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

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 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

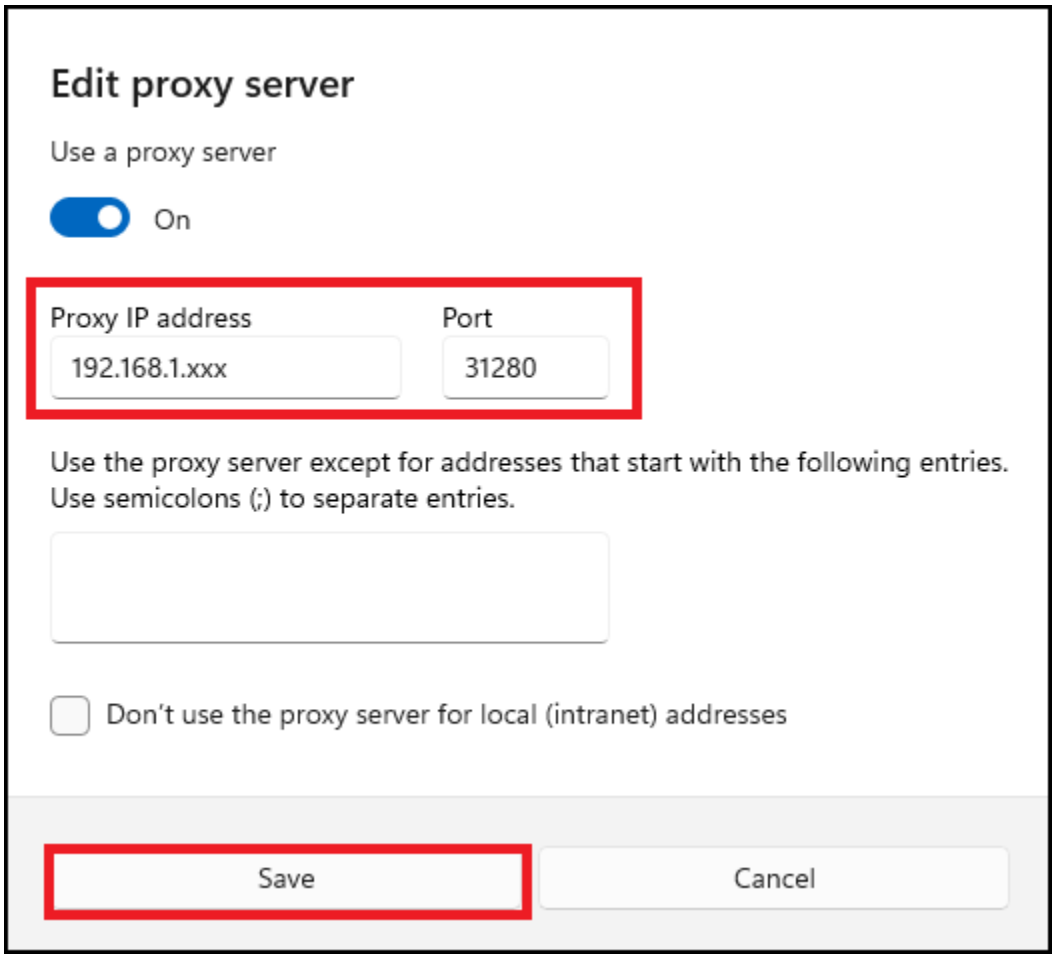
Filtering for the Test Workstation

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.

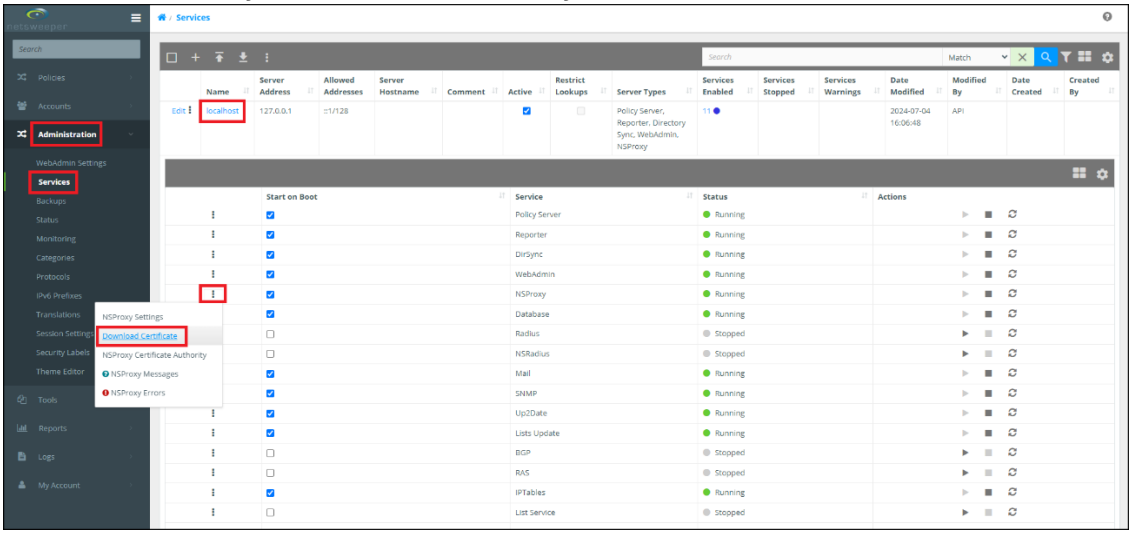
NSProxy Certificate Installation on the Test workstation

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

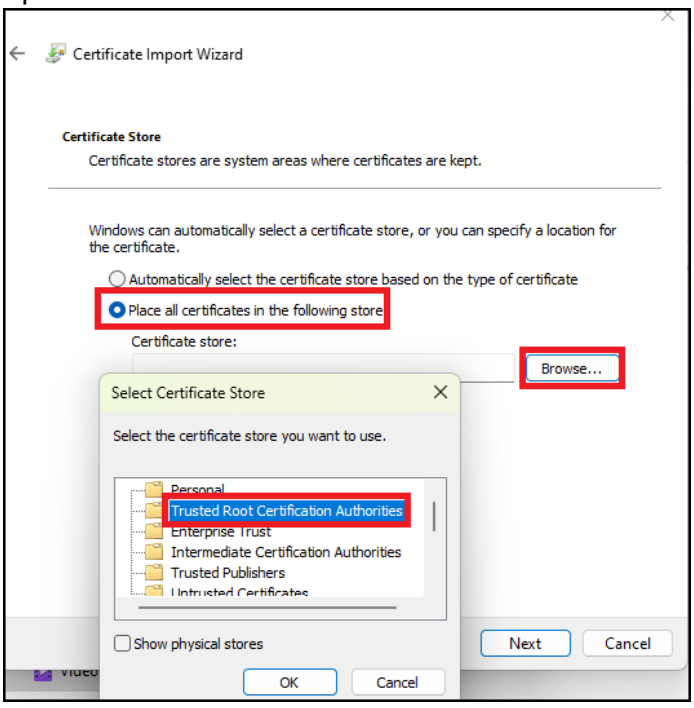


Importing a Certificate

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 certificated 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.

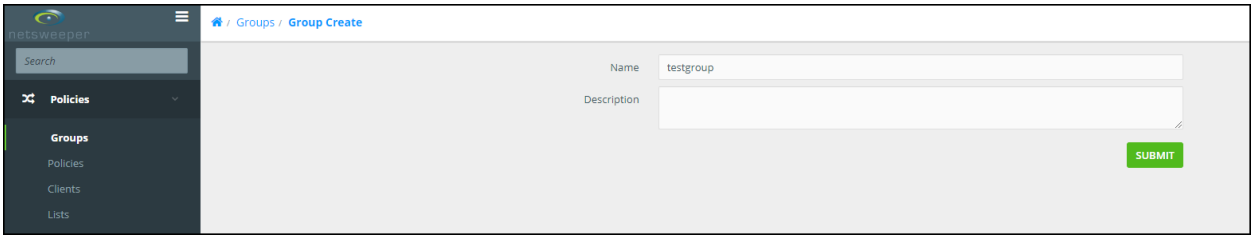
The Precondition section will:

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

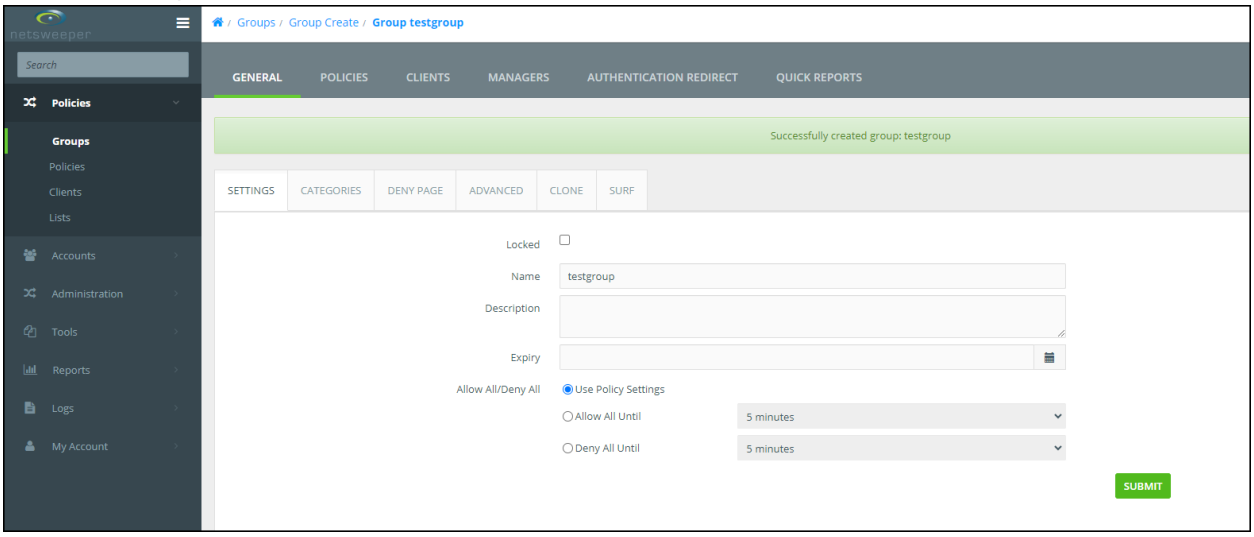
This document will assume that this section is completed as part of the precondition

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.

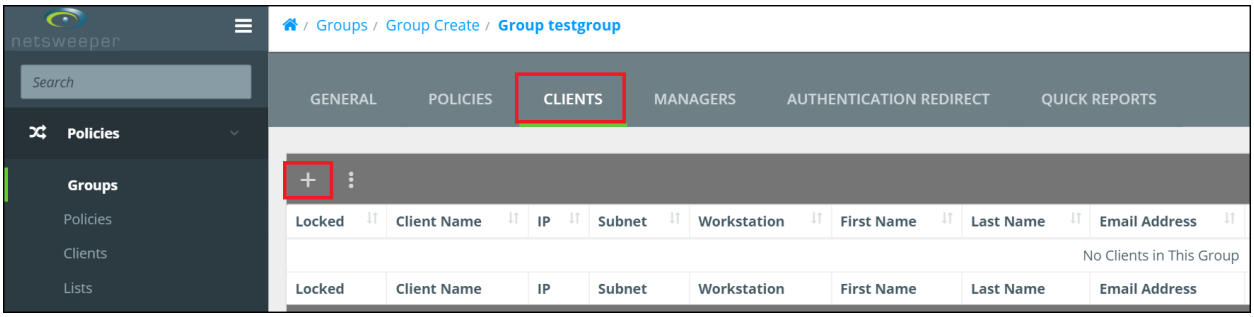


4. The new Group is created.

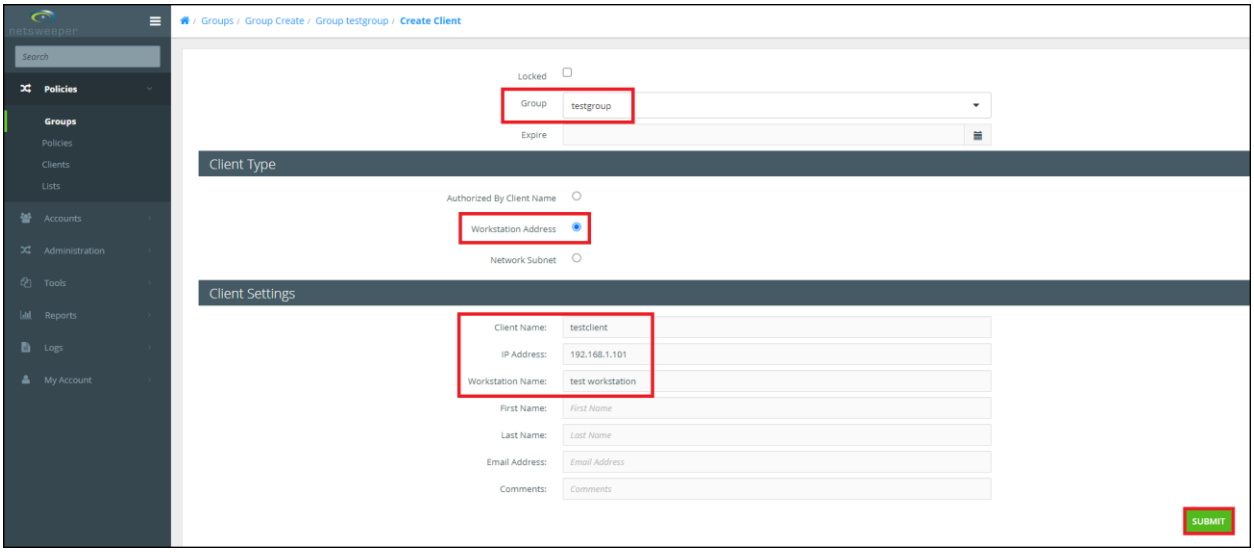


Create a Client ‘testclient’

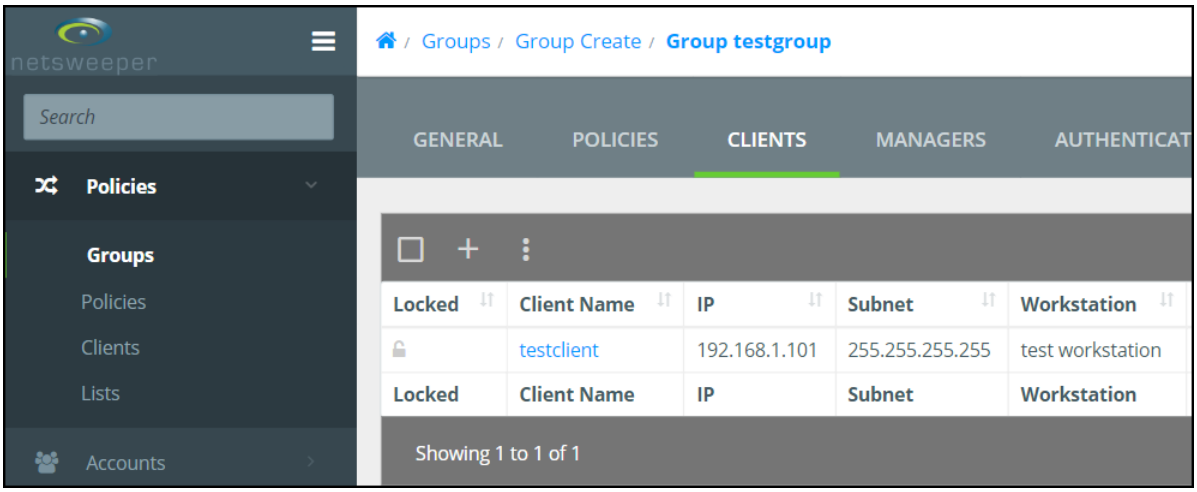
1. Navigate to your new Group’s Clients tab and select the **Create** button.



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.

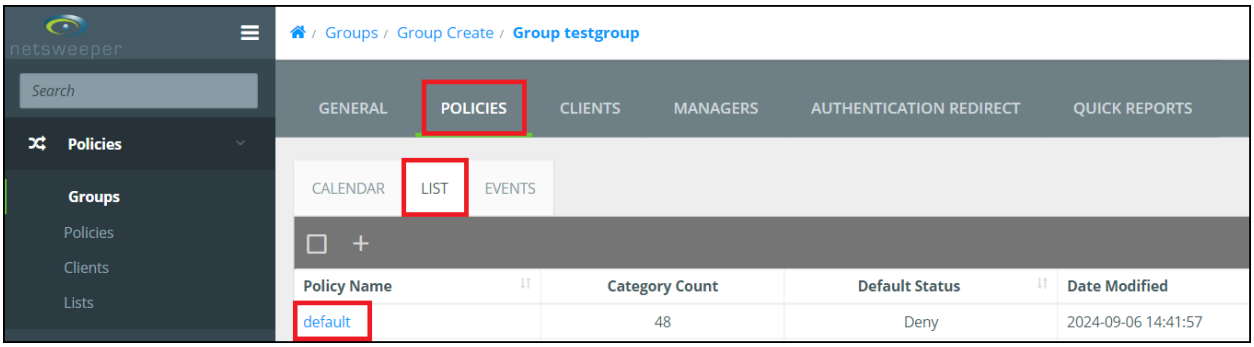


4. The new Client displays in the Group’s Clients tab.



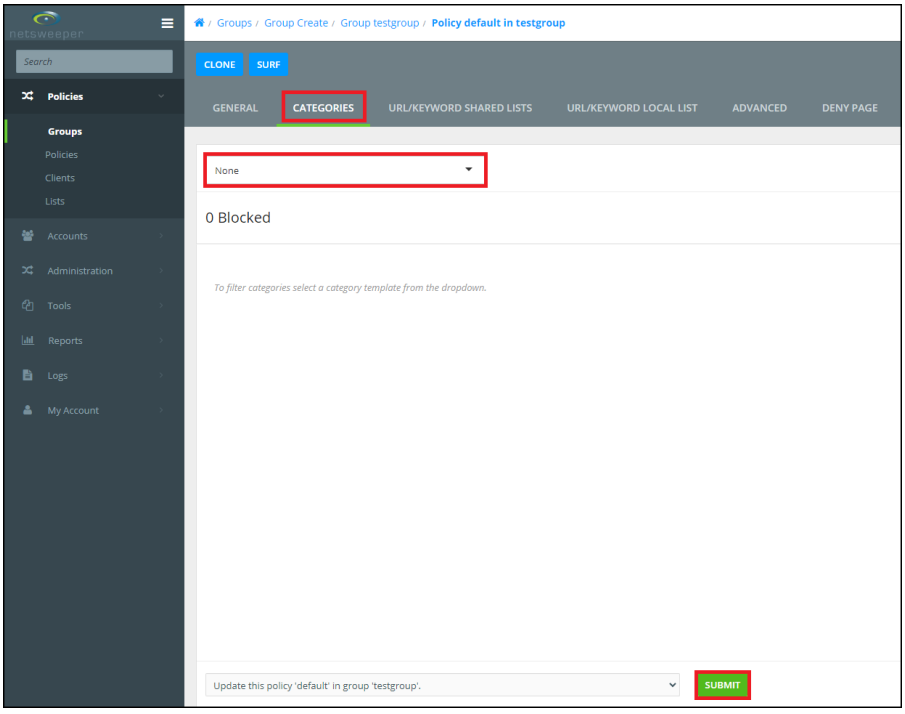
Create a Policy ‘testpolicy’

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



3. Rename the Policy ‘testpolicy’ and select **Submit**.

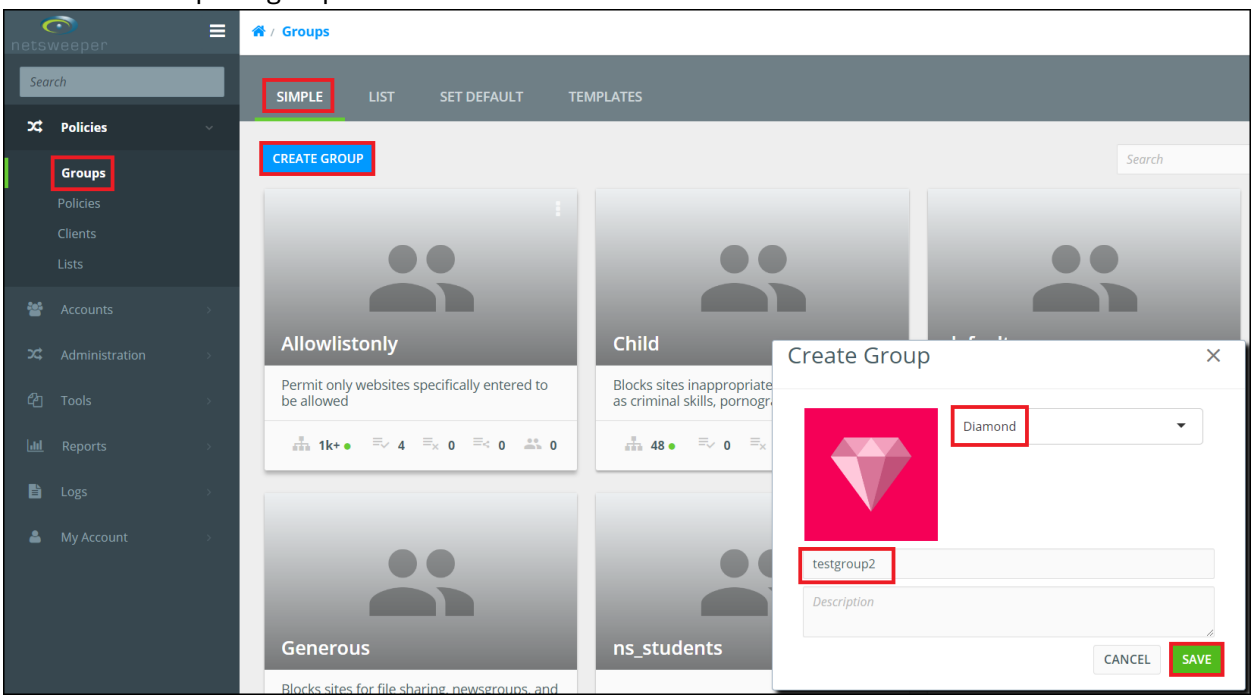
4. Navigate to the Policy’s **Categories** tab and choose the **None** Category Template.



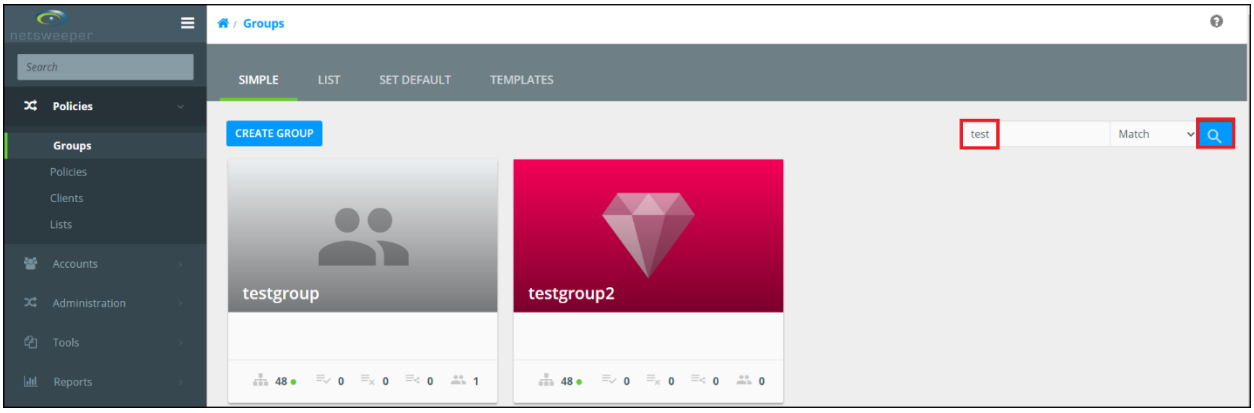
5. Select the **Submit** button to save your changes.

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 filed 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

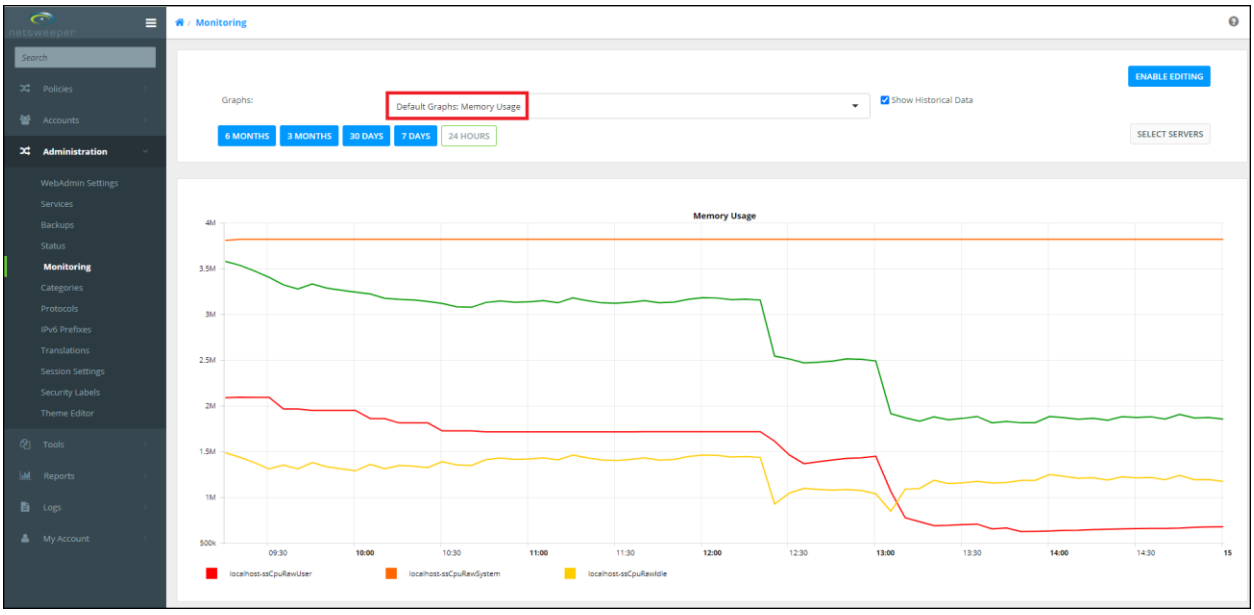
The Netsweeper solution must have been running and intercepting traffic for a period of at least 1 hour with testing taking place to generate allowed and denied request.

