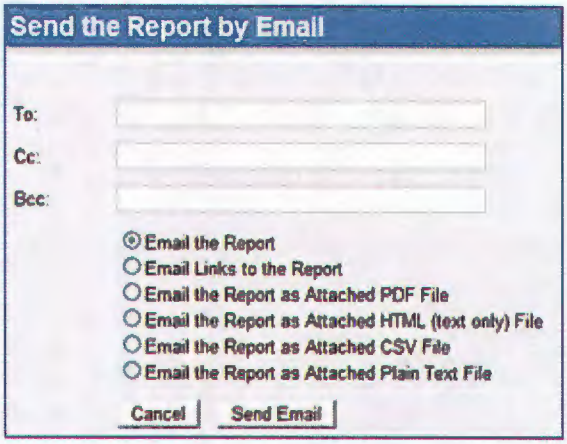


Figure 67: Email your Report

Editing a Report

To edit a report:

- Select **Demand Reports**, **Scheduled Reports**, or **Continuous Reports** from the **Reports** menu, depending on the type of report you want to edit.
- Select **Edit** beside the Report you want to edit.
- All of your original report settings automatically display.
- Change the filter settings you want to change, and click **Next>**.
- To edit a report group (Summary or Detail Group), select the name of the Group.
- To remove a report Group, select **Delete**.

  You must have at least one report group in your report. Once you have completed editing the group, click **Next>**.
- Edit the remaining report settings as you want.
- Click **Next>** to go to the end of the Report Wizard.
- At any time, click **Prev** (Previous) to return to the previous screen and make a change. However, once you begin editing a report group, you must finish editing that group before returning to the **Filters** window.
- To regenerate the report, select **Finish**.

Deleting a Report

If you no longer need a report, you can delete it.

To permanently delete a report:

1. Select **Demand Reports**, **Scheduled Reports**, or **Continuous Reports** from the **Reports** menu, depending on the type of report you want to delete.
2. Select **Delete** beside the report name.
3. Click **OK** to confirm the deletion.

Using the Request Log

Only *admin* and *master admin* accounts have direct access to the entire Request Log. This section describes how to open the request log and browse through the requests.

Quick Search provides a simple way to search through the logs for specific requests accessible to all administrators. See Using Quick Search.

The entire Request Log can be opened using the WebAdmin.

To access the Request Log:

1. Select **Request Log Files** from the **Reports** menu.

   The **Request Log Files** page displays:

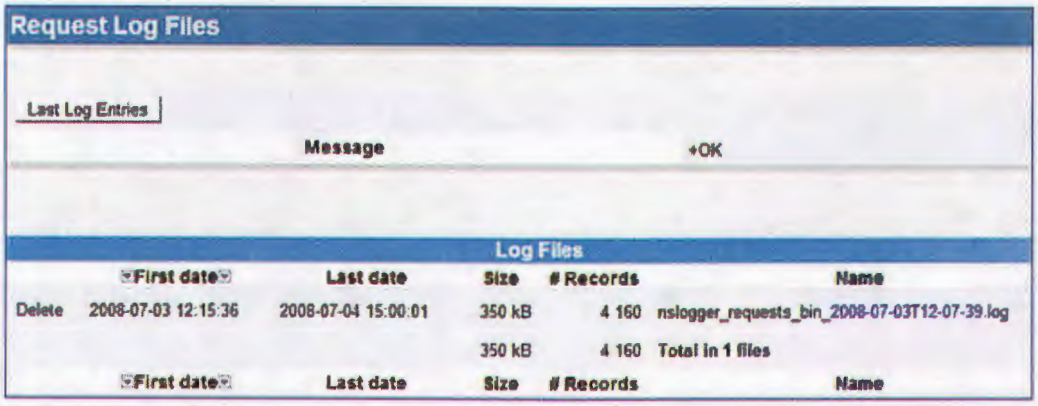


   Figure 68: Request Log Files Screen

2. Select **Last Log Entries** to view the 50 most recent entries.
3. Click **Delete** to delete the log (not recommended).
4. View the date of the oldest record in the log in the **First Date** column.
5. View the date of the most recent record in the **Last Date** column.
6. View the size of the log in the **Size** column.
7. View the total number of records in the log as shown in the **# Records** column.
8. To view the log, select the log name in the **Name** column.
9. To move through a log, use the page numbers and the navigation arrows (<<, <, >, and >>).

Using Advanced Reporting Features

In general, there are five main tasks involved in creating a report with the Report Wizard:

- Applying report filters
- Choosing your report groups
- Sorting your report data
- Choosing how to display each report Group with a graph or table
- Choosing how and when a report should be emailed

This chapter provides more detailed information on each of these tasks and how to use some of the advanced features available for these tasks. Not all tasks are required for every type of report. Use this chapter if you need more information about a specific task in the Report Wizard, or to learn more about the available features.

Using Report Filters

To reduce the size of reports and make them easier to read, use report filters to extract only the log entries you need. For example, include only a certain group of users, requests to particular Web site, or Web sites in certain categories.

Applying report filters is one of the first steps in creating any report with the Report Wizard. By default, a list of simple filters is displayed by the Report Wizard. While these simple filters are precise enough for most situations, there is also an advanced set of filters available if you require them.

Creating Simple Report Filters

When creating a report with the Report Wizard, you have the opportunity to apply one or more filters to the report.

To apply simple report filters:

Type your criteria in the fields. Only entries that meet those restrictions will be included in your report.

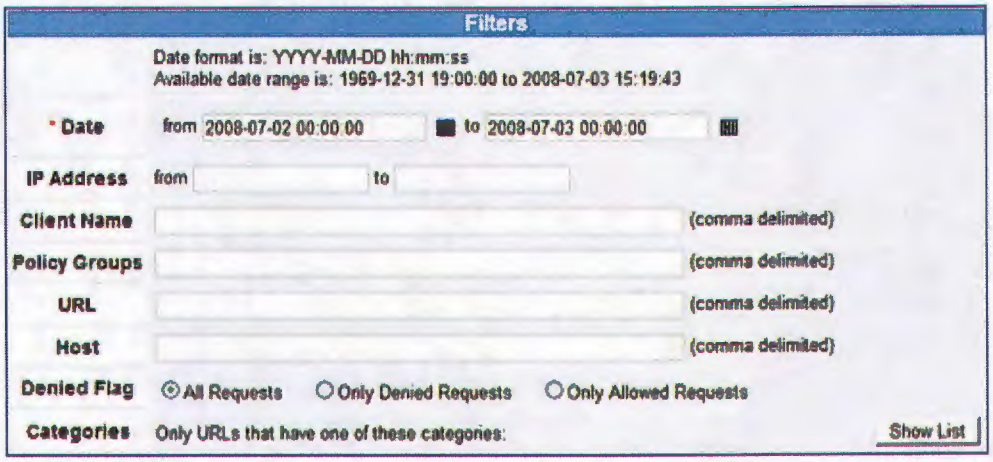


Figure 69: Simple Report Filters

Filter	Description
Date (only available for demand reports)	This includes only requests occurring during the time specified. When typing in the date, use the format shown on screen or click the calendar icon to select a date from the calendar. Each demand report should have a date filter. By default, a filter spanning the last 24 hours is automatically assigned. The report cannot include data from dates no longer stored in the logs. To determine how long your Netsweeper configuration stores the logs, see Using the Request Log.
IP Address	Every computer on your network is assigned a unique IP address. In most cases, each computer on the filtered network uses a static (unchanging) IP address. The IP Address filter is most useful in specifying a range of IP addresses. If you want to include non-sequential IP addresses or do not know the users' IP addresses, use the **Client Name** or **Group Policy** filters instead. Some deployments may use dynamically assigned IP addresses, using DHCP along with some form of external authentication. These deployments use the **Client Name** filter instead of the **IP Address** filter.
Client Name	A client name represents a specific computer. Admins or sysops can enter multiple Client Names in the Client Name field, separating them with commas but no spaces: *user1,user2,user3,user4*. Each Client belongs to a Group. Select **Client Manager** from the menu bar to view the **Client Names** assigned to you. Not all administrators have the permissions required to access the Client Manager. If you want to include an entire Group (or several Groups), use the Policy Groups filter instead.
Policy Groups	This filter includes only the requests made by members of the filtering groups specified. Select the names of the groups you want to include in the Policy Groups filter, separating the group names by commas but no spaces. For example: *group1,group2,group3*.
URL	Each web request is identified by a Uniform Resource Locator (URL). The URL is the full address that appears in the address bar of your browser when you visit a Web site. When you type one or more URLs in this filter, the report excludes requests to all other URLs. A *URL* identifies a specific page at a Web site, not the entire site. For example, http://www.netsweeper.com/Contact is a different URL than http://support.netsweeper.com If you wish to include all the pages at a particular Web site (such as netsweeper.com), use the **Host** filter instead.
Host	Unlike URLs, hosts can house multiple web resources, such as an entire Web site; not just a single web page. To include requests to all URLs that have the same host, select the host in the Host filter. You can enter multiple hosts, separated by commas with no spaces. For example: http://example1.com,http://example2.co.uk,http://example3.ca
Denied Flag	*Yes* indicates the request was denied, and *no* indicates that it was allowed. You can use the Denied Flag filter to list only denied requests or allowed requests. By default, all requests are included in the report unless you change this filter.

Filter	Description
Categories	This allows you to include only requests assigned to selected categories. To apply this filter, click **Show List** and select the categories you want to include. If you select no categories, the filter is not applied and the report includes all categories.

Switching between Simple and Advanced Filters

To switch from a **Simple Filter** to an **Advanced Filter:**

Click **Advanced Filter** at the bottom of a **Simple Filter** page.

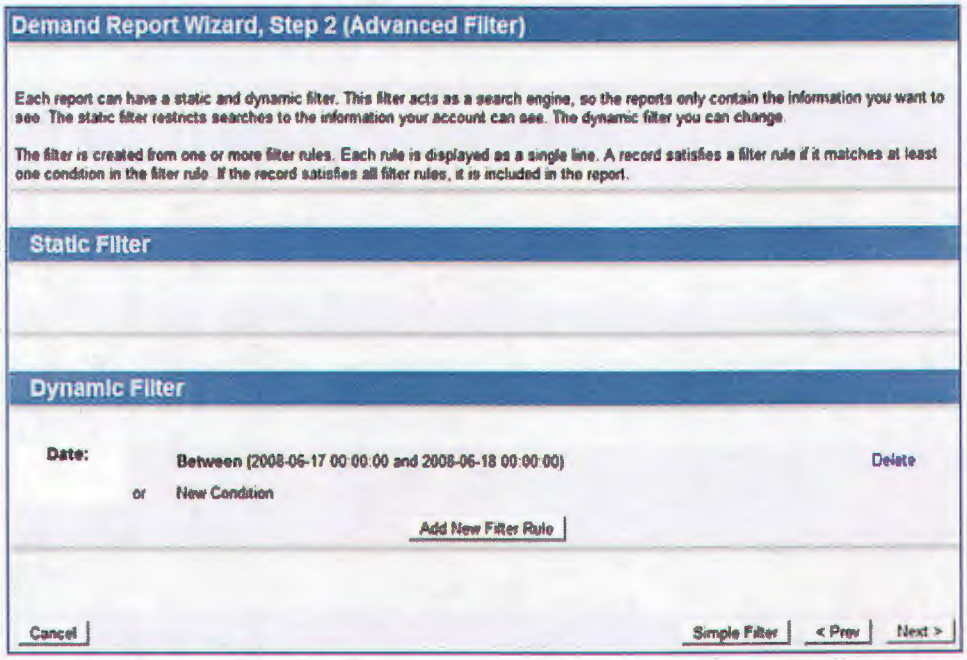


Figure 70: Advanced Filter screen

To switch from an **Advanced Filter** to a **Simple Filter**:

Click **Simple Filter** at the bottom of an **Advanced Filter** page.

Creating an Advanced Filter Rule

To create an advanced filter:

Select **Add New Filter Rule**. Most of the advanced filters use the following string comparisons:

- Less Than (<)
- Less Than or Equal To (≤)
- Equal To (=)
- Greater Than or Equal To (≥)
- Greater Than (>)
- Not Equal To (≠)
- Between

These comparisons sort the entries chronologically, numerically, alphabetically, and include only the entries that fall in the range you specify.

Use the following guidelines when setting advanced filters:

- The date 2006-12-26 15:41:01 is less than 2007-01-05 03:40:55 because it occurs first chronologically.
- The letter *a* is less than the letter *b* because a occurs first in the alphabet. For example, *apple* is less than *orange* and *ape* is less than *apple*.
- IP addresses are typically displayed as four octets in dotted decimal notation (that is, four numbers between 0 and 255, separated by decimals). When comparing IP addresses, the first octet is compared first, followed by each subsequent octet, as necessary. So, *10.1.1.1* is less than *192.168.2.1* (because 10 is less than 192) and *192.168.2.45* is less than *192.168.2.59.*

Using Report Groups

Detail and **Summary Groups** define how the information in the report is grouped together. Group data based on the user name, Web site, or category information using Summary Groups or show a detailed log of each request using Detail Groups.

