



Netsweeper User Acceptance Document 8.2

Netsweeper Inc. Corporate Headquarters

180 Northfield Dr W.

Unit 4, 1st floor.

Waterloo, ON, Canada N2L 3K8

T: +1 (519) 772-0889

F: +1 (519) 772-0896

support@netsweeper.com

© 2024 Netsweeper Inc.

All rights reserved.

Every effort has been made to ensure the accuracy of this document. However, Netsweeper Inc. makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability and fitness for a particular purpose. Netsweeper Inc. shall not be liable for any error or for incidental or consequential damages in connection with the furnishing, performance, or use of this document or the examples herein. The information in this documentation is subject to change without notice.

Netsweeper and Netsweeper Inc. are trademarks or registered trademarks of Netsweeper Incorporated in Canada and/or in other countries. Other product names mentioned in this document may be trademarks or registered trademarks of their respective companies and are the sole property of their respective manufacturers.

Contents



netsweeper

.....	1
Netsweeper User Acceptance Document 8.2	1
Netsweeper User Acceptance Document	4
About the Resource Page	4
Filtering for the Test Workstation	4
NSProxy Certificate Installation on the Test workstation.....	4
Importing a Certificate	5
Preconditions – Setup Filtering Group and Client	6
Creating a Group ‘testgroup’	6
Create a Client ‘testclient’	7
Create a Policy ‘testpolicy’	8
Create a Simple Group ‘testgroup2’	9
Monitoring.....	10
Test Procedure: Monitoring.....	10
Notes	10
Enabling Reports Fields in the WebAdmin Settings.....	12
Testing Local Lists	13
Test Procedure: Local Lists	13
Request Logs Advanced Filters	15
Domain Filter	20
Test Procedure: Domain Filter.....	20
Deny Specific Category.....	22
Category Templates.....	25
Test Procedure: Deny Specific Category	25
Time Based Policies: Using Policy Events.....	28
Test Procedure: Policy Events	28
Lists Window.....	36
System Deny List	36
Importing a System List.....	42
Additional Precondition 1: Adding a Test List	42

Additional Precondition 2: Creating a URL Import List	42
Test Procedure: Importing a System List	43
Clients	45
Clients Identified by Subnet.....	45
Accounts Window	48
SysOp Permissions	48
Delegated Administration	51
Test Procedure: Delegated Administration.....	51
Categories	53
Creating and Using Custom Categories.....	53
Policies and Categories	59
Allow Selected Categories – Allow Policy.....	59
Category Lookup	61
CNS Categorization.....	61
List Update.....	63
Test Procedure: List Update.....	63
Centralized Management	64
Testing Connections and Access	66
Verify SSH Login.....	66
Boundary Tests.....	67
URL List Import Limit.....	67
Request Loggin and Reporting.....	69
Creating a Detailed Demand Report.....	69
Creating a Summary Demand Report	73
HTTPS Filtering Tests.....	76
HTTPS Filtering at Domain Level	76
Document Sign-off	77
Acceptance Test Approval	77
Acceptance Tests Passed	77

Netsweeper User Acceptance Document

About the Resource Page

Certain files and other resources can be found at this resource page.

https://helpdesk.netsweeper.com/docs/main_page/Content/Main_Page/User_Acceptance_Documents.htm

Filtering for the Test Workstation

The Netsweeper solution must be deployed so that it can route RST packets to both the filtered workstation and the web server.

- Specific UDP ports must be able to communicate to the central WebAdmin (UDP 3161).
- In the 8.2 default install, NSProxy is enabled.
- This document assumes that NSProxy is enabled.

NSProxy Certificate Installation on the Test workstation

On your test workstation, setup the proxy in your browser. Use the IP of your Policy Server and the port 31280.

Edit proxy server

Use a proxy server

☒ On

Proxy IP address	Port
192.168.1.xxx	31280

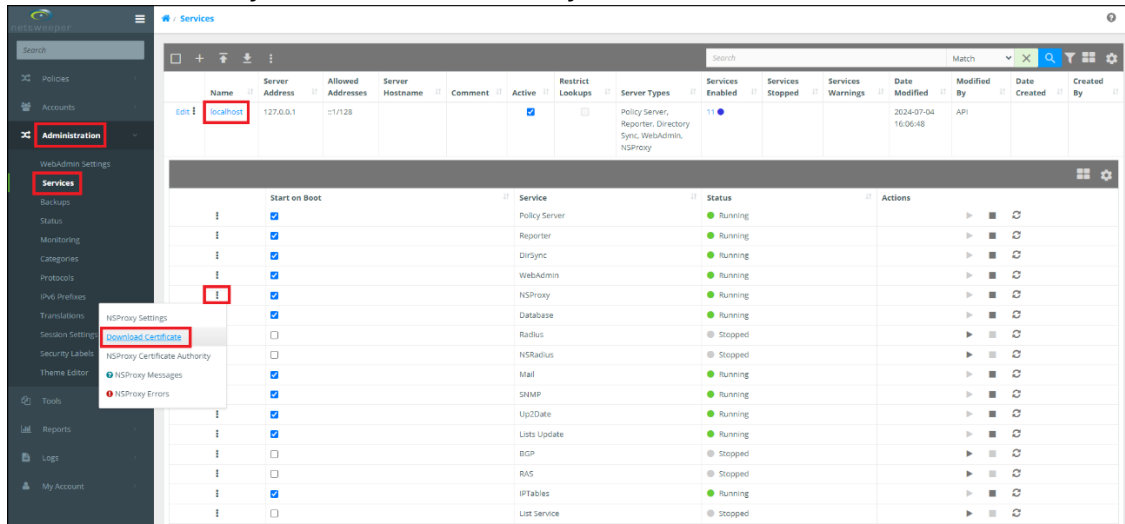
Use the proxy server except for addresses that start with the following entries.
Use semicolons (;) to separate entries.

☐ Don't use the proxy server for local (intranet) addresses

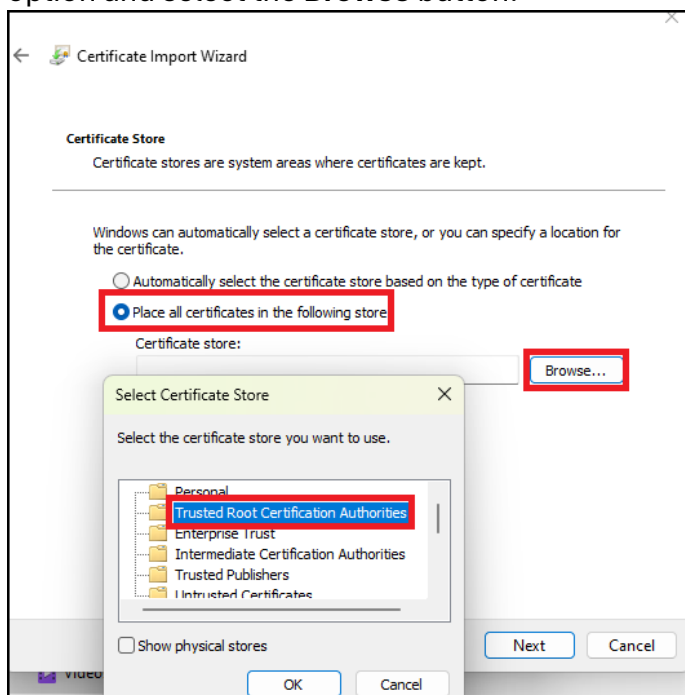
Save Cancel

Importing a Certificate

1. In the WebAdmin, navigate to Administration > Services.
2. Expand the 'localhost' to display the Server Management options.
3. In the 'NSProxy' section, choose the **Download Certificate** button. The certificate is downloaded to your download directory.



4. Copy the certificate to your test workstation.
5. In test workstation, double-click on the newly downloaded certificate.
6. Select **Install Certificate** and follow the steps in the Certificate Import Wizard.
7. On the Certificate Store step, choose the 'Place all certificates in the following store' option and select the **Browse** button.



8. Continue to follow the steps in the wizard to install the certificate as a Root CA.

Preconditions – Setup Filtering Group and Client

As a precondition of some of the procedures in the is document, a filtered Client workstation must be available for generating traffic and be assigned to a known Group and Client. You will need to assign the IP of your test workstation to your Client. The testgroup group must only have one group default policy.

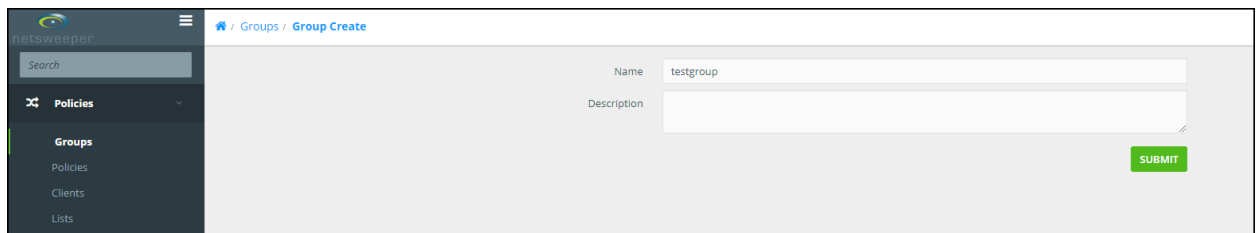
The Precondition section will:

- Create a Group ‘testgroup’
- Create a Client ‘testclient’
- Create a Policy ‘testPolicy’
- Create a Simple Group ‘TestGroup2’

This document will assume that this section is completed as part of the precondition

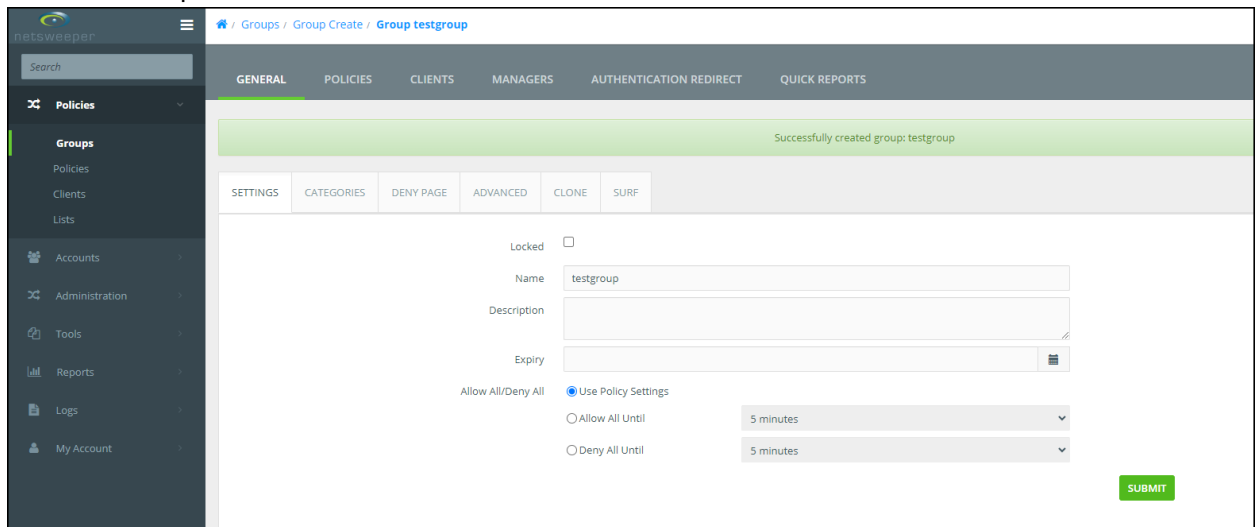
Creating a Group ‘testgroup’

1. In the WebAdmin, navigate to Policies > Groups and choose the **List** tab.
2. In the Groups window, select the **Create** button.
3. In the ‘Group Create’ window, enter the name ‘testgroup; and select the **Submit** button.



The screenshot shows the 'Group Create' form in the Netsweeper WebAdmin. The left sidebar contains a search bar and a menu with 'Policies' (selected), 'Groups', 'Clients', and 'Lists'. The main content area has a breadcrumb 'Groups / Group Create' and a form with fields for 'Name' (containing 'testgroup') and 'Description'. A green 'SUBMIT' button is located at the bottom right of the form.

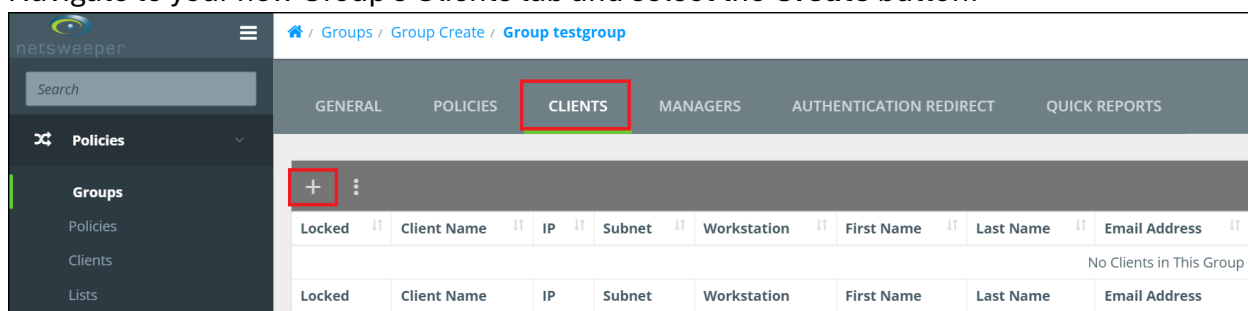
4. The new Group is created.



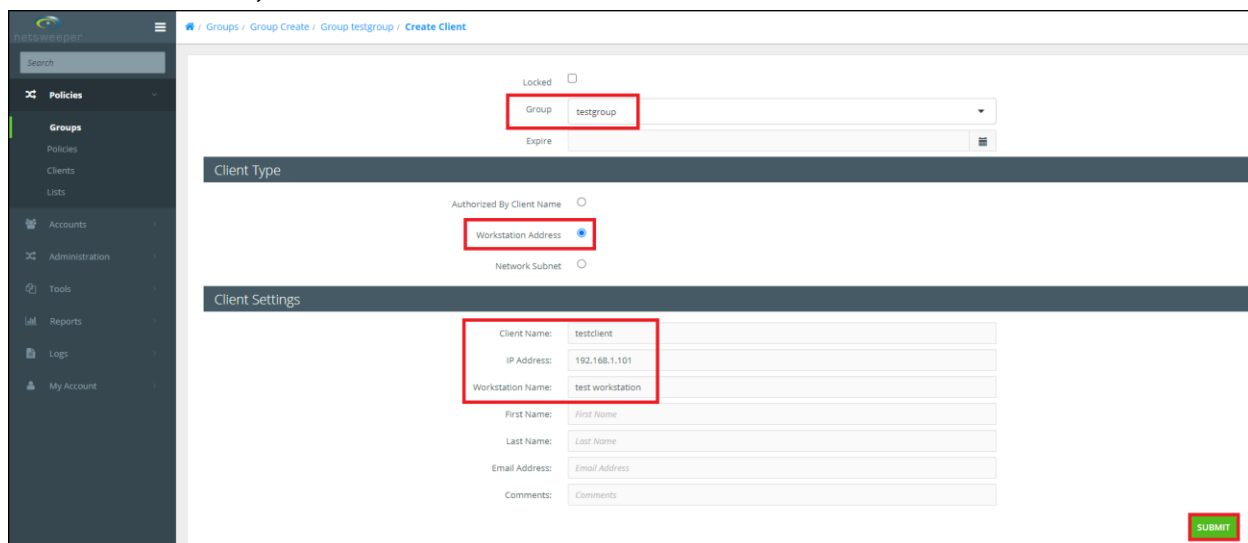
The screenshot shows the 'Group testgroup' configuration page in the Netsweeper WebAdmin. The left sidebar is the same as the previous screenshot. The main content area has a breadcrumb 'Groups / Group Create / Group testgroup' and a tabbed interface with 'GENERAL', 'POLICIES', 'CLIENTS', 'MANAGERS', 'AUTHENTICATION REDIRECT', and 'QUICK REPORTS'. The 'GENERAL' tab is active, showing a green success message 'Successfully created group: testgroup'. Below this are tabs for 'SETTINGS', 'CATEGORIES', 'DENY PAGE', 'ADVANCED', 'CLONE', and 'SURF'. The 'SETTINGS' tab is active, showing a form with fields for 'Name' (containing 'testgroup'), 'Description', and 'Expiry'. There is a 'Locked' checkbox and a 'Use Policy Settings' radio button. Below these are two rows of radio buttons for 'Allow All/Deny All' with dropdown menus for '5 minutes'. A green 'SUBMIT' button is at the bottom right.

Create a Client 'testclient'

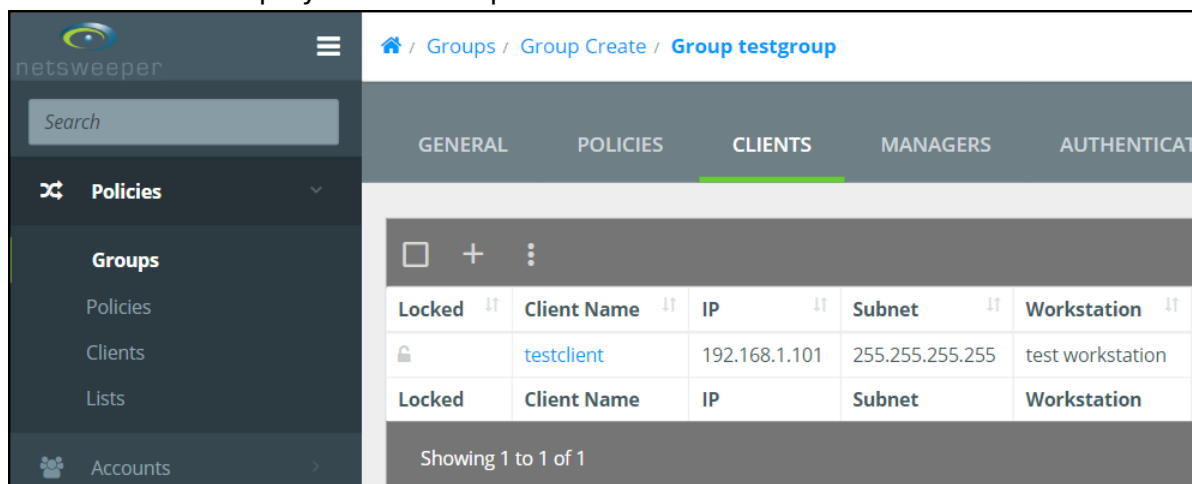
1. Navigate to your new Group's Clients tab and select the **Create** button.



2. In the 'Create Client' window, ensure that the new 'testgroup' is selected and choose the **Workstation Address** option within the 'Client Type' section.
3. Enter the Client Name 'testclient,' the IP address of your test workstation, and a workstation name, then select the **Submit** button.

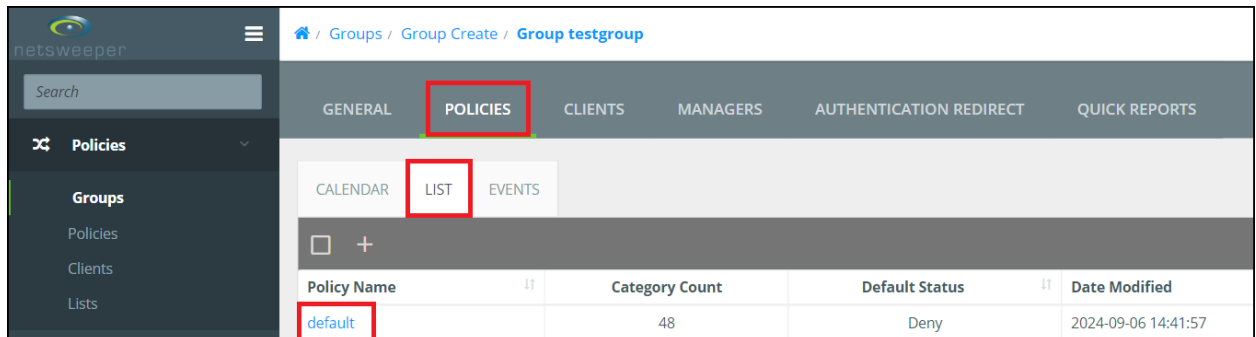


4. The new Client displays in the Group's Clients tab.



Create a Policy 'testpolicy'

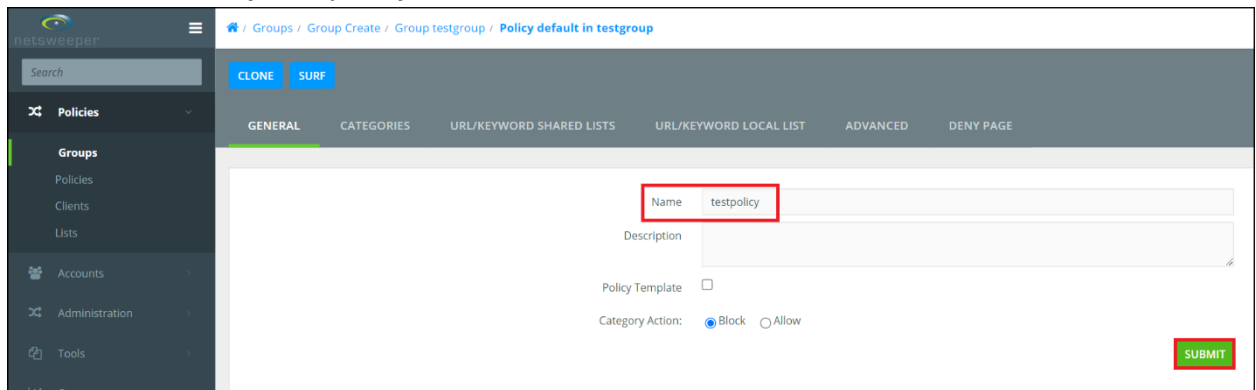
1. In your testgroup, navigate to the **Policies** tab and the **List** subtab.
2. Select the Default Policy.



