



GX integration with McAfee Web Gateway Application Note



Table of Contents

1	Intro	oduction	3
	1.1	Scope	3
	1.2	Background	3
	1.3	Audience	3
	1.4	Conventions	4
	1.5	Purpose	4
2	Pre-	-requisites	5
3	Inte	egration Steps	6
	3.1	Initial Configuration of ICAP	6
	3.2	Configure the new Reqmod	7
	3.3	Configure the new Respmod	9
	3.4	Configure ICAP Media Type Rule Set	. 10
4	Enh	nanced configuration	. 12
	4.1	Configure McAfee Web Gateway to convert HTTP/2.0 Requests to HTTP/1.1 (Only for G)	X
	1.6.0 c	or Older)	. 12
	4.2	Configurating McAfee WGW ICAP to fail open	. 12
	4.3	Configure McAfee Web Gateway to implement GX profile switching based on Active	45
	Directo	ory User Group:	. 15
	4.3.	.1 Enabling GX User Profile Support	. 15
_	4.3.	.2 Configure the McAfee WGW to use the ICAP headers	. 16
5	Irou	ubleshooting	. 20
	5.1	Missing Images on Websites	. 20
	5.1.	.1 McAfee Web Gateway Timeout	. 20
	5.2	Formatting on webpages ruined and content missing	. 22
6	Sup	ported Data Types	. 27
7	Refe	erences	. 28
8	Арр	pendix A	. 29
	8.1	ICAP Error IDs	. 29



1 Introduction

1.1 Scope

This document outlines how to integrate a McAfee Web Gateway with Deep Secure's Gateway extension (GX) appliance. We have tested against the McAfee Web Gateway (MWG) version 8.2.4 and previous version of the MWG also. GX provides a bi-directional guarding capability for ICAP, as discussed in the *GX Configuration Guide*.

This document details the configuration steps needed for the McAfee Web Gateway to send data to, and receive data from, GX.

1.2 Background

A typical deployment is as shown below.



Figure 1-1: GX and McAfee deployment

1.3 Audience

This guide is for Deep Secure GX system administrators, who are assumed to have a full understanding of network topology and routing.



1.4 Conventions

This guide uses the conventions shown in Table 1-1:

Convention	Indicates					
Emphasis	Terms in a definition list or emphasis for important introductory words in a					
	paragraph.					
Options	Menu names, options, buttons, keys and other items from the user interface or the					
	keyboard.					
Italics	Cross-reference to related information in another document.					
<variable></variable>	A value you must supply, for example in a command line.					
[<variable>]</variable>	An optional value you can supply, for example, in a command line.					
😨 Imp app	ortant information that emphasises or supplements points in the text, or that may ly only in special cases.					
🔺 A ca the	aution that alerts you that failure to take or avoid a specified action could result in loss of data.					
^{Tip} A h	tip that suggests an alternative method for applying a technique or procedure or elps you to understand the benefits and capability of the product.					

Table 1-1: Conventions in this document

1.5 Purpose

This guide takes you through the steps you need to follow to integrate MWG with a GX appliance.

Network traffic should flow, as expected, after performing the steps in this guide. If not, the fault-finding guidance towards the end of this document should be followed.



2 Pre-requisites

Before configuring McAfee to work with Deep Secure Gateway eXtension there are a number of prerequisites that should be set.

Ensure MWG is installed and the Management interface is reachable.

Ensure the MWG has been configured with, as a minimum, 2 IP addresses that represent:

- a Management interface;
- a Data interface

Ensure the Deep Secure GX has been setup as documented in the GX Configuration Guide.

Ensure the Deep Secure GX Data network is configured to be in the same IP range as that on the internal interface on the MWG.

This guide has been written with a fresh installation of McAfee Web Gateway. If this guide is being used to integrate the Deep Secure GX Appliance into an already configured McAfee Web Gateway, the guidance in this document may not work and you may need to speak to a McAfee technical advisor to resolve.



3 Integration Steps

3.1 Initial Configuration of ICAP

The following steps detail how to configure the MWG to receive data and send data to the GX via ICAP.

A For the purpose of the following configuration steps, it is assumed that the MWG is already configured correctly to perform its proxy role. If not, please refer to the appropriate MWG configuration documentation to complete these steps.

Connect to the McAfee Web Management page and configure the media types that will be sent to the GX. To do this, navigate to Policy -> Lists -> Media Type and right click choosing Add.

Give the new Media Type an appropriate name, for example GXMediaTypes. Once the new MediaType Rule has been created right click and select Edit. Select the different content types from the list of available content types you wish to send to the GX.

🥜 🗙	L □ Append from file	Type to filter content
No.	MediaType	Comment
1	application/pdf	Adobe PDF document
2	image/jpeg	Graphic file in JPEG format
3	image/png	Graphic file in PNG format

Figure 3.2 Example list of Data types

Next create a new Rule Set within the Media Type Filtering Rule Set for the ICAP Clients. Right click on the Policy -> Rule Set -> Media Type Filtering -> Add -> Rule Sets from Library.

^{Tip} You may need to unlock this feature before the previous set can be performed.







The Choose the appropriate heading in the Rule set list to determine where the ICAP client will be created. In the example below the Media Type Filtering heading was selected before creating the ICAP Client.

