

**McAfee Security Connected**  
*Integrating ePO and MWG*



<b>Table of Contents</b>	
<b>Overview</b>	<b>3</b>
<b>User Accounts &amp; Privileges</b>	<b>3</b>
<b>Prerequisites</b>	<b>3</b>
<b>Configuration Steps</b>	<b>4</b>
<b>Configuring Web Gateway for ePO</b>	<b>4</b>
<b>Configuring ePO for Web Gateway</b>	<b>10</b>
<b>Configuring Common Catalog</b>	<b>14</b>
<b>Testing Common Catalog</b>	<b>18</b>
<b>Value Add</b>	<b>21</b>

## Overview

ePO and Web Gateway integration. ePO can show Web Gateway data in the dashboards. ePO can also do full web traffic reporting of Web Gateway with the installation of Content Security Reporter. Content Security Reporter allows one to pivot in on a dashboard for more detail. One can pivot on a URL in Content Security Reporter (CSR) and get threat information from McAfee Global Threat Intelligence (GTI). In addition to full web traffic reporting, Content Security Reporter also allows an admin to immediately add a site to a white or black list through the Common Catalog ePO plugin, which is what we will cover in this document.

Although not covered in this document, ePO can also be used to deploy McAfee Client Proxy, or MCP, to mobile users. MCP is then used to automatically redirect that client to Web Gateway or Web SaaS.

## User Accounts & Privileges

Content Security Reporter requires administrator privileges to install on a Windows 2008 server.

## Prerequisites

This integration requires McAfee Web Gateway version 7.1 or higher. MWG 7.1 may be downloaded here: [https://contentsecurity.mcafee.com/software\\_mwg7\\_download](https://contentsecurity.mcafee.com/software_mwg7_download).

This integration requires ePO version 4.6.5 and newer. It may be found on the McAfee download site <http://www.mcafee.com/us/downloads/downloads.aspx>.

This also requires McAfee Content Security Reporter version 2.0 and higher. CSR may be downloaded here: [https://contentsecurity.mcafee.com/product\\_csr](https://contentsecurity.mcafee.com/product_csr).

You will need a Content Security Portal account in order to download Web Gateway. If you do not have an account you may request one by emailing the Advanced Technologies Group at "DL Web Gateway and Identity SE team". You will also need a grant number to download Content Security Reporter and ePO.

You will need a McAfee grant number to download ePO and the Content Security Reporter software.

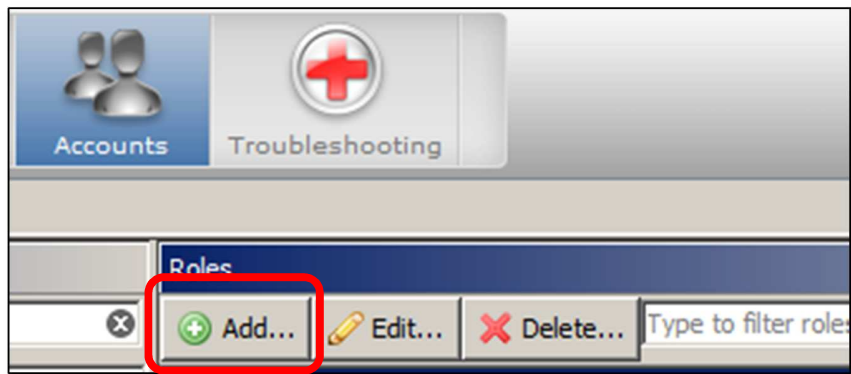
The configuration steps that follow will assume that you already have Web Gateway installed and configured and have successfully run traffic through it to generate logged traffic. It will be assumed that ePO is installed and running. It will also be assumed that Content Security Reporter has been installed and configured and is receiving log data from Web Gateway. Please see the respective documentation for these products located on <https://contentsecurity.mcafee.com/> for those configurations.

## Configuration Steps

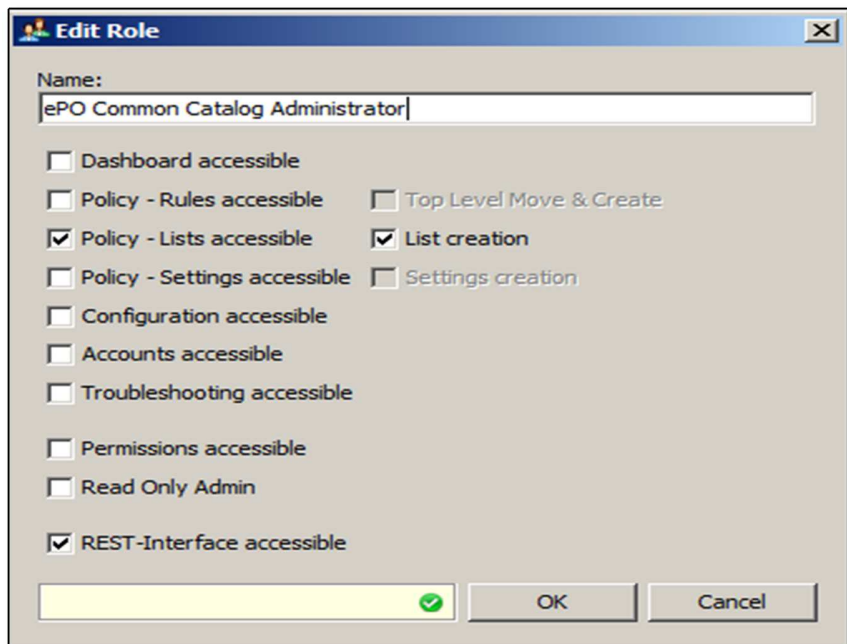
There will be a couple configurations required to get web gateway, ePO, and Content Security Reporter to seamlessly work together. We will need to get Content Security Reporter to talk to ePO, and we will need to get Web Gateway to talk to ePO.

