Netsweeper Inc.
Corporate Headquarters
140 Columbia St. W.
Suite 302
Waterloo, ON, Canada N2L 3K8
CANADA
T: +1 (519) 772-0889
F: +1 (519) 772-0896
support@netsweeper.com

Netsweeper User Acceptance Document 8.1

Contents: User Acceptance Document 8.1

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/UAT/8_1_Resources/User_Acceptance_Resource_8_1_Page.html

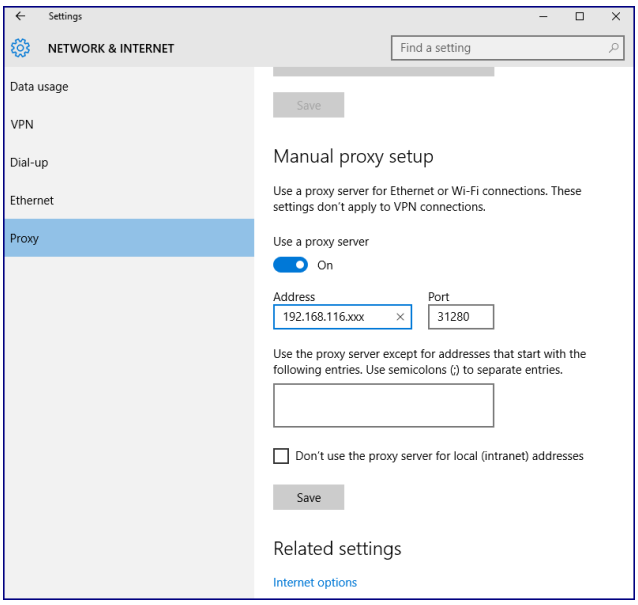
Filtering for the Test Workstation

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 Web Admin (UDP 3161).
- In the 8.1 default install, NSProxy is enabled.
- This document assumes that NSProxy is enabled.

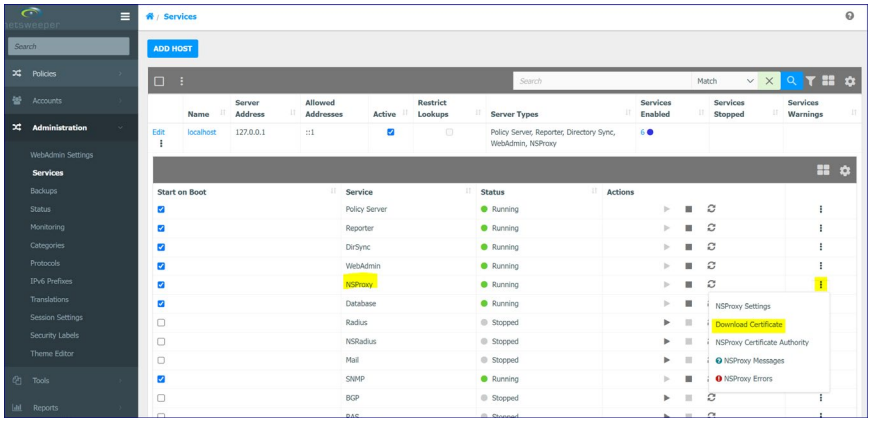
NSProxy Installation on Testworkstation

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

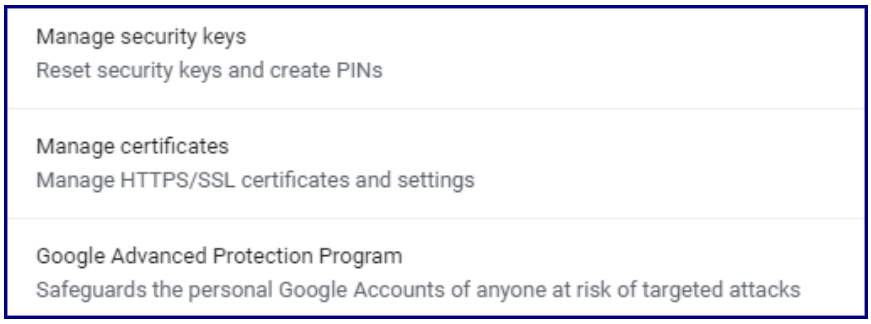


Importing a Certificate

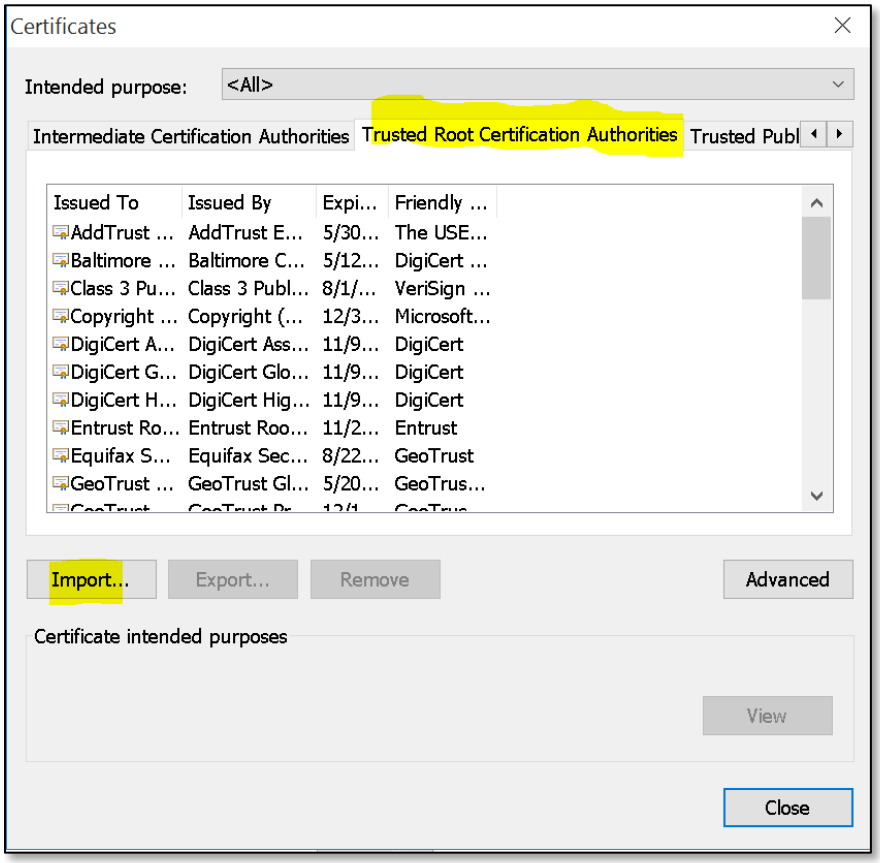
1. In the WebAdmin, go to Administration > Services and click on the **Services** tab.
2. Expand the localhost to display the Server Management page.
3. In the 'NSProxy' section, click the **Download Certificate** link. The certificated is downloaded to your download directory.



4. Copy the certificate to your workstation.
5. In your browser, go to Settings and click **Manage certificates**.



6. Click the **Trusted Root Certification Authorities** and click **Import**.



7. Follow the steps in the wizard to import the certificate.

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.

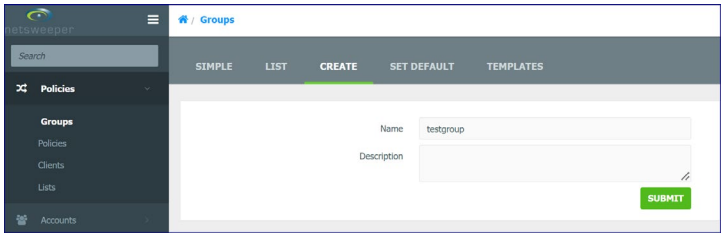
The Precondition section will:

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

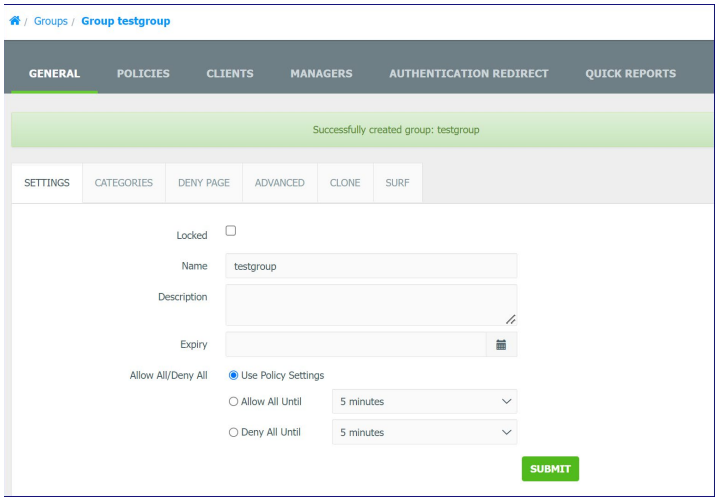
This document will assume that this section is completed as part of the precondition.

Creating a Group ‘testgroup’

1. In the WebAdmin, go to Policies > Groups.
2. In the 'Groups' window, click the **Create** tab.
3. In Name field enter **testgroup** and click **Submit**.

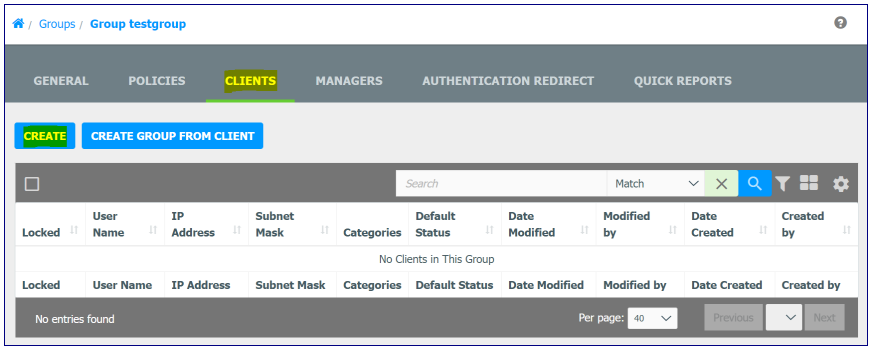


4. The Group is created.

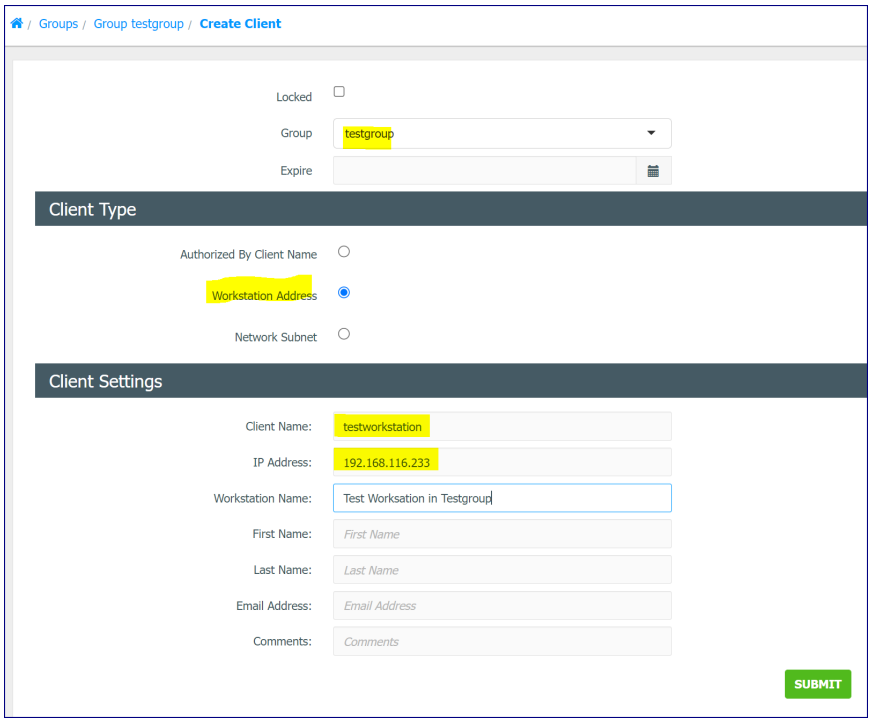


Create Testworkstation Client

1. Click the **Clients** tab and the **Create** button.



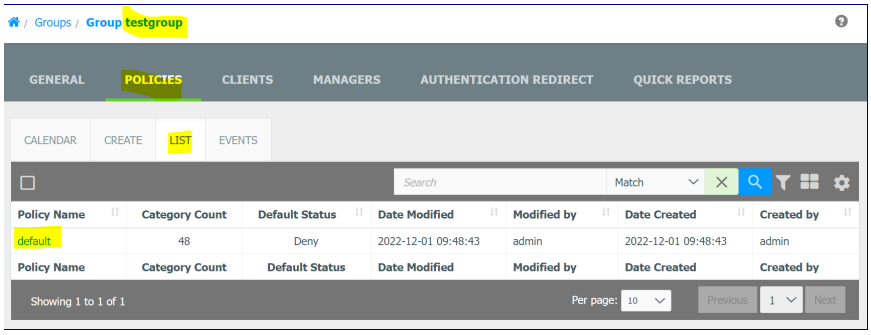
2. In the ‘Add Client to Group’ ensure that the ‘testgroup’ is selected and click the ‘Workstation Address’ radio button in the ‘client Type section.
3. Enter the ‘Client Name’ **testworkstation**, the IP of your test workstation and a Workstation Name. Your window should look like the image below.



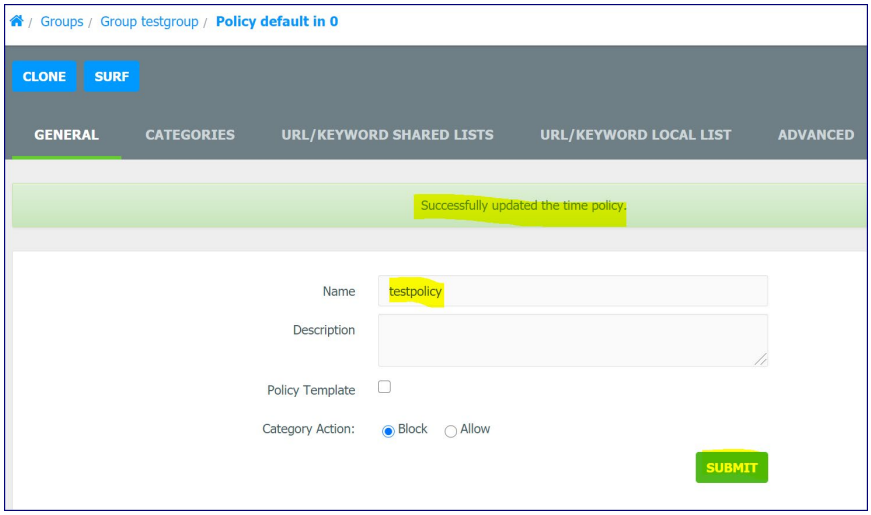
4. When done, click **Submit**. The new Client displays in the **Clients’** tab.

Create Policy ‘testpolicy’

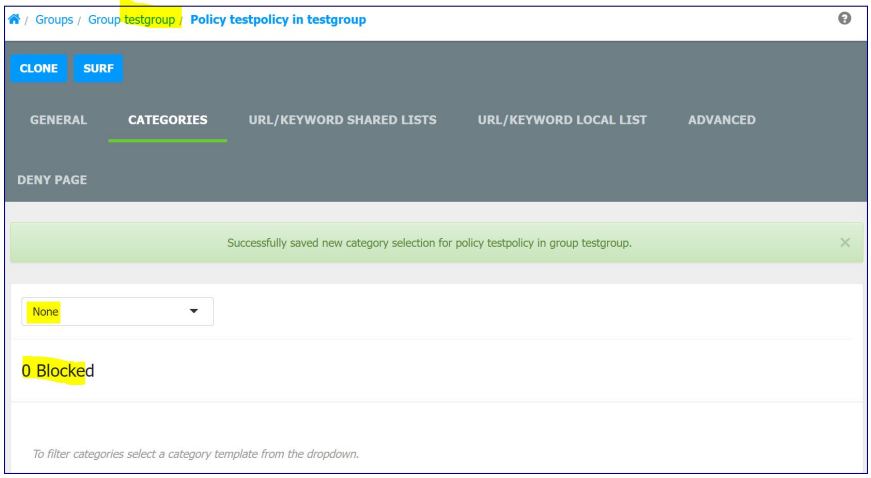
1. In the testgroup, click the **Policies** tab and then the **List** tab.
2. Click the **default** Policy Name.



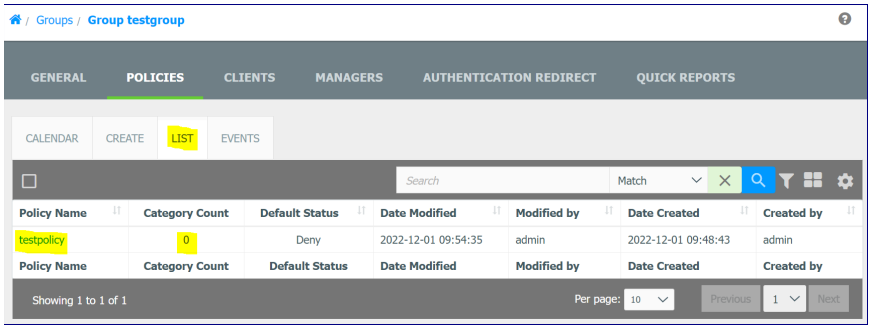
3. Rename the Policy to **testpolicy** and click **Submit.**



4. Click the **Categories** tab and select the **None** Category Template**.**
5. Click **Submit.**

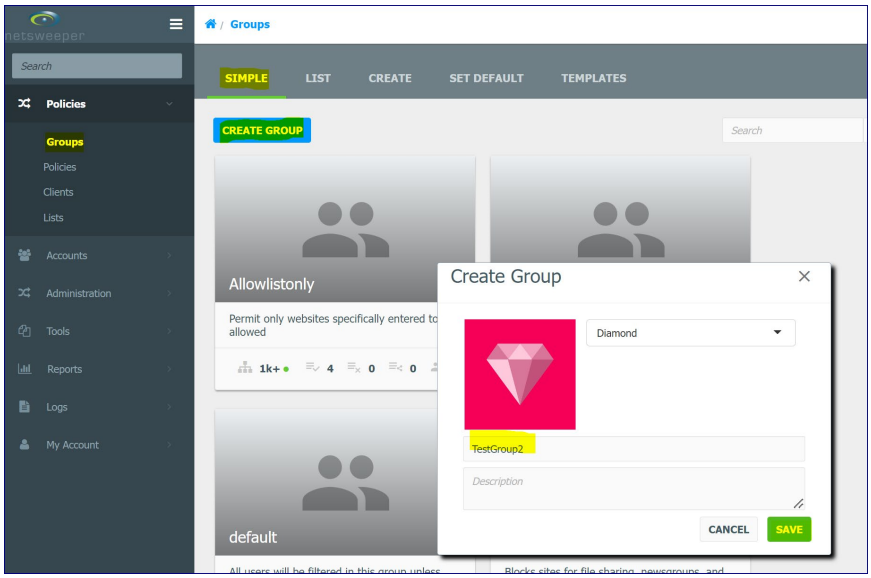


6. Click the breadcrumb to return to the testgroup main page. You should see a Category Count of 0.



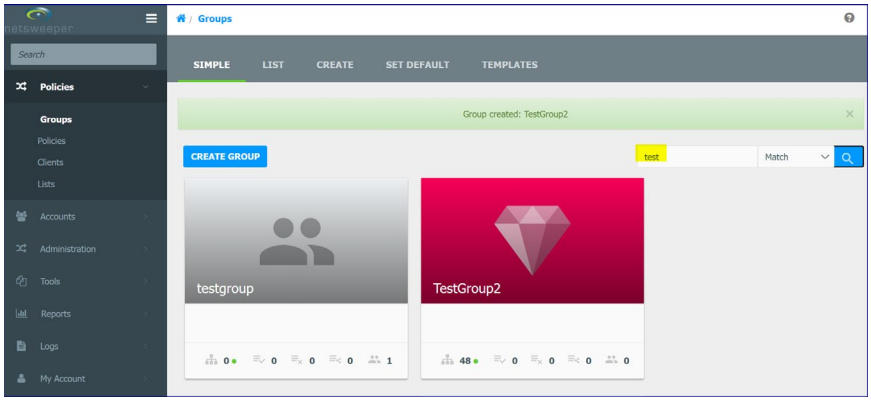
Creating a Simple Group 'TestGroup2'

1. Go to Policies > Groups and click the **Simple** tab.
2. Click the **Create Group** button.
3. In the 'Create Group' window, select **Diamond** for the icon.
4. Name the group **TestGroup2** and click the **Save** button.



5. In the **Simple** tab, enter **test** in the Search field and click Search.

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

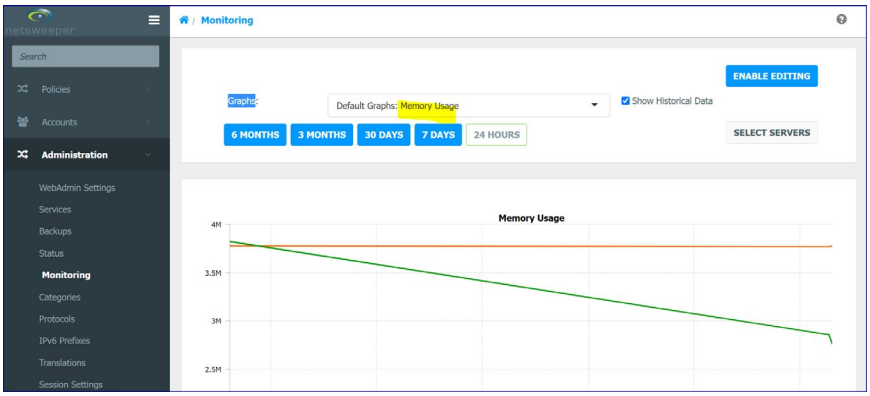
The Netsweeper solution must have been running and intercepting traffic for a period of at least 1 hour with testing taking place to generate allowed and denied request.

Test Procedure: Monitoring

1. In the WebAdmin, select 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.

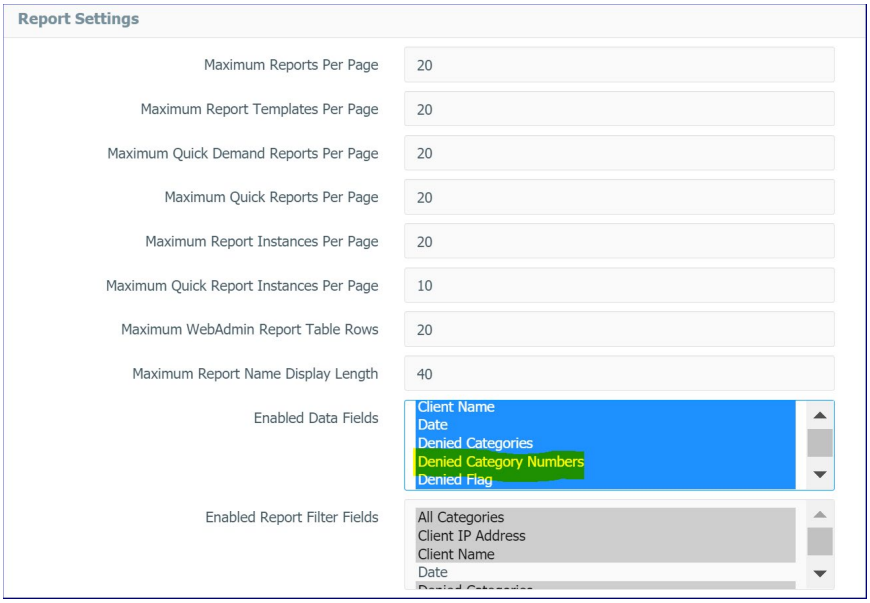
SMMP MIBs in 8.1

Notes	
Result (Pass or Fail)	
Result Comments	

Enabling Report Fields in WebAdmin Settings

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

1. Go to Administration > **WebAdmin Settings**.
2. Scroll down to **Report Settings.**
3. **Hold the <CRTL> key so as not to de-select all the other selected fields.**
4. Choose **Denied Category Numbers** from the 'Enabled Data Fields'.
5. Click **Submit** to save the 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.