The screenshot shows the Netsweeper interface with the 'Policies' tab selected. The 'LIST' subtab is active, displaying a table of policies. The 'default' policy is highlighted in the table.

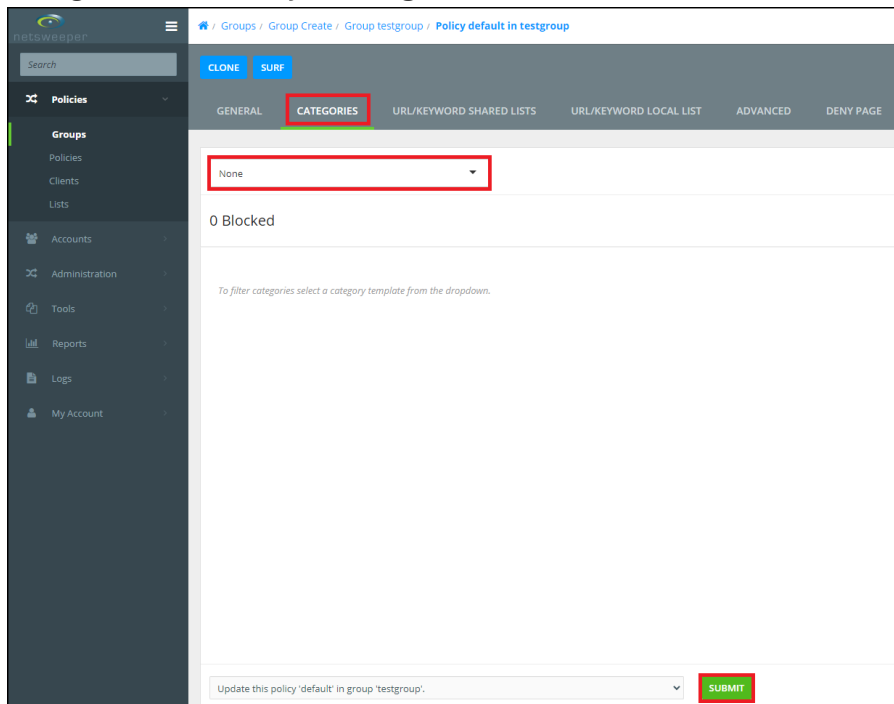
Policy Name	Category Count	Default Status	Date Modified
default	48	Deny	2024-09-06 14:41:57

3. Rename the Policy 'testpolicy' and select **Submit**.



The screenshot shows the Netsweeper interface with the 'Policy default in testgroup' page. The 'Name' field is set to 'testpolicy'. The 'SUBMIT' button is highlighted.

4. Navigate to the Policy's **Categories** tab and choose the **None** Category Template.

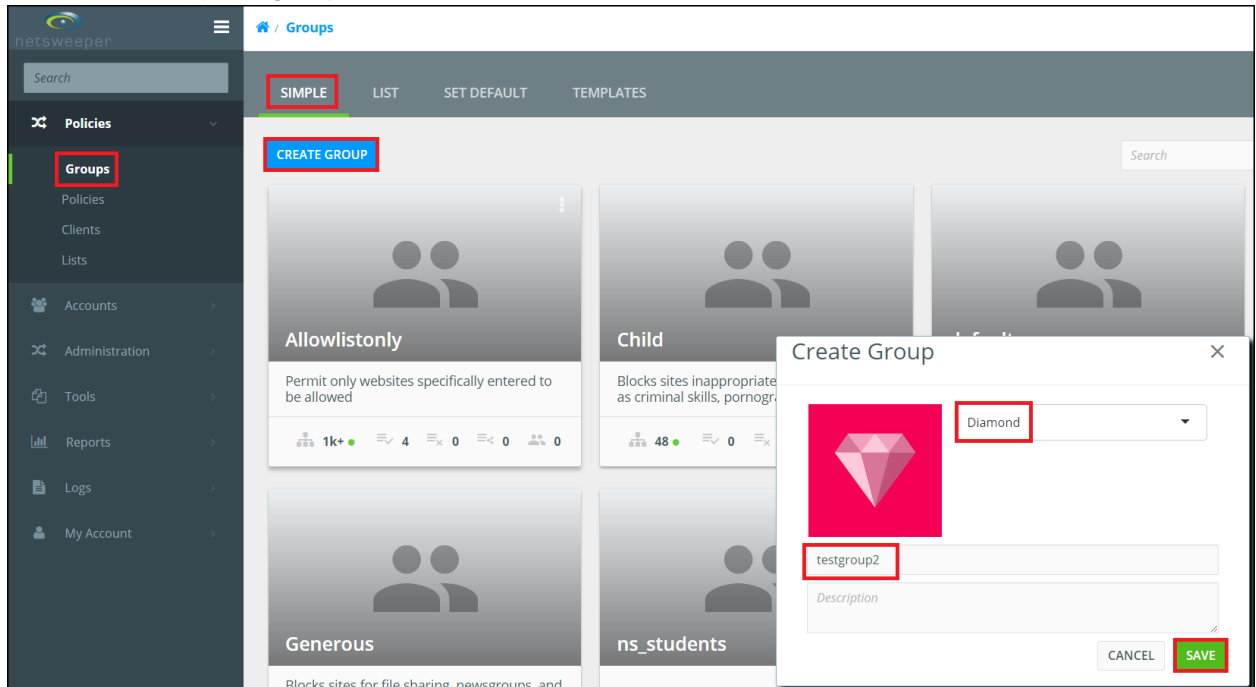


The screenshot shows the Netsweeper interface with the 'Policy default in testgroup' page. The 'CATEGORIES' tab is active. The 'None' category template is selected in the dropdown menu. The 'SUBMIT' button is highlighted.

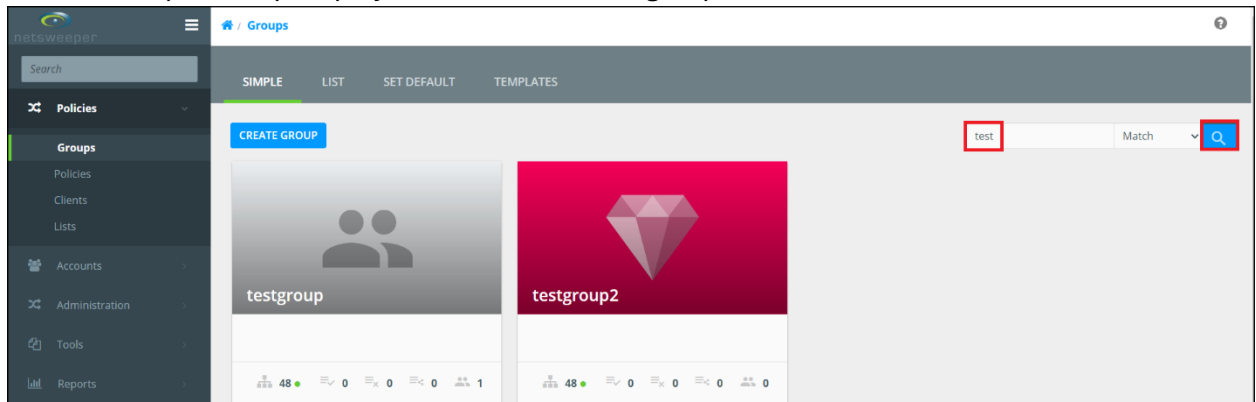
5. Select the **Submit** button to save your changes.

Create a Simple Group 'testgroup2'

1. Navigate to Policies > Groups and choose the **Simple** Tab.
2. Select the **Create Group** button.
3. In the Create Group window, choose the Diamond Icon.
4. Name the Group testgroup2 and select the **Save** button.



5. In the Simple tab, type 'test' in the Search field and select the Search button.
6. The new Simple Group displays, as well as the 'testgroup' created earlier.



7. We will use this Group later.

Monitoring

Purpose

Normal operation of the Netsweeper solution involves monitoring fundamental statistics on each server. Information such as Netsweeper Request per second, Netsweeper Cache, Netsweeper errors, etc..., are gathered over time and made available for analysis by the system administrator. The WebAdmin interface for the Netsweeper solution provides access to relevant system status information, providing average and maximum values over time. This test case will verify the correct operation of a portion of the Netsweeper filtering platform's monitoring capabilities.

Precondition

The Netsweeper solution must have been running and intercepting traffic for a period of at least 1 hour with testing taking place to generate allowed and denied request.

Test Procedure: Monitoring

1. In the WebAdmin, navigate to Administration > Monitoring.
2. Select Default Graphs: Memory Usage from the 'Graphs' dropdown list.

Pass Criteria

The monitoring graph will appear showing the Memory usage varying over the past hour.



Notes

There are hundreds of SNMP MiBs that can be viewed using the system monitoring page. We suggest testing these MiBs. MiB's that are outlined in the Netsweeper Configuration manuals. Each service that is documented in these manuals has a list of MiB's available.

SNMP MIBs in 8.2

Notes	
Results (Pass or Fail)	
Results Comments	

Enabling Reports Fields in the WebAdmin Settings

For the next test, we will be required to enable a Report Data Field.

1. Navigate to Administration > WebAdmin Settings
2. Scroll down to the **Reports Settings** section.
3. **Hold the <CTRL> key so as not to de-select all the other selected fields.**
4. Choose **Denied Category Numbers** from the 'Enabled Data Fields'.
5. Select the **Submit** button to save your changes.

The screenshot shows the Netsweeper WebAdmin interface. The left sidebar contains a search bar and a menu with categories: Policies, Accounts, Administration, Services, Backups, Status, Monitoring, Categories, Protocols, IPv6 Prefixes, Translations, Session Settings, Security Labels, and Theme Editor. Under 'Administration', 'WebAdmin Settings' is highlighted. The main content area is titled 'Report Settings' and contains various configuration options. The 'Enabled Data Fields' section is expanded, showing a list of fields: Denied Category Numbers, Denied Host, Destination IP Address, and Device Brand. The 'Denied Category Numbers' field is selected. Other sections include 'Enabled Report Filter Fields', 'Enabled Template Filter Fields', 'Enabled Quick Report Intervals', 'Maximum Report Start Date Depth', 'Maximum Demand Report Date Range', 'Default Quick Report View', 'Allow Reporter to email Report data', 'Report Default Email Type', 'Report Default File Format', and 'Require Authorization to view Report data'. A red 'SUBMIT' button is located at the bottom right of the form.

Testing Local Lists

Purpose

Each individual Policy has a Local List with a list of specific URLs to allow or deny. This list can contain a mix of URLs, keywords, and file extensions. This test verifies the function of the local list, and that local filtering only applies to the appropriate group.

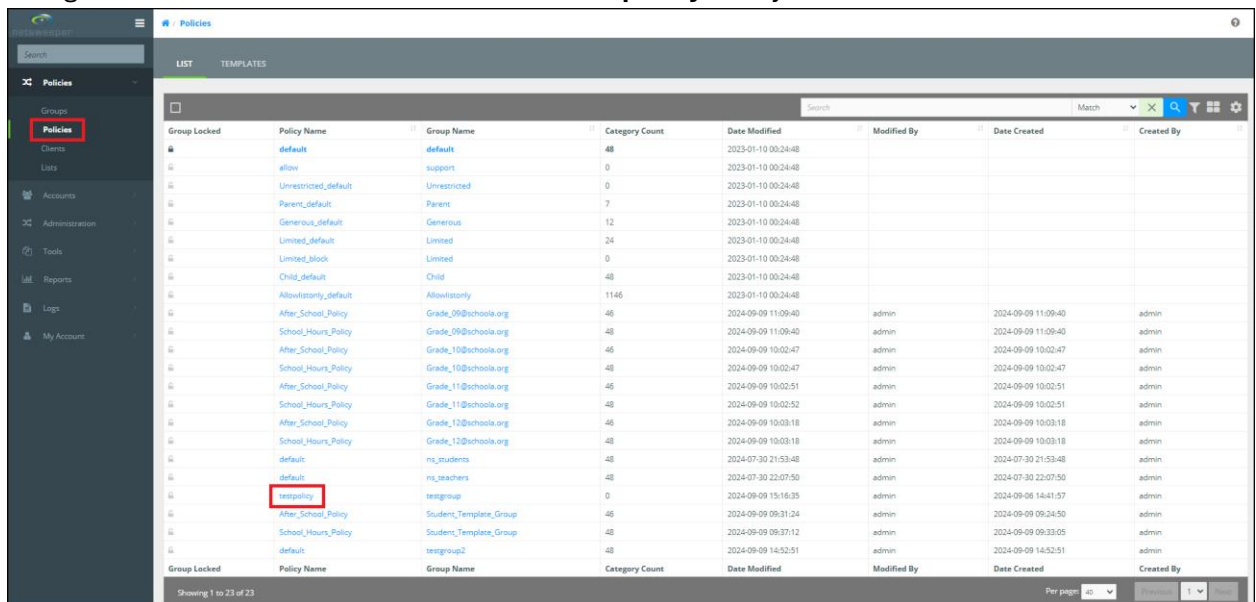
Precondition

See: Setting up Filtering Group and Client

Test Procedure: Local Lists

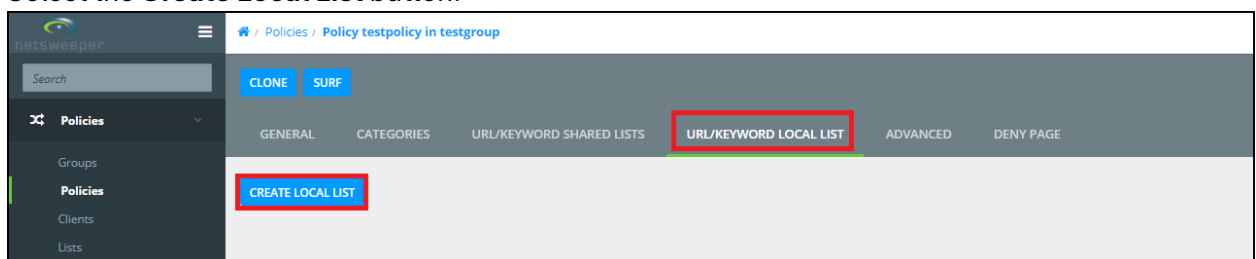
In the WebAdmin:

1. Navigate to Policies > Policies and select the **testpolicy** Policy.



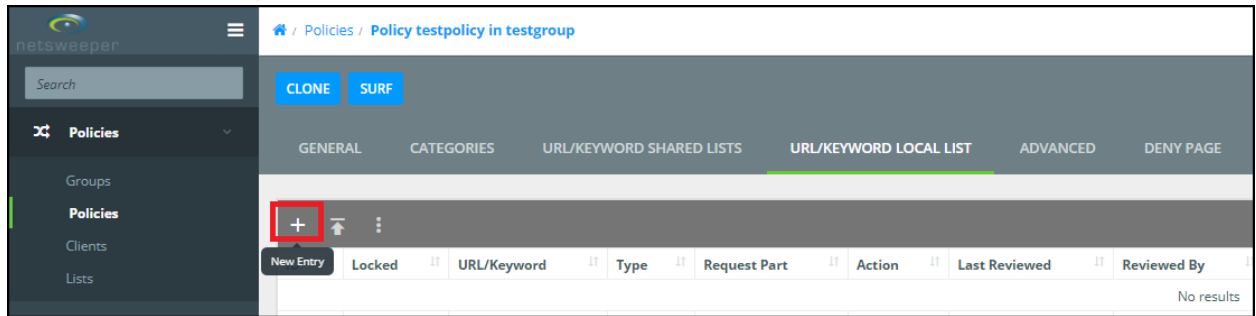
Group Locked	Policy Name	Group Name	Category Count	Date Modified	Modified By	Date Created	Created By
	default	default	48	2023-01-10 00:24:48			
	allow	support	0	2023-01-10 00:24:48			
	Unrestricted_default	Unrestricted	0	2023-01-10 00:24:48			
	Parent_default	Parent	7	2023-01-10 00:24:48			
	Generous_default	Generous	12	2023-01-10 00:24:48			
	Limited_default	Limited	24	2023-01-10 00:24:48			
	Limited_block	Limited	0	2023-01-10 00:24:48			
	Child_default	Child	48	2023-01-10 00:24:48			
	AllowIntently_default	AllowIntently	1146	2023-01-10 00:24:48			
	After_School_Policy	Grade_09@schoola.org	48	2024-09-09 11:09:40	admin	2024-09-09 11:09:40	admin
	School_Hours_Policy	Grade_09@schoola.org	48	2024-09-09 11:09:40	admin	2024-09-09 11:09:40	admin
	After_School_Policy	Grade_10@schoola.org	48	2024-09-09 10:02:47	admin	2024-09-09 10:02:47	admin
	School_Hours_Policy	Grade_10@schoola.org	48	2024-09-09 10:02:47	admin	2024-09-09 10:02:47	admin
	After_School_Policy	Grade_11@schoola.org	48	2024-09-09 10:02:51	admin	2024-09-09 10:02:51	admin
	School_Hours_Policy	Grade_11@schoola.org	48	2024-09-09 10:02:51	admin	2024-09-09 10:02:51	admin
	After_School_Policy	Grade_12@schoola.org	48	2024-09-09 10:03:18	admin	2024-09-09 10:03:18	admin
	School_Hours_Policy	Grade_12@schoola.org	48	2024-09-09 10:03:18	admin	2024-09-09 10:03:18	admin
	default	ns_students	48	2024-07-30 21:53:48	admin	2024-07-30 21:53:48	admin
	default	ns_teachers	48	2024-07-30 22:07:50	admin	2024-07-30 22:07:50	admin
	testpolicy	testgroup	0	2024-09-09 15:16:35	admin	2024-09-09 14:41:57	admin
	After_School_Policy	Student_Template_Group	48	2024-09-09 09:31:24	admin	2024-09-09 09:24:50	admin
	School_Hours_Policy	Student_Template_Group	48	2024-09-09 09:37:12	admin	2024-09-09 09:33:05	admin
	default	testgroup2	48	2024-09-09 14:52:51	admin	2024-09-09 14:52:51	admin

2. Choose the **URL/Keyword Local List** tab.
3. Select the **Create Local List** button.

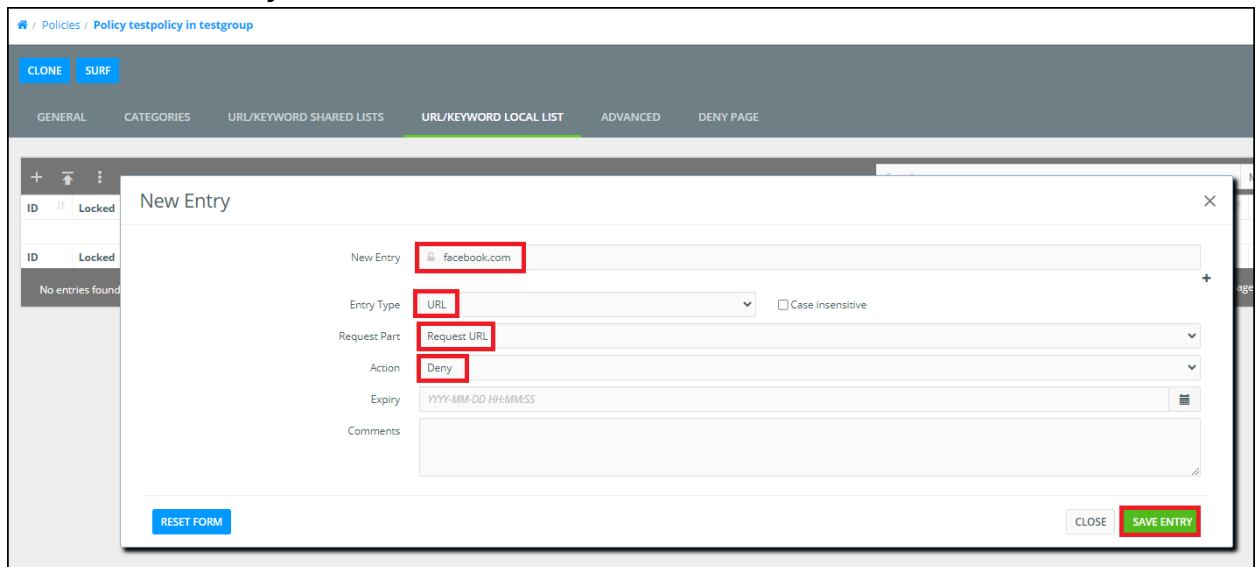


GENERAL	CATEGORIES	URL/KEYWORD SHARED LISTS	URL/KEYWORD LOCAL LIST	ADVANCED	DENY PAGE
CREATE LOCAL LIST					

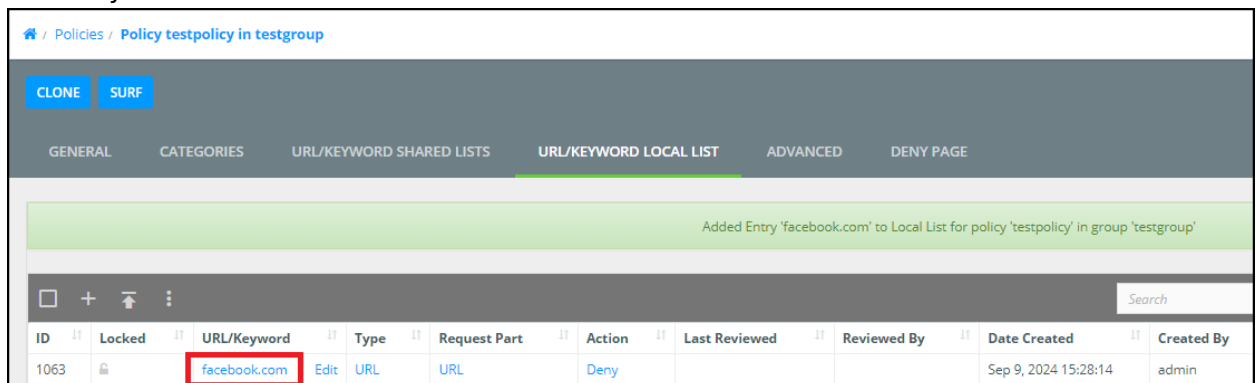
4. Select the New Entry button.



