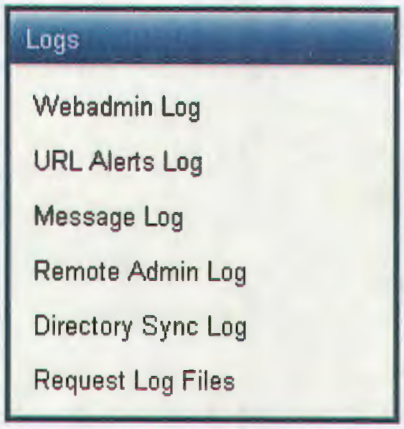


See Using System Tools.

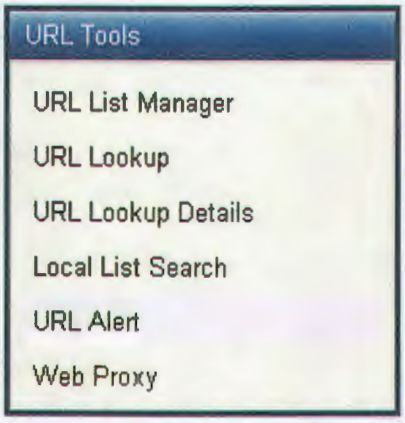


See Using Monitoring Tools.

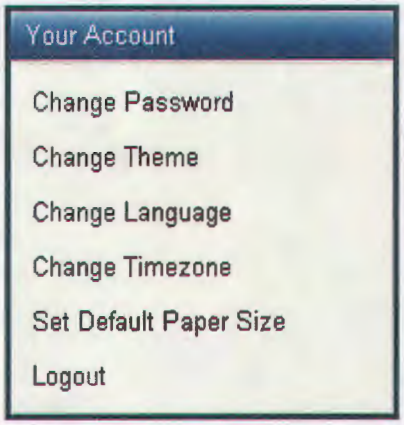
See Using Report Tools.



See Using Logs.



See Using URL Tools.



See Using 'Your Account' Tools

Managing Policies

Rather than creating individual filtering policies for each user, it is more efficient to create groups of users who share the same filtering requirements – *affinity groups* – and then create one or more policies for each group.

Table 2 Possible affinity groups

Parents

Young students

Teenagers

Office workers

Parolees or persons under lawful monitoring

Compulsive gamblers

Teachers

Library patrons

Law enforcement workers

This chapter describes how to create clients (users), groups, policies, and time segments to use in managing your users and their Internet activity.

About Policy Management

Groups, *policies*, *clients* and *time segments* are key concepts used in managing your users and applying filtering policies to them.

About Groups

Grouping clients (Internet users) with similar filtering requirements offers greater efficiency for filtering management. A group can contain any number of users (called *clients*) and must contain at least one active filtering policy.

About Policies

A *policy* defines acceptable or unacceptable Internet content a group of clients.

About Clients

If you are using an external authentication system, you can use the users' Windows ID or account user name as their Netsweeper account name.

If you are not using an external authentication system, you will create a client account for each computer on your network, based on each computer's IP address.

For roaming or off-network devices with a **Netsweeper Client Filter** installed, you will create a client based on the user's Windows Login name. Netsweeper automatically assigns Windows user names without a matching client in the WebAdmin to the *default group*.

Note *Never delete the default group from the WebAdmin. However, you can select a group of your creation to designate as the default group.*

Tip *Assign limited or no Internet access to your default group. This ensures that all new clients are protected from offensive Internet content until you can assign them to the appropriate filtering group. You can only assign a client to one group at a time; however, you can change a client's group assignment later, if needed.*

About Time Segments

A *time segment* is the period of time in which a policy governs the group members' Internet activity. A group may have multiple policies, each with its own time segment. The time segments feature allows you to set more or less restrictive Internet filtering at different times of the day or night for a group of users. Only one policy is active at any time, and the active policy governs all clients in the group for its time segment.

Using the Policy Management Tools

The five Policy Management tools are all accessed from the Policy Management menu in the WebAdmin.

Policy Management	Function
Group Manager	Create and manage user groups
Policy Manager	Create and manage filtering policies on a per-user or per-group basis
Client Manager	Create and manage users
Search Keywords	Allows you to prevent Search Engine results from displaying for searches of specific objectionable keywords or phrases.
Request Servers	Allows you to add remote request servers to those devices that Netsweeper allows to make URL requests through a Netsweeper filtering system. By default the Netsweeper does not allow categorization requests from remote request servers.

Using the Group Manager

Creating a group

You must create your groups before you can assign clients to them or create filtering policies for them.

To create a group:

1. In the WebAdmin, select **Group Manager** from the **Policy Management** menu.
2. Click **Add New Group**.
3. On the **Add New Group** page, type in a name[1] for the group (for example, "library patrons") and a description of the group.

[1] Group names can only contain alphanumeric characters without spaces. If the group names you create do not conform to this standard, Netsweeper will display an error message.

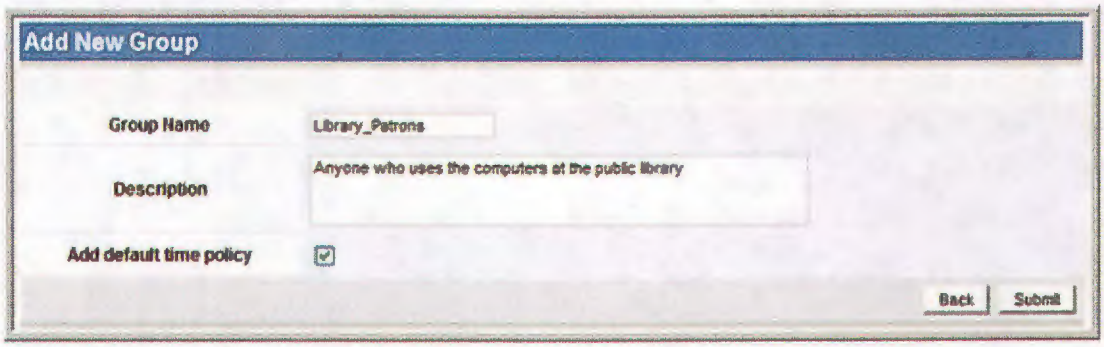


Figure 5 Add New Group page

4. Select the **Add default time policy**[2] box.

5. Click **Submit**.

The **Group Policy** page for this new group now displays.

6. Click **Apply Settings** on the WebAdmin task bar in the top right corner of the page and then click **Apply**.

[2] You can later change the assigned time policy from the default.

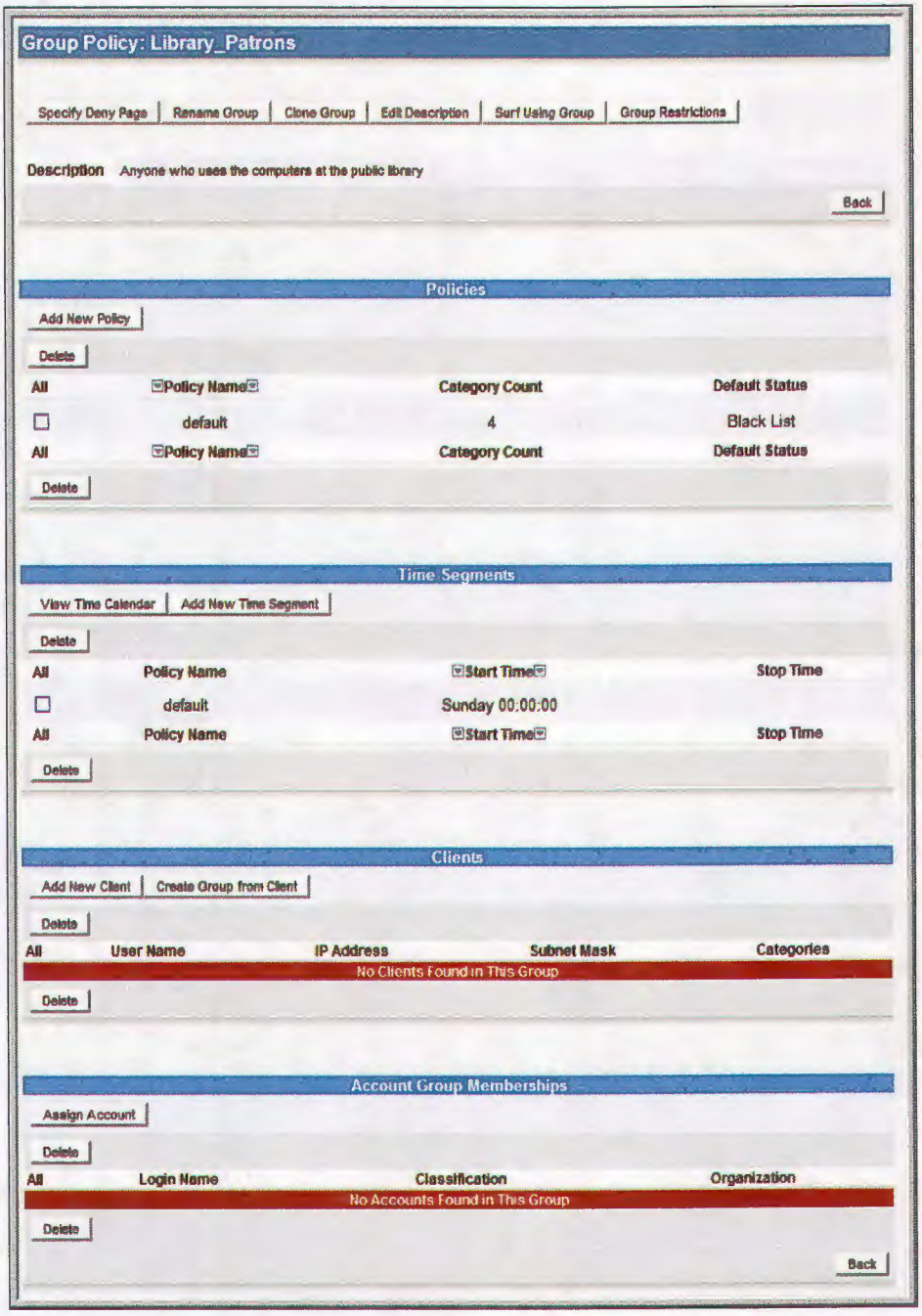


Figure 6 Group Policy page

You can also choose the group you want to serve as the default group[3], the group that Netsweeper will use for filtering any user not assigned to a group.