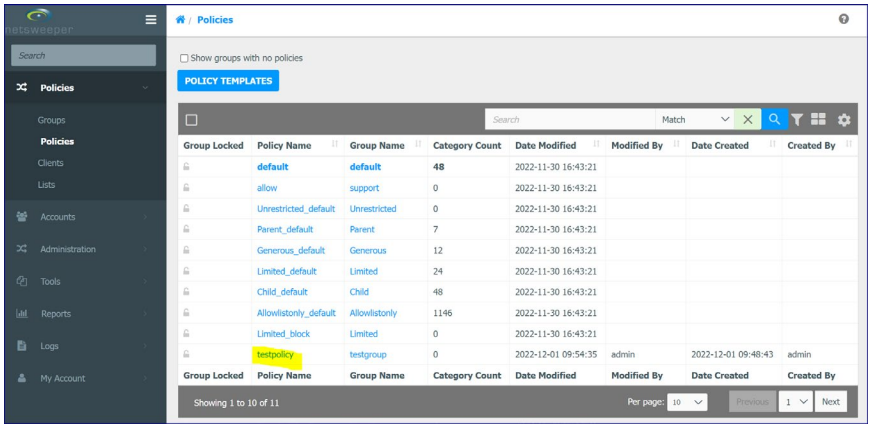
Precondition

See: Setting up Filtering Group and Client

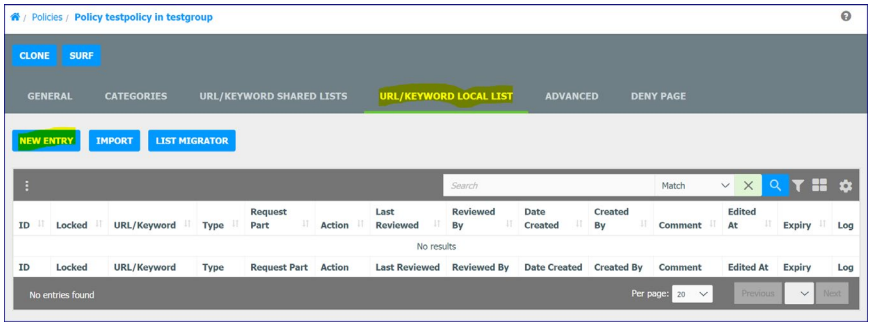
Test Procedure: Local Lists

In the WebAdmin:

1. Go to Policies > Policies and click the **testpolicy** Policy Name.

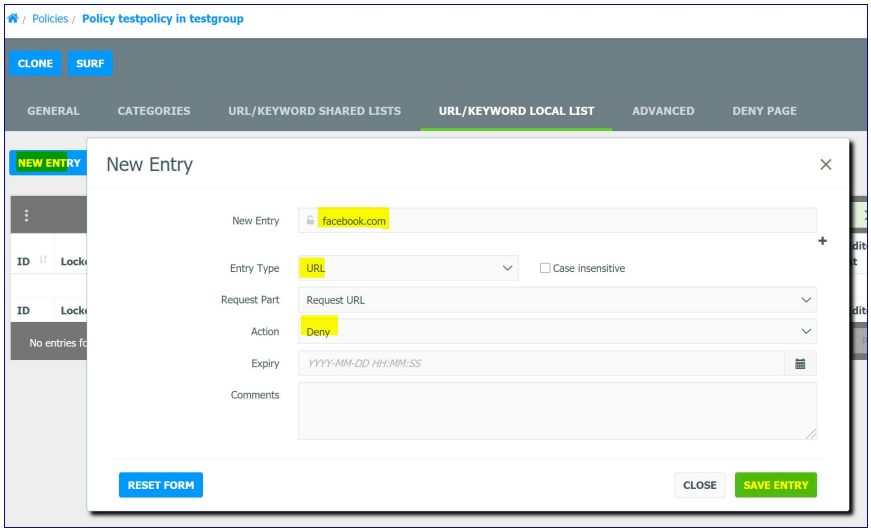


2. Click the **URL/Keyword Local List** tab.
3. Click the **Create Local List** button.
4. Click the **New Entry** button.



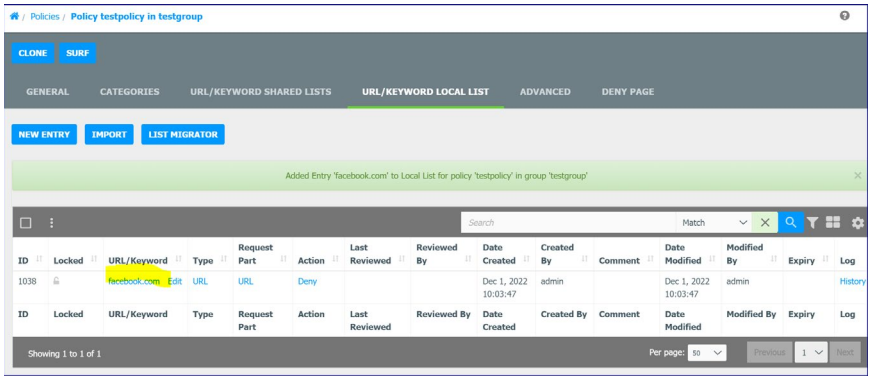
5. Add facebook.com in the ‘New Entry’ field (or another***example.com w***here *example.com* represents the URL of your choice.)
6. Ensure **URL** ‘Entry Type’ is selected in the dropdown list.
7. Ensure **Request URL** is selected from the ‘Request Part’ section.

8. Select **Deny** in the ‘Action’ section.



9. Click the **Save Entry** button.

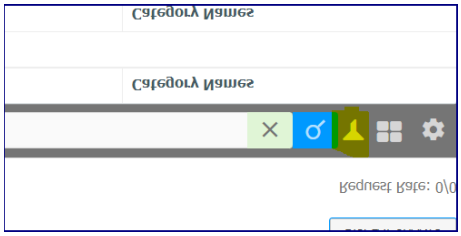
10. The entry is added to the Local List.



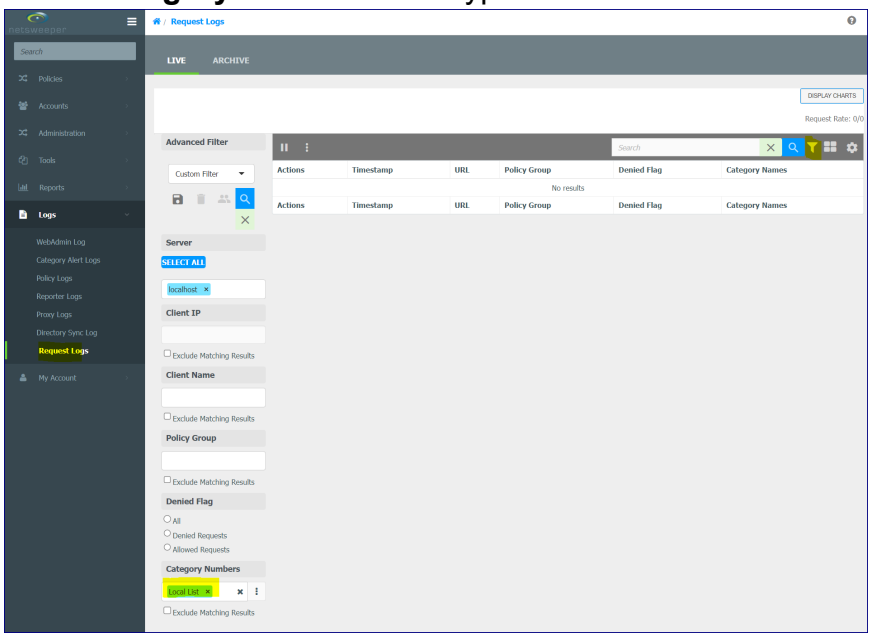
Request Logs Advanced Filters

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

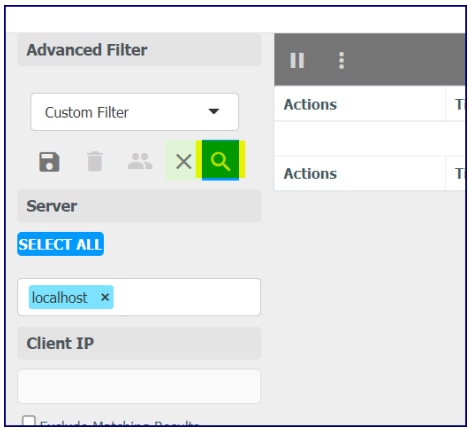
1. Go to Logs > Request Logs and click the **Advanced Filter** icon in the Table Header.



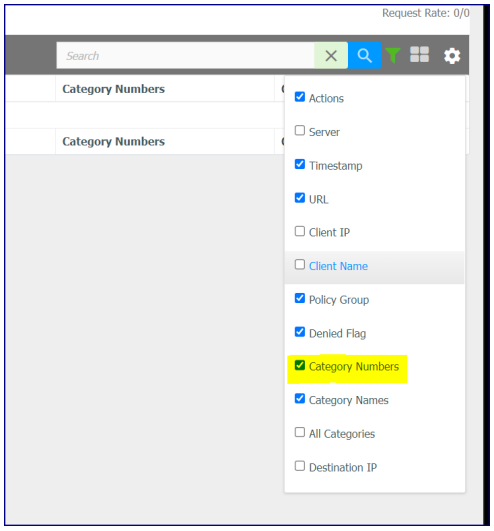
2. In the **Category Numbers** field type and then choose **Local List**.



3. Click the **Search** icon.

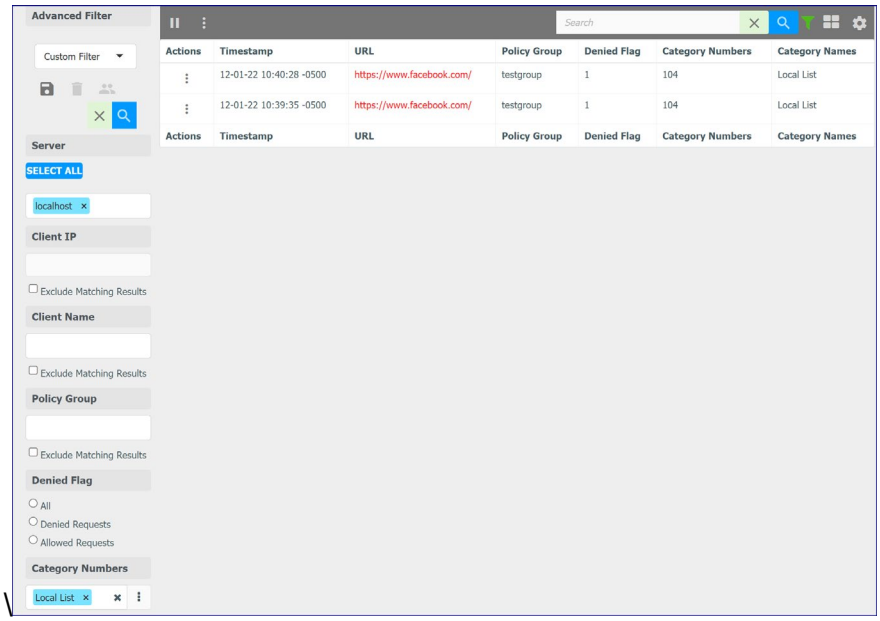


4. Click the Settings icon and place a checkmark beside **Category Names.** Please note that the green Filter icon indicates that the window is filtered.



On the test Workstation filtered by testgroup:

1. Clear the cache in your browser.
2. Browse to the link:
   https://*facebook.com*
   https://www.*facebook.com*
3. This is the site we enter in our Local List in the previous step.
4. Request Logs should show that all the sites are unreachable. The 'Category Numbers' field should display '104' and the 'Category Names' field should display 'Local List'.



5. And a deny page displays in the testworkstation browser.

Pass Criteria

Using the filtered workstation in the **testgroup** group, browse to facebook.com or *example.com (if using)*. The Webpage **will** be unreachable.

Notes	
Result (Pass or Fail)	
Result 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.

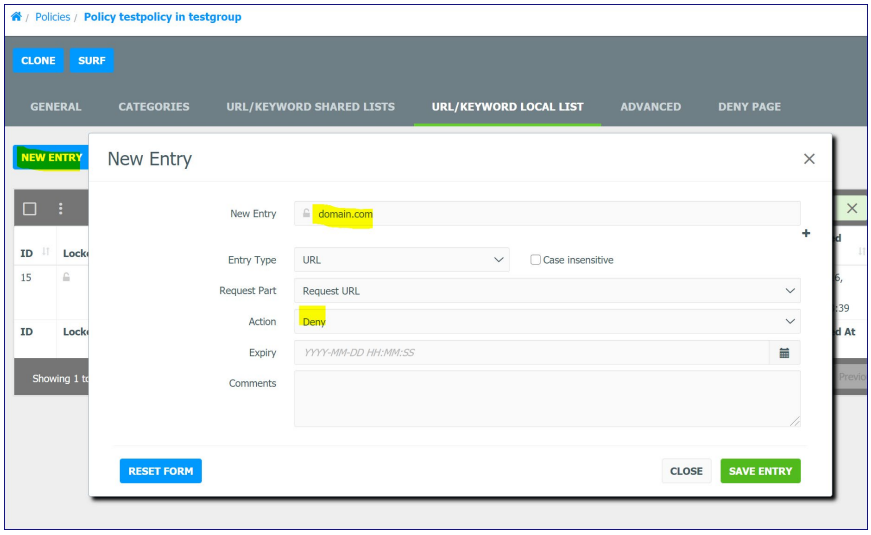
Precondition

See: Setting up Filtering Group and Client

Test Procedure: Domain Filter

In the WebAdmin:

1. Go to Policies > Policies and click on **testpolicy**.
2. Click the **URL/Keyword Local List** tab.
3. Click the **New Entry** button.
4. Add ***domain.com*** in the 'New Entry' field. (Where *domain.com* represent the URL of your choice).
5. Ensure **URL** 'Entry Type' is selected in the dropdown list.
6. Ensure **Request URL** is selected from the 'Request Part' section.
7. Select the **Deny** tab in the 'Action' section.



8. Click the **Save Entry** button.

On your Test Workstation:

1. Clear the cache in your browser.

2. 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*
3. 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	
Result (Pass or Fail)	
Result 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.

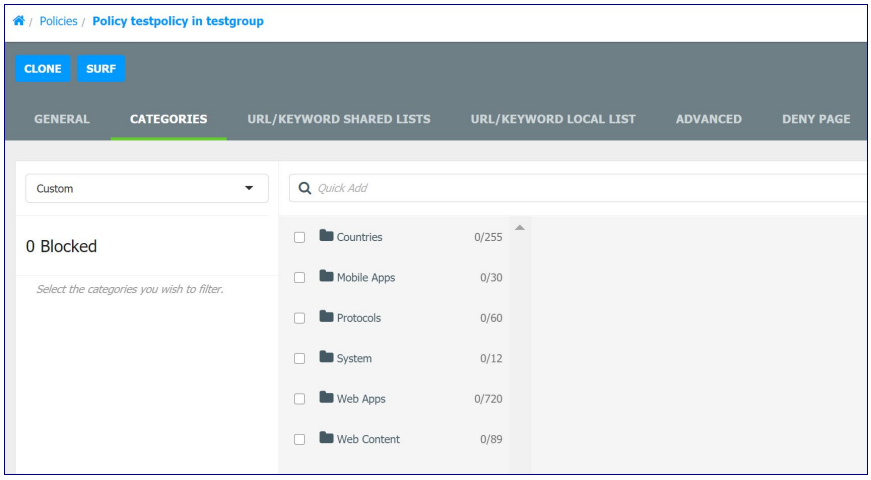
Precondition

See: Setting up Filtering Group and Client

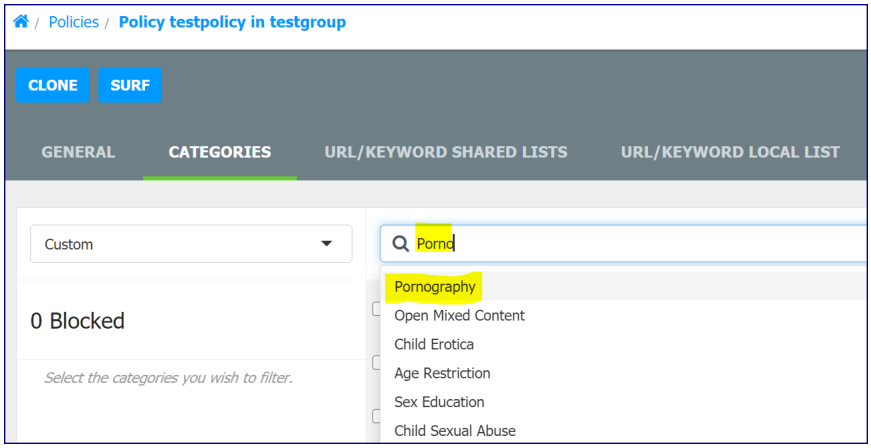
Test Procedure: Deny Specific Category

In the WebAdmin:

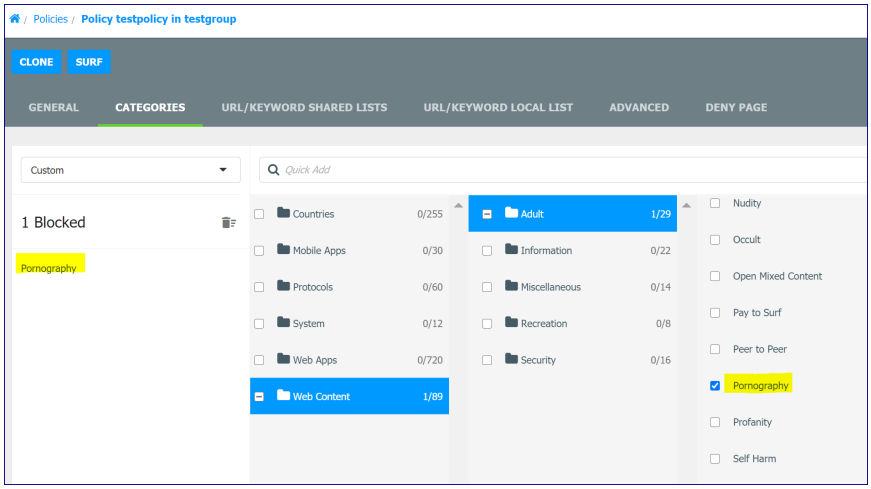
1. Go to Policies > Policies and click on **testpolicy**.
2. Click the **Categories** tab.
3. Select the **Custom** Category Template.



4. Type **Pornography** in the 'Quick Add' field and click to add it.

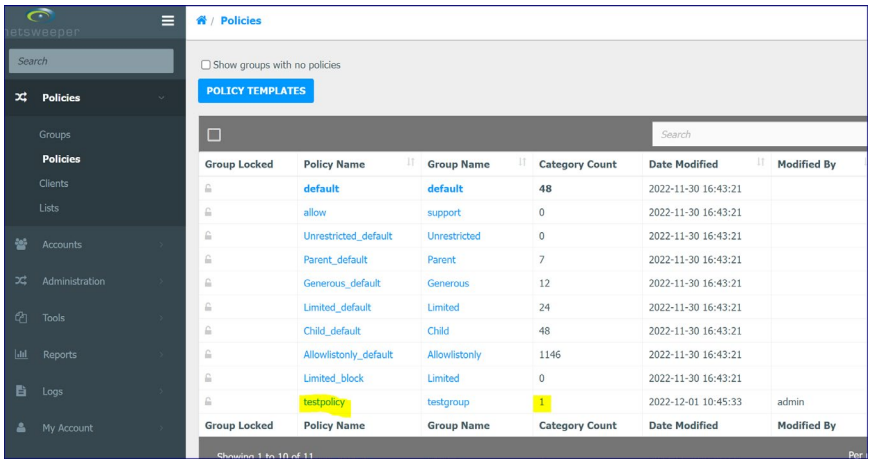


5. Click **Submit** to add the ‘Pornography’ Category.



6. Go to Policies > Policies

7. You can see that the ‘Category Count’ for the **testpolicy** is **1**.



On your Test Workstation:

1. Clear the cache in your browser.
2. Browse to a pornography links such as sex.com.
3. The intended Webpage is unreachable.

Pass Criteria

Using the filtered workstation in the **testgroup** group, browsing to URL that belongs to the selected Pornography Category **will not** be reachable.

Notes	
Result (Pass or Fail)	

Result 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.