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.

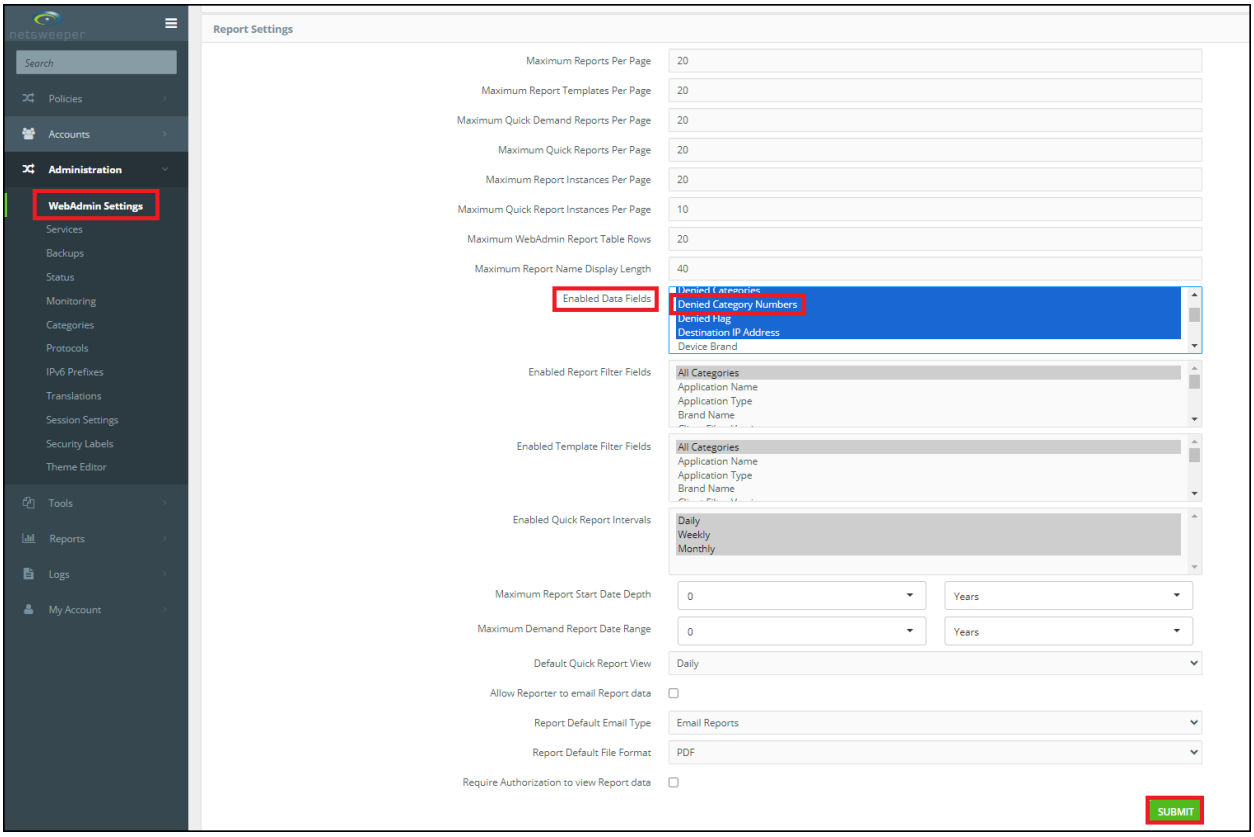
SNMP MIBs in 8.2

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.



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.

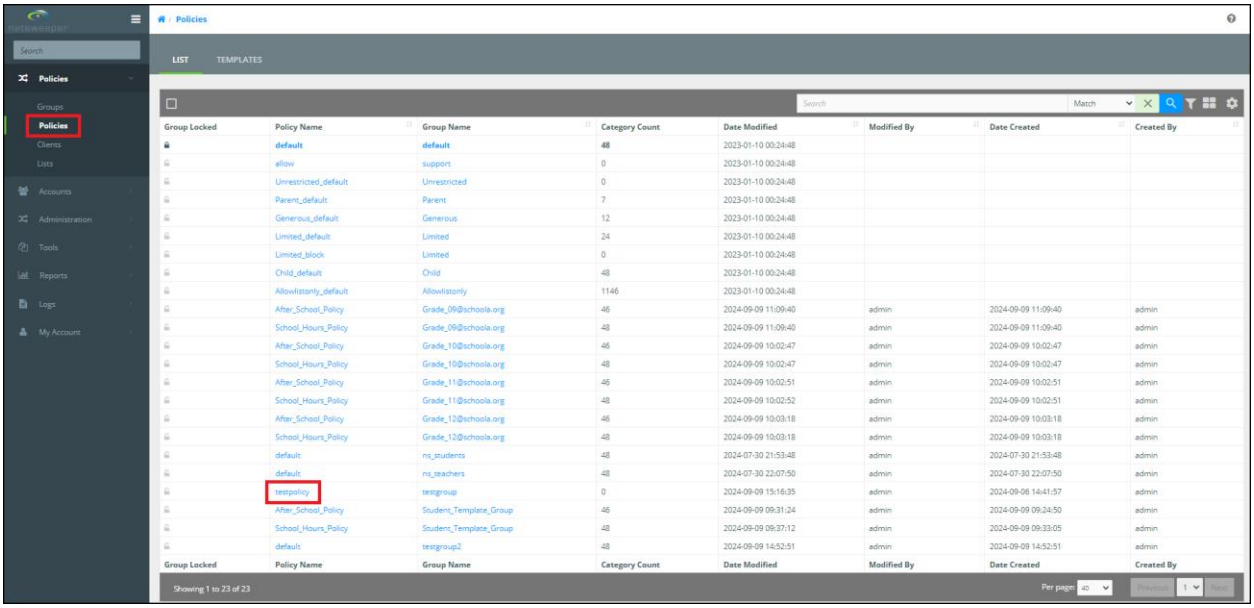
Precondition

See: Setting up Filtering Group and Client

Test Procedure: Local Lists

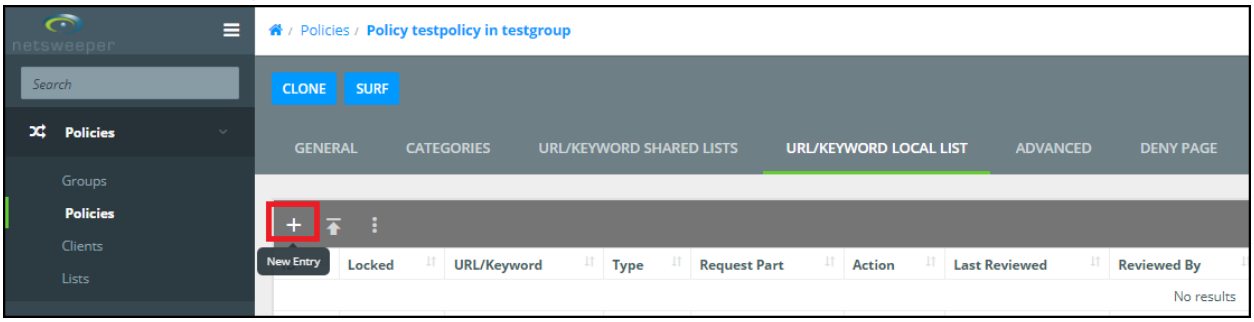
In the WebAdmin:

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

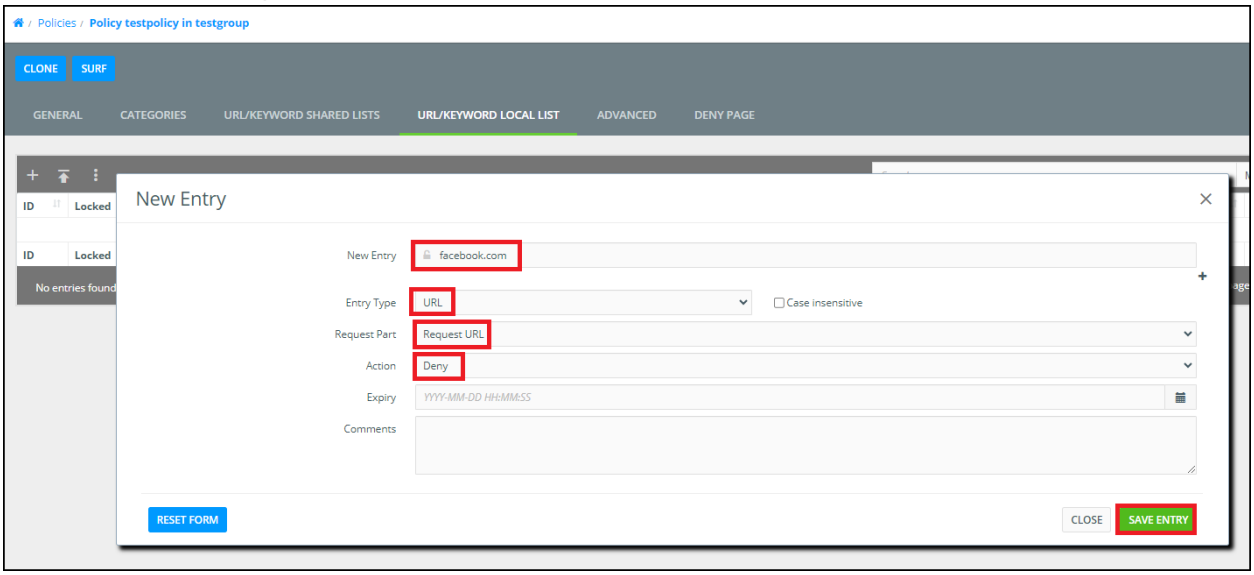


2. Choose the **URL/Keyword Local List** tab.
3. Select the **Create Local List** button.

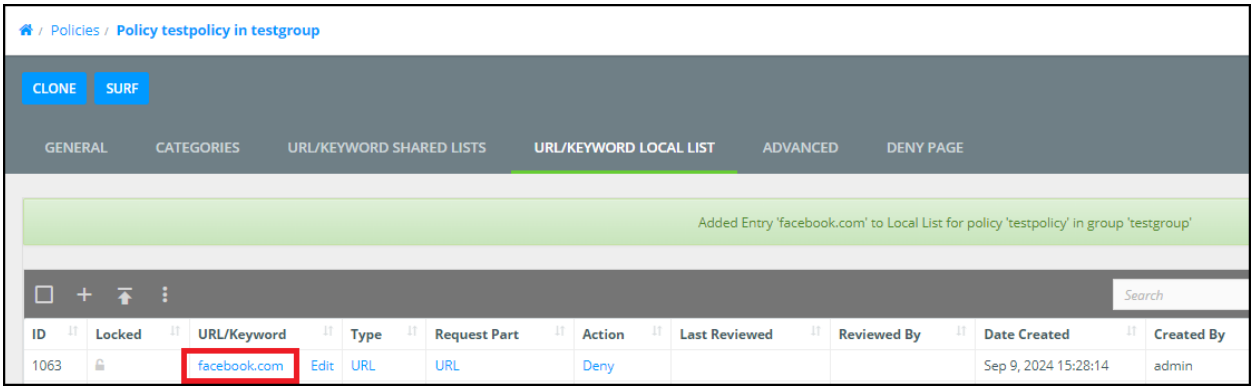
4. Select the New Entry button.



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.



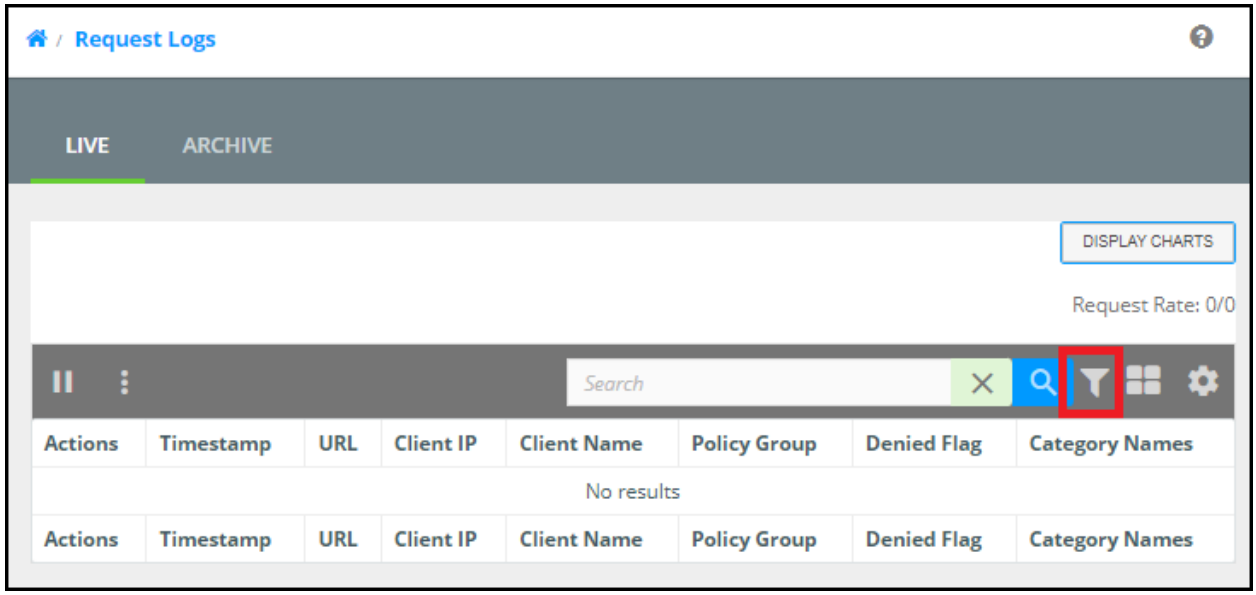
10. The entry is added to the Local List.



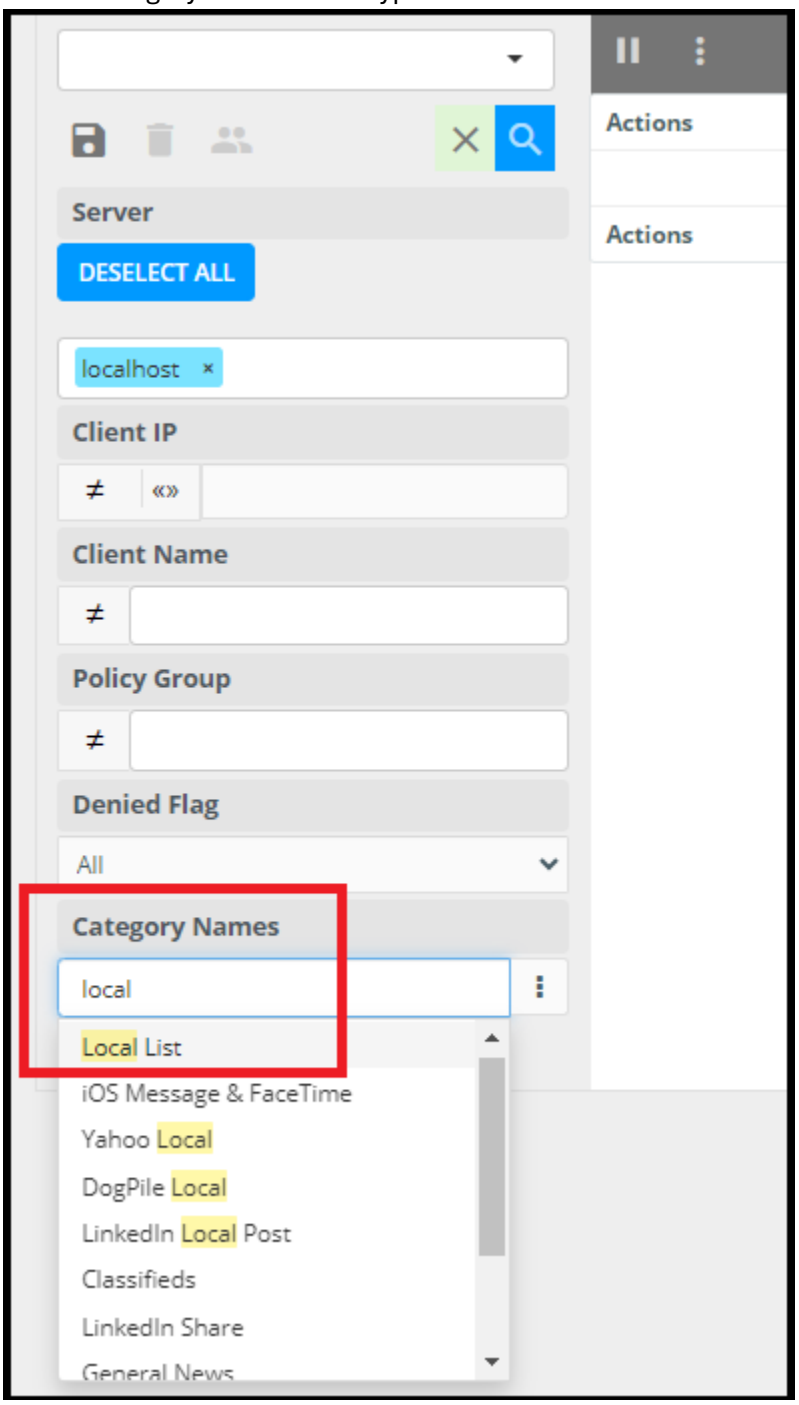
Request Logs Advanced Filters

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

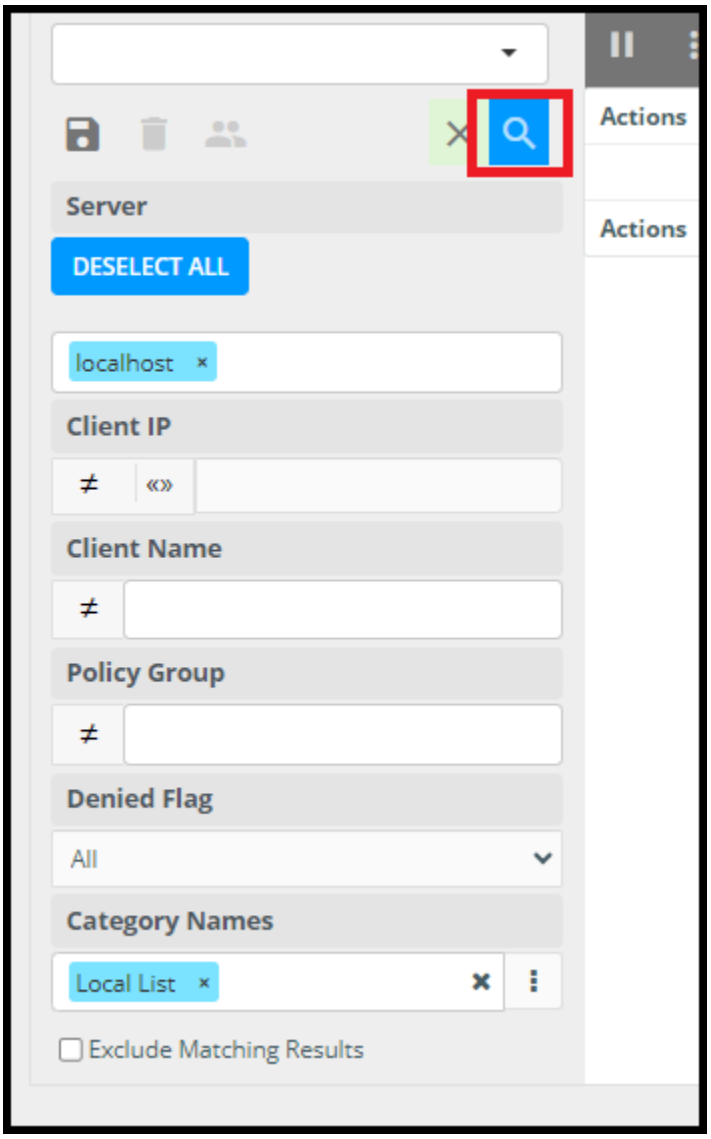
1. Navigate to Logs > Request Logs and select the **Advanced Filter** button in the Table Header.



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

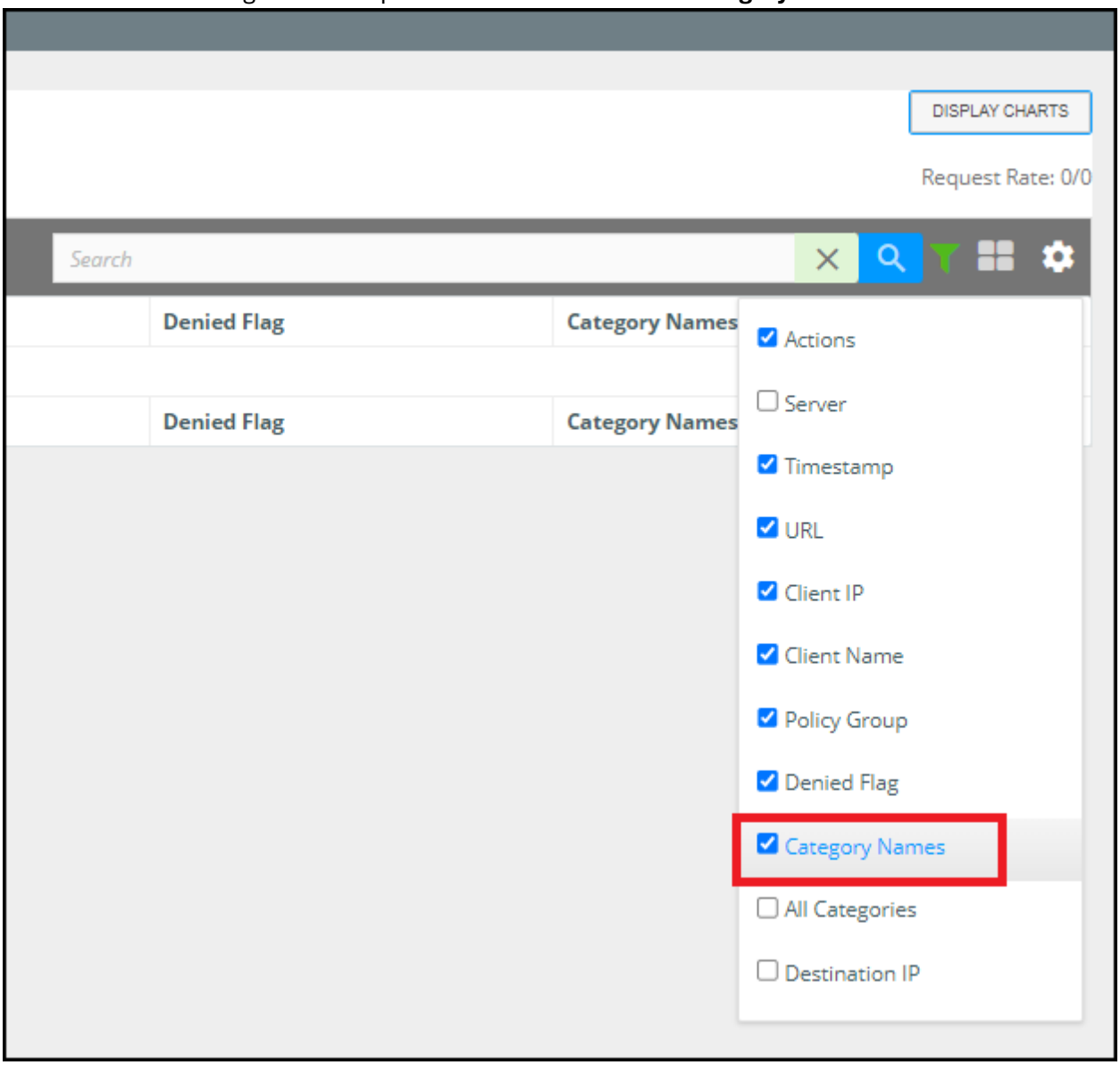


3. Select the **Search** icon within the Advanced Filter.



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

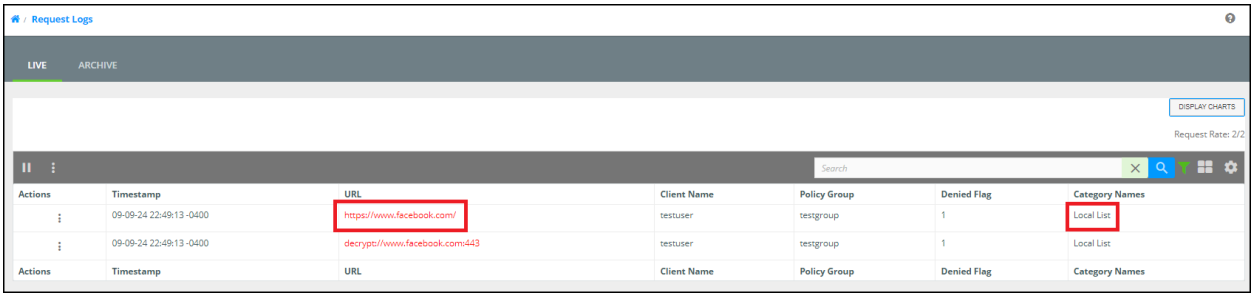
5. Hover over the 'Settings' icon and place a checkmark beside **Category Names**.