After you create a group, you can clone the group, including all policies, by clicking **Clone Group** from the **Group** menu. Since clients can only belong to one group, Netsweeper does not copy clients to a cloned group.

7. If you make a mistake in creating a group, delete the group.

Deleting a Group

To delete a group, select the check box for the group from the **Group Manager** and then click **Delete**. You can also rename the group or edit its description.

Surfing Using Group

For information on the **Surf Using Group** feature, see the **Web Proxy Tech Note** on the support site, at http://support.netsweeper.com.

You can restrict the group to a range of IP addresses. Select **Group Restrictions** from the **Group** menu and type in the range of IP addresses to which you would like this group to apply.

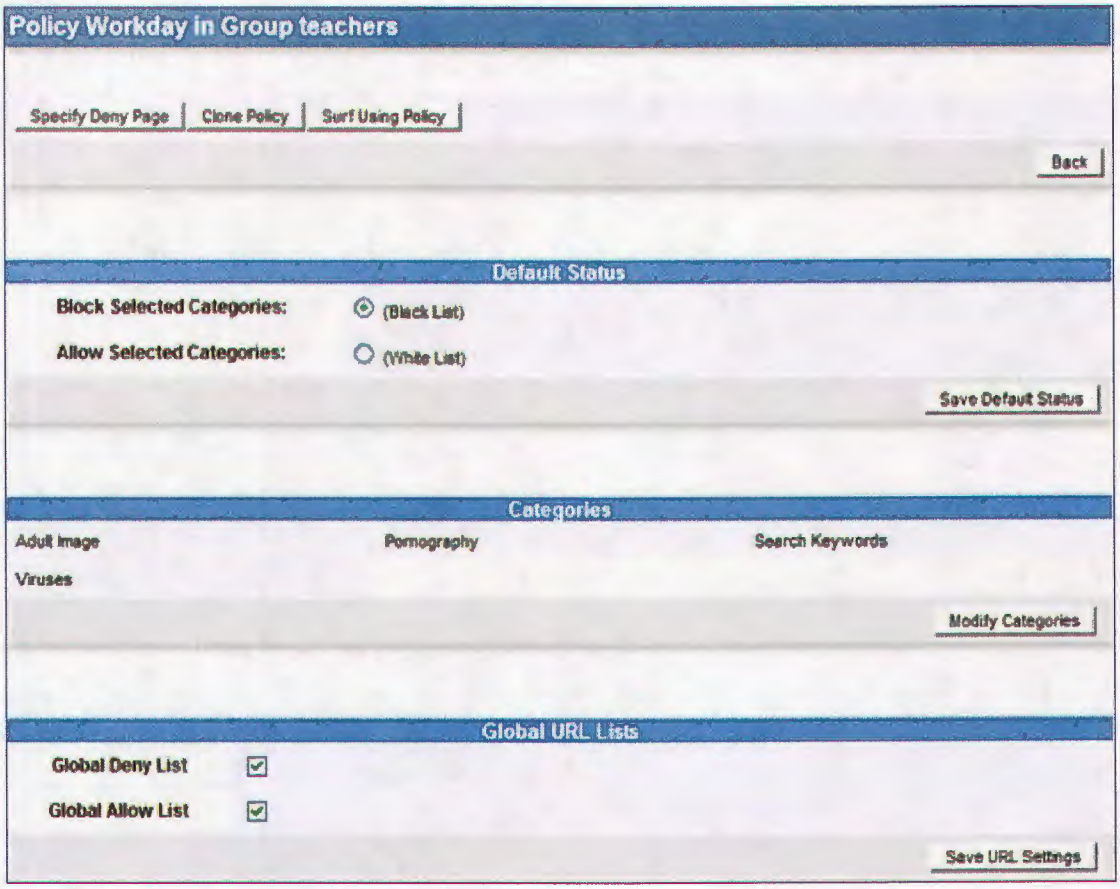


Figure 7 Policy page

[3] It is important that you NEVER delete the default group.

Assigning Policies to a Group

A *policy* defines the filtering rules for every client (user) assigned to a specific group.

To create a policy and assign it to a group:

1. Select **Group Manager** from the **Policy Management** menu.
2. Select the group name.
3. In the **Policies** section, click **Add New Policy**.
4. Type in a policy name and then click **Submit**.
5. Click **Modify Categories**.
6. Select the box by each category to which you want to block this group's access.
7. Click **Submit**.
8. Click **Apply Settings** on the WebAdmin task bar in the top right corner of the page and then click **Apply**.

Assigning Time Segments to a Policy

Time segments are blocks of time in a week. You can create multiple policies for one group, each with different degrees of Internet access, and assign them to become active at different time segments during the week.

When you add a policy, you must apply time segments to it or the default time segments will apply.

A color-coded *time calendar* in the WebAdmin displays a week with all the time segments with their policy assignments. See

To assign time segments to a policy:

1. Select **Group Manager** from the **Policy Management** menu.
2. Select the group name.
3. Click **Add New Time Segment** in the **Time Segments** section.
4. Select the day and the time that you want this time segment[4] to start. You can also choose when you want the time segment to end, but this is not required.
5. Click **Submit**.
6. Click **Apply Settings** on the WebAdmin task bar in the top right corner of the page and then click **Apply**.

---

[4] Create multiple time segments at once by selecting more than one day for the time segment. For example, if you want the policy to start at 6 p.m. every day, select all seven days and type *18:00:00* as the time.

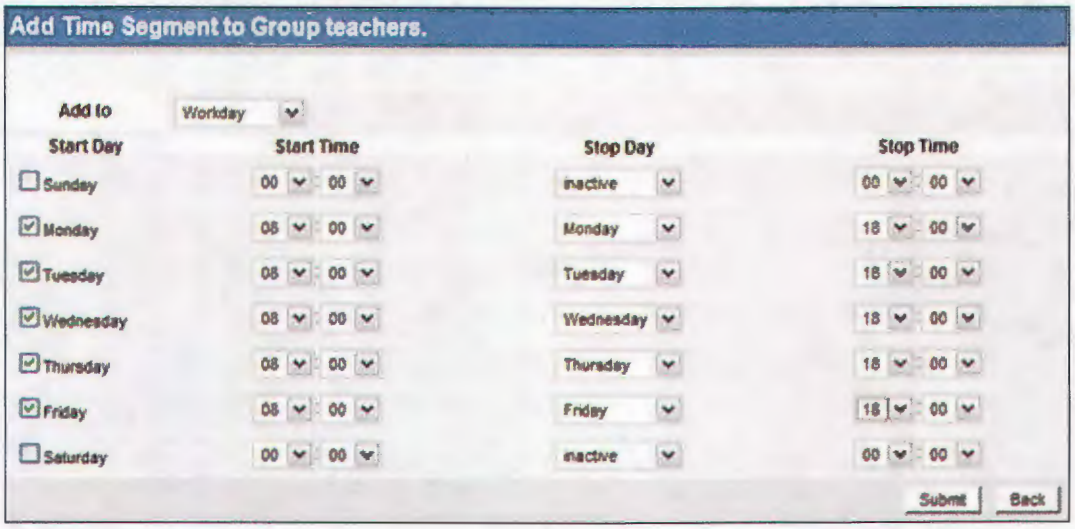


Figure 8 Add time segments

Changing a Time Segment

To change the start time(s) or end time(s) for a policy:

1. Select **Group Manager** from the **Policy Management** menu.
2. Select the name of the group you want to modify.
3. Find the existing time segment in the **Time Segments** section and select the policy name.
4. Set the new start time or end time and then click **Submit**.
5. Select **Apply Settings** on the WebAdmin task bar in the top right corner of the page and then click **Apply**.