## Configuring Web Gateway for ePO

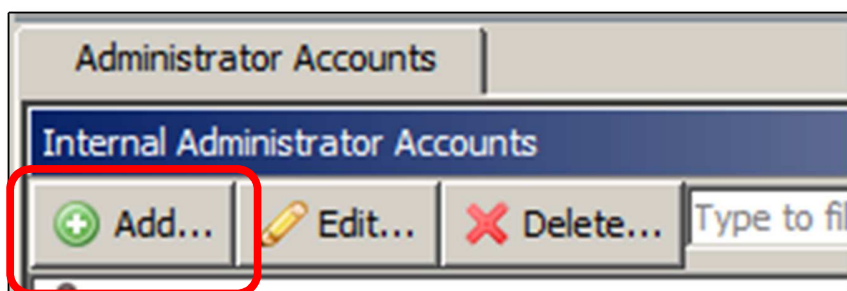
1. Log in to Web Gateway as an administrator
2. **Navigate** to the “Accounts” tab and **Click** the “Add” button in the “Roles” box



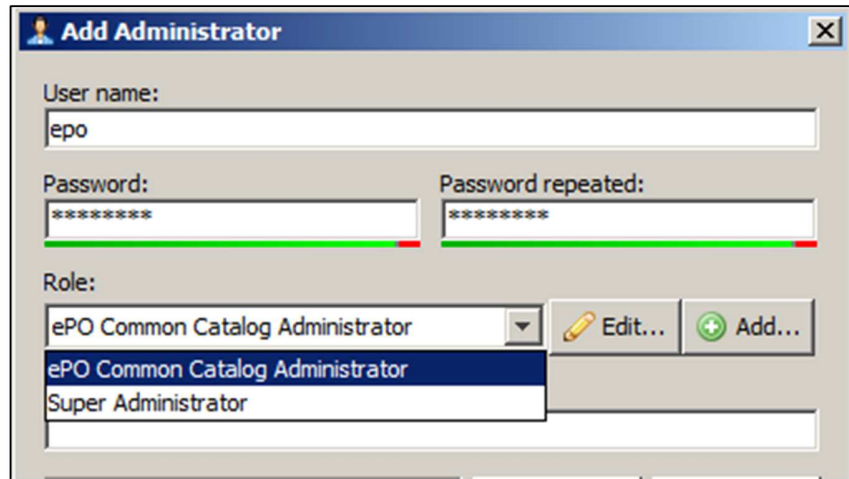
3. Create a role for communication with ePO
  - a. Create a descriptive name for the role
  - b. **Tic** the boxes to assign the following roles
    - i. Policy – Lists accessible
    - ii. List creation
    - iii. REST – Interface accessible
  - c. **Click** “OK”



4. **Click** the “Add” button in the “Internal Administrator Accounts” box

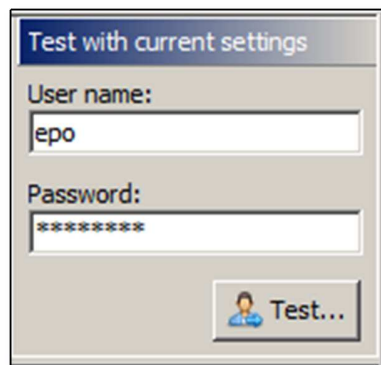


5. Create a user for communication with ePO
  - d. Create a user name and password for the ePO user
  - e. **Select** the ePO role created in the previous step
  - f. **Click** "OK"

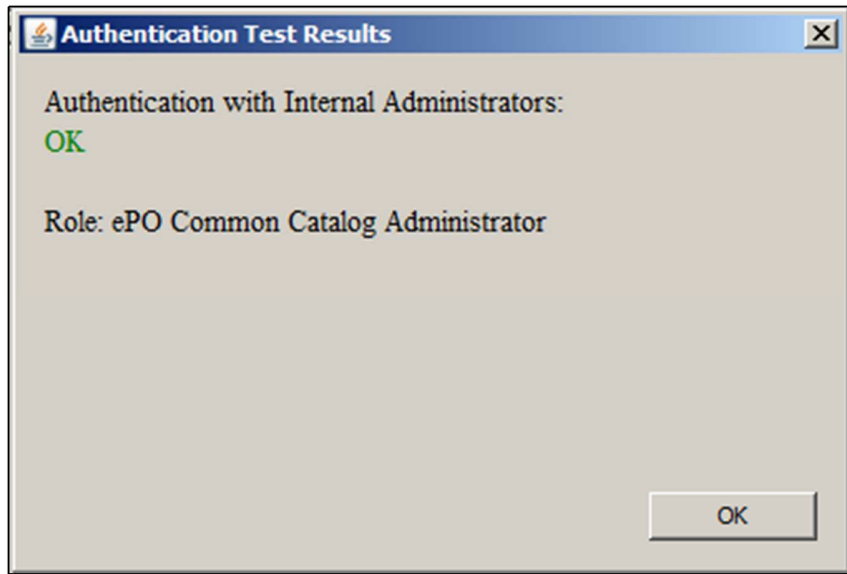


The screenshot shows a dialog box titled "Add Administrator". It has a blue header bar with a user icon and the title. Below the header, there are three main sections: "User name:" with a text box containing "epo"; "Password:" and "Password repeated:" with two masked text boxes containing "\*\*\*\*\*"; and "Role:" with a dropdown menu. The dropdown menu is open, showing three options: "ePO Common Catalog Administrator" (highlighted in blue), "ePO Common Catalog Administrator", and "Super Administrator". To the right of the dropdown menu are two buttons: "Edit..." with a pencil icon and "Add..." with a plus icon.