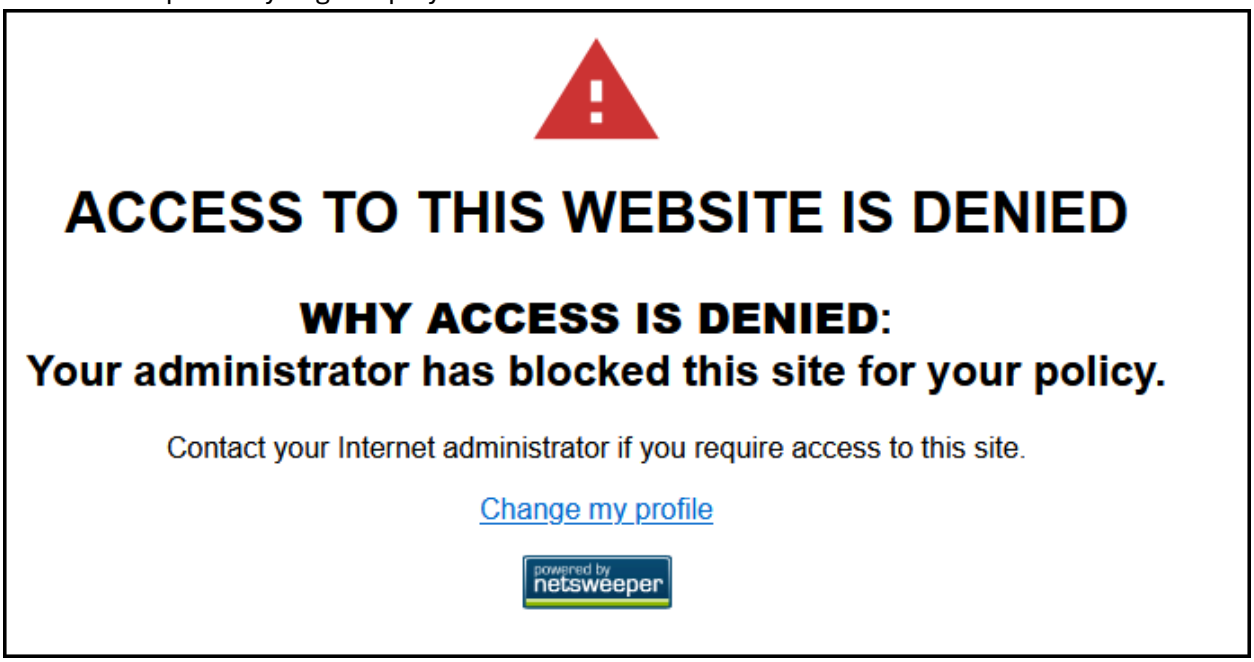
On the Test Workstation filtered by the 'testgroup' Group:

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'.



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.

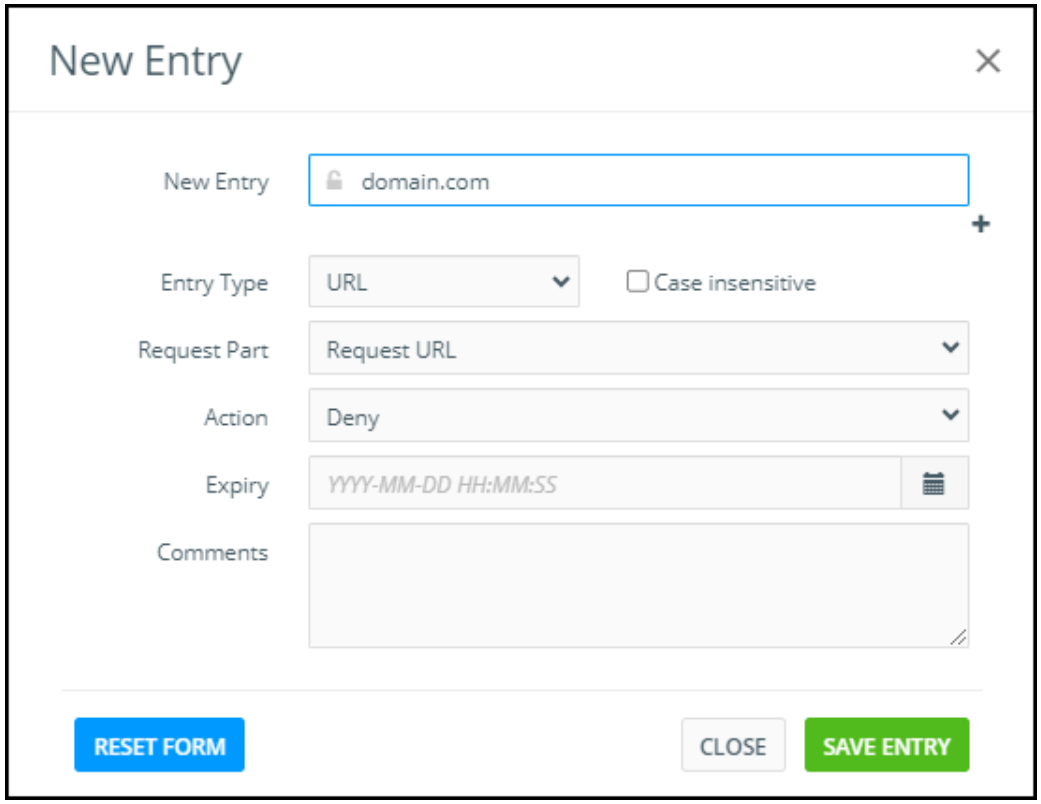
Precondition

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.



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

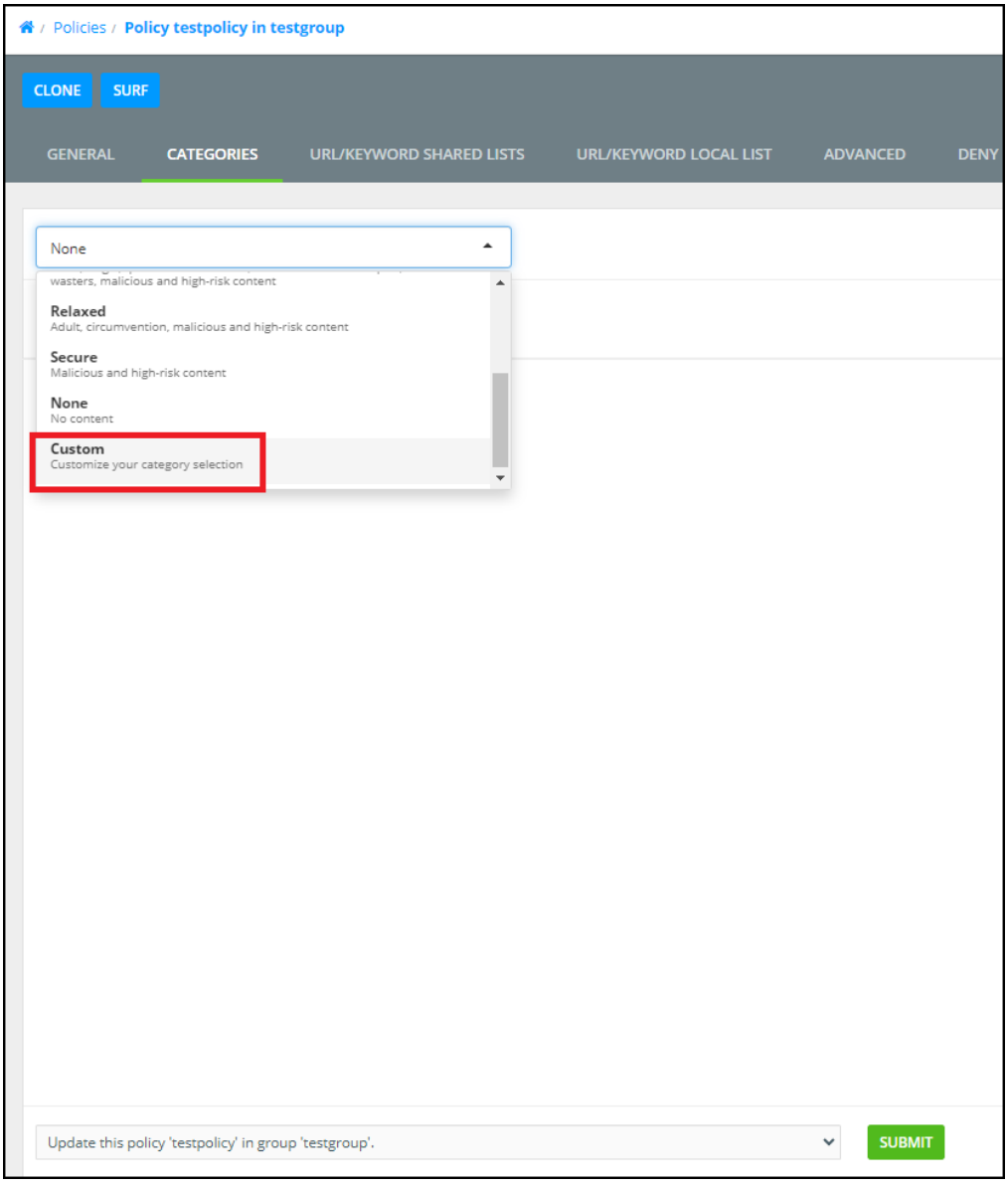
The Netsweeper solution can filter based on the Category which the URL belongs to. The system administrator can select the categories that will not be accessible to the end users.

Precondition

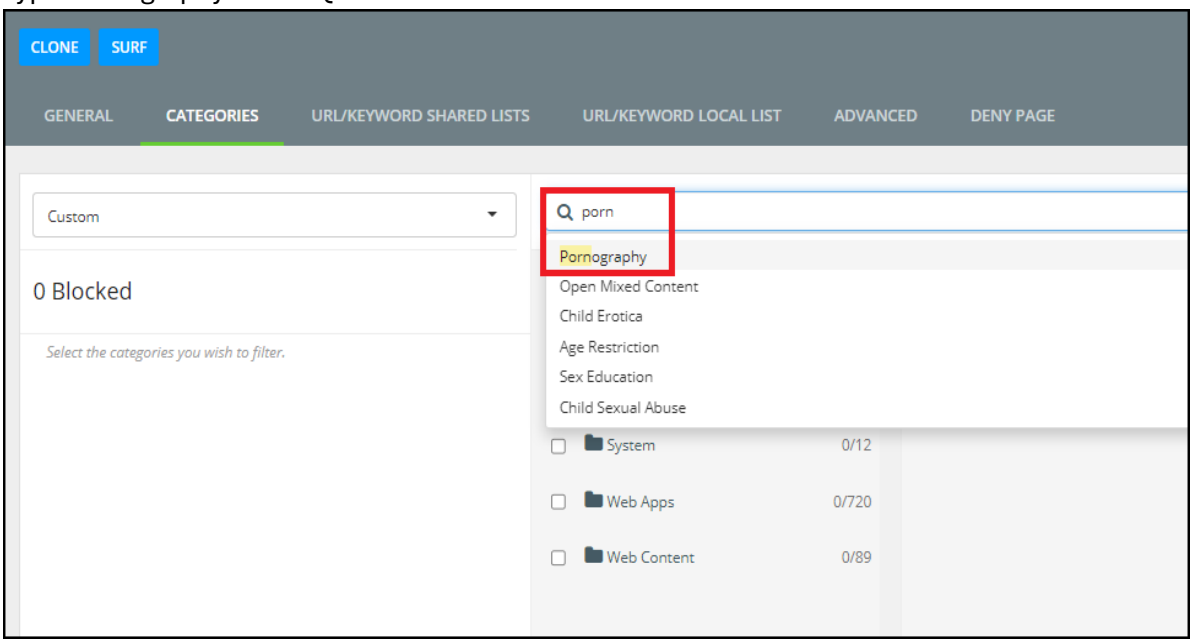
See: Setting up Filtering Group and Client

In the WebAdmin:

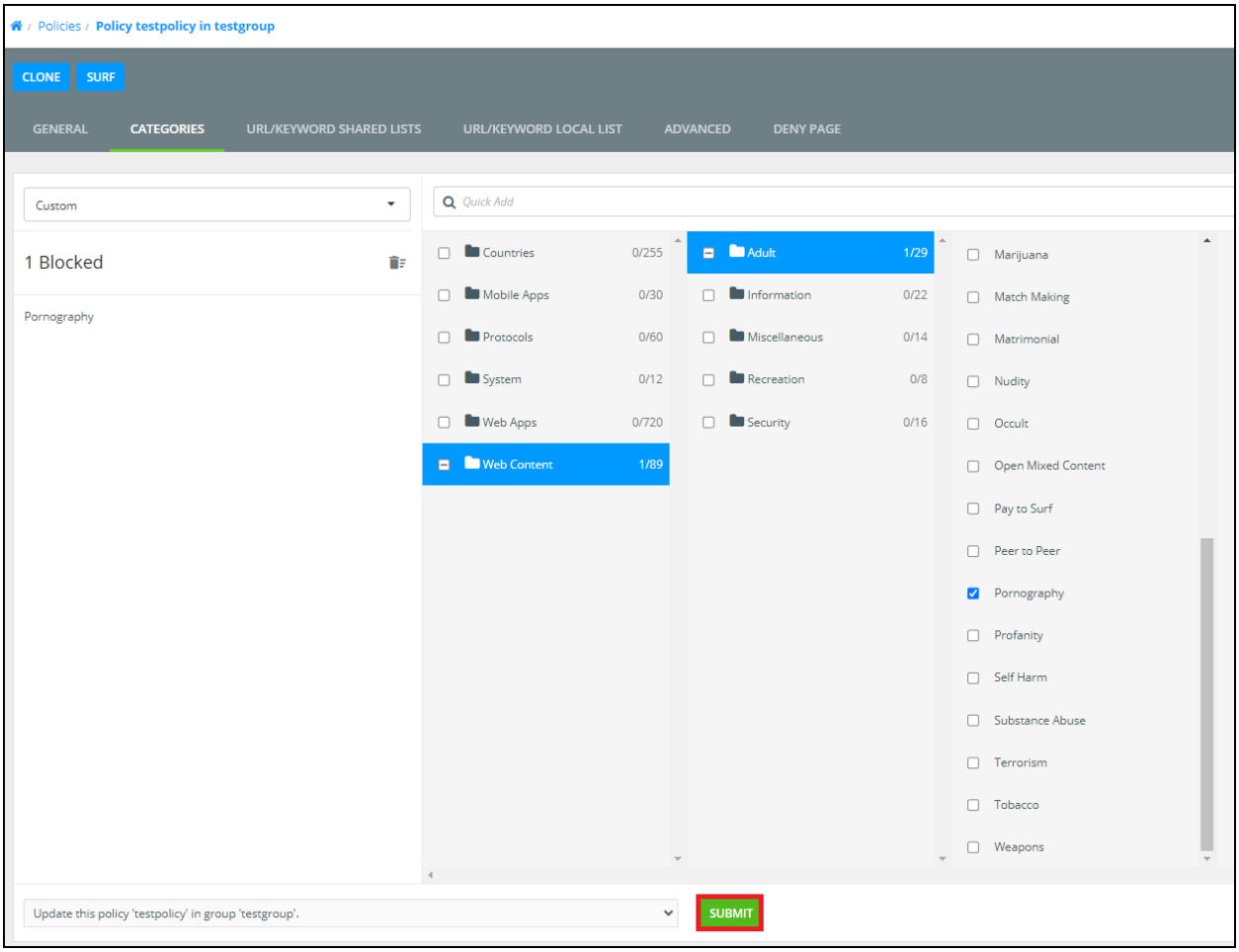
1. Navigate to Policies > Policies and select your testpolicy.
2. Choose the **Categories** tab.
3. Select the **Custom** Category Template.



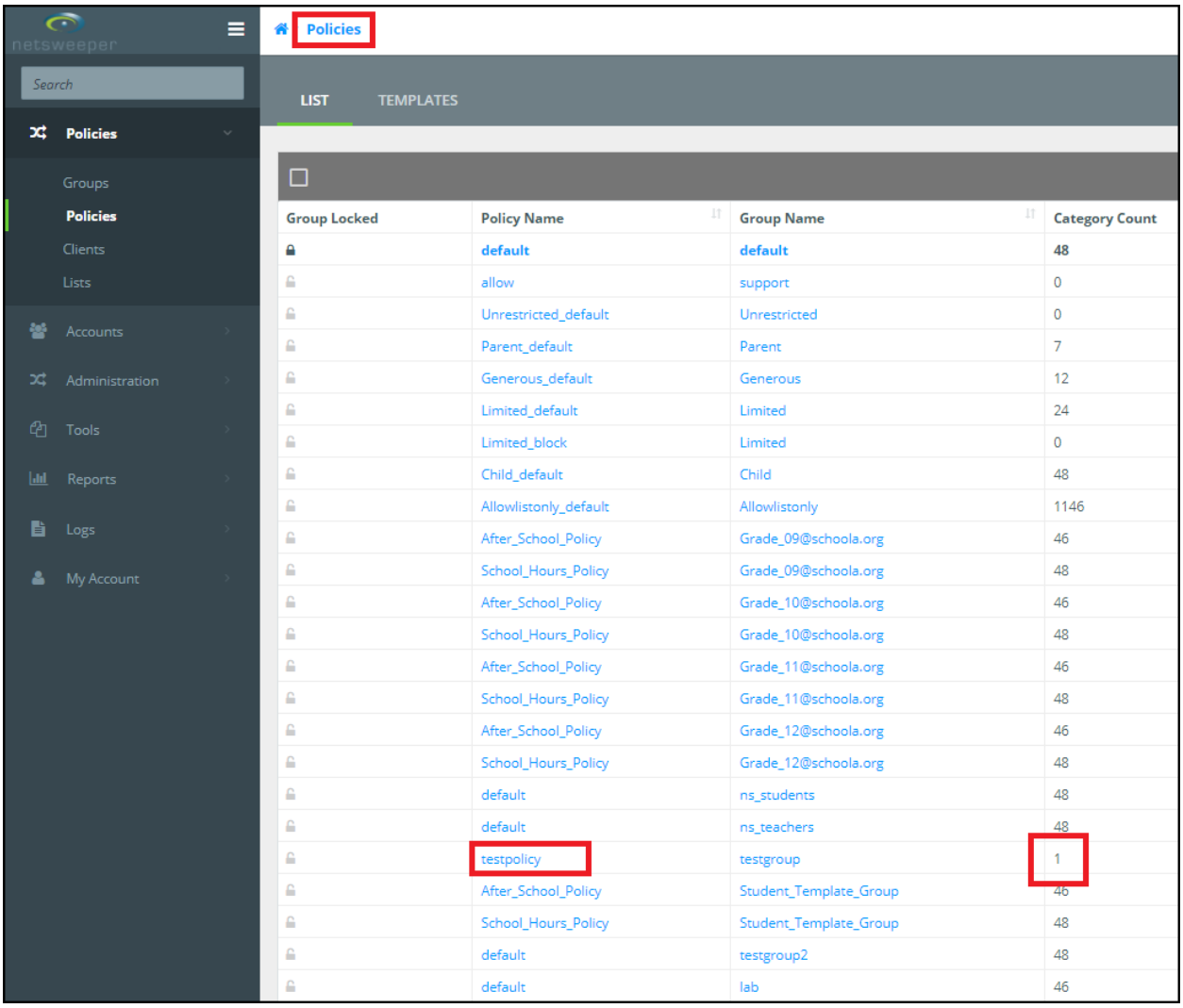
4. Type Pornography in the ‘Quick Add’ field and then select the result.



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



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



On Your Test Workstation

1. Browse to a pornography site such as playboy.com.
2. 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.

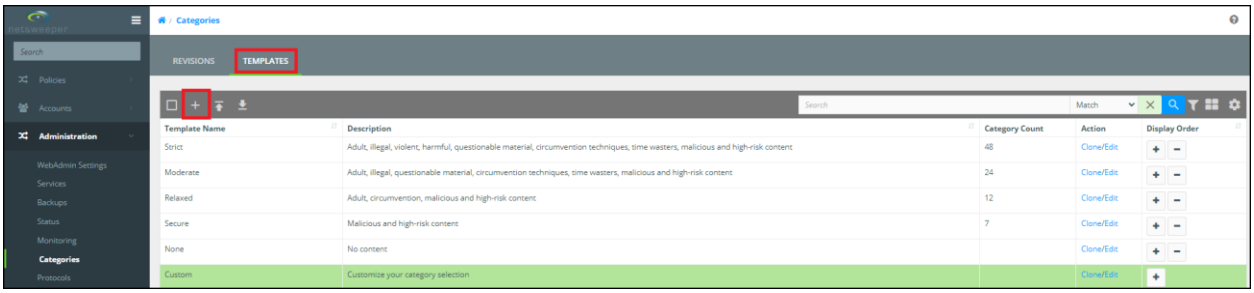
Precondition

See: Setting up Filtering Group and Client

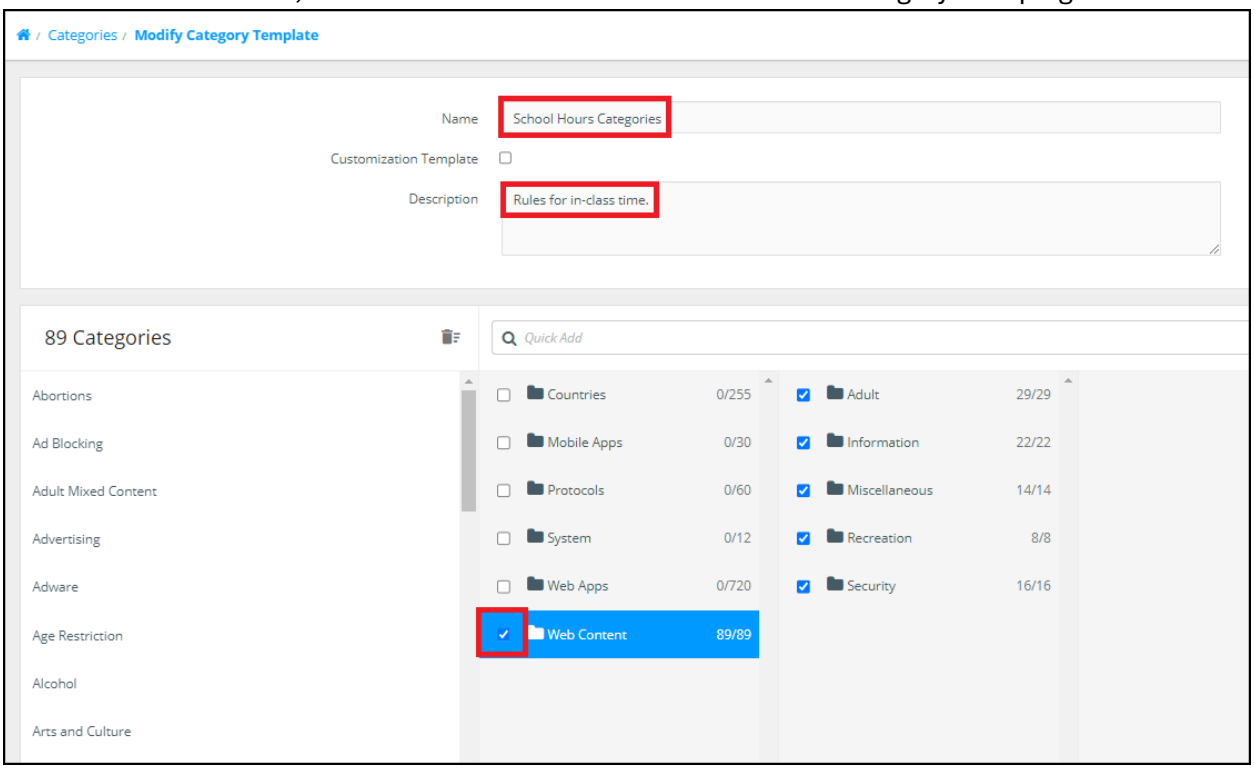
Test Procedure: Deny Specific Category

In the WebAdmin

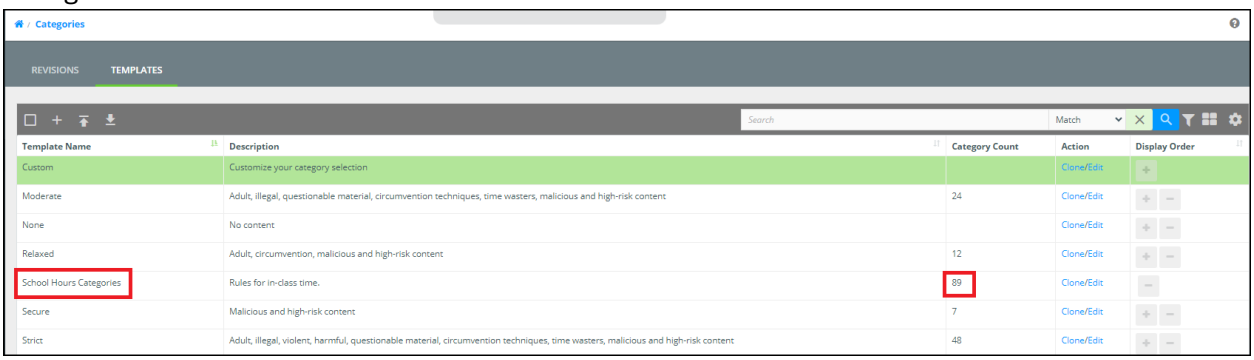
1. Navigate to Administration > Categories and choose the **Templates** tab.
2. Select the **Create** button.



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.

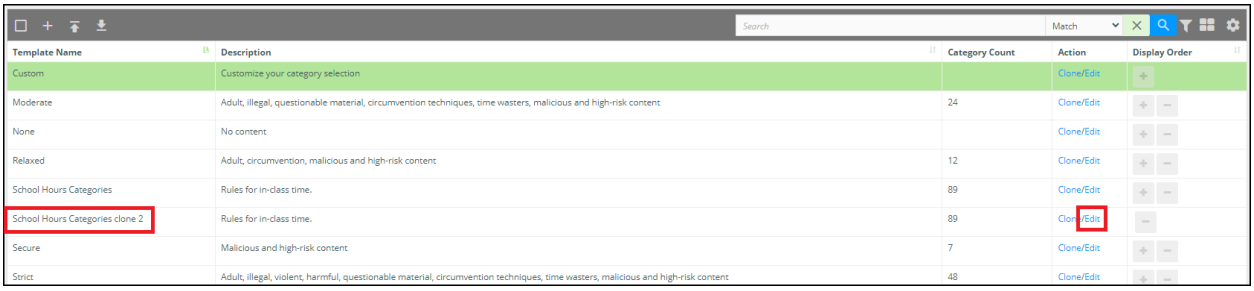


5. Select the **Submit** button. You will see a banner stating, “Successfully added a new category template.”
6. Use your breadcrumbs to return to the Templates tab of the Categories window. You will see your new ‘School Hours Categories’ Template along with the number of blocked Categories it enforces.