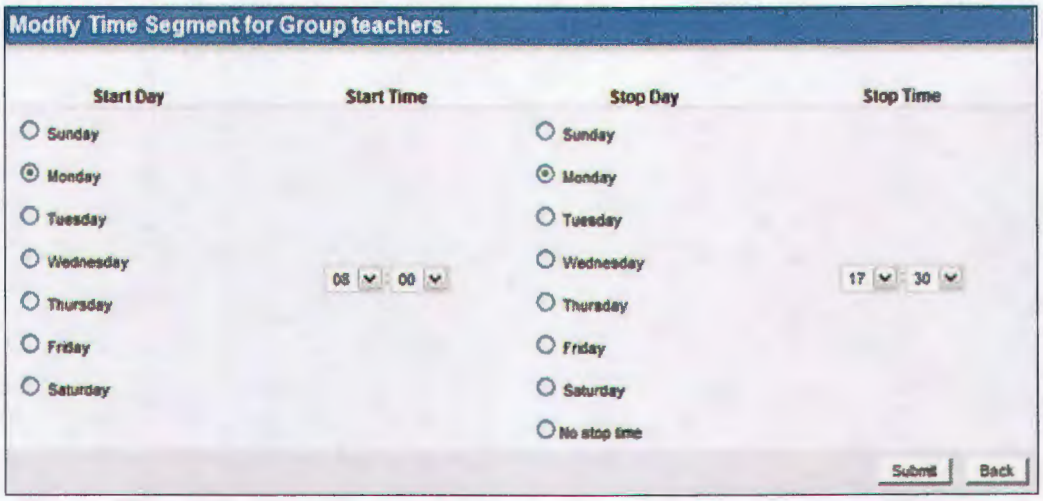


Figure 9 Modify Time Segment page

Viewing a Time Calendar

The Time Calendar is a visual representation of when your policies are active. It is an excellent tool to verify that you have set up the Time Segments to your liking.

To view a group's time calendar:

1. Select **Group Manager** in the **Policy Management** menu.
2. Select the name of the group you want to modify.
3. Click **View Time Calendar**.

Sample Calendar for a Group with One Time Segment

If you want to use one policy at all times, you only need to create one policy. By default, new policies start at midnight on Sunday and remain active all the time.

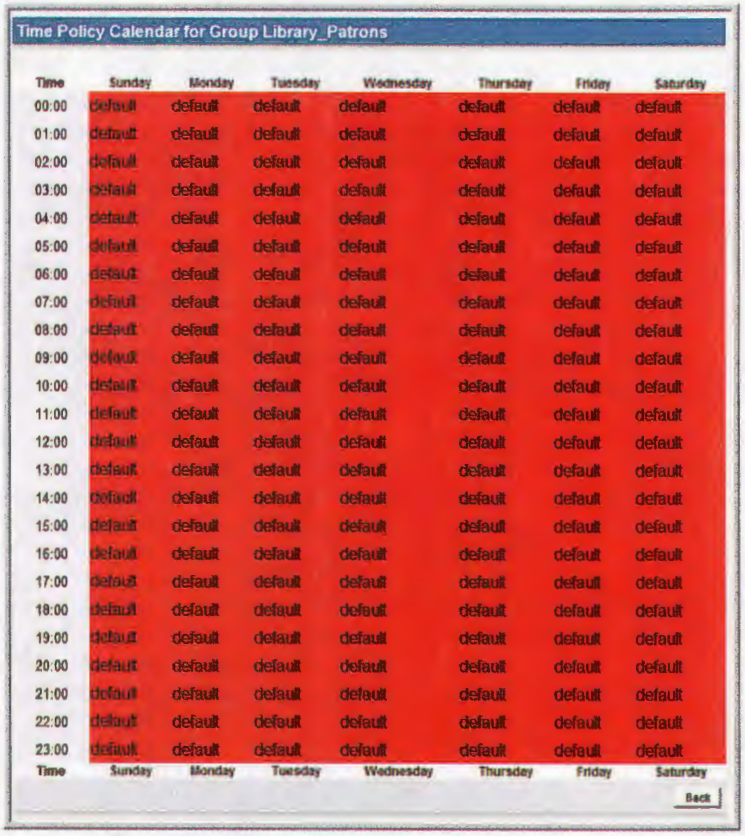


Figure 10 The calendar for a group with only one policy (the default)

Sample Calendar for a Group with Two Time Segments

If you want to run one policy during the week and another on weekends, you can set the Weekdays policy to start Monday at 0:00:00 and set the Weekends policy to start Saturday at 0:00:00. The following screen capture is the Time Calendar for this example:

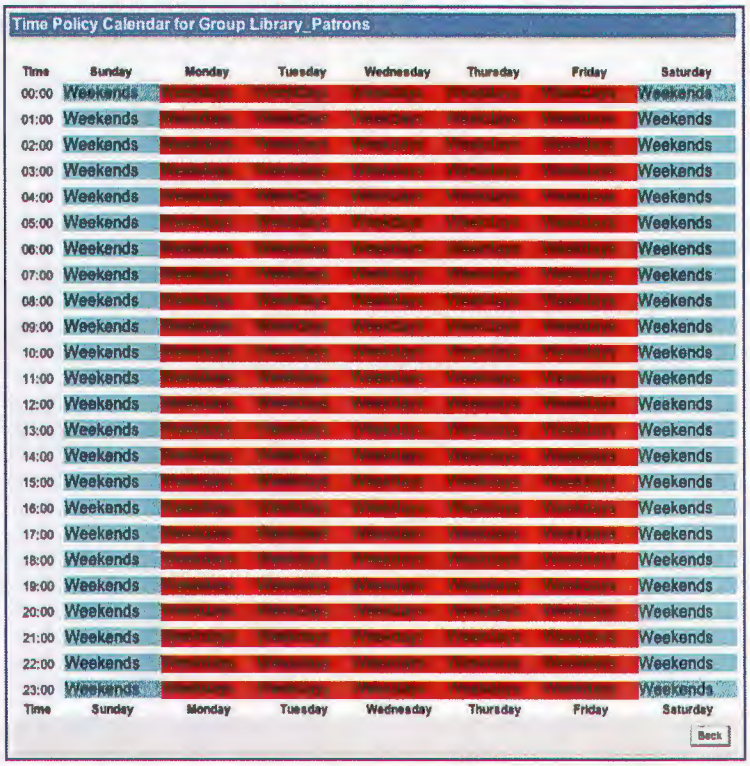


Figure 11 Time calendar for a group with two policies

Sample Calendar for a Group with Three Policies

If you want to create a group with policies for limited access during business hours, moderate access during lunch, and unrestricted access after business hours, you can set up something like the following:

- Limited access on Monday through Friday from 8:00 to 17:00.
- Moderate access on Monday through Friday at 12:00 to 13:00.
- Unrestricted access beginning the first day of the week (0:00 on Sunday).

This arrangement of three policies and their time segments would look like this:

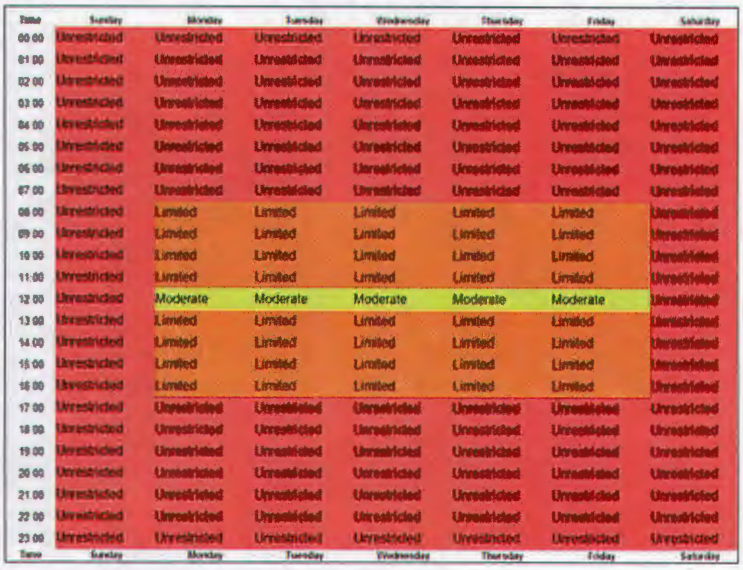


Figure 12 Time Calendar for three policies

Changing the Filtering for a Policy

To change the categories or protocols filtering for a policy:

1. Select **Group Manager** from the **Policy Management** menu.
2. Select the name of the group you want to modify.
3. Select the name of the policy you want to modify.
4. Go to step 3 below.

OR

1. Select **Policy Manager** from the **Policy Management** menu.
2. Find the policy you want to modify and then click the policy name.
3. Find the **Default Status** to confirm the policy uses *black list* filtering. This is the recommended mode.

   If the policy uses *white list* filtering, confirm with the *master admin* that white list is the intended mode.
4. Click **Modify Categories** in the **Categories** section.
5. Select the option of which policies you want to change.
6. If you are using black list filtering, select all categories and protocols to which you want to block access. If you are using white list filtering, select all categories and protocols to which you want to allow access.
7. Click **Submit**.
8. Click **Apply Settings** on the WebAdmin task bar in the top right corner of the page and then click Apply.
9. Now you have a choice:
   - If you click **Specify Deny Page** in the **Policy Manager**, you are given the choice whether to use the **Global Deny Page**, the **Group Deny Page**, a **Custom Deny Page** or to log only.
   - If you click **Custom Deny Page**, you can modify the **Deny Pages** for each group separately. You are also given the choice of what you want to log for the policy.

Cloning a Policy[5]

To clone a policy:

1. On the WebAdmin menu bar, click **Policy Management** and then select **Policy Manager** from the Policy Management dropdown menu.
2. Click the name of the policy you want to clone in the **Policy Name** column.

   This displays the page for that policy. At the top of the page, click **Clone Policy**.

