McAfee Security Connected Integrating ePO and MWG

W McAfee

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

#### **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 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: <u>https://contentsecurity.mcafee.com/software\_mwg7\_download</u>.

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

This also requires McAfee Content Security Reporter version 2.0 and higher. CSR may be downloaded here: <u>https://contentsecurity.mcafee.com/product\_csr</u>.

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 <u>https://contentsecurity.mcafee.com/</u> 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"

🥵 Edit Role		×
Name:		
ePO Common Catalog Administr	ator	
Dashboard accessible		
Policy - Rules accessible	Top Level Move & Create	
▼ Policy - Lists accessible	☑ List creation	
Policy - Settings accessible	Settings creation	
Configuration accessible		
Accounts accessible		
Troubleshooting accessible		
Permissions accessible		
Read Only Admin		
REST-Interface accessible		
	OK Cancel	

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 prvious step
    f. Click "OK"

🤱 Add Administrator	×
User name: epo	
Password: *******	Password repeated:
Role:	
ePO Common Catalog Administrator	💌 🥜 Edit 💿 Add
ePO Common Catalog Administrator Super Administrator	

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

Test with current settings		
User name:		
еро		
Password:		
*******		
🧏 Test		



- 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  $\rightarrow$  Rule Sets" tab
- 10. Now **Select** "Add → Top Level Rule set..."

Server: mwg-73   Server Time: 2013-10-29 15:07 CDT	UI Version 7.3	.2.3.0 (16052)
Web Gateway 7	Dashboard	Policy
Rule Sets Lists Settings		
③ Add - 🗒 🖉 🗙 🛧 🕂 ← →	<b>€ </b>	
E Rule Set		
🔚 Rule Set from Library		
Top Level Rule Set /IP based Session with O	TP)	
Global Whitelist		

11. Select "Import rule set from Rule Set Library"



12. Navigate to "ePO → Bypass ePO Requests"

8	🛱 Add from Rule Set Library			
ł	Please choose a Rule Set from the Library and solve conflicts if neccesary			
	Rule Set Library:	Ð E	Import conflicts: 🖉 Auto-Solve Conflict	s
	Application Control	-	Conflict	Solved
	Authentication     Cloud Services     Coaching/Quota		SSL Client Context with CA Engine Setting 'Default CA' already exists in current configuration.	0
	Common Rules  Common Rules  DLP  Common PO  PO  PO  PO  PO  PO  PO  PO  PO  PO	10		
	Error Handling			

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

Rule Sets	Lis	Lists Set		ettings	
🕢 Add 👻	-	Ø	×	1	+
Bypass ePO Requests SSL Scanner Welcome Page					

## Configuring ePO for Web Gateway

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

Menu T	Extensions	Dashboards System Tree Queries & Reports Po
Reporting	•	Master Repository View and edit the packages in the Master Repository.
Systems		Distributed Repositories Create and edit HTTP, FTP, or UNC package repositories.
Software	• <b>•</b>	Extensions Install or remove extensions to alter functionality.
Automation		Install or re
Common Catalog	•	Obtain a summary of installations of your software on computers that have the McAfee Agent installed.
Gateway Protection		Software Manager Check in. update, or remove licensed or evaluation software.

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

Install Extension	an dean dean dean
Select an extension (ZIP) file to install:           Browse_         mwg-extension-package.zip	]
0	K Cancel

- 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  $\rightarrow$  Configuration  $\rightarrow$  Registered Servers"

Menu P	Reg Serv	istered vers	Dashboards System Tree Queries & Reports Pol
Reporting	۲		Report Server Settings Manage report server settings including log sources, database, and nefrenance orbitation
Systems			and performance options.
			Server Settings
Policy	۲		Manage server settings including ports, license keys, proxies, and certificates.
Software	F		Personal Settings Configure your password and other settings for your environment.
Automation	•	Pagistarad Samars	
Common Catalog	►		Register access to other servers for this server to communicate with.
Gateway Protection	•	2	Agent Handlers Configure multiple servers for communication with your Managed Systems
User Management	۲	C:>]	Registered Executables
Configuration	۲		Register an executable program or script on the ePO server that can be run in response to a configured Response event (must be viewed from the server system's console).

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

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

14. Give your registered appliance a descriptive name

Menu V Registered Servers	Dashboards System Tree Q
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	1 Description
Hostname	mwg-73
Host address	192.168.157.18
Administration Port	4712
Statistics Retrieval Port	0000
Clear Credentials	
Console Credentials	For access to the host GUI
Username	admin
Password	•••••
Communication Credentials	For statistics retrieval and list management
Username	еро
Password	•••••
Test Connection	Test Connection
Options	☑ Allow ePO to manage lists on this system

# **Configuring Common Catalog**

- Registered Menu Servers V Dashboards System 7 Common Catalog View and create catalogs Reporting ► t Systems . Policy ► Software . Automation ► Common Catalog ►
- 1. Navigate to "Menu → Common Catalog"

2. Select "Actions  $\rightarrow$  New Catalog" and name your catalog

New Catalog	
Name: Bob Demo Description:	
	OK Cancel

3. 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"

Γ	Name 🔺	Actions
П	Bob Catalog	Rename   Edit   Delete   Duplicate
Π	Bob Demo	<u>Rename</u>   <u>Edit</u>   <u>Delete</u>   <u>Duplicate</u>
Γ	DemoMCP - MCP	Rename   Edit   Delete   Duplicate
Π	McAfee Default	View   Duplicate
	My Default - MCP	Rename   Edit   Delete   Duplicate