5. Enter facebook.com into the 'New Entry' field (or another 'example.com' where *example.com* represents the URL of your choice).
6. Ensure the 'Entry Type' is set to **URL**.
7. Ensure 'Request Part' is set to **Request URL**.
8. Set the 'Action' to **Deny**.
9. Select the **Save Entry** Button.



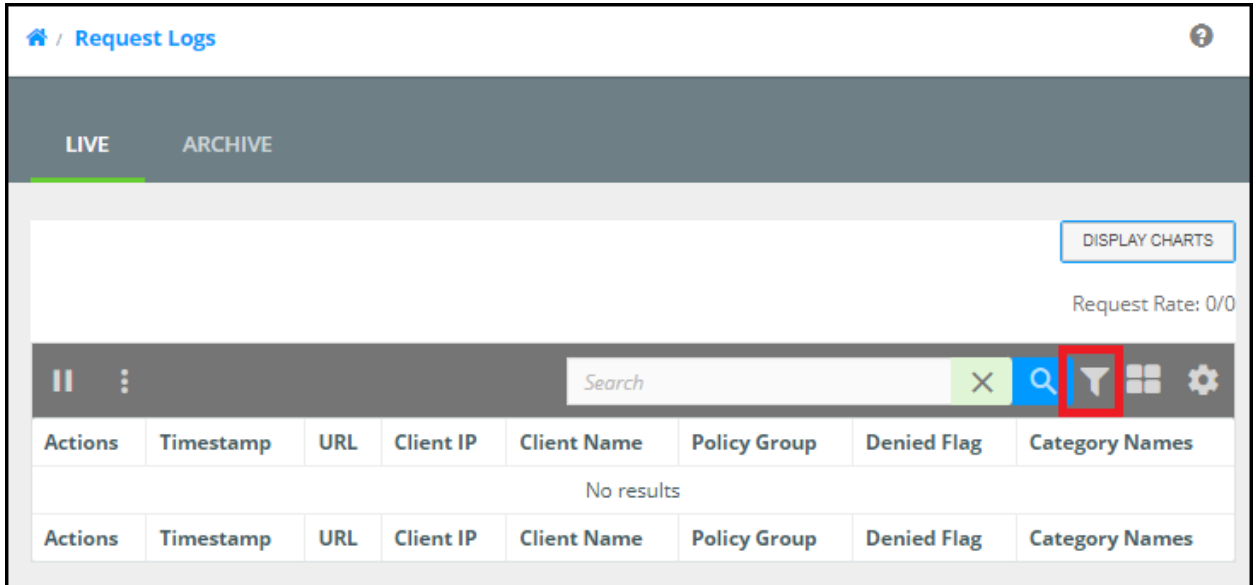
10. The entry is added to the Local List.



Request Logs Advanced Filters

We now want to add a Request Log Filter to our Request Logs window.

1. Navigate to Logs > Request Logs and select the **Advanced Filter** button in the Table Header.



The screenshot shows the 'Request Logs' interface. At the top, there's a header with a home icon and 'Request Logs' text. Below this is a tab bar with 'LIVE' and 'ARCHIVE' tabs. The main area contains a 'DISPLAY CHARTS' button and a 'Request Rate: 0/0' indicator. A table header bar includes a search bar, a close button, a search icon, a filter icon (highlighted with a red box), a grid icon, and a settings icon. The table below has columns: Actions, Timestamp, URL, Client IP, Client Name, Policy Group, Denied Flag, and Category Names. The table is currently empty, showing 'No results'.

Actions	Timestamp	URL	Client IP	Client Name	Policy Group	Denied Flag	Category Names
No results							
Actions	Timestamp	URL	Client IP	Client Name	Policy Group	Denied Flag	Category Names

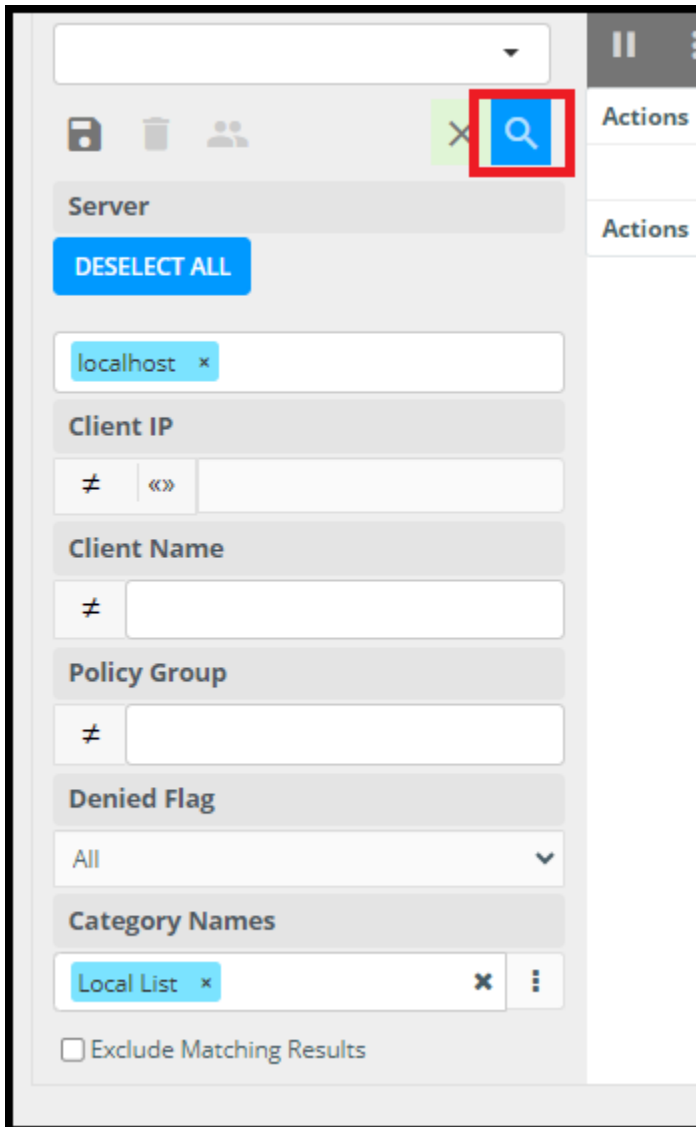
2. In the 'Category Names' field type 'local' and select the **Local List** result.

The screenshot shows a web application interface with various search filters. The 'Category Names' field is highlighted with a red box, and a dropdown menu is open showing the following options:

- local
- Local List
- iOS Message & FaceTime
- Yahoo Local
- DogPile Local
- LinkedIn Local Post
- Classifieds
- LinkedIn Share
- General News

The 'Local List' option is highlighted in yellow, indicating it is the selected result.

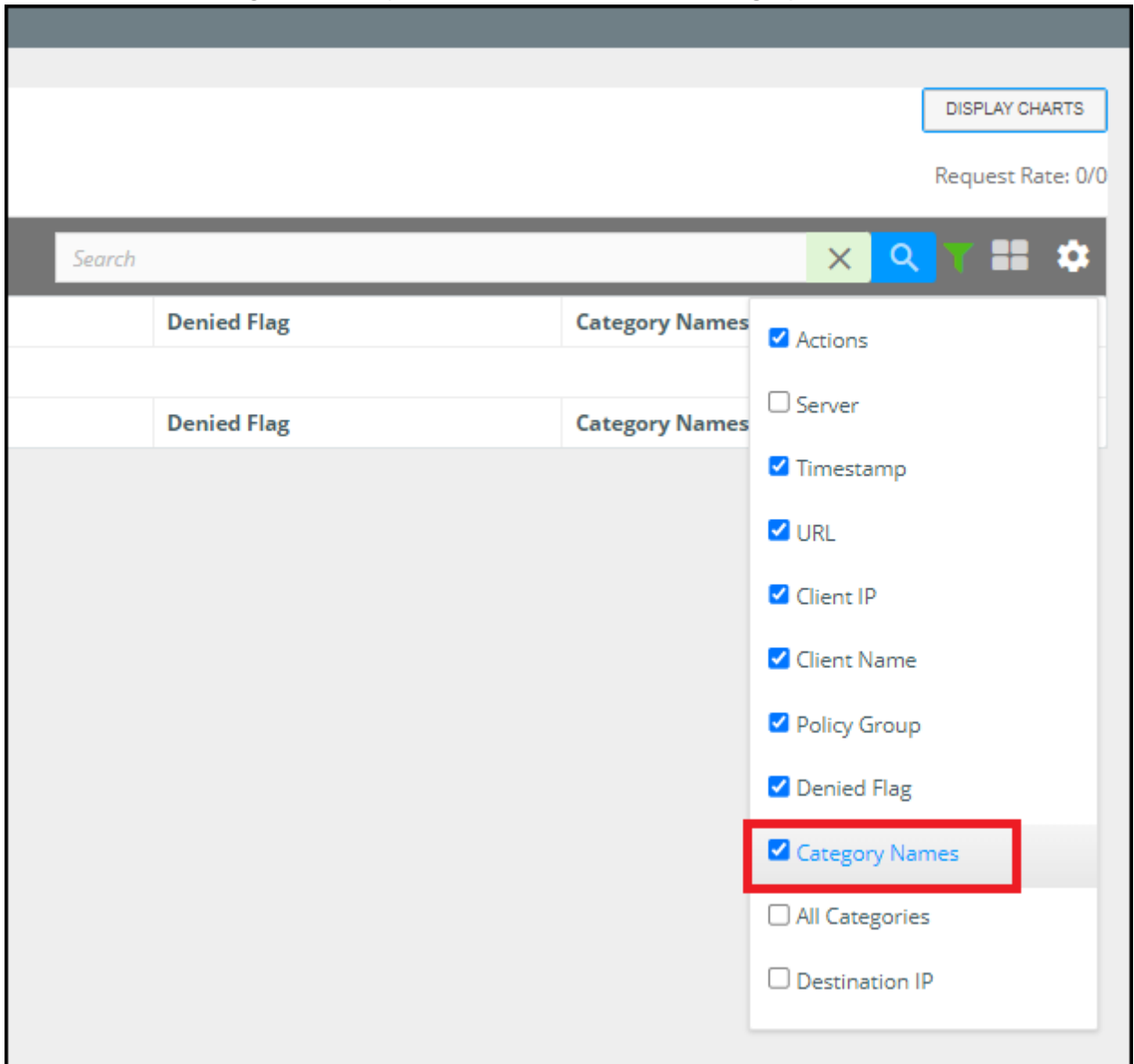
3. Select the **Search** icon within the Advanced Filter.



The screenshot shows the 'Advanced Filter' panel in a software interface. At the top, there is a search bar and a toolbar with icons for save, delete, and users. A red rectangle highlights a blue search icon (magnifying glass) in the toolbar. Below the toolbar, the filter panel is organized into sections: 'Server' with a 'DESELECT ALL' button; 'Client IP' with a dropdown menu showing 'localhost'; 'Client Name' with a dropdown menu showing '≠'; 'Policy Group' with a dropdown menu showing '≠'; 'Denied Flag' with a dropdown menu showing 'All'; and 'Category Names' with a dropdown menu showing 'Local List'. At the bottom, there is a checkbox labeled 'Exclude Matching Results'.

4. Note that the Filter Icon is now green, indicating an Advanced Filter is applied.

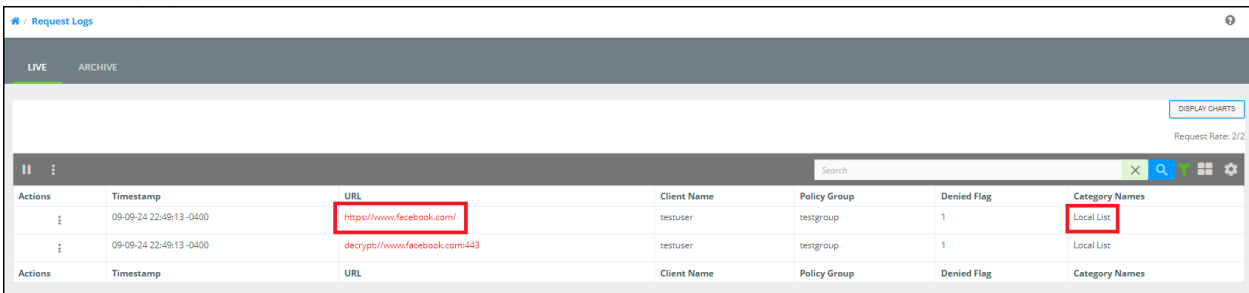
5. Hover over the 'Settings' icon and place a checkmark beside **Category Names**.



On the Test Workstation filtered by the 'testgroup' Group:

1. Clear the cache in your browser.
2. Browse to <https://facebook.com> (the site we entered in our Local List).

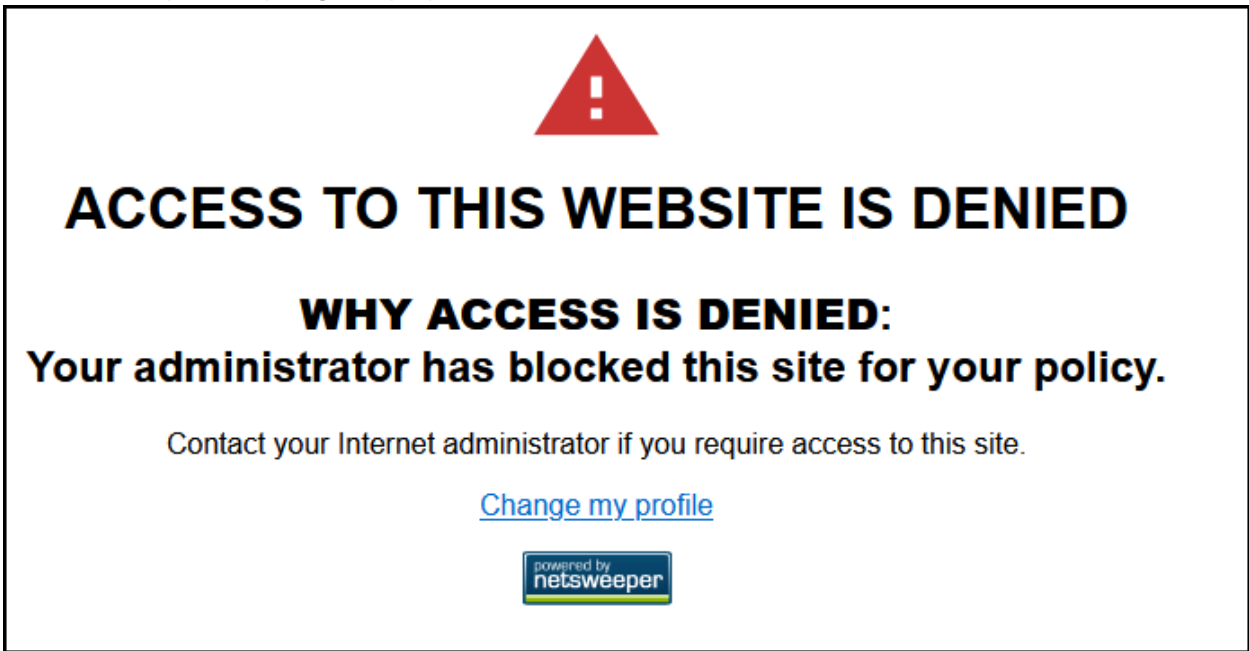
3. The Request Logs should show that the site is unreachable. The 'Category Names' column should display 'Local List'.



The screenshot shows the 'Request Logs' interface with a table of log entries. The first entry is highlighted with a red box around the URL 'https://www.facebook.com/' and the 'Category Names' column value 'Local List'. The second entry is also highlighted with a red box around the URL 'decrypt://www.facebook.com:443' and the 'Category Names' column value 'Local List'.

Actions	Timestamp	URL	Client Name	Policy Group	Denied Flag	Category Names
⋮	09-09-24 22:49:13 -0400	https://www.facebook.com/	testuser	testgroup	1	Local List
⋮	09-09-24 22:49:13 -0400	decrypt://www.facebook.com:443	testuser	testgroup	1	Local List

4. The Netsweeper Deny Page displays in the test workstation's browser.



Pass Criteria

Using the filtered workstation in the testgroup Group, browse to facebook.com (or the URL added to the Local List). The webpage will be unreachable.

Notes	
Results (Pass or Fail)	
Results Comments	

Domain Filter

Purpose

The Netsweeper solution can block specific domains. For example, it can block any URL or subdomain of a specific domain. This test case verifies that domain filtering behaves as expected for a Group's Local List.

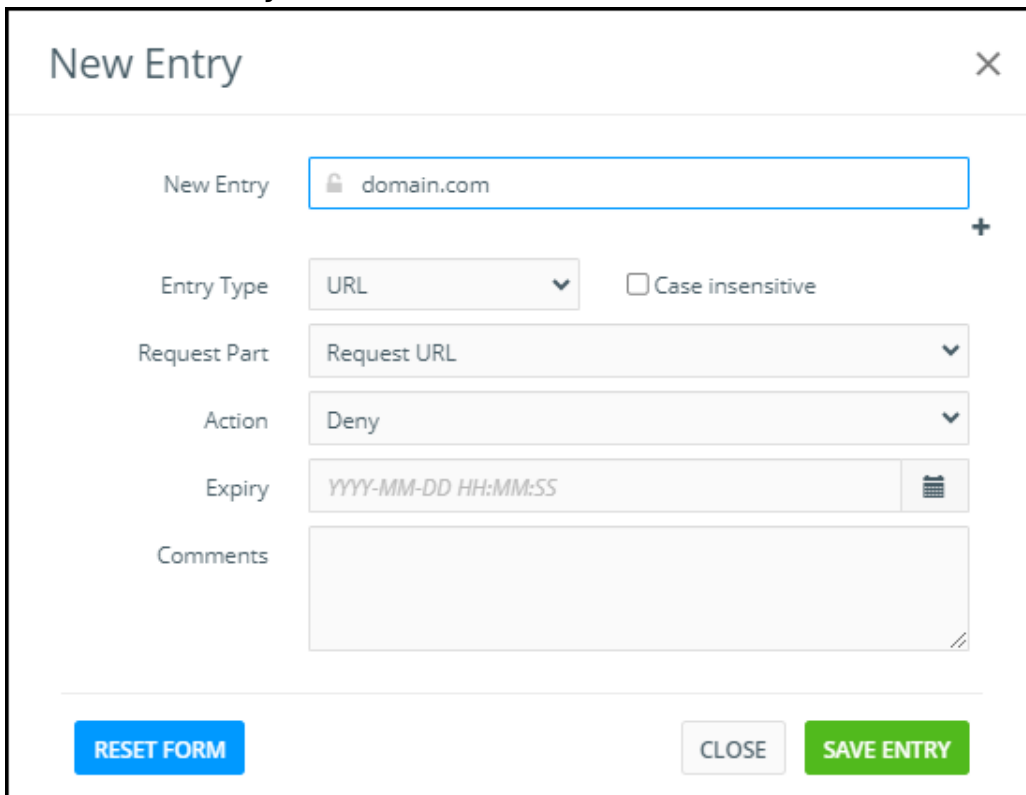
Precondition

See: Setting up Filtering Group and Client

Test Procedure: Domain Filter

In the WebAdmin:

1. Navigate to Policies > Policies and select your testpolicy.
2. Choose the **URL/Keyword Local List** tab.
3. Select the **New Entry** button.
4. Add *domain.com* in the 'New Entry' field, (where *domain.com* represents the URL of your choice).
5. Ensure the 'Entry Type' field is set to **URL**.
6. Ensure the 'Request Part' field is set to **Request URL**.
7. Set the 'Action' to **Deny**.
8. Select the **Save Entry** Button.



The screenshot shows the 'New Entry' form in the Netsweeper WebAdmin interface. The form is titled 'New Entry' and has a close button (X) in the top right corner. It contains several fields and buttons:

- New Entry:** A text input field containing 'domain.com' with a lock icon on the left and a plus sign on the right.
- Entry Type:** A dropdown menu set to 'URL' with a checkmark icon on the right. Next to it is a checkbox labeled 'Case insensitive' which is unchecked.
- Request Part:** A dropdown menu set to 'Request URL' with a downward arrow icon on the right.
- Action:** A dropdown menu set to 'Deny' with a downward arrow icon on the right.
- Expiry:** A text input field containing 'YYYY-MM-DD HH:MM:SS' with a calendar icon on the right.
- Comments:** A large text area for entering comments.
- Buttons:** At the bottom, there are three buttons: 'RESET FORM' (blue), 'CLOSE' (grey), and 'SAVE ENTRY' (green).

9. Save your New Entry.

On your Test Workstation

1. Browse to these six links:
http://domain.com
http://www.domain.com
http://mail.domain.com
https://domain.com
https://www.domain.com
ftp://domain.com
2. Content is unreachable for all six links.

Pass Criteria

Using the filtered workstation in the testgroup group, browse to any URL that belongs to your specified *domain.com*. The webpage will not be reachable.

Notes	
Results (Pass or Fail)	
Results Comments	

Deny Specific Category

Purpose

The Netsweeper solution can filter based on the Category which the URL belongs to. The system administrator can select the categories that will not be accessible to the end users.

Precondition

See: Setting up Filtering Group and Client

In the WebAdmin:

1. Navigate to Policies > Policies and select your testpolicy.
2. Choose the **Categories** tab.
3. Select the **Custom** Category Template.