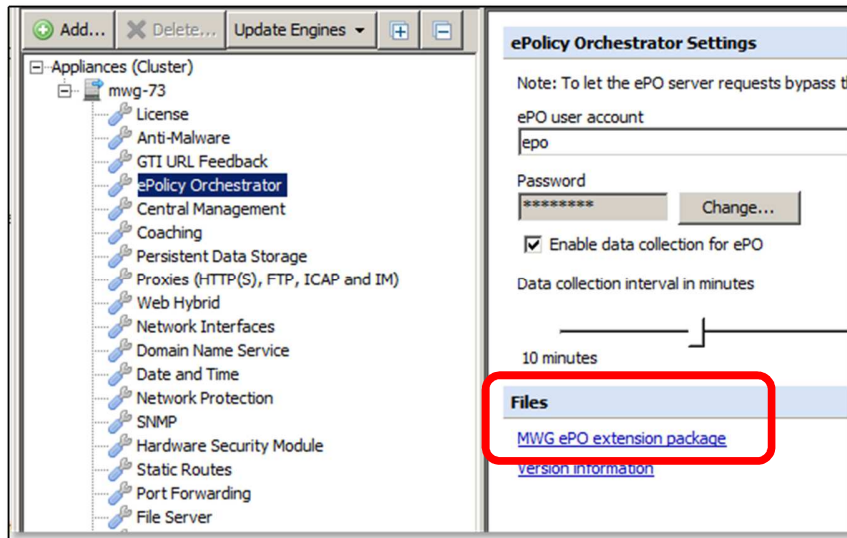
6. Test the new user to the right side of the "Roles" box



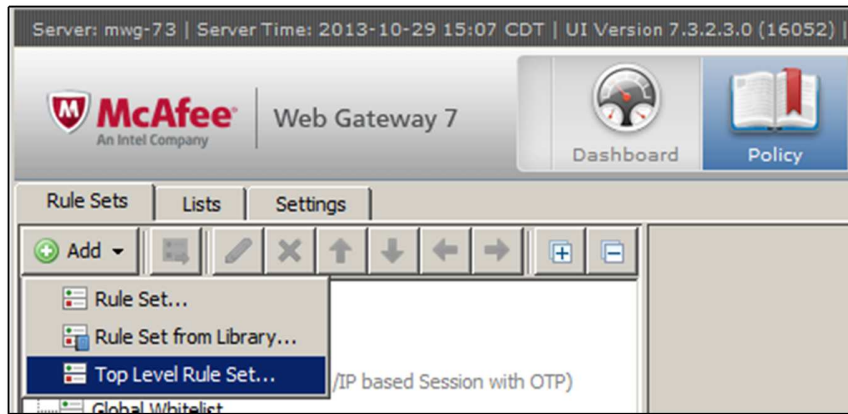
The screenshot shows a dialog box titled "Test with current settings". It has a grey header bar with the title. Below the header, there are two main sections: "User name:" with a text box containing "epo"; and "Password:" with a masked text box containing "\*\*\*\*\*". At the bottom right of the dialog box is a button labeled "Test..." with a user icon.



7. **Navigate** to “Configuration → ePolicy Orchestrator”
8. Next **Click** the “MWG ePO extension package” and save the zip file to disk

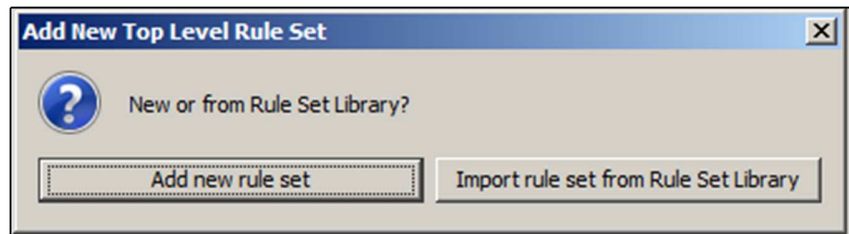


9. **Navigate** to “Policy → Rule Sets” tab
10. Now **Select** “Add → Top Level Rule set...”

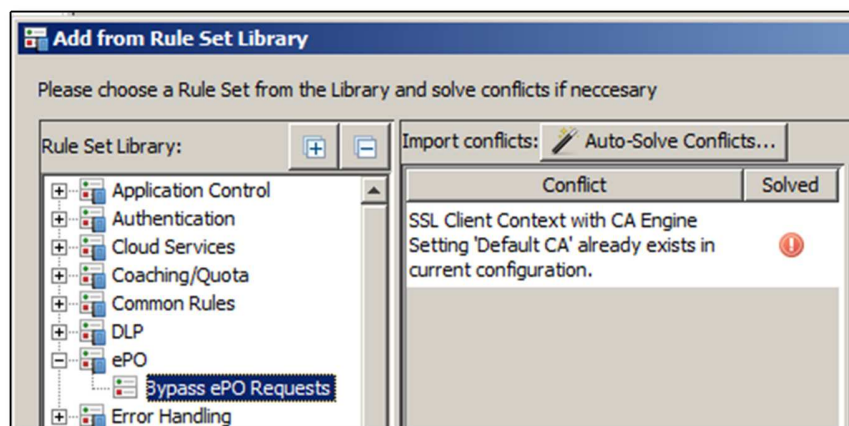




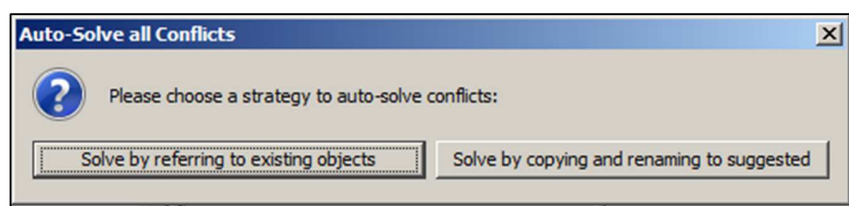
11. **Select** “Import rule set from Rule Set Library”