Each report must have at least one Group. A report can use more than one Group in a report, including multiple Summary Groups and up to one Detail Group. However, you can not include multiple Detail Groups in the same report. In effect, this means you can create multiple reports in a single file. However, reports can get quite large when you include more than one Group.

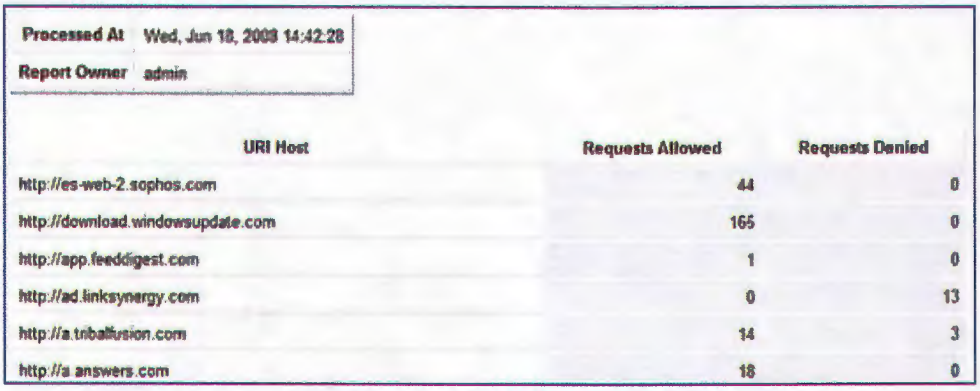
Choosing Summary Groups

Report data can be grouped together using one of the summary fields. Depending on the type of report, there are up to seven types of summary fields available:

- URI
- Host of URI
- IP Address
- User
- Policy Group
- Category
- Denied Flag
- Date Range (Ranging from 1 minute up to 1 month)

The Summary Group is the primary field used for the report. For example, if you select **Host of URI**, all requests made to a host are counted and displayed. In a table, each host appears as an item in the first column; in a pie graph, each host composes a "slice" of the pie; and in a line or bar graph, each host represents a point on the horizontal axis.

The following example was created with a **Host of URI** Summary Group:



Processed At Wed, Jun 18, 2008 14:42:28
Report Owner admin

URI Host	Requests Allowed	Requests Denied
http://es-web-2.sophos.com	44	0
http://download.windowsupdate.com	165	0
http://app.feeddigest.com	1	0
http://ad.linksynergy.com	0	13
http://a.tribalfusion.com	14	3
http://a.answers.com	18	0

Figure 71: Example report using Host of URI Summary Group

Choosing Fields

These are the secondary fields. When selecting these fields, the order in which you select affects the order they display in the report.

To move a field up or down, click and drag it to the position you want. See Sorting Your Report.

Once you have decided how to group the data, you can choose from of the following fields to include in the report:

Field	Description
Request Count	The total number of requests made by summary group.
Request Count Percent	The proportion (percentage) of requests, compared to all requests, made by summary group.
Requests Allowed	The total number of requests made by the summary group that were allowed.
Requests Denied	The total number of requests made by the summary group denied.
Page Count	The total number of page requests by summary group.
Page Count Percent	The proportion (percentage) of requested pages, compared to all page requests, by summary group.
Pages Allowed	The total number of allowed page requests by Summary Group.
Pages Denied	The total number of denied page requests by Summary Group.
File Count	The number of nonpage files requests by the Summary Group.
File Count Percent	The percentage of nonpage files requests, compared with all nonpage file requests, by Summary Group.
Files Allowed	The total number of allowed nonpage file requests by Summary Group.
Files Denied	The total number of denied nonpage file requests by Summary Group.

Choosing Detail Groups

Detail Group reports show each individual request (excluding those removed by the report filters). These detail reports are only available as tables. Since each request is stored in the Request Log as a single entry with seven fields, each of the fields can be included in the report as one of the columns headings in the table.

Seven report fields are available for Detail Groups:

- URI
- URI host
- IP address
- User (Client name)
- Policy Group
- Category
- Denied flag

The following example was created with a Detail Group:

Processed At Wed, Jun 18, 2008 15:11:12
Report Owner admin

Date	URI Host	Policy Group	Category	Denied Flag
2008-06-17 08:31:26	http://updates.junglebyte.com	PrimarySchools	General	Allowed
2008-06-17 08:31:30	http://www.google.com	PrimarySchools	Search Engine	Allowed
2008-06-17 08:33:08	http://stats.update.microsoft.com	PrimarySchools	Technology	Allowed
2008-06-17 08:33:14	http://download.windowsupdate.com	PrimarySchools	Technology,No Text	Allowed
2008-06-17 08:33:14	http://www.update.microsoft.com	PrimarySchools	Technology,No Text	Allowed
2008-06-17 08:33:14	http://download.windowsupdate.com	PrimarySchools	Technology,No Text	Allowed
2008-06-17 08:33:14	http://download.windowsupdate.com	PrimarySchools	Technology,No Text	Allowed
2008-06-17 08:33:16	http://download.windowsupdate.com	PrimarySchools	Technology,No Text	Allowed

Figure 72: Example report using a Detail Group

The order in which you select your fields determines the order that they display in the report.

To move a field up or down in the list, click and drag it to the position you want.

See Sorting Your Report.

Sorting a Report

Reports can be sorted to appear in many different ways. Choose the order that columns and rows appear in a table or the order on items along x-axis in a bar or line graph. The first step in sorting your report is to choose the fields in the report.

Sorting by Columns

The order in which you choose the fields is the order that the items display in a table or graph. However, line graphs use a separate line for each field. Pie graphs, on the other hand, can only include one field.

To adjust the order after you have selected your fields, click and drag a field up or down the list in the **Report Fields** column.

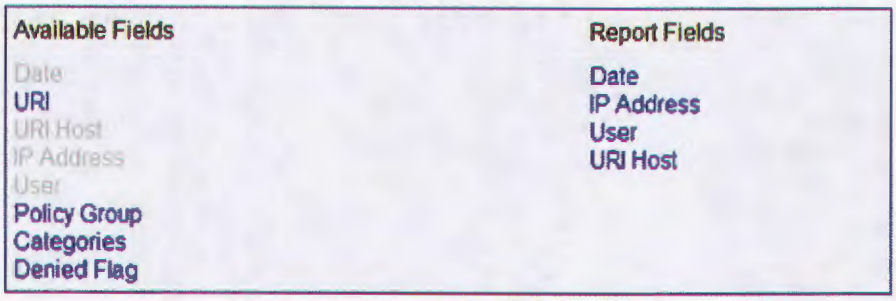


Figure 73: Detail Group column sorting

If you are creating a Summary Group, choose one field to Group the information (URI, Host of URI, IP address, User, Policy Group, Category, Denied flag, or a Date Range) before choosing additional fields. This field is always used as the first column in a table or as the x-axis values in a bar or line graph. The remaining Summary Group fields are then sorted in the order in which you select them.

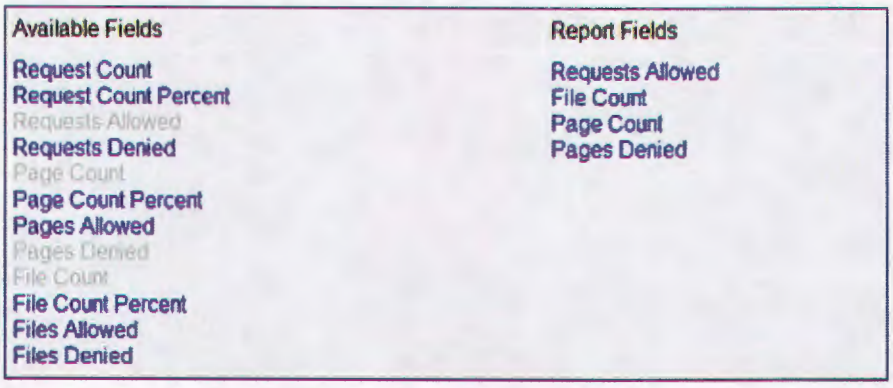


Figure 74: Summary Group column sorting

Sorting by Rows

The order that rows (in a table) or groups of bars (in a 2D or 3D bar graph) appear in can be sorted alphabetically, numerically, or chronologically, depending on the field. For example, the **User** field can be used to sort the rows alphabetically, the **Date Range** fields can sort them chronologically, and the **IP address** field can sort them numerically.

Each field can be sorted in **Ascending** or **Descending** order. When choosing your row sorting, the screen looks similar to this, though the **Available Fields** will vary.

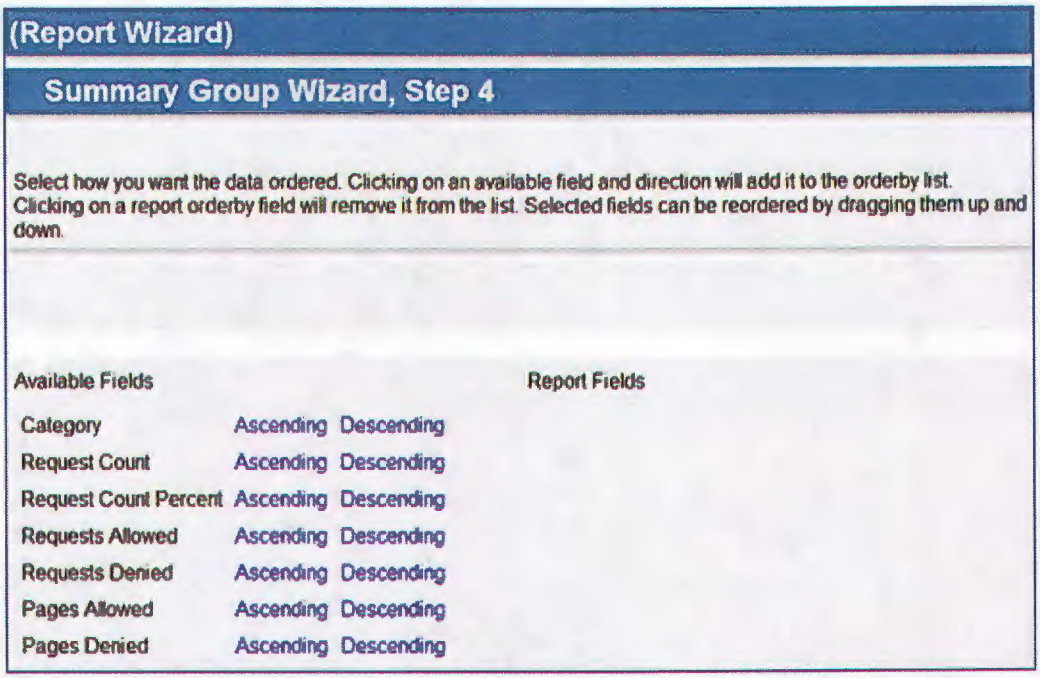


Figure 75: Row sorting a Summary Group

To sort the rows, select **Ascending** or **Descending** beside the field you want to sort by.

For example, if you selected **Requests Denied Ascending**, then **Pages Allowed Descending**, in order in a Summary Group, the report would be ordered from the highest number of **Requests Denied** down to the lowest. If two or more groups had the same number of **Requests Denied**, that block of groups would be sorted from lowest number of **Pages Allowed** to highest. In the event that a tie still exists after all the sorting options are exhausted, the remaining fields are used to break the tie in the order they were selected.

Using Graphs and Tables

During the creation of most reports, you are provided the option of choosing what format the information is presented in. The Reporter has five different presentation formats available:

- Data Tables
- Pie Graphs
- 2D Bar Graphs
- 3D Bar Graphs
- Line Graphs

Detail Group Options

When creating a Detail Group in a Scheduled or Demand Report, only data tables can be displayed.

Graph Options for Summary Groups

Not all formats are available for every report. For example, since each entry in a Detail Group is unique, these report groups can only be presented as tables. Continuous Reports use only line graphs. For Scheduled and Demand Reports, the following table lists the available presentations for each type of report.

Demand and Scheduled Reports

Graph Options	Data Table	Pie Graph	2D Bar Graph	3D Bar Graph	Line Graph
URI	✓				
Host of URI	✓				
IP Address	✓	✓	✓	✓	
User	✓	✓	✓	✓	
Policy Group	✓	✓	✓	✓	
Category	✓	✓	✓	✓	
Denied Flag	✓	✓	✓	✓	
Date Range	✓		✓	✓	✓

✓ = The presentation format is available

Continuous Reports

All continuous reports display as line graphs.

Data Tables

Data tables are the most common format used for presenting reports and are always available when creating a Scheduled Report or a Demand Report. Selecting the table and modifying its options are the final steps in creating a report Group.