Common Catalog					
Catalog: Bob Demo					
Common Catalog Domain Name					
▼ Data					
String	Show selected rows				
Pattern	Г	Name			
<ul> <li>Source / Destination</li> </ul>	Source / Destination				
Domain Name					
Network Address (IP)					
Network Port					
Process List					

4. Select "Actions  $\rightarrow$  New" and give your list a meaningful name and optional description

Common Catalog > Domain Name > Edit				
Edit domain name:				
Name:	Global Domain Name Block			
Description:	Globally Block Domains			
Domain Name:	Domain Name			

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

	0 items in 0	) pages. Go	to page:	1	144 4
Domain Name					
startribune.com					Add
Common Catalog > Domain Nan	e > Edit				
Edit domain name:					
Name:	Global Domain Name Block				
Description:	Globally Block Domains				
Domain Name:	Domain Name				Actions
	startribune.com				Edit   Delete

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

Common Catalog	
Catalog: Bob Demo	
Common Catalog	Domain Name
▼ Data	
String	Show selected rows
Pattern	Name
▼ Source / Destination	Global Domain Name Block
Domain Name	
Network Address (IP)	

7. **Navigate** to "Menu  $\rightarrow$  Gateway Protection  $\rightarrow$  McAfee Web Gateway"



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

McAfee Web Gateway					
Common Catalog Assignments:	▼ ☐ All Ca	atalogs			
	McAfee Default				
	Bo	ob Catalog			
	M	y Default - MCP			
		emoMCP - MCP			
	Re Bo	ob Demo			
6-Wi	-				
Settings:	Allow automatic catalog updates				
	Update when catalog data, catalog assignments or gateways change				
		Catalog enforceme	ent interval (minutes): 20		
Actions:	Update No	w.			
Managed Systems:	Name	Host	Last Updated (UTC)		
	MWG 7.3.1	192.168.157.18	Oct 30, 2013 3:41:26 PM		

### **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



 In ePO Navigate to "Dashboards → CSR: Web Activity" Look for a "Monitor" such as "Top Web Bandwidth Consumption by User and Site"

-	Top Web Bandwidth Consumption Usage by User and Site				
-	Username->Site	Sum of Bytes			
Ŧ	bwicklun	892.59 MB			
-	download.cdn.mozilla.net	663.55 MB			
<b>–</b>	www.foxnews.com	63.03 MB			
<b>•</b>	v3.moatads.com	56.12 MB			
<b>•</b>	quote.cnbc.com	55.91 MB			
-	apx.moatads.com	53.98 MB			
-	bob.wicklund@wicklund.net	126.48 MB			
-	quote.cnbc.com	51.54 MB			
-	pagead2.googlesyndication.com	24.03 MB			
<u> </u>	www.cobc.com	23.38 MB			
-	www.directv.com	13.99 MB			
<b>_</b>	kstp.com	13.54 MB			
_	Total	1019.08 MB			

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

V	Top Web Bandwidth Consu	ımp	otion Us	age by	/ Us	
	Username->S	Username->Site				
v	bwicklun					
•	download.cdn.mozilla.net					
•	www.foxnews.com					
•	v3.moatads.com					
•	quote.cnbc.com					
	apx.moatads.com					
	bob.wicklund@wicklund	.ne	et			
	quote.cnbc.com					
Ľ	pagead2.googlesyndicatio	on.o	com			
Ľ	www.cnbc.com					
	Add Filter (Domain/Site)					
-	Pivot to	Þ				
	Add to List					
	Remove from List					
	View GTI info					
	View site					
- <sup>-</sup>						

6. In the pop-up dialog **Select** the catalog and list you created in the previous steps and **Click** "OK"

Add to List		
www.directv.com	is in 0 of 3 lists	Open Common Catalog
Domain Name Lists	startribune.com	
▼ Bob Catalog		
Domain Name Allow		
Domain Name Block		
▼ Bob Demo		
Global Domain Name Block		
		OK Cancel

7. 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

Rule Sets Lists Settings		
💿 🥜 🗶 🛼 Import 🗍 Export 🔃 View 👻 📻	٢	⊗ 🖉 × 🕇 ∔
Type to filter lists	No.	
⊡Custom Lists	1	startribune.com
	2	* startribune.com
⊕ HostAndCertificate	3	www.directv.com
€	4	*.www.directv.com
i ⊡Local User		
i → Number		
String		
-Wildcard Expression		
ECA360 Search Terms		
= ePO: Bob Catalog Domain Name Allow		
ePO: Bob Demo Global Domain Name Block		

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

🔾 Add Rule 🖉 Edit 🗶 Delete 😭 Move up 🕹 Move down 📄 Copy 🔀 Paste Show details		
Enabled	Name/Criteria	Action
<b>v</b>	Allow URLs That Match in <u>URL WhiteList</u> <sup>▲</sup> URL matches in list <u>URL WhiteList</u> <sup>▲</sup>	E Stop Rule Set
	Block URLs That Match in <u>ePO: Bob Catalog Domain Name Block</u> URL.Host matches in list <u>ePO: Bob Catalog Domain Name Block</u>	Block < <u>URL Blocked</u> >

## 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.