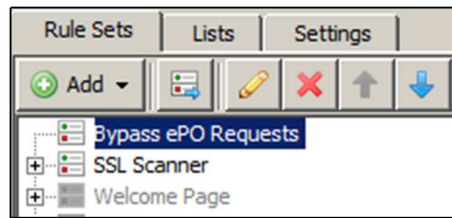
12. **Navigate** to “ePO → Bypass ePO Requests”



13. **Click** “auto-Solve Conflicts...” button and **Select** “Solve by referring to existing objects”

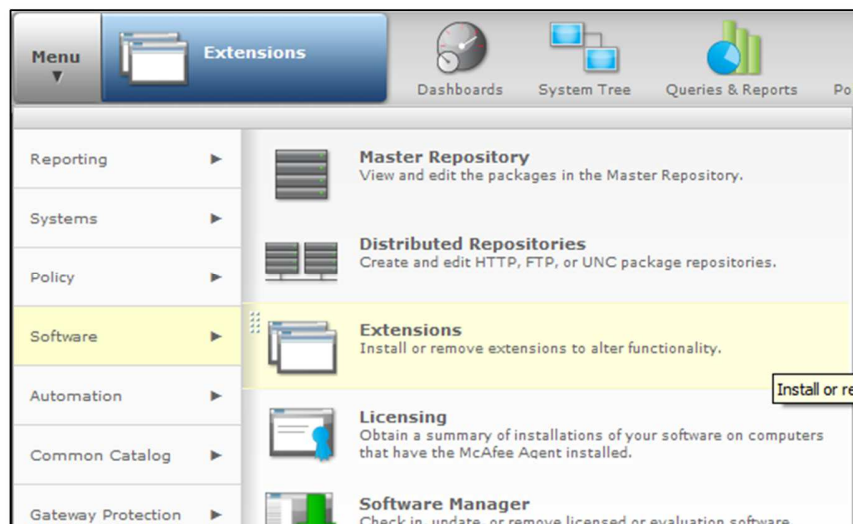


14. Move the new rule set to the top of the rule sets and **Click** the “Save Changes” button

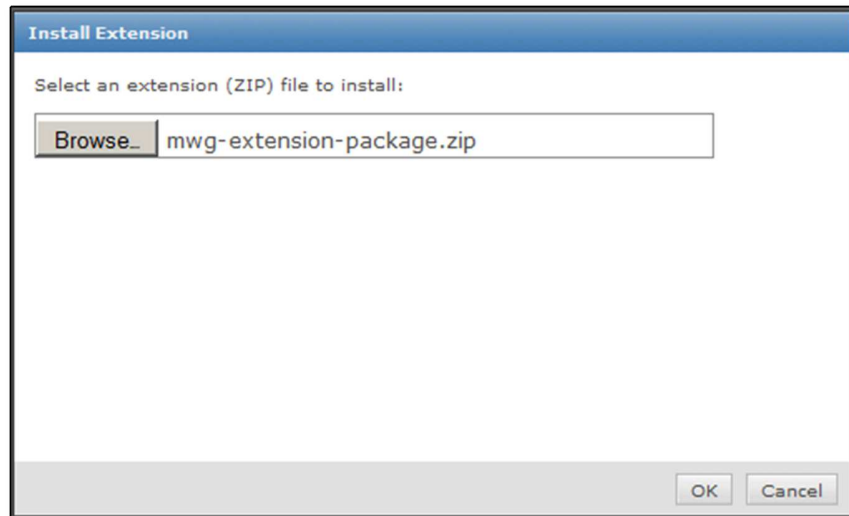


### Configuring ePO for Web Gateway

1. log in to ePO as an administrator
2. **Click** on the “Menu” dropdown and **Select** “Software → Extensions”

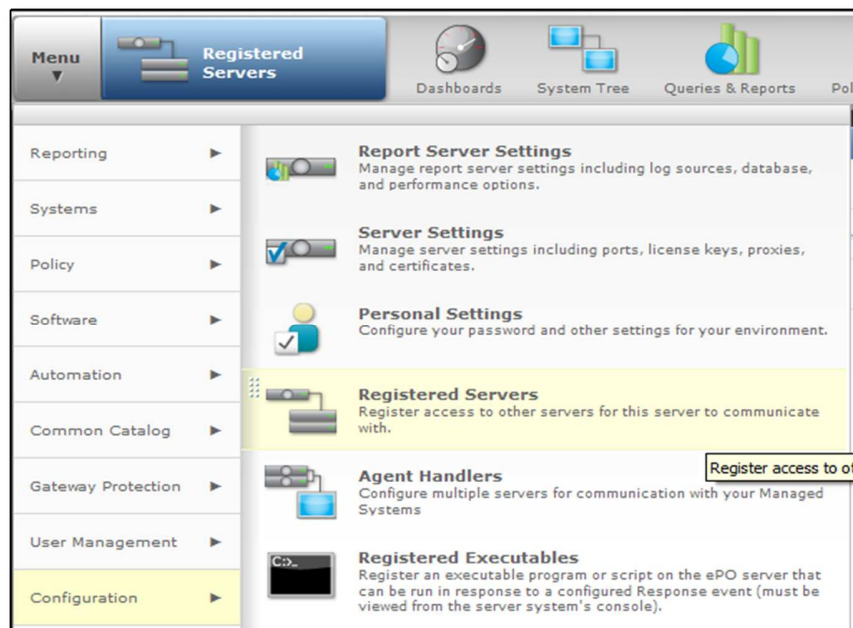


3. **Select** “Install Extensions” and browse to the extensions zip file you saved from the previous section.