When customizing the tables in your report, you will have some or all of the following options:

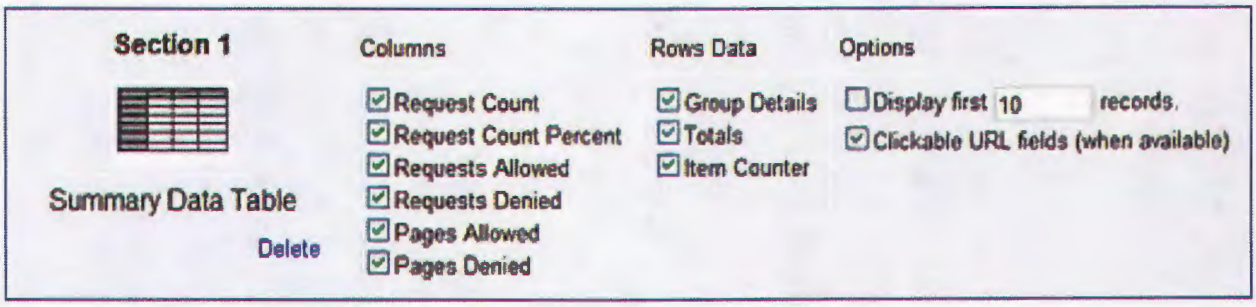


Figure 76: Data Table options

Data Table Options	Description
Columns	Select the checkboxes beside fields you want to use as **Columns** in the table. By default, all fields are selected. Clear the check boxes beside fields you want to omit.
Rows Data	Select whether the individual **Group Details** rows should be displayed. Typically, you should leave this option selected. This option is only available for Summary Groups. Select whether to display the **Totals** row, which sums up the total number (or Totals percentage) of request, pages, or files out of all the records in the report. This option is only available for Summary Groups. Selecting the Item Counter options counts the items in the report.
Other options	Limit the number of records in the report by selecting **Display first 10 records**. You can also change the number of records in the report by editing the number in the text field. Choose whether any URLs listed in the report should be hyperlinks pointing to the actual URL by selecting **Clickable URL fields (when available)**. This field is selected by default.

Pie Graphs

Pie graphs, available only for Summary Groups, are useful for comparing a single field in the report.

Each slice of the pie is a different color and represents one of the Summary Groups (the IP address, user, Policy Group, category, or denied flag setting that you selected when creating the report).

Pie graphs are not available for URI or Host of URI Summary Groups.

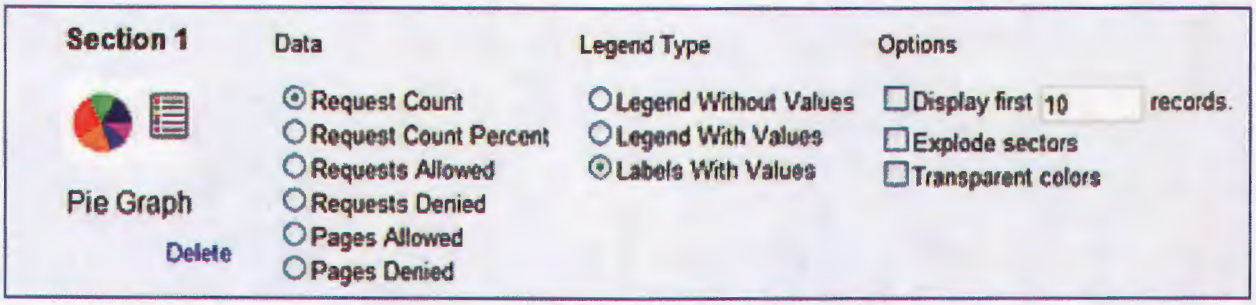


Figure 77: Pie Graph options

Pie Graph Options	Description
Data Field	Select which **Data** field to use in the pie chart. Remember, you can create several pie graphs, each with a different **Data** field.
Legend Type	Select the **Legend Type**. The legend is a table used to identify which Group is associated with each slice of the pie. You can choose a legend with or without the numerical values displayed or you can choose to display labels for each slice surrounding the pie graph. In general, a legend without values is not recommended for large reports.
Other options	Limit the number of records in the report by selecting **Display first 10 records**. That is, show only the top 10 entries in the report. You can also increase or decrease the limit by editing the number in the text box. Select **Explode Sectors** to add some space between the slices so that smaller slices are more easily distinguished. Select **Transparent colors** to display the slices with transparent colors.

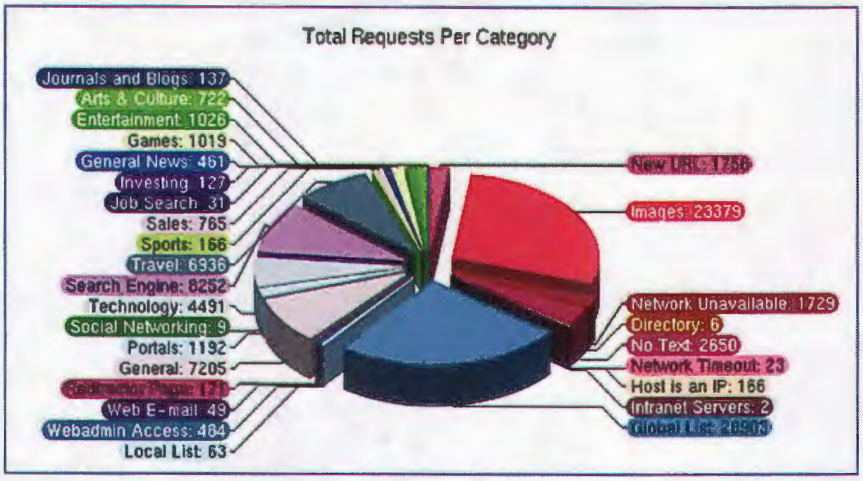


Figure 78: Exploded Sectors example

2D Bar Graphs

2D bar graphs have the following options:

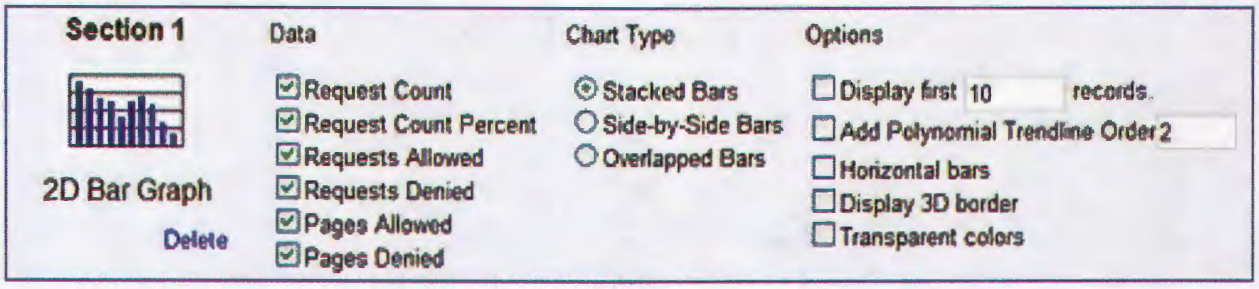
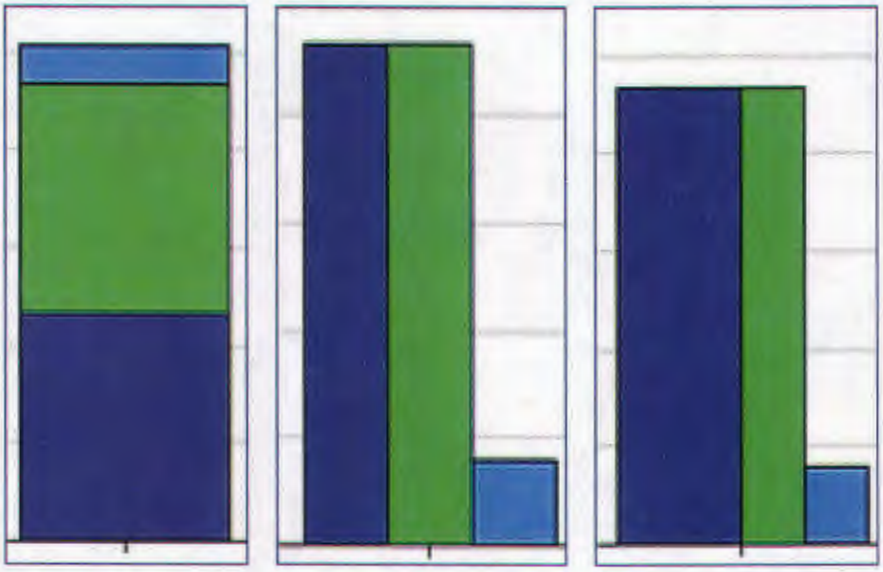


Figure 79: 2D Bar Graph options

2D Bar Graph Options	Description
Data	Select the checkboxes beside the Data fields you want. Each selected field is included as a different colored bar. Each different Summary Group has its own set of bars.
Chart Type	Select how each set of bars should be displayed using Chart Type: Stacked bars, Side-by-Side bars or Overlapped bars. (See illustration below the table.)
Other Options	Limit the number of records in the report by selecting Display first 10 records. That is, show only the top 10 entries in the report. You can also change the number of records the report is limited to by editing the number in the text box. Add a Polynomial Trend line to chart the direction of changes in activity. This option is only recommended for Date Range summary groups. You can also edit the order of the trend line. Display a 3D border around each bar. This makes small, hard-to-see bars more visible. You can also set the bars to display in Transparent Colors.



Stacked *Side-by-side* *Overlapped*

3D Bar Graphs

3D bar graphs have the following options:

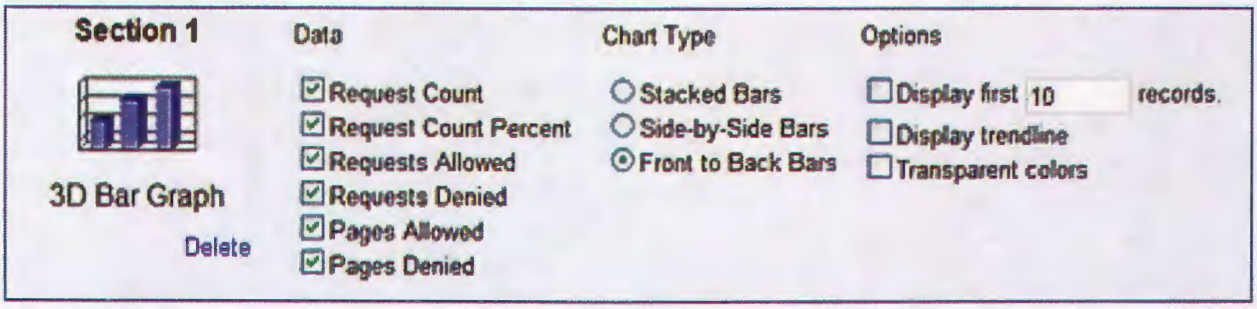


Figure 80: 3D Bar Graph options

3D Bar Graph Options	Description
Data	Select the check boxes beside any **Data** options you want to include. Clear the check box beside any **Data** options you want to omit. Each selected field displays as a different colored bar.
Chart Type	Select how each set of bars should be displayed using **Chart Type:** Stacked bars, Side-by-Side bars or Front-to-back bars. (See illustration below the table.)
Other Options	Limit the number of records in the report by selecting **Display first 10 records**. You can also change the number of records in the report by editing the number in the text box. Select **Display Trend line** to chart the direction of changes in activity. This option is only recommended for **Date Range** summary groups. You can also edit the order of the trend line. **Display a 3D border** around each bar. This makes small, hard-to-see bars more visible. Select whether you want the bars to display in **Transparent Colors**.