The screenshot shows the Netsweeper WebAdmin interface for editing a policy. The breadcrumb navigation at the top reads: [Policies](#) / [Policy testpolicy in testgroup](#). Below the breadcrumb are two buttons: **CLONE** and **SURF**. A horizontal tab bar contains six tabs: **GENERAL**, **CATEGORIES** (which is selected and underlined in green), **URL/KEYWORD SHARED LISTS**, **URL/KEYWORD LOCAL LIST**, **ADVANCED**, and **DENY**. The main content area displays a dropdown menu for selecting a category template. The dropdown is open, showing the following options:
None
wasters, malicious and high-risk content
Relaxed
Adult, circumvention, malicious and high-risk content
Secure
Malicious and high-risk content
None
No content
Custom (highlighted with a red rectangular box)
Customize your category selection
At the bottom of the interface, there is a text field containing the text "Update this policy 'testpolicy' in group 'testgroup'." and a green **SUBMIT** button.

4. Type Pornography in the 'Quick Add' field and then select the result.

CLONE SURF

GENERAL CATEGORIES URL/KEYWORD SHARED LISTS URL/KEYWORD LOCAL LIST ADVANCED DENY PAGE

Custom

0 Blocked

Select the categories you wish to filter.

Q porn

Pornography

Open Mixed Content

Child Erotica

Age Restriction

Sex Education

Child Sexual Abuse

☐ System 0/12

☐ Web Apps 0/720

☐ Web Content 0/89

5. Select the **Submit** button to save your changes.

Home / Policies / Policy testpolicy in testgroup

CLONE SURF

GENERAL CATEGORIES URL/KEYWORD SHARED LISTS URL/KEYWORD LOCAL LIST ADVANCED DENY PAGE

Custom

1 Blocked

Pornography

Q Quick Add

☐ Countries 0/255

☐ Mobile Apps 0/30

☐ Protocols 0/60

☐ System 0/12

☐ Web Apps 0/720

☒ Web Content 1/89

☒ Adult 1/29

☐ Information 0/22

☐ Miscellaneous 0/14

☐ Recreation 0/8

☐ Security 0/16

☐ Marijuana

☐ Match Making

☐ Matrimonial

☐ Nudity

☐ Occult

☐ Open Mixed Content

☐ Pay to Surf

☐ Peer to Peer

☒ Pornography

☐ Profanity

☐ Self Harm

☐ Substance Abuse

☐ Terrorism

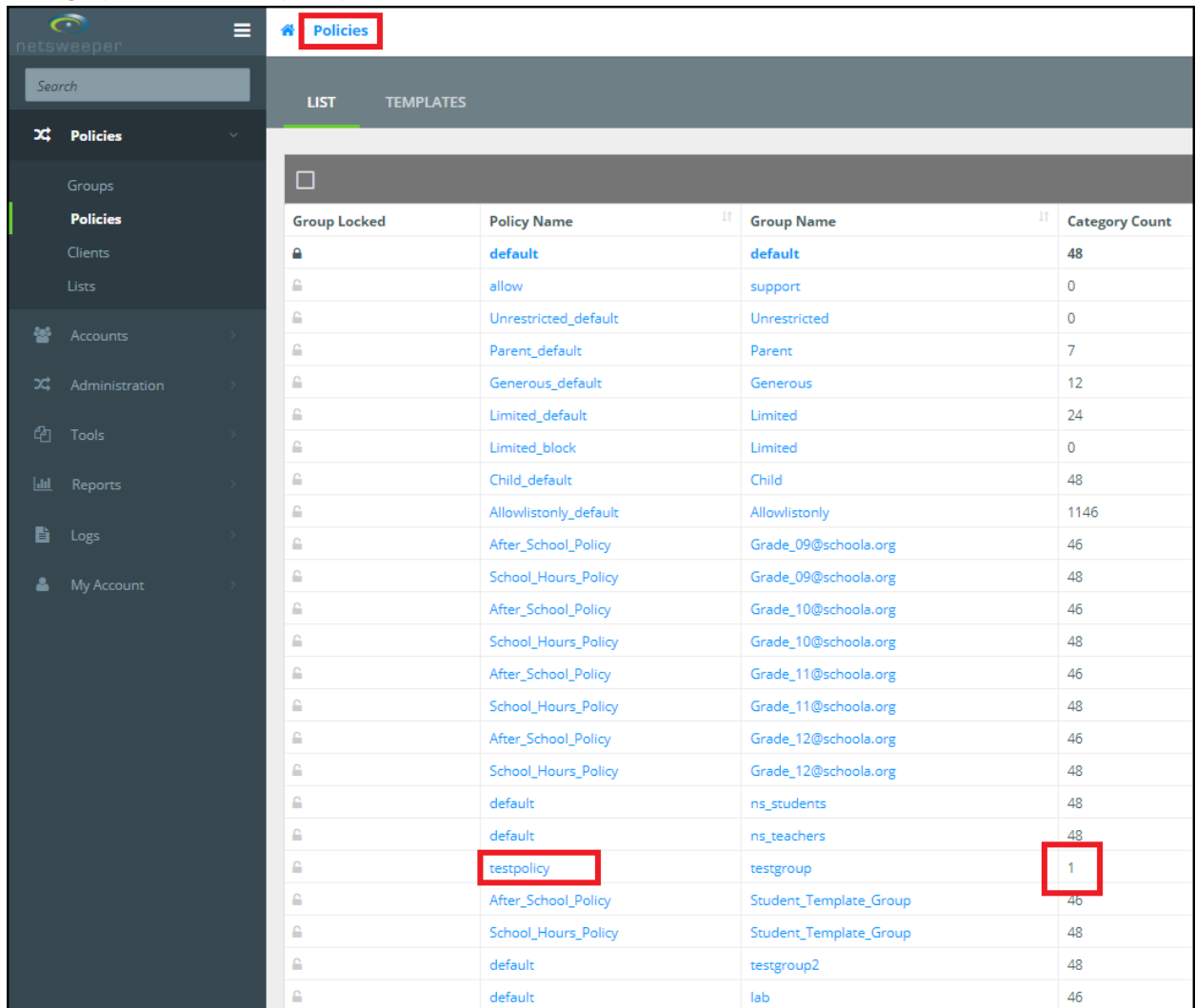
☐ Tobacco

☐ Weapons

Update this policy 'testpolicy' in group 'testgroup'.

SUBMIT

- Use your breadcrumbs to navigate back to the Policies window, where you can see that the Category count for testpolicy is now 1.



Group Locked	Policy Name	Group Name	Category Count
	default	default	48
	allow	support	0
	Unrestricted_default	Unrestricted	0
	Parent_default	Parent	7
	Generous_default	Generous	12
	Limited_default	Limited	24
	Limited_block	Limited	0
	Child_default	Child	48
	Allowlistonly_default	Allowlistonly	1146
	After_School_Policy	Grade_09@schoola.org	46
	School_Hours_Policy	Grade_09@schoola.org	48
	After_School_Policy	Grade_10@schoola.org	46
	School_Hours_Policy	Grade_10@schoola.org	48
	After_School_Policy	Grade_11@schoola.org	46
	School_Hours_Policy	Grade_11@schoola.org	48
	After_School_Policy	Grade_12@schoola.org	46
	School_Hours_Policy	Grade_12@schoola.org	48
	default	ns_students	48
	default	ns_teachers	48
	testpolicy	testgroup	1
	After_School_Policy	Student_Template_Group	46
	School_Hours_Policy	Student_Template_Group	48
	default	testgroup2	48
	default	lab	46

On Your Test Workstation

- Browse to a pornography site such as playboy.com.
- The intended webpage is unreachable.

Pass Criteria

Using the filtered workstation in the testgroup Group, browsing to a URL that belongs to the Pornography Category will not be reachable.

Notes	
Results (Pass or Fail)	
Results Comments	

Category Templates

Purpose

The Netsweeper solution allows for the creation of Category Templates. Category Templates define a set of Categories recommended for the default Policies and these can be applied to Policies and Clients.

Precondition

See: Setting up Filtering Group and Client

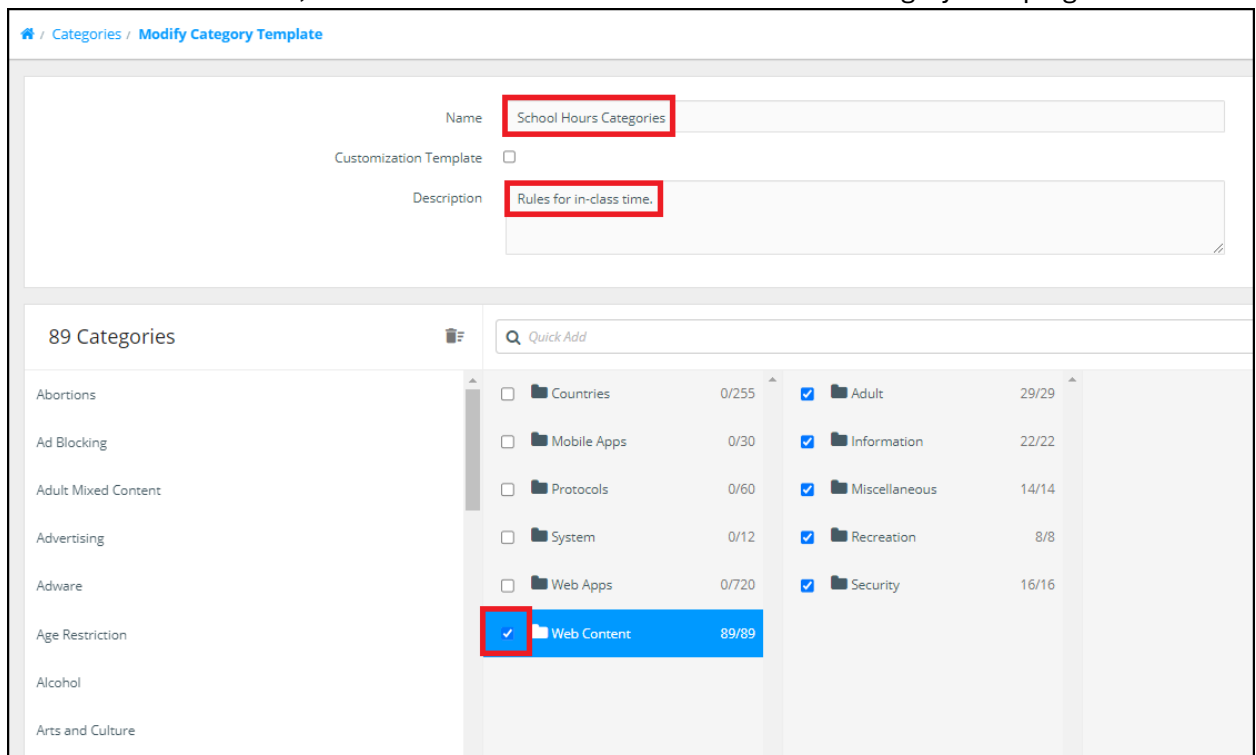
Test Procedure: Deny Specific Category

In the WebAdmin

1. Navigate to Administration > Categories and choose the **Templates** tab.
2. Select the **Create** button.



3. Name your template 'School Hours Categories' and add an optional description.
4. In the Hierarchical view, select the checkbox for the **Web Content** Category Grouping.



5. Select the **Submit** button. You will see a banner stating, “Successfully added a new category template.”
6. Use your breadcrumbs to return to the Templates tab of the Categories window. You will see your new ‘School Hours Categories’ Template along with the number of blocked Categories it enforces.

Template Name	Description	Category Count	Action	Display Order
Custom	Customize your category selection		Clone/Edit	+
Moderate	Adult, illegal, questionable material, circumvention techniques, time wasters, malicious and high-risk content	24	Clone/Edit	+
None	No content		Clone/Edit	+
Relaxed	Adult, circumvention, malicious and high-risk content	12	Clone/Edit	+
School Hours Categories	Rules for in-class time.	89	Clone/Edit	+
Secure	Malicious and high-risk content	7	Clone/Edit	+
Strict	Adult, illegal, violent, harmful, questionable material, circumvention techniques, time wasters, malicious and high-risk content	48	Clone/Edit	+

7. Select the **Clone** button beside the ‘School Hours Categories’ Template.

Template Name	Description	Category Count	Action	Display Order
Custom	Customize your category selection		Clone/Edit	+
Moderate	Adult, illegal, questionable material, circumvention techniques, time wasters, malicious and high-risk content	24	Clone/Edit	+
None	No content		Clone/Edit	+
Relaxed	Adult, circumvention, malicious and high-risk content	12	Clone/Edit	+
School Hours Categories	Rules for in-class time.	89	Clone /Edit	+
Secure	Malicious and high-risk content	7	Clone/Edit	+
Strict	Adult, illegal, violent, harmful, questionable material, circumvention techniques, time wasters, malicious and high-risk content	48	Clone/Edit	+

8. Select the **Edit** button beside the 'School Hours Categories clone 2' Template.

Template Name	Description	Category Count	Action	Display Order
Custom	Customize your category selection		Clone/Edit	+
Moderate	Adult, illegal, questionable material, circumvention techniques, time wasters, malicious and high-risk content	24	Clone/Edit	+
None	No content		Clone/Edit	+
Relaxed	Adult, circumvention, malicious and high-risk content	12	Clone/Edit	+
School Hours Categories	Rules for in-class time.	89	Clone/Edit	+
School Hours Categories clone 2	Rules for in-class time.	89	Clone/ Edit	+
Secure	Malicious and high-risk content	7	Clone/Edit	+
Strict	Adult, illegal, violent, harmful, questionable material, circumvention techniques, time wasters, malicious and high-risk content	48	Clone/Edit	+

9. Rename this Template to ‘After School Categories’ and update the optional description.

10. In the left column, scroll down to 'Social Networking' and select the **delete** button to remove that category from our Template.

[Categories](#) / [Modify Category Template](#)

Name: School Hours Categories clone 2

Customization Template: ☐

Description: Rules for after class.

89 Categories

Search engine

Self Harm

Sex Education

Social Networking

Sports

Streaming Media

Substance Abuse

Quick Add

☐	Countries	0/255
☐	Mobile Apps	0/30
☐	Protocols	0/60
☐	System	0/12
☐	Web Apps	0/720
☒	Web Content	89/89

11. Select the **Submit** button to apply your changes.
12. Use your breadcrumbs to return to the Templates tab of the Categories window, where we now see our 'After School Categories' added. These Templates will be used in the following procedure.

Time Based Policies: Using Policy Events.

Purpose

In some cases, users may wish to block access to sites only at specific times. This test case will verify that time policies operate as expected.

Precondition

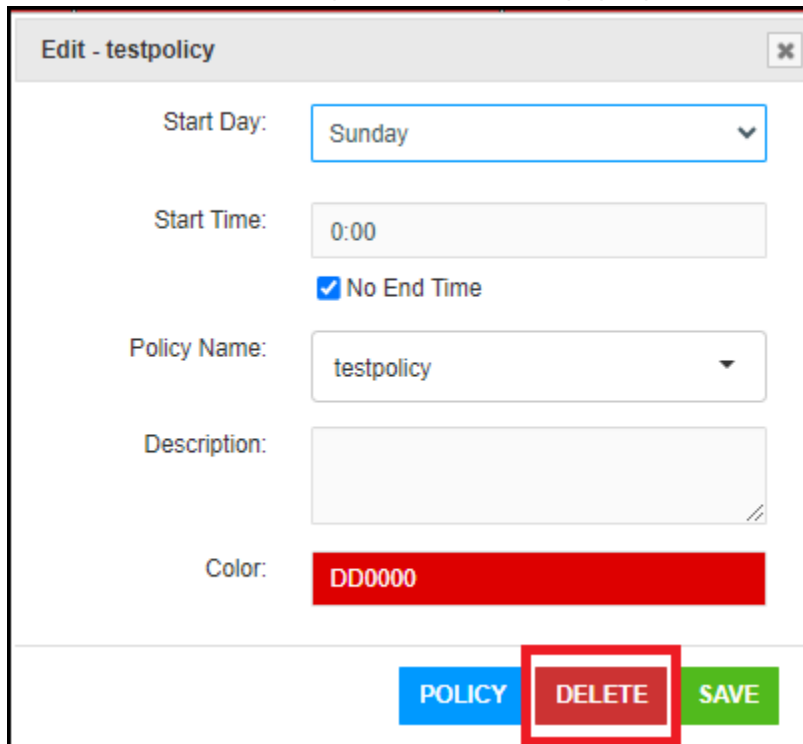
See: Setting up Filtering Group and Client

The created 'After School' and 'School Hours' Category Templates.

Test Procedure: Policy Events

In the WebAdmin:

1. Navigate to Policies > Groups and choose the **List** tab.
2. Select the 'testgroup' and choose the Policies tab.
3. Choose the 'Default' Policy Event. and in the pop-up-box, select the **Delete** button.



The screenshot shows a web-based interface for editing a policy. The title bar of the dialog is 'Edit - testpolicy'. The form contains the following fields and controls:

- Start Day:** A dropdown menu currently showing 'Sunday'.
- Start Time:** A text input field showing '0:00'.
- No End Time:** A checkbox that is checked.
- Policy Name:** A dropdown menu currently showing 'testpolicy'.
- Description:** A large text area for entering a description.
- Color:** A color selection field showing a red swatch with the code 'DD0000'.

At the bottom of the dialog, there are three buttons: 'POLICY' (blue), 'DELETE' (red, highlighted with a red rectangular box), and 'SAVE' (green).

4. Select the **Create** button.

The screenshot shows the Netsweeper Groups page for 'Group testgroup'. The 'POLICIES' tab is selected in the top navigation bar. Below the navigation bar, there are tabs for 'CALENDAR', 'LIST', and 'EVENTS'. A yellow warning message states: 'WARNING: There are no Policy Events for this group. Clients in this group will have no internet access.' Below this, a green message states: 'Successfully Deleted Policy Event From Group testgroup.' At the bottom, there are three buttons: 'CREATE' (highlighted with a red box), 'IMPORT', and 'EXPORT'. Below the buttons is a calendar grid with columns for Sunday, Monday, Tuesday, Wednesday, and Thursday, and rows for 12AM and 1AM.

5. In the Create window, select the **No End Time** checkbox.
6. Enter 'After_School_Policy' (with no spaces) in the 'Policy Name' field and add an optional description.
7. Enter the value 3636FF into the 'color' field and select the **Save** button.

The screenshot shows the 'Create' window for a policy. The 'Start Day' is set to 'Sunday' and the 'Start Time' is '0:00'. The 'No End Time' checkbox is checked and highlighted with a red box. The 'Policy Name' field contains 'After_School_Policy' and is highlighted with a red box. The 'Description' field is empty. The 'Color' field contains '3636FF' and is highlighted with a red box. A green 'SAVE' button is at the bottom right.

8. The 'After_School_Policy' Policy Event is created.

The screenshot shows the Netsweeper interface with the 'POLICIES' tab selected. A green banner at the top of the main content area reads 'Created Policy Event in group 'testgroup''. Below this, there are three buttons: 'CREATE', 'IMPORT', and 'EXPORT'. The main area displays a calendar grid with columns for each day of the week (Sunday through Saturday) and rows for time slots (12AM, 1AM, 2AM, 3AM, 4AM). The 'After_School_Policy' event is shown as a black bar spanning from 12:00 am to 12:00 am on Sunday. The rest of the calendar grid is blue.

9. Select the **Create** button again.

10. Set the 'Start Day' and 'Stop Day' fields to Monday.

11. Select the **Multiple Days** checkbox.

12. Set the 'Start Time' as 8:00 and the 'Stop Time' as 16:00.

13. In the 'Day Selection' field choose Monday to Friday inclusive.

14. Enter the 'Policy Name' School_Hours_Policy with no spaces and add an optional description.

15. Enter the Color value FF308A.

Create

Start Day:Monday

Start Time:8:00

☐ No End Time☒ Multiple Days

Stop Day:Monday

Stop Time:16:00

Day Selection:Monday x Tuesday x Wednesday x Thursday x Friday x

Policy Name:School_Hours_Policy

Description:Policy for in-class hours.

Color:FFE08A

SAVE

16. Select the **Save** button.

17. The School Hours Policy displays during its designated days and times.

	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
12AM	After_School_Policy 12:00 am to 12:00 am	12:00 am to 12:00 am	12:00 am to 12:00 am	12:00 am to 12:00 am	12:00 am to 12:00 am	12:00 am to 12:00 am	12:00 am to 12:00 am
1AM							
2AM							
3AM							
4AM							
5AM							
6AM							
7AM							
8AM		School_Hours_Policy 08:00 am to 04:00 pm Policy for in-class hours.	School_Hours_Policy 08:00 am to 04:00 pm Policy for in-class hours.	School_Hours_Policy 08:00 am to 04:00 pm Policy for in-class hours.	School_Hours_Policy 08:00 am to 04:00 pm Policy for in-class hours.	School_Hours_Policy 08:00 am to 04:00 pm Policy for in-class hours.	
9AM							
10AM							
11AM							
12PM							

18. Next, navigate to the List subsection of the Policies tab and confirm that the 'After School Policy' and the 'School Hours Policy' are listed.