4. This will install, or update, 7 extension
5. coreCatalog
6. EWG
7. mcc\_help
8. ewg\_help
9. mwg
10. catalogFramework
11. mwg\_help

12. **Browse** to "Menu → Configuration → Registered Servers"



13. Click on "New Server" and Select "McAfee Web Gateway 7" from the dropdown

Registered Server Builder	1 Description
Server type:	Database Server
Name:	Database Server Directory Services Connector Email and Web Security 5.x ePO LDAP Server McAfee Email Gateway 6.7.x McAfee Email Gateway 7.0 McAfee Web Gateway 6.x <b>McAfee Web Gateway 7</b> Report Server SNMP Server
Notes:	

14. Give your registered appliance a descriptive name

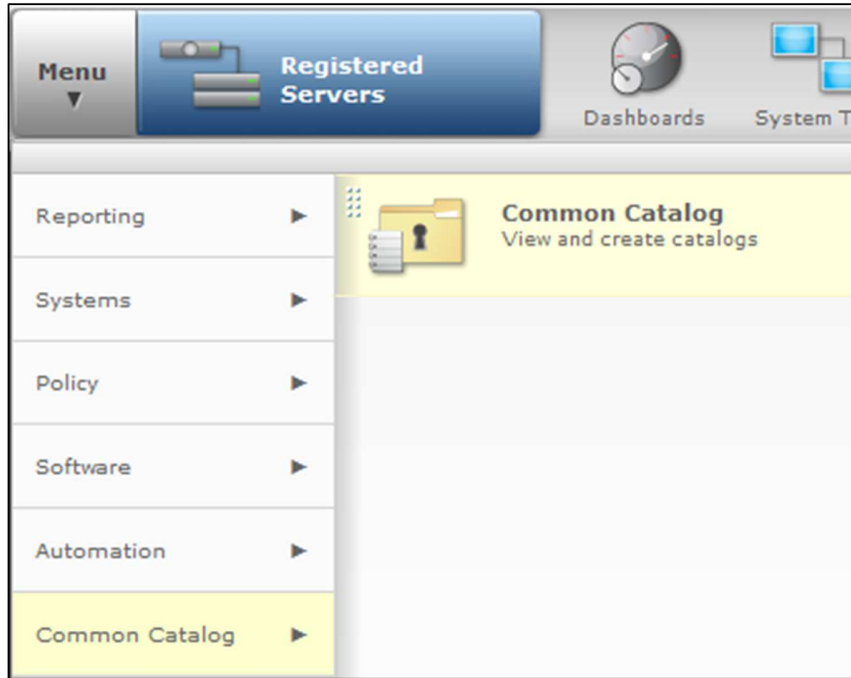
Registered Server Builder	1 Description
Server type:	McAfee Web Gateway 7
Name:	MWG 7.3.1
Notes:	

15. Click "Next" and fill in the MWG appliance information and Click "Save"

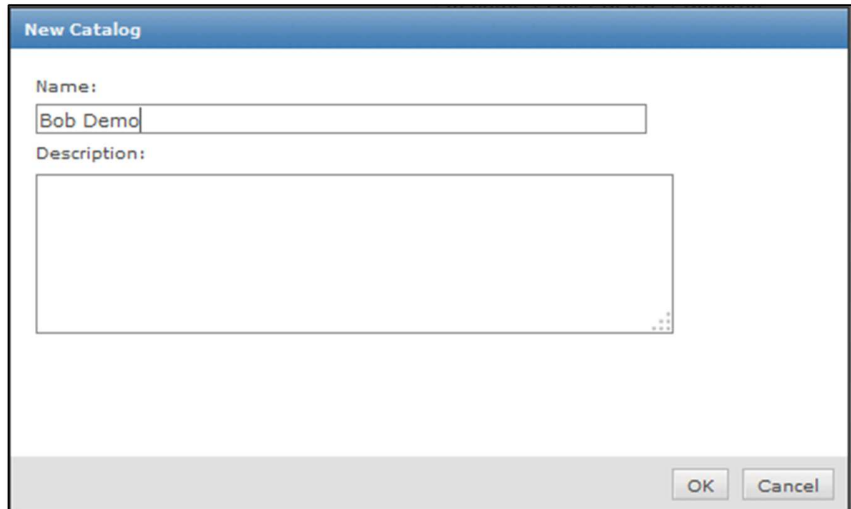
Registered Server Builder	<a href="#">1. Description</a>
Hostname	<input type="text" value="mwg-73"/>
Host address	<input type="text" value="192.168.157.18"/>
Administration Port	<input type="text" value="4712"/>
Statistics Retrieval Port	<input type="text" value="9090"/>
<input type="checkbox"/> Clear Credentials	
Console Credentials	For access to the host GUI
Username	<input type="text" value="admin"/>
Password	<input type="password" value="....."/>
Communication Credentials	For statistics retrieval and list management
Username	<input type="text" value="epo"/>
Password	<input type="password" value="....."/>
Test Connection	<input type="button" value="Test Connection"/>
Options	<input checked="" type="checkbox"/> Allow ePO to manage lists on this system