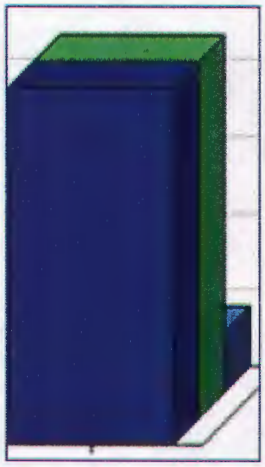


Figure 81: Front to Back Bars

Line Graphs

Line graphs are only available if you select a **Date Range** as your Summary Group. Line graphs have the following options:

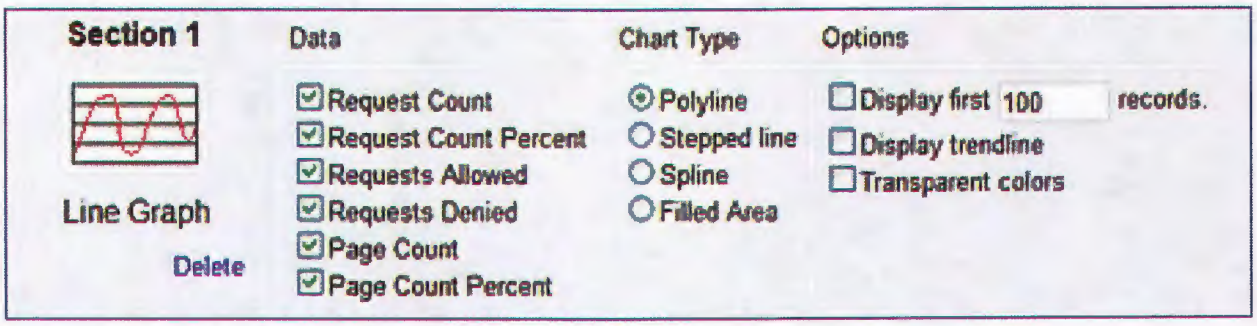
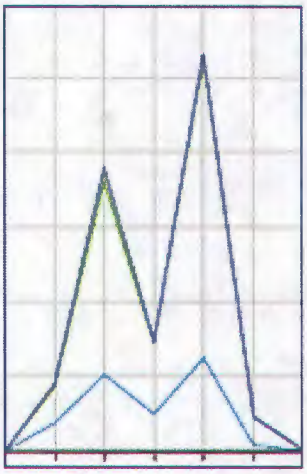


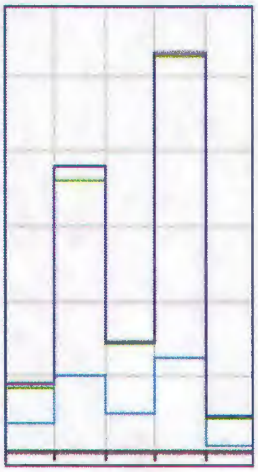
Figure 82: Line Graph options

3D Bar Graph Options	Description
Data	Select the check box beside any **Data** option you want to include. Clear the check box beside any **Data** options you want to omit. Each field displays as a different colored line.
Chart Type	Select the type of chart: • In a **Polyline** graph, the line is composed of many small line segments, creating a "jagged" effect. • A **Stepped Line** shows a plateau at each data point. • A **Spline** shows a single curved line. • A **Filled Area** graph fills the area between the lines. See the samples below this table.
Other Options	Limit the number of records in the report by selecting **Display first 100 records**. You can also change the number of records in the report by editing the number in the text box. Select **Display Trend line** to chart the direction of changes in activity. This option is only recommended for **Date Range** summary groups. You can also edit the order of the trend line. Select whether you want the bars to display in **Transparent Colors**.

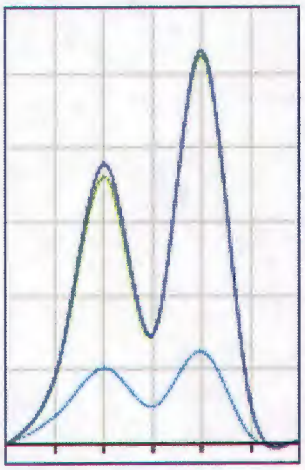
Table 12 Chart Types



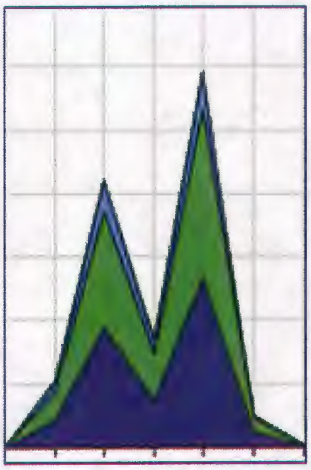
Polyline



Stepped Line



Spline



Filled Area

Using Email Options

The Report Wizard offers several options for how and when emails should be sent. **Report Delivery** offers options for how the report is delivered, **Empty Reports** offers options for how to handle empty reports, and **Conditional Sending** allows for the addition of conditions under which the report will be sent.

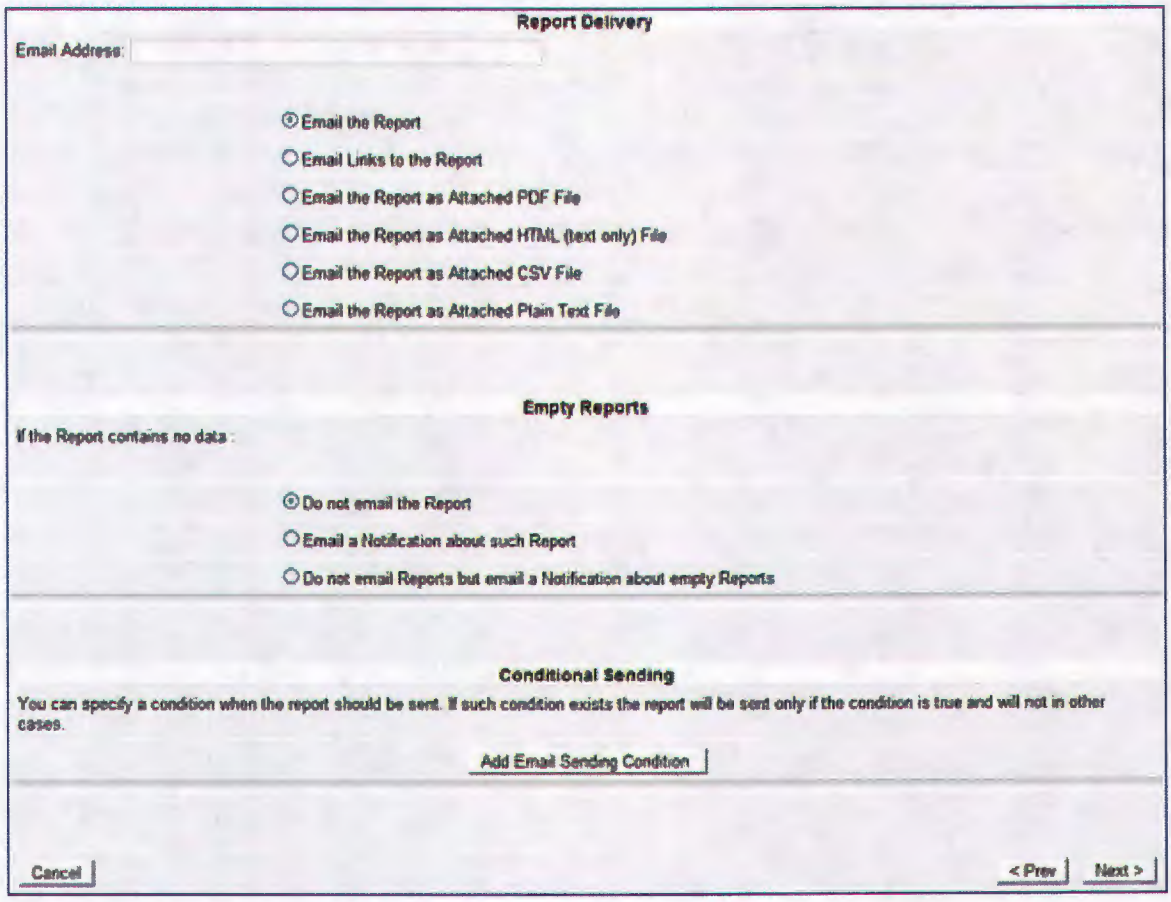


Figure 83: Email Options screen in Report Wizard

Setting the Email Recipients of a Report

Type your email address in the **Email Address** field and the report will be sent as an email shortly after it is processed. If you want to send the report to more than one address, you can enter multiple email addresses, separated by commas with no spaces. For example, example1@netsweeper.com,example2@netsweeper.com.

If you leave the **Email Address** field blank, the report is not emailed but you can still view the report using the WebAdmin. See Viewing a Report.

Setting Report Delivery Options

Select your desired **Report Delivery** option. We recommend the default option, **Email the Report**.

Report Delivery Option	Description
Email the Report	This is the default option. This HTML based format can be read by most email clients and can contain all table and graph formats.
Email Links to the Report	The email sent includes only links that you can use to download the report in various formats. The report is served from your Netsweeper Server.
Email the Report as Attached PDF File	Attach the report as a PDF
Email the Report as Attached HTML (text only) File	Attach the report as an HTML text file. (No graphs are shown in a text file).
Email the Report as Attached CSV File	Attach the report as a comma separated values (CSV) file.
Email the Report as Attached Plain Text File	Attach the report as a plain text (.txt) file.

Setting Empty Report Options

Select an **Empty Reports** option to decide what to do if a report contains no data. The options are:

Empty Report Option	Description
Do not email the report	No email is sent to the report recipients.
Email a Notification about such Reports	An email notifies report recipients that the report was empty.
Do not email Reports but email a Notification about empty Reports	This setting overrides all of the above settings. Reports are never sent by email, but in the event that an empty report is generated, a notification email is sent.

Setting Conditions for Emailing a Report

To set conditions for emailing a report, select **Add Email Sending Condition** from the **Email Options** screen in the Report Wizard.

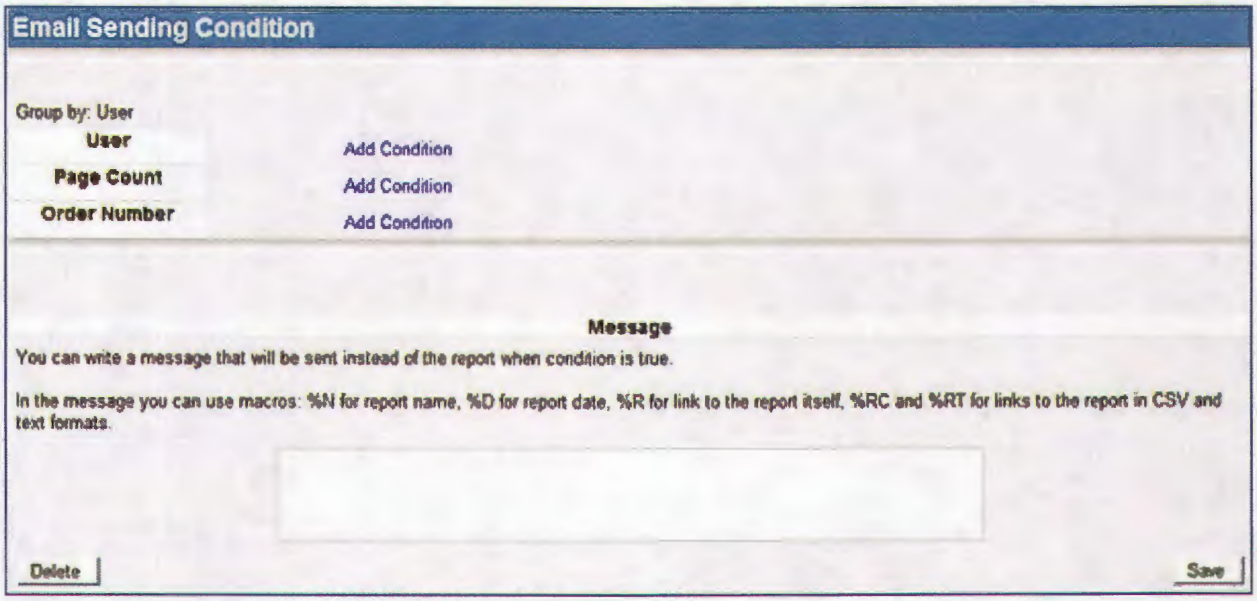


Figure 84: Email Sending Conditions Screen

To add a condition for the sending of a report:

1. Select **Add Condition** beside one of these: User, Page Count, or Order Number.
2. Select one of the string comparison options and enter a user, or a number, depending on which condition you selected. For more information, see Advanced Report Filters, as the conditions will behave similarly.
3. Click **Finish**.
4. Repeat steps 1-3 until you have added all the conditions that you want.
5. If you want to send a message, instead of a report, when the conditions are met, type the message in the box provided and click **Save**.
6. Click **Finish**. The report will now be sent only if the conditions are met.

Configuring the Reporter

Only the built-in *master admin* account can access these settings through the WebAdmin. Other *admin* and *sysop* accounts do not have access to these settings. If you do not have access to the built-in *master admin* account, contact an administrator with access if you need the Reporter settings adjusted.

The Reporter Settings control how much disk space is used by the Reporter and define which types of requests are defined as "pages". The WebAdmin Settings allow you to specify which Quick Reports are available to all other accounts on the Policy Server.

This chapter describes how each of these settings work and how to adjust them.