[Home](#) / [Groups](#) / [Group testgroup](#)

[GENERAL](#)
[ADVANCED](#)
[POLICIES](#)
[CLIENTS](#)
[MANAGERS](#)
[AUTHENTICATION REDIRECT](#)

[CALENDAR](#)
[LIST](#)
[EVENTS](#)

+

Policy Name	Category Count	Default Status
testpolicy 	1	Deny
After_School_Policy	48	Deny
School_Hours_Policy	48	Deny

Policy Name

Category Count

Default Status

19. Select the 'testpolicy' Policy's row and select the **Delete** button in the Table Header bar.

20. Select the 'After_School_Policy' and then navigate to the Categories tab for that Policy.

21. Select the 'After School Categories' Template created in the previous procedure and select the **Submit** button.

Groups / Group testgroup / Policy After_School_Policy in testgroup

CLONE SURF

GENERAL CATEGORIES URL/KEYWORD SHARED LISTS URL/KEYWORD LOCAL LIST ADVANCED DENY PAGE

After School Categories

88 Blocked

Abortion	Ad Blocking	Adult Mixed Content	Advertising
Adware	Age Restriction	Alcohol	Arts and Culture
Body Modification	Bullying	Business	Child Erotica
Child Sexual Abuse	Classifieds	Content Server	Copyright Infringement
Criminal Skills	Culinary	Directory	Education
Educational Games	Entertainment	Environmental	Extreme
Financial Services	Gambling	Games	General News
Government	Hacking	Hate Speech	Health
HTTP Errors	Humor	Infected Hosts	Intimate Apparel
Job Search	Journals and Blogs	Legal	Lifestyle Choices
Malicious Web Obfuscation	Malware	Malware Hosts	Marijuana
Match Making	Matrimonial	Medication	Military
Nudity	Occult	Open Mixed Content	Parked
Document (Categories)	Don't Surf	Don't Block	Blockchain

Update this policy 'After_School_Policy' in group 'testgroup'.

SUBMIT

22. Use the breadcrumbs to return to the Group 'testgroup'.
23. Select the School Hours Policy and repeat the steps to assign the School Hours Categories.
24. When done, verify that the 'List' subsection of the 'Policies' tab looks like this:

Groups / Group testgroup

GENERAL ADVANCED POLICIES CLIENTS MANAGERS AUTHENTICATION REDIRECT

CALENDAR LIST EVENTS

+

Policy Name	Category Count	Default Status
After_School_Policy	88	Deny
School_Hours_Policy	89	Deny
Policy Name	Category Count	Default Status

Pass Criteria

1. Navigate to Tools > Trace Request.
2. Select the 'Group Name' testgroup and the 'Policy Name' After_School_Policy.
3. Enter facebook.com or another 'Social Networking' site and select the **Send Request** button.
4. The site is allowed under 'Social Networking'.

[Trace Request](#)

Client Name

Client IP Address

BROWSE IP

Group Name

testgroup ×

Policy Name

After_School_Policy ×

URL:

http://facebook.com

Destination IP Address:

User Agent:

Referrer:

Client Module Name:

Event Type:

Check Policy

☐ Show All Steps

SEND REQUEST

Policy Server: localhost (127.0.0.1)

Step	List URL/Keyword	Result
Protocol CNS List	http://	Category: Hypertext Transfer
Master List Lookup	facebook.com	Category: Social Networking, Hypertext Transfer
Policy Categories Check		Category: Social Networking, Hypertext Transfer Decision: Allowed

5. Change the 'Policy Name' to 'School_Hours_Policy' and select the **Send Request** button again. The site is now denied by 'Social Networking'.

[Trace Request](#)

Client Name

Client IP Address

Group Name

Policy Name

testgroup

School_Hours_Policy

BROWSER IP

URL:

Destination IP Address:

User Agent:

Referrer:

Client Module Name:

Event Type:

http://facebook.com

Check Policy

☐ Show All Steps

SEND REQUEST

Policy Server: localhost (127.0.0.1)

Step	List URL/Keyword	Result
Protocol CNS List	http://	Category: Hypertext Transfer
Master List Lookup	facebook.com	Category: Social Networking, Hypertext Transfer
Policy Categories Check		Category: Social Networking, Hypertext Transfer Decision: Denied
Response URL Test		Category: Host is an IP Replace URL: https://192.168.222.150/webadmin...
Filter Bypass List Lookup	https://192.168.222.150	Category: Filter Bypass List, Host is an IP Decision: Allowed

Notes	Policy Events are granular on a per-minute-basis.
Results (Pass or Fail)	
Results Comments	

Lists Window

This section will test global filtering through the 'Lists' window.

System Deny List

Purpose

When websites need to be blocked globally, regardless of group policy, then the **System Deny List** is used. URLs placed on this list will be denied for all clients, regardless of group membership and specific policy/list settings.

Precondition

See: Setting up Filtering Group and Client

Additional Precondition: Adding a System Wide 'testlist'

1. Navigate to Policies > Lists and select the **Create** button.
2. Type 'testlist' into the List Name field.
3. Select the checkbox for **System Wide List** in the 'List Assignments' section.
4. In the 'Restrictions' section, select the checkbox for **Deny** under 'Restrict Actions'.

The screenshot shows the 'New List' configuration window in the Netsweeper interface. The 'List Name' field is set to 'testlist'. In the 'List Assignments' section, the 'System Wide List' checkbox is selected. The 'Restrictions' section is expanded, showing 'Restrict Actions' with 'Deny' selected. Other sections like 'Restrict Types' and 'Restrict Request Parts' are also visible but not fully configured. The 'Permissions' section at the bottom has buttons for 'ADD SYSOP', 'ADD SYSOP DEFAULTS', 'REMOVE ALL SYSOP PERMISSIONS', and 'CREATE LIST'.

5. Select the **Create List** button. The 'testlist' appears in the Lists window.

Lists

LISTS SEARCH ASSIGNMENTS ADD ENTRY SUGGESTIONS

List Created Successfully

LOCAL SHARED

List Name	Actions	Entries	Comment	Date Modified	Log	Policies	Roles	Modified By	Date Created	Created By
Filter Bypass List	Allow	2	Former Filter Bypass Lis...	Sep 9, 2024 19:34:19	History		filterbypass			
School A Cat List	Categorize	6	Category rules only!	Sep 9, 2024 19:34:19	History	School_Hours_Policy, School_Hours_Policy, School_Hours_Policy, School_Hours_Policy, School_Hours_Policy, default,	override	admin	Sep 6, 2024 10:44:03	admin
School A Shared List	Allow, Deny	7	Allow/Deny websites only	Sep 6, 2024 10:42:11	History	School_Hours_Policy, School_Hours_Policy, School_Hours_Policy, School_Hours_Policy, School_Hours_Policy, After_School_Policy	admin	admin	Sep 6, 2024 10:19:22	admin
schoola cat	Categorize	5		Sep 9, 2024 19:25:21	History		categoryurl	admin	Jul 4, 2024 16:19:05	admin
schoola shared	Any	6		Sep 9, 2024 16:34:26	History	After_School_Policy	admin	admin	Jul 4, 2024 16:18:25	admin
Selective Decryption	Any	2	Automatically created at ...	Sep 10, 2024 03:24:38	History	School_Hours_Policy, School_Hours_Policy, School_Hours_Policy, School_Hours_Policy, School_Hours_Policy, default, After_School_Policy	admin			
System Deny List	Deny	1	Former System Deny List ...		History		system			
System Wide Search Keywords	Categorize	598	Former Policy: Search Ke...	Sep 15, 2022 15:15:43	History		system			
testlist	Deny	0		Sep 12, 2024 08:26:19	History		system	admin	Sep 12, 2024 08:26:19	admin

Showing 1 to 25 of 25

Additional Precondition: Create a Local List

In order to test our System-Wide Deny ‘testlist’, the group our testclient is assigned to must have a Local List that explicitly allows the URL we want to test with.

In the WebAdmin:

1. Navigate to Policies > Policies to open the Policies window.
2. At the bottom of the page, select the 'Per page' setting and increase the value as needed.
3. Choose the 'School_Hours_Policy' for our 'testgroup'.

Policies

LIST

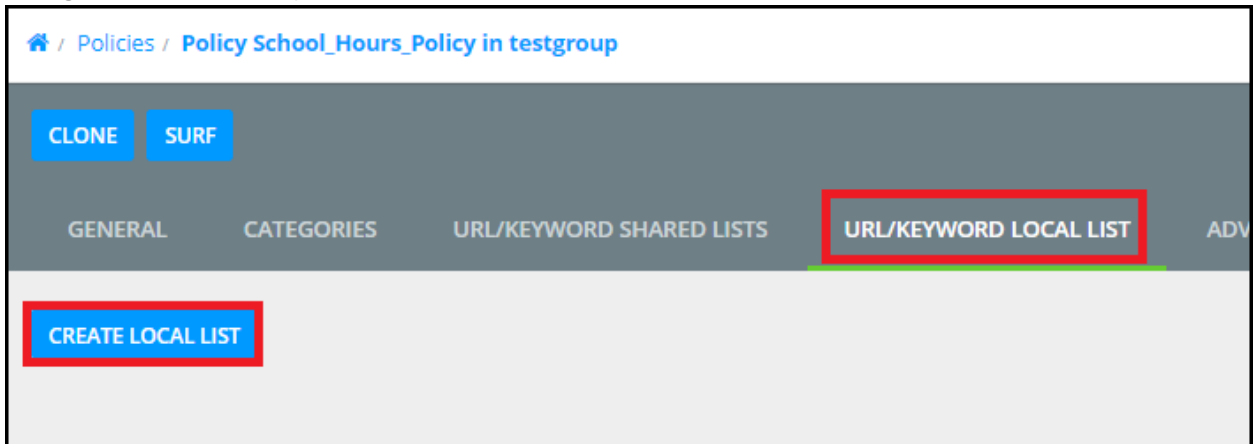
TEMPLATES

Search

Masch

Group Locked	Policy Name	Group Name	Category Count	Date Modified	Modified By	Date Created	Created By
	default	default	48	2023-01-10 00:24:48			
	allow	support	0	2023-01-10 00:24:48			
	Unrestricted_default	Unrestricted	0	2023-01-10 00:24:48			
	Parent_default	Parent	7	2023-01-10 00:24:48			
	Generous_default	Generous	12	2023-01-10 00:24:48			
	Limited_default	Limited	24	2023-01-10 00:24:48			
	Limited_block	Limited	0	2023-01-10 00:24:48			
	Child_default	Child	48	2023-01-10 00:24:48			
	Allowlistonly_default	Allowlistonly	1146	2023-01-10 00:24:48			
	After_School_Policy	Grade_09@schoola.org	46	2024-09-09 16:32:01	admin	2024-09-09 11:09:40	admin
	School_Hours_Policy	Grade_09@schoola.org	48	2024-09-09 11:09:40	admin	2024-09-09 11:09:40	admin
	After_School_Policy	Grade_10@schoola.org	46	2024-09-09 10:02:47	admin	2024-09-09 10:02:47	admin
	School_Hours_Policy	Grade_10@schoola.org	48	2024-09-09 10:02:47	admin	2024-09-09 10:02:47	admin
	After_School_Policy	Grade_11@schoola.org	46	2024-09-09 10:02:51	admin	2024-09-09 10:02:51	admin
	School_Hours_Policy	Grade_11@schoola.org	48	2024-09-09 10:02:52	admin	2024-09-09 10:02:51	admin
	After_School_Policy	Grade_12@schoola.org	46	2024-09-09 10:03:18	admin	2024-09-09 10:03:18	admin
	School_Hours_Policy	Grade_12@schoola.org	48	2024-09-09 10:03:18	admin	2024-09-09 10:03:18	admin
	default	ns_students	48	2024-07-30 21:53:48	admin	2024-07-30 21:53:48	admin
	default	ns_teachers	48	2024-07-30 22:07:50	admin	2024-07-30 22:07:50	admin
	After_School_Policy	testgroup	88	2024-09-11 15:31:19	admin	2024-09-11 15:14:30	admin
	School_Hours_Policy	testgroup	89	2024-09-11 15:31:28	admin	2024-09-11 15:22:12	admin
	After_School_Policy	Student_Template_Group	46	2024-09-09 09:31:24	admin	2024-09-09 09:24:50	admin

4. Navigate to the URL/Keyword Local List tab and select the **Create Local List** button.



5. Select the **New Entry** button.
6. Add 'pinterest.com' into the Entry field.
7. Ensure the 'Entry Type' field is set to **URL**.
8. Ensure the 'Request Part' field is set to **Request URL**.
9. Set the 'Action' to **Allow**.

The 'New Entry' form is shown with the following fields: 'New Entry' (pinterest.com), 'Entry Type' (URL), 'Request Part' (Request URL), 'Action' (Allow), 'Expiry' (YYYY-MM-DD HH:MM:SS), and 'Comments'. The 'SAVE ENTRY' button is highlighted with a red box.

10. Select the **Save Entry** Button. The URL is added to the Local List.

The screenshot shows the 'URL/KEYWORD LOCAL LIST' tab with a green notification bar stating: 'Added Entry 'pinterest.com' to Local List for policy 'School_Hours_Policy' in group 'testgroup''. Below the notification is a table with the following data:

ID	Locked	URL/Keyword	Type	Request Part	Action	Last Reviewed	Reviewed By	Date Created	Created By
1068		pinterest.com	URL	URL	Allow			Sep 12, 2024 11:39:04	admin

The 'pinterest.com' entry and the 'Allow' action are highlighted with red boxes. The table footer shows 'Showing 1 to 1 of 1'.

Modify the System-Wide List:

1. Navigate to Policies > Lists.
2. Choose the 'testlist' and then select the **New Entry** button.
3. Add 'pinterest.com' into the Entry field.
4. Ensure the 'Entry Type' field is set to **URL**.
5. Ensure the 'Request Part' field is set to **Request URL**.
6. Note that there is no 'Action' field this time. This is because we restricted the Action to Deny.

New Entry

New Entry

Entry Type ☐ Case insensitive

Request Part

Expiry

Comments

[RESET FORM](#) [CLOSE](#) [SAVE ENTRY](#)

7. Select the **Save Entry** button.
8. The Deny entry is added.

[Home](#) / [Lists](#) / [Edit List: testlist](#)

ENTRIES SETTINGS RULES ALERTS POLICIES

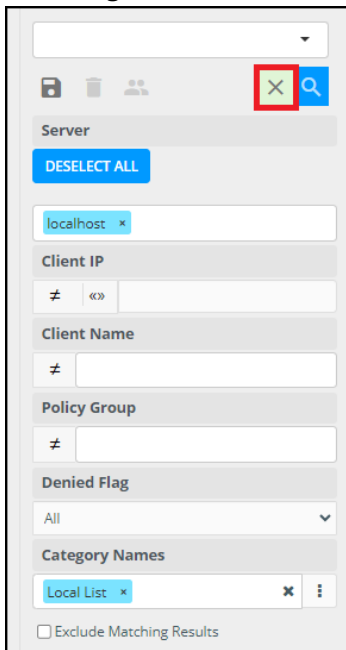
Added Entry 'pinterest.com' to List 'testlist'

ID	Locked	URL/Keyword	Type	Request Part	Action	Last Reviewed	Reviewed By	Date Created	Created By
1069	☐	pinterest.com	URL	URL	Deny			Sep 12, 2024 11:44:23	admin

Showing 1 to 1 of 1

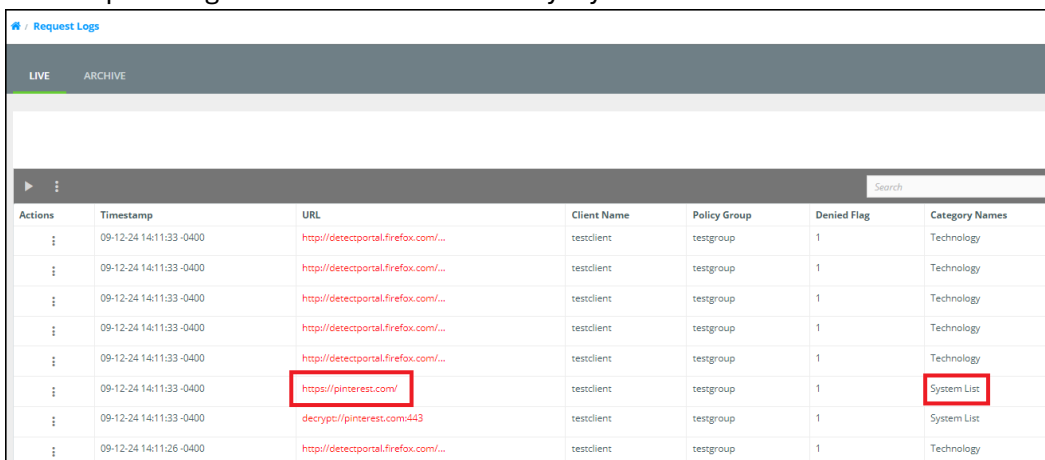
In Your WebAdmin:

1. Navigate to Logs > Request Logs.
2. Clear the Advanced Filter from the earlier procedure by expanding the Filter pane and selecting the **X** button.



The screenshot shows the 'Filter' pane in the WebAdmin interface. It includes fields for 'Server' (with a 'DESELECT ALL' button), 'Client IP', 'Client Name', 'Policy Group', 'Denied Flag', and 'Category Names'. The 'Category Names' field is set to 'Local List'. A red box highlights the 'X' button used to clear the filters.

3. Browse to *pinterest.com* on Your Test Workstation. The intended webpage will be unreachable.
4. The 'Request Logs' shows that it is denied by 'System List'.



Request Logs						
LIVE ARCHIVE						
Search						
Actions	Timestamp	URL	Client Name	Policy Group	Denied Flag	Category Names
⋮	09-12-24 14:11:33 -0400	http://detectportal.firefox.com/...	testclient	testgroup	1	Technology
⋮	09-12-24 14:11:33 -0400	http://detectportal.firefox.com/...	testclient	testgroup	1	Technology
⋮	09-12-24 14:11:33 -0400	http://detectportal.firefox.com/...	testclient	testgroup	1	Technology
⋮	09-12-24 14:11:33 -0400	http://detectportal.firefox.com/...	testclient	testgroup	1	Technology
⋮	09-12-24 14:11:33 -0400	http://detectportal.firefox.com/...	testclient	testgroup	1	Technology
⋮	09-12-24 14:11:33 -0400	https://pinterest.com/	testclient	testgroup	1	System List
⋮	09-12-24 14:11:33 -0400	decrypt/pinterest.com:443	testclient	testgroup	1	System List
⋮	09-12-24 14:11:26 -0400	http://detectportal.firefox.com/...	testclient	testgroup	1	Technology

Pass Criteria

Using the filtered workstation in the 'testgroup' group, browsing to a URL in the 'testlist' assigned to the System Deny List will **not** be reachable.

This occurs even though *pinterest.com* is allowed in the 'testgroup' Group's Policy Local List due to the Policy Service's List Processing order. The System Wide List will always take precedence over Local Lists.

Notes	Policy Events are granular on a per-minute-basis.
Results (Pass or Fail)	
Results Comments	

Importing a System List

Purpose

The Netsweeper solution provides functionality for importing long System Lists (allow and deny.) Typically, these lists come from an external list (CSV file, spread sheet, etc.). This test case verifies the system list import feature.

Precondition

See: Setting up Filtering Group and Client

Additional Precondition 1: Adding a Test List

1. Navigate to Policies > Lists and select the **Create** button.
2. Type 'importlist' into the 'List Name' field.
3. Select the checkbox for **System Wide List** in the 'List Assignments' section.
4. Select the **Create List** button.

The screenshot shows the 'New List' configuration interface. The 'List Name' field contains 'importlist'. Under 'List Assignments', the 'System Wide List' checkbox is checked. Other options like 'Category List', 'Suggest List', 'Filter Bypass List', and 'Override Category List' are unchecked. The 'List Service Enabled' checkbox is also unchecked. The 'List Service Interval (seconds)' is set to 0. The 'List Service Next Run Time' is set to 'Next Run Time: 2024-02-16 10:00:00'. The 'Restrictions' section is expanded, showing various options for 'Restrict Actions', 'Restrict Types', and 'Restrict Request Parts'. The 'Assigned Categories' field is empty. At the bottom, there are buttons for 'Add SYSP', 'Add SYSP DEFAULTS', 'REMOVE ALL SYSP PERMISSIONS', and 'CREATE LIST'.

Additional Precondition 2: Creating a URL Import List

- You can download the systemlisttest.csv as a zip file from this source:

https://helpdesk.netsweeper.com/docs/UAT/8_2_Resources/User_Acceptance_Resource_8.2_Page.html

- Alternatively, you can create your own .csv document by adding the content shown below.

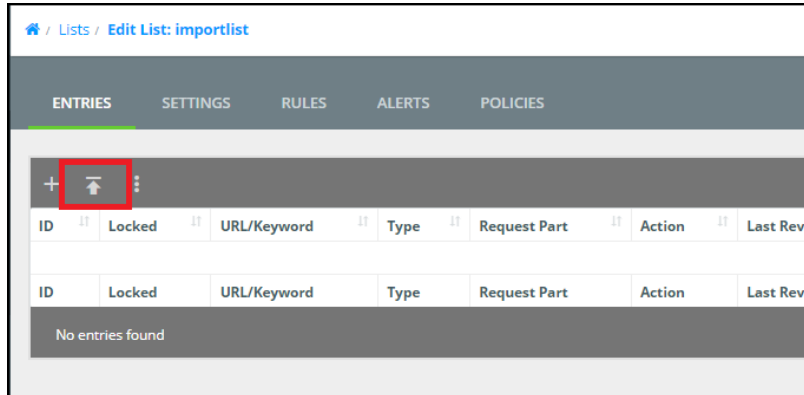
URL/Keyword	Type	Action	Action Arguments	Comments	Case Insensitive	Request Part
http://paypal.com	U	D			0	U
http://pinterest.com	U	A			0	U

- Save the file as systemlisttest.csv. Use the UTF-16LE format.
- Please verify that no other Lists contain either of those URLs.