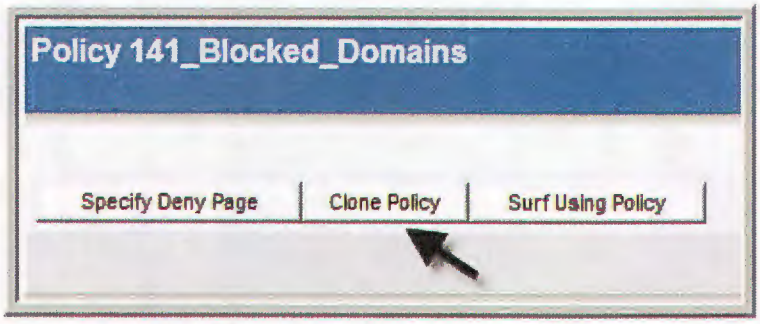
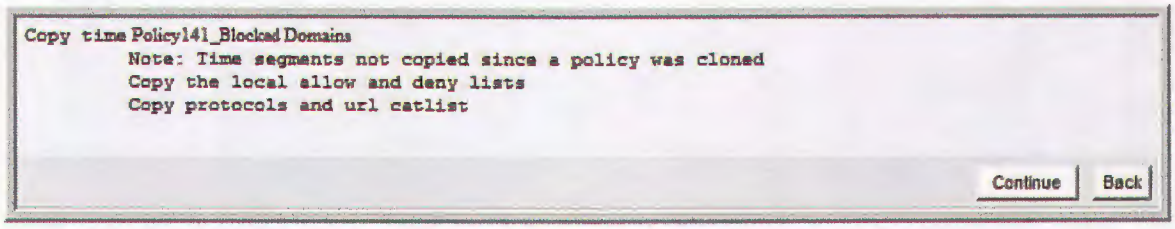


Figure 13 Clone Policy button at top of Policy page for Policy 141_Blocked_Domains

3. The cloned policy page displays. In the **Policy Name** box, type a name for the cloned policy and then click **Submit**.

4. A notice will describe what exactly has been copied from the old policy. Time segments are not cloned, but the deny page, local allow and deny lists, and the Protocol and URL category list are all copied into the new policy. Click **Continue**.



5. The detail page for the cloned policy now displays. You can modify the policy, changing the Deny Page, Default Status, Categories, Global URL Lists, Local URL/Keyword List, and so on.

[5] Time segments assigned to a policy will not clone with the cloning of the policy.

Deleting a Policy[6]

To delete a policy. select the checkbox beside the policy name in the **Policy Manager** and then click **Delete**.

For more information on the **Surf Using Policy** feature, see the **Web Proxy Technical Note** on the support site, at http://support.netsweeper.com.

You could also change the status to *white list* (**Allow selected categories**) or *black list* (**Deny selected categories**) of the categories chosen.

If you clear the check box by **Global Deny and Allow Lists**, then the lists will not apply to this policy.

Adding Clients by User Name

For each **Netsweeper Client Filter** user, create a client within a group. This client should be based on the Windows user name. You must first log into the WebAdmin before you can create a client.

To create a client within a group:

1. Select **Group Manager** from the **Policy Management** menu.
2. Select the group[7] to which you want to add this client.
3. In the **Clients** section, click **Add New Client**.
4. If you want this to be a temporary client, type in an expiry date.
5. Click **Authorized By Client Name**.
6. Type the user's Windows login name in lowercase as the **Client Name**.
7. Select any categories you want to block for this client only.
8. Click **Submit**.
9. Click **Apply Settings** on the WebAdmin task bar in the top right corner of the page and then click **Apply**.

Adding Clients by Password

This option is for use with the Enterprise Filter, more specifically with Squid.

To add a client to a group by password:

1. Select **Group Manager** from the **Policy Management** menu.

---

[6] Do not delete the default policy, as this may cause filtering errors. You can, however, change the policy that is designated as the default policy.

[7] If there are a number of groups, use the **Search** box or advance through the pages by clicking the page number. You can also sort a page alphabetically by group clicking the first letter in the **Group** name below the **Search** box.

2. Select the group[8] to which you want to add this client.
3. In the **Clients** section, click **Add New Client**.
4. If you want this to be a temporary client, type in an expiry date.
5. Click **Authorized By Password**.
6. Type in the user's exact Windows login name as the **Client Name** and type in a password for the user.
7. Select any categories you want to block *only* for this client.
8. Click **Submit**.
9. Click **Apply Settings** on the WebAdmin task bar in the top right corner of the page and then click **Apply**.

Adding Clients by IP address

If you are using the Enterprise Filter and not using any external authentication methods, such as Radius or Active Directory, you can assign clients based on the IP address of their computer.

To add clients to a group by their computer IP address:

1. In the WebAdmin, create a client account for each user based on the user's Windows user ID.
2. Select **Group Manager** from the **Policy Management** menu.
3. Select the group to which you want to add this client.

   Use the **Search** box or advance through the pages by clicking the page number. Pages can also be sorted alphabetically by clicking the first letter in the group name below the **Search** box.
4. In the Clients section, click **Add New Client**.
5. If you want this to be a temporary client, type in an expiry date.
6. Click **Computer Address**.
7. Type in the user's exact Windows login name as the Client Name and the computer's IP Address.
8. Select any categories you want to block for this client only.
9. Click **Submit**.
10. Click **Apply Settings** on the WebAdmin task bar in the top right corner of the page and then click **Apply**.

---

[8] Use the **Search** field or advance through the pages by clicking the page number. You can sort pages alphabetically by **Group** name by clicking the first letter in the Group name below the **Search** box.

Adding Clients by Network Subnet

This option is for use with the Enterprise Filter. If you have many users in a range of IP addresses that you would like to filter in the same group, you can add them all at once using a network subnet.

To add clients to a group by their network subnet:

1. In the WebAdmin, select **Group Manager** from the **Policy Management** menu.
2. Find the group that you want to add this client to and then click it. If you don't have a lot of groups created yet, you should be able to scroll down to find the group. If you do have many groups created, you may need to use the Search box or advance through the pages by clicking the page number. Pages can also be sorted alphabetically by clicking the first letter in the group name below the Search box.
3. In the **Clients** section, click **Add New Client**.
4. If you want this to be a temporary client, type in an expiry date.
5. Click **Network Subnet**.
6. Type in the user's exact Windows login name as the **Client Name**, the user's **IP Address**, and the **Subnet Mask**.
7. Select any categories you only want to block for this client.
8. Click **Submit**.
9. Click **Apply Settings** on the WebAdmin task bar in the top right corner of the page and then click **Apply**.

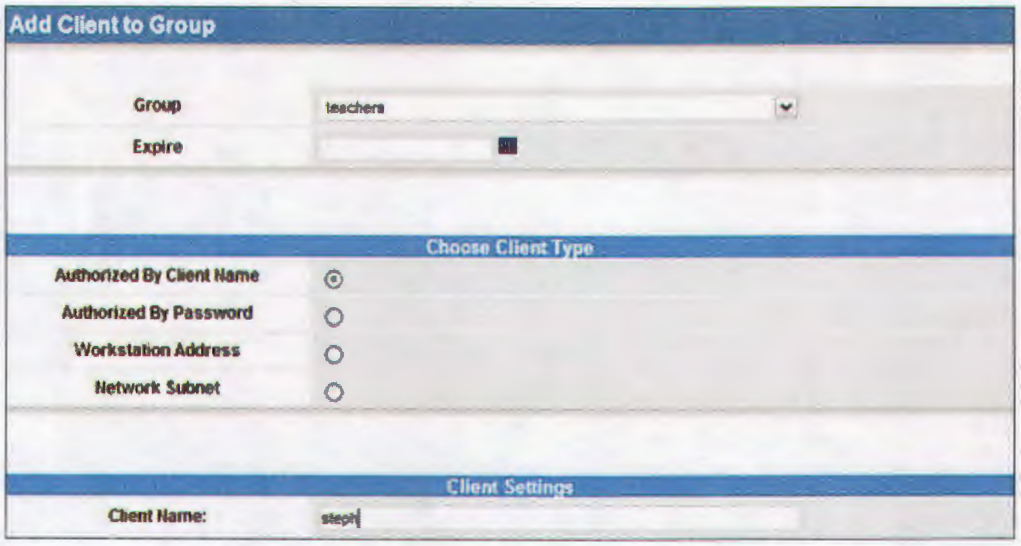


Figure *14*: Add client to the group Teachers

Adding Multiple Clients

In many businesses, it is important to be able to identify specific users in reports, such as employees, managers, administrators, or visitors.

If you use an authentication service, such as Microsoft Active Directory, you can assign users to groups and then replicate those group names on the Netsweeper Policy Server. Netsweeper supports Microsoft Active Directory, LDAP, Novell, and Radius authentication methods and has a robust API to integrate with other authentication systems.

For more information on synchronizing from Active Directory, go to the Netsweeper support site at http://support.netsweeper.com.

Modifying a Policy's Category and Protocol Filtering

To change the categories or protocols blocked for a particular policy:

1. Select **Policy Manager** from the **Policy Management** menu.
2. Find the policy you want to modify and then click the policy name.
3. Find the **Default Status** to confirm the policy uses black list filtering (the recommended mode for filtering). If the policy instead uses white list filtering, confirm with the *master admin* that white list is the intended mode.
4. Click **Modify Categories** in the **Categories** section.
5. Select the option of which policies you want to change.
6. If you are using *black list* filtering, select all categories and protocols to which you want to *block* access. If you are using *white list* filtering, select all categories and protocols to which you want to *allow* access.
7. Click **Submit**.
8. Click **Apply Settings** on the WebAdmin task bar in the top right corner of the page and then click **Apply**.
9. If you click **Specify Deny Page** in the **Policy Manager**, you are given the choice whether to use the **Global Deny Page**, the **Group Deny Page**, a **Custom Deny Page** or to log only.
10. If you click **Custom Deny Page**, you can modify the **Deny Pages** for each group separately. You are also given the choice of what you want to log for the policy.