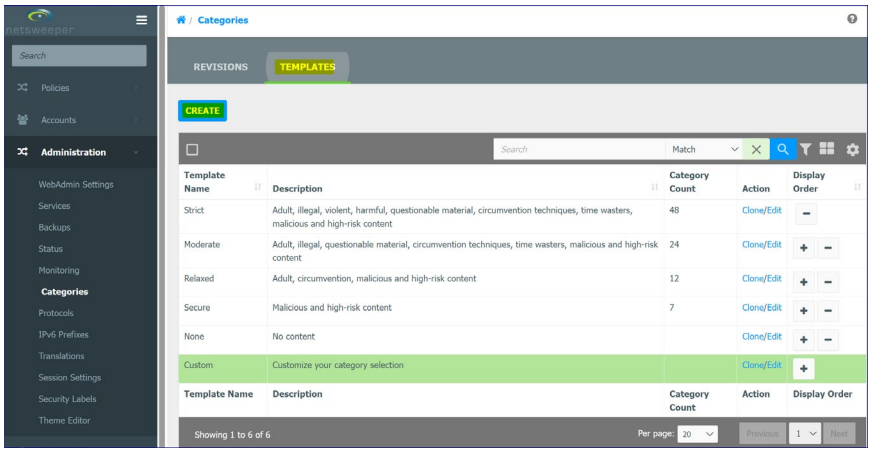
Precondition

See: Setting up Filtering Group and Client

Test Procedure: Deny Specific Category

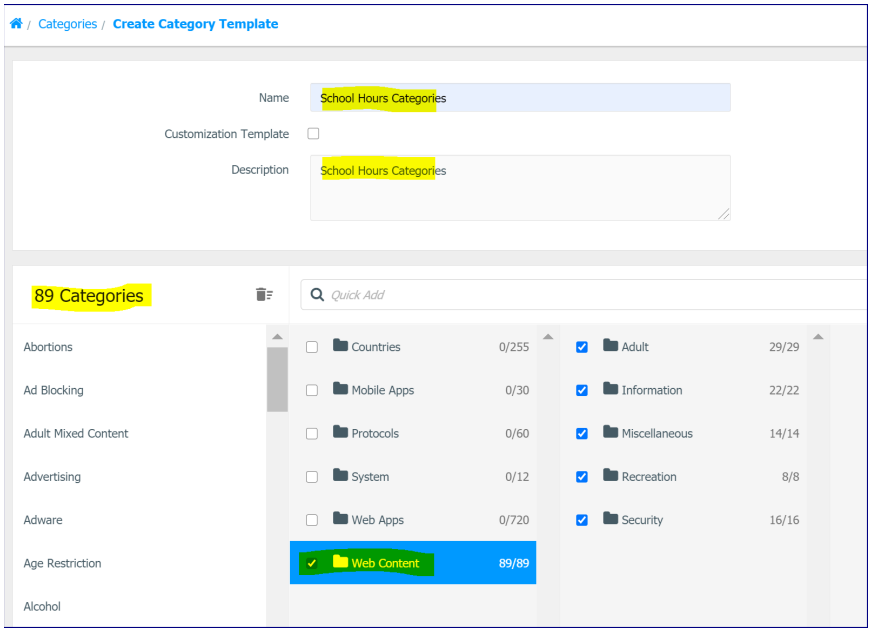
In the WebAdmin:

1. Go to Administration > Categories and click on the **Templates** tab.
2. Click the **Create** button.

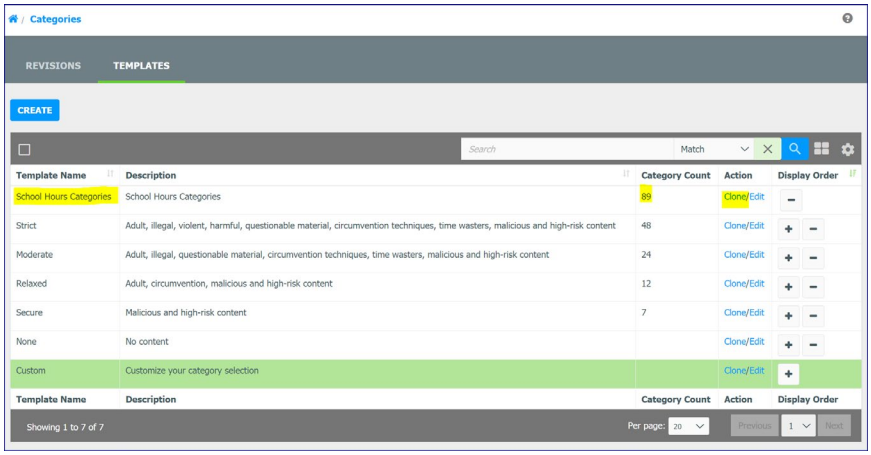


3. Name the Template **School Hours Categories** and **a mandatory Description**.

4. In the **Hierarchy View** tab, add a checkmark to the **Web Content** folder and click to select all Categories.

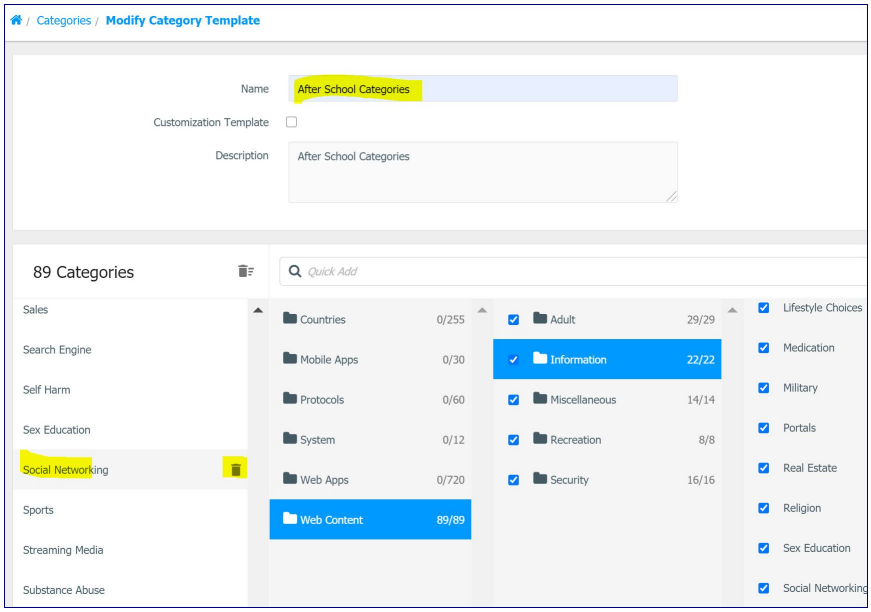


5. Click **Submit**. The 'Successfully added a new category template' message displays.
6. Use the Breadcrumbs to return to the **Templates** tab. You will see the 'School Hours Categories' Template.

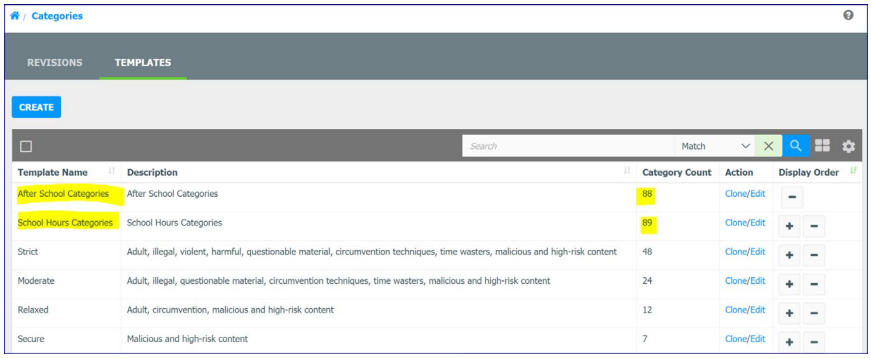


7. Click the **Clone** link beside **School Hours Categories** Template.
8. Click the **Edit** link for the cloned Category Template
9. Change the name of this Template to **After School Categories** and Description field and click **Submit**.
10. In the left column, scroll down to **Social Networking** and click to delete the Category. This Category, which includes Facebook and YouTube, will now be

allowed for this Category Template.



11. Click **Submit** again to add the updated Categories.
12. Return to the **Templates** tab and you should see the Category Templates we just created. These will be used in the next procedure.



Time Based Policy: 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

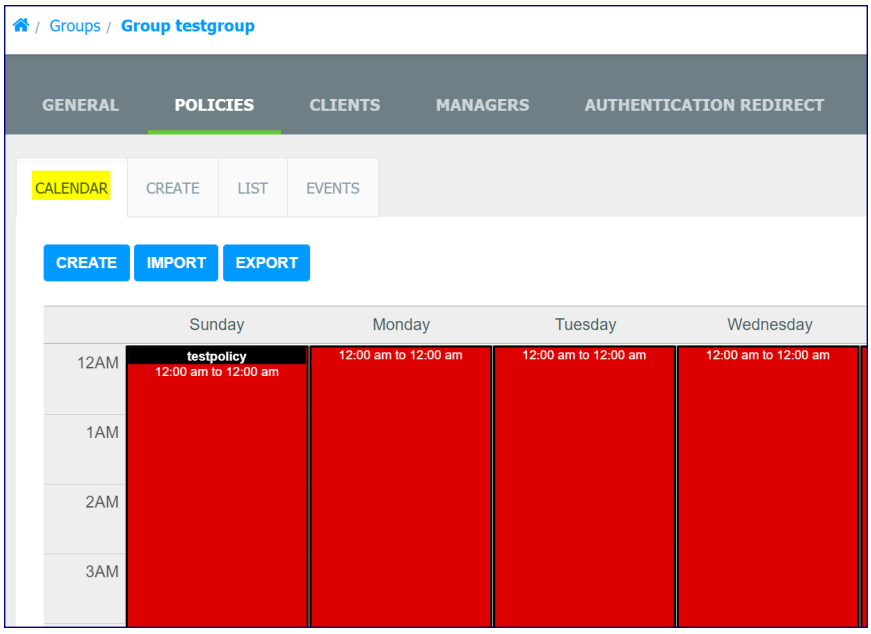
See: Setting up Filtering Group and Client

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

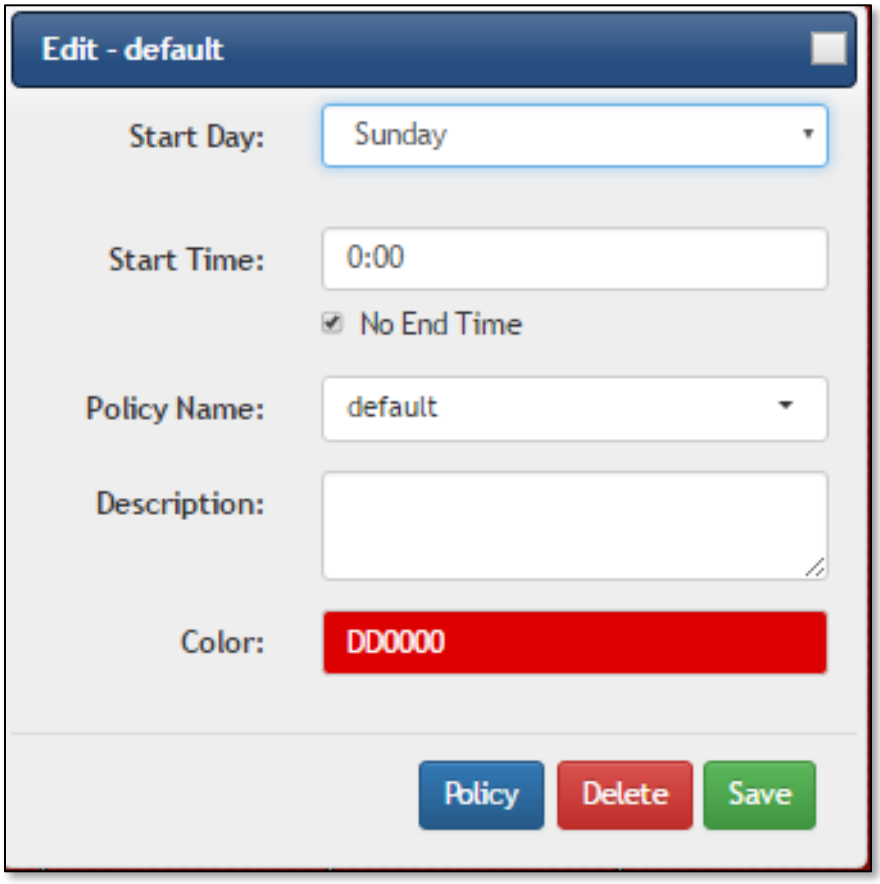
Test Procedure: Policy Events

In the WebAdmin:

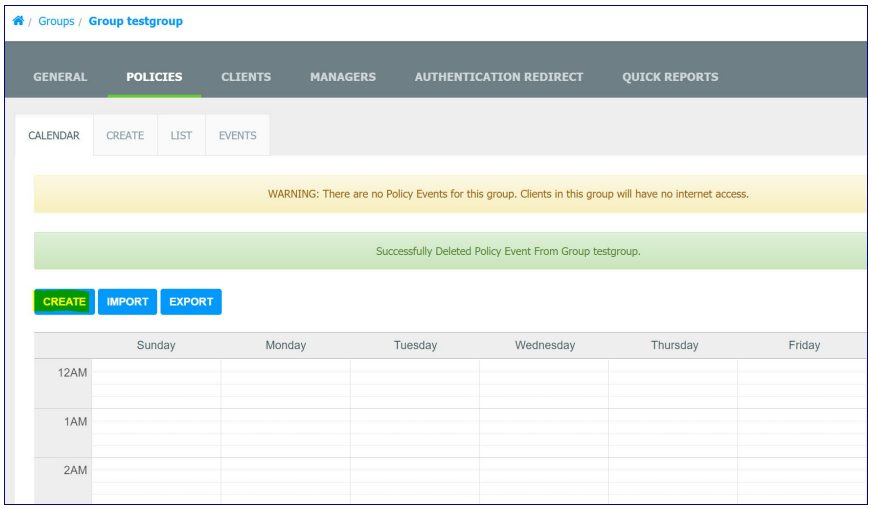
1. Go to Policies > Groups and click the **List** tab.
2. Click on **testgroup**.
3. Click the **Policies** tab.
4. We are going to delete the default Calendar Event so in the Policy Calendar tab, click the default Policy Event (in red)



5. Click the **Delete** button.

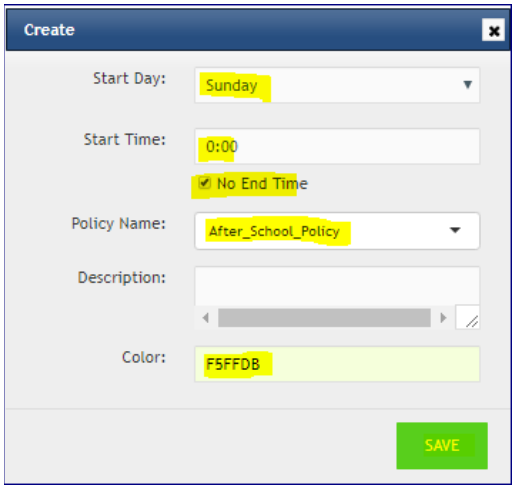


6. Click the **Create** button.

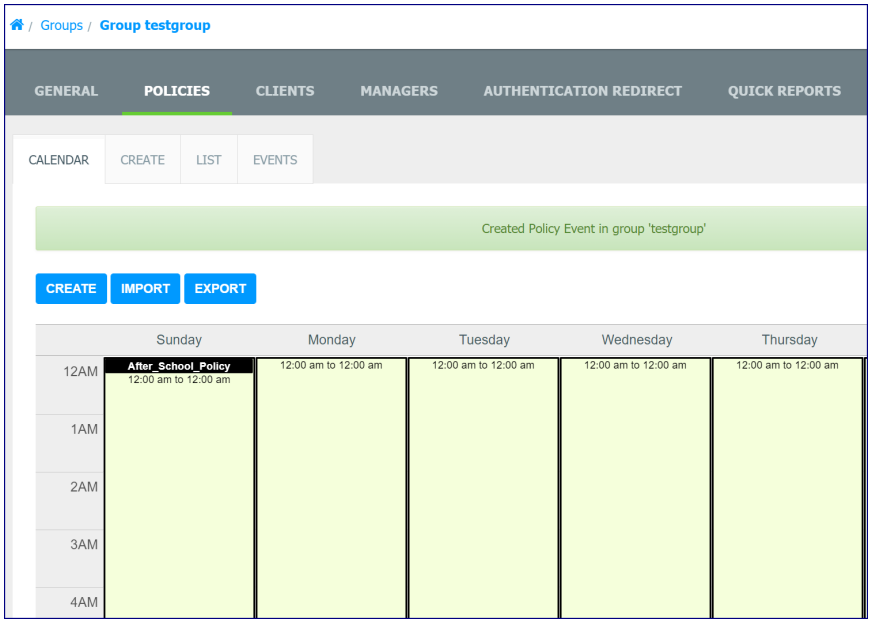


7. In the Create window, click the No End Time checkbox.
8. Enter **After_School_Policy** (with no spaces) in the 'Policy Name field and a description.

9. Enter the Color **F5FFDB** and click **Save**.

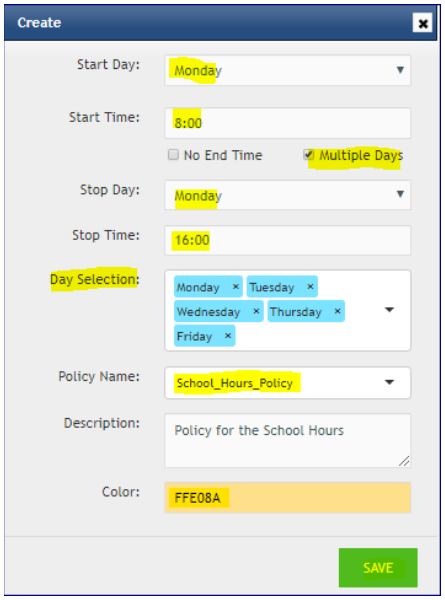


10. The default ‘After School Policy’ is created.

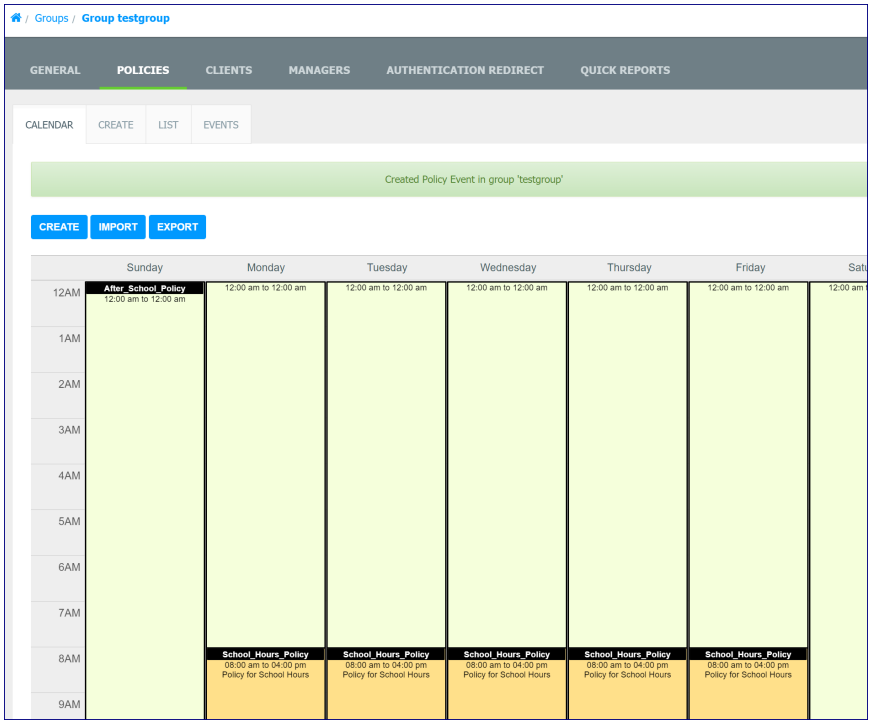


11. Click the **Create** button again.
12. Select ‘Start Day’ and ‘Stop Day’ as Monday.
13. Select ‘Multiple Days’
14. Select ‘Start Time’ as 8:00 and ‘Stop Time’ as 16:00.
15. In the ‘Day Selection’ field select Monday to Friday inclusive.
16. Enter the ‘Policy Name’ **School_Hours_Policy** with no spaces and a description.
17. Enter the Color **FFE08A**.

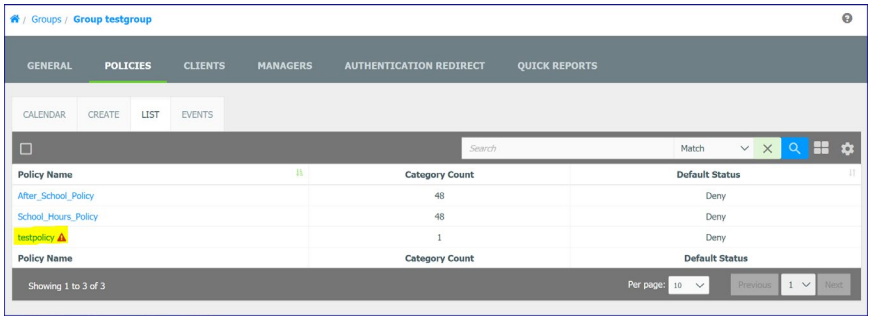
18. Click **Save**.



19. The ‘School Hours Policy’ display in the designated time.



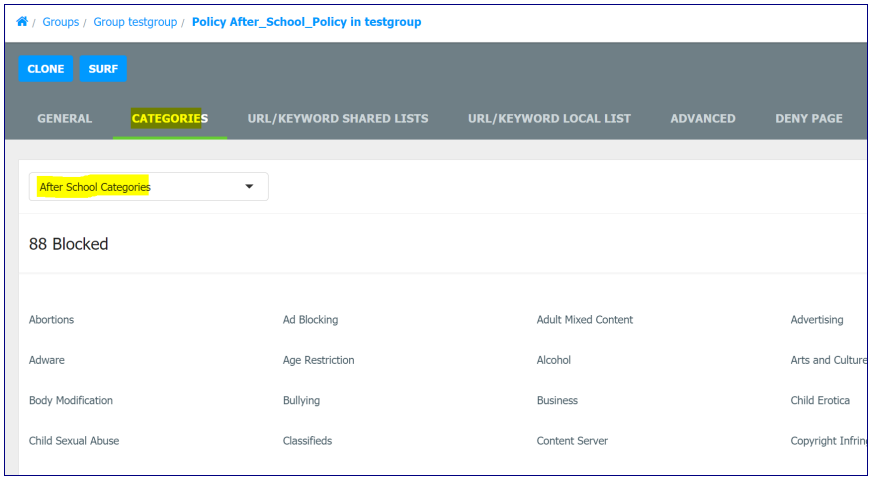
20. Click the **List** tab and confirm that the ‘After School Policy’ and the ‘School Hours Policy’ are listed.



21. Select the **testpolicy (Errors)** Policy and click the **Delete** icon in the Table Header bar.

22. Click the **After_School_Policy** and then on the **Categories** tab for that Policy.

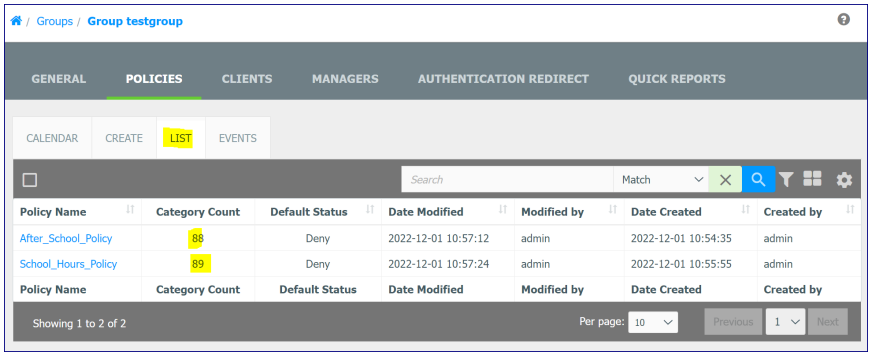
23. Select the **After School Categories** Template created in the previous procedure and click **Submit.**



24. Use the breadcrumbs to return to the Policy List.

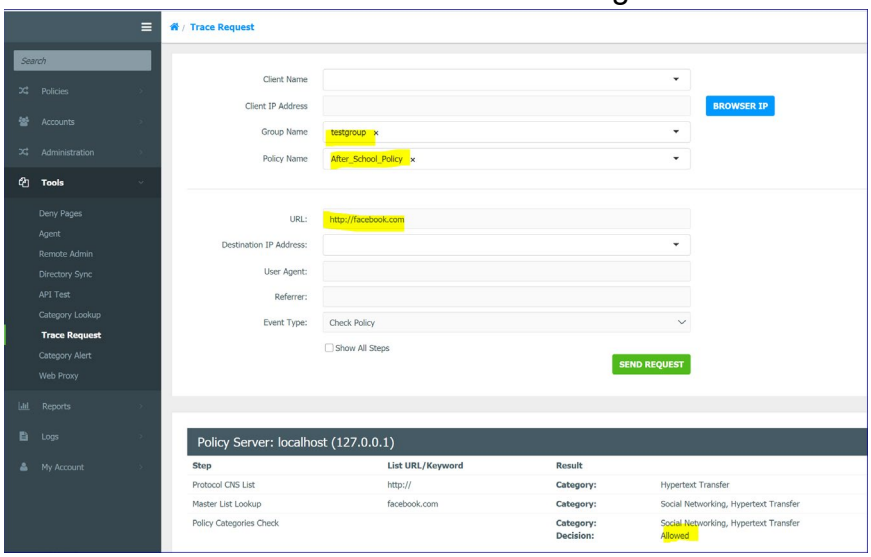
25. Select the **School Hours Policy** and repeat the steps to assign the School Hours Categories.