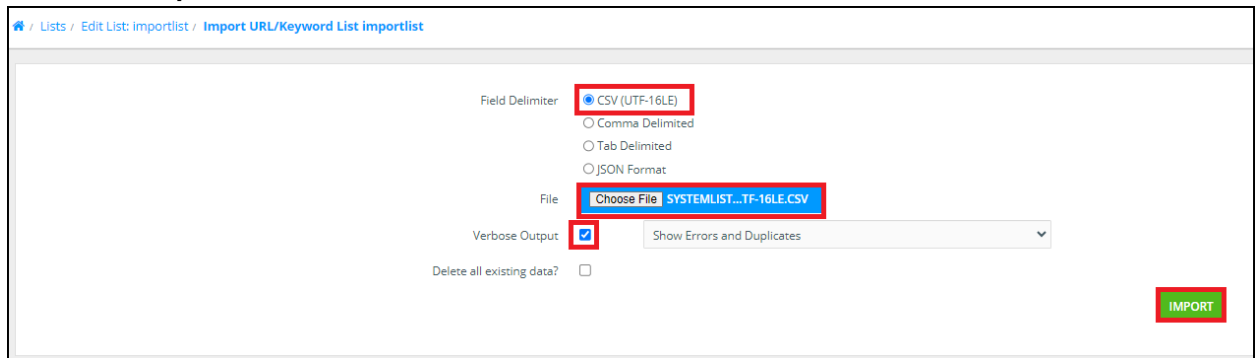
Test Procedure: Importing a System List

In the WebAdmin:

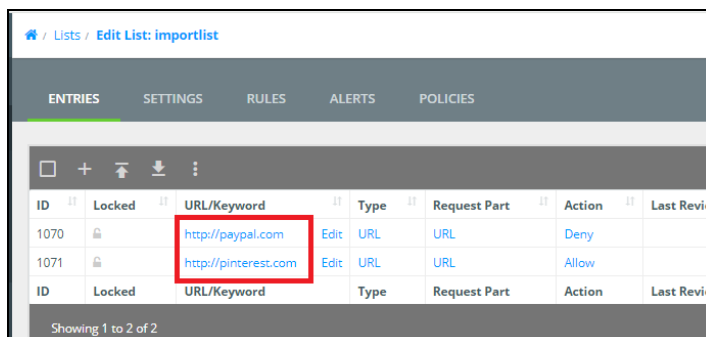
1. Navigate to Policies > Lists and select the **Lists** tab.
2. Choose the 'importlist' we created previously.
3. Select the **Import** button.



4. In the 'Import URL/Keyword List' window, leave the **Field Delimiter** set to 'CSV (UTF-16LE)'
5. Select the **Choose File** button and add your newly downloaded (or created) file.
6. Select the checkbox for **Verbose Output**.
7. Select the **Import** button.



8. On page 2 of the 'Import URL/Keyword List' window, select **Import** again.
9. The file imports. You will see the message:
"Imported File systemlisttestUTF-16LE.csv of size 646 bytes into URL/Keyword List importlist. 2 of 2 entries were added."
10. Select the **Continue** button to return to the 'Edit List' window.
11. You will see the two new entries listed.



- 12. Navigate to Tools > Trace Request.
- 13. In the URL field, enter:
`http://paypal.com`
- 14. Select the **Send Request** button.
- 15. Policy Server results should state that request was ‘Denied’ at the System Lists Lookup Step. The name of the List (Importlist) that denied the request is also listed.

Trace Request

Client Name

Client IP Address

Group Name

Policy Name

BROWSER IP

URL

Destination IP Address

User Agent

Referrer

Client Module Name

Event Type

http://paypal.com

Check Policy

Show All Steps

SEND REQUEST

Policy Server: localhost (127.0.0.1)

Step	List URL/Keyword	Result
System Lists Lookup	http://paypal.com from "importlist"	Category: System List Decision: Denied
Response URL Test		Category: Host is an IP Replace URL: https://192.168.222.150/webadmin...
Filter Bypass List Lookup	https://192.168.222.150	Category: Filter Bypass List, Host is an IP Decision: Allowed

Pass Criteria

- Request for http://paypal.com, you should be blocked.
- Request for http://pinterest.com, you should not be blocked.

Notes	You can also view the various lists in the Lists window and see that the URLs have been added.
Results (Pass or Fail)	
Results Comments	

Clients

Clients Identified by Subnet

Purpose

The Netsweeper solution enables clients to be identified using a subnet. This test verifies that a client can be identified by a subnet and receive the expected filtering policy.

Precondition

See: Setting up Filtering Group and Client

A filtered Client workstation must be available for browsing the Internet and the IP address of the filtered workstation should be within a known network subnet.

A second filtered client workstation must be available for browsing the Internet and the IP address of the filtered workstation should be within a second network subnet.

Test Procedure: Clients Identified by Subnet

In The WebAdmin:

1. Navigate to Policies > Groups, choose the **List** tab and select the **Create** button.
2. Type 'lockdown' for the 'Group Name' and select the **Submit** button.
3. Select the **Policies** tab and the **List** sub-tab.
4. Choose the **default** policy.
5. Navigate to the Policy's Categories tab.
6. Choose the Custom Category Template and place a checkmark beside all Category groups to select all available Categories.

The screenshot shows the 'Categories' tab in the Netsweeper WebAdmin. The breadcrumb trail is: Groups / Group Create / Group lockdown / Policy default in lockdown. There are 'CLONE' and 'SURF' buttons at the top. Below are tabs: GENERAL, CATEGORIES (active), URL/KEYWORD SHARED LISTS, URL/KEYWORD LOCAL LIST, ADVANCED, and DENY PAGE. On the left, a dropdown menu shows 'Custom' selected. Below it, a list of blocked categories is shown, including '1166 Blocked', '888 Poker and Casino', 'Abortions', 'Ad Blocking', 'Adult Mixed Content', 'Advertising', 'Adware', and 'Afghanistan'. On the right, a table lists categories with checkboxes and counts:

Category	Count	Selected
Countries	255/255	☒
Mobile Apps	30/30	☒
Protocols	60/60	☒
System	12/12	☒
Web Apps	720/720	☒
Web Content	89/89	☒
Adult	29/29	☒
Information	22/22	☒
Miscellaneous	14/14	☒
Recreation	8/8	☒
Security	16/16	☒

At the bottom, there is a dropdown menu with the text 'Update this policy 'default' in group 'lockdown'.' and a red 'SUBMIT' button.

7. Select the **Submit** button to save your changes.

8. Select the **Group lockdown** breadcrumb and then the **Clients** tab.
9. Select the Create button.
10. In the 'Client Type' section, choose the **Network Subnet** option.
11. In the 'Client Name' section, type Client1
12. In the 'IP Address or IP Range' field type: 192.168.4.0
13. In the 'Subnet Mask' field type: 255.255.255.224

Locked ☐

Group **lockdown**

Expire

Client Type

Authorized By Client Name ☐

Workstation Address ☐

Network Subnet ☒

Client Settings

Client Name: **client1**

IP Address or IP Range: **192.168.4.0**

Subnet Mask: **255.255.255.224**

Workstation Name:

First Name:

Last Name:

Email Address:

Comments:

SUBMIT

14. Select **Submit**.
15. Navigate to Policies Groups and select the **List** tab.
16. Select the **default** Group and then the Clients tab.
17. Select the **Create** button.
18. In the 'Client Type' section, choose the **Network Subnet** option.
19. In the 'Client Name' section, type Client2
20. In the 'IP Address' field enter an IP Address range that is within 192.168.4.31-192.168.4.245.
21. Select **Submit**.
22. Navigate to Policies > Clients to verify the two new Clients and their respective IP information.

On the Test Workstations:

1. Using the filtered workstation of an IP that is in the range of the subnet for **client1**, browse to http://www.any_url.com (Where any_url.com represents the HTTP URL request of your choice). You should be blocked as **client1** that is a member of a group lockdown.
2. Using the filtered workstation of an IP that is OUTSIDE of the subnet range of **client1**, browse to <http://www.example.com>. (Where example.com in this case represent the HTTP URL which would be usually allowed by the filtering group). Your URL request should not be blocked.

Pass Criteria

Using the filtered workstation in the **client1**, browse to http://www.any_url.com/. You should be blocked.

Using the filtered workstation in the **client2**, browse to <http://www.example.com/> (Where example.com in this case represents the HTTP URL which would be usually allowed by the filtering group). You should **not** be blocked.

Notes	
Results (Pass or Fail)	
Results Comments	

Accounts Window

SysOp Permissions

Purpose:

The Netsweeper solution provides permissions that can be enabled or disabled for each SysOp account. This test case will verify a portion of the capabilities provided by the permissions feature in the WebAdmin.

Precondition:

SysOp Permissions

Create testsysop1:

In The WebAdmin:

1. Navigate to Accounts > Accounts and select the **Create** button.
2. Choose the **Advanced** tab.
3. Enter the Login Name testsysop1 and testorganization in the Organization field.
4. Enter and confirm a password, 'Netsweeper1' and choose **Sysop** as the 'Classification'.
5. Check the box marked **Create Account Group Policy**.

The screenshot shows the 'Account Create' form in the WebAdmin interface. The 'Advanced' tab is selected. The form contains the following fields and options:

- Login Name:** testsysop (highlighted with a red box)
- First Name:** First Name
- Last Name:** Last Name
- Email Address:** Email
- Organization:** testorganization (highlighted with a red box)
- Description:** Description
- No Password:** ☐
- Account Password:** [masked] (highlighted with a red box)
- Verify Password:** [masked] (highlighted with a red box)
- Classification:** ☒ Sysop (highlighted with a red box), ☐ Admin, ☐ User
- Account Templates:** Select Account Templates
- Expiry:** YYYY-MM-DD HHMM:SS
- Web Admin Theme:** Global Web Admin Theme
- Create account group policy:** ☒ (highlighted with a red box)
- Assign to all managed groups:** ☐
- Change password on login:** ☐
- Enforced Categories:** ☒ Use system-wide categories, ☐ Override system-wide categories

Fields with asterisks (*) are required.

SUBMIT

6. Select **Submit**. You are returned to the 'Accounts' window.

Assign Permissions:

1. Select **testsysop1** to open the 'Edit Account' window.
2. Select the **Permissions** tab.
3. Place checkmarks beside the **Policy** and **List** Permission Groupings shown here:

The screenshot shows the 'Edit Account testsysop' window with the 'PERMISSIONS' tab selected. The 'Account Templates' section is at the top. Below it, there are tabs for 'EDIT' and 'LIST'. A row of buttons includes 'IMPORT', 'EXPORT', 'DEFAULT ACCESS', 'SELECT ALL', 'DESELECT ALL', 'EXPAND ALL', and 'COLLAPSE ALL'. The main area is a list of permission categories with checkboxes. The following categories are checked: 'Policy General', 'Policy Advanced', 'List General', and 'List Admin'. Other categories like 'Group Interfaces', 'Group General', 'Group Advanced', 'Group Admin', 'Client General', 'Client Advanced', 'Account General', 'Account Advanced', 'Account Admin', 'Tools', 'Client Filter Settings', 'Logs General', 'Logs Admin', 'Reports', 'Directory Sync', and 'Organization' are unchecked. A 'SUBMIT' button is located at the bottom right of the list.

4. Select **Submit** and confirm the modification by choosing **OK** on the warning window. The 'Account Permissions Updated' message displays.

Create testsysop2:

1. Navigate to Accounts > Accounts.
2. Select the **Create Advanced** tab.
3. Enter the Login Name testsysop2.
4. Enter testorganization in the 'Organization' field.
5. Enter and confirm a password, Netsweeper1.
6. Choose **Sysop** as the 'Classification'.
7. Check the box marked **Create Account Group Policy**.
8. Select Submit. You are returned to the Accounts window.

Modify testsysop2 Permissions:

1. Select the **testsysop2** Account to open the 'Edit Account' window.
2. Select the **Permissions** tab.
3. Enable **Policy General > Policies** permission only. Do not enable any other permissions.
4. Select **Submit** and confirm the modification by choosing **OK** on the warning window. The 'Account Permissions Updated' message displays.

Test Procedure: SysOp Permissions

Testsysop1

1. Login as testsysop1 with the password Netsweeper1.
2. Navigate to Policies > Policies.
3. Choose the **default** Policy.
4. Select the **URL/Keyword Local List** tab.
5. You can see the **Create** button.
6. In the Policies menu you can also see the Lists window (Policies > Lists).

Testsysop2

1. Login as testsysop2 with the password Netsweeper1.
2. Navigate to Policies > Policies.
3. Choose the **default** Policy.
4. Select the **URL/Keyword Local List** tab.
5. You can **not** see the **Create** button.
6. In the Policies menu you can **not** see the Lists window (Policies > Lists).

Pass Criteria

For the testsysop1, the button to create a Local List on a Policy is enabled and the 'Lists' menu is a menu option under 'Policies'.

For the testsysop2, the button to create a Local List on a Policy is not visible and the 'Lists' option is not a menu option under 'Policies'.

Notes	
Results (Pass or Fail)	
Results Comments	

Delegated Administration

Purpose

The Netsweeper solution provides functionality that enables the delegation of policy management for specific groups to specific sysop accounts. This test case will verify that sysop roles can be partitioned with control over specific groups of browsing users.

Preconditions

This functionality can be verified out of the box.

Test Procedure: Delegated Administration

In the WebAdmin:

1. Navigate to Accounts > Accounts and choose the **testsysop1** Account we created previously.
2. Select the **Permissions** tab.
3. Choose the **Deselect All** button to remove all previously granted permissions.
4. Enable all Group, Policy, and Client permission-groupings; except Group Admin.

The screenshot shows the Netsweeper WebAdmin interface for the 'testsysop1' account. The 'PERMISSIONS' tab is selected, displaying a list of permissions. The 'Deselect All' button is highlighted. The list includes Group Interfaces, Group General, Group Advanced, Group Admin, Policy General, Policy Advanced, Client General, Client Advanced, Account General, Account Advanced, Account Admin, Tools, Client Filter Settings, List General, List Admin, Logs General, Logs Admin, Reports, Directory Sync, and Organization. A green SUBMIT button is at the bottom right.

- 5.
6. Select **Submit** and then select **OK** when prompted.

Assume Identity: sysop1

1. Select the **Assume Identity** tab.
2. As testsysop1, navigate to Policies > Groups and select the **List** tab.
3. Choose the **testsysop1** Group.
4. Select the **Clients** tab and then the **Create** button.
5. Enter testclient in the 'Client Name' field and select **Submit**. The client is added.
6. Use the special breadcrumb at the top of the window to exit 'Assume Identity'.

You are logged in as 'testsysop1'. To return to the account you assumed identity from, click [here](#)

Pass Criteria

The testsysop Account should have a restricted view in the WebAdmin and only buttons related to Group, Policy and Client Management should display.

The Groups and Policies windows should display only testsysop1 Group and the Policy(s) for that group.

Notes	
Results (Pass or Fail)	
Results Comments	

Categories

Creating and Using Custom Categories

Purpose

In some circumstances, it may be required to assign a number of specific web sites to a category not existing in standard set of Netsweeper categories (e.g. 'News Sites').

Custom categories function exactly like any other category in that they can be denied or allowed and the Category name appears in Deny Pages, Request Logs, Reports, etc.

This test verifies the ability to create and use custom categories.

NOTE: This test has been broken into five procedures.

Precondition

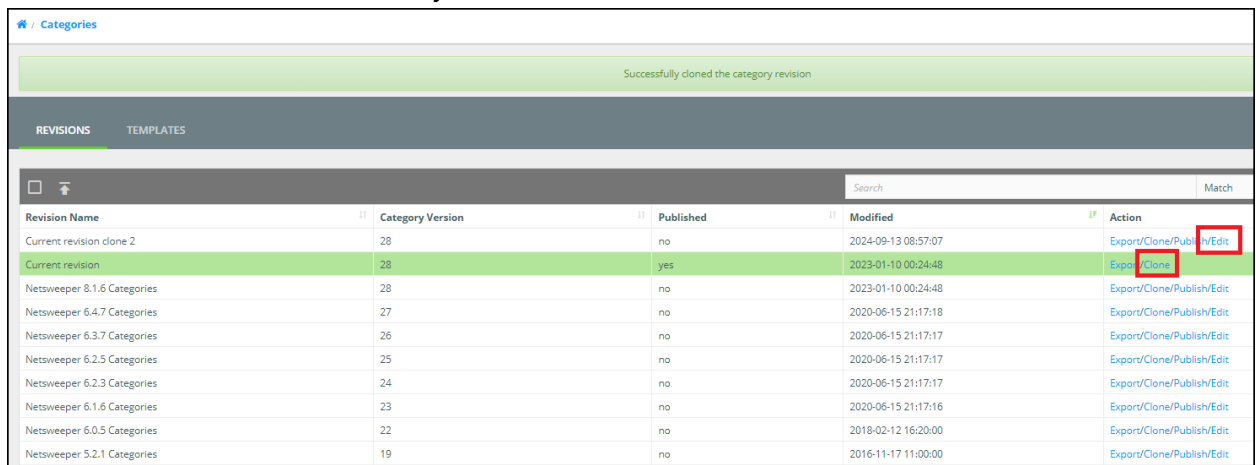
See: Setting up Filtering Group and Client

Only the Category Deny List should be filtered.

Test Procedure 1: Creating a Custom Category

In the WebAdmin:

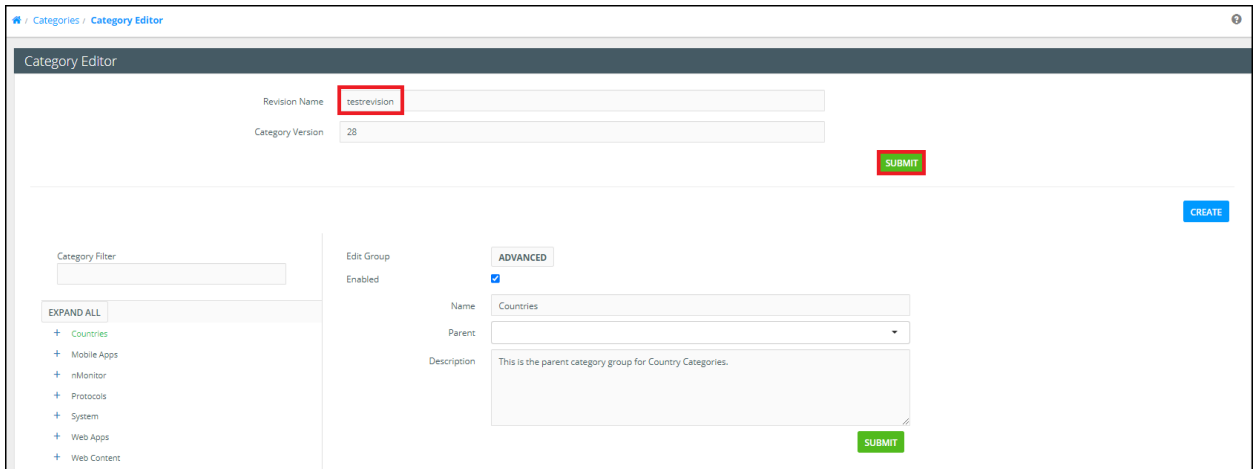
1. Navigate to Administration > Categories.
2. Select the **Clone** button in the Action column for the Current Revision.
3. Select the Edit button for the newly cloned Revision.



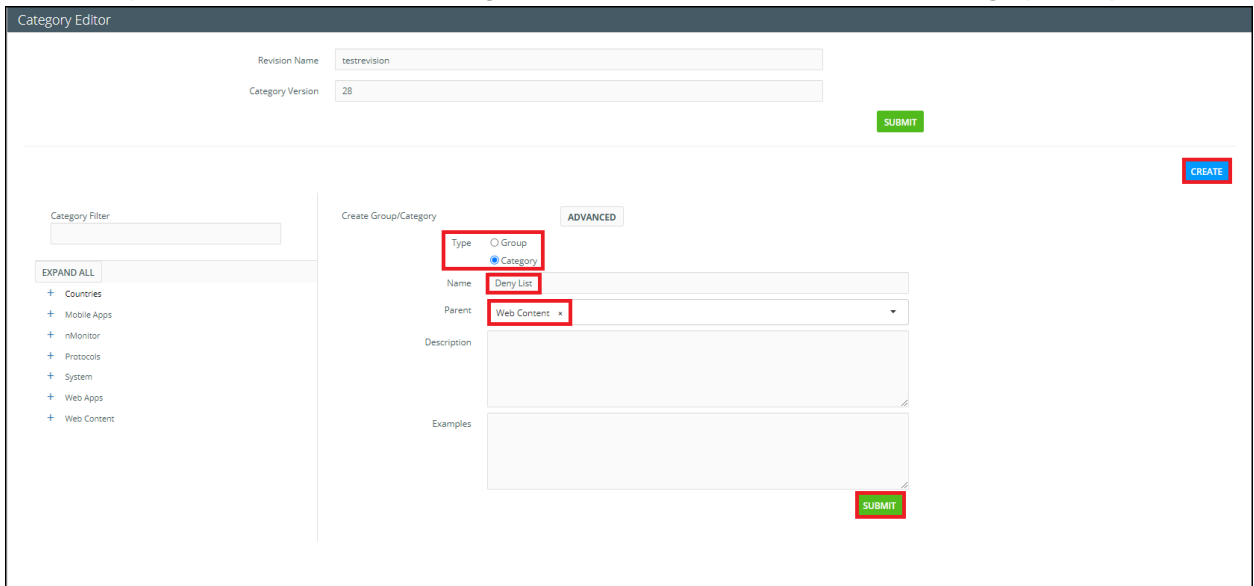
The screenshot shows the 'Categories' page in the Netsweeper WebAdmin. At the top, a green banner displays the message 'Successfully cloned the category revision'. Below this, there are tabs for 'REVISIONS' and 'TEMPLATES'. A table lists various category revisions. The 'Current revision' is highlighted in green. In the 'Action' column for the 'Current revision', the 'Clone' button is highlighted with a red box. Another 'Clone' button is visible in the 'Action' column for 'Current revision clone 2', also highlighted with a red box. The table includes columns for Revision Name, Category Version, Published status, Modified date, and Action.