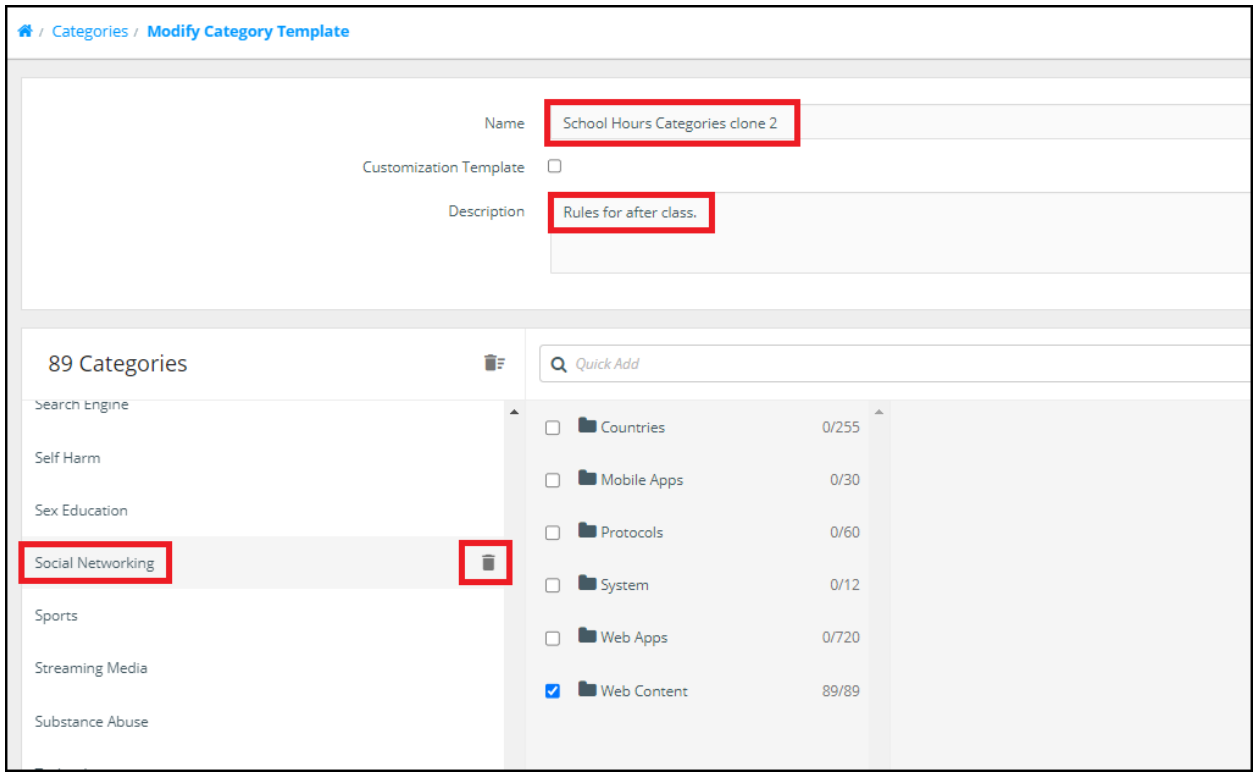
7. Select the **Clone** button beside the ‘School Hours Categories’ Template.

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



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.



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

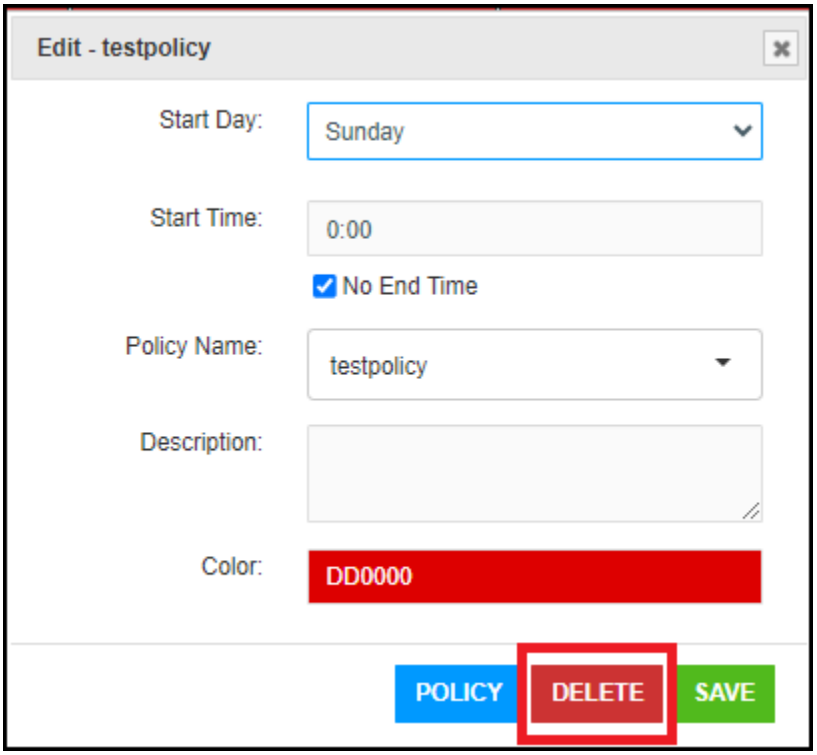
See: Setting up Filtering Group and Client

The created ‘After School’ and ‘School Hours’ Category Templates.

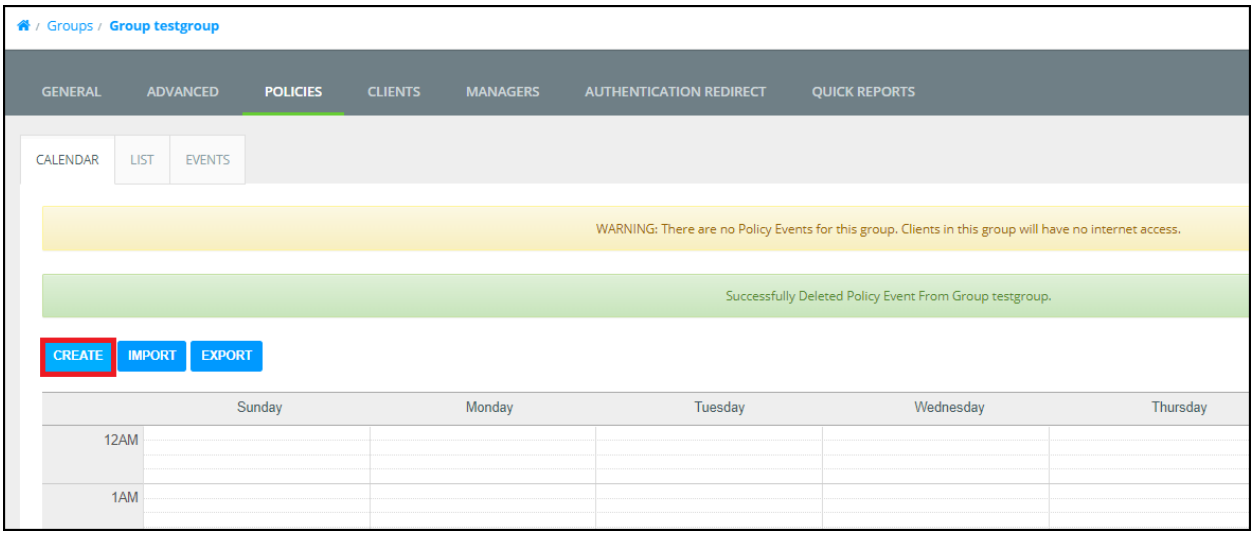
Test Procedure: Policy Events

In the WebAdmin:

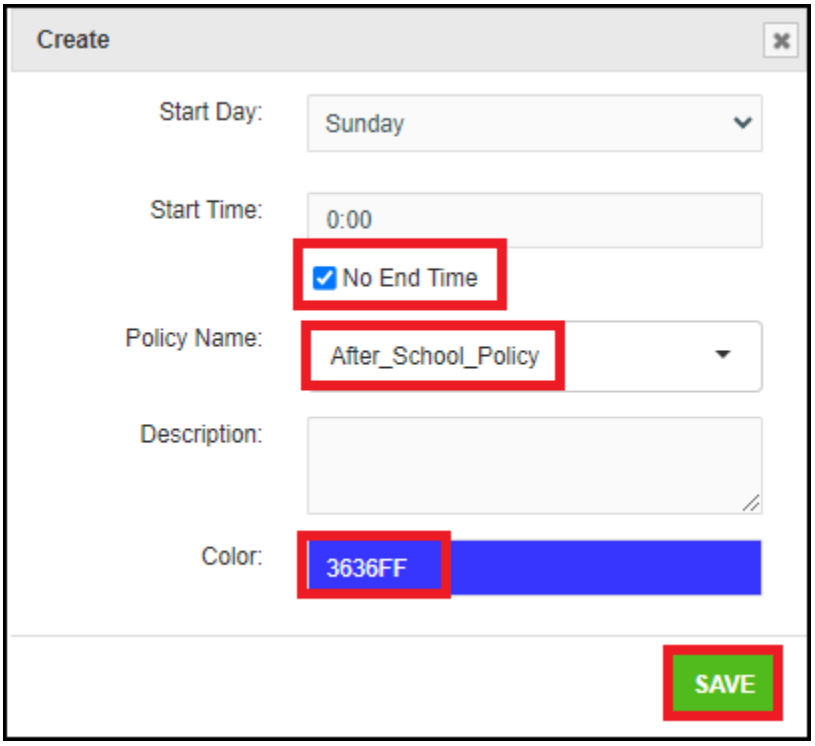
1. Navigate to Policies > Groups and choose the **List** tab.
2. Select the ‘testgroup’ and choose the Policies tab.
3. Choose the ‘Default’ Policy Event. and in the pop-up-box, select the **Delete** button.



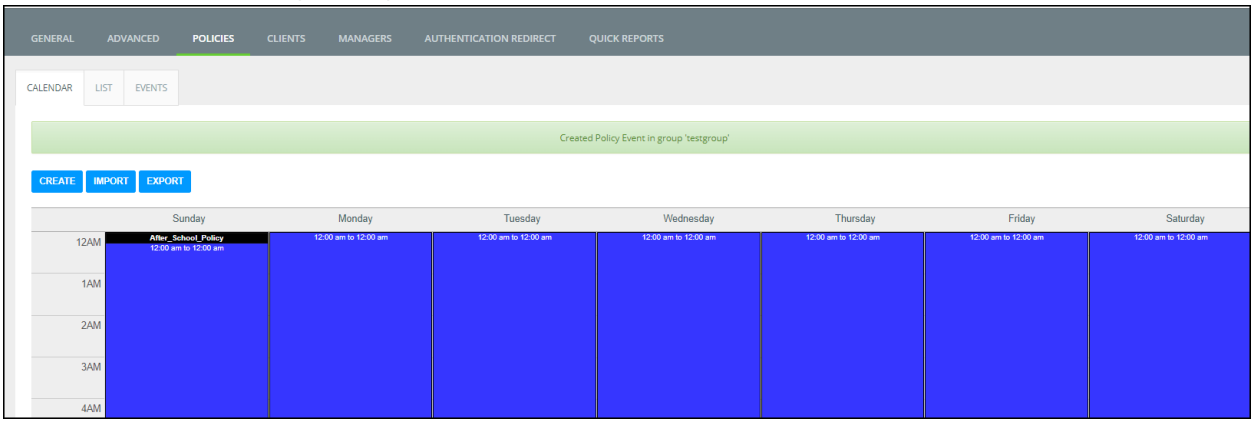
4. Select the **Create** button.



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.

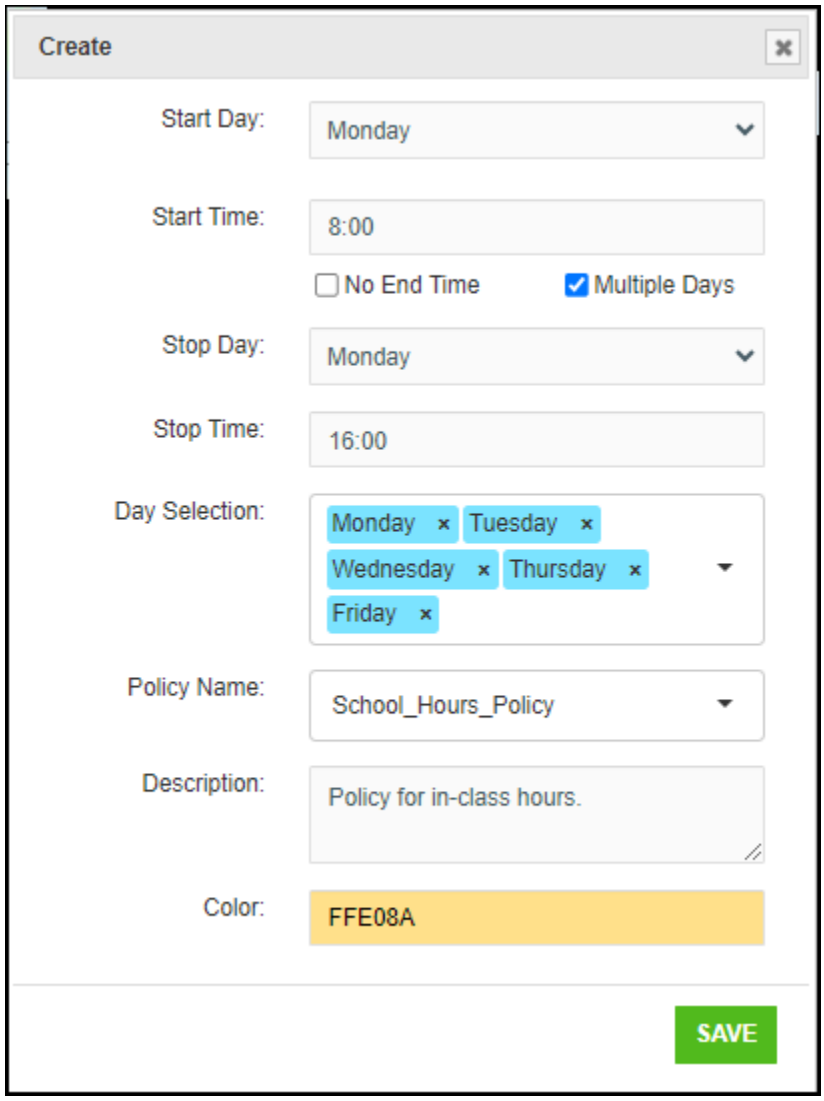


8. The ‘After_School_Policy’ Policy Event is created.



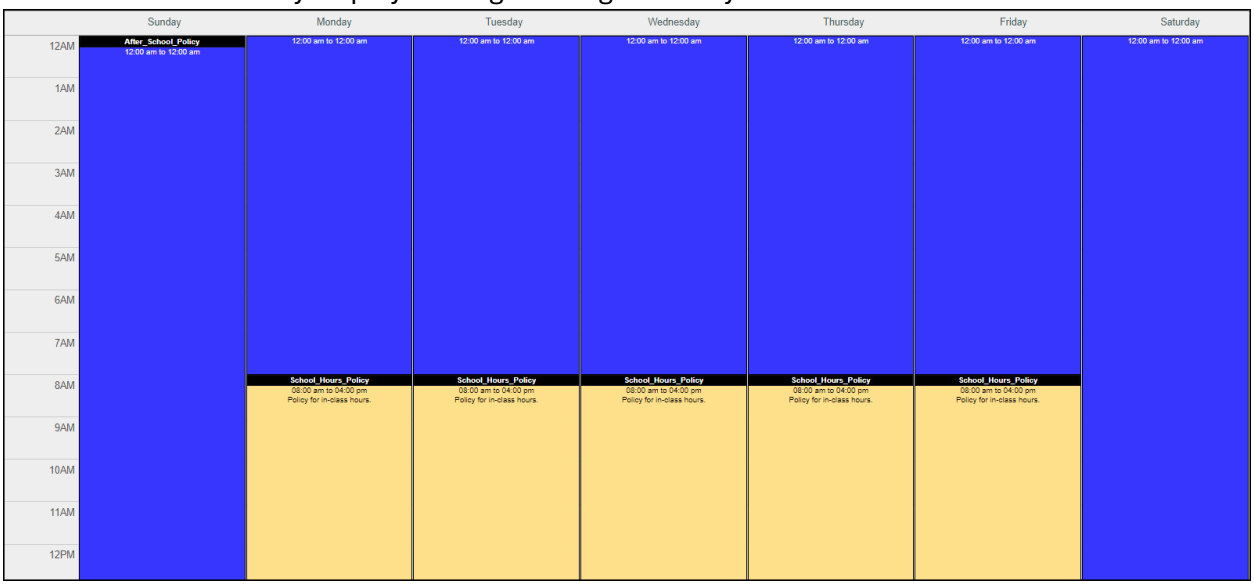
9. Select the **Create** button again.
10. Set the ‘Start Day’ and ‘Stop Day’ fields to Monday.
11. Select the **Multiple Days** checkbox.
12. Set the ‘Start Time’ as 8:00 and the ‘Stop Time’ as 16:00.
13. In the ‘Day Selection’ field choose Monday to Friday inclusive.
14. Enter the ‘Policy Name’ School_Hours_Policy with no spaces and add an optional description.

15. Enter the Color value FF308A.

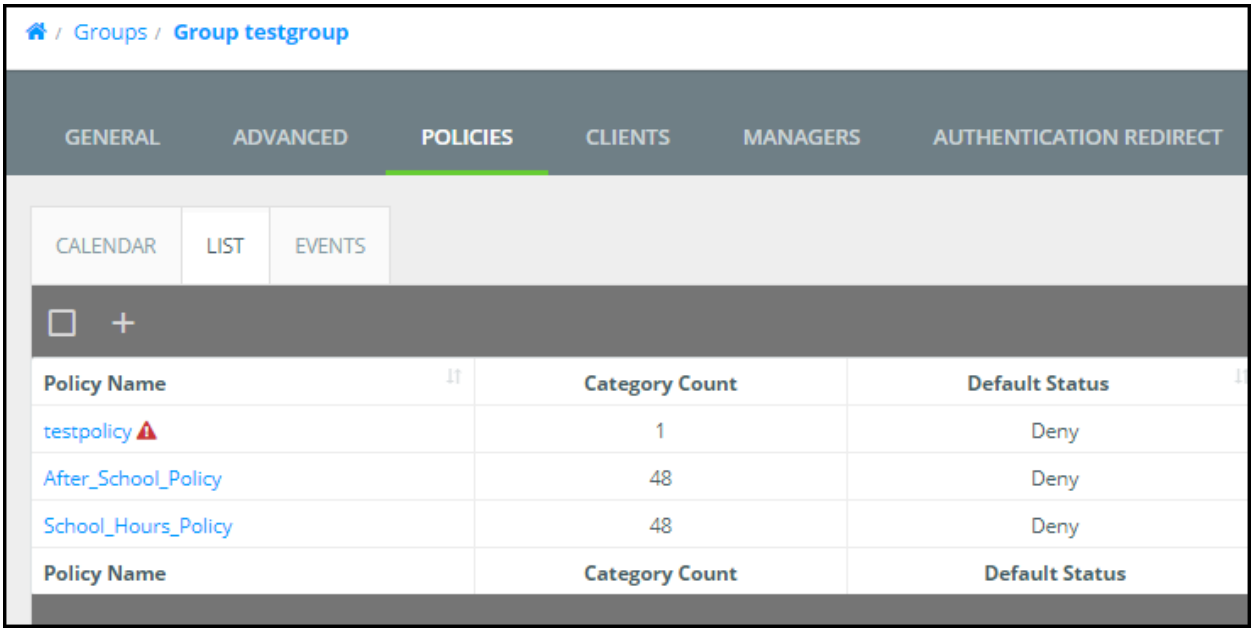


16. Select the **Save** button.

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

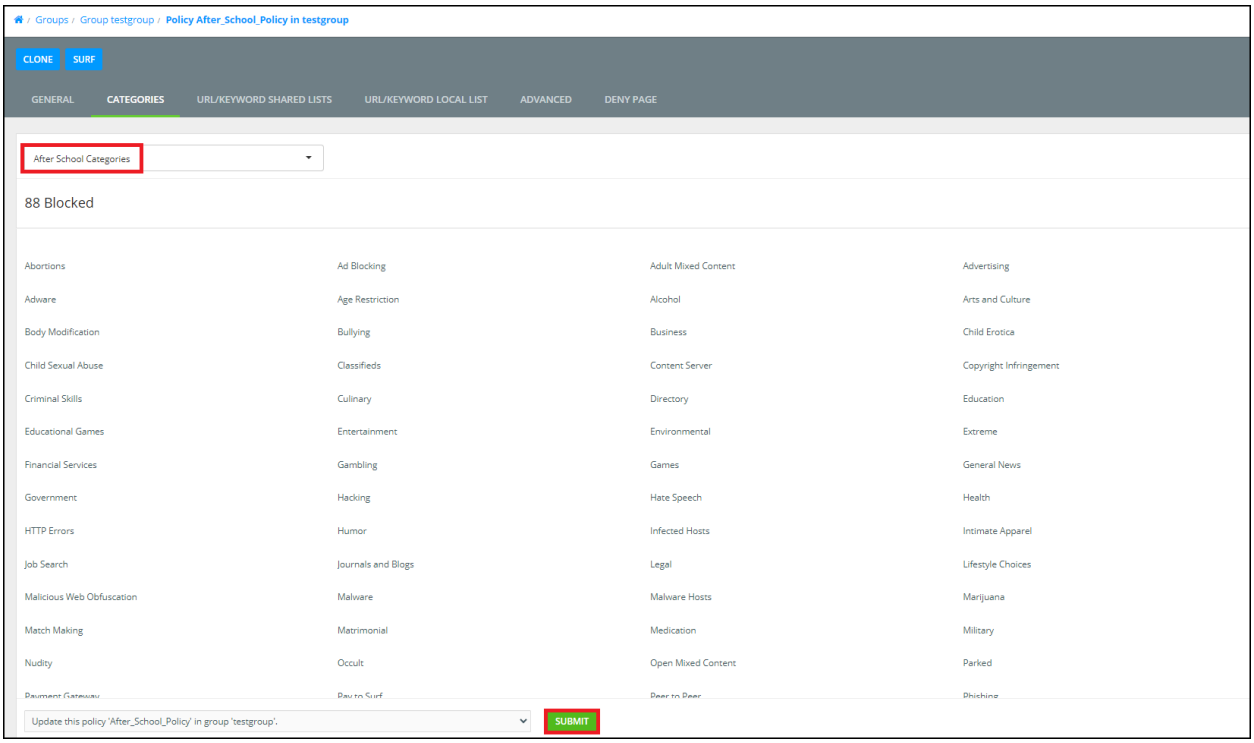


18. Next, navigate to the List subsection of the Policies tab and confirm that the 'After School Policy' and the 'School Hours Policy' are listed.

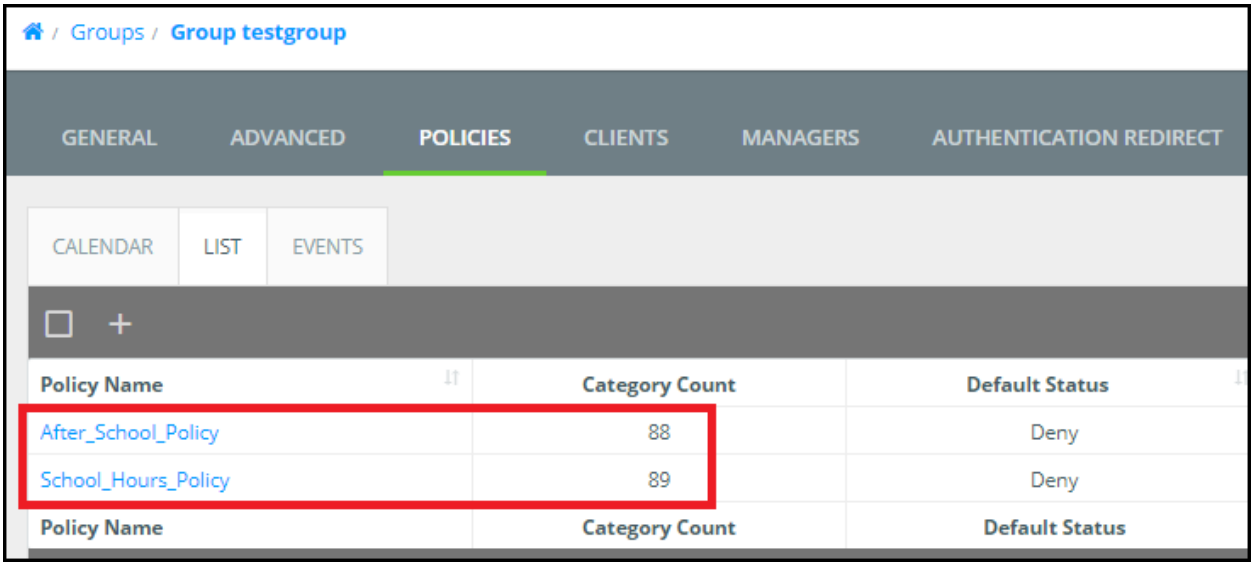


19. Select the 'testpolicy' Policy's row and select the **Delete** button in the Table Header bar.
20. Select the 'After_School_Policy' and then navigate to the Categories tab for that Policy.