Deleting a Client

To delete a client from a group:

1. Select **Client Manager** from the **Policy Management** menu.
2. Select the checkbox beside the client name you want to delete.
3. Click **Delete**.

To move a client to another group:

1. Select Client Manager from the Policy Management menu.
2. Select the client name.
3. Choose the new group from the Group menu and then click Submit.
4. Click Apply Settings on the WebAdmin task bar in the top right corner of the page and then click Apply.

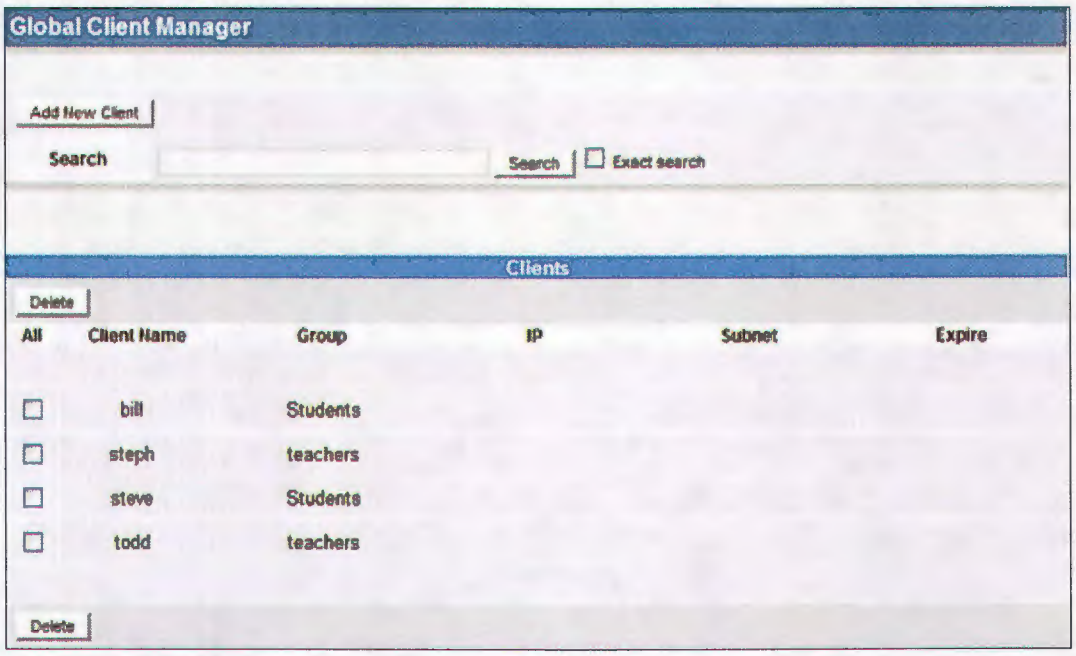


Figure 15 Client Manager

Adding Clients to Groups

There are four methods for adding clients to groups – by user name, password, IP address, or network subnet. The instructions for adding a client by user name are below. See the *Netsweeper WebAdmin Guide* for details on the other methods.

You can also add multiple clients. See Adding Multiple Clients in the *Netsweeper WebAdmin Guide*.

Adding Clients by User Name

For each Netsweeper Client Filter user, create a client within a group. This client should be based on a user's Windows user name.

To add a client by Windows user name:

1. Using your browser, log on to the *WebAdmin*.
2. Select **Group Manager** from the **Policy Management** menu.
3. Select the group to which you want to add this client.

   If there are a number of groups, use the **Search** box or advance through the pages by clicking the page number. You can also sort a page alphabetically by group clicking the first letter in the **Group** name below the **Search** box.
4. In the **Clients** section, click **Add New Client**.
5. If you want this to be a temporary client, type in an expiry date.
6. Click **Authorized By Client Name**.
7. Type the user's Windows login name in lowercase as the **Client Name**.
8. Select any categories you want to block for this client only.
9. Click **Submit**.
10. Click **Apply Settings** on the WebAdmin task bar in the top right corner of the page and then click **Apply**.

Adding Clients by Password

This option is for use with the Enterprise Filter, more specifically with Squid. You must first log into the WebAdmin to create a client.

To add a client to a group by password:

1. Select **Group Manager** from the **Policy Management** menu.
2. Select the group to which you want to add this client.

   If there are a number of groups, use the **Search** box or advance through the pages by clicking the page number. You can also sort a page alphabetically by group clicking the first letter in the **Group** name below the **Search** box.
3. In the Clients section, click **Add New Client**.
4. If you want this to be a temporary client, type in an expiry date.
5. Click **Authorized By Password**.

6. Type in the user's exact Windows login name as the Client Name and type in a password for the user.
7. Select any categories you want to block only for this client.
8. Click Submit.
9. Click Apply Settings on the WebAdmin task bar in the top right corner of the page and then click Apply.

Adding Clients by IP Address

If you are using the Enterprise Filter and not using any external authentication methods, such as Radius or Active Directory, you can assign clients based on the IP address of their computer.

To add clients to a group by their computer IP address:

1. Log into the Netsweeper WebAdmin.
2. Create a client account for each user based on the user's Windows user ID.
3. Select **Group Manager** from the **Policy Management** menu.
4. Select the group to which you want to add this client.

   Use the **Search** box or advance through the pages by clicking the page number. Pages can also be sorted alphabetically by clicking the first letter in the group name below the **Search** box.
5. In the Clients section, click **Add New Client**.
6. If you want this to be a temporary client, type in an expiry date.
7. Click **Computer Address**.
8. Type in the user's exact Windows login name as the Client Name and the computer's IP Address.
9. Select any categories you want to block for this client only.
10. Click **Submit**.
11. Click **Apply Settings** on the WebAdmin task bar in the top right corner of the page and then click **Apply**.

Adding Clients by Network Subnet

This option is for use with the Enterprise Filter. If you have many users in a range of IP addresses that you would like to filter in the same group, you can add them all at once using a network subnet.

To add clients to a group by their network subnet:

1. In the WebAdmin, select **Group Manager** from the **Policy Management** menu.
2. Find the group that you want to add this client to and then click it.

   If you don't have a lot of groups created yet, you should be able to scroll down to find the group. If you do have many groups created, you may need to use the Search box or advance through the pages by clicking the page number. Pages can also be sorted alphabetically by clicking the first letter in the group name below the Search box.
3. In the **Clients** section, click **Add New Client**.
4. If you want this to be a temporary client, type in an expiry date.
5. Click **Network Subnet**.
6. Type in the user's exact Windows login name as the **Client Name**, the user's **IP Address**, and the **Subnet Mask**.
7. Select any categories you only want to block for this client.
8. Click **Submit**.
9. Click **Apply Settings** on the WebAdmin task bar in the top right corner of the page and then click **Apply**.

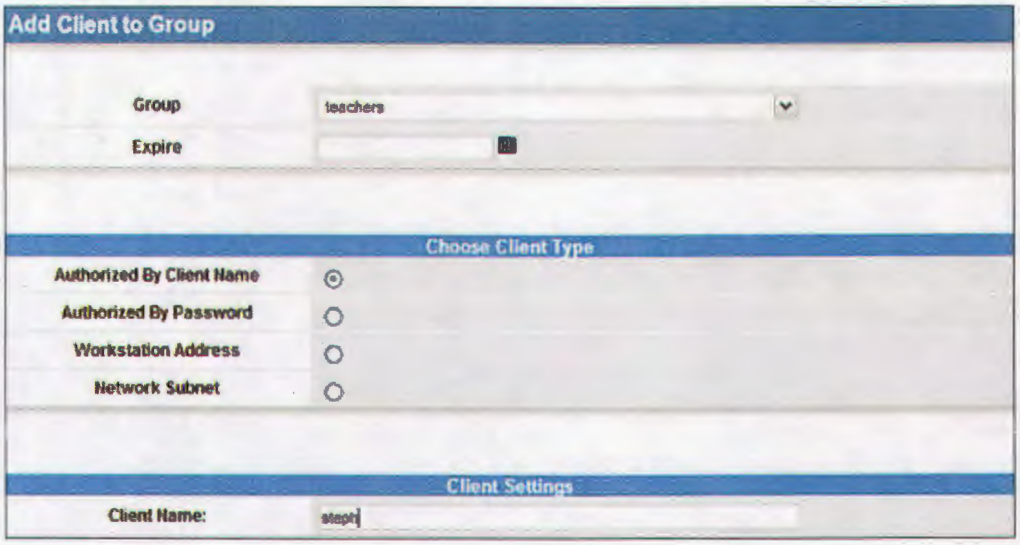


Figure *16*: Add client to the group Teachers

Adding Multiple Clients

In many businesses, it is important to be able to identify specific users in reports, such as employees, managers, administrators, or visitors.

If you use an authentication service, such as Microsoft Active Directory, you can assign users to groups and then replicate those group names on the Netsweeper Policy Server. Netsweeper supports Microsoft Active Directory, LDAP, Novell, and Radius authentication methods and has a robust API to integrate with other authentication systems.

For more information on synchronizing from Active Directory, go to the Netsweeper support site at http://support.netsweeper.com.

Modifying a Client

To delete a client from a group:

1. Click **Policy Management** on the WebAdmin's menu bar.
2. Select **Client Manager** from the **Policy Management** menu.
3. Select the checkbox beside the client name you want to delete.
4. Click **Delete**.