Revision Name	Category Version	Published	Modified	Action
Current revision clone 2	28	no	2024-09-13 08:57:07	Export/Clone/Publish/Edit
Current revision	28	yes	2023-01-10 00:24:48	Export/Clone/Publish/Edit
Netsweeper 8.1.6 Categories	28	no	2023-01-10 00:24:48	Export/Clone/Publish/Edit
Netsweeper 6.4.7 Categories	27	no	2020-06-15 21:17:18	Export/Clone/Publish/Edit
Netsweeper 6.3.7 Categories	26	no	2020-06-15 21:17:17	Export/Clone/Publish/Edit
Netsweeper 6.2.5 Categories	25	no	2020-06-15 21:17:17	Export/Clone/Publish/Edit
Netsweeper 6.2.3 Categories	24	no	2020-06-15 21:17:17	Export/Clone/Publish/Edit
Netsweeper 6.1.6 Categories	23	no	2020-06-15 21:17:16	Export/Clone/Publish/Edit
Netsweeper 6.0.5 Categories	22	no	2018-02-12 16:20:00	Export/Clone/Publish/Edit
Netsweeper 5.2.1 Categories	19	no	2016-11-17 11:00:00	Export/Clone/Publish/Edit

4. Rename the clone as testrevision and select **Submit**.



5. Select the **Create** button.
6. Choose Category as the 'Type'.
7. Enter Deny List as the 'Name' and assign its 'Parent' as the 'Web Content' Category Group.



8. Select **Submit**. The new Category displays under the 'Web Content' grouping.
9. Use your breadcrumbs to return to the **Categories** window.
10. Choose the **Publish** button beside the testrevision and select **OK** when prompted.

Revision Name	Category Version	Published	Modified	Action
testrevision	28	no	2024-09-13 09:20:52	Export/Clone/Publish/Edit
Current revision	28	yes	2023-01-10 00:24:48	Export/Clone
Netsweeper 8.1.6 Categories	28	no	2023-01-10 00:24:48	Export/Clone/Publish/Edit
Netsweeper 6.4.7 Categories	27	no	2020-06-15 21:17:18	Export/Clone/Publish/Edit

11. The “Successfully published groups and categories in the revision. Successfully restarted reporter(s).” message displays.

Test Procedure 2: Creating and Assigning a Re-Categorization List

1. navigate to Policies > Lists and select the **Create** button.
2. Enter recategorizationlist for this 'List Name'.
3. In the 'List Assignments' section, choose the **Categorization List** option.
4. In the 'Restrictions' section, choose the **Categorize** 'Restrict Action'.

The screenshot shows the 'New List' configuration interface. The 'List Name' field is populated with 'recategorizationlist'. In the 'List Assignments' section, the 'Categorization List' option is selected. The 'Restrictions' section shows 'Categorize' selected under 'Restrict Actions'. The 'Permissions' section at the bottom contains buttons for 'ADD SYSOP', 'ADD SYSOP DEFAULTS', 'REMOVE ALL SYSOP PERMISSIONS', and a green 'CREATE LIST' button.

5. Select the **Create List** button.
6. Use your breadcrumbs to return to the **Lists** window.

Test Procedures 3: Adding New Entries to the List

1. Choose the **recategorization** list from the Lists window.
2. Select the **New Entry** button.
3. Enter facebook.com in the 'New Entry' field.
4. In the 'Categories' section, type and select **Deny List**.

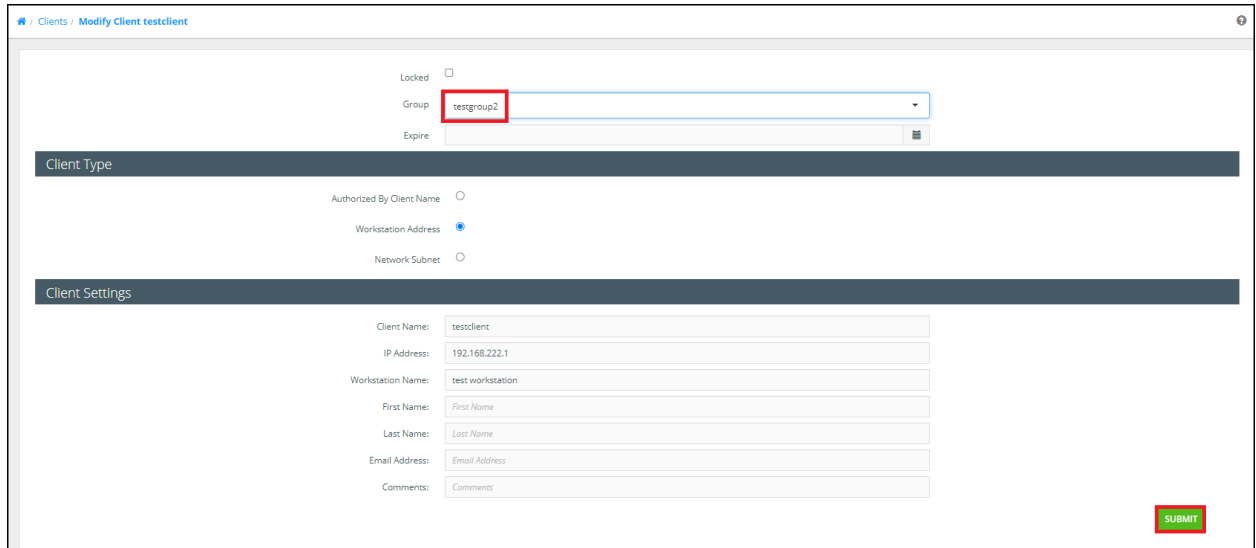
The screenshot shows the 'New Entry' form. The 'New Entry' field contains 'facebook.com'. The 'Entry Type' is set to 'URL'. The 'Request Part' is set to 'Request URL'. In the 'Categories' section, 'Deny List' is selected. The 'Expiry' field is set to 'YYYY-MM-DD HH:MM:SS'. The 'Comments' field is empty. At the bottom, there are buttons for 'RESET FORM', 'CLOSE', and a green 'SAVE ENTRY' button.

5. Select **Save Entry**. The new entry is added.
6. Repeat steps 2-5 for two new URLs of your choice that have not been used previously.

Adding testclient to testgroup2

Earlier we created a Simple Group testgroup2. We will add the testclient to this Group.

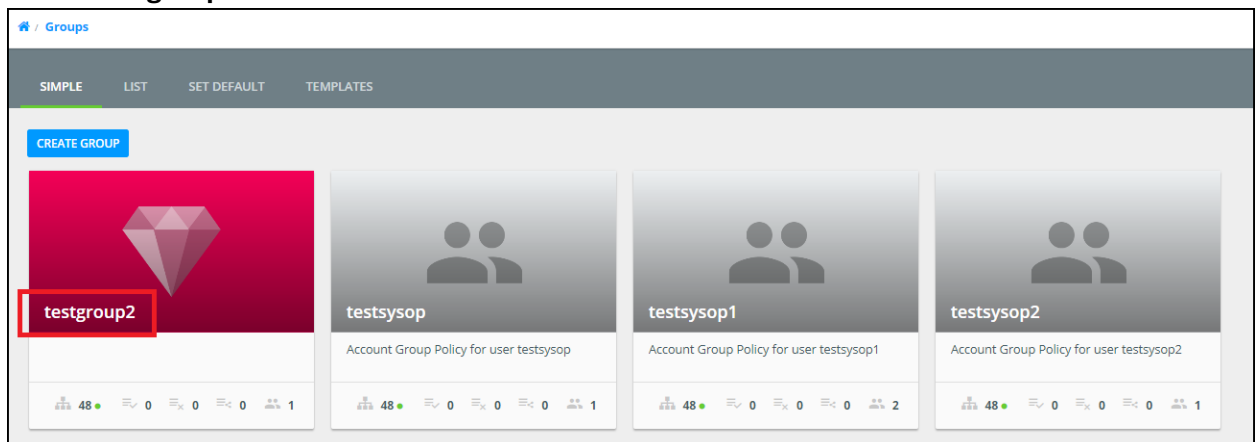
1. Navigate to Policies > Clients.
2. Choose the **testclient** Client.
3. Assign the Client to testgroup2 by choosing it from the **Group** dropdown.



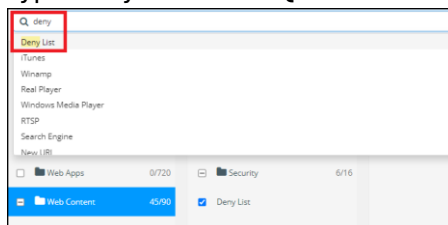
4. Select **Submit**.

Test Procedure 4: Blocking sites for testgroup2

1. Navigate to Policies > Groups and select the **Simple** tab.
2. Chose **testgroup2**.



3. Select the **Categories** tab and Choose **Custom** from the dropdown list.
4. Type Deny List in the 'Quick Add' field and choose it.



5. Select **Submit**. This will block the 'Deny List' category for this Group.

Create a Request Log Filter

We will create a Request Log Filter for the Deny List Custom Category.

1. Navigate to Logs > Request Logs and select the **Advanced Filter** button.
2. Type and select **Deny List** in the Advanced Filter's 'Category Names' field.
3. Select the **Search** button in the Advanced Filter to apply the filter.

The screenshot shows the 'Advanced Filter' interface. At the top, there is a dropdown menu. Below it are icons for save, delete, and share. A 'Search' button is visible. The 'Server' section has a 'DESELECT ALL' button. The 'Client IP' section has a dropdown menu with 'localhost' selected. The 'Client Name' section has a dropdown menu. The 'Policy Group' section has a dropdown menu. The 'Denied Flag' section has a dropdown menu set to 'All'. The 'Category Names' section has a dropdown menu set to 'Deny List'. At the bottom, there is a checkbox for 'Exclude Matching Results'.

Test Procedure 5: Verifying the Custom Categories

On the Test Workstation:

1. With the filtered 'Request Logs' window open, browse the the three URLs you recategorized in the recategorizelist previously.
2. The intended web pages will be unreachable by the filtered test workstation.
3. The three URLs display as denied with the Category Name 'Deny List'.

Pass Criteria

Using the filtered workstation in the testgroup2 Group, browsing each URL assigned to the Deny List Category will not be reachable. In the 'Request Logs' they should appear as denied and categorized as Deny List

Notes	
Results (Pass or Fail)	
Results Comments	

Policies and Categories

Allow Selected Categories – Allow Policy

Purpose

When it is simpler to prohibit web access based on a short list of permitted Categories, Allow List mode is used.

This means that only the selected categories will be allowed, which is the opposite of the standard out of the box ‘Deny List’ mode. This test verifies that ‘Allow List’ mode functions as expected.

Precondition

See: Setting up Filtering Group and Client

Test Procedure: Allow List Mode

In the WebAdmin:

1. Navigate to Policies > Groups, choose the **List** tab and select the **Create** button.
2. Name the new Group testgroup3.
3. Navigate to Tools > Trace Request, select testgroup3 in the Group field and enter guinness.com in the URL field.
4. Select **Send Request** and confirm that guinness.com is denied under the ‘Alcohol’ Category.

Trace Request

Client Name:

Client IP Address: [BROWSER IP](#)

Group Name:

Policy Name:

URL:

Destination IP Address:

User Agent:

Referrer:

Client Module Name:

Event Type:

☐ Show All Steps

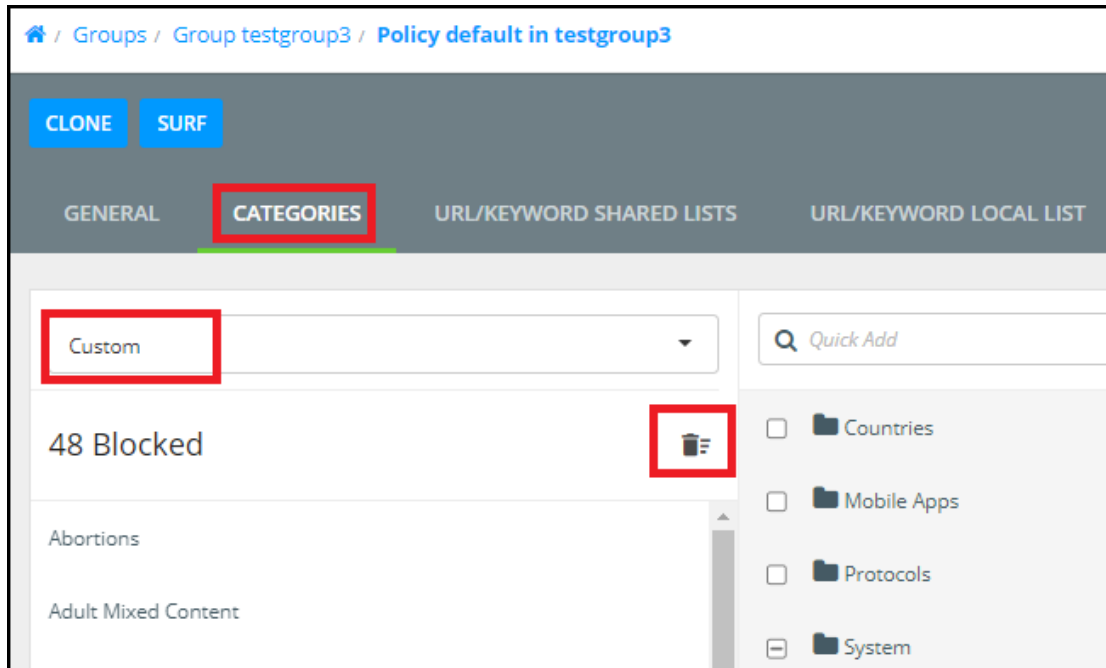
[SEND REQUEST](#)

Policy Server: localhost (127.0.0.1)

Step	List URL/Keyword	Result
Protocol CNS List	http://	Category: Hypertext Transfer
Master List Lookup	guinness.com	Category: Alcohol, Hypertext Transfer
Policy Categories Check		Category: Alcohol, Hypertext Transfer Decision: Denied
Response URL Test		Category: Host is an IP Replace URL: https://192.168.222.150/webadmin...
Filter Bypass List Lookup	https://192.168.222.150	Category: Filter Bypass List, Host is an IP Decision: Allowed

5. Navigate back to testgroup3 and then to their **Policy** tab and **List** subtab.

6. Choose the **default** Policy.
7. In the General tab, choose **Allow** for the 'Category Action' option and select **Submit**.
8. Next, choose the Policy's **Categories** tab, select the **Custom** category template and delete all the selected Categories.



9. In the 'Quick Add' field, type Alcohol and add it to the left pane.
10. Select **Submit**.
11. Repeat the Trace Request in steps 3 and 4 of this section.
12. You will see the 'Alcohol' Category is now allowed.
13. Repeat the Trace Request with the URL google.com.
14. You will see that google.com is denied under the 'Search Engine' Category.

Pass Criteria

Using the testgroup3 in the testgroup3 group, browsing the URL <http://guinness.com> will be reachable but google.com will be denied.

Notes	
Results (Pass or Fail)	
Results Comments	

Category Lookup

CNS Categorization

Purpose

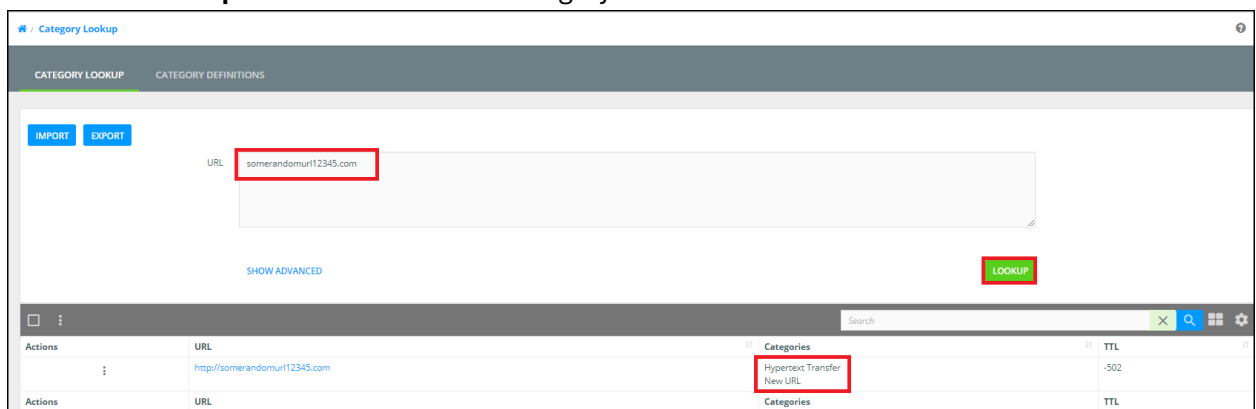
This test verifies that New URLs (not present in any lists or the cache) are categorized first as New URL and then later with a Netsweeper Categorization.

Precondition

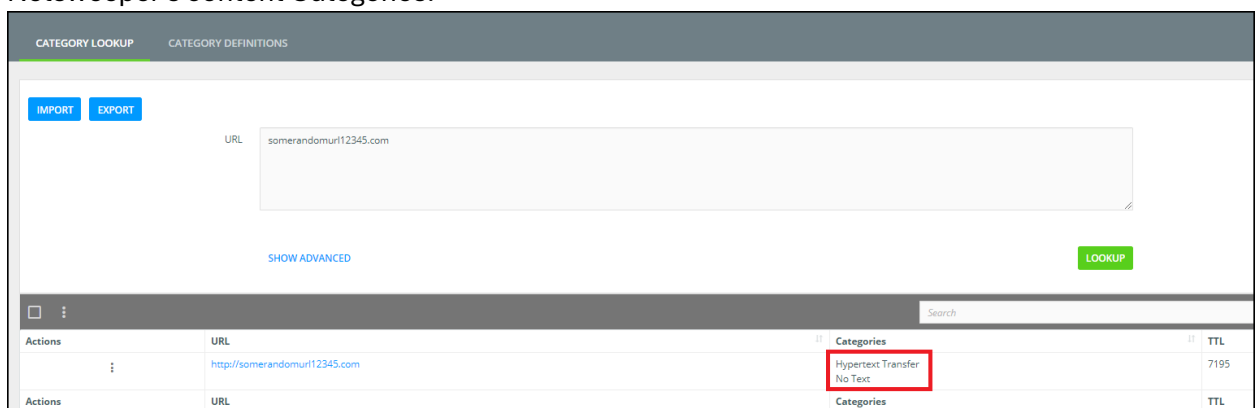
CNS connectivity with your Netsweeper Policy Server.

Test Procedure: CNS Categorization

1. Navigate to Tools > Category Lookup.
2. Enter a completely random “URL” (the goal is to find a string that has never been categorized before, it does not need to be a real URL, it does not need to resolve, etc). Be sure to add ‘.com’ to the end of your “URL.”
3. Select the **Lookup** button and note the Category that is returned.



4. Select the Lookup button again. The Category changes from ‘New URL’ to one of Netsweeper’s content Categories.



Pass Criteria

When the Category Lookup function was tested the first time, the Category will be New URL. (If New URL is not the returned category, you may need to try a different URL). When you use the Category

Lookup function subsequent times, the category will eventually change to a Netsweeper content category. Processing time should average about 2-5 seconds.

Notes	We suggest using random URLs, even if they are not real, because this is a quickest way to find a New URL. Categorization times vary slightly depending on the time of day and the region.
Results (Pass or Fail)	
Results Comments	

List Update

Purpose

This test verifies that all lists on all Policy Servers have been updated to the latest list automatically.

Precondition

No preconditions.

Test Procedure: List Update

In the WebAdmin:

- 1. Navigate to Administration > Status.
- 2. Select the **Lists** tab.

Pass Criteria

Under the Policy Servers list, you should see the list of the configured Policy Servers, list name, list version and last update date. Please note that depending on your serial versions, a Policy Server's Lists may be different.

netsweeper Search Polices Accounts Administration WebAdmin Settings Services Backups Status Monitoring Categories Protocols IPv6 Prefixes Translations Session Settings Security Labels Theme Editor	Status					
	OVERVIEW SERVICES LISTS POLICY SERVERS					
	Policy Server Lists					
	Policy Server	List	Revision	Last Update	Last Update Check	Last Time Loaded
	localhost 127.0.0.1	protocolist	1100	Thu, 04 Jul 2024 16:09:19 -0400	Fri, 13 Sep 2024 15:20:00 -0400	Fri, 13 Sep 2024 13:00:26 -0400
		did	2090100	Mon, 22 Jul 2024 10:15:24 -0400	Fri, 13 Sep 2024 15:20:00 -0400	Fri, 13 Sep 2024 14:41:03 -0400
		safeearchlist	1100	Thu, 04 Jul 2024 16:09:20 -0400	Fri, 13 Sep 2024 15:20:00 -0400	Fri, 13 Sep 2024 14:41:04 -0400
		embeddedurlist	1100	Thu, 04 Jul 2024 16:09:08 -0400	Fri, 13 Sep 2024 15:20:00 -0400	Fri, 13 Sep 2024 14:41:04 -0400
		protocolmslist	1100	Thu, 04 Jul 2024 16:09:18 -0400	Fri, 13 Sep 2024 15:20:00 -0400	Fri, 13 Sep 2024 13:00:26 -0400
		cnseelist	1100	Thu, 04 Jul 2024 16:09:07 -0400	Fri, 13 Sep 2024 15:20:00 -0400	Fri, 13 Sep 2024 14:41:03 -0400
		geoplist	1100	Thu, 04 Jul 2024 16:09:10 -0400	Fri, 13 Sep 2024 15:20:00 -0400	Fri, 13 Sep 2024 13:00:26 -0400
		preemptivelist	19886100	Fri, 13 Sep 2024 12:20:17 -0400	Fri, 13 Sep 2024 15:20:00 -0400	Fri, 13 Sep 2024 13:00:26 -0400
		suggestlist	19783100	Thu, 12 Sep 2024 16:20:25 -0400	Fri, 13 Sep 2024 15:20:00 -0400	Fri, 13 Sep 2024 14:41:04 -0400
		masterlist	19942100	Fri, 13 Sep 2024 13:00:15 -0400	Fri, 13 Sep 2024 15:20:00 -0400	Fri, 13 Sep 2024 13:00:34 -0400
	rsprotyfusscan			1100	Thu, 04 Jul 2024 16:09:17 -0400	Fri, 13 Sep 2024 15:20:00 -0400
	Service Start Time :			Fri, 13 Sep 2024 08:16:31 -0400		
	Last Check :			1 sec ago		

Notes	
Results (Pass or Fail)	
Results Comments	

Centralized Management

Purpose

This test verifies that any policy modification done on the management server is replicated on all policy servers.