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

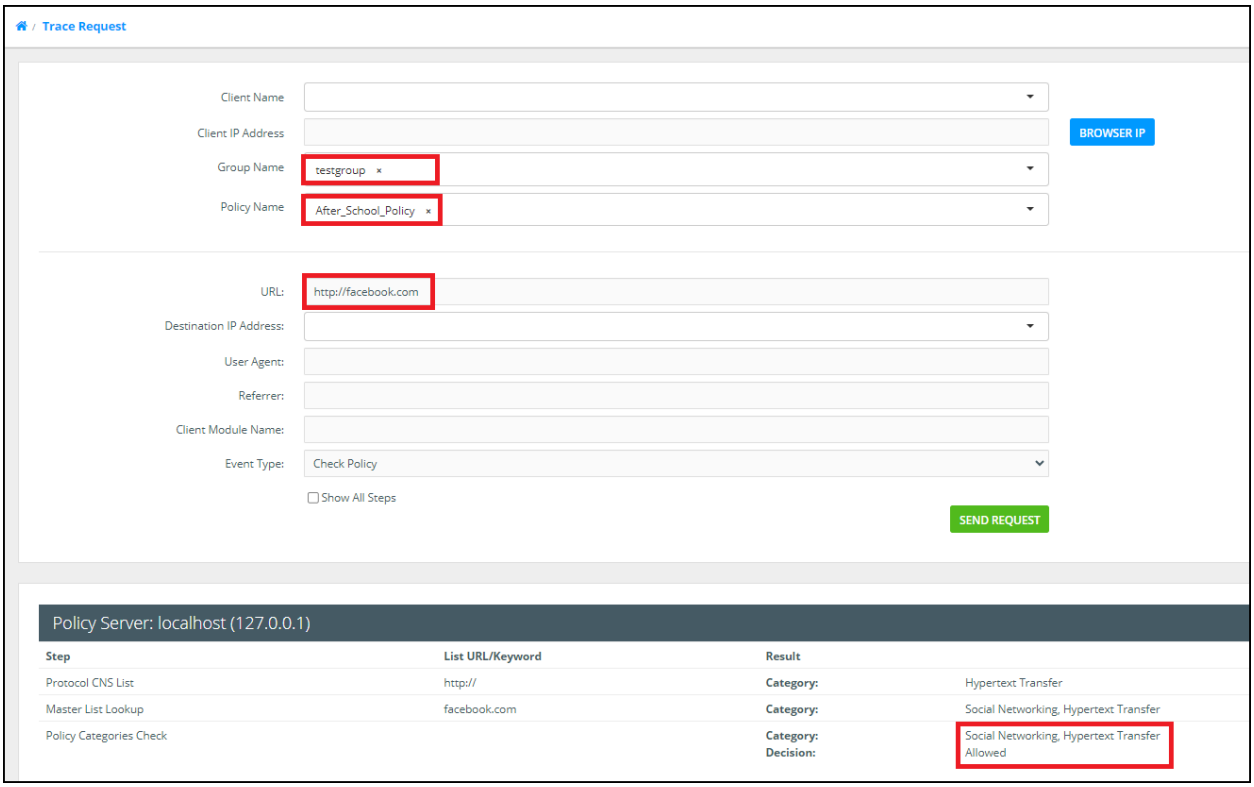


22. Use the breadcrumbs to return to the Group ‘testgroup’.
23. Select the School Hours Policy and repeat the steps to assign the School Hours Categories.
24. When done, verify that the ‘List’ subsection of the ‘Policies’ tab looks like this:

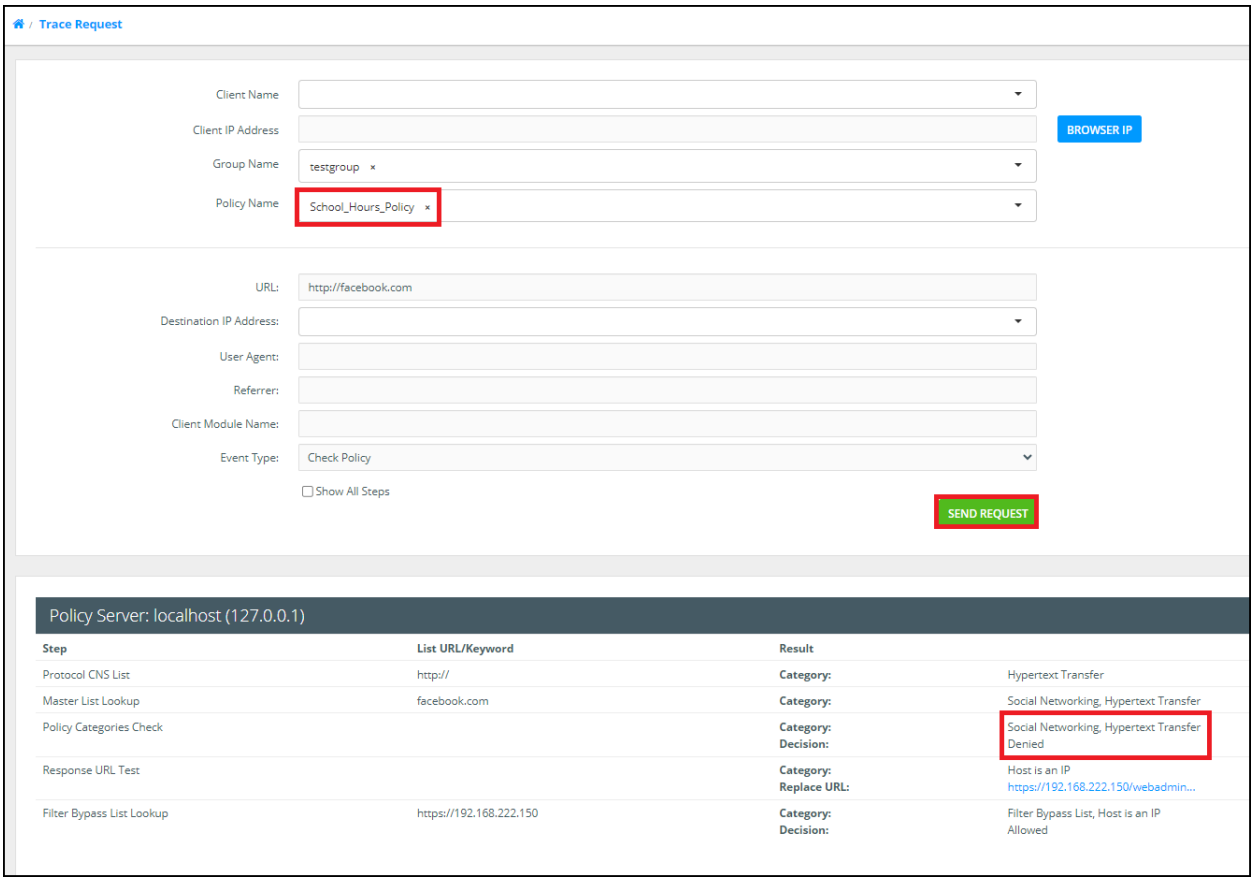


Pass Criteria

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'.



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



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

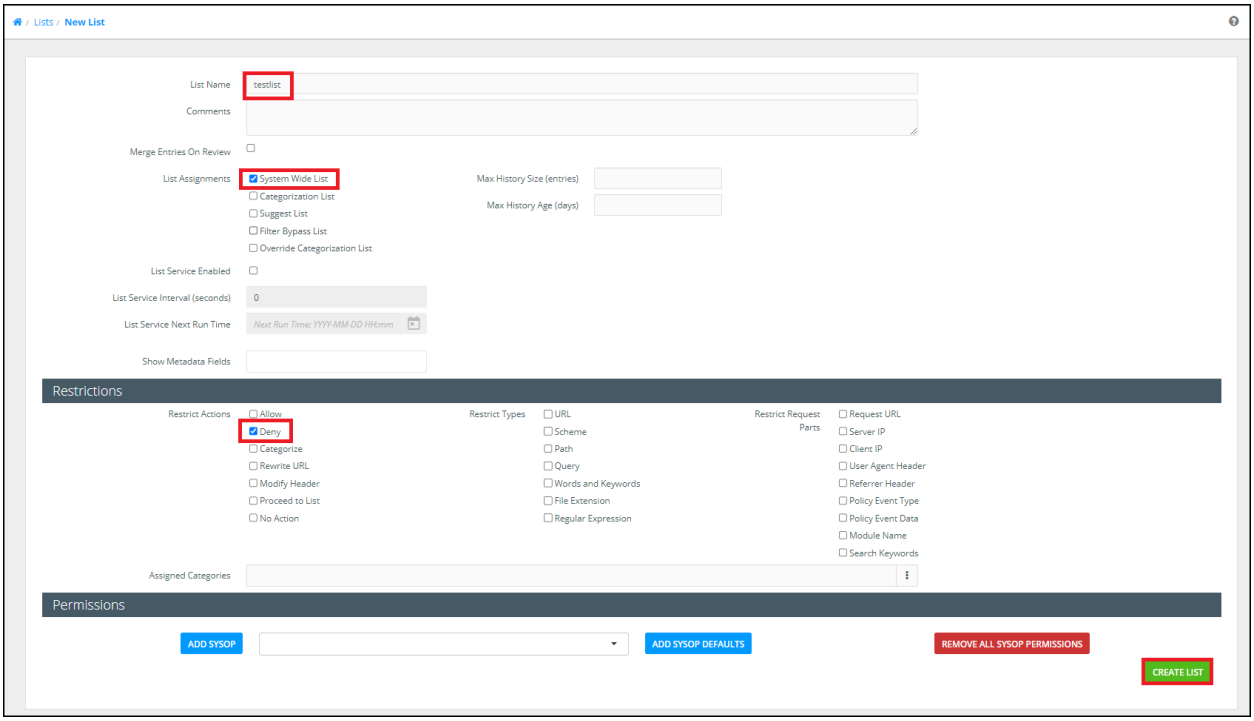
When websites need to be blocked globally, regardless of group policy, then the **System Deny List** is used. URLs placed on this list will be denied for all clients, regardless of group membership and specific policy/list settings.

Precondition

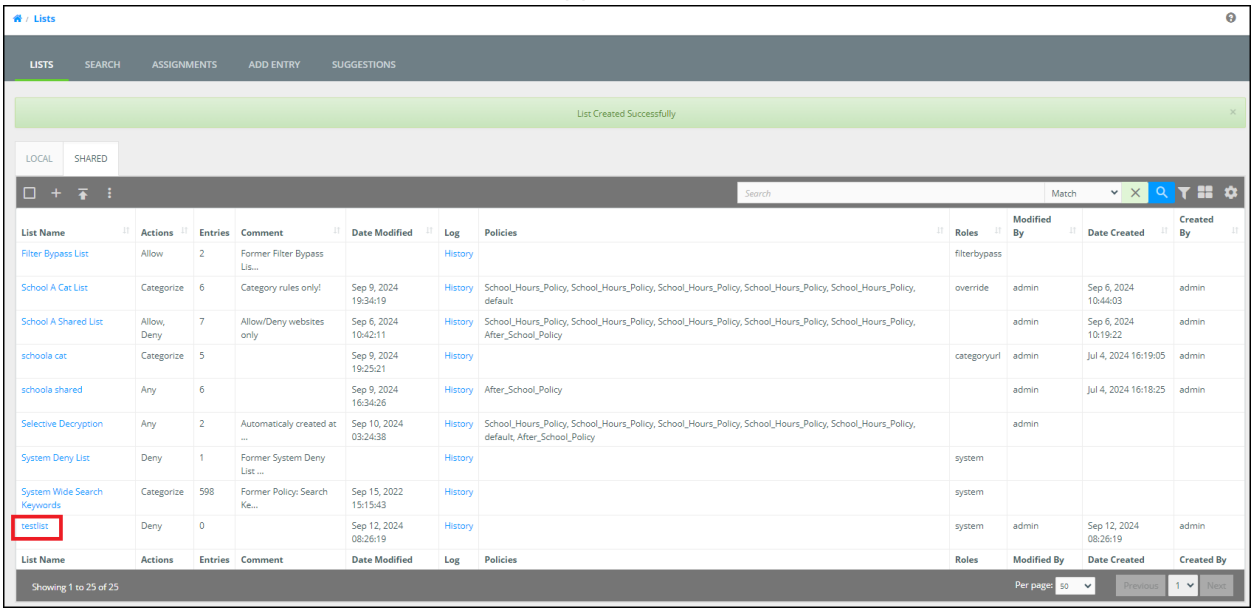
See: Setting up Filtering Group and Client

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’.



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

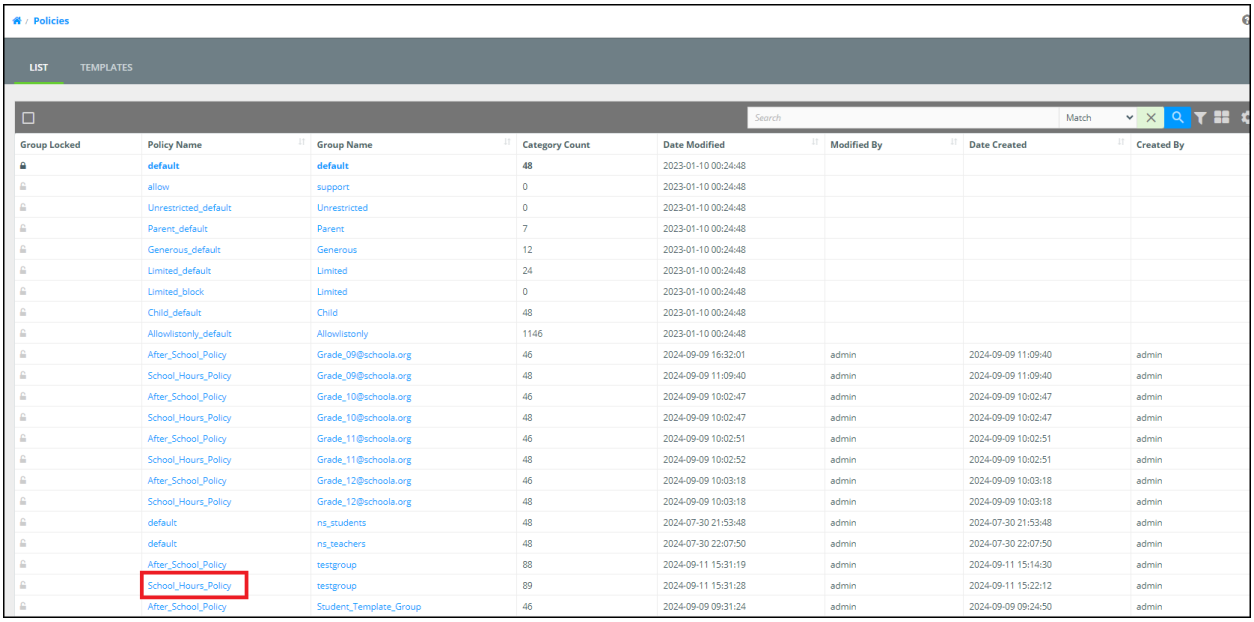


Additional Precondition: Create a Local List

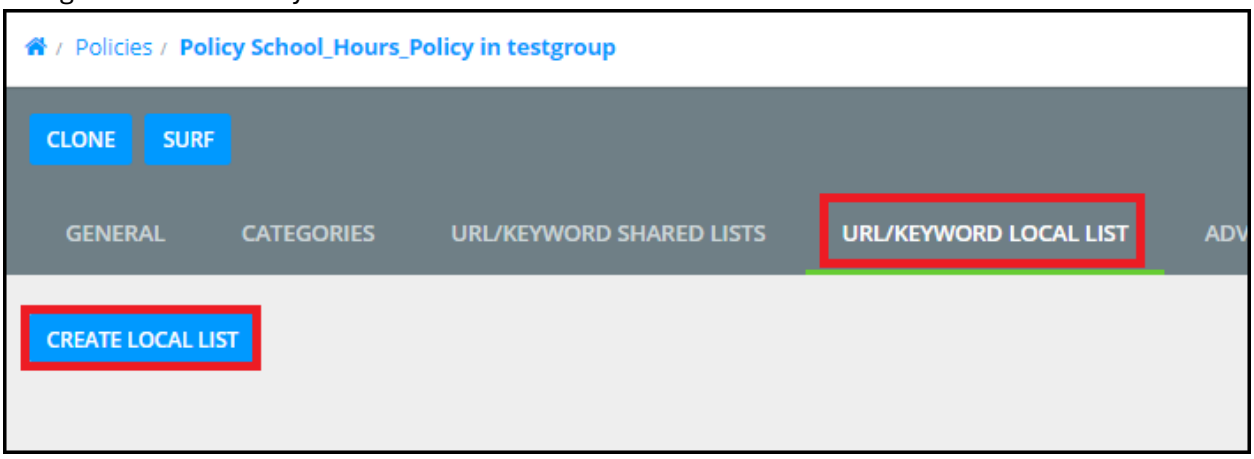
In order to test our System-Wide Deny ‘testlist’, the group our testclient is assigned to must have a Local List that explicitly allows the URL we want to test with.

In the WebAdmin:

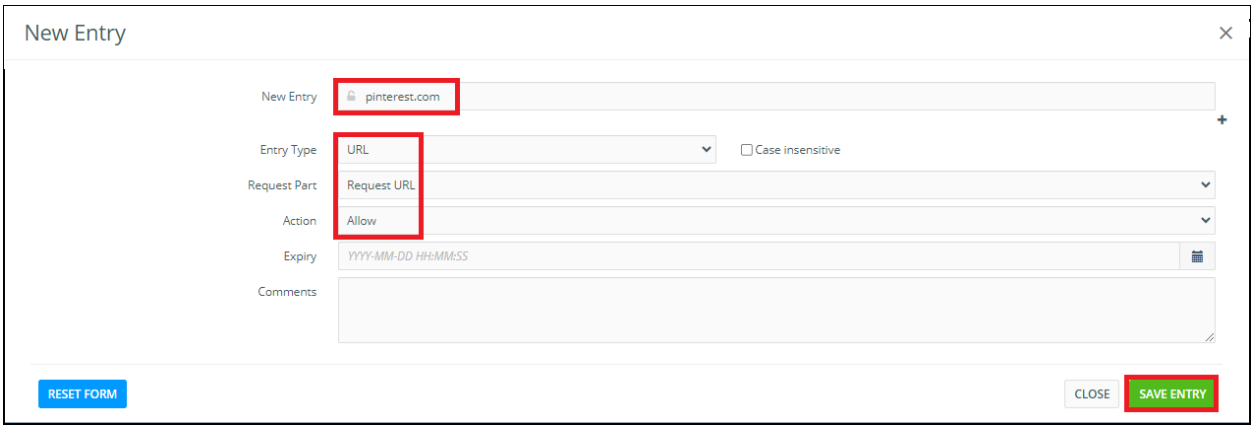
1. Navigate to Policies > Policies to open the Policies window.
2. At the bottom of the page, select the ‘Per page’ setting and increase the value as needed.
3. Choose the ‘School_Hours_Policy’ for our ‘testgroup’.



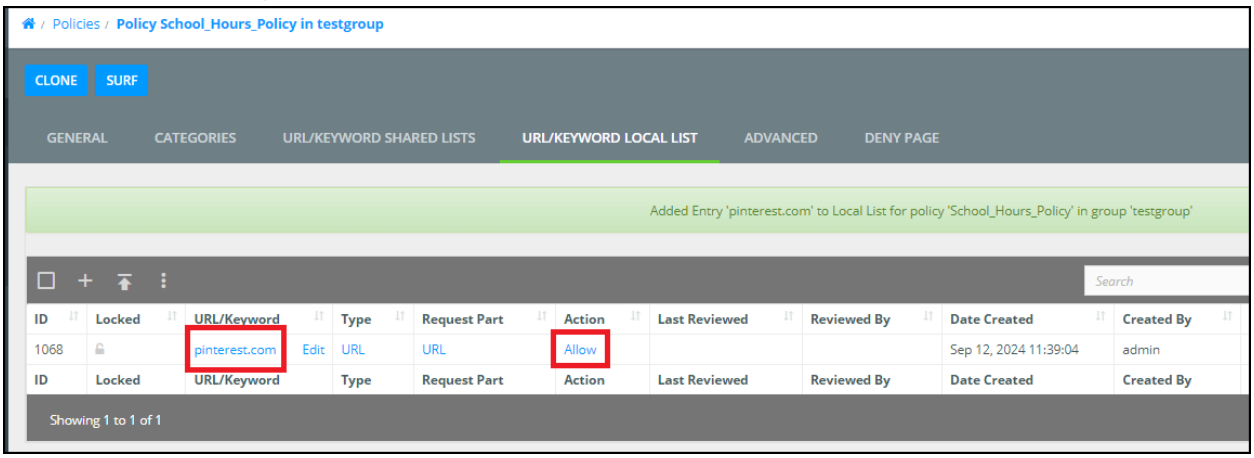
4. Navigate to the URL/Keywork Local List tab and select the **Create Local List** button.



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**.

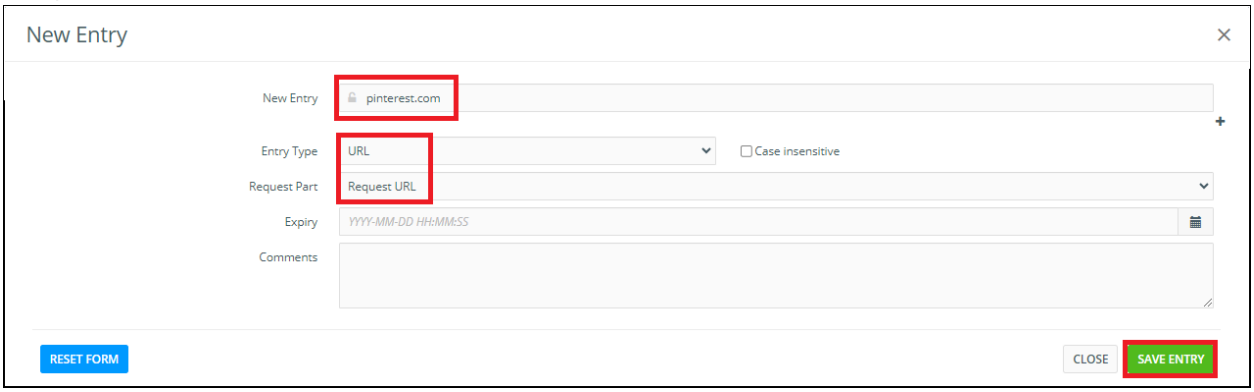


10. Select the **Save Entry** Button. The URL is added to the Local List.

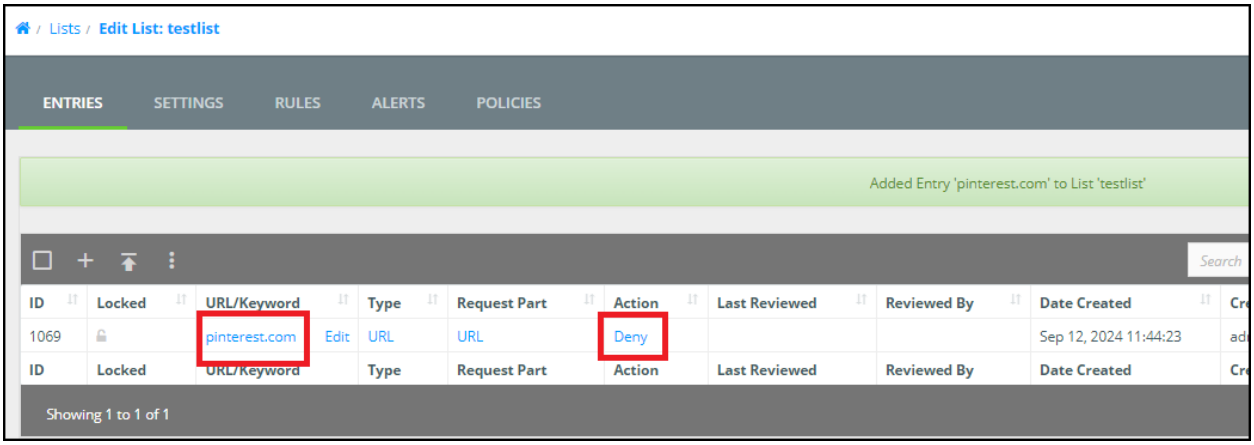


Modify the System-Wide List:

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.

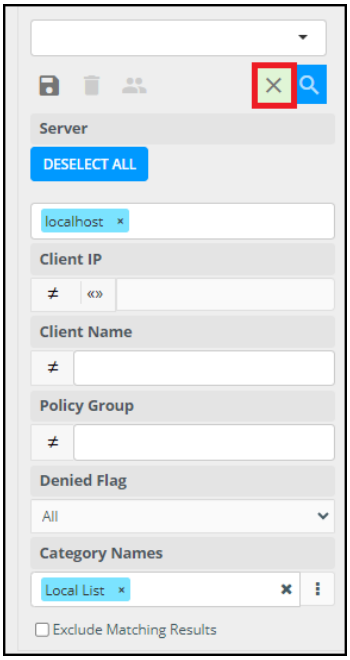


7. Select the **Save Entry** button.
8. The Deny entry is added.

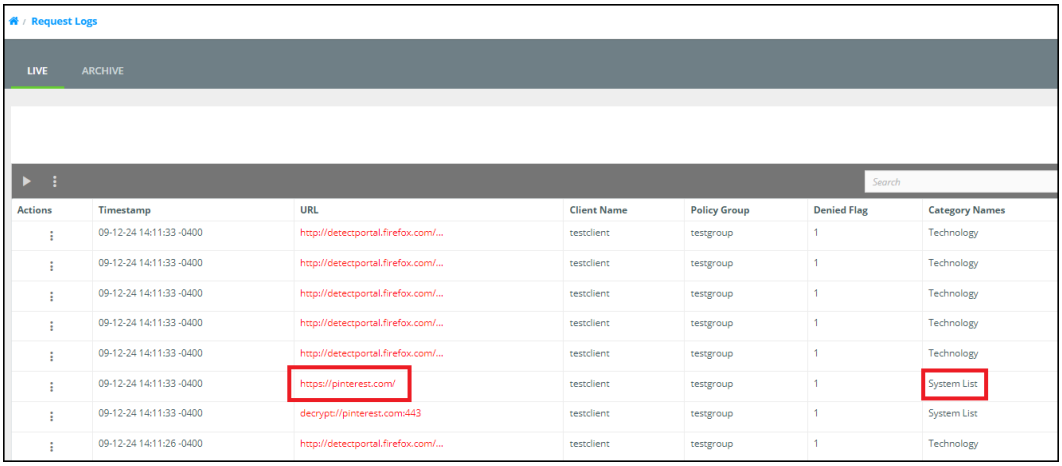


In Your WebAdmin:

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.



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'.



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

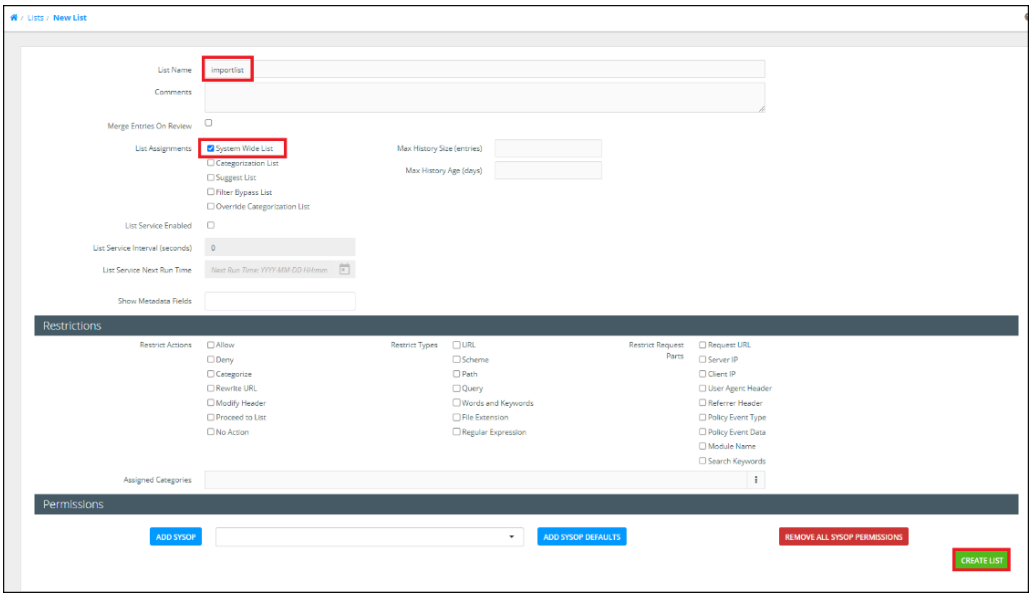
The Netsweeper solution provides functionality for importing long System Lists (allow and deny.) Typically, these lists come from an external list (CSV file, spread sheet, etc.). This test case verifies the system list import feature.