26. When done, verify that you Policies > List tab looks like this.

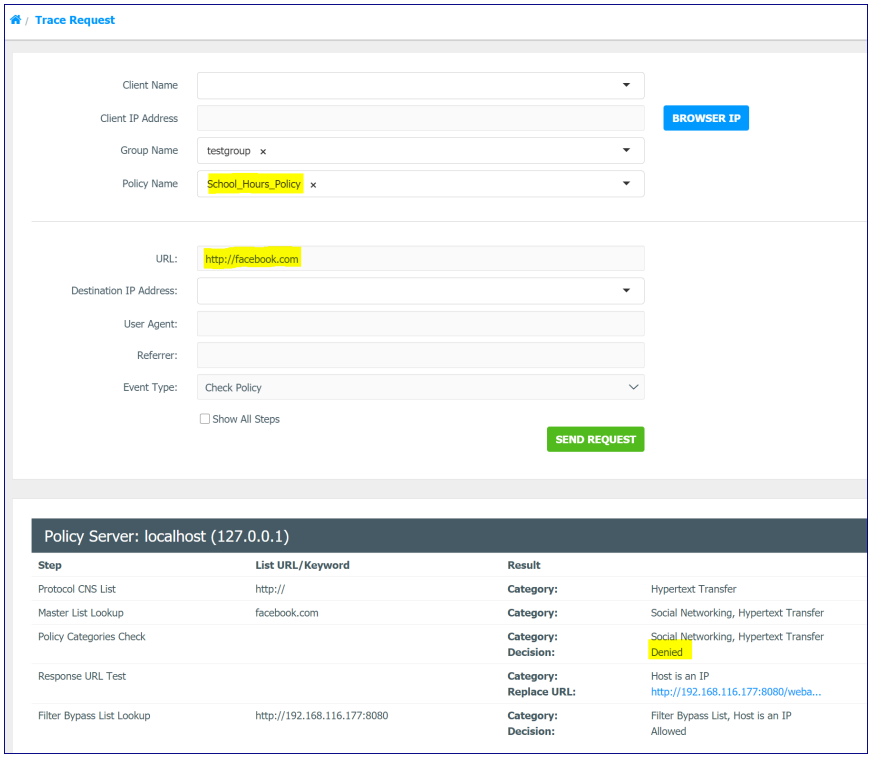


Pass Criteria

1. Go to Tools > Trace Request window.
2. Select the ‘Group Name’ **testgroup** and the ‘Policy Name’ **After_School_Policy,**
3. Enter facebook.com or another ‘Social Networking’ site and click the **Send Request** button.
4. The site is allowed under ‘Social Networking’.



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



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

Lists Window

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

System Deny List

Purpose

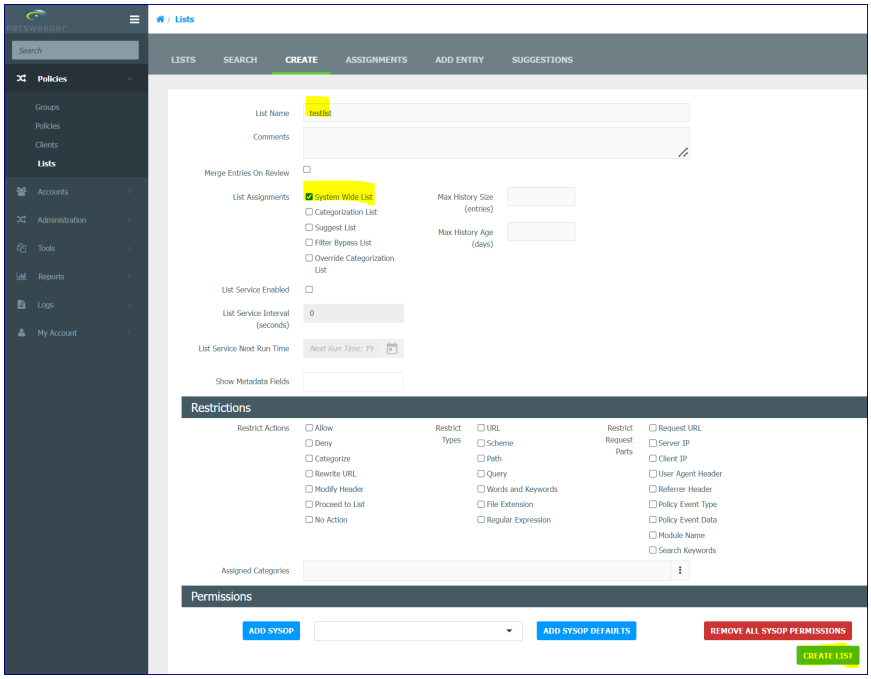
When websites need to be blocked globally, regardless of group policy, then the **System Deny List** is used. URLs placed on this list will be denied for all clients, regardless of group membership and specific policy/list settings.

Precondition

See: Setting up Filtering Group and Client

Additional Precondition: Adding a Test List

1. Go to Policies > Lists and click the **Create** tab.
2. Type **testlist** in the List Name
3. Click the **System Wide List** in the 'List Assignments' section.



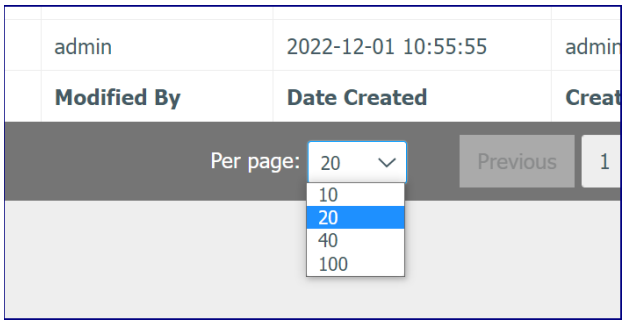
4. Click the **Create List** button.
5. The **testlist** appears in the ‘Lists’ window.

Test Procedure: System Deny List

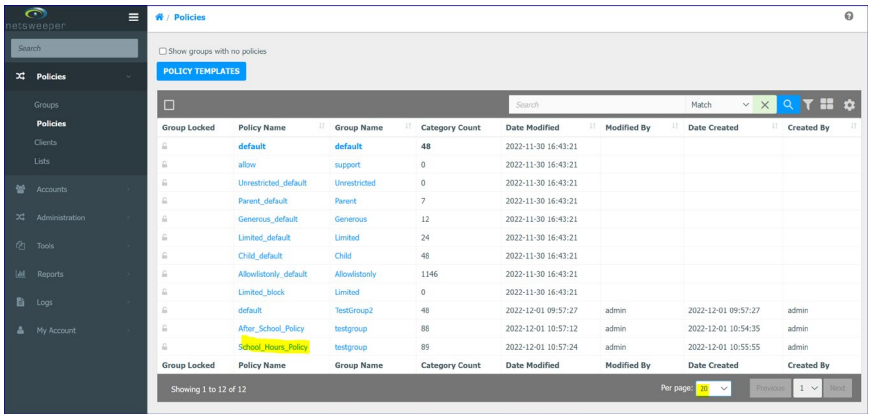
In the WebAdmin:

Modify Local List: The group that the user is assigned to must have a Local List that explicitly allows the URL you want to test with.

1. Go to Policies > Policies to open the Policies window.
2. At the bottom of the page, choose 20 from the Per page setting.

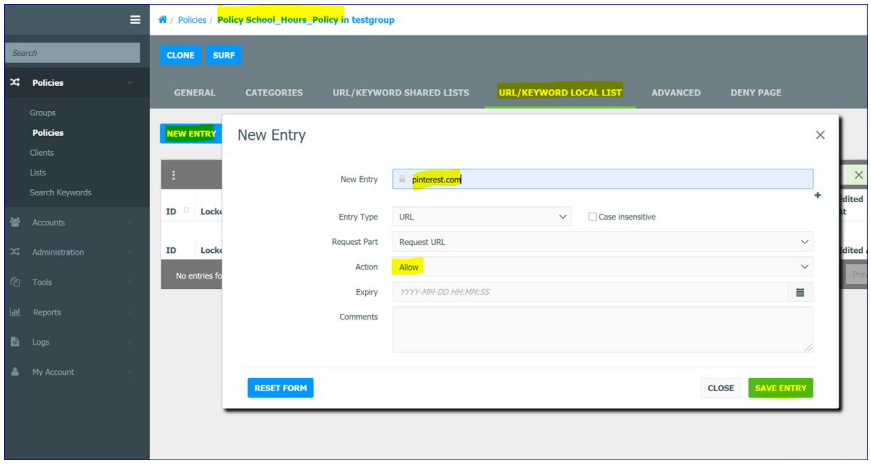


3. Click the **School_Hours_Policy** link for the Policy.

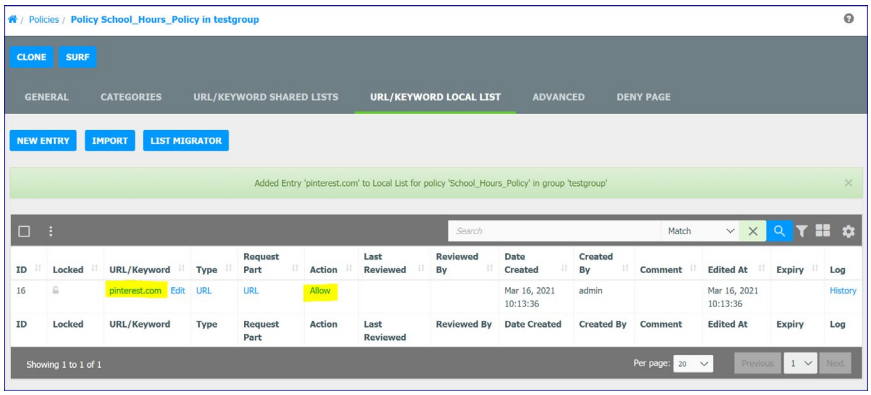


4. Click the **URL/Keyword Local List** tab.
5. Click the **Create Local List** button if displayed.
6. Click the **New Entry** button.
7. Add ***pinterest.com*** as the 'New Entry'.
8. Select the **URL** 'Entry Type' from the dropdown list.
9. Ensure **Request URL** is selected from the 'Request Part' section.

10. Select **Allow** in the ‘Action’ section.

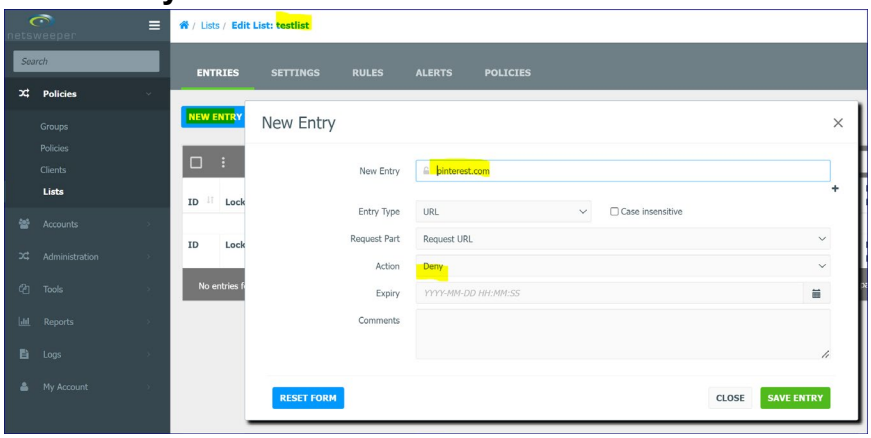


11. Click **Save Entry**. The URL is added to the Local List.

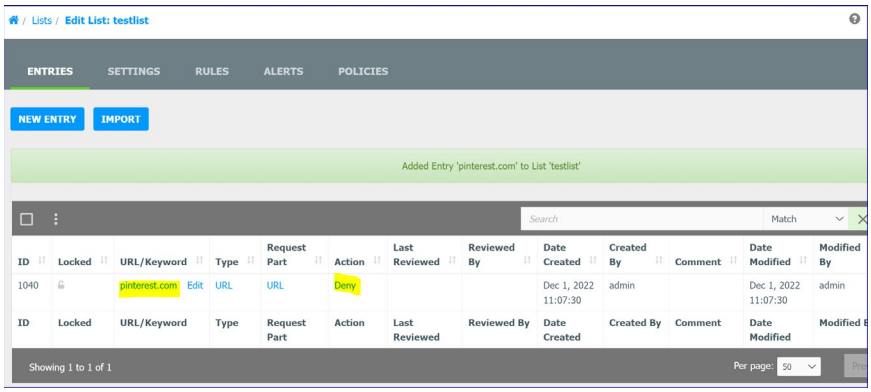


Modify System-Wide URL List:

1. Go to Policies > Lists
2. Click the **testlist** and click the **New Entry** button.
3. Add ***pinterest.com*.** (The same URL entry that was used in Step 5 for the **testgroup** Local List)
4. Select **Deny** in the 'Action' section.



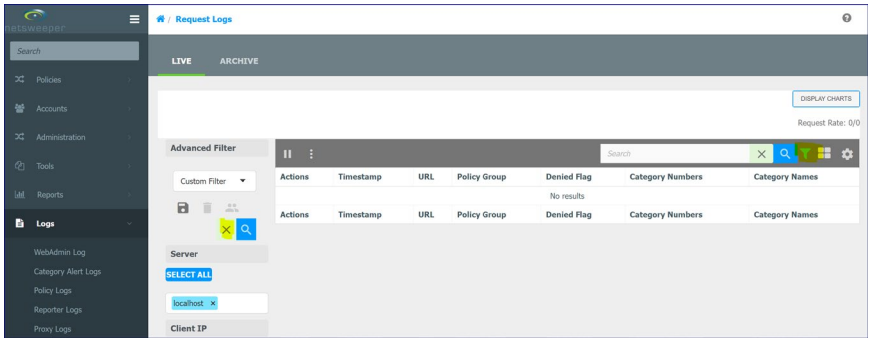
5. Click the **Save Entry** button.
6. The Deny entry is added.



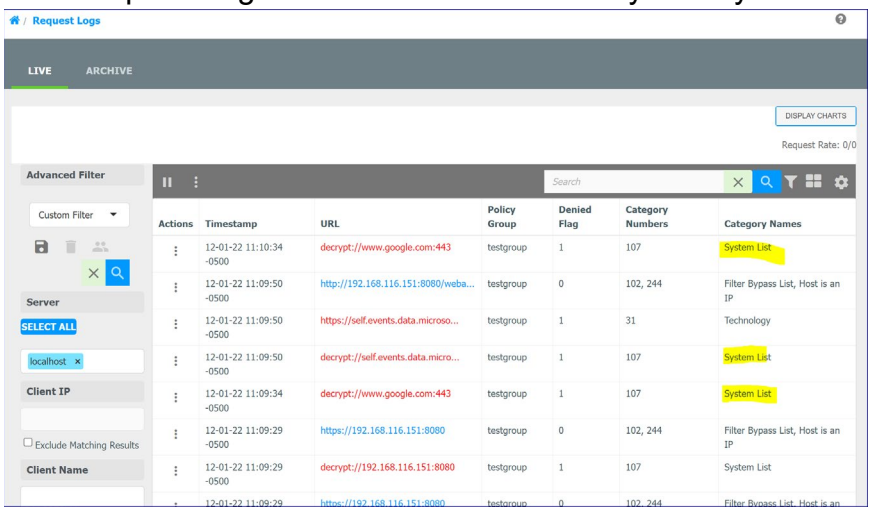
On your Test Workstation:

1. Open the 'Request Logs' window under the Logs menu.

2. Clear the Advanced Filtering from the earlier procedure by opening the filtering pane and click the X. The Advanced Filter icon should no longer be green.



3. Clear the cache in your browser on the testworkstation.
4. Browse to *pinterest.com*.
5. The intended webpage will be unreachable.
6. The 'Request Logs' shows that it is denied by the '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 policy due to List Processing order. The **System Wide List** will always take precedence over **Local Lists**.

Notes	
Result (Pass or Fail)	

Result Comments	

Importing a System List

Purpose

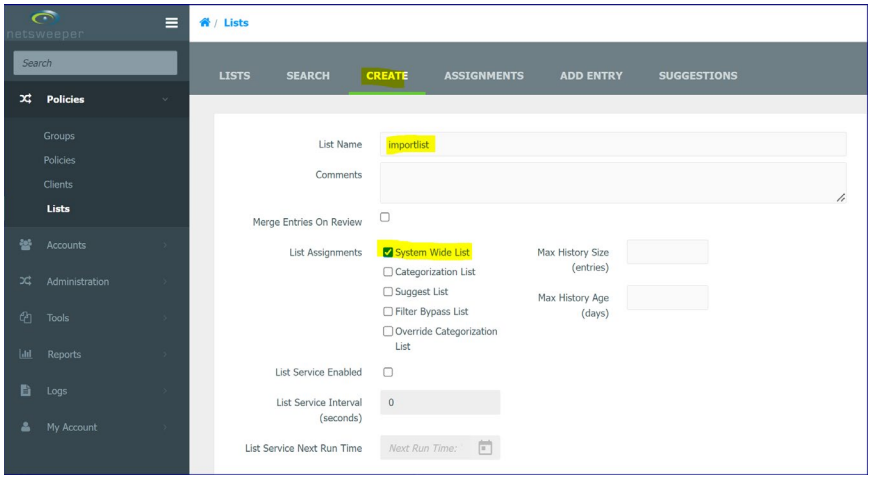
The Netsweeper solution provides functionality for importing long System Lists (allow and deny.) Typically, these lists come from an external list (CSV file, spread sheet, etc.). This test case verifies the system list import feature.

Precondition

See: Setting up Filtering Group and Client

Additional Precondition 1: Adding a Test List

1. Go to Policies > Lists and click the **Create** tab.
2. Type **importlist** in the List Name
3. In the List Assignments section select **System Wide List**.
4. Click the **Create List** button.



5. Additional Precondition 2: Creating a URL Import List

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

https://helpdesk.netsweeper.com/docs/UAT/8_1_Resources/User_Acceptance_Resource_8_1_Page.html

1. You can also create a .csv document.
2. Add the content as 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

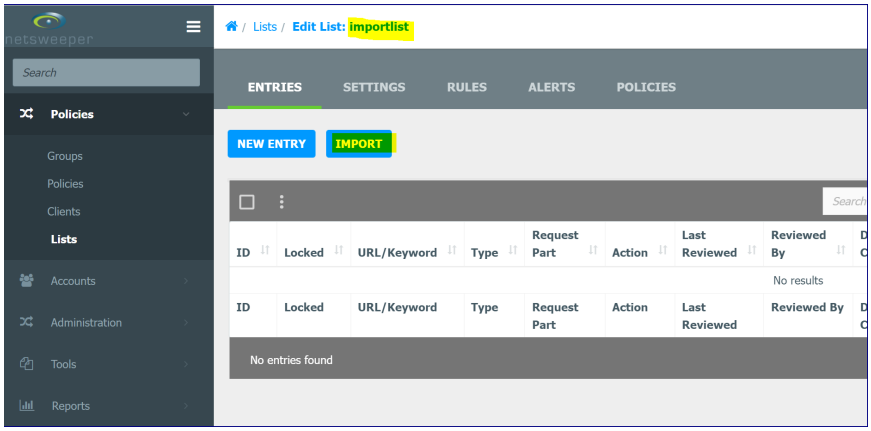
3. Save the file as **systemlisttest.csv**. Use the UTF-16LE format.

Please verify that no other lists contain paypal.com or pinterest.com.

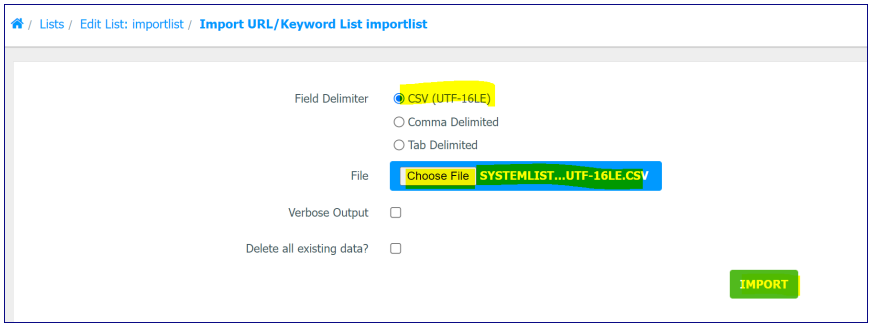
Test Procedure: Importing a System List

In the WebAdmin:

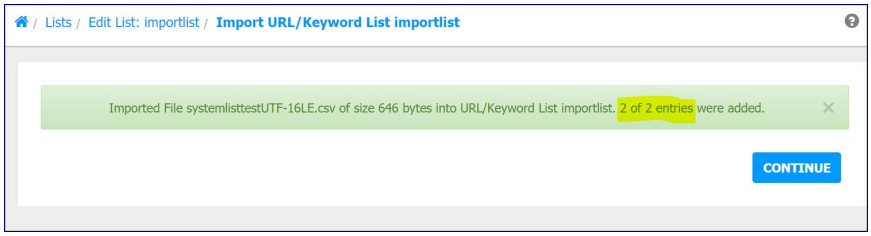
1. Go to Policies > Lists, click the **Lists** tab**.**
2. Click the **importlist** link that was created in *Additional Precondition 2*.
3. Click the **Import** button.



4. Click the **Choose File** button and select the **systemlisttestUTF-16LE.csv** file.
5. Click the **Import** button to open the 'Import URL/Keyword List' window.