Setting Report Restrictions

The Reporter Settings allow you to set various restrictions on what types of reports are available, how much hard disk space the Reporter can use and what information that report email should include. The following report settings are accessed by selecting **System Configuration** from the **Reports** menu and selecting **Reporter Settings.**

Note *Apply settings after making any changes to the Reporter Settings. To apply settings, select **Apply Settings** from the top right-hand corner of the WebAdmin, and click **Apply**.*

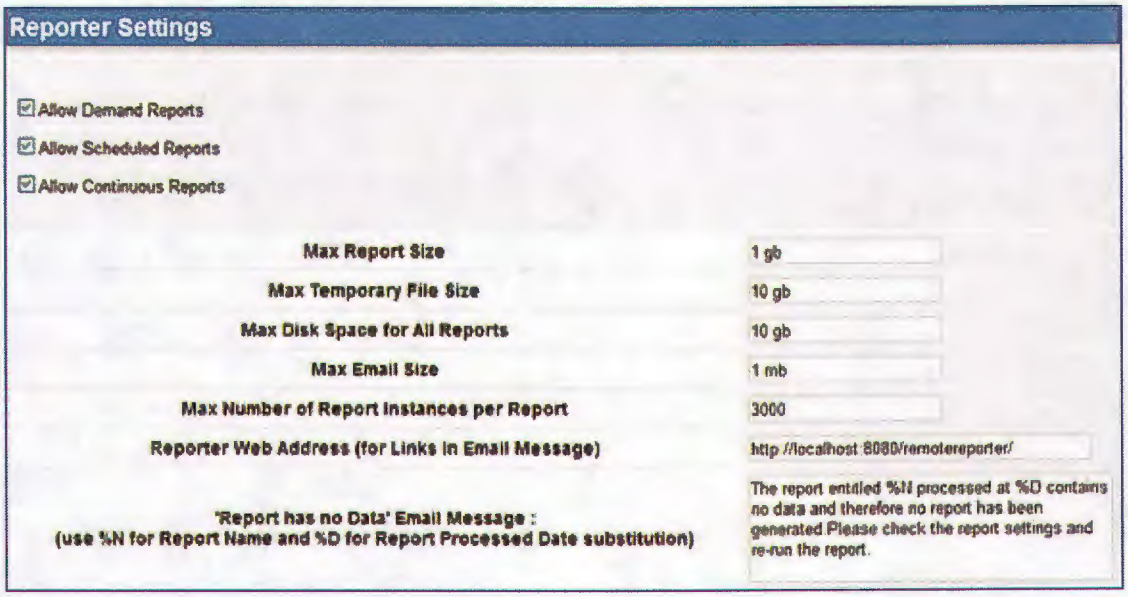


Figure 85: Reporter Settings

Allowing Demand, Scheduled, and Continuous Reports

Option	Description
Allow Demand Reports	Choose whether to allow users to create and view Demand Reports. Note that this will also disable Quick Search and Quick Demand Reports.
Allow Scheduled Reports	Choose whether to allow users to create and view Scheduled Reports.
Allow Continuous Reports	Choose whether to allow users to create and view Continuous Reports.

Setting Hard Disk Restrictions

Hard Disk Restriction	Description
Maximum Report Size	Set the maximum size (disk space) that a report can reach. Reports that exceed this size are not processed, not available on the WebAdmin, and not emailed.
Maximum Temporary File Size	During processing, each report creates a temporary file to store data removed after the report is finished. Set the maximum size of this file.
Maximum Disk Space for All Reports	Set a limit on the total amount of disk space allowed for all reports on the server. The Reporter regularly checks the total size of all reports on the server and removes the oldest reports if the limit is exceeded.
Maximum Email Size	Set the maximum size of a report that can be emailed. If a report exceeds this size, either no email is sent, an email with links to the report on the server is sent, or a notification indicating that the report was too large is sent, depending on the settings of the individual report.
Maximum Number of Report Instances per Report	A Scheduled Report generate many times. Each time it generates, a new "instance" is created. Set the limit on the number of instances stored on the server. Once the limit is reached, the oldest report is deleted to make room for a new report. Old scheduled reports may be removed before the instance limit is reached if the maximum disk space for all reports limit is reached first.

Customizing Report Emails

Report Email Option	Description
Reporter Web address (for a link in an email message)	Type in the host name and WebAdmin port of the Reporting Server. In single server deployments, this should always be in the format *http://localhost:8080* unless you are using a port other than 8080 for the WebAdmin.
"Report has no data" email	This is the message sent by email when an empty report generates. In the actual email, %N is replaced by the name of the report and %D is replaced by the date of the report.

Defining a Page by an HTML Extension

Counting the number of requests a user makes does not necessarily provide a true reflection of their level of activity. A single web page is often composed of many different resources, each of which must be accessed with a separate request. Because of this, when you access a single web page, your browser may make several requests in order to display the page.

To report only on the actual pages visited, instead of the total number of requests, the Reporter classifies all requests as either "pages" or "files" based on the request's file extension. Every request is categorized as a page or a file. Only requests with a file extension in the HTML Extensions list are classified as pages, while all others are classified as files. Requests commonly classified as files include images (**.jpg*, **.gif*, **.png*) and cascading style sheets (**.css*).

Thus, the Reporter can report on actual web pages visited instead of simply the total number of requests. However, new file extensions may emerge, which means not all possible pages may be included in the HTML Extensions list, and a page may include multiple requests with file extensions in the extensions list. Thus, the Reporter can only provide an estimate, not necessarily an exact measurement of the number of pages accessed.

Default HTML Extensions List

The following extensions are included in the HTML Extensions list by default on all Netsweeper Servers:

Common Text Pages

Type	Description
htm	Common HTML file.
html	Common HyperText Markup Language (HTML) file.
sgm	SGML (Standard Generalized Markup Language) file.
sgml	SGML file.
wml	Wireless Markup Language (WML) file.
wmlp	Alternate Wireless Markup Language file
xhtml	EXtensible HyperText Markup Language (XHTML) file.
xml	EXtensible Markup Language (XML) file.

Active Pages

Type	Description
asmx	ASP.NET Web Service page
asp	Microsoft Active Server Page (ASP)
aspx	ASP.NET (Microsoft .NET Active Server Page) page
cfm	Cold Fusion Markup language page
jsp	Java Server Page
xsp	eXtensible Server Page (Microsoft .NET)

Pages Generated by Script Language

Type	Description
cgi	Common extension for Common Gateway Interface (CGI) scripts
ksh	Korn Shell script
php	Hypertext Preprocessor (PHP) script
php3	PHP (version 3) script
php4	PHP (version 4) script
phtm	Additional extension for PHP script pages
phtml	Additional extension for PHP script pages
pl	Perl script
py	Python script
sh	Shell script
shtm	Server Side Includes HTML
shtml	Server Side Includes HTML
tcl	Toolkit Common Language (Tcl) script

Editing the HTML Extensions List

Once you add an extension to the HTML Extensions List, any files that use that extension will now be classified as *pages* instead of *files*.

Adding an HTLM Extension

To add an extension to the HTML extensions list:

1. Select **System Configuration** from the **System Tools** menu.
2. Click **Reporter Settings**.
3. At the bottom of the list beside the **Add** button, type the extension without the period.
4. Click **Add**.

   If you remove an extension from the HTML Extensions List, the Reporter will classify any files that used that extension as files.

Removing an HTML Extension from the List

To remove an extension from the list:

1. Select **System Configuration** from the **System Tools** menu.
2. Select **Reporter Settings**.
3. Select **Delete** beside the extension name you want to delete.
4. Click **OK**.

Note *Apply settings after making any changes to the* ***Reporter Settings****. To apply settings, select* ***Apply Settings*** *from the top right-hand corner of the WebAdmin, and click* ***Apply****.*

Allowing Others to Use Quick Reports

The **WebAdmin Settings** allow you to choose which Quick Reports are available for all administrators, sysops, and users on the system.

To enable the Quick Reports you want available to other Login accounts:

1. Select **System Configuration** from the **System Tools** menu.
2. Select **WebAdmin Settings**.
3. Scroll down to **Enabled Quick Reports** under the **General Settings** heading.
4. Press the **Ctrl** key and select the names of all of the Quick Reports you want available. Selected names are available, and unselected names are unavailable.
5. Click **Submit**.

Note *Apply settings after making any changes to the* ***System Configuration****. To apply settings, select* ***Apply Settings*** *from the top right-hand corner of the WebAdmin, and click* ***Apply****.*

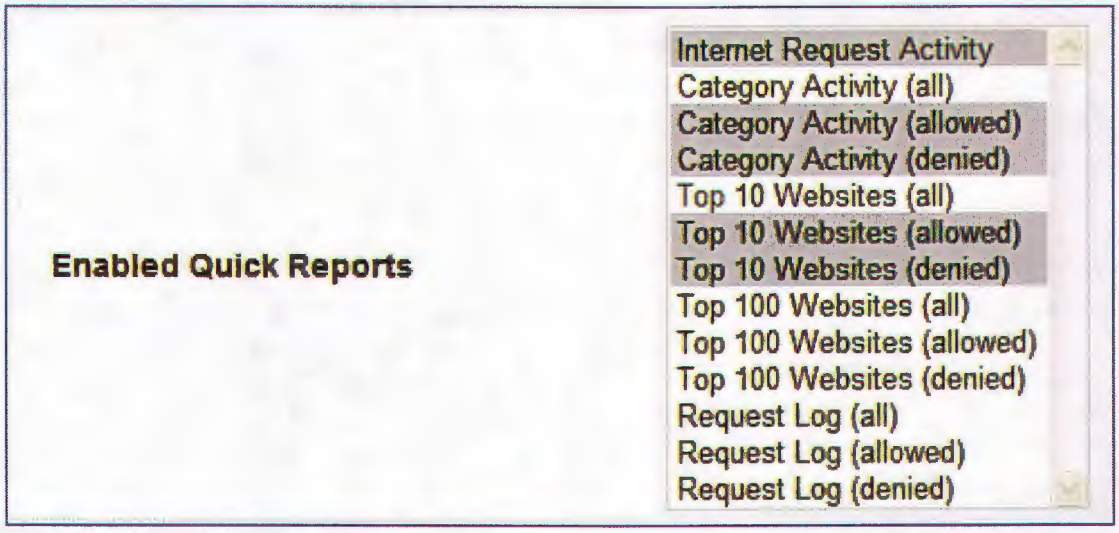
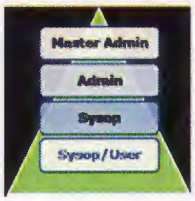


Figure 86: Enabled Quick Reports



Using Logs

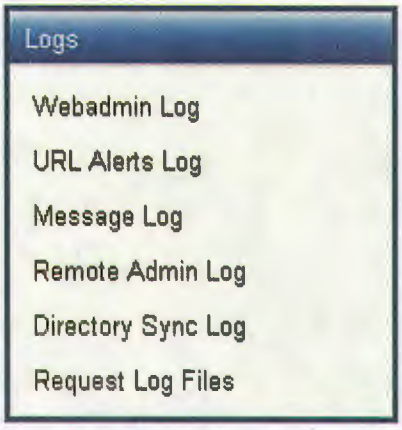
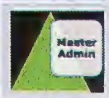
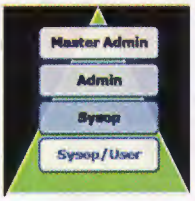


Figure 87 Logs menu

Logs		Function
WebAdmin Log		Stores debugging information and account Internet activity that you can search by user name, action, type, or IP and sort in ascending or descending order by date
URL Alerts Log		Stores URL alerts, which you can search by user name, action, type, or IP and sort by ascending or descending date
Message Log		Stores information about the general operation of the Netsweeper Policy Server
Remote Admin Log		Stores information about changes in filtering groups as well as information about remote administration
Directory Sync Log		Stores information about Active Directory that you can search by keyword or source URL
Request Log Files		Stores the last 50 Internet requests made to the Netsweeper Policy Server



Using URL Tools

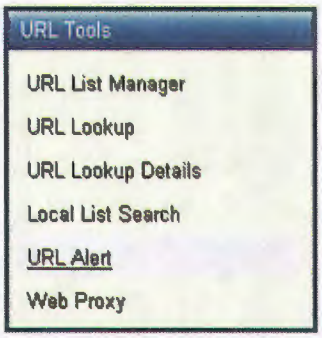


Figure 88 URL Tools menu

The tools accessed through the URL Tools menu allow you to create precise custom filtering for your Netsweeper system. You can block or allow individual websites by adding their URLs to a Deny or Allow list. The URL Tools also allow you to ask Netsweeper to review the classification of a URL that you feel is incorrect.

You can create custom URL Allow and Deny lists to override the default category assignments of the Netsweeper categorization engines. This allows you to create exceptions to the filtering policies. For example, you may want to block access to most social networking sites but allow access to a site whose content you trust.

You can use the URL lookup tools to see the categories that the Netsweeper categorization engines, using Artificial Intelligence, have assigned a specific URL. If you suspect that a site has been incorrectly categorized, then you can create a URL Alert to notify Netsweeper that one of our human content analysts should review the site.

Table 13 URL Tools Menu Options

URL Tools	Function
URL List Manager	Allows you to type in the URLs of individual websites that you want to allow or block or import a list of URLs.
URL Lookup	Allows you to look up the category assigned to a URL.
URL Lookup Details	Allows you to look up the category assigned to a particular URL and provides the correct syntax if you want to block the website.
Local List Search	Allows you to search for an individual URL in your Local List[12] to determine whether the URL has been blocked or allowed for a specific group, policy, or client.
URL Alert	Allows *admins*, *sysops* and users to request that Netsweeper check the accuracy of a URL's categorization.
Web Proxy	Allows you to test the filtering policies for a group by assuming the group's identity to browsing the Internet.