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.



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.

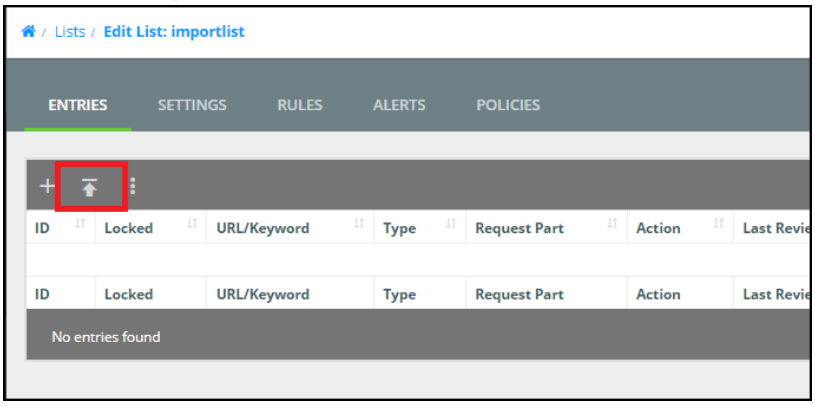
URL/Keyword	Type	Action	Action Arguments	Comments	Case Insensitive	Request Part
http://paypal.com	U	D			0	U
http://pinterest.com	U	A			0	U

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

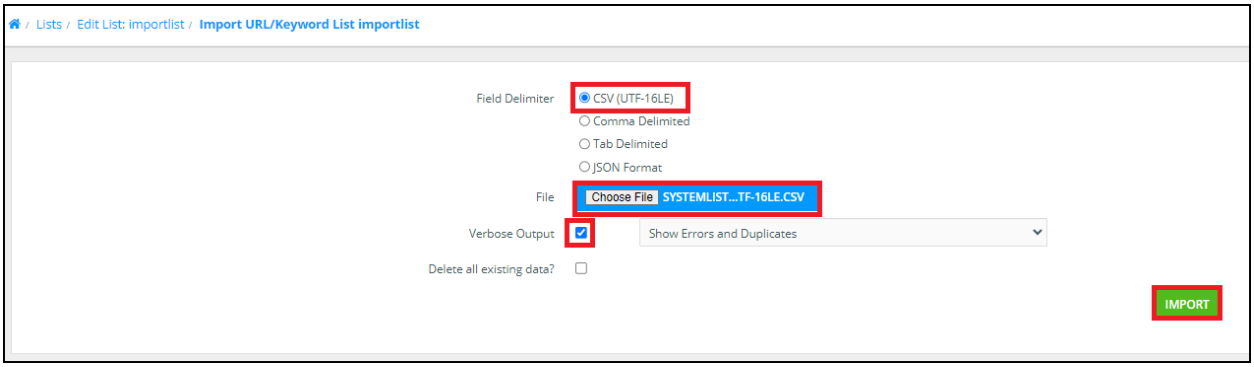
Test Procedure: Importing a System List

In the WebAdmin:

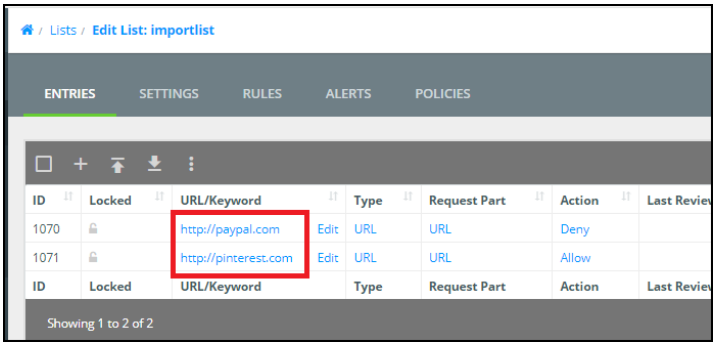
1. Navigate to Policies > Lists and select the **Lists** tab.
2. Choose the 'importlist' we created previously.
3. Select the **Import** button.



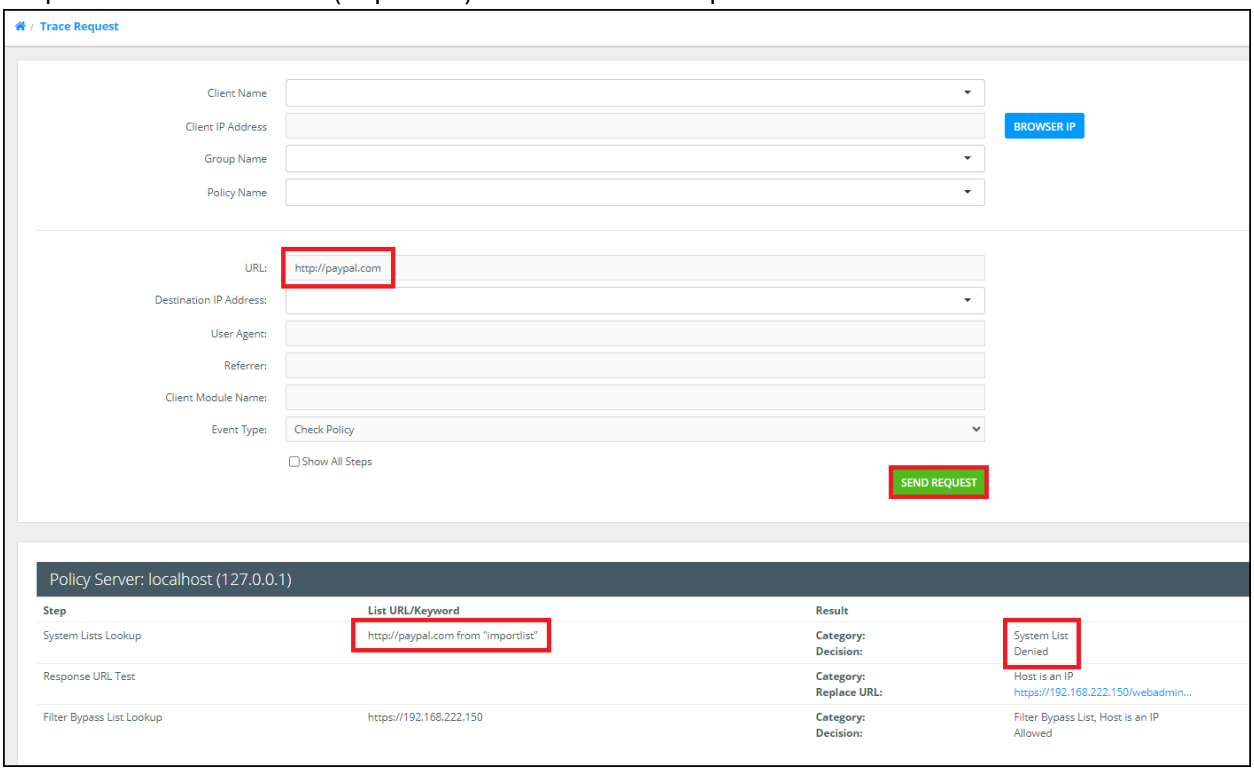
4. In the 'Import URL/Keyword List' window, leave the **Field Delimiter** set to 'CSV (UTF-16LE)'
5. Select the **Choose File** button and add your newly downloaded (or created) file.
6. Select the checkbox for **Verbose Output**.
7. Select the **Import** button.



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.



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

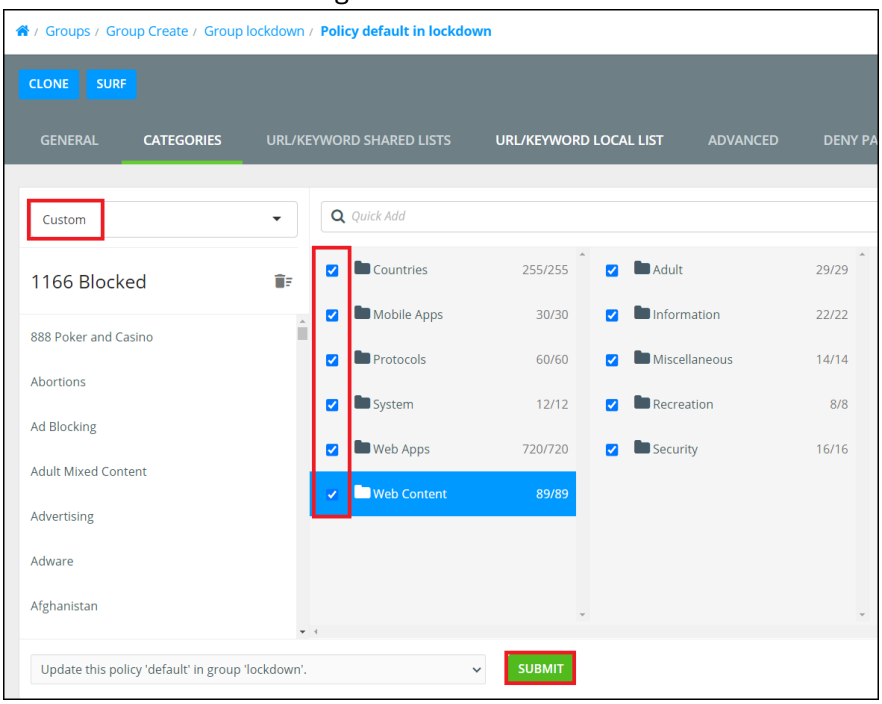
A filtered Client workstation must be available for browsing the Internet and the IP address of the filtered workstation should be within a known network subnet.

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

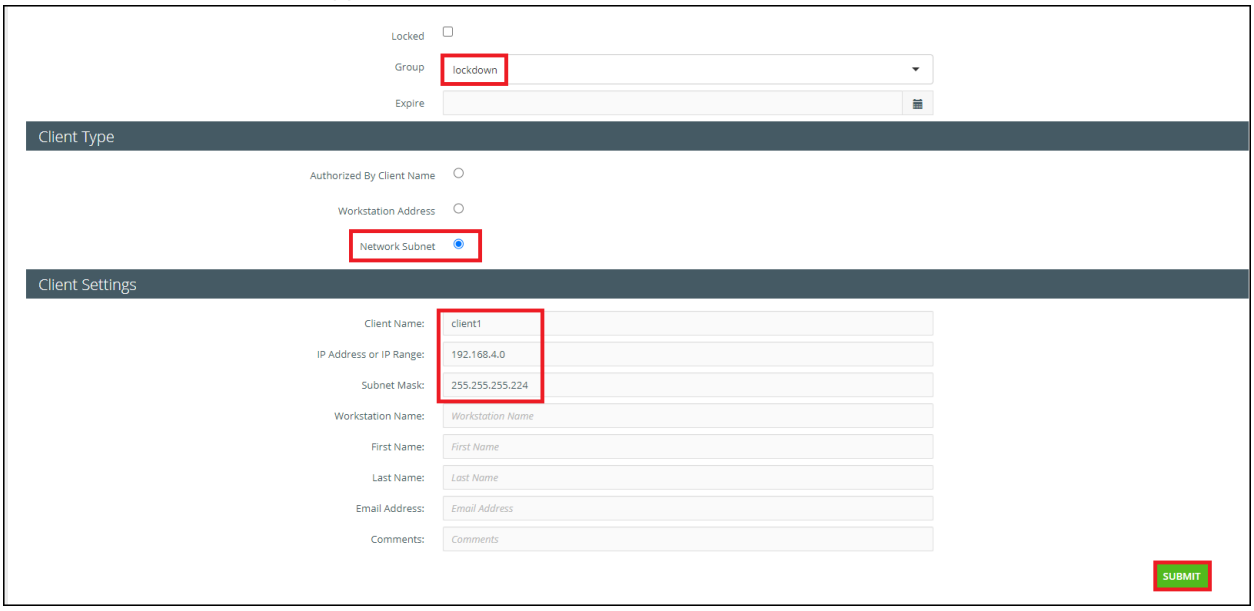
In The WebAdmin:

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.



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



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.

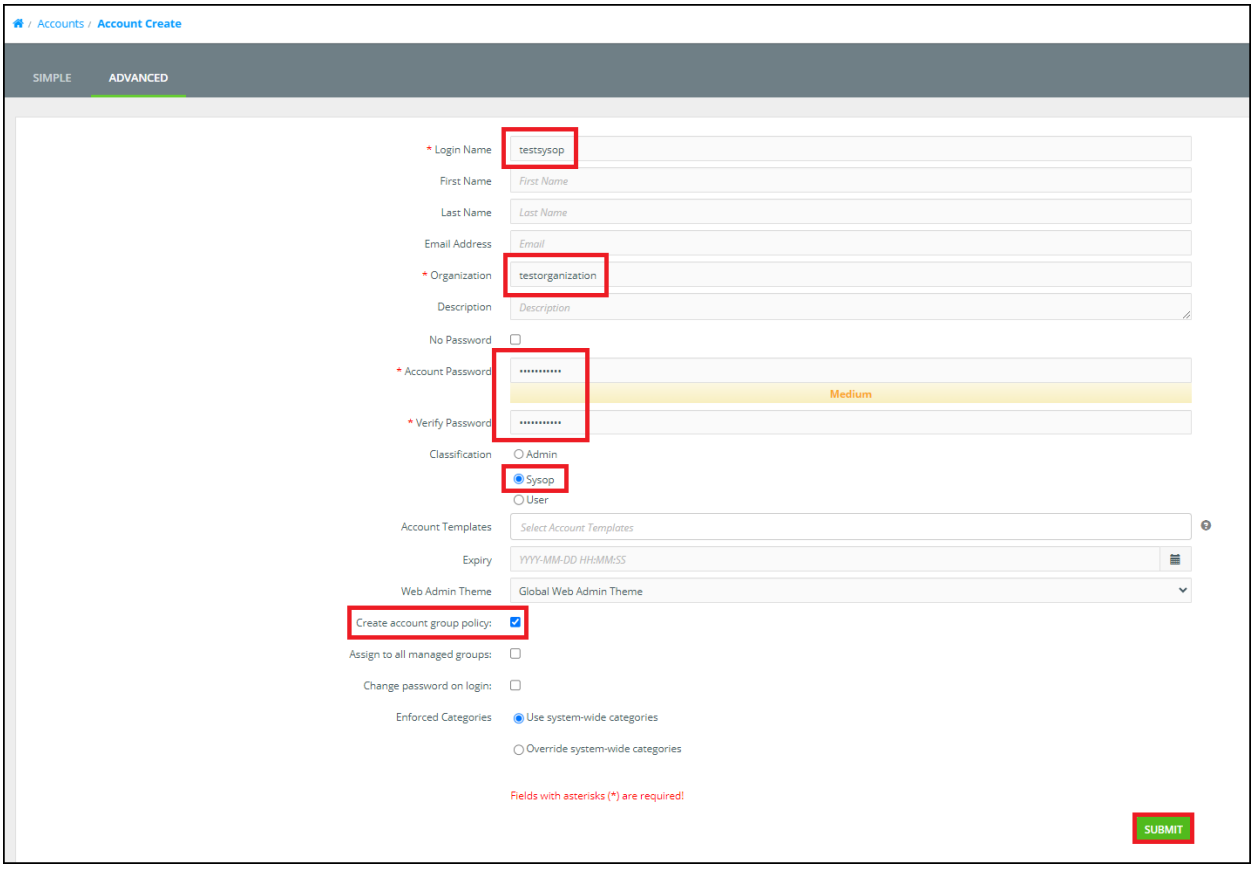
Precondition:

SysOp Permissions

Create testsysop1:

In The WebAdmin:

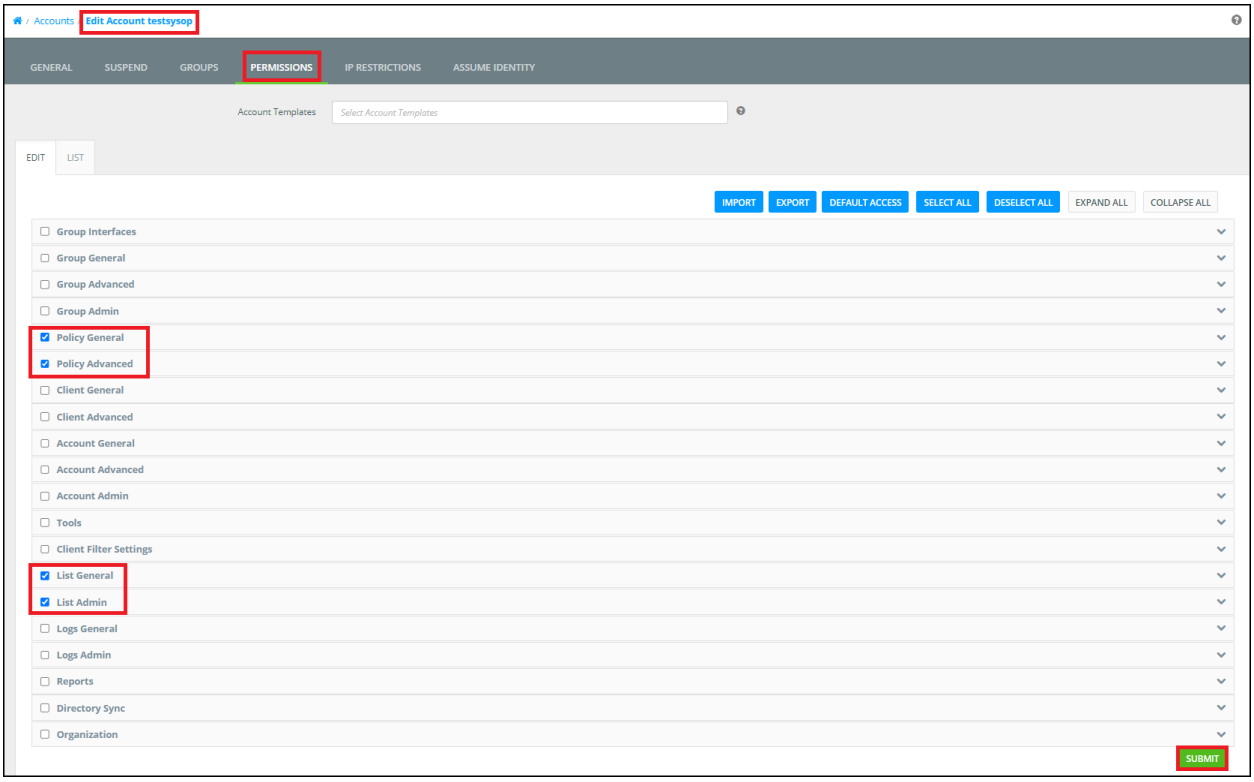
1. Navigate to Accounts > Accounts and select the **Create** button.
2. Choose the **Advanced** tab.
3. Enter the Login Name testsysop1 and testorganization in the Organization field.
4. Enter and confirm a password, 'Netsweeper1' and choose **Sysop** as the 'Classification'.
5. Check the box marked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



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:



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.

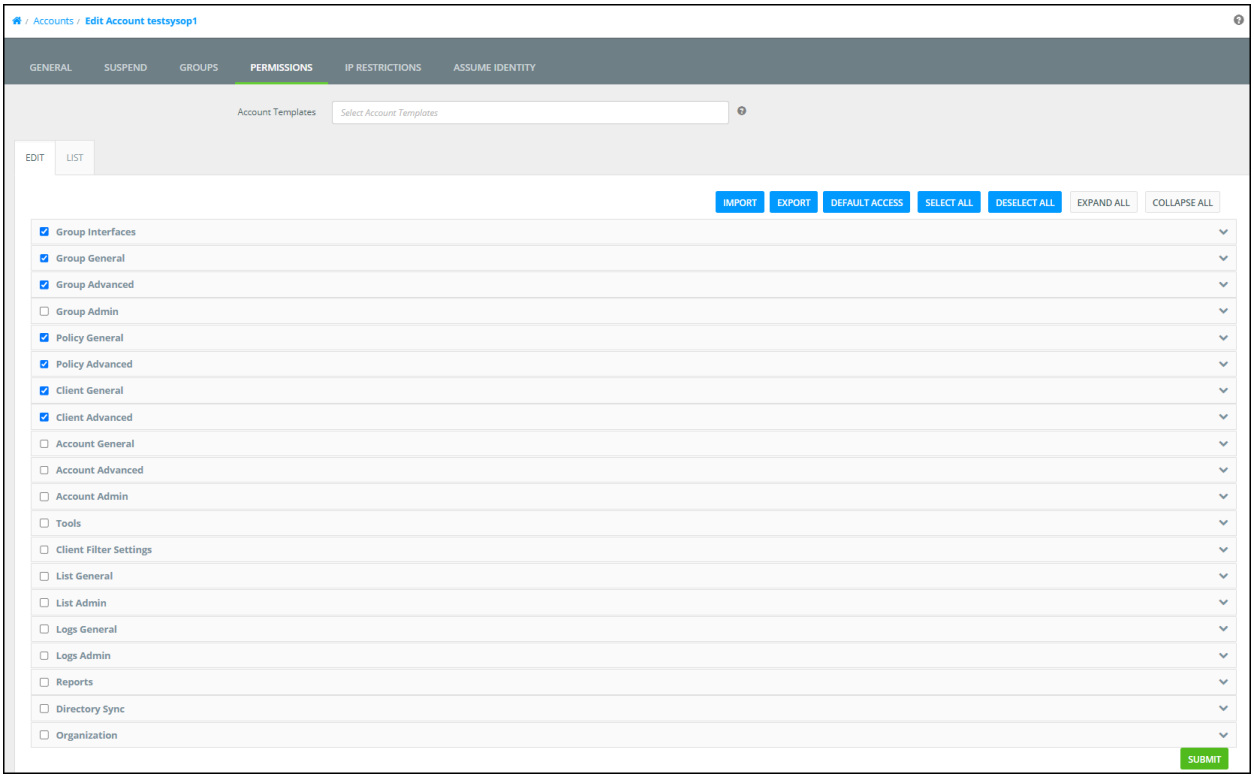
Preconditions

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.



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

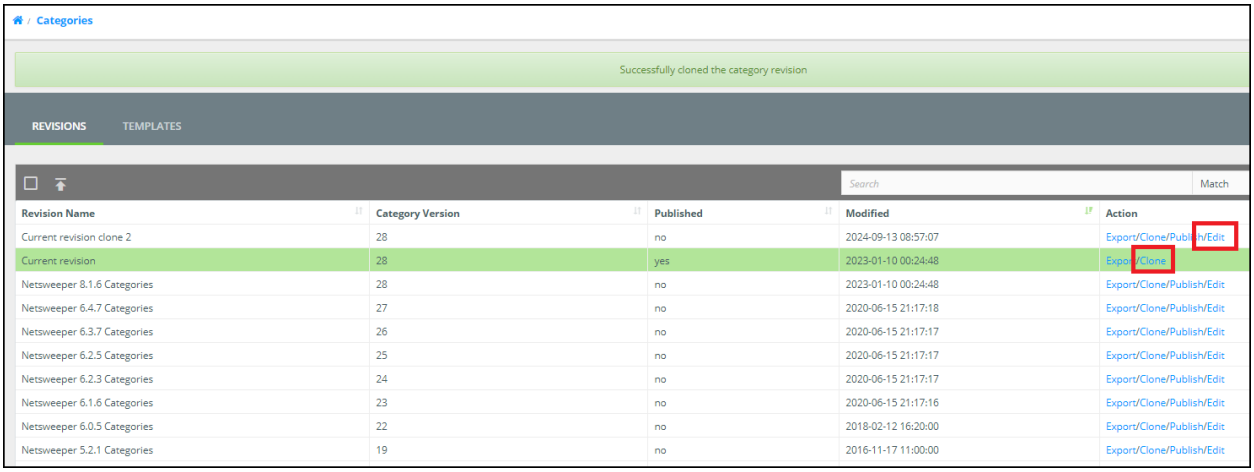
See: Setting up Filtering Group and Client

Only the Category Deny List should be filtered.