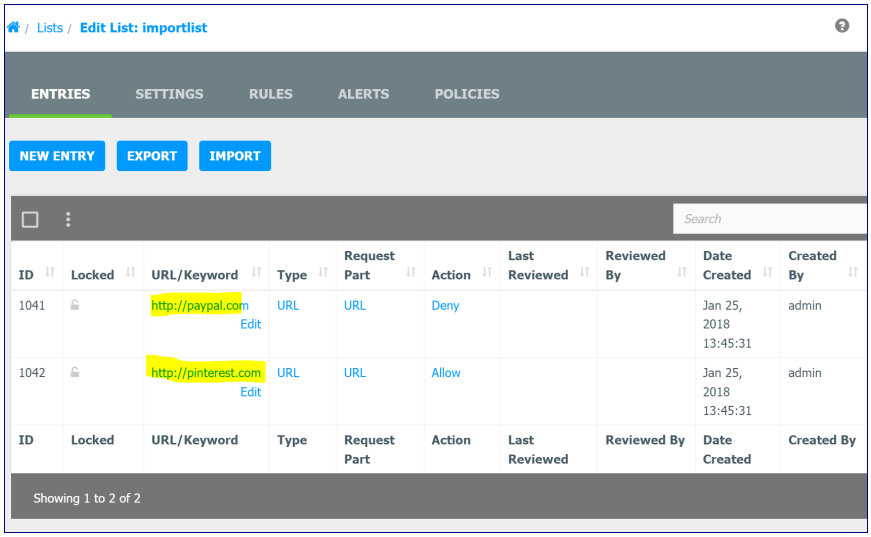


6. Click **Import** again. You will see that '2 of 2 entries were added'.



7. Click the **Continue** button to return to the Edit List window.

8. You will see the two new entries: Pinterest.com and Paypal.com.

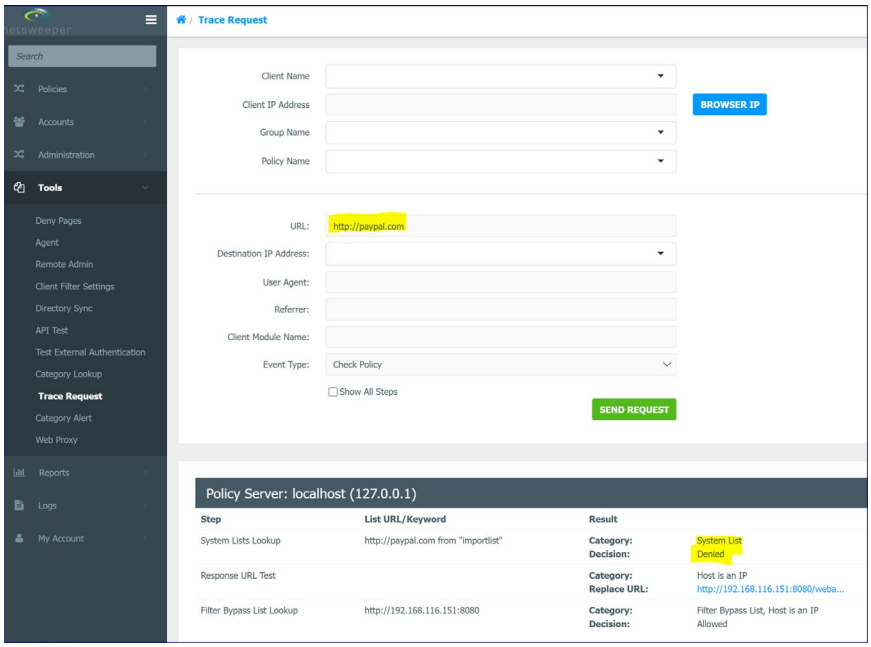


9. Go to Tools > Trace Request

10. In the URL field, enter:
    http://paypal.com

11. Click **Send Request**

12. 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.
Result (Pass or Fail)	
Result 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.

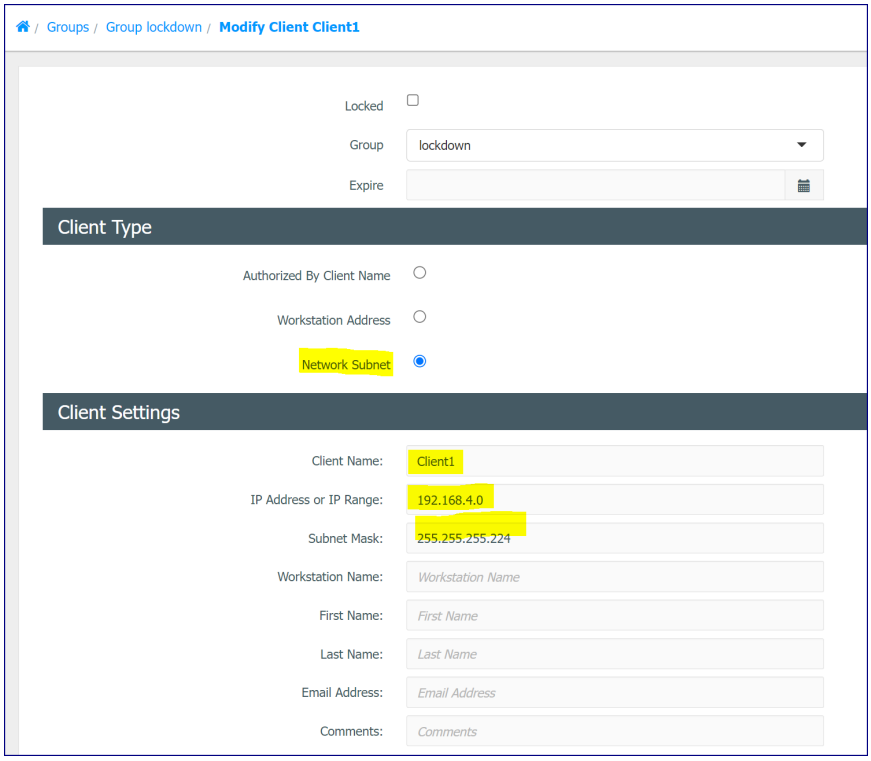
A second filtered client workstation must be available for browsing the Internet and the IP address of the filtered workstation should be within a second network subnet.

Test Procedure: Clients Identified by Subnet

In the WebAdmin:

1. Go to Policies > Groups and click the **Create** tab.
2. Type **lockdown** for the ‘Group Name’ and click **Submit.** The ‘Group Policy’ window displays.
3. Click the **Policies** tab and then the **List** tab.
4. Click the **default** policy.
5. Click the **Categories** tab.
6. Select **Custom** and place a checkmark beside all the top-level Groups to select all the Categories.
7. Click **Submit**.
8. Click the **Group lockdown** breadcrumb and then on the **Clients** tab.
9. Click the **Create** button.
10. In the ‘Client Type’ section select **Network Subnet**.
11. For ‘Client Name’ enter **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. Click **Submit**.
15. Go to Policies > Groups and click the **List** tab
16. Click the **default** Group.
17. Click the **Clients** tab and then the **Create** button.
18. In the ‘Client Type’ section select **Network Subnet**.
19. For ‘Client Name’ enter **client2**.
20. In the ‘IP Address’ field enter an IP Address range that is within 192.168.4.31-192.168.4.245.
21. Click **Submit**.
22. Go to Policies > Clients to verify the two new Clients and their respective IP Addresses and Subnets.
23. Enter details for a client in the first network subnet.

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	
Result (Pass or Fail)	
Result Comments	

Accounts Window

SysOp Permissions

Purpose

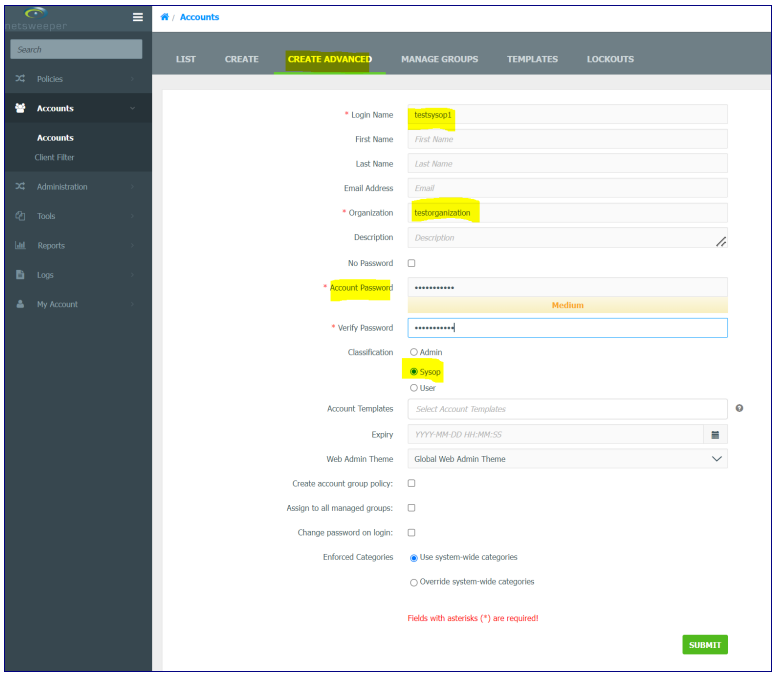
The Netsweeper solution provides permissions that can be enabled or disabled for each **SysOp** account. This test case will verify a portion of the capabilities provided by the permissions feature in the WebAdmin.

Precondition: SysOp Permissions

In the WebAdmin:

Create testsysop1:

1. Go to Accounts > Accounts.
2. Click the **Create 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.

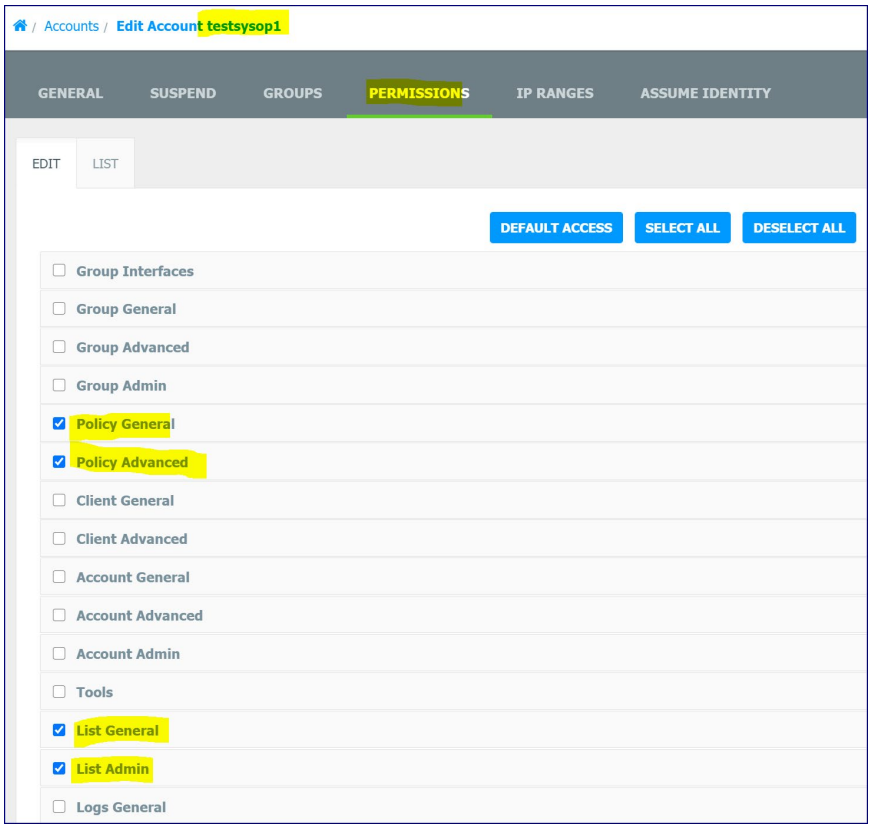


6. Click **Submit**. You are returned to the 'Accounts' window.

Assign Permissions:

1. Click the **Edit** link beside 'testsysop1' to open the 'Edit Account' window.

2. Click the **Permissions** tab.
3. Place checkmarks beside the Policy and List Permission Groups shown here.

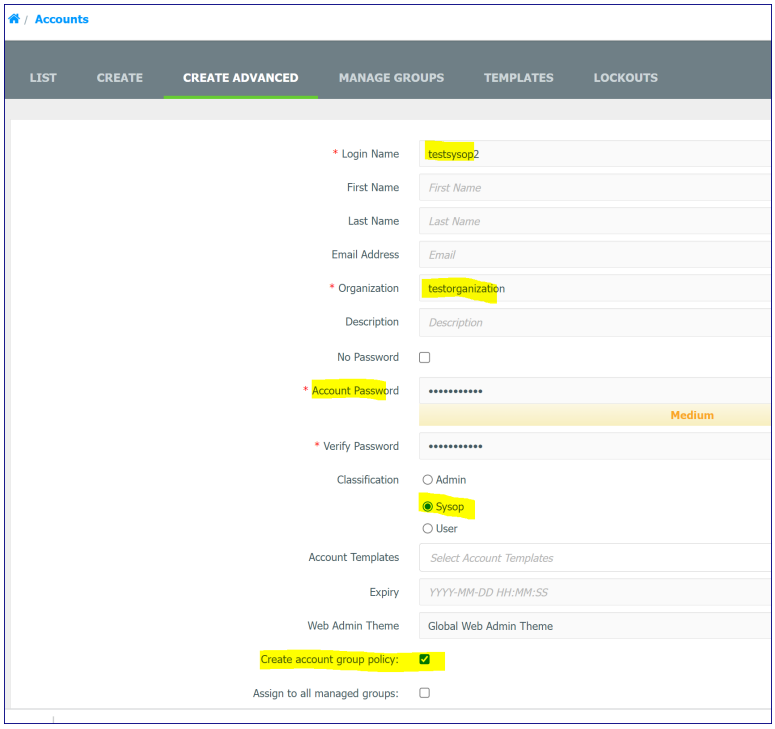


4. Click **Submit** and confirm the modification by clicking **OK** on the warning window. The 'Account Permissions Updated' message displays.

Create testsysop2:

1. Go to Accounts > Accounts
2. Click 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. Click **Submit**. You are returned to the 'Accounts' window.

Modify testsysop2 permissions:

1. Click the **Edit** link beside 'testsysop2' to open the 'Edit Account' window.
2. Click the **Permissions** tab.
3. Enable **Policies** only. Do not check any other permissions.

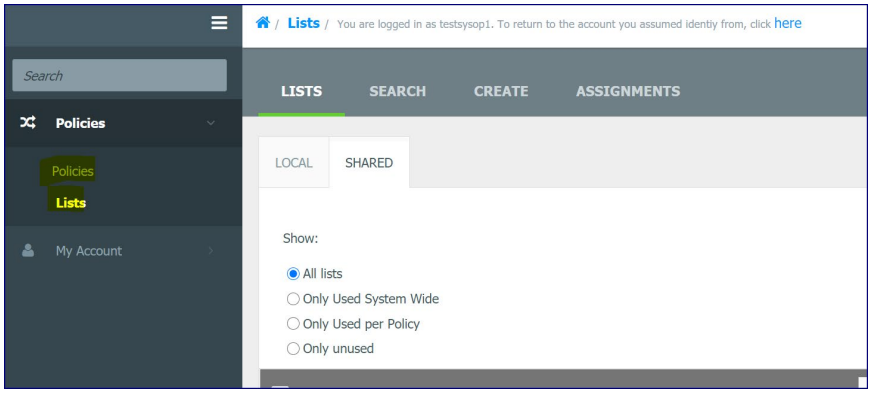
4. Click **Submit** and confirm the modification by clicking **OK** on the warning window. The 'Account Permissions Updated' message displays.

Test Procedure: SysOp Permissions

Log in as testsysop1:

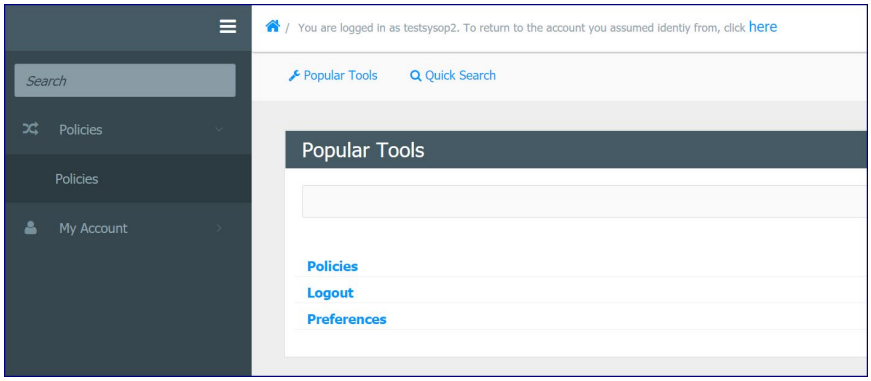
1. Log in as **testsysop1** with password Netsweeper1.
2. Go to Policies > Policies.
3. Click on the **default** Policy.

4. Click the URL / Keyword Local List tab.
5. You can see the **Create Local List** button.
6. In the **Policies** menu you can also see the **Lists** option.



Log in as testsysop2:

1. Log in as **testsysop2** with password Netsweeper1.
2. Go to Policies > Policies.
3. Click on the **default** Policy.
4. Click the URL / Keyword Local List tab.
5. You cannot see the **Create Local List** button.
6. Ensure that '**Lists**' is not a menu option.



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	

Result (Pass or Fail)	
Result 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

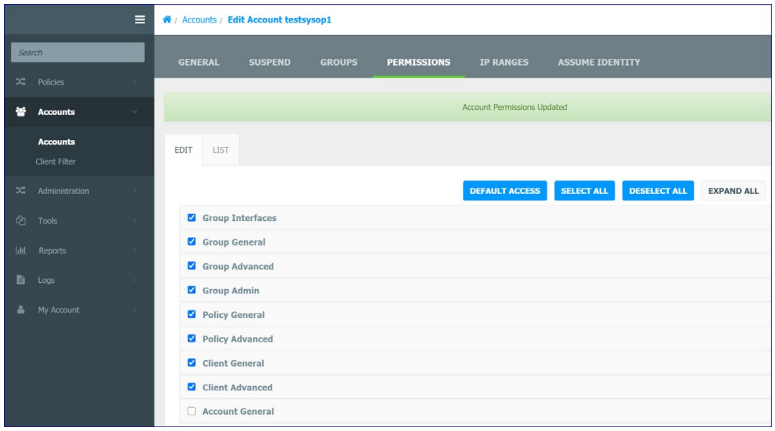
In the WebAdmin:

Create testsysop:

1. Go to Accounts > Accounts and select testsysop1. This is the SysOp we created in the previous procedure.

Modifying testsysop1's Permissions

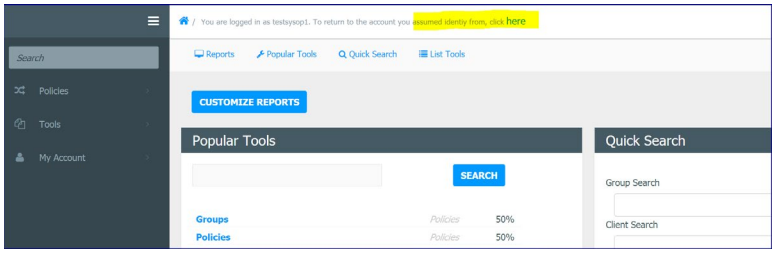
1. Click the **Edit** link beside 'testsysop1' to open the 'Edit Account' window.
2. Click the **Permissions** tab.
3. Choose the **Deselect All** button to deselect the previous permissions we added.
4. Enable: Group, Policy and Client Permissions.
5. Click **Submit** and confirm the modification by clicking **OK** in the warning window. The 'Account Permissions Updated' message displays.



Assume Identity testsysop1

1. Click the **Assume Identity** tab.
2. Go to Policies > Groups and click the **List** tab.
3. Click the **testsysop** group.

4. Click the **Clients** tab and then the **Add New Client** button.
5. Enter **testclient** in the ‘Client Name’ field.
6. Click **Submit**. The Client is added to the ‘Clients’ list.
7. Click the link at the top of the window to return from 'Assume Identity'.



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 **testsysop** group and the Policy(s) for that group.

Notes	
Result (Pass or Fail)	
Result 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

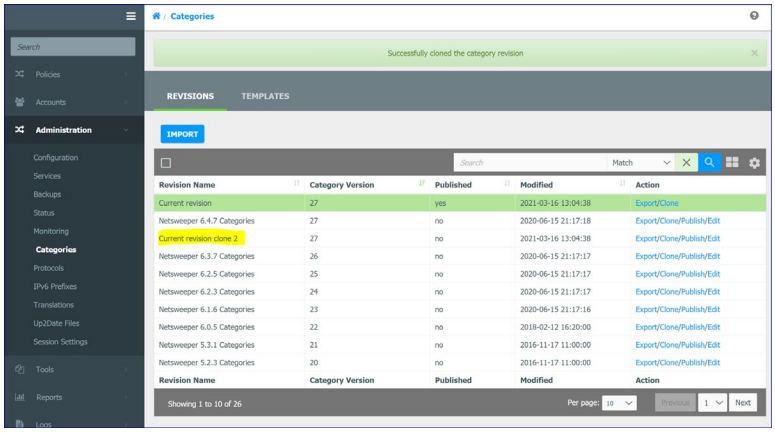
See: Setting up Filtering Group and Client

Only the Category Deny List should be filtered.

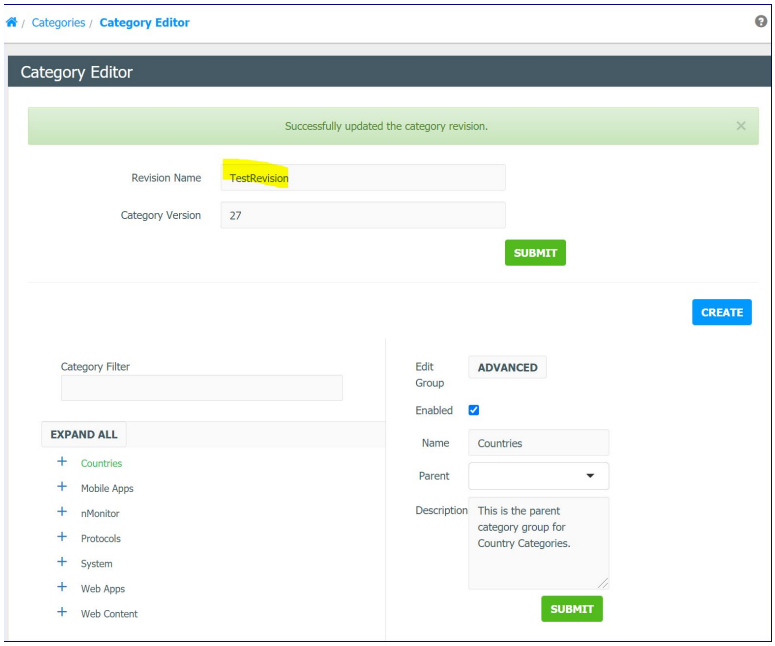
Test Procedure 1: Creating a Custom Category

In the WebAdmin:

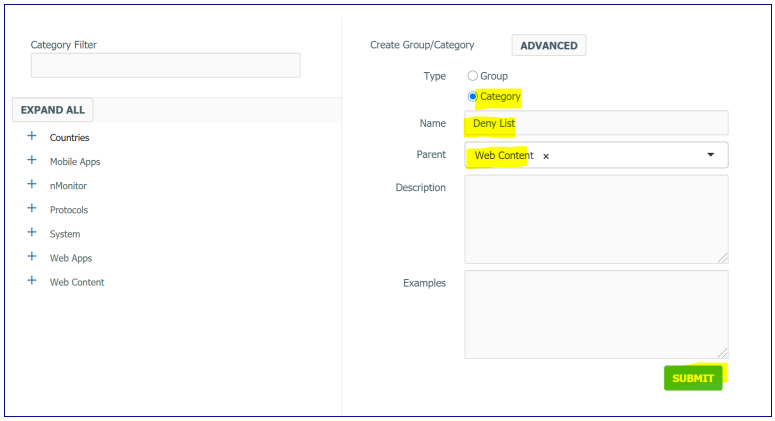
1. Go to Administration > Categories.
2. Click the **Clone** Action for the ‘Published’ Revision (marked in green). A new Revision displays below the published revision.
3. Click the **Edit** link for the newly cloned Revision to open the ‘Category Editor’.