Precondition

Out-of-the-box functionality with filtering enabled.

Test Procedure

In the WebAdmin:

1. Navigate to Policies > Lists.
2. Choose the **System Deny List**.
3. Select the **New Entry** button.
4. Add test-globaldeny.com to the System Deny List.
5. Select **Save Entry**.
6. Navigate to Tools > Trace Request.
7. In the URL field, enter http://test-globaldeny.com and select **Send Request**.

The screenshot shows the 'Trace Request' interface. At the top, there are dropdown menus for Client Name, Client IP Address, Group Name, and Policy Name, along with a 'BROWSE IP' button. Below these are input fields for URL (containing 'http://test-globaldeny.com'), Destination IP Address, User Agent, Referrer, Client Module Name, and Event Type (set to 'Check Policy'). A 'SEND REQUEST' button is at the bottom right. Below the form is a table showing the results of the trace request.

Step	List URL/Keyword	Result
System Lists Lookup	test-globaldeny.com from "System Deny List"	Category: System List Decision: Denied
Response URL Test		Category: Host is an IP Replace URL: https://192.168.222.150/webadmin...
Filter Bypass List Lookup	https://192.168.222.150	Category: Filter Bypass List, Host is an IP Decision: Allowed

Pass Criteria

In the output, you will find that all Policy Server's Category decisions are that it is System List Denied.

Using the WebAdmin to run a Trace Request, test a URL assigned to the System Deny List and it will be Denied at the System Lists Lookup Step.

Notes	
Results (Pass or Fail)	
Results Comments	

Testing Connections and Access

Verify SSH Login

Purpose

This test verifies ability to login using SSH to Netsweeper servers.

Precondition

Network connectivity and no firewall blocking port 60104.

Test Procedure

Use any SSH client and try to login to any Netsweeper server, use port 60104. Default username is admin and password is netsweeper.

Pass Criteria

SSH Client will be able to login to the Netsweeper system.

Notes	
Results (Pass or Fail)	
Results Comments	

Boundary Tests

URL List Import Limit

Purpose

The Netsweeper solution provides functionality for importing long System Lists (allow and deny.) Typically, these lists come from an external list (CSV file, spread sheet, etc.).

This test case verifies the system list import feature can handle up to 600,000 entries.

Test Configuration

The Netsweeper solution must be deployed so that it can route RST packets to both the filtered workstation and the web server.

A filtered client workstation must be available for browsing the internet.

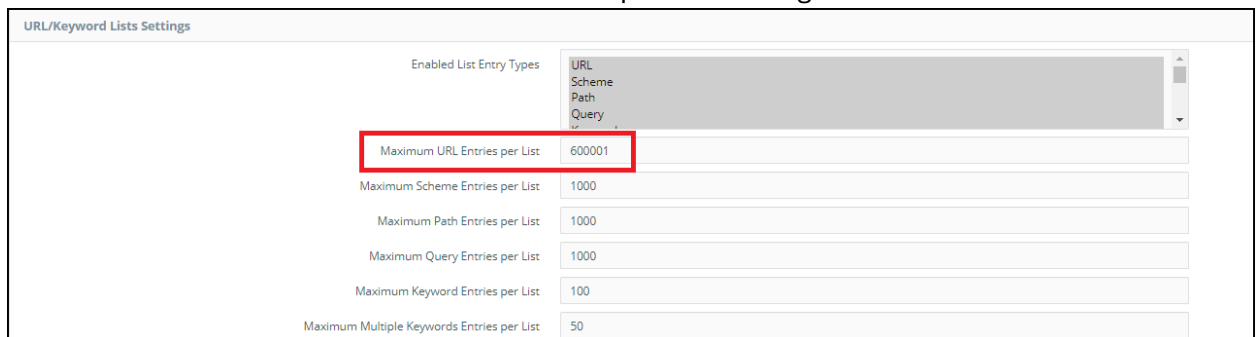
NOTE: RESET POL DB & RECREATE PIC/TEXT WAS HERE

You will require the Netsweeper 600000 URL Import.csv file. The zip file can be downloaded from here:

https://helpdesk.netsweeper.com/docs/UAT/8_1_Resources/User_Acceptance_Resource_8.1_Page.html

Modifying WebAdmin Settings

1. Navigate to Administration > WebAdmin Settings.
2. Scroll down to the 'URL/Keyword List Settings' section.
3. Increase the value for the 'Maximum URL Entries per List' setting to 600001.



URL/Keyword Lists Settings	
Enabled List Entry Types	URL Scheme Path Query
Maximum URL Entries per List	600001
Maximum Scheme Entries per List	1000
Maximum Path Entries per List	1000
Maximum Query Entries per List	1000
Maximum Keyword Entries per List	100
Maximum Multiple Keywords Entries per List	50

4. Select **Submit** to apply your changes.

De-Select all Categories for testgroup3

1. Navigate to Policies > Groups, choose the **List** tab select **testgroup3**.
2. Go to the Group's **Policies** tab and then the **List** subtab.
3. Select the **default** Policy.
4. In the **Categories** tab, select the 'None' Category Template.
5. Select **Submit**.

Test Procedure: URL List Import Limit

In the WebAdmin:

1. Navigate to Policies > Lists.
2. Select the **Create** button.
3. Enter **Deny List** into the 'List Name' field.
4. Choose the **System Wide List** option from the 'List Assignments' section.
5. Select the **Deny** checkbox in the 'Restrict Actions' section.
6. Select the **Create List** button.

Importing a List:

1. Choose the **Deny List** from the 'Lists' window.
2. Select the **Import** button.
3. Select the **Choose File** button and add the 'Netsweeper4-600000_URL_Import-UTF-16LE.csv' file.
4. Select the **Import** button. The 'Import URL / Keyword List' window displays.
5. Select Import again. The list will import. (This can take some time).
6. Once the import is complete you will receive the message:
'Imported File Netsweeper4- 600000 URL Import.csv of size 38177763 bytes into URL/Keyword List "Deny List". 600000 of 600000 entries were added.'
7. Select **Continue** and then use your breadcrumbs to return to the **Lists** window.
8. Ensure that the 'Entries' column for the Deny List shows '600000'.

Test Procedure: Verifying the Deny List with Trace Request.

In the WebAdmin:

1. Navigate to Tools > Trace Request.
2. Select the 'Group Name' field and choose **testgroup3**.
3. In the 'URL' field, type http://facebook.com and select **Send Request**.
4. Policy Server results should state that request was 'Allowed' since URL entry was not on the list that we just imported.
5. Leave Group Name untouched, Clear the URL field and enter: http://sex.com and **Send Request**.
6. Policy Server results should state that request was 'Denied' as this URL entry was in the list that we imported.

Pass Criteria

You should be denied and allowed as expected. You can also view the various lists in the Lists window and see that the URLs have been added.

Notes	
Results (Pass or Fail)	
Results Comments	

Request Loggin and Reporting

Creating a Detailed Demand Report

Purpose

The Netsweeper solution can log every URL requested, along with some subscriber and category information, if configured to do so. Every URL requested by a filtered workstation will be logged. This test verifies that the Netsweeper filtering platform logs all subscribers' browsing activity.

Precondition

See 'Preconditions - Setup Filtering, Groups and Clients'

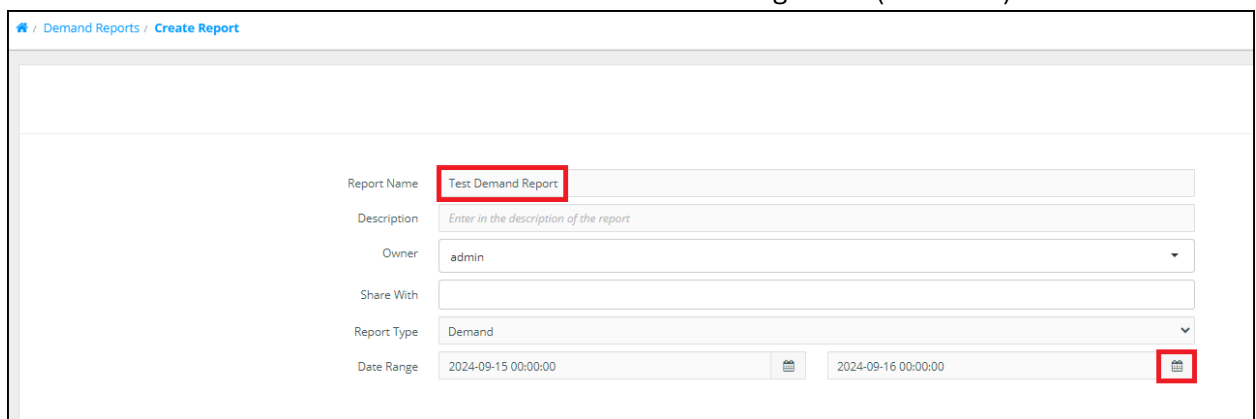
Test Procedure

On the Test Workstation:

Generate some web traffic to be logged by your Policy Server. This can be achieved by surfing any webpage online.

In the WebAdmin:

1. Navigate to Reports > Demand Reports and select the Create Report button.
2. In the 'Report Name' field, enter **Test Demand Report**.
3. Select the Calendar button for the 'end-date' in the 'Date Range' field (as shown).



4. Use the calendar to set the 'date' value to tomorrow's date and select **OK**.

5. Next, select the **Add Filter** button.

The screenshot shows a report configuration interface. At the top, there are fields for 'Report Name' (Test Demand Report), 'Description' (Enter in the description of the report), 'Owner' (admin), 'Share With', 'Report Type' (Demand), and 'Date Range' (2024-09-16 00:00:00 to 2024-09-17 00:00:00). Below these fields, there are three sections: 'Filters', 'Report Output', and 'Delivery Options'. The 'Filters' section is expanded, showing an 'ADD FILTER' button highlighted with a red rectangle, and a 'LOAD FILTERS' link. The 'Report Output' section is also expanded, showing three options: 'ADD SUMMARY GROUP', 'ADD TOP ESTIMATION', and 'ADD REPORT DETAILS'. The 'Delivery Options' section is collapsed.

6. Set the 'Field' value to **Client Name**, leave the 'Condition' set to **Equal To**, and in the 'Value' field, choose the **testclient** associated with your test workstation.

The screenshot shows the 'Add Filter' dialog box. It has a title bar with a close button (X). Inside, there are three dropdown menus: 'Field' (Client Name), 'Condition' (Equal To), and 'Value' (testclient). Below the dropdowns, there is a blue link 'ADD CONDITION'. At the bottom right, there are two buttons: 'CANCEL' and 'SAVE'.

7. Select **Save** to apply the Filter.

8. Next, Select the **Add Report Details** option for the Report Output section.

Report Name: Test Demand Report

Description: Enter in the description of the report

Owner: admin

Share With:

Report Type: Demand

Date Range: 2024-09-16 00:00:00 to 2024-09-17 00:00:00

▼ Filters

[ADD FILTER](#)

[LOAD FILTERS](#)

▼ Report Output

Group related data and create graphical presentations with the summarized results

[ADD SUMMARY GROUP](#)

Summarize the data using a quick estimation of the top results

[ADD TOP ESTIMATION](#)

Show specific details for each individual request

[ADD REPORT DETAILS](#)

► Delivery Options

9. Select the **Policy Group** and **URI** fields, accept Table as the Presentation type.

Add Report Details

Fields: Policy Group x URI x

[EDIT SORT](#)

Presentations

Table

Policy Group, URI

[CANCEL](#) [SAVE](#)

10. Select **Save** to apply the Report Details.

11. Select the **Create Report** button and **OK** when prompted.

Report Name

Test Demand Report

Description

Enter in the description of the report

Owner

admin

Share With

Report Type

Demand

Date Range

2024-09-16 00:00:00

2024-09-17 00:00:00

Filters

Client Name

= "testclient"

ADD FILTER

LOAD FILTERS

Report Output

Group related data and create graphical presentations with the summarized results

ADD SUMMARY GROUP

Summarize the data using a quick estimation of the top results

ADD TOP ESTIMATION

Show specific details for each individual request

ADD REPORT DETAILS

Delivery Options

CREATE REPORT

12. The New Report displays. Select the **View** button to display the full report in a new tab.

/ Demand Reports / Create Report

Report Test Demand Report

Report Status

Processed Ok [2024-09-16 14:17:50]

Next Run Time

0000-00-00 00:00:00

Run Interval

0

Last Time Edited

2024-09-16 14:17

Total Size

11.9 MB

View Count

1

Report Actions

Refresh / Edit / Clone / Delete / Create Template / Show Definition / Rerun

Policy Group

URI

testgroup

decrypt/pinterest.com:443

testgroup

https://pinterest.com/

testgroup

http://detectportal.firefox.com/canonical.html

testgroup

http://detectportal.firefox.com/success.txt?pv6

testgroup

http://detectportal.firefox.com/success.txt?pv4

testgroup

http://detectportal.firefox.com/canonical.html

testgroup

decrypt//192.168.222.150:443

testgroup

https://192.168.222.150:443

testgroup

decrypt//192.168.222.150:443

testgroup

decrypt//192.168.222.150:443

testgroup

http://detectportal.firefox.com/success.txt?pv4

testgroup

http://detectportal.firefox.com/success.txt?pv6

testgroup

https://192.168.222.150:443

testgroup

https://192.168.222.150:443

Actions

Export Data As

Server

Report Date

Process Start Date

Process Time

Size

View Count

Last Viewed

Chart

View / mail / View PDF

HTML / CSV / CSV(UTF16) / Text / GZipped CSV

localhost

2024 Mon, Sep 16 14:17

2024-09-16 14:17:49

00:00:01

11.9 MB

1

2024-09-16 14:17:51

Show

Actions

Export Data As

Server

Report Date

Process Start Date

Process Time

Size

View Count

Last Viewed

Chart

Showing 1 to 1 of 1

Per page 20

Previous

1

Next

Pass Criteria

The report will show all the URL entries that have been requested by the ‘testclient’.

Notes	
Results (Pass or Fail)	
Results Comments	

 netsweeper

© 2024, Netsweeper Inc.

Creating a Summary Demand Report

Purpose

Create custom Demand Reports that shows all allowed or denied requests for a specific time / from specific IPs / for only specific category / specific URI, etc.

Precondition

See: Setting up Filtering Group and Client

On the Test Workstation:

Browse to both allowed and denied sites.

In the WebAdmin:

1. Navigate to Reports > Demand Reports.
2. In the 'Report Name' field, enter **Test Demand Report**.
3. Select the Calendar button for the 'end-date' in the 'Date Range' field.
4. Use the calendar to set the 'date' value to tomorrow's date and select **OK**.
5. Select the **Add Filter** button.
6. Set the 'Field' value to **Client Name**, leave the 'Condition' set to **Equal To**, and in the 'Value' field, choose the **testclient** associated with your test workstation.
7. Select **Save** to apply the Filter.
8. Next, Select the **Add Summary Group** option for the Report Output section.
9. For the 'Group Data By' field, select **Denied Categories**.
10. Add **Request Count** and **Request Count Percent** to the 'Fields' List.

The screenshot shows the 'Add Summary Group' dialog box. The 'Group Data By' dropdown is set to 'Denied Categories'. The 'Category Group' dropdown is set to 'All Categories'. The 'Fields' section shows 'Request Count' and 'Request Count Percent' selected. The 'ADD PRESENTATION' button is highlighted. The 'CANCEL' and 'SAVE' buttons are at the bottom right.

11. Set the 'Display' field to **Pie Chart** and select **Save** to apply our Presentation.

Add Summary Group > Presentation

Presentation

Display: Pie Chart

Data: Request Count

Legend: Legend Without Values

Options

☐ Maximum Records: 10

☐ Explode Sectors

☐ Transparent Colors

☐ Grouped Categories

☐ Others Sum

CANCEL SAVE

12. Select **Save** again to apply our Summary Group.

Add Summary Group

Group Data By: Denied Categories

Category Group: All Categories

Fields: Request Count, Request Count Percent

[SELECTED VS OTHER](#)

[EDIT SORT](#)

Presentations

Pie Chart
Request Count

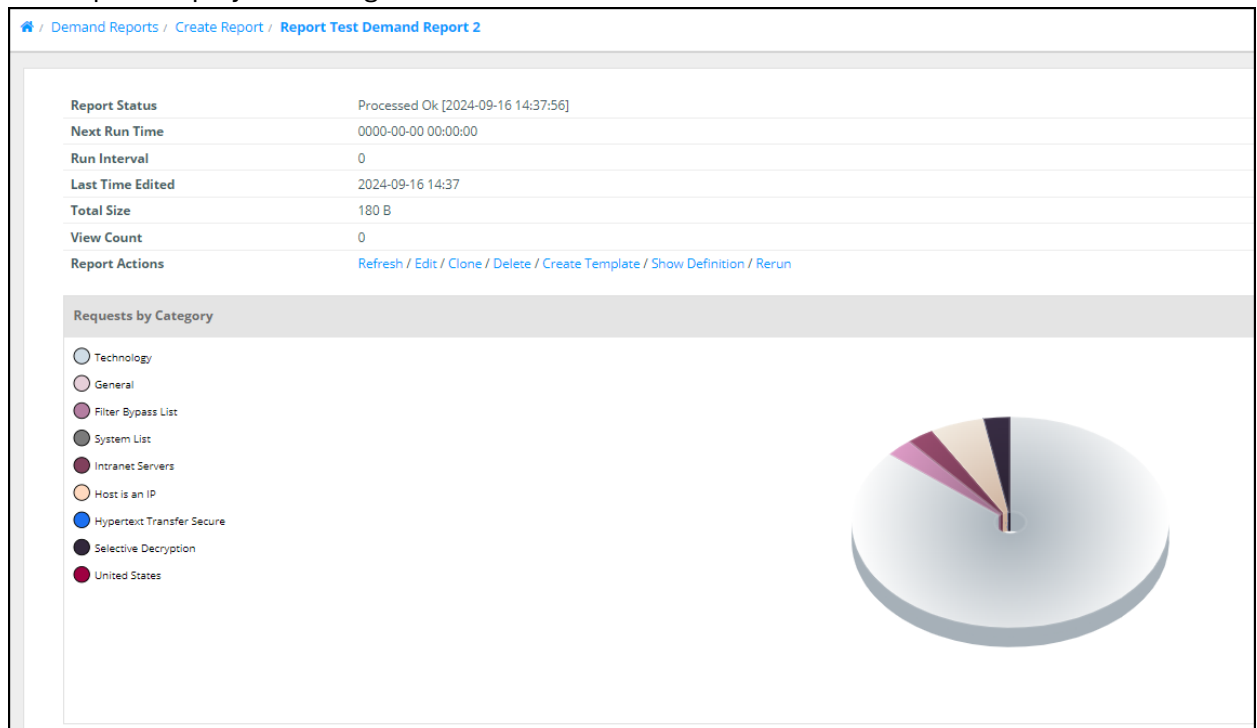
[ADD PRESENTATION](#)

[OPTIONS](#)

CANCEL SAVE

13. Select the **Create Report** button and then **OK** when prompted.

14. The Report Displays as configured.



Pass Criteria

The Report displays showing denied sites that have been visited. It displays the Category, Total Requests and Request Percent columns.

Notes	
Results (Pass or Fail)	
Results Comments	

HTTPS Filtering Tests

HTTPS Filtering at Domain Level

Purpose

The Netsweeper solution can block specific HTTPS URL but only up to TLD Top Level Domain. This test case verifies that HTTPS URL filtering behaves as expected.

Precondition

See: Setting up Filtering Group and Client.

Test Procedure: Filtering at the Domain Level

This Procedure will add https://example.com to the local deny list group policy for the filtering.

Use the filtered workstation to visit https://example.com

In the WebAdmin:

1. Navigate to Policies > Groups and in the **Lists** tab choose **testgroup2**.
2. Go to the **Policies** tab and then the **List** subtab.
3. Select the **default** Policy.
4. Go to the **URL/Keyword Local List** tab and select the **Create Local List** button (if needed).
5. Select the **New Entry** button.
6. Add https://youtube.com into the 'New Entry' field.
7. Ensure that 'Entry Type' is set to **URL**, 'Request Part' is set to **Request URL** and 'Action' is set to **Deny**.
8. Select **Save Entry**.

On your Test Workstation: (Ensure you're being filtered in 'testgroup2')

Browse to https://youtube.com.

A 'Connection is Untrusted' page displays.

If the Capture Module is used, then Netsweeper will just break the https connection. A browser would then state that connection was reset

Pass Criteria

You will not be able to visit the https://youtube.com. Using the filtered workstation in the testgroup2 Group, browsing to a URL that belongs to the Local List as a 'Deny' URL will not be reachable.

Notes	Without installing a Certificate of Authority, a Connection Not Trusted page will be served instead of our Deny Page.
Results (Pass or Fail)	
Results Comments	

Document Sign-off

Acceptance Test Approval

The client for this project agrees that the acceptance tests contained within this document are suitable for verifying that the solution delivered by Netsweeper meet the requirements of this project.

Client Name	
Authorized Party Signature	
Authorized Party Name	
Date	

Acceptance Tests Passed

Client Name	
Authorized Party Signature	
Authorized Party Name	
Date	