Managing the URL Lists

You will use URL Lists to allow or deny specific URLs to undo allow or deny rulings based on category assignments. Several URL lists with different authority levels are available. From highest authority to lowest, they are as follows:

List	Authority Level	Ranking
Deny Page Allow URL List	Highest	◆◆◆◆◆
System URL Lists	Higher	◆◆◆◆
Local URL/Keyword Lists	Medium	◆◆◆
Global URL Lists	Lower	◆◆
Category URL List	Lowest	◆

A URL that is both on the Global URL Allow List and the System URL Deny list would always be denied, since System lists have more authority than Global lists.

Deny Page Allow URL List

If you have created custom deny pages, all files in the deny pages must be added this list.

To test whether your all of your deny page files have been properly added, type the **Deny Page** URL into **the Deny Page Test Tool** in the WebAdmin. If you discover errors, add the inaccessible URLs to the **Deny Page URL Allow List**.

[12] *Sysops* can only view local lists assigned to them.

System URL Lists

The **System URL Allow** and **Deny Lists** are used to override all other filtering settings. Add a URL to the **Allow List** and Netsweeper will allow access to it. Similarly, add a URL to the **System Deny URL List**, and Netsweeper will deny access.

Local URL/Keyword Lists

The Local URL/Keyword Lists are used to always allow or deny a URL for a particular policy. Only users assigned to that policy's group, during times when the policy is active, will be affected. Both URL's and keywords can be type ined in this list.

Keywords are a string of characters that can appear in a URL. For example, adding "sex" to the Local Deny List would block access to sites like http://www.sex.com, http://www.middlesex.com, and http://www.sussex.co.uk. As you can see from this example, it is important to be very careful when using keywords.

These lists can be overridden by entries in the System URL List.

Global URL Lists

The Global URL Lists are similar to the System URL Lists. They are used to allow or deny access to specific URLs to all users on the system. However, these lists can be overridden by the Local or System Lists, or simply turned off on a per policy basis.

Category URL List

The Category URL Lists are for URLs that you want to add to a category, or URLs that you want to re-categorize. This list is overridden by all the other lists because it has the same priority as the categories themselves.

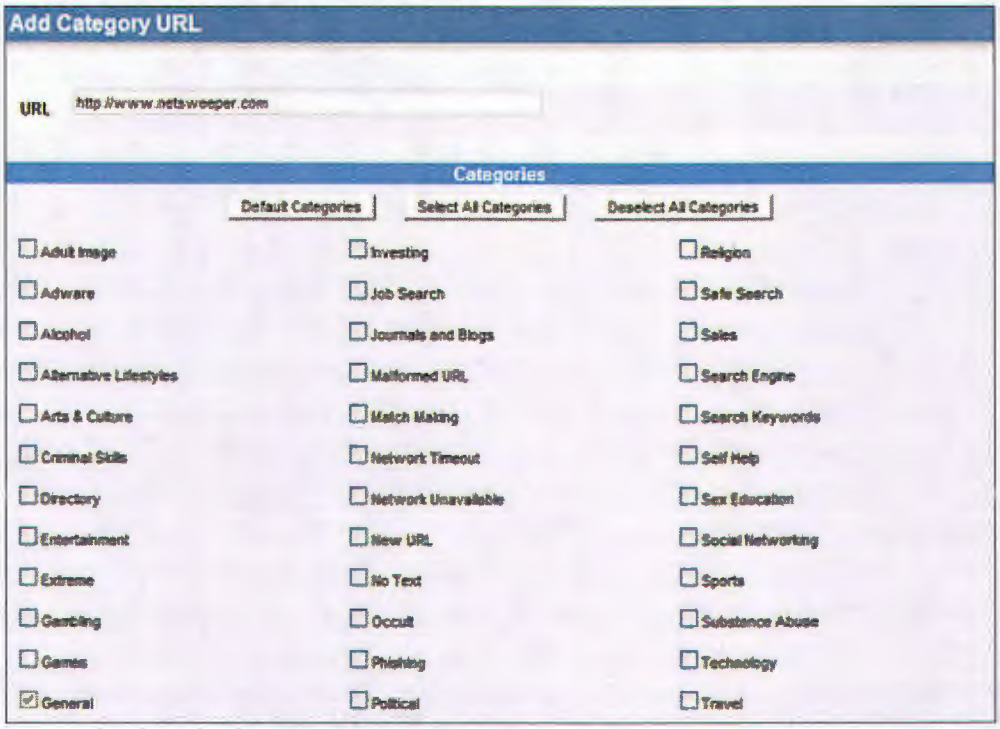


Figure 89 ***Add Category URL*** *window*

Parsing a URL

One of the subtle features of the Netsweeper Policy Server is how Netsweeper *parses* or interprets a URL. By understanding the parsing, you can minimize the number of entries and provide extremely accurate filtering.

Review and consider URLs carefully before adding or modifying them to ensure you accomplish the outcome you want.

The format of a URL is: *protocol://host/path*

The Netsweeper Policy Server breaks the host and path into individual segments. The host may also contain user name credentials or an optional port number.

The format is:

```
protocol://username@hostsegments:port/pathsegments
protocol:// - typically http://
```

Term	Description
host or host segments	Host or host segments start after the protocol, or after the @ if user name credentials are present. Processing stops at /, ?, and #. The entire host is always converted to lower case. The host is parsed into host segments by the . (period) character. Sequential periods are treated as a single period. The number of host segments in a URL string cannot exceed 5000 - if more are found they are not used during assembly. Host segments cannot be empty (for example: www..com is invalid). If the host segments form an IP address the Host is an IP category is assigned.
Port	The port starts after the colon (:) in the host and must be numeric. • If the protocol is http and the port is 80, the port is removed. • If the protocol is https and the port is 443, the port is removed.
path or path segments	The path starts after the host and stops when the question mark (?), number sign (#_, or the end of the entry occurs. Paths are broken into path segments by slash (/) characters. There can only be 5,000 path segments. If additional path segments exist, they are not used.

How Netsweeper Processes the Lists

From the validation sequence the entry is broken down into small, unique tokens, used during the processing stage.

The asterisk (*) in these examples represents a wild card that matches any character or string of characters or no character at all (empty string) and is case insensitive.

When no path or port is specified, Netsweeper assigns a wild card to the beginning and ending of the URL entry. See examples below.

Note *Only the path segment of a URL is case sensitive. Searches for keywords are NOT case sensitive.*

URL	Translation
http://com	http://*.com/*
http://tv.com	http://*.tv.com/*
http://www.tv.com	http://*.www.tv.com/*
http://www.TV.com	http://*.www.tv.com/*

When a port is specified, only the end of the URL will have a wild card. However, if the HTTP protocol is used and port 80 is specified, or the HTTPS protocol is used and port 443 is specified, the port is removed. See examples below:

URL	Translation
http://example.com:80	http://*.example.com/*
http://example.com:81	http://example.com:81/*
http://www.tv.com:100	http://www.tv.com:100/*

When a path is specified only the end of the URL has a wild card. See examples below.

URL	Translation
http://tv.com/comedy	http://tv.com/comedy/*
http://Test1.example.com:80/One/TWO	http://test1.example.com/One/TWO/*

The following illustrate some common issues with the URL lists:

URL	Translation
http://www..com/	http://*.www.com/*
http://joe@tv.com:80/joe?smith	http://tv.com/joe/*
http://happy.com/bob/joe	http://happy.com/bob/joe/*
http://Test.com/path/to/#/file	http://test.com/path/to/*

Creating URL Lists

A common error is to include many URLs in a list when a single one would do. Categorizing an entire host/domain generally provides the best results, and automatically allows for additional pages that may be added in the future. Although the time needed to process a single URL in an allow/deny list is very small, it may become significant if you have thousands of unnecessary URLs that get processed for every URL request.

Rather than adding multiple variations of tv.com which are individual pages, the host/domain tv.com should be added. Before adding any URL that is more than just the host/domain, investigate whether you can just categorize the host/domain.

Some hosts/domains, such as Geocities, host a variety of content and to categorize geocities.com as a pornography site would be inaccurate. However, there are plenty of pornography sites at Geocities. In these cases, consider the shortest URL that you can define to accurately categorize the site you are concerned about. Since paths are case sensitive, every attempt should be made to categorize without a path segment.

In addition, you may want to consider adding to your allow list top level domains that you trust. For example, domain registration for .edu and .gov are generally highly controlled and could in most cases be considered safe and globally allowed.

Another issue to consider is how often you review and purge your allow/deny lists. In many cases, undesirable URLs (pornography, racial, violence, and so on) move or change on a monthly basis. Having an allow/deny list full of dead sites is inefficient.

Adding a URL to a URL Lists

Netsweeper allows a URL on the Allow List *unless* a list with higher priority overrides it. Netsweeper always denies a URL on the Deny List *unless* a list with higher priority overrides it. Only use the Deny Page Allow URL List for files added to a Custom Deny Page.

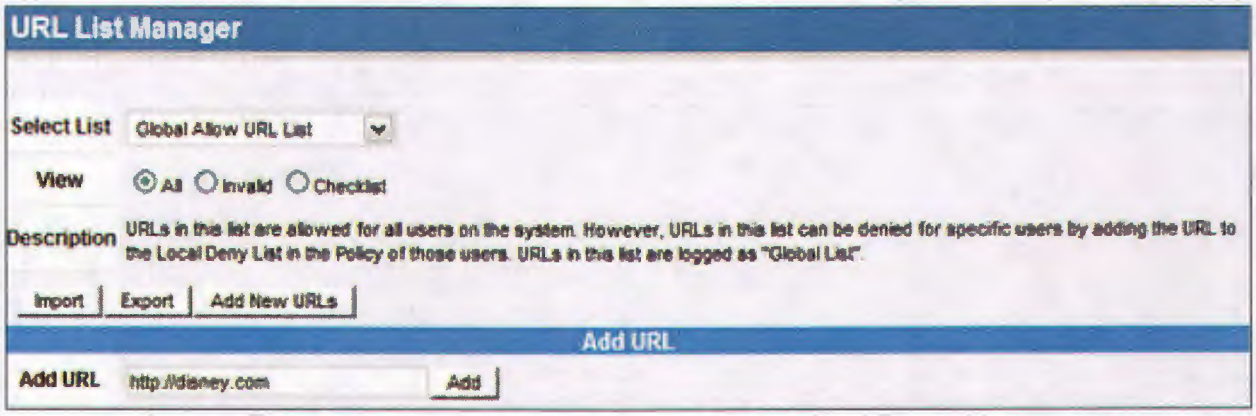


Figure 90: URL List Manager

To add a URL to one of the URL lists:

1. In the WebAdmin, select **URL List Manager** from the **URL Tools** menu.
2. Select the list to which you want to add the URL from the **Select List** menu.
3. To add a single URL, type in the URL in the **Add URL** box and then click **Add**.

   To add several URLs at once, click **Add New URLs**, type in one URL per line in the **Add New URLs** box, and then click **Submit**.
4. Click **Apply Settings** on WebAdmin task bar in the top right corner of the page and then click **Apply**.

Note Search the URL lists by typing in a keyword or a source URL in single quotes.

Importing a URL list

If you have a list of URLs that you want to add to a specific list in the URL List Manager, you can import a file. You can import either a text file or a CSV file. The file must have at least two columns: the URLs and the list you want to add them to, and each row must be either comma or tab delimited. If you have more columns, you can choose to ignore them.

To import a URL list:

1. In the WebAdmin, click **URL Tools** on the WebAdmin menu bar and select **URL List Manager** from the drop-down list.
2. Click **Import**.
3. If there are no headings in the file, clear the checkbox beside **Headings**.
4. Select how the fields are delimited. You can choose to replace all the existing data from the list.
5. Click **Browse** and find the file you want to open. Select the file and then click **Open**.
6. Click **Import**.
7. Identify which columns in your file are URLs and which are lists. Ignore the rest of the fields.
8. Click **Submit**.
9. Click **Apply Settings** from the WebAdmin task bar in the top right corner of the page and then click **Apply**.

Note *Place each custom URL list in a separate file and upload it individually in the URL List Manager.*

Each list has a corresponding keyword that you must include in the file. The list of keywords is shown below.

Table 14 Keywords for uploading URL lists

List	Keywords
Allow URL List	suggest_allow
Global Deny URL List	suggest_deny
System Allow URL List	system_allow
System Deny URL List	system_deny
System Allow Protocol List	systemproto_allow
System Deny Protocol List	systemproto_deny
Deny Page Allow URL List	deny_allow

Example

- "Global URLs","List"
- "http://facebook.com","suggest_deny"
- "http://google.ca","suggest_allow"
- "http://netsweeper.com","suggest_allow"

Adding URLs or Words to the Allow or Deny Lists

You will use the Local URL List and Keyword List to always allow or deny a URL for a particular policy. Only users assigned to that policy's group, during times when the policy is active, will be affected. Both URLs and keywords can be type ined in this list. You must include the http:// or https:// included at the beginning of the URL; otherwise, the URL will be treated as keywords.