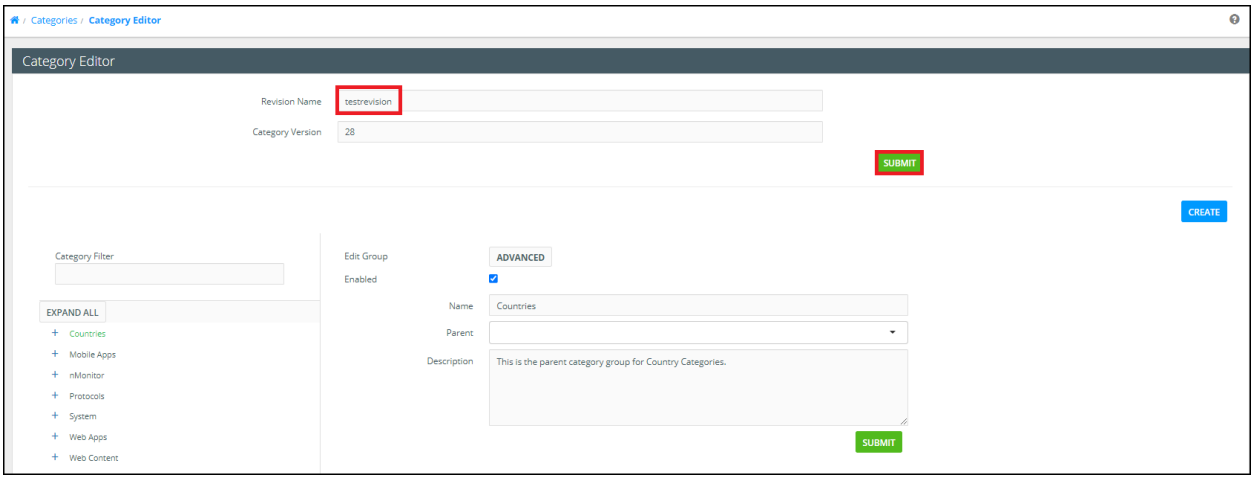
Test Procedure 1: Creating a Custom Category

In the WebAdmin:

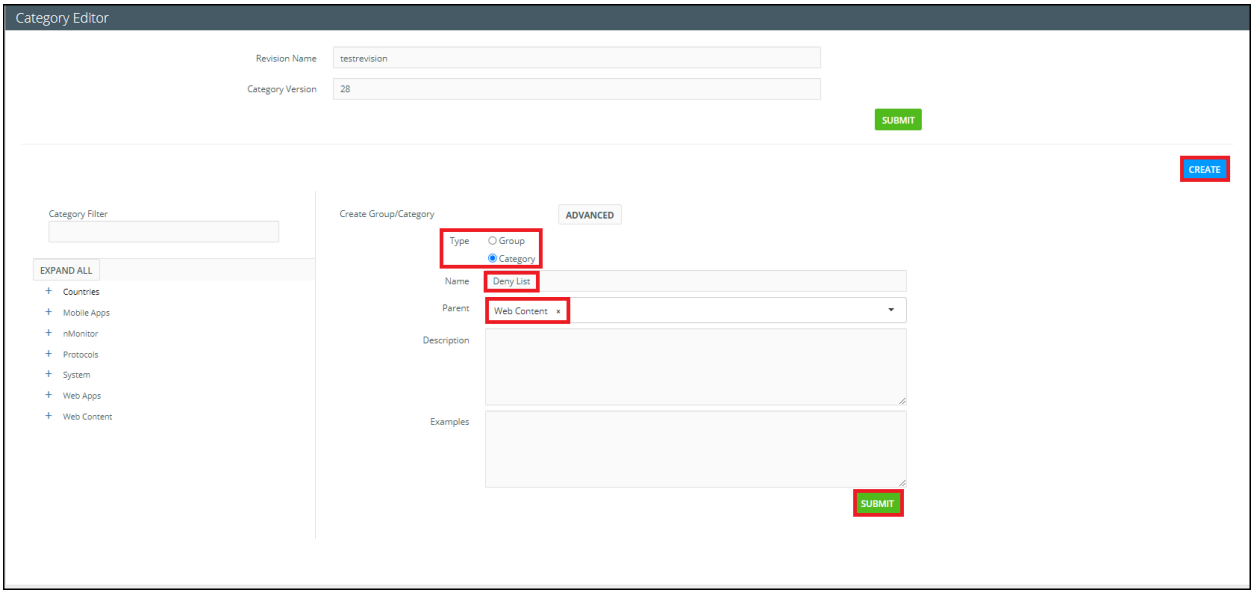
1. Navigate to Administration > Categories.
2. Select the **Clone** button in the Action column for the Current Revision.
3. Select the Edit button for the newly cloned Revision.



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.



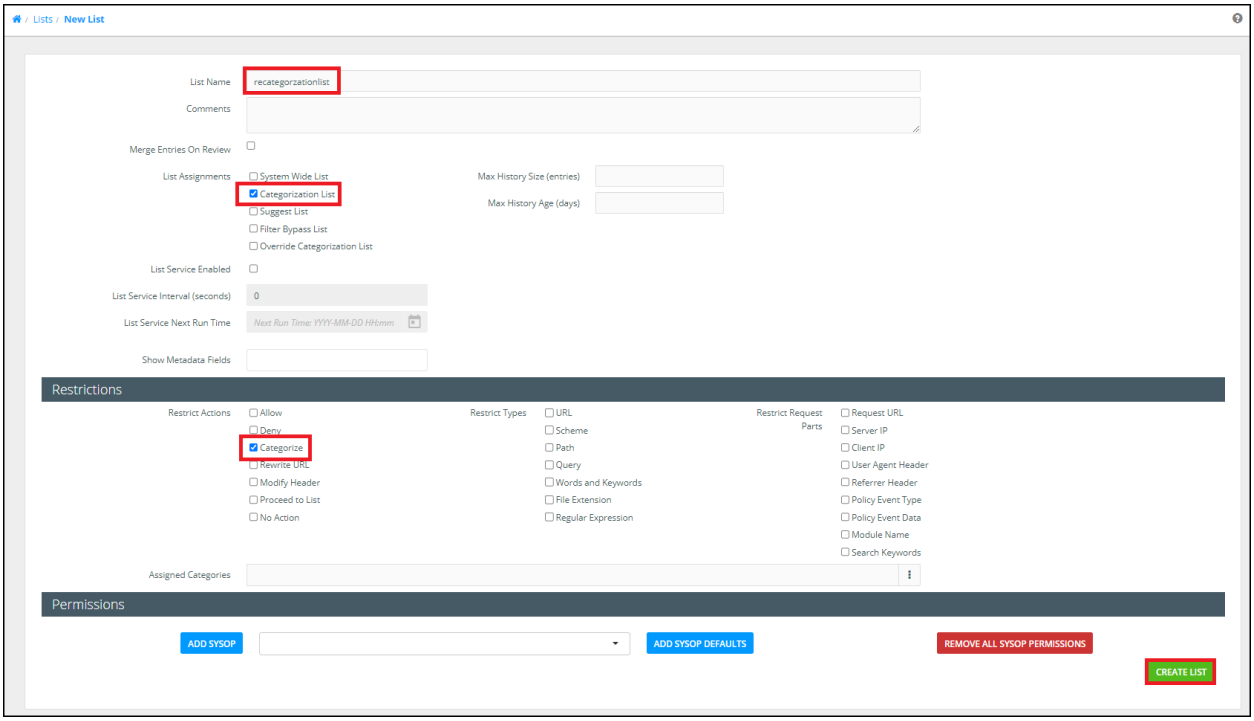
8. Select **Submit**. The new Category displays under the 'Web Content' grouping.
9. Use your breadcrumbs to return to the **Categories** window.
10. Choose the **Publish** button beside the testrevision and select **OK** when prompted.

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

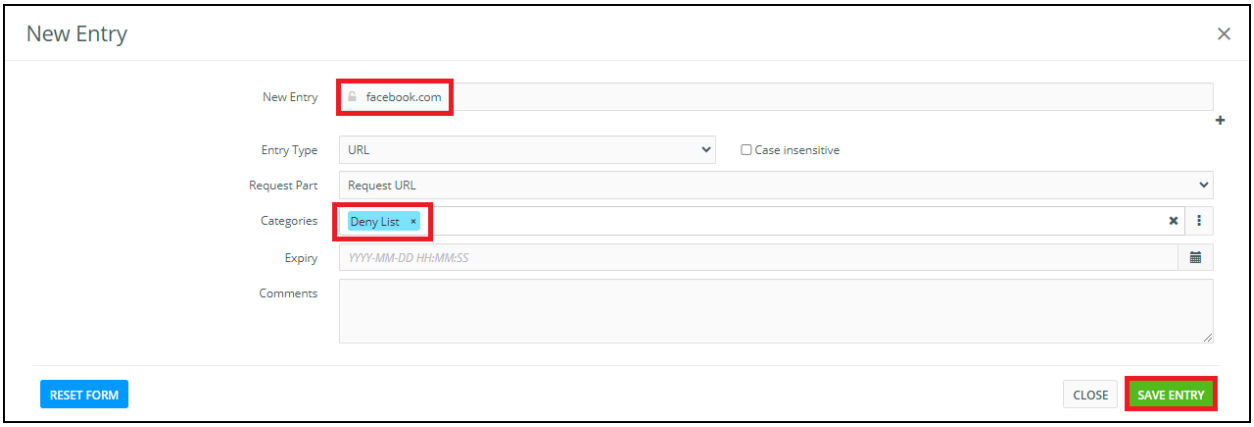
1. navigate to Policies > Lists and select the **Create** button.
2. Enter recategorizatoinlist for this 'List Name'.
3. In the 'List Assignments' section, choose the **Categorization List** option.
4. In the 'Restrictions' section, choose the **Categorize** 'Restrict Action'.



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**.

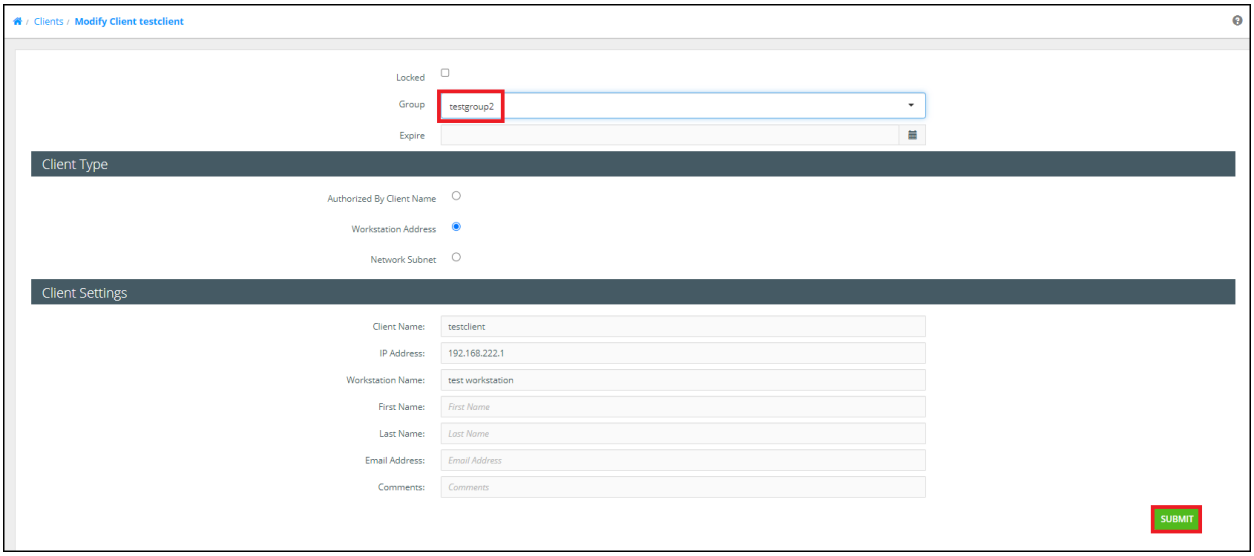


5. Select **Save Entry**. The new entry is added.
6. Repeat steps 2-5 for two new URLs of your choice that have not been used previously.

Adding testclient to testgroup2

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

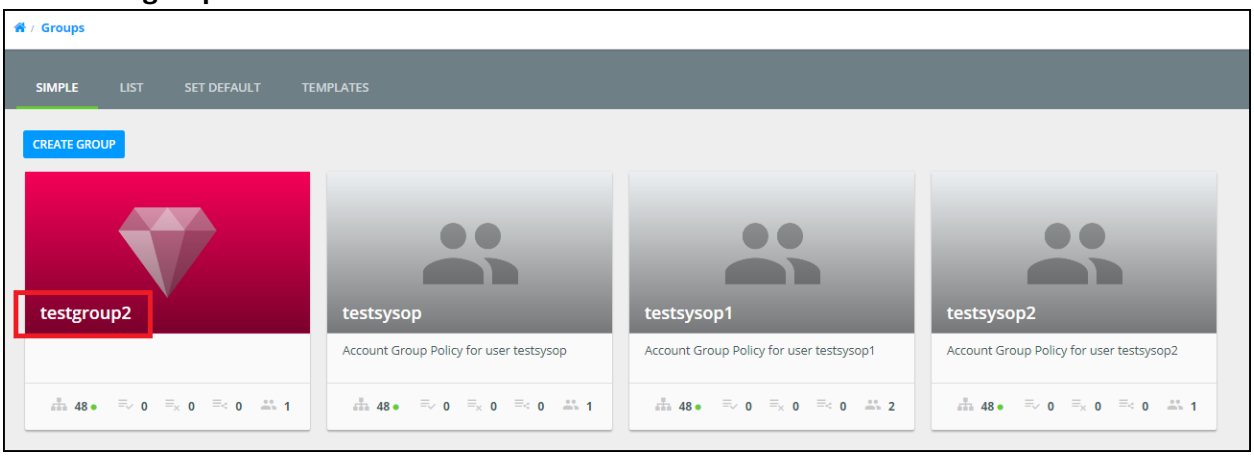
1. Navigate to Policies > Clients.
2. Choose the **testclient** Client.
3. Assign the Client to testgroup2 by choosing it from the **Group** dropdown.



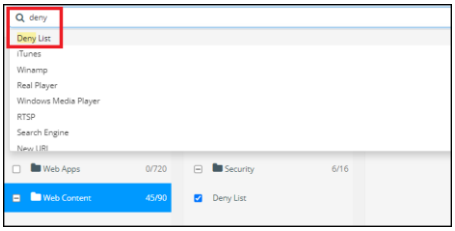
4. Select **Submit**.

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.

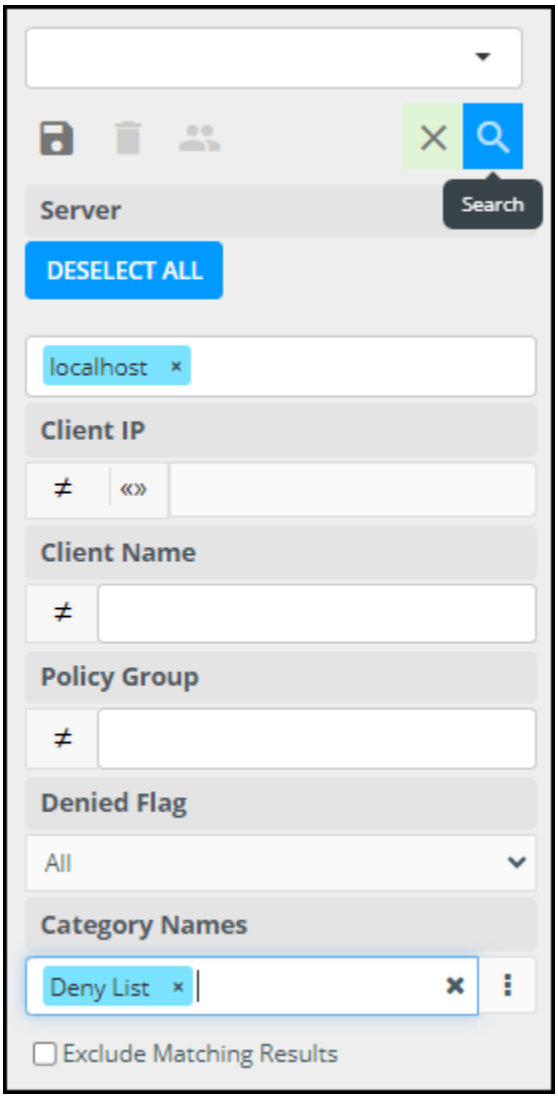


5. Select **Submit**. This will block the 'Deny List' category for this Group.

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.



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.

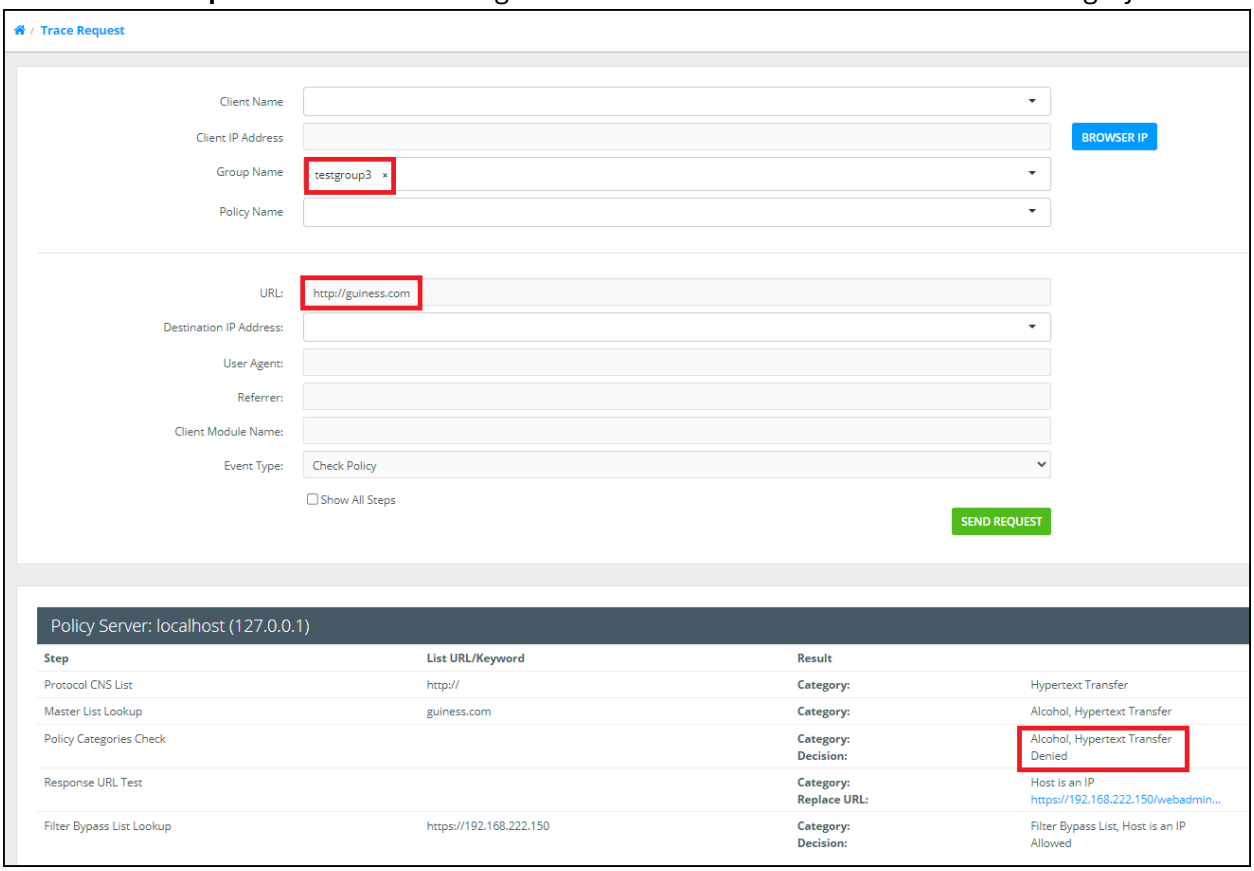
Precondition

See: Setting up Filtering Group and Client

Test Procedure: Allow List Mode

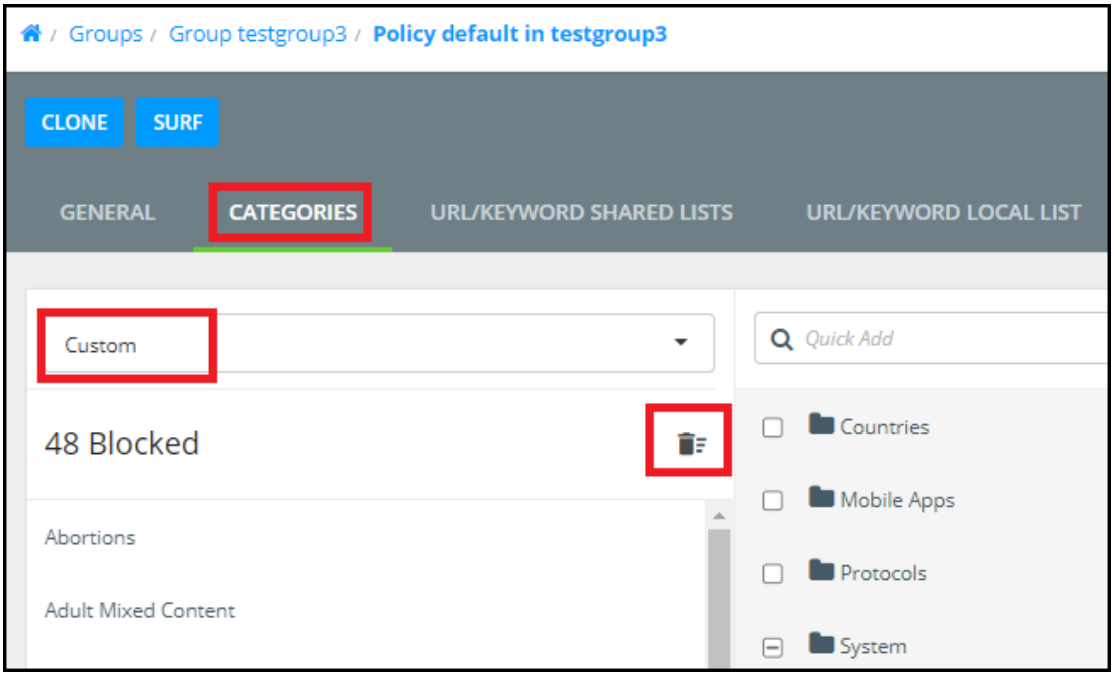
In the WebAdmin:

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 guiness.com in the URL field.
4. Select **Send Request** and confirm that guiness.com is denied under the 'Alcohol' Category.



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

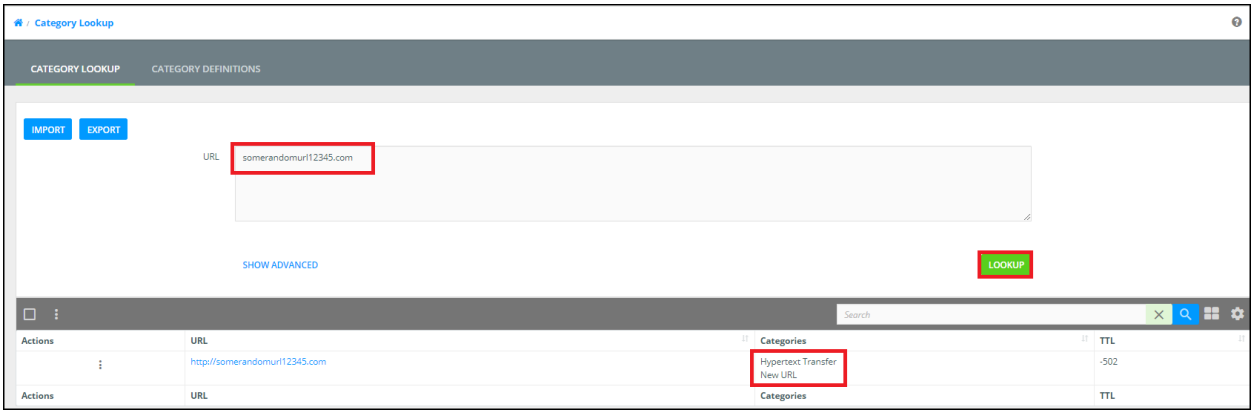
This test verifies that New URLs (not present in any lists or the cache) are categorized first as New URL and then later with a Netsweeper Categorization.

Precondition

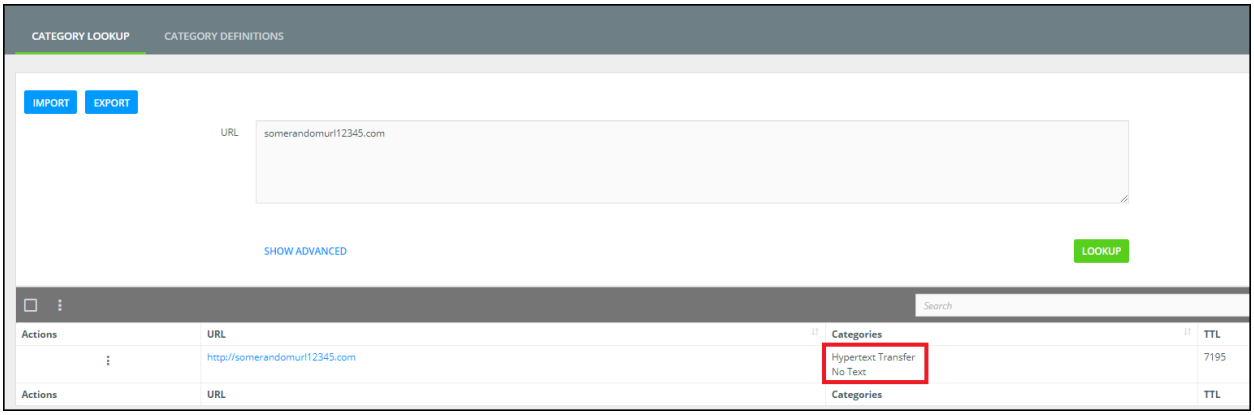
CNS connectivity with your Netsweeper Policy Server.

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.

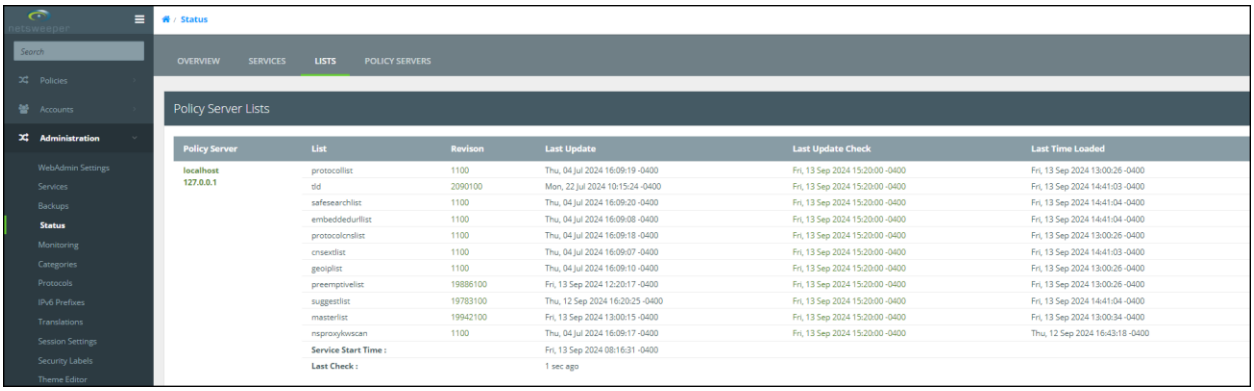
Test Procedure: List Update

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.



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.