## Configuring Common Catalog

1. **Navigate** to “Menu → Common Catalog”



2. **Select** “Actions → New Catalog” and name your catalog



- We will now create a new catalog entry so that the list will sync with Web Gateway. **Click** “Edit” on the catalog you just created and **Click** on “Domain Name”

Name	Actions
Bob Catalog	<a href="#">Rename</a>   <a href="#">Edit</a>   <a href="#">Delete</a>   <a href="#">Duplicate</a>
Bob Demo	<a href="#">Rename</a>   <a href="#">Edit</a>   <a href="#">Delete</a>   <a href="#">Duplicate</a>
DemoMCP - MCP	<a href="#">Rename</a>   <a href="#">Edit</a>   <a href="#">Delete</a>   <a href="#">Duplicate</a>
McAfee Default	<a href="#">View</a>   <a href="#">Duplicate</a>
My Default - MCP	<a href="#">Rename</a>   <a href="#">Edit</a>   <a href="#">Delete</a>   <a href="#">Duplicate</a>

**Common Catalog**

Catalog: Bob Demo

Common Catalog	Domain Name																
<p>▼ Data</p> <p>String</p> <p>Pattern</p> <p>▼ Source / Destination</p> <p style="background-color: yellow;">Domain Name</p> <p>Network Address (IP)</p> <p>Network Port</p> <p>Process List</p>	<p><input type="checkbox"/> Show selected rows</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 50%;">Name</th> <th style="width: 50%;"></th> </tr> </thead> <tbody> <tr><td> </td><td> </td></tr> <tr><td> </td><td> </td></tr> <tr><td> </td><td> </td></tr> <tr><td> </td><td> </td></tr> <tr><td> </td><td> </td></tr> <tr><td> </td><td> </td></tr> <tr><td> </td><td> </td></tr> </tbody> </table>	Name															
Name																	

- Select** “Actions → New” and give your list a meaningful name and optional description

**Common Catalog > Domain Name > Edit**

Edit domain name:

<b>Name:</b>	<input style="width: 90%;" type="text" value="Global Domain Name Block"/>																
<b>Description:</b>	<input style="width: 90%;" type="text" value="Globally Block Domains"/>																
<b>Domain Name:</b>	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 50%;">Domain Name</th> <th style="width: 50%;"></th> </tr> </thead> <tbody> <tr><td> </td><td> </td></tr> <tr><td> </td><td> </td></tr> <tr><td> </td><td> </td></tr> <tr><td> </td><td> </td></tr> <tr><td> </td><td> </td></tr> <tr><td> </td><td> </td></tr> <tr><td> </td><td> </td></tr> </tbody> </table>	Domain Name															
Domain Name																	

5. At the bottom of the page **Type** in a domain entry, **Click** “add”, and then **Click** “Save

A screenshot of a web form titled "Domain Name". At the top, it says "0 items in 0 pages. Go to page: 1" with navigation arrows. Below this is a text input field containing "startribune.com" and an "Add" button to its right.

A screenshot of a web form titled "Common Catalog > Domain Name > Edit". It shows the "Edit domain name:" section with the following fields:  
Name: Global Domain Name Block  
Description: Globally Block Domains  
Domain Name: startribune.com  
Actions: Edit | Delete

6. Your list should now show up in the “Domain Name” section of your catalog

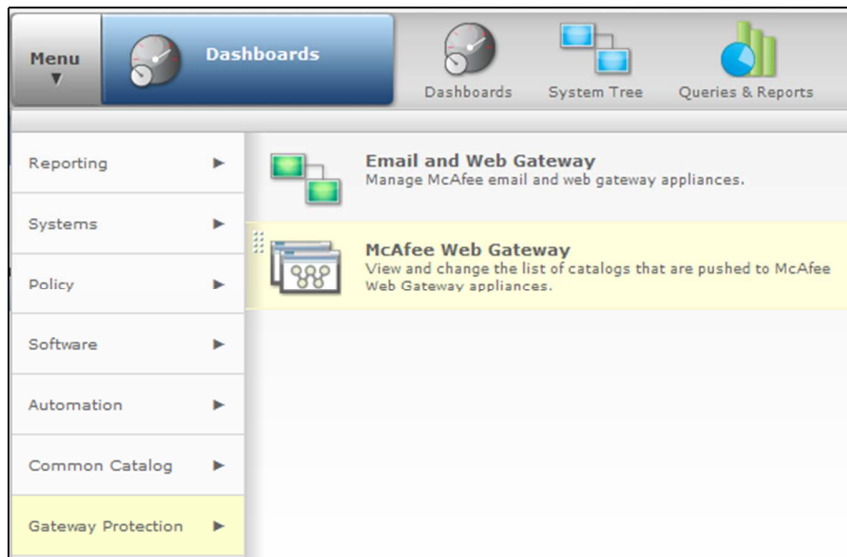
A screenshot of the "Common Catalog" interface. The "Catalog" dropdown is set to "Bob Demo". The left sidebar shows a tree view with "Domain Name" selected. The main content area shows a table with the following data:

Name
Global Domain Name Block

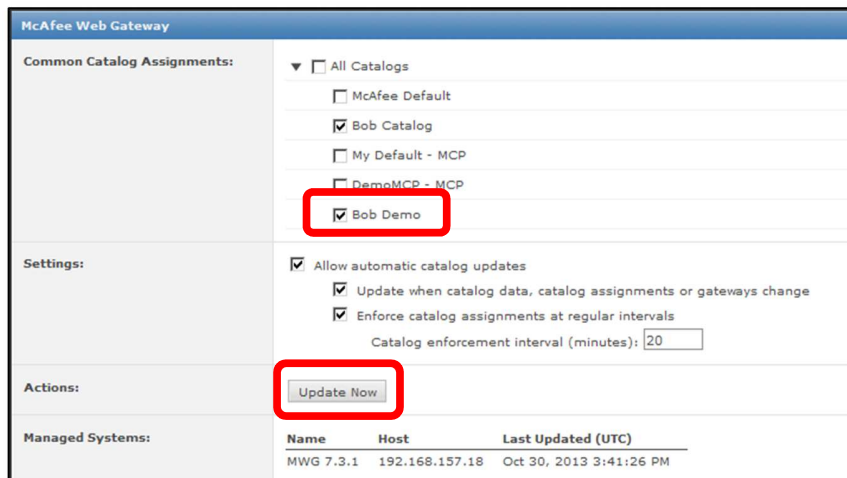
The "Global Domain Name Block" entry is highlighted with a red box.



7. **Navigate** to “Menu → Gateway Protection → McAfee Web Gateway”

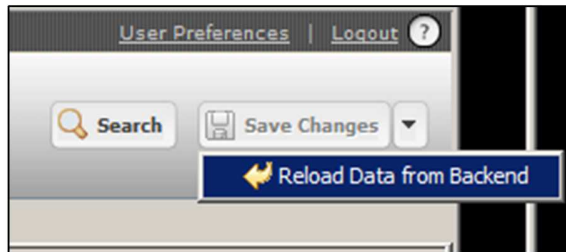


8. **Tic** the box next to your newly configured catalog and **Click** the “Update Now” button

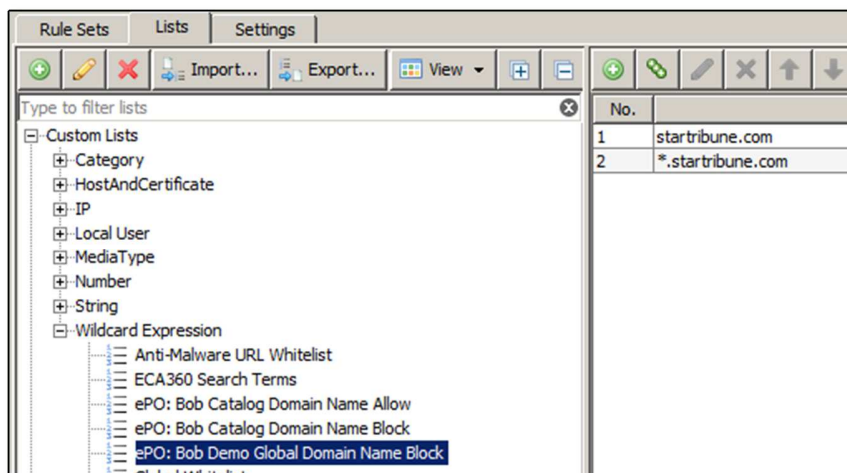


## Testing Common Catalog

1. Log in to the Web Gateway as an administrator
2. On the upper right section of the admin UI **Click** the down arrow next to “Save Changes” and **Click** “Reload Data From Backend”



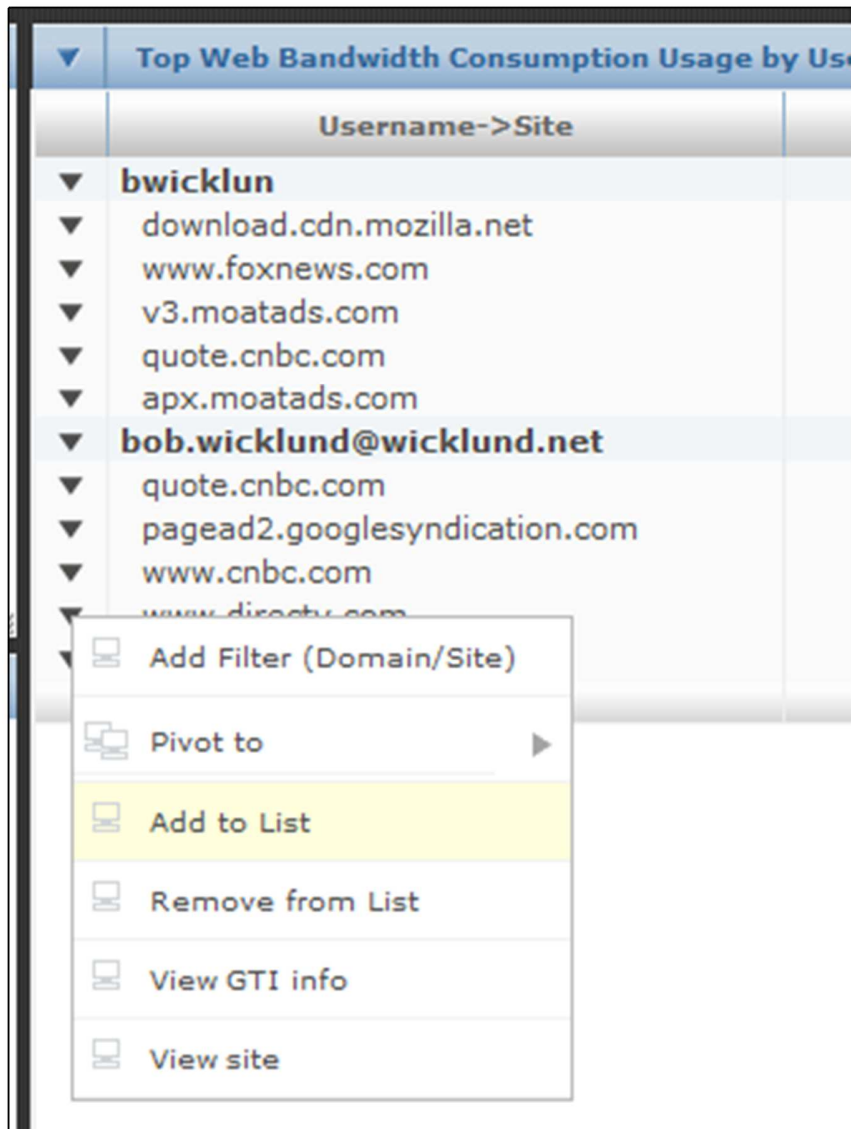
3. **Navigate** to “Policy → Lists → Wildcard Expressions” and verify that your new list and the domain name you added in the previous step show up