Keywords are a special case. They are a string of characters that can appear anywhere within a URL. For example, adding "sex" to the Local Deny List would block access to sites like http://www.sex.com, http://www.middlesex.com, and http://www.sussex.co.uk. As you can see from this example, it is important to be very careful when using keywords.

To add a URL or a keyword:

1. In the WebAdmin, select **Group Manager** from the **Policy Management** menu.
2. Select the name of the group with the policy you want to modify.
3. Select the name of the policy you want to modify.
4. **Click Local Allow URLs/Keywords or Local Deny URLs/Keywords** from the **Local List** menu, depending on whether you want to allow or deny the site for users of this policy.
5. Type in the URL or keyword in the **Add Entry** box and then click **Add**.
6. Click **Apply Settings** on the WebAdmin task bar in the top right corner of the page and then click **Apply**.

Note *Select the encode box if you type in any non-alphanumeric characters.*

Importing URL Lists

To import a list of URLs for the **Local Allow** and **Local Deny** lists, follow the procedure described in **Importing a List**. However in this case, the entries for the **Local Allow** and **Local Deny** lists can go in the same file. Additionally, the keywords for the **Local Allow** and the **Local Deny** lists, respectively, are 1 and 2.

The **Checklist Report** will categorize all websites type ined in the **Local List**. This function allows *admins* and *sysops* to verify the **Local Allow** and **Local Deny** lists.

Creating URL Alerts

The **URL Alert** tool allows administrators, *sysops* and users to prompt Netsweeper to check the accuracy of a URL's categorization.

To submit a URL Alert:

1. Type in one or more URLs you feel are inaccurately categorized.
2. Click **Submit**.

   Your message is sent via email to the Netsweeper Review Team, which will review the URL and make a decision as to the validity of your request.

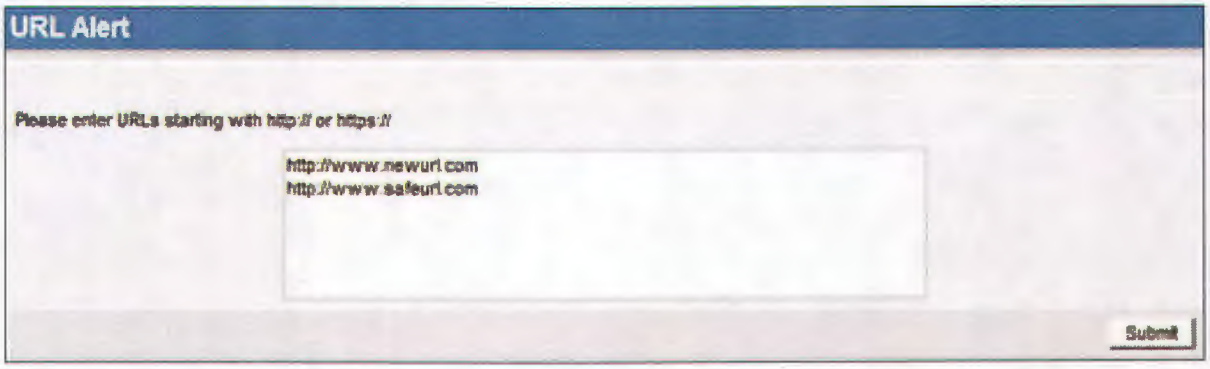


Figure *91*: URL Alert

Using the Web Proxy

By using the Web Proxy, you can test the filtering policies for each group you create by assuming the identity of a group member and then browsing the Internet under the group's policy.

To use the Web Proxy to test a filtering policy:

1. Select **Web Proxy** from the **System Tools** menu.
2. Select the group whose policy you want to test.
3. Click **Surf As**.
4. Browse to filtered URLs or protocols.

Note *You can also click **Surf using group** when you are looking at a group, or surf using policy when you are looking at an individual policy.*

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

Figure 92: URL for Web Proxy

Using the 'Your Account' Tools

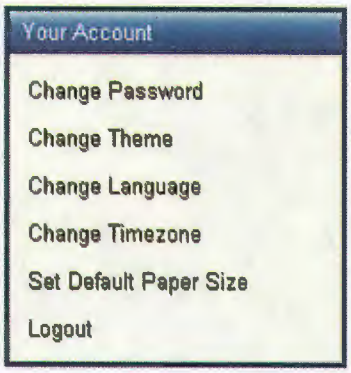


Figure 93 Your Account menu

Table 15 Your Account Menu Options

Your Account Menu Options	Function
Change Password	Changes your account password
Change Theme	Changes the WebAdmin interface
Change Language	Changes the language in which the WebAdmin displays
Change Time Zone	Changes the time zone of the WebAdmin
Set Default Paper Size	Changes the default paper size for printout of logs or reports

Changing your Password

To change your password:

1. Select **Change Password** from the **Your Account** menu.
2. Type the new password in the **New Password** and **New Password Again** boxes.
3. Click **Submit**.
4. Click **Apply Settings** on the WebAdmin task bar in the top right corner of the page and then click **Apply**.

Changing your Theme (User Interface)

The instructions for using the **WebAdmin** vary, depending on which user interface you choose from among the nine different **Themes** available to you. After logging in to the **WebAdmin**, you can apply a theme locally, to one account, or, if you are a *admin* or *sysop* user, you can apply it globally, to all accounts under your control.

The instructions contained in this guide apply to the three newest themes – **Business**, **School**, **SMB** – which feature a nine-button menu bar, a three-button **Quick Links** bar, a three-button WebAdmin task bar, and a link to Netsweeper Technical Support at the bottom of the page. We would recommend that you choose one of these three themes for best compatibility with our documentation.

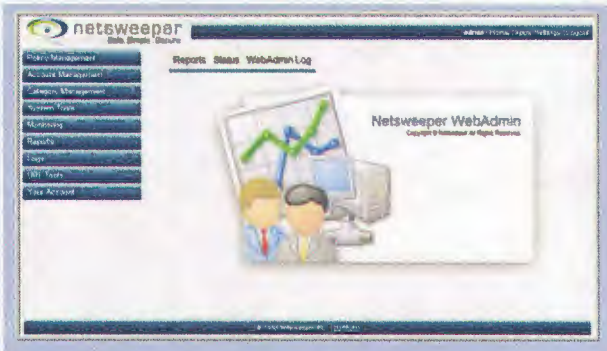
Figure 94 WebAdmin Home Page, Business Theme

Choosing a Theme

To choose a theme:

1. Click **Your Account** on the WebAdmin menu bar.
2. Select **Change Theme** from the **Your Account** drop-down list.
3. Select the theme you want from the **Account Theme** and **Global Themes** drop-down lists.
4. Click **Submit**.
5. Click **Logout**.
6. Log back on to the WebAdmin.

Available Account and Global Themes (User Interfaces)



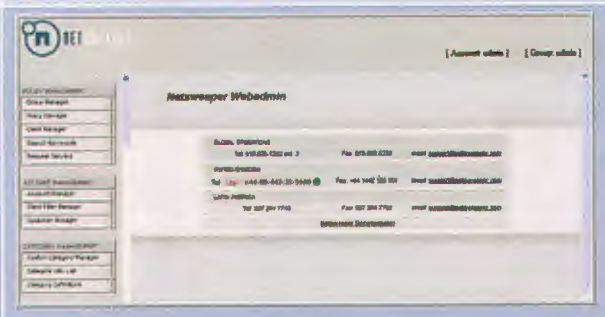
Business

School

SMB

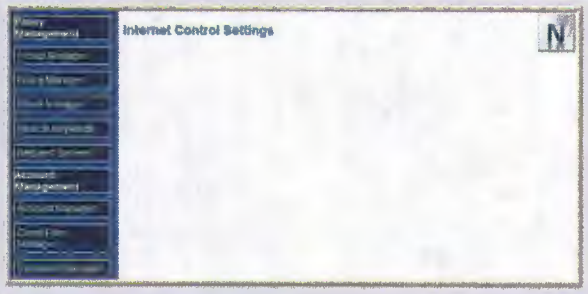
ISP

Default



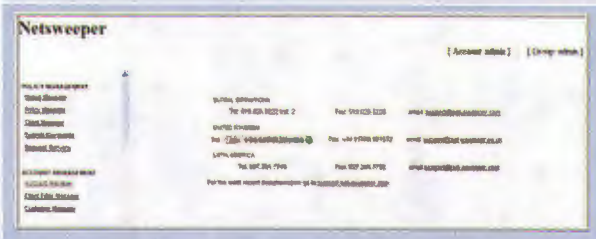
Classic

Available Account and Global Themes (User Interfaces)



Light

Client Filter



Default (Old)

To change your theme (user interface):

1. Select **Change Theme** from the **Your Account** menu.
2. You now have a choice:
   - To change the theme for the *admin* account only, select a theme from the options in the **Account Theme** dropdown list and then click **Submit**.
   - To change the theme for all accounts on the WebAdmin, select a theme from the options in the **Global Theme** dropdown list and then click **Submit**.

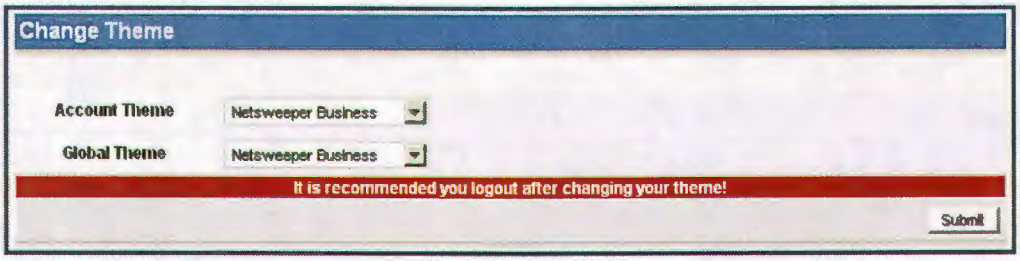


Figure 95 Change Theme page

3. Click **Apply Settings** on the WebAdmin task bar in the top right corner of the page and then click **Apply**.
4. Log out of the WebAdmin and then log on again.

Changing the WebAdmin Display Language[13]

To change the WebAdmin display language:

1. In the WebAdmin, select **Change Language** from the **Your Account** menu.
2. Select a language icon under **Global Language** if you want to change the language globally (for all accounts assigned to your administrative control),

   or

   Select a language icon under **Account Language** if you want to change the display language for your account.

Figure 96 Change Language page

Changing the WebAdmin Time Zone

To change the WebAdmin time zone:

1. Select **Change Time Zone** from the **Your Account** menu.
2. Select a time zone from the dropdown list and then click **Submit**.
3. Click Apply Settings on the WebAdmin task bar in the top right corner of the page and then click Apply.

Figure 97 Change Time zone page

[13] The WebAdmin is available in other languages besides French and English by request.

Figure 98 Time zone list

Setting the Default Paper Size for Printing

To set the default paper size for printing from the WebAdmin:

1. Select **Set Default Paper Size** from the **Your Account** menu.
2. Click the arrow for the drop down list beside **Account Default Paper Size** and select a paper size from the list.

   The options are: letter, legal, A3, A4, and A5.
3. Click **Submit**.
4. Click **Apply Settings** on the WebAdmin task bar in the top right corner of the page and then click **Apply**.

Logging Out

To log out of the WebAdmin, select **Logout** from the **Your Account** menu, or click **Logout** on the taskbar.

Deploying the Client Filters

This document describes deployment methods for the two client filter editions.

- Large organizations should use the Client Filter Enterprise Edition, in which a group of *admins* and *sysops* manage group filtering "policies" through a Web-based interface, called the WebAdmin. The organization's Active Directory or other authentication system validates Netsweeper users and assigns them to filtering groups.
- Small organizations and home users should use the Client Filter Residential Edition, in which a person designated as a profile manager creates filtering "profiles" for users and assigns each a profile and a password.

Differences between the Two Client Filter Editions

Method	Large-Scale (Enterprise)	Small-Scale (Residential)
Who manages the filtering?	Master *admin*, *admins*, and *sysops*	An *admin* or *sysop* creates up an account for the organization through the WebAdmin, and then a person in that organization uses the client filter's Profile Manager to create profiles for each of the organization's filtered users.
How do they do it?	Web-based WebAdmin software	Profile Manager software installed on each PC
What is filtered?	Groups are filtered according to the dictates of their filtering policy.	Profiles are filtered, perhaps individually, according to the dictates of their profile.
What else?	Focuses on efficient management of large groups of users	Focuses on simplicity and ease of use and hides complex features
Procedure	1. *Admins* or *sysops* create groups, policies, time segments, and assign clients to groups. 2. Deploy the Netsweeper client filters to individual computers. See the *WebAdmin Guide* for details.	1. An *admin* or *sysop*, using the WebAdmin, creates an account for the small organization or family. 2. Then the small business or home user can log in with the first time log in and set up the account. See the *Protection Pack User Guide* for details.