Moving a Client to Another Group

To move a client to another group:

1. In the WebAdmin, select **Client Manager** from the **Policy Management** menu.
2. Select the client name.
3. Choose the new group from the **Group** menu and then click **Submit**.
4. Click **Apply Settings** on the WebAdmin task bar in the top right corner of the page and then click **Apply**.

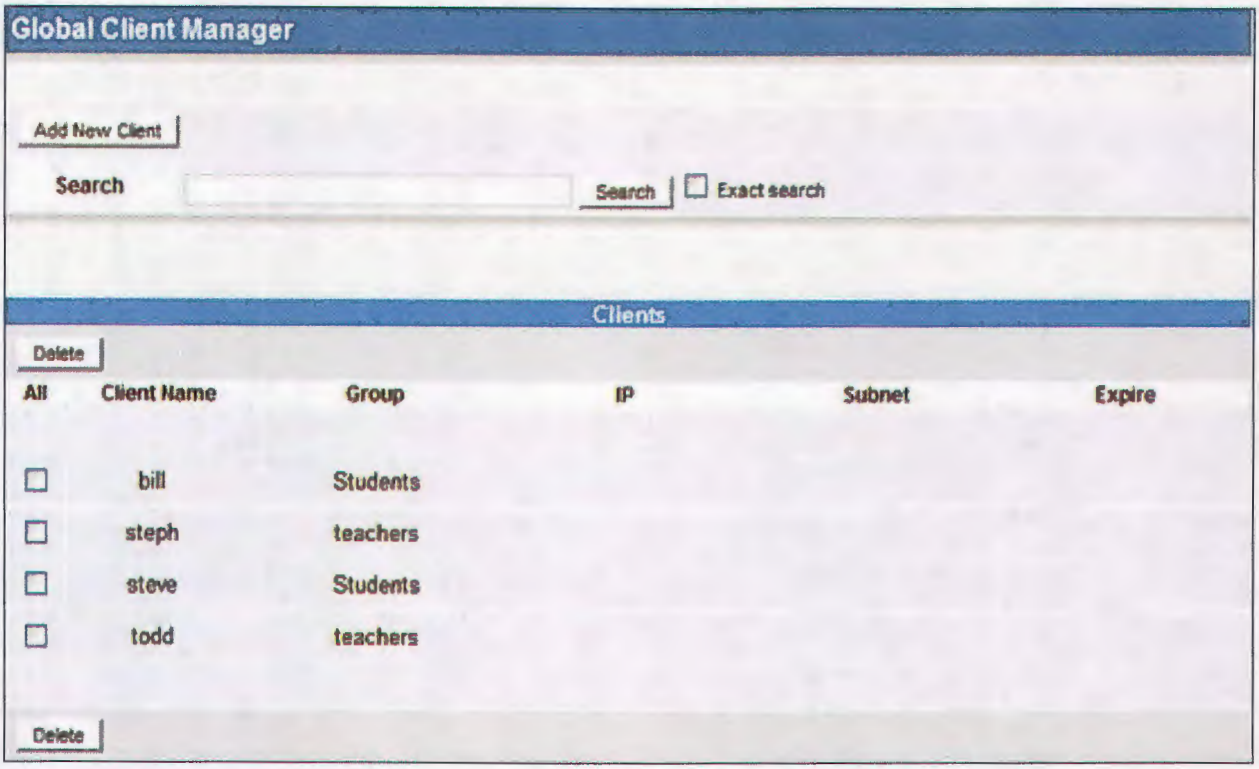


Figure *17*: Global Client Manager

Using Search Keywords[9]

Search Keywords is an application listed on the **Policy Management** menu.

To open the **Search Keywords** page, click **Policy Management** on the WebAdmin menu bar and then click **Search Keywords** from the resulting dropdown menu.

The **Search Keywords** tool allows you to create a list of objectionable words or phrases on which you want to prevent users from performing Internet searches.
If a user visits a Search Engine and searches for one of these words, the page will be denied.

This only works for URLs that have been categorized as a search engine site. The filter will block sites like http://www.google.com or http://www.altavista.com if a URL contains any of the search keywords.

Use the Category URL List to assign a Search Engine site to a URL, if you want the search keywords to apply. For example: http://com as a search engine site would enforce search keywords on all http://*.com/* websites.

[9] You can turn this feature off in a policy.

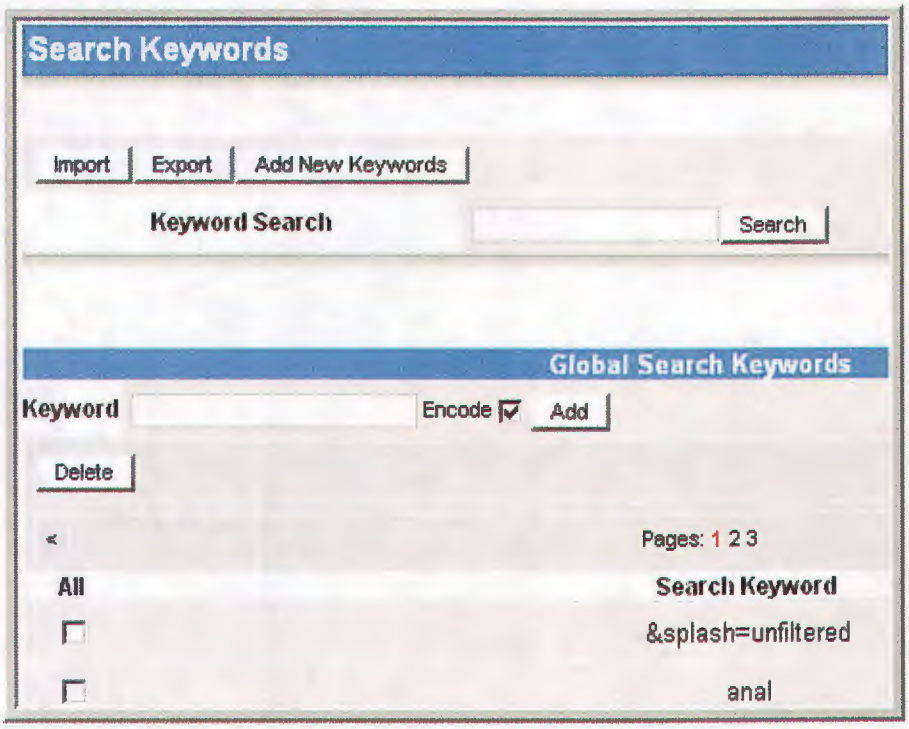


Figure 18: Search Keywords tool, page 1 (partial) of 3

The **Add New Keyword** function will add a new search keyword, which will be blocked in Search Engine Site URLs. You can create two different types of keywords: *regular* and *encoded*.

If you copied the keyword a browser URL address bar, it is encoded. Encoding the keyword replaces any non-alphanumeric characters, except the hyphen (-), underline (_), and period (.), with a percent (%) sign followed by the character's 2-digit hex equivalent. Spaces are replaced by plus (+) signs. You cannot add a word already in the list.

You can also importing a list from a comma- or tab-delimited text file. Export the current list by clicking **Export**.

Using the 'Request Servers' Tool

Request servers are those devices that Netsweeper allows to make URL requests through a Netsweeper filtering system.

By default, Netsweeper does not allow categorization requests from remote request servers.

If you want to allow access to remote request servers, you must use the **Request Servers** tool to notify the Policy Server of their existence. This is the same as the **request_server** entries in the file *nsd.conf*. You will add both the **Site Name** and **IP Address or IP Range** information to register a **Request Server** with the Netsweeper Policy Server. Optionally, you can indicate a range of IP addresses by typing *CIDR /XX* at the end of an IP Address.

Allowing any IP Address as a Request Server

To allow any IP address to serve as a request server, add the address **0.0.0.0**.

Note *When possible, type in a more restrictive mask than "0.0.0.0" to increase the security of the policy server.*

To add a Request Server:

1. Select **Request Servers** from the **Policy Management** menu.
2. Click **Add New Request Server**.
3. Type in a descriptive site name to identify the IP or IP range you are adding, such as **Netsweeper Client Filter Users**.
4. Type *0.0.0.0* as the IP address.
5. Select the **Active** check box. Clear all of the check boxes below this box.
6. Click **Add New**.
7. Click **Apply Settings** from the WebAdmin task bar in the top right corner of the page and then click **Apply**.

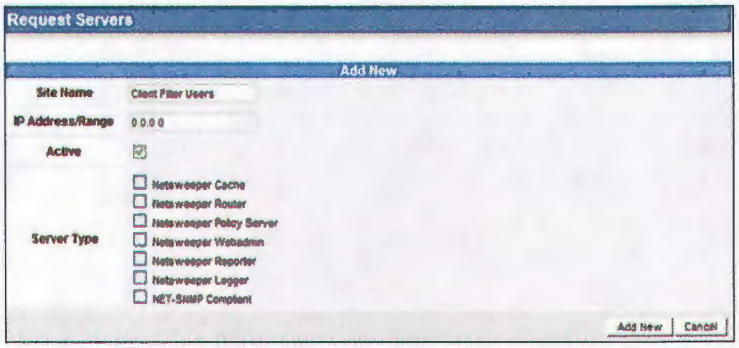
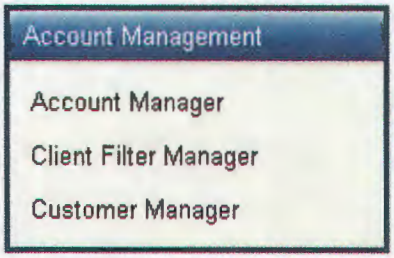


Figure *19*: Add a new Request Server

Managing Accounts

The **Account Management** tools allow you to create *sysop* and *admin* users and assign them groups to delegate administration tasks. They also allow you to manage the **Netsweeper Client Filter** accounts.