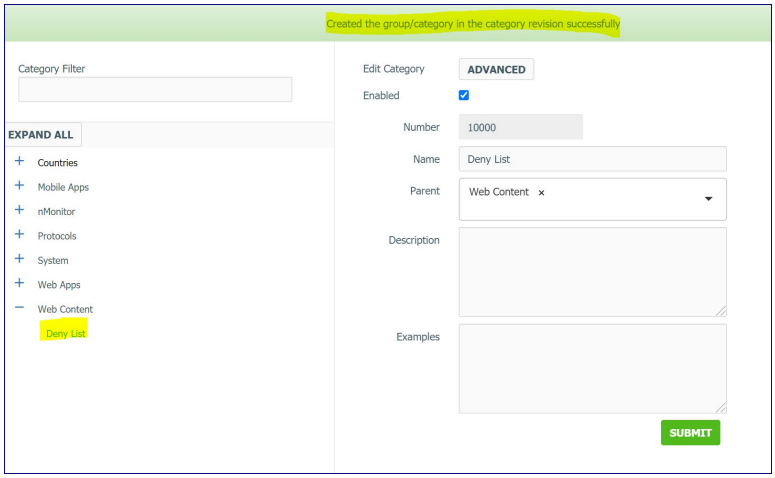
4. Name the Revision: **TestRevision** and click **Submit**.



5. Click the **Create** button.
6. Select ‘Category‘ as the Type .
7. Enter **Deny List** for the ‘Name’ and assign its ‘Parent’ as the **Web Content** Category Group.

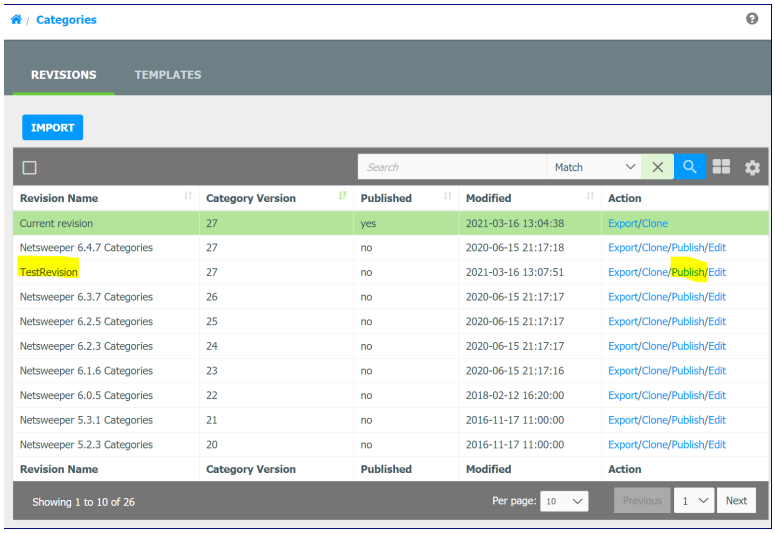


8. Click **Submit**. The new Category displays under the 'Web Content' group.

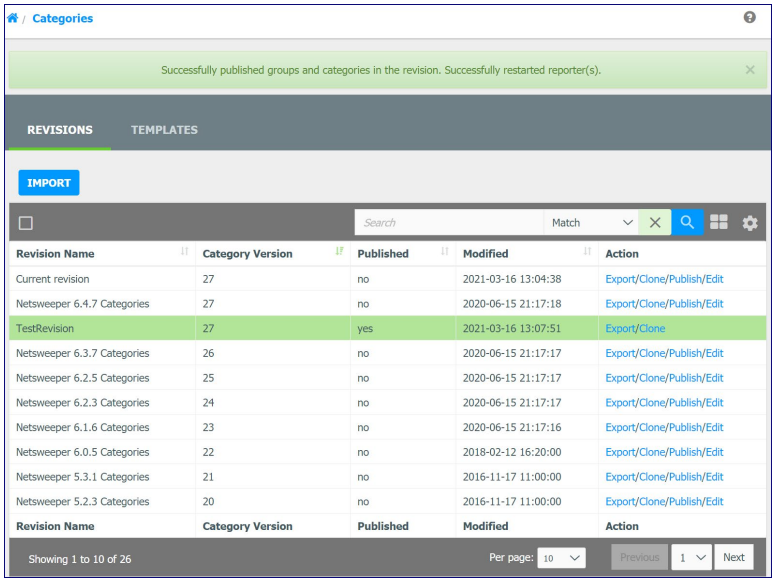


9. Click the breadcrumb to return to the Categories window.

10. Click the **Publish** link beside the TestRevision and click **OK** to confirm the choice.

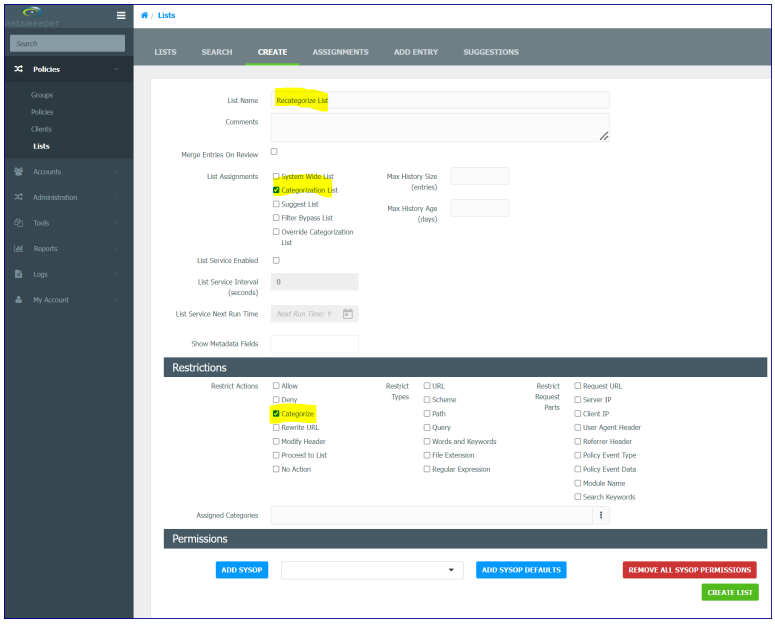


11. The ‘Successfully published groups and categories in the revision’ message displays.



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

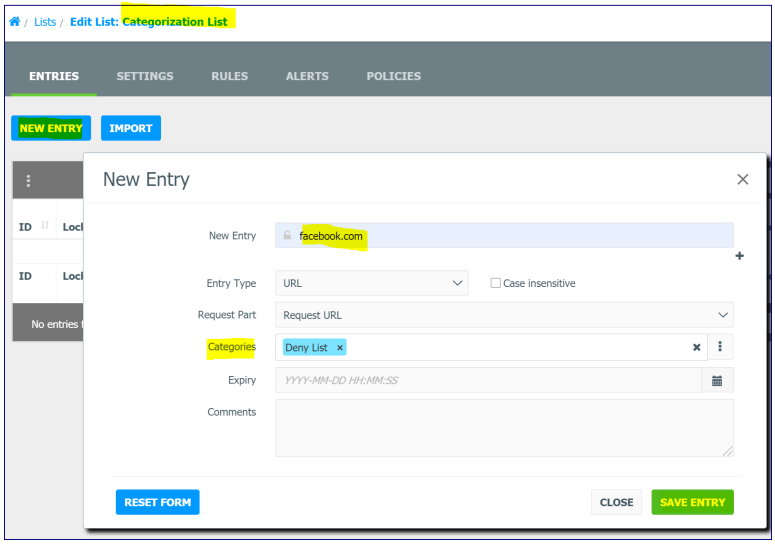
1. Go to Policies > Lists and click the **Create** tab.
2. Enter **Recategorizelist** for the ‘List Name’
3. In the 'List Assignments' section select **Categorization List**.
4. In the 'Restrictions' section choose **Categorize**.



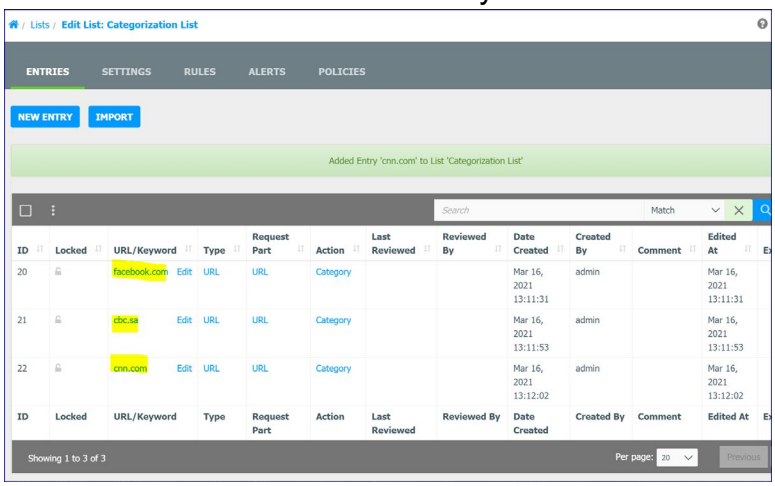
5. Click the **Create List** button.
6. Return to the ‘Lists’ window.

Test Procedures 3: Adding New Entries to the List

1. Select the **Recategorizelist** you created above.
2. Click the **New Entry** button.
3. Enter ***facebook.com*** in the 'New Entry' field.
4. In the 'Categories' section type **Deny List** in the field.
5. The 'Deny List' Category displays in the Categories section.



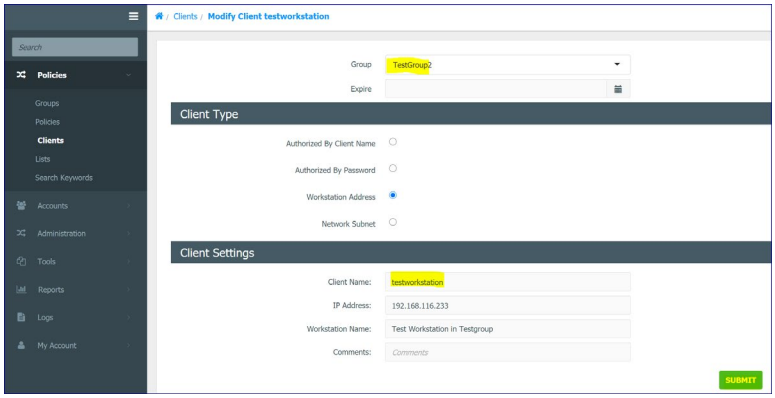
6. Click **Save Entry**. The new entry is added to the list.
7. Repeat the New Entry steps above for ***example1.com***, ***example2.com*** (Where *example1.com* and *example2.com* represents the HTTP URL that was not used in the previous testing).
8. The List Entries Table should look like this.
   NOTE. The URLs seen below may differ from the ones that you have used.



Adding Testworkstation to TestGroup2

Earlier we created a Simple Group TestGroup2. We will add the Testworkstation to this Group.

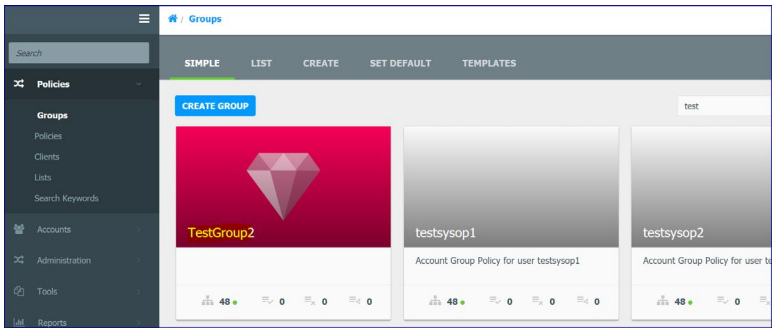
1. Go to Policies > Clients.
2. Click the **testworkstation** to open the modify window.
3. Assign the testworkstation to TestGroup2 by selecting it from the 'Group' dropdown.



4. Click **Submit**.

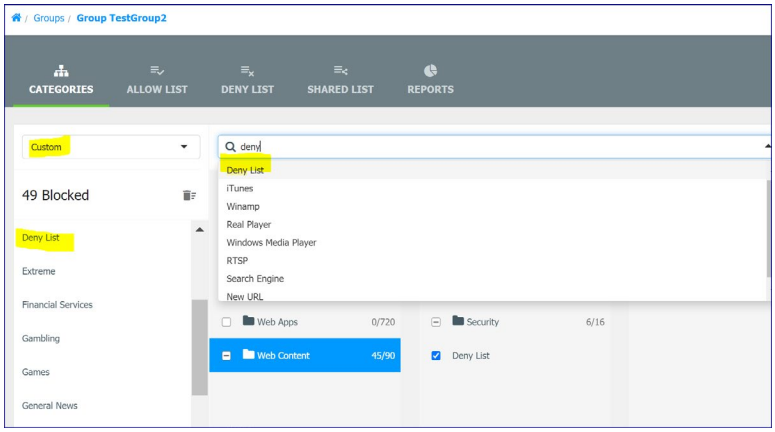
Test Procedures 4: Blocking Sites for the testgroup

1. Go to Policies > Groups and click the **Simple** tab.
2. Click the **TestGroup2** icon.



3. Click the **Categories** tab and select **Custom** from the dropdown list.

4. Type the Custom Categories **Deny List** we created earlier in the 'Quick Add' field and select it.

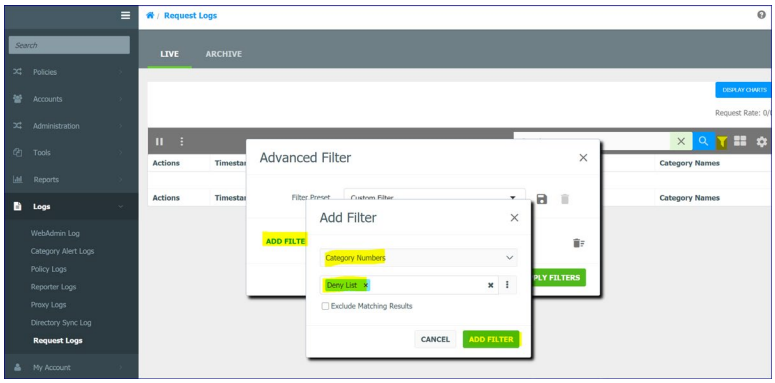


5. The Category **Deny List** is added.
6. Click **Submit**. This will block the ‘Deny List’ category for this Group.

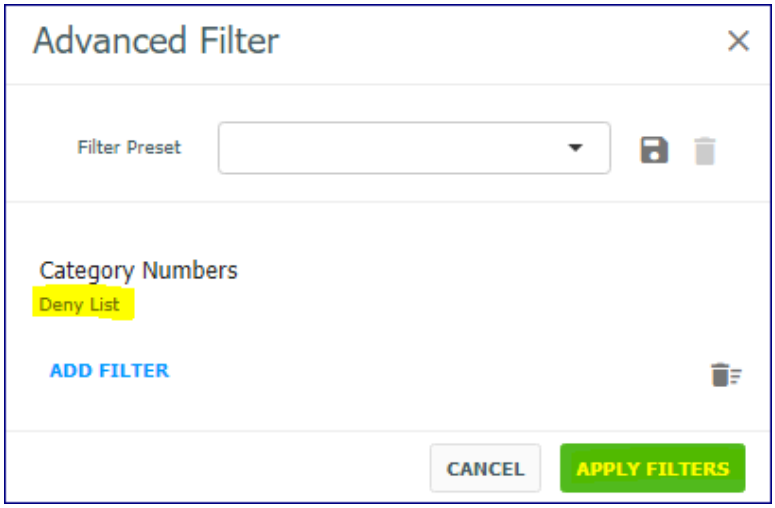
Create a Request Log Filter

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

1. Go to Logs > Request Logs and click the **Advanced Filter** icon to open the 'Advanced Filter' popup.
2. Click the **Add Filter link**.
3. Select **Category Numbers** from the dropdown and type **Deny List** in the next field.
4. Click the **Add Filter** button.



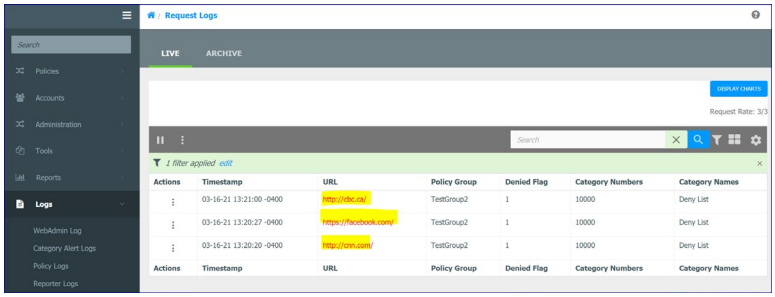
5. The Filter is added. Click the **Apply Filters** button.



Test Procedures 5: Verifying the Custom Categories

On the Test Workstation:

1. With the filtered 'Request Logs' window open, browse to three URLs we recategorized in the **recategorizelist** earlier:
2. http://*example.com*
   http://*example1.com*
   http://*example2.com*
3. The intended webpages will be unreachable on the testworkstation.
4. The three URLs display as 'Denied" with the 'Category Number 'Denied 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	

Result (Pass or Fail)	
Result 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.

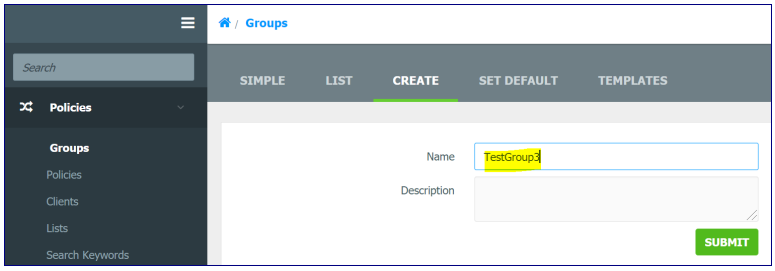
Precondition

See: Setting up Filtering Group and Client

Test Procedure: Allow List Mode

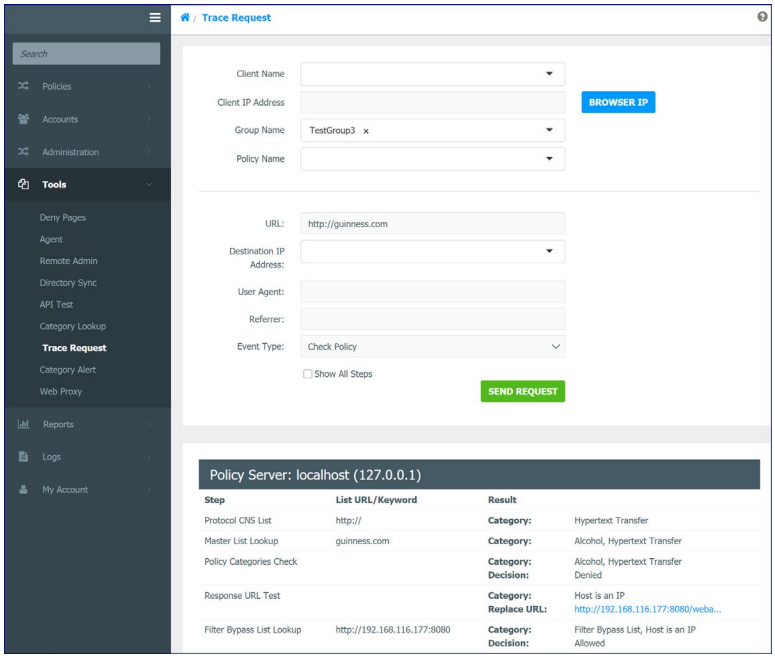
In the WebAdmin:

1. In the 'Groups' window create TestGroup3.



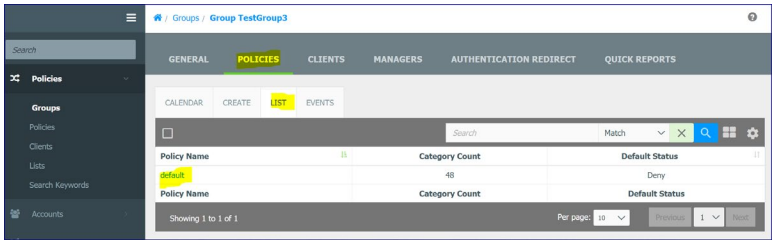
2. In the Tools > Trace Request window ensure select testgroup3 as the 'Group Name' and enter Guinness.com in the URL field.

3. Click the **Send Request** button and confirm that Guinness.com is denied under the Category of 'Alcohol'.

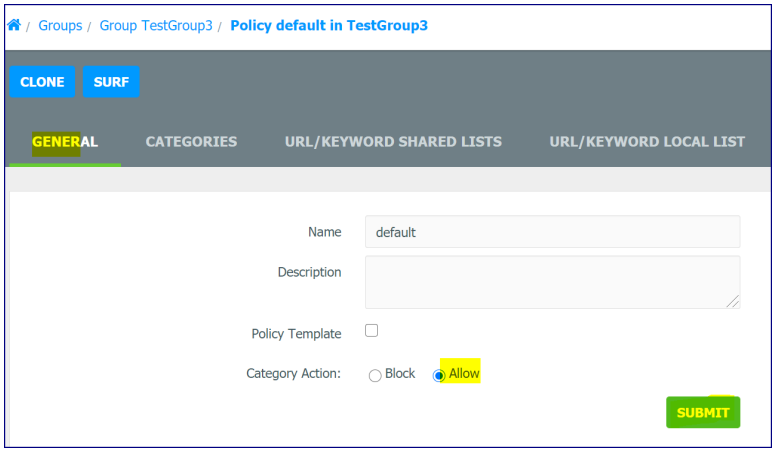


4. Return to TestGroup3 and click the **Policies** and **List** tabs.

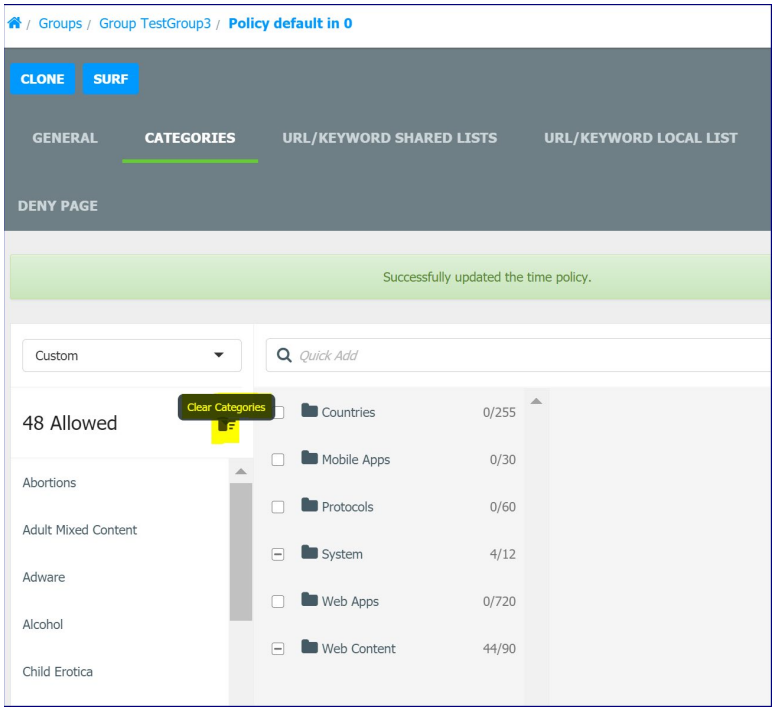
5. Click the **default** policy.