Organizing Filtering Profiles or Policies

After your IT team installs and configures the Netsweeper operating system (covered in the Netsweeper Server Setup Guide) to work with your authentication system, those *admins* and *sysops* handling policy creation and administration determine whether to deploy the Client Filter Residential Edition or the Client Filter Enterprise Edition.

Residential Edition or Enterprise Edition?

The Netsweeper Client Filter has two formats: Residential Edition and Enterprise Edition. If you are a large service provider, you may prefer to use the Client Filter Residential Edition with your smaller customer accounts and the Client Filter Enterprise Edition with your larger customer accounts. You can deploy both editions from the same server.

Residential Edition	Enterprise Edition
Service providers often deploy the Netsweeper Client Filter Residential Edition for distribution to families, schools, or small- to medium-sized businesses that want simple, easy-to-manage filtering, logging, and reporting for a small number of users. The Profile Manager has a simple user interface that allows a customer *admin* or parent (in the case of a family) to create basic filtering profiles as well as simple logs and reports. Account authorization is by account username and password. User authorization is by profile name and optional password.	Service providers, businesses, governments, and schools usually deploy the Netsweeper Client Filter Enterprise Edition when they need a tool that allows them to centrally deploy the filter to a large network of computers and users and efficiently manage content filtering for those users. In this edition, only *admins* or *sysops* have access to the management interface, the WebAdmin software. When individuals use the Client Filter Enterprise Edition, their Netsweeper user name is identical to their Windows user name. *Admins* or *sysops* can either type each Windows user name into the WebAdmin or use our Active Directory Sync tool, available from Netsweeper Support.

Residential Edition vs. Enterprise Edition

Residential Edition	Enterprise Edition
To deploy the Client Filter Residential Edition:	To deploy the Client Filter Enterprise Edition:
1. The service provider-level *admin* or *sysop* fine tunes any default filtering profiles for the user base, using the Policy Management tools.	1. The policy *admins* and *sysops* group users into affinity groups by their filtering needs. They may configure their authentication system to automatically route users into their affinity groups.
2. The service provider-level *admin* or *sysop* uses the Account Management tools in the WebAdmin to create an account name and password for each of the service provider's business, school, or family customers.	2. The *admin* or *sysop* creates at least one filtering policy per affinity group.
3. The customer uses that account name (generally an email address) and password to download the client filter Profile Manager onto his/her organization's computers.	3. If a group has multiple policies, governing different times or days, then the *admin* or *sysop* applies time segments to each of the group's policies.
4. The customer *admin* or parent then uses the Profile Manager to create the filtering profiles that he/she will use in managing filtering under that account.	4. The *admin* or *sysop* modifies each policy, tweaking the Allow and Deny lists, URL and protocol lists, Search Keywords, and other policy details as needed.
5. The customer *admin* or parent uses the Profile Manager to modify the default profiles, if needed.	5. The *admin* or *sysop* creates simple or complex reports for monitoring users' Internet activity.
6. The customer *admin* or parent creates simple reports to monitor profile users' Internet activity.	6. The *admin* or *sysop* tests the policies and reports.

Deploying the MSI version of the Client Filter

If you are deploying the Microsoft Installer (MSI) version of the product, you can use Microsoft's tools to transform your packages and silently deploy the client filter.

Adding Multiple Clients

After you have deployed the client filters, you will add clients to the various group Policies. The only difference between a *single-client* software deployment and a *multiple-client* software deployment is that the client names will need to have the "@company[x].company.com" domain appended to their names in a multiple-client deployment.

This will also allow you to use the same usernames across the system.

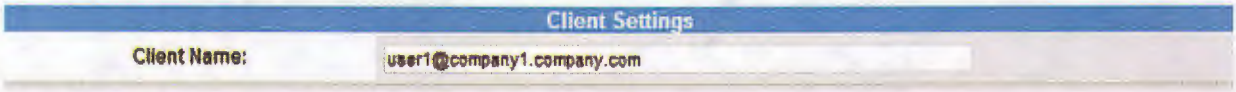


Figure 99 Client Settings window with append to usernames

Filtering Multiple Organizations

Internet Service Providers (ISPs) can manage filtering for a number of customer businesses or organizations from the same Netsweeper Policy Server. This chapter describes how an ISP would configure this arrangement.

Task Summary

To support multiple companies on the same Policy Server:

1. Create a DNS[14] entry in your DNS server configuration for each company for which you are deploying Netsweeper.
2. Test your DNS entries by using the *ping* command.
3. Configure the Netsweeper Policy Server to manage all of the companies.
4. Create users, groups, policies and time segments for each company.
5. Deploy the Netsweeper client filters to each company's computers.

Creating a DNS Entry for Each Company

Create a Berkeley Internet Name Domain (BIND) configuration to make company1, company2, and company3 respond to the Netsweeper Policy Server's IP address.

An example BIND configuration:

```
$TTL 3D

@ IN SOA ns1.company.com. support.company.com.(
      2007121121 ; serial, todays date + todays serial #
      3600 ; refresh, seconds
      3600 ; retry, seconds
      3600 ; expire, seconds
      3600 ); minimum, seconds
      NS ns1.company.com.
      NS ns2.company.com.
      MX    10 mail.company.com.
@           IN    A      192.168.1.1
company1    IN    A      192.168.1.2
company2    IN    A      192.168.1.2
company3    IN    A      192.168.1.2
```

[14] Domain Name Server

Note *Replace the IP address 192.168.1.2 in the example above with the external IP address of your Netsweeper Policy Server.*

Testing the DNS changes

After you make the changes in your DNS, test your changes by using the *ping* command. (Ensure that neither your firewall nor the Netsweeper Policy Server is blocking the *ping*.)

To test the DNS, type in:

```
# ping company1.company.com
```

The result of the *ping* should be similar to this:

```
Pinging company1.company.com [192.168.1.2] with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time=7ms TTL=245
Reply from 192.168.1.2: bytes=32 time=6ms TTL=245
Reply from 192.168.1.2: bytes=32 time=8ms TTL=245
Ping statistics for 192.168.1.2:
Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 6ms, Maximum = 8ms, Average = 7ms
```

Filtering More than One Organization

Edit the */usr/local/netsweeper/etc/nsd.conf* file using *nano*, a free curses-based text editor.

To edit the */usr/local/netsweeper/etc/nsd.conf* file:

1. Type in the line below:

   ```
   # nano -w /usr/local/netsweeper/etc/nsd.conf
   ```

2. At the end of the configuration file, add the following line:

   ```
   rus_append policyserver
   ```

3. Save the file and restart the policy server.

   ```
   # nsdctl restart
   ```

Deploying the MSI version of the Client Filter

If you are deploying the MSI version of the product, you can transform your packages and silently deploy the client filter.

Deploying the Executable Version of the Client Filter

If you are deploying the executable version of the client filter software, type in the following command to specify which Netsweeper Policy Server to use:

```
setup.exe /POLICY_SERVER=company1.company.com:3431 /S
```

Adding Multiple Clients

After you have deployed the client filters, you will add clients to the various group Policies. The only difference between a *single-client* software deployment and a *multiple-client* software deployment is that the client names will also need to have the "@company[x].company.com" domain appended to their names.

This will also allow you to use the same usernames across the system.

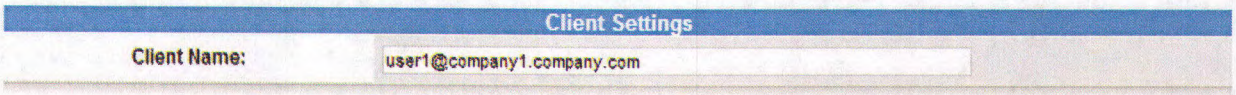
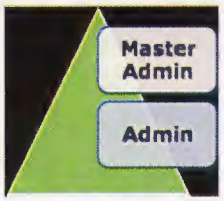


Figure 100 Client Settings window with append to usernames



Duties of the Master Admin

The Netsweeper *master admin* in a large or geographically dispersed organization may choose to share administration of the Netsweeper system with other technically trained *admins* and delegate some tasks to *system operators* or *sysops*. These *sysops* will share some, but not all, of the privileges of the Netsweeper *admins*. The *master admin*istrator will determine what privileges and duties the *sysops* have.

See the **Netsweeper Sysop Guide** for ideas about delegating the Netsweeper administrative duties among *admins* and *sysops*.

The level of access you have to the WebAdmin depends on the type of WebAdmin Login account you have. There are four types of WebAdmin Login accounts:

Login Type	Description
Master *admin*	The *master admin* account is a special, built-in account designed for the head Netsweeper Server administrator. Typically, this is the person in charge of maintaining the server and managing the accounts of other administrators. This account has access to all the features that a regular administrator has, plus a few extra system settings.
Admin	The *admin* account is for administrators who manage one or more groups of users. These accounts have access to all of the Netsweeper Reporter's features and can report on all users, but cannot access any of the System Configuration settings, including the Reporter Settings.
Sysop	The *sysop* account is for assistant administrators who have restricted access to administrative features. The level of access that *sysops* have on the system depends on the individual *sysop* permission settings. Sysops can only report on groups and clients assigned to their account. Sysop permissions can only be modified by an Admin or Master Admin. For more information on *sysop* permissions, see the Sysop Permissions Guide on the support site at http://support.netsweeper.com.
User	In most Netsweeper deployments, user accounts have no direct access to the WebAdmin. Users can only access their own account.

Creating an Admin Account

To create an *admin* account:

In the WebAdmin, select **Account Manager** from the **Account Management** menu.

1. Click **Add New Account**.

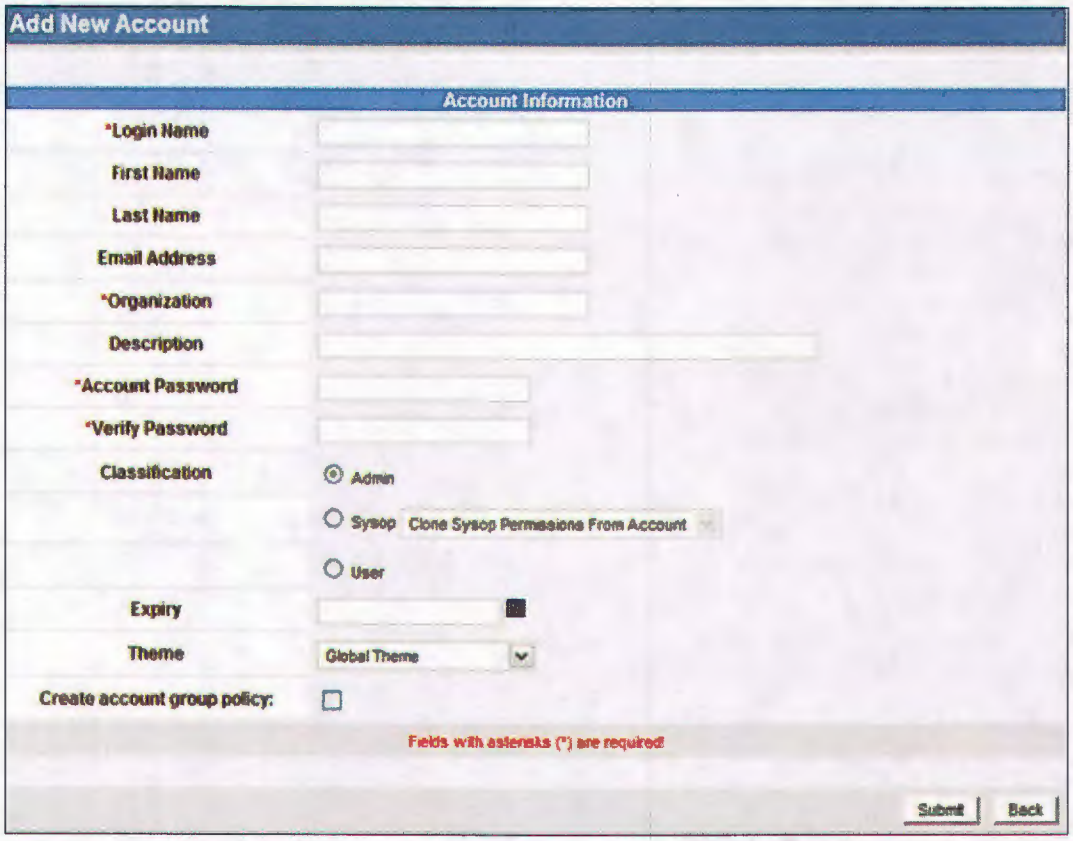


Figure 101: Add New Account page

2. Type in the **Login Name**, **Organization**, and **Account Password**. Type the password again in the **Verify Password** box.
3. Click **Admin** in the **Classification** field.
4. If you click **Create account group policy**, a group and policy will be created for this account. The *admin* user will join the group as a client and be filtered.
5. Click **Submit**.
6. Click **Apply Settings** on the WebAdmin task bar in the top right corner of the page and then click **Apply**.