Account Management menu

Account Management[10]	Function
Account Manager	Manage client accounts (including resetting passwords), create *admin* and *sysop* accounts and delegate administration tasks,
Client Filter Manager	Manage client filters
Customer Manager	Manage customers

When you create an account, you have the option to give an expiry date. You can also suspend an account.

Using the Account Manager

Adding a new account

To add a new account:

1. Click **Account Management** on the WebAdmin menu bar.
2. Select **Account Manager** from the drop-down list.
3. Click **Add New Account**.

   The **Add New Account** page displays.

[10] For more information on delegating administrative tasks to system operators (*sysops*), see the **Sysop Permissions Guide** at http://support.netsweeper.com.

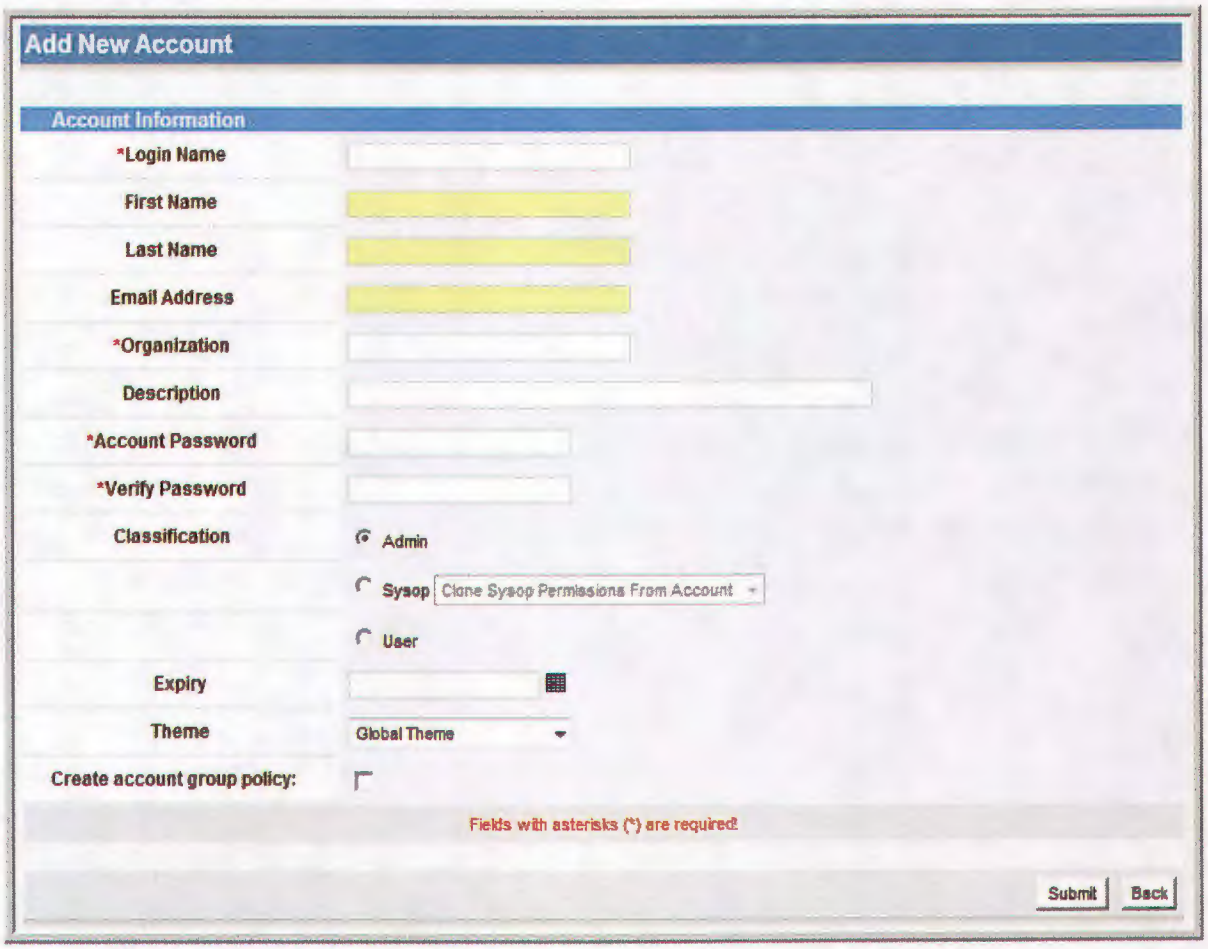


Figure 20 Add New Account page

4. Complete the **Account Information** on the **Add New Account** page, making sure that you complete the **Login Name**, **Organization**, **Account Password**, and **Verify Password** boxes.
5. Select a classification for the user: **Admin**, **Sysop**, or **User**.
6. If the new account is for a sysop, you can clone the sysop permissions from another account, if another sysop account has been created. Click the down arrow in the box to the right of Sysop and select an option from the resulting list.
7. Set an expiry date for the account by clicking the calendar tool and selecting a date.
8. Select a theme (interface) for the account by clicking the down arrow in the box to the right of Theme and selecting an option from the resulting list.
9. If this account will have its own group policy and not use one you have previously created, select the box by **Create Account Group Policy**.
10. Click **Submit**.

    A message will display at the top of the page advising you that the account has been added.
11. Click **Apply Settings** on the taskbar to load the new account into all of the policy servers.
12. Click **Apply**.

Resetting a Password

To reset an account password:

1. Click **Account Management** on the WebAdmin menu bar.
2. Select **Account Manager** from the drop-down list.
3. Find the account name in the **Accounts** list and click the **Edit** button beside it (in the **Actions** column).

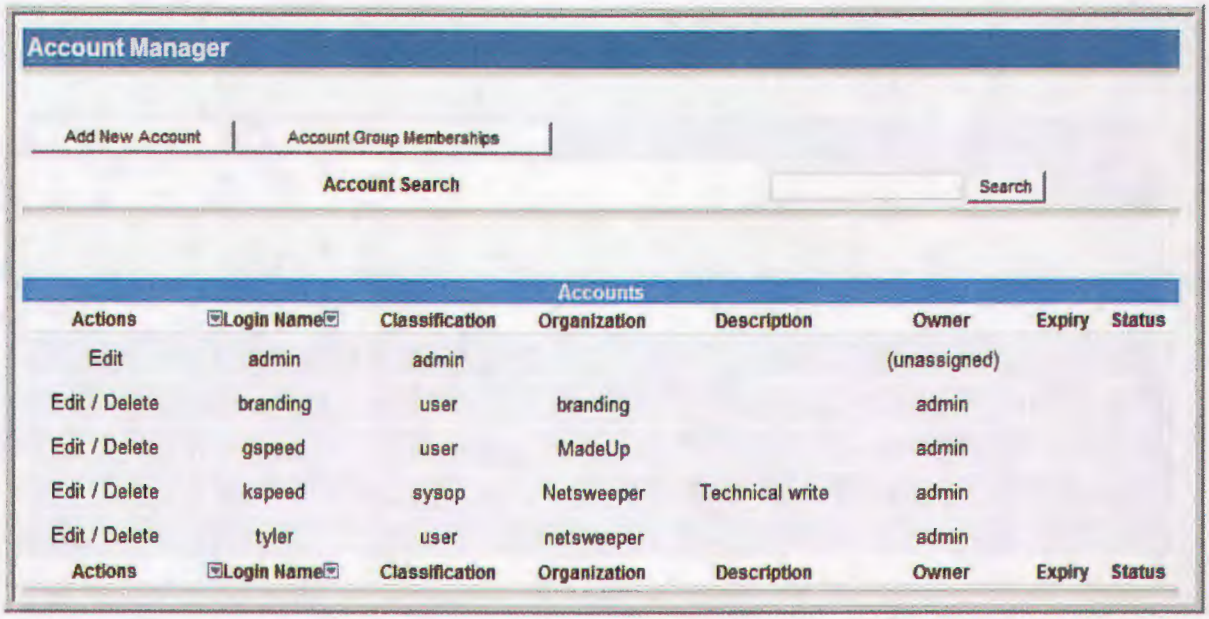


Figure 21 Account Manager window with Accounts list.

The Account Information page for that account will display.

4. Create a new password for the account and type it in both the Account Password and **Verify Password** boxes.
5. Click **Submit**.
6. Click **Apply Settings** on the taskbar to load the new account into all of the policy servers.
7. Click **Apply**.

You can also reset a password in the Client Filter Manager.

Resetting a Password from the Client Filter Manager

To reset a password in the Client Filter Manager:

1. On the WebAdmin menu bar, click **Account Management** and select **Client Filter Manager** from the drop-down list.
2. Find the account **Login Name** in the **Accounts** list, and Click **Modify** in the **Actions** column, to the left of the account name.
3. This displays the **Client Filter Manager** page for that account.
4. Click **Change Password** beside the **Actions** box.

5. On the **Change [Login Name]'s Password** page, type the new password in the **New Password** and **New Password Again** box and then click **Submit**.
6. Click **Apply Settings** on the taskbar to load the new account into all of the policy servers.
7. Click **Apply**.