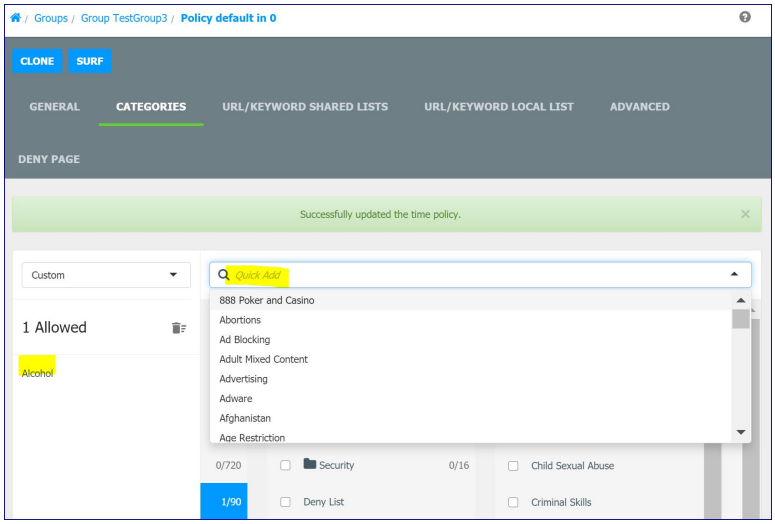
6. In the **General** tab select **Allow** for 'Category Action' and click **Submit.**



7. Click the **Categories** tab, select **Custom** from the dropdown list and delete all the Categories.

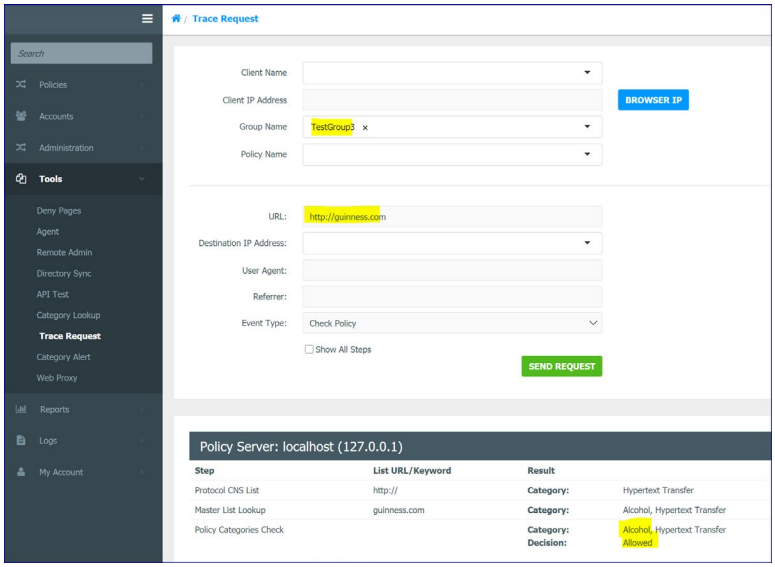


8. In the 'Quick Add' field, type **Alcohol** and add it to the left pane.
9. Click **Submit**.



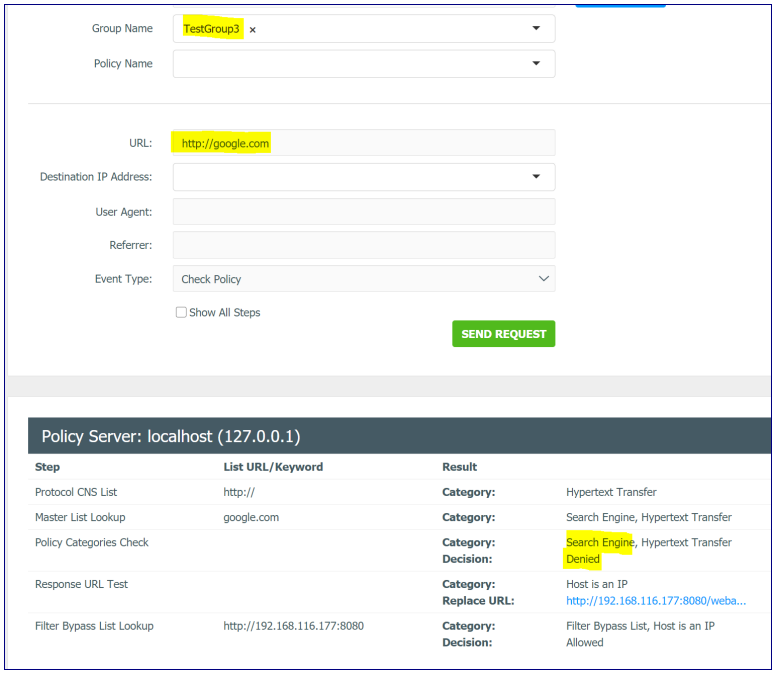
10. Go to 'Trace Request'.
11. Select Testgroup3 from the 'Group Name' dropdown list and enter Guinness.com as the URL.

12. Click the **Send Request** button. You will see that the Category 'Alcohol' is allowed.



13. Enter **google.com** in the URL field and click **Send Request.**

14. You will see that Google is denied under the Category 'Search Engine'.



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	

Result (Pass or Fail)	
Result 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.

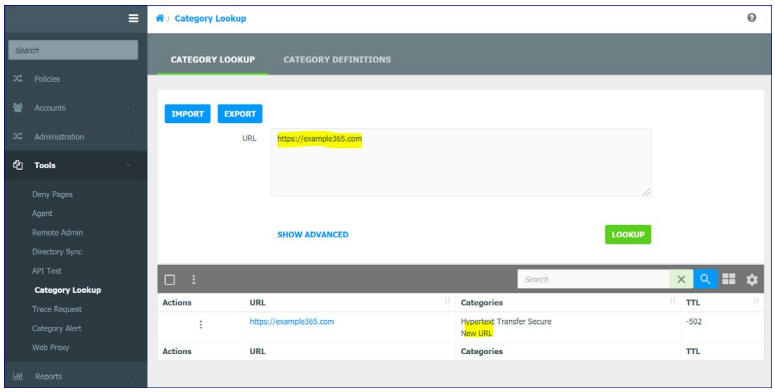
Precondition

CNS connectivity with your Netsweeper Policy Server.

Test Procedure: CNN Categorization

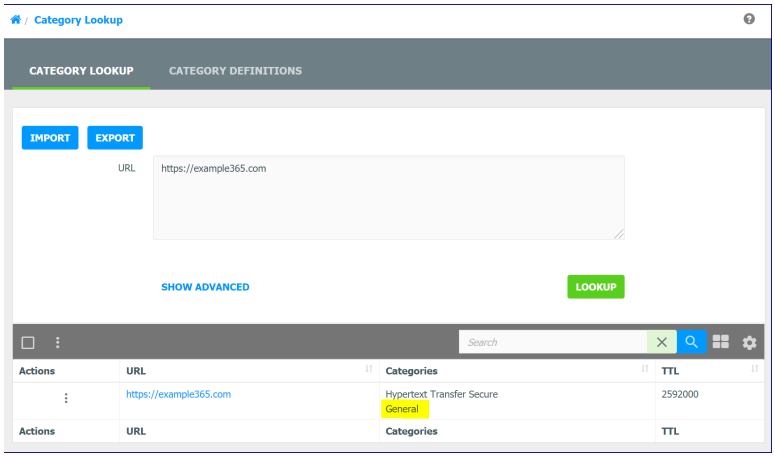
In the WebAdmin:

1. Go to Tools > Category Lookup.
2. Enter a completely random URL (the goal is to find a URL that has never been categorised before. It does not matter if it does not resolve.) In this test we are using example365.com (In your testing you may be using a different URL of your choice). Be sure to add the .com to the end of your URL.
3. Click the **Lookup** button and note the Category returned.



4. Click **Lookup** several more times, approximately once a second, category changes from **New URL** to one of Netsweeper's content categories (i.e. **News, General,**

etc…).



Pass Criteria

When the **Find** button first clicked 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 click the **Find** button 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 region.
Result (Pass or Fail)	
Result 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.

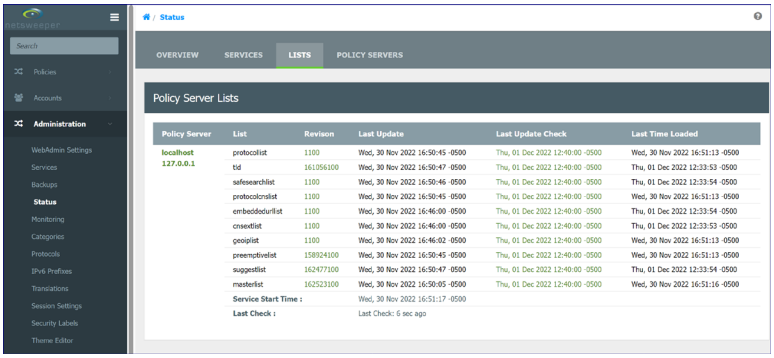
Test Procedure: List Update

In the WebAdmin:

1. Go to Administration > Status.
2. Click on 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 List may be different.



Notes	
Result (Pass or Fail)	
Result Comments	

Centralized Management

Purpose

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

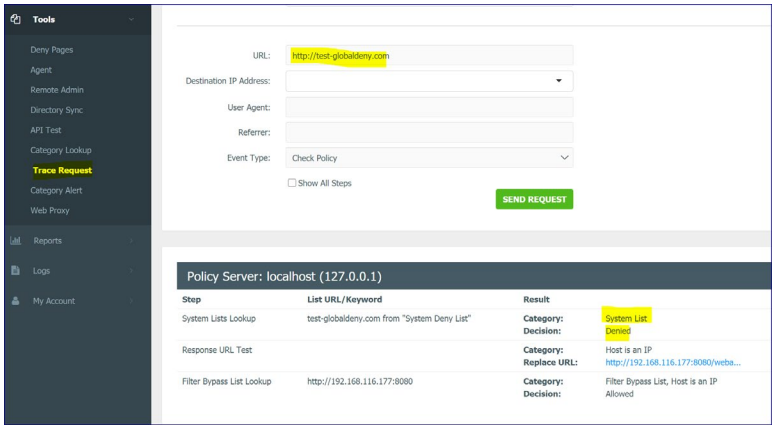
Precondition

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

Test Procedure

In the WebAdmin:

1. Go to Policies > Lists.
2. In the Lists tab, click the **System Deny List.**
3. Click the **New Entry** button.
4. Add **test-globaldeny.com** to the System Deny List.
5. Ensure **Request URL** is selected from the ‘Request Part’ section.
6. Click **Save Entry**.
7. Go to Tools > Trace Request
8. In URL field enter **http://test-globaldeny.com** and click **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	

Result (Pass or Fail)	
Result 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	
Result (Pass or Fail)	
Result Comments	

Boundary Tests

URL List Import Limit

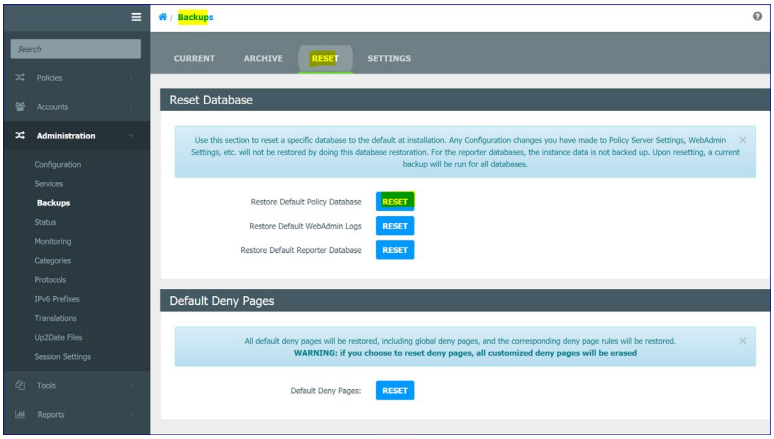
Purpose

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.



Re-create your testgroup and testworkstation.

See: Creating a Group ‘testgroup’ and Test Workstation Client

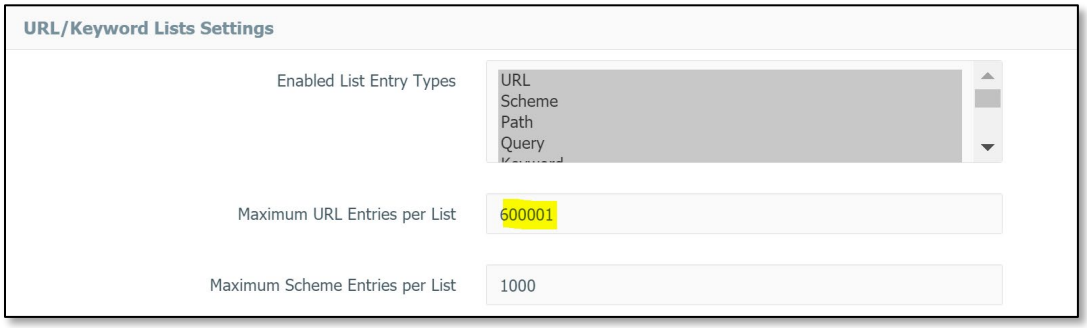
You will require the **Netsweeper 600000 URL Import.csv** file. The zip file can be downloaded from here:

https://helpdesk.netsweeper.com/docs/UAT/8_1_Resources/User_Acceptance_Resource_8_1_Page.html

Modifying WebAdmin Settings

1. Go to Administration > **WebAdmin Settings** button.
2. Scroll down to ‘URL/Keyword Lists Settings’.

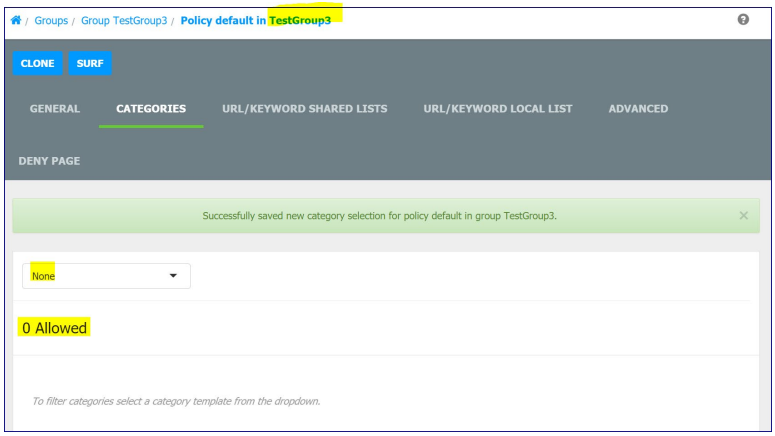
3. Change the ‘Maximum URL Entries per List’ number to 600001.



4. Click the **Submit** button.

De-select all Categories for the Testgroup3

1. Go to Policies > Groups and in the List tab select **testgroup3**.
2. Click the **Policies** tab and then the **Policy** List tab.
3. Click the **default** Policy.
4. In the **Categories** tab, Select **None** under Categories Selection.
5. Click **Submit**.

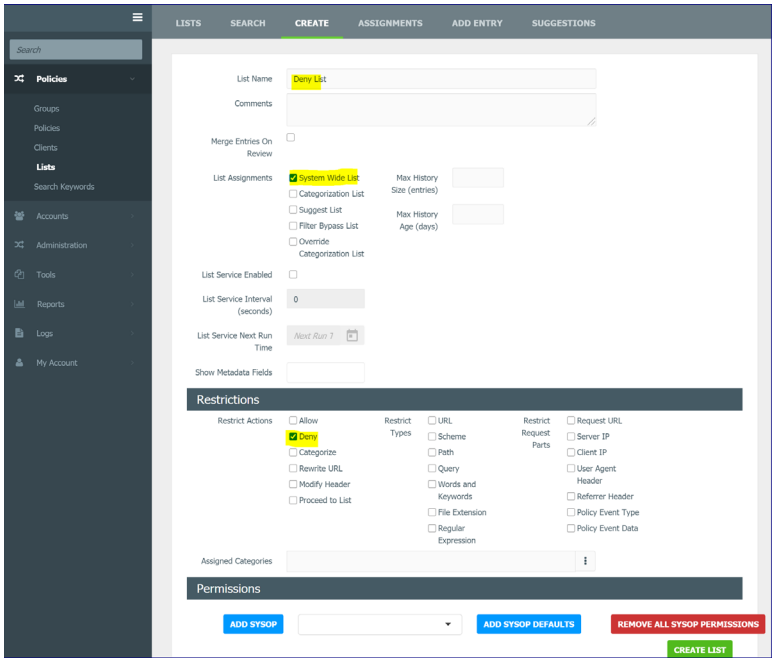


Test Procedure: URL List Import Limit

In the WebAdmin:

1. Go to Policies > Lists.
2. Click the **Create** button.
3. Enter **Deny List** in the ‘List Name’ field.

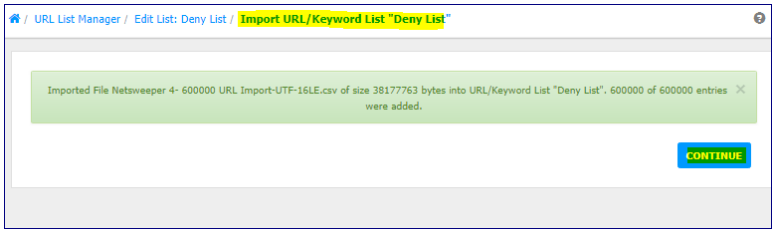
4. Choose System Wide List from List Assignments and select the **Deny** checkbox in ‘Restrictions’.



5. Click the **Create List** button.
6. Return to the ‘Lists’ window.

Importing a List:

1. Click the **Deny List** link and click the **Import** button.
2. Choose the **Netsweeper 4- 600000 URL Import-UTF-16LE.csv** and click the **Import** button. The ‘Import URL / Keyword List’ window displays.
3. Leave the defaults as is and click **Import**. The import may take a while.
4. Once the import is complete message ‘Imported File Netsweeper4- 600000 URL Import.csv of size 38177763 bytes into URL/Keyword List "Deny List". 600000 of 600000 entries were added.’
5. Go to Policies > Lists.
6. Ensure that the Entries field shows 600000 for the ‘Deny List’.



7. Open the ‘Deny List’ to confirm that the items have been added.

In WebAdmin:

1. Go to Tools > Trace Request
2. For Group Name select the **testgroup3** and in the URL field, enter: http://facebook.com
3. Click **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
6. Click **Send Request.**
7. Policy Server results should state that request was '**Denied**' since URL entry was on the list that we have imported and associated with the System Deny List.

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	
Result (Pass or Fail)	
Result Comments	

Request Logging 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'

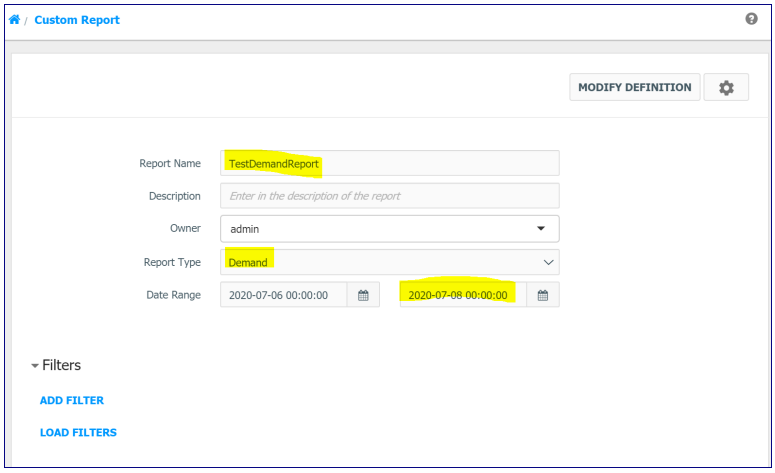
Test Procedure

On the Test Workstation:

Generate some HTTP traffic to be logged by your policy server. This can be achieved by surfing any webpage online.

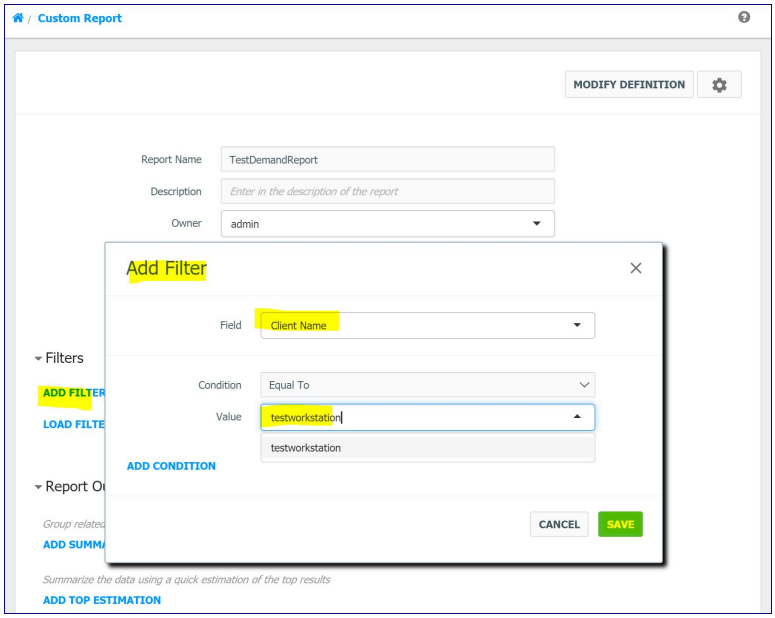
In the WebAdmin:

1. Go to Reports > Custom Report.
2. Enter **TestDemandReport** as the 'Report Name'.
3. Confirm **Demand Report** is selected and choose tomorrow's date in the 'to' date.