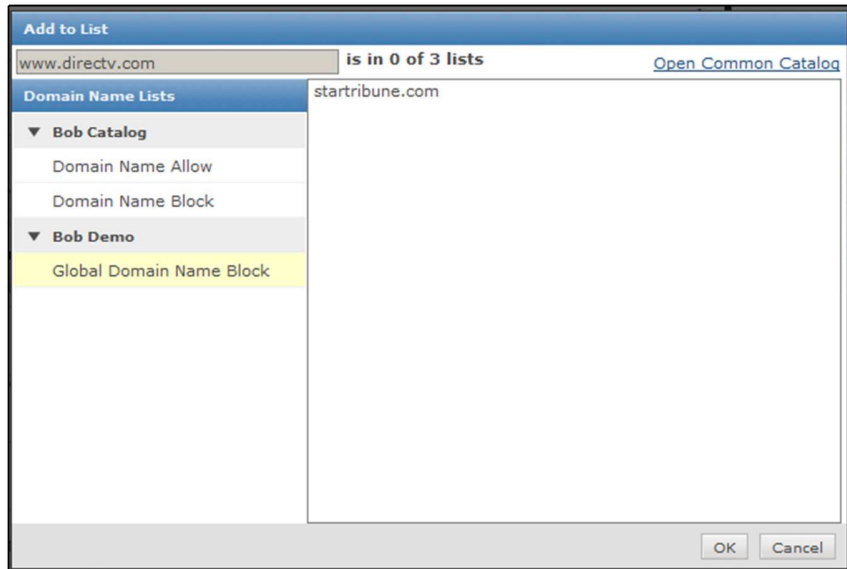
4. In ePO **Navigate** to “Dashboards → CSR: Web Activity” Look for a “Monitor” such as “Top Web Bandwidth Consumption by User and Site”

Username->Site	Sum of Bytes
<b>bwicklun</b>	<b>892.59 MB</b>
download.cdn.mozilla.net	663.55 MB
www.foxnews.com	63.03 MB
v3.moatads.com	56.12 MB
quote.cnbc.com	55.91 MB
apx.moatads.com	53.98 MB
<b>bob.wicklund@wicklund.net</b>	<b>126.48 MB</b>
quote.cnbc.com	51.54 MB
pagead2.googleadsyndication.com	24.03 MB
www.cbs.com	23.38 MB
www.directv.com	13.99 MB
kstp.com	13.54 MB
<b>Total</b>	<b>1019.08 MB</b>

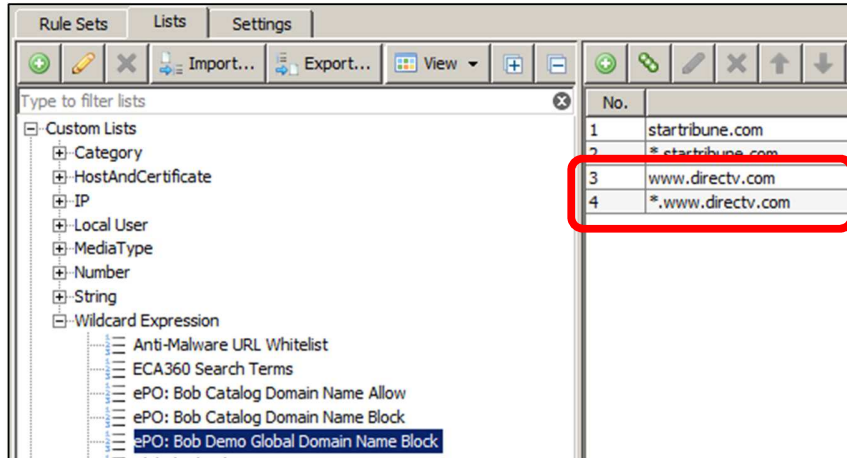
5. **Click** on the down arrow next to one of the domains listed and **Select** "Add to List"



- In the pop-up dialog **Select** the catalog and list you created in the previous steps and **Click “OK”**



- In the Web Gateway UI **Navigate** back to “Policy → Lists → Wildcard Expressions” and verify that your new list updated with the domain you just added



- This list can then, of course, be used in a Web Gateway rule



## Value Add

Using the integration of ePO, Web Gateway, and Content Security Reporter allows an admin to get instant analysis of their web traffic and web security posture. They can pivot in on high level dashboards to get more detail. They can click to actually go to the web site or get McAfee GTI detail on the site. They also would have the ability to take an immediate allow, or block, action on a person, URL, or category, right from the reporting dashboard.