Suspending an Account

To suspend an account:

1. In the WebAdmin, select **Account Manager** from the **Account Management** menu.
2. Click **Edit** beside the account you want to suspend.
3. Click **Suspend/Resume Account**.
4. Select the checkbox beside the option you want to disable and then click **Submit**. (To resume an account, clear the checkboxes and then click **Submit**.)
5. Click **Apply Settings** on the WebAdmin task bar in the top right corner of the page and then click **Apply**.

Using the Client Filter Manager

On the **Client Filter Management** page, you can:

- Reset or remove installs once an account has reached its install limit.
- Reset a user account password.
- Upload a new version of the **Netsweeper Client Filter**.
- Generate uninstall keys, used to uninstall the **Netsweeper Client Filter** when a user has forgotten a password and the affected computer has no Internet connection to use in retrieving a new password.

With the **Client Filter Management** permission, you can uninstall any **Netsweeper Client Filter** using the same Policy Server, even those outside of its group it belongs to. You can also install the **Netsweeper Client Filter** on virtually an unlimited number of computers under the same account. For these reasons, we recommend that only *admin* users have access to these advanced functions.

The **Client Filter Manager** allows you to assume the identity of the account for testing purposes. You can adjust the maximum number of installs, maximum number of profiles, set an expiry date for the account, or change the password, by clicking **Modify** beside the account. You can reset the number of installs to zero for an account by clicking **Reset Installs**. You can reset the accounts preferences for the Profile Manager by clicking **Reset Preferences**.

You can use the **Release Manager** to upload a new version of the **Netsweeper Client Filter** and then when users log on, it will tell them to update with newer version.

Resetting a Password from the Client Filter Manager

To reset a password in the Client Filter Manager:

1. On the WebAdmin menu bar, click **Account Management** and select **Client Filter Manager** from the drop-down list.

2. Find the account **Login Name** in the **Accounts** list, and Click **Modify** in the **Actions** column, to the left of the account name.
3. This displays the **Client Filter Manager** page for that account.
4. Click **Change Password** beside the **Actions** box.
5. On the **Change [Login Name]'s Password** page, type the new password in the **New Password** and **New Password Again** box and then click **Submit**.
6. Click **Apply Settings** on the taskbar to load the new account into all of the policy servers.
7. Click **Apply**.

Generating an Uninstall Key

When a user wants to remove or reinstall a client filter on his computer, the software will generate a security key and notify the user to contact his or her *admin* or *sysop* for an uninstall key. The *admin* or *sysop* will then generate an **Uninstall Key** in the **Client Filter Manager**.

However, if a user forgets his or her password and does not intend to uninstall the client filter, the *admin* or *sysop* merely resets the password in the Account Manager.

To generate an uninstall key:

1. Click **Account Management** on the WebAdmin menu bar. Select **Client Filter Manager** from the resulting dropdown menu.
2. Click **Uninstall Key Generator**.
3. Type in the six-digit Security key that the user provides.
4. Click **Generate Key**.

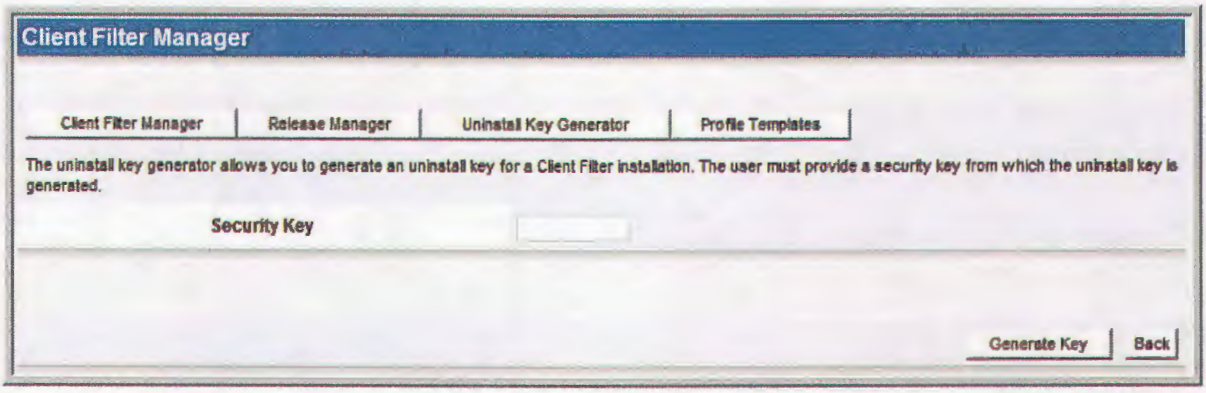


Figure 22: Uninstall Key Generator

Using the Customer Manager

Managing URL and Protocol Categories

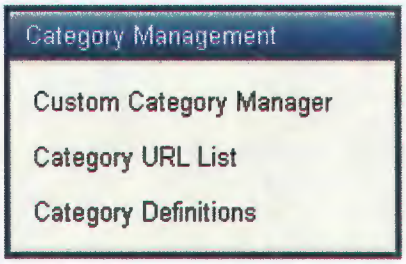


Figure 23 Category Management menu options

Category Management

The Category Management tools allow an *admin* or *sysop* to manage the blocked or allowed URL and protocol categories and create custom categories.

Table 3 Category Management Menu Options

Category Management Tool	Function
Custom Category Manager	This tool allows you to create or redefine filtering categories and assign URLs to these categories
Category URL List	This tool lists the built-in and custom URL and protocol filtering categories.
Category Definitions	This is a list of the category definitions for all the built-in categories used by Netsweeper. You can sort the category definitions by category name, group or number or search the category definition list.

Custom Category Manager

The Custom Category Manager allows the addition and maintenance of custom categories. Any category you create will show up in your Category Definitions. It will also show up in the logs and reports for your users when they try to access a URL that you have added as part of a new category.

Category URL List

Netsweeper allows you to override the categories assigned to a particular site by adding that URL to an Allow or Deny list.

Category Definitions

The Category Definitions page contains Netsweeper's official definitions of what type of content a page must contain to be included into each of the available categories. Additionally, if you create a new category, it will also show up in the **Category Definitions** page in the WebAdmin.

You can sort the definitions by name, number, or group. If you are looking for a particular category, you can search the list by keyword.

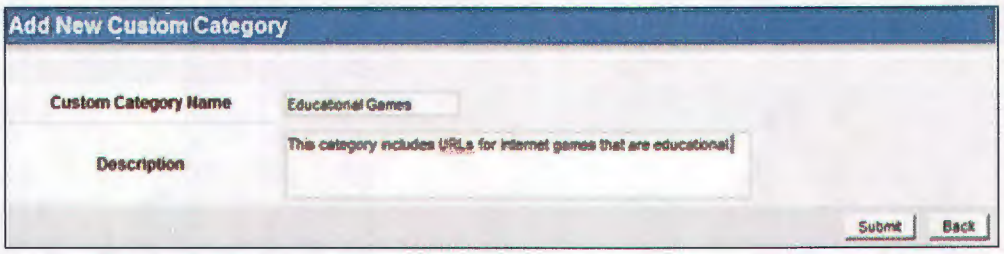


Figure **24**: Add a Custom Category

Adding a Custom Category

It is possible for you to create your own custom categories. These are categories that you want to filter or monitor, that are not in the Netsweeper default categories. The maximum number of custom categories is seven.

To add a custom category:

1. Select **Custom Category Manager** from the **Category Management** menu.
2. Click **Add New Category**.
3. Type in the **Category** name and a short description of the category.
4. Click **Submit**.
5. Click **Apply Settings** on the WebAdmin task bar in the top right corner of the page and then click **Apply**.
6. Add the list of URLs you want to associate with the category.

Adding URLs to the Category URL List

If there are URLs that you want to filter as part of a category, or URLs that you feel are incorrectly categorized, you can add them to the Category URL List and choose the category to which they belong.

To add a URL to the Category URL List:

1. Choose one of the following:
   - Select **Category URL List** from the **Category Management** menu,

   or

   - Click **Custom Category Manager** from the main menu and then click **Modify Category URL List**.
2. Click **Add New URL**.
3. Type in the URL (See How URL Lists???, for proper syntax.) and select the checkbox by any categories to which you want it assigned. Custom categories are at the bottom.
4. Click **Submit**.
5. Click **Apply Settings** on the WebAdmin task bar in the top right corner of the page and then click **Apply**.
6. Click the created link to check the URL address.
7. To edit the URL, click **Edit** beside the URL address.

Tip *If you have many URLs to add, import a list. Use the Categories Definitions page to find the category numbers, which are the keywords in this case.*

What Are the Built-In Netsweeper Categories?

Internet filtering fundamentally revolves around a filtering company's ability to categorize a URL. Netsweeper provides more than 50 different URL categories for you to use in filtering Internet content.

The following pages list the Netsweeper categories visible to the user/administrator. There are also a number of internal categories that are generally invisible to the user/administrator that are used to manage error conditions and internal processing. It is possible for a URL to belong to more than one category.

The Netsweeper categories can be filtered in "black list" or "white list" mode. In "black list" mode, when you choose a category, users will be blocked from going to or seeing any URL that has been determined to belong to that category. For example, when you select the Sports category, users are not allowed to go to URLs that are determined to be sports websites.

In "white list" mode, when you select a category, you are only allowed to go to URLs in that category. A common question is whether Netsweeper has a Child Safe category. This is an example of a white list category. To achieve this goal, you can import a list of acceptable websites and block all others.

The following list contains the categories that Netsweeper currently filters. The URLs listed are representative but not a complete list. Example websites were active at the time of writing.