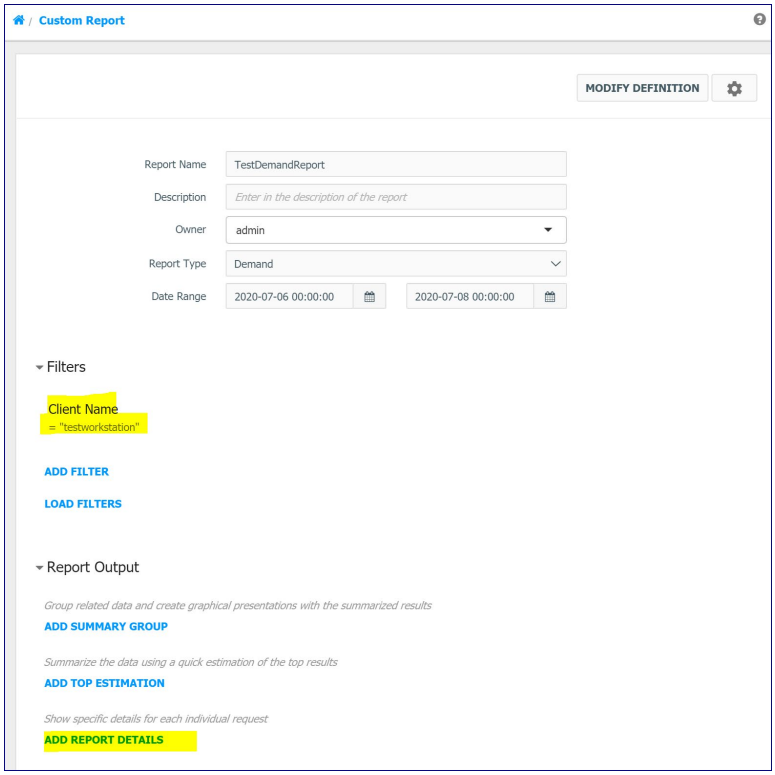


4. Click the **Add Filter** link.

5. Select **Client Name** with a Value of **testworkstation**. Click **Save**.

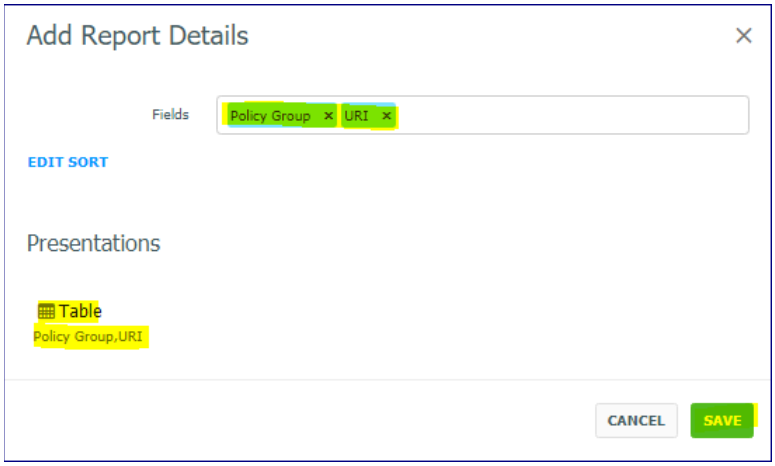


6. Confirm the new filter is added and then click the **Add Report Details** link.

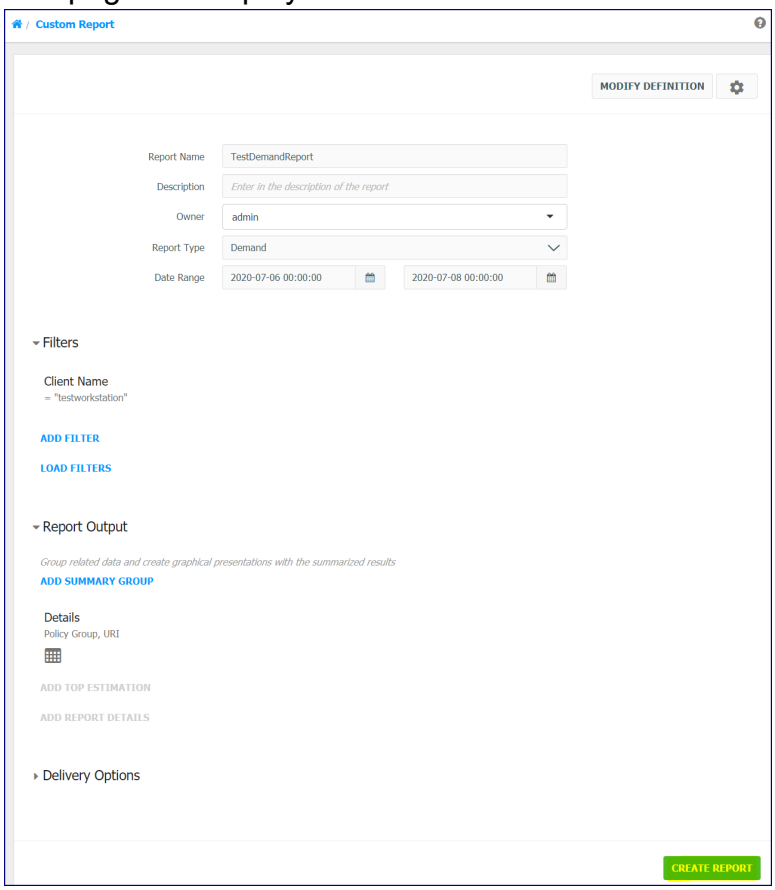


7. Select Policy Group and URI and accept **Table** as the Presentation type.

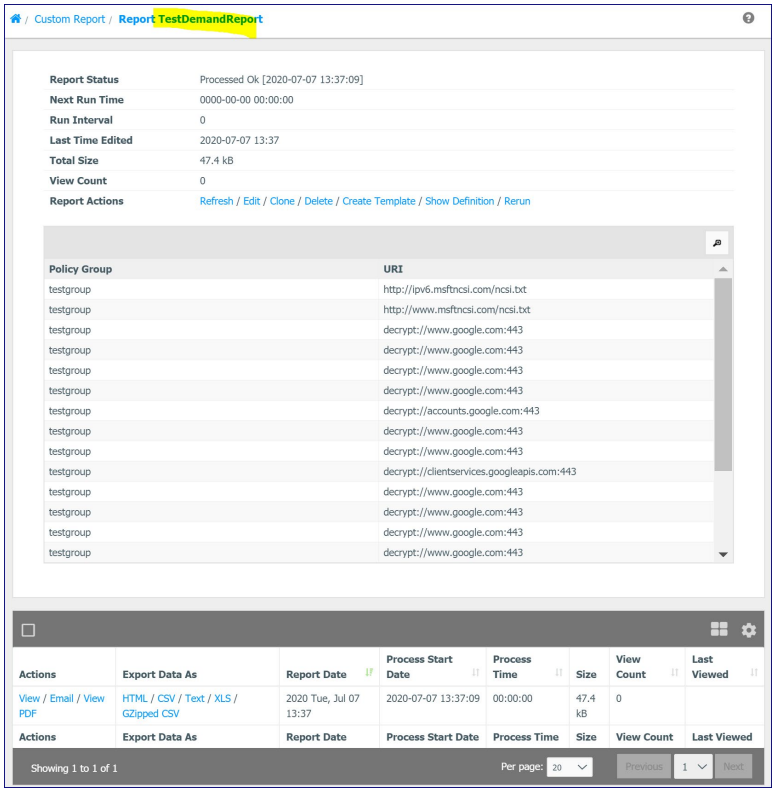
8. Click **Save**.



9. The page will display the Details chosen. Click the **Create Report** button. .



10. The new Report displays. Click the **View** link to display the report.



Pass Criteria

The report will show all the URL entries that have been requested by a **testworkstation** client.

Notes	
Result (Pass or Fail)	
Result 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

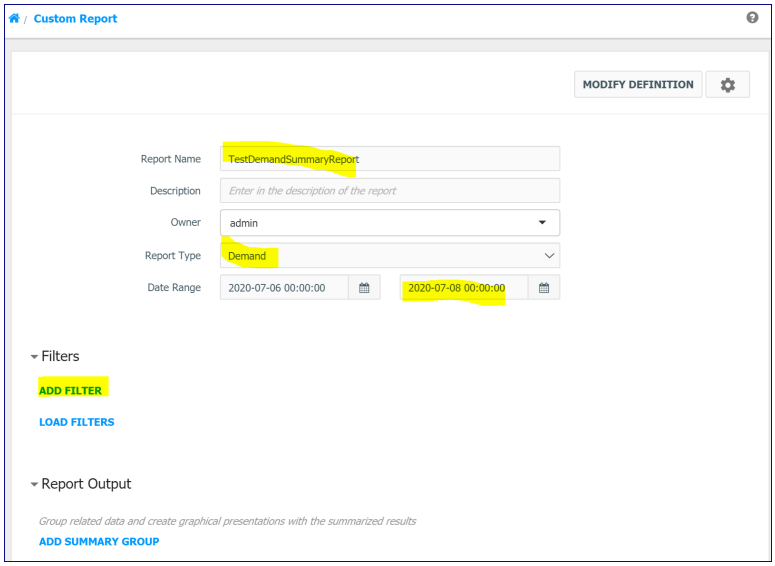
See: Setting up Filtering Group and Client

Test Procedure on the Test Workstation:

Browse to both denied and allowed sites.

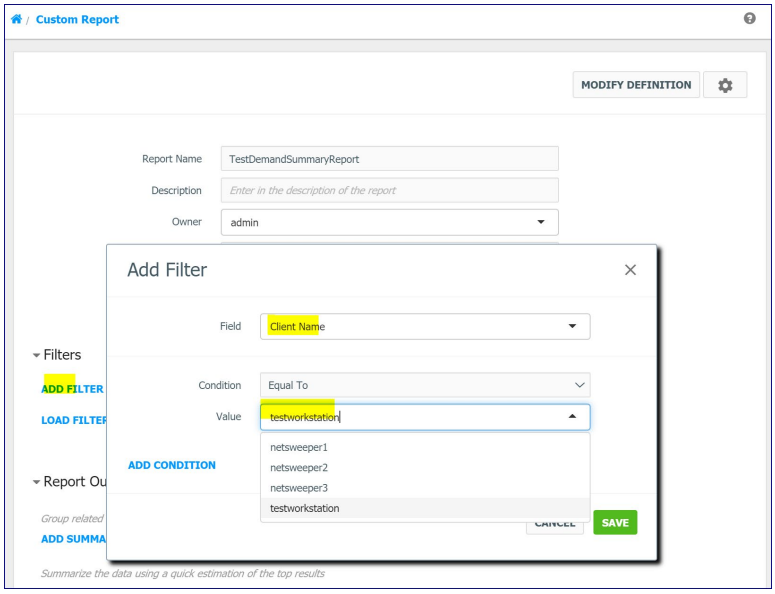
In the WebAdmin:

1. Go to Reports > Custom Report.
2. Enter **TestDemandReport** as the 'Report Name'.
3. Confirm **Demand Report** is selected and choose tomorrow's date in the 'to' date.



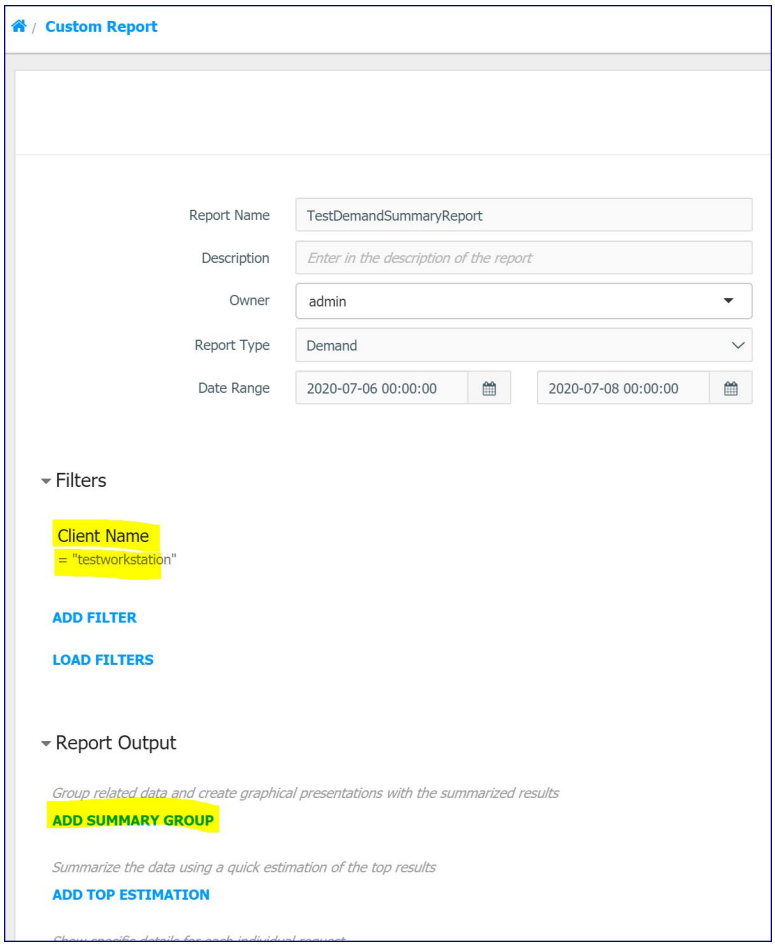
4. Click the **Add Filter** link.

5. Select **Client Name** with a Value of **testworkstation**. Click **Save**.

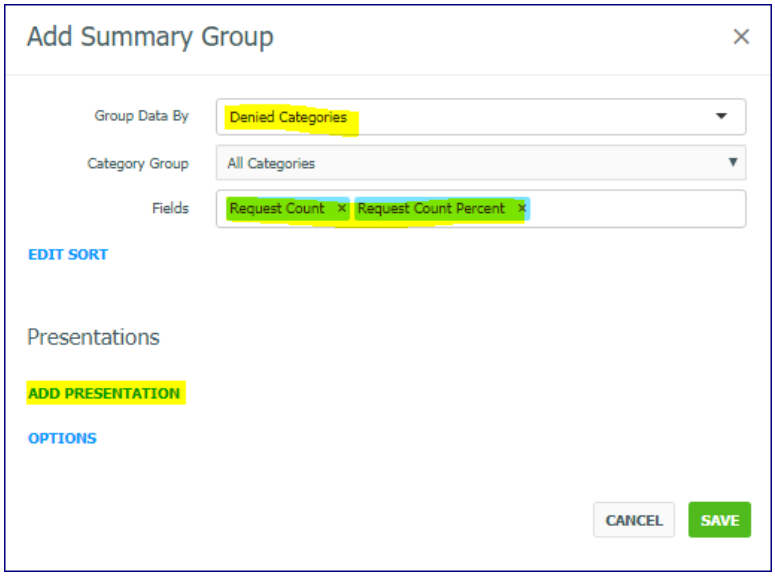


6. The new filter displays.

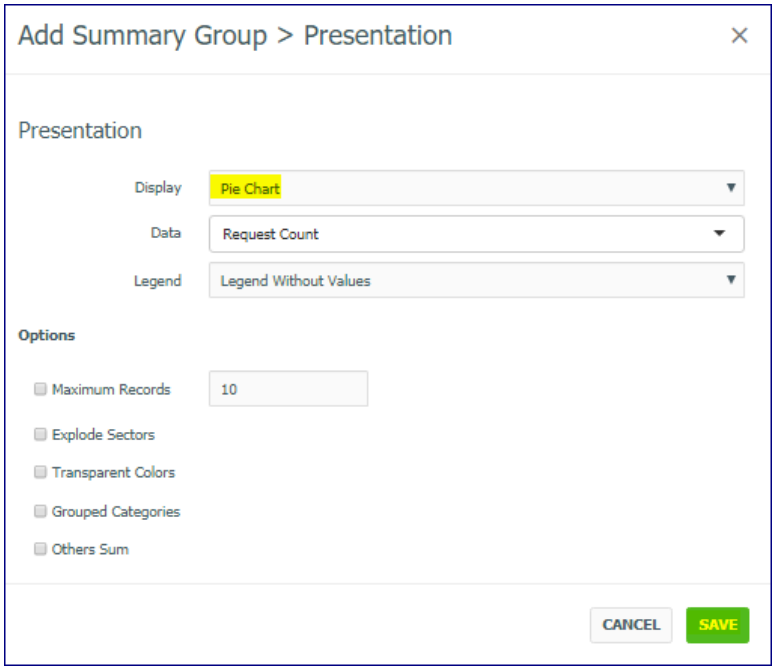
7. Click the **Add Summary Group** link.



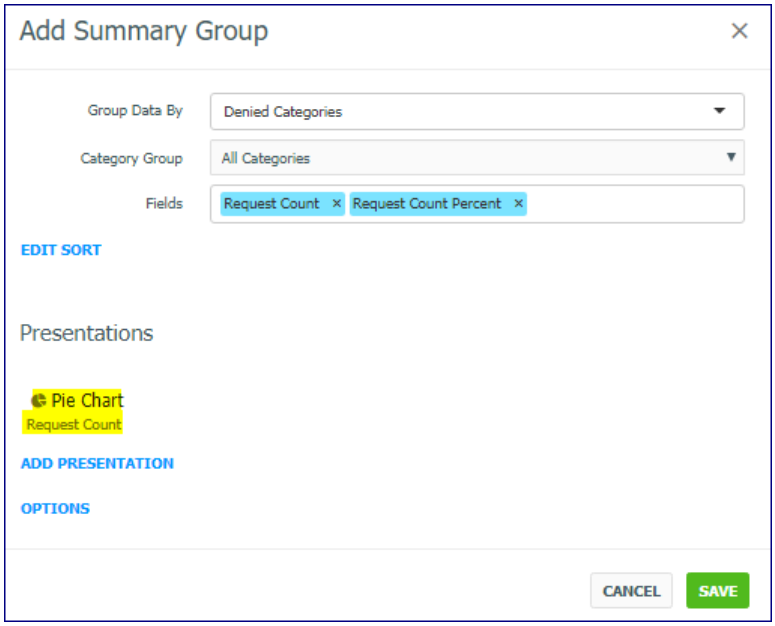
8. Select **Denied Categories** and then add **Request Count** and **Request Count Percent** to the 'Fields' List.



9. Click **the Add Presentation** link.
10. Select **Pie Chart** and choose **Save**.

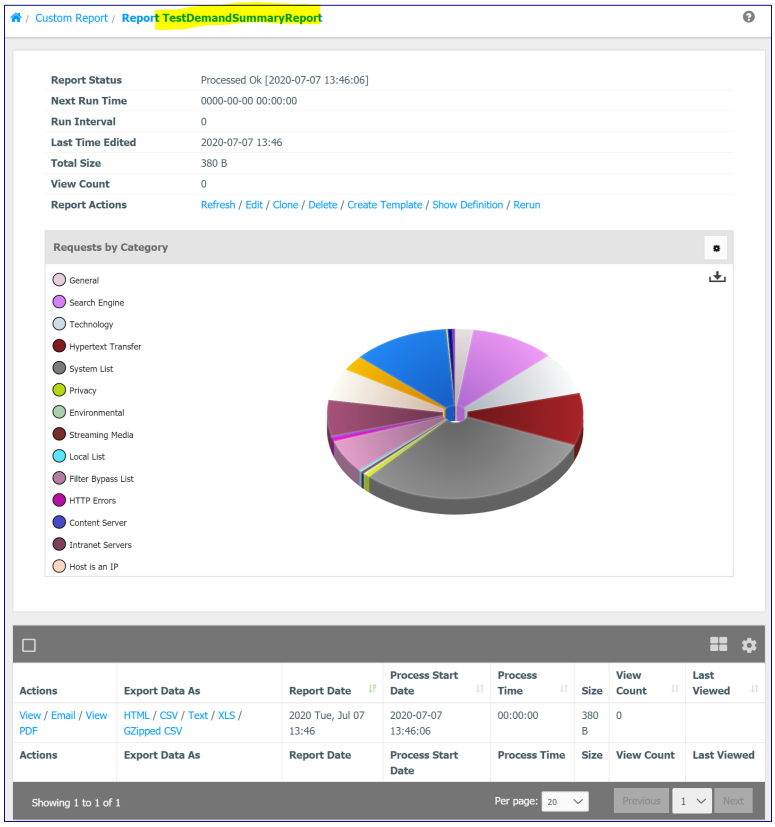


11. Save the 'Summary Group' window.



12. Click the **Create Report** button.

13. The Report displays.



Pass Criteria

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

Notes	
Result (Pass or Fail)	
Result 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

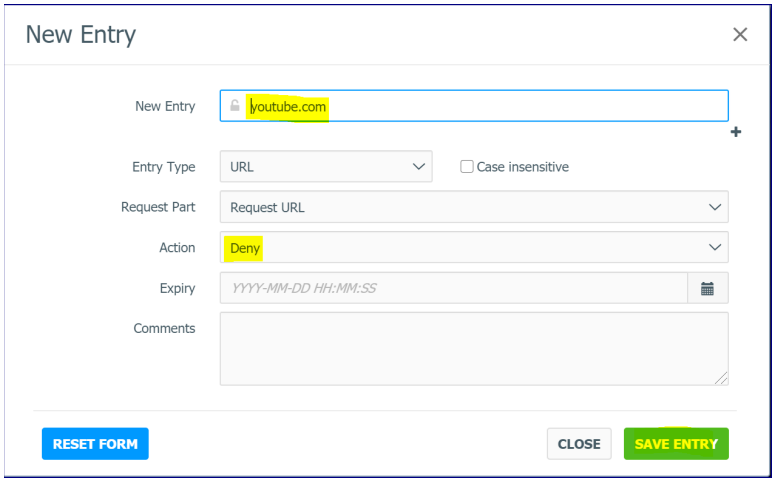
This Procedure will add https://*example.com* to the local deny list group policy for the filtering.

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

In the WebAdmin:

1. Go to Policies > Groups and in the **Lists** tab click on **testgroup**.
2. Click the **Policies** tab and then on the **List** tab.
3. Click the **default** link for the Policy.
4. Click the **URL/Keyword Local List** tab and then on the **Create Local List** button.
5. Click the **New Entry** button.
6. Add **https://*youtube.com*** in the ‘New Entry’ field (Where *example.com* in this case represents the popular search engine of your choice).
7. Ensure that **URL** is selected from the dropdown.
8. Ensure **Request URL** is selected from the ‘Request Part’ section.

9. Select **Deny** in the 'Action' section.



10. Click the **Save Entry** button.

On your Test Workstation:

1. Clear the cache in your browser.
2. Browse to:
   https://*youtube.com*
3. 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://*example.com* (Where example.com represents the HTTPS webpage of your choice).

Using the filtered workstation in the **testgroup** group, browsing to a URL that belongs to the Local List as a 'Deny' URL **will not** be reachable.

Notes	In HTTPS, No Deny page will be served, connection reset page will be displayed instead. When same domain is accessed via HTTP, then content will be available. In addition, you may have to specify the www or m (mobile) before the domain name in order for URL to be detected e.g. https://m.*example.com*, https://www.*example.com*
Result (Pass or Fail)	
Result 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

The ***client*** for this project agrees that the acceptance tests contained within this document have been executed completely, and to the satisfaction of the requirements of this project.

Client Name	
Authorized Party Signature	
Authorized Party Name	
Date	