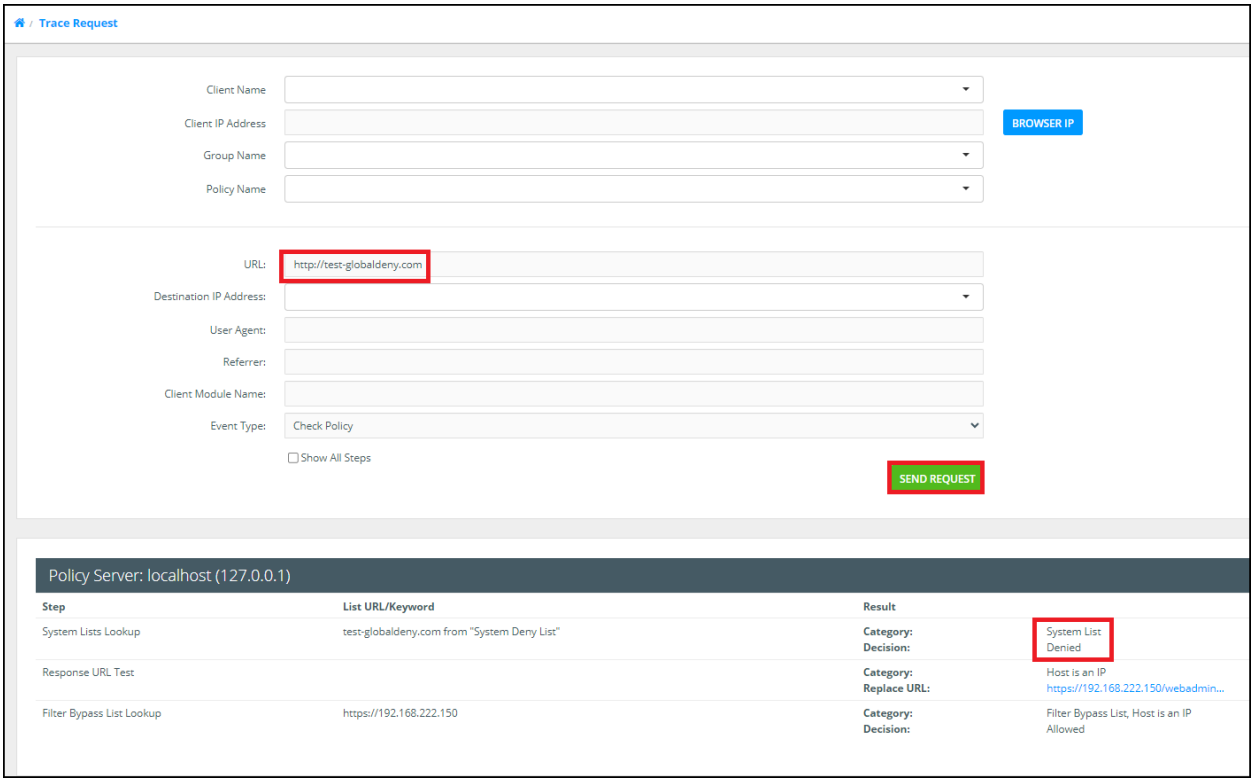
Precondition

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-globalydeny.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**.



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.

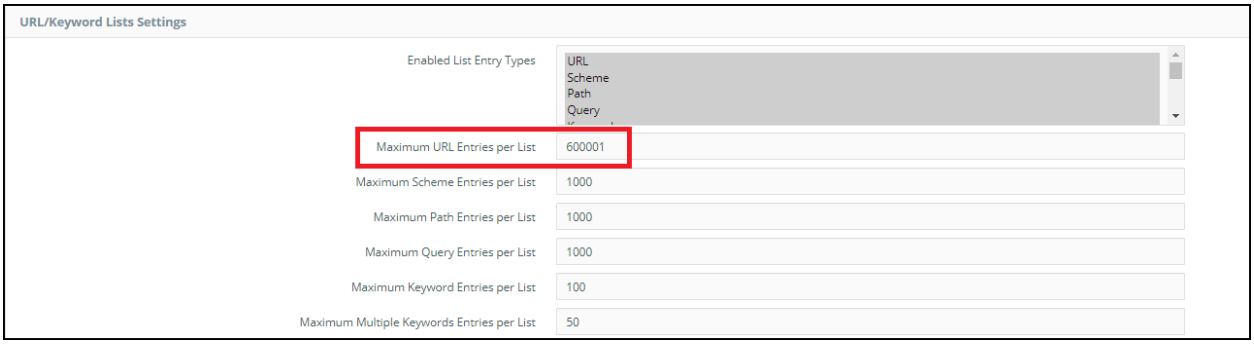
NOTE: RESET POL DB & RECREATE PIC/TEXT WAS HERE

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.



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'\

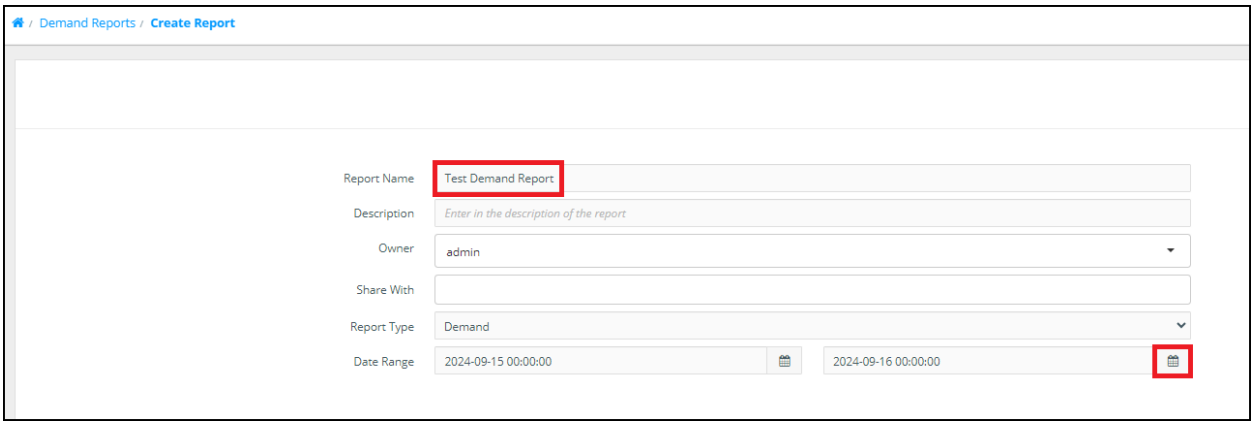
Test Procedure

On the Test Workstation:

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

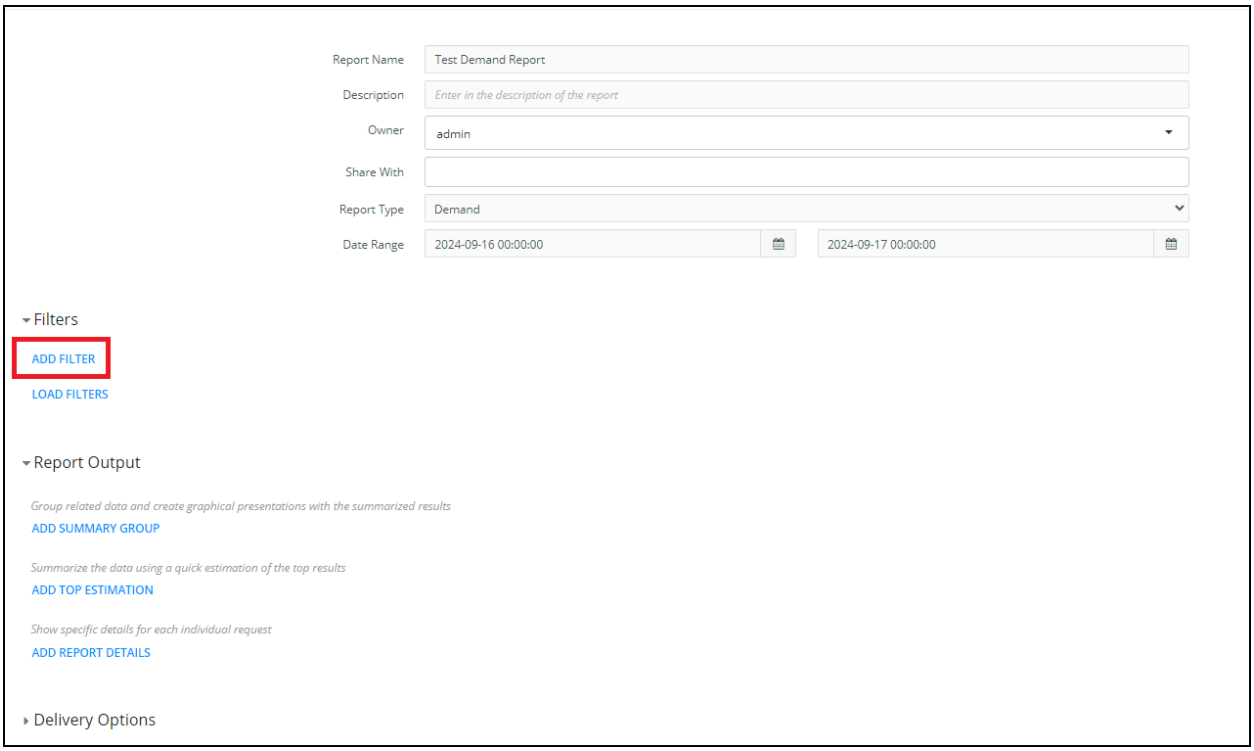
In the WebAdmin:

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).

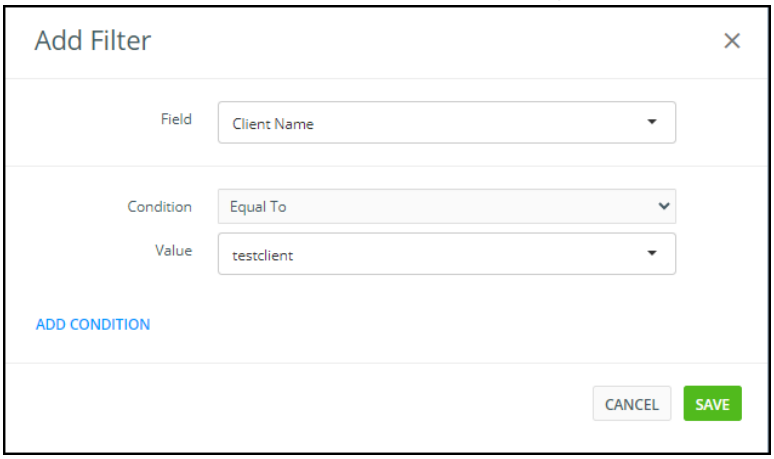


4. Use the calendar to set the 'date' value to tomorrow's date and select **OK**.

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

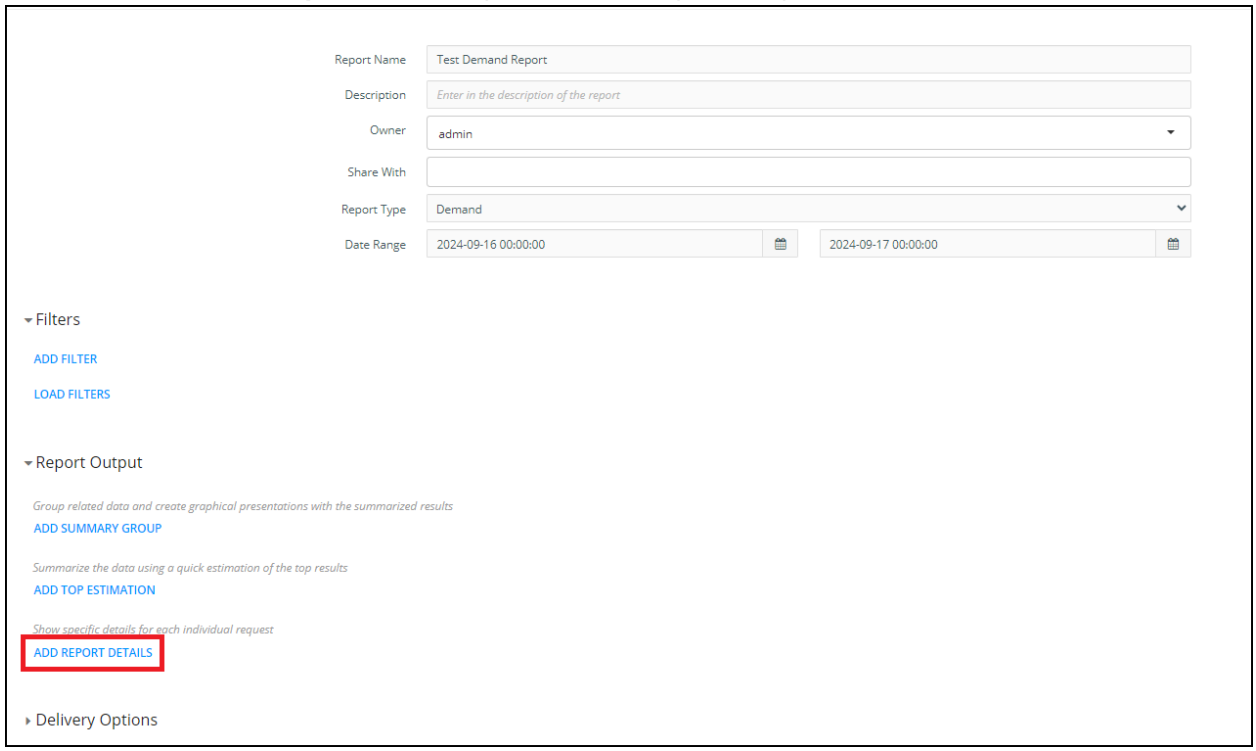


6. Set the 'Field' value to **Client Name**, leave the 'Condition' set to **Equal To,** and in the 'Value' field, choose the **testclient** associated with your test workstation.

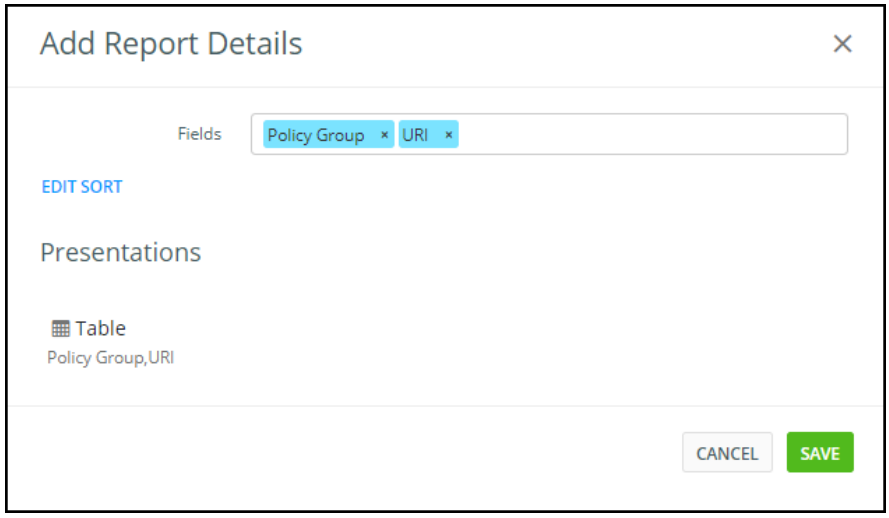


7. Select **Save** to apply the Filter.

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

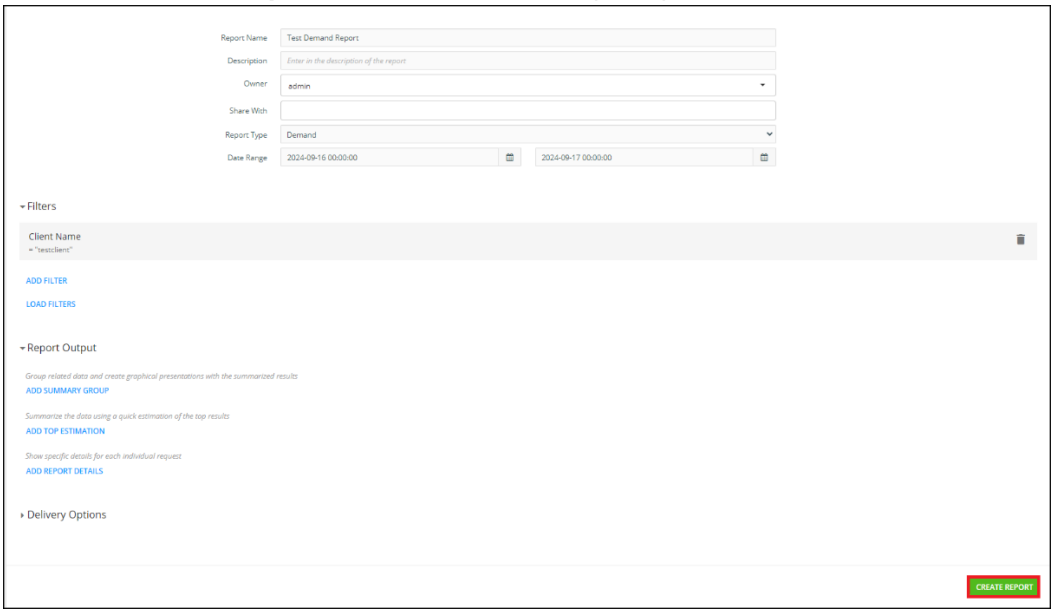


9. Select the **Policy Group** and **URI** fields, accept Table as the Presentation type.

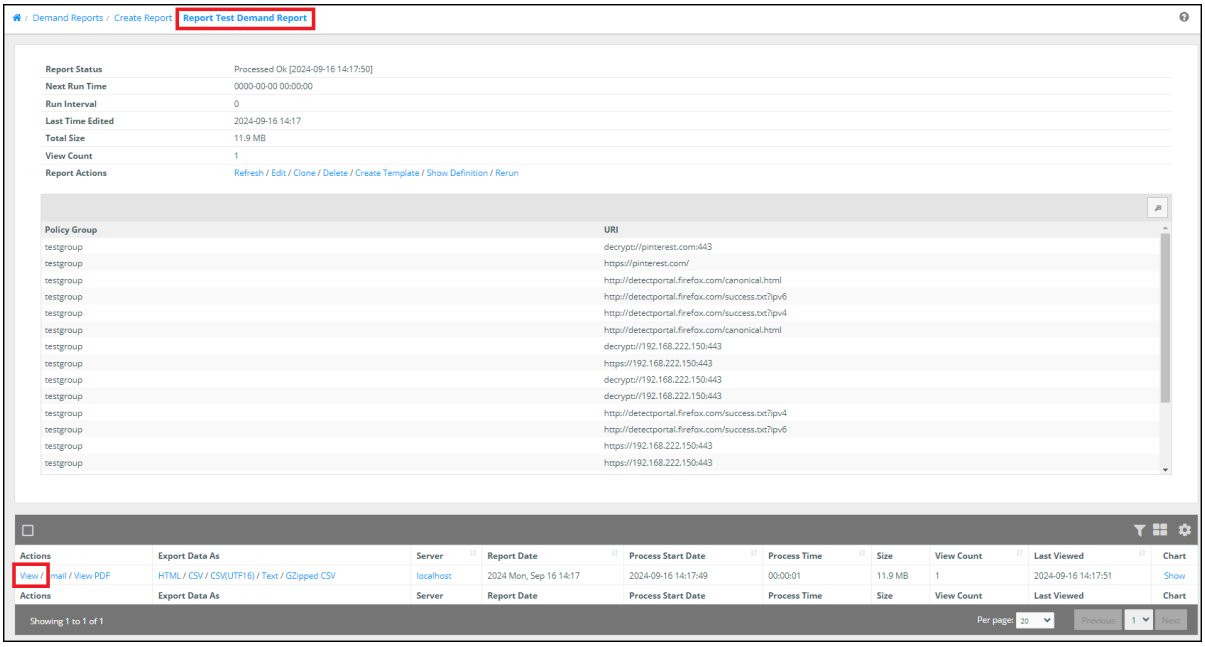


10. Select **Save** to apply the Report Details.

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



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



Pass Criteria

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

Notes	
Results (Pass or Fail)	
Results Comments	

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

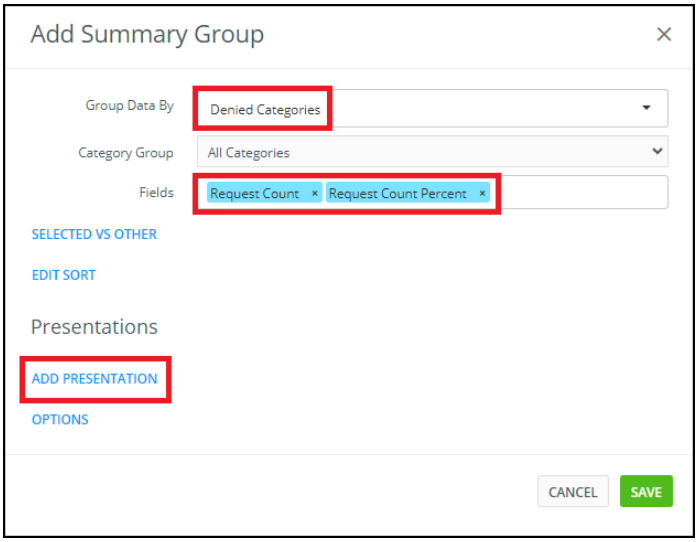
See: Setting up Filtering Group and Client

On the Test Workstation:

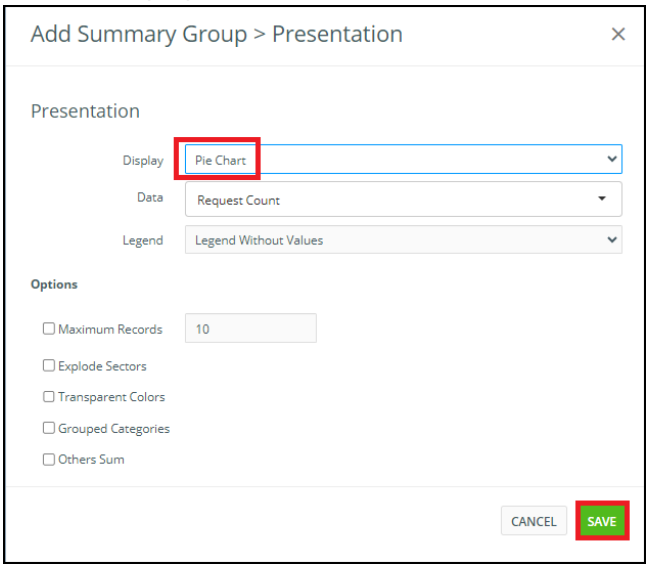
Browse to both allowed and denied sites.

In the WebAdmin:

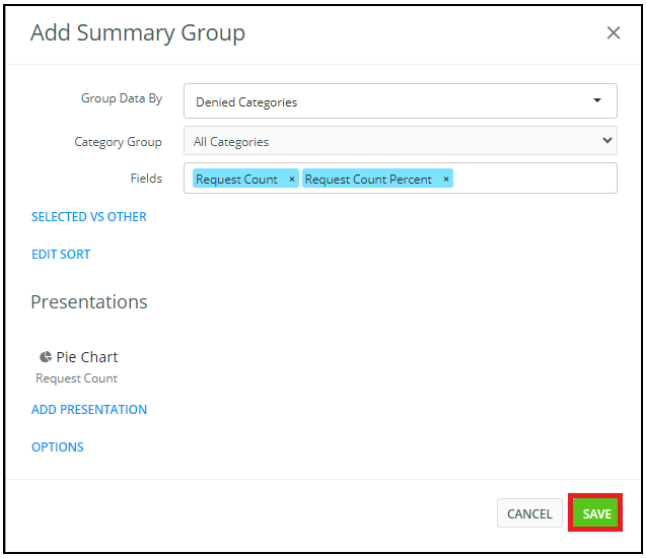
1. Navigate to Reports > Demand Reports.
2. In the 'Report Name' field, enter **Test Demand Report**.
3. Select the Calendar button for the 'end-date' in the 'Date Range' field.
4. Use the calendar to set the 'date' value to tomorrow's date and select **OK**.
5. Select the **Add Filter** button.
6. Set 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.



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

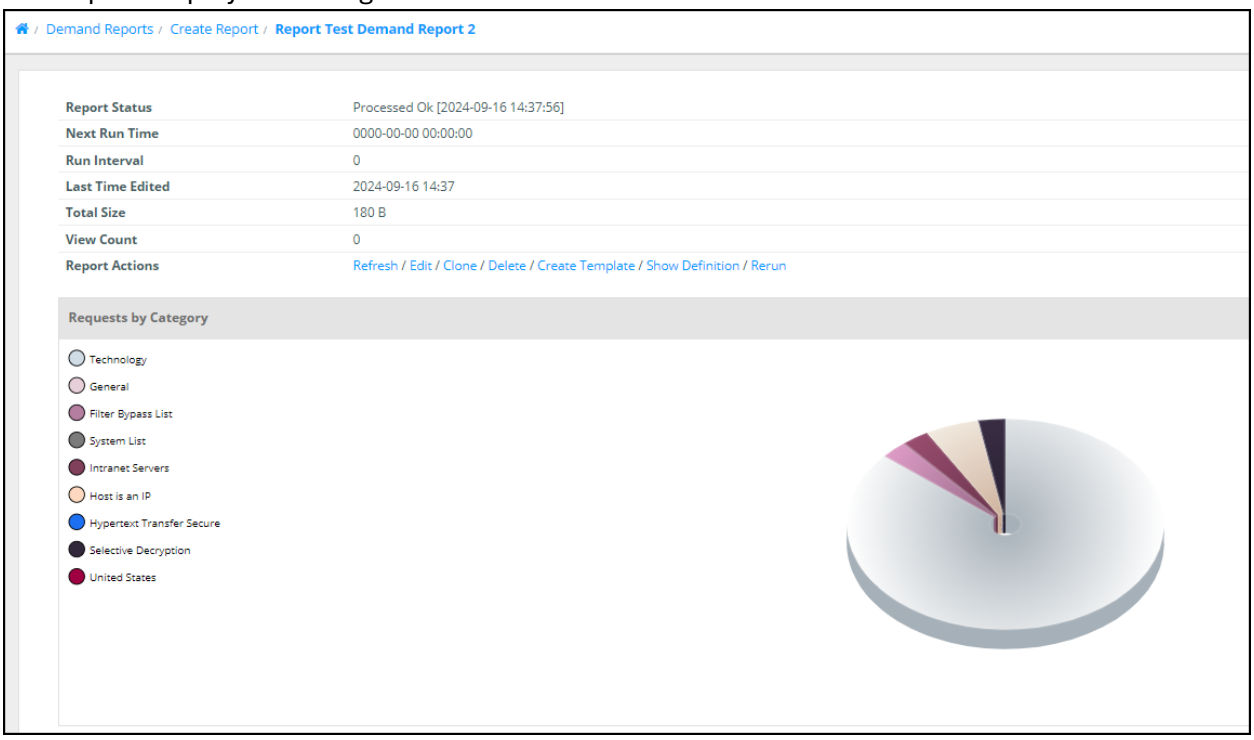


12. Select **Save** again to apply our Summary Group.



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	