Once the Rule Set Library is opened expand the ICAP Client heading and select ICAP Client and click OK.

tel Security Vieb Gateway	Dashboard Dolor Configuration	Accepted Tread-Instance		Search H Save Changes *
Sets Lists Settings Templates				
I I	√ 55% ∑ theble throbin Coult Apples to:	Comerse Related data rate case ¹¹ AND Concersor Provided Concersor ≥ The definition Concersor case - Mono (more) (III) Concer III) Prove datale		
Googe inneses Exploit Proxy Authentication and Authorization Common Rules URL Filtering	Brabled Name/Criteria		Action	Events
Neda Type Filering S Uplad Neda Type Download Media Types SUBJECT		lig Add from Rule Set Ubory		
		Laststaber The sheet for the proving the fack bit. Measure possible larger Caststaber The sheet for the proving the fack bit. Measure possible larger Caststaber The sheet for the proving the fack bit. Measure possible larger Caststaber The sheet for the proving the fack bit. Measure possible larger Caststaber The sheet for the proving the fack bit. Measure possible larger Caststaber The sheet for the proving the fack bit. Measure possible larger Caststaber The sheet for the proving the fack bit. Measure possible larger Caststaber The sheet for the proving the fack bit. Measure possible larger Caststaber The sheet for the proving the fack bit. Measure possible larger Caststaber The sheet for the proving the fack bit. Measure possible larger Caststaber The sheet for the proving the fack bit. Measure possible larger Caststaber The sheet for the proving the fack bit. Measure possible larger Caststaber The sheet for the proving the fack bit. Measure possible larger Caststaber The sheet for the proving the fack bit. Measure possible larger Caststaber The sheet for the proving the fack bit. Measure possible larger Caststaber The sheet for the proving the sheet for the proving the sheet for the provi		
Rule Sets Log Handler Dror Handler Line Turford Ensection				

Figure 3.5 Example of ICAP Client Rule Set Library

Once the ICAP Client has been added select the setting and Click Unlock View.

3.2 Configure the new Reqmod

To configure the newly created ReqMod navigate to Policy -> Lists -> ICAP Servers -> Reqmod Server and right click on the predefined URI and select Edit.

In the URI field add a URI matching the example below:

icap://DATA IP of GX:1344/reqmod



Server moggpt Server Timel 2018-10-22 16:10 UTC UI	Nersen 7.6.2.14.9 (22746) User afens Esle: Separ Admins			Une Privercos Labout 🖓
Rule Sets Lists Settings Templates				
🗿 🥒 🗶 🚑 Import 🌲 Export 📰 Vew 🔹 🕀 📻	🔘 🥔 🗙 🕆 🌲 🔔 Append from file			Type to filter content
Type to filter lists	No. LRI (Format: ican[s]://P:port/imethod])	Respect max concurrent connection limit	Comment	
El: Custon Litis Chegory Bookist — Cohegory Bookist — Cohegory Bookist — Cohegory Bookist for Special Group — HeatAndCertificate — — — — — — — — — — — — — — — — — — —	1 cap://b.8.6.0.1344tegrod	71.0°		
Advance Candon Advance		Edit (CAP Server X IEE Fromat: couple//Prest/prefixed/ icou//72.21.30.4(1)44/errord X Image: Trans. soncarrent convection list. X		
How the structure of the control of the structure of		Comment:		

Figure 3.6 Example ICAP Server Configuration

Finally configure the ReqMod Rule set. To do this for the ReqMod, navigate to Policy -> Rule
Set -> Media Type Filtering -> ICAP Client -> ReqMod and right click selecting
Add Rule.

- Name Choose a meaningful name
- Rule Criteria Click the Add button and select Advanced Criteria. Select the following
 properties for the Advanced Criteria: Selected Property ICAP.ReqMod.Satisfaction
 and set Settings to ReqMod, Selected Operator equals, Compare with Value –
 Boolean, True.



Selected Property:		Selected Operator:	Compare w	with Value - Boolean V	
ICAP.ReqMod.Satisfaction <reqmod></reqmod>		equals	true		
Filter: <none> -</none>					
Type to filter properties	0				
ICAP.ReqMod.Satisfaction	^	does not equal	false		_
Will be true if ICAP server responds to a reqmod request with		equals	true		
a response header.					
ICAP.RespMod.EncapsulatedHTTPChanged					
will be true if ICAP server changes the HTTP state of the response.					
ICAP RespMod Response Header Exists (String)					
Will be true if RespMod server response contains a specified					
header.					
ICAP.RespMod.ResponseHeader.ExistsMatching()					
Will be true if RespMod server response contains header with					
given name, which matches the wildcard expression.					
List.OfApplicationControl.Exists(String)					
Returns true if list with given name exists.					
List.OfApplicationControl.IsEmpty(List of n Name)					
Returns true if list is empty					
List.OfCategory.Exists(String)					
Returns true if list with given name exists.					
List.OfCategory.IsEmpty(List of Category)	¥				
Add 'Boolean' User Defined Property					

Figure 3.9 Example ReqMod Rule Criteria

- Action Continue
- Events Leave Blank

3.3 Configure the new Respmod

To configure the newly created ReqMod navigate to Policy -> Lists -> ICAP Servers -> Respmod Server and right click on the predefined URI and select Edit.

In the URI field, add a URI matching the example below:

icap://DATA IP of GX:1344/respmod

Finally configure the RespMod Rule set. To do this for the RespMod navigate to Policy -> Rule Set -> Media Type Filtering -> ICAP Client -> RespMod and right click selecting **Add Rule**.

- Name Choose a meaningful name
- Rule Criteria Click the Add button and select Advanced Criteria. Select the following properties for the Advanced Criteria, Property ICAP.RespMod.EncapsulatedHTTPChanged and set Settings to RespMod / Operator equals / Compare with Value – Boolean True.



🔰 Edit Criteria					×
Selected Property: ICAP.RespMod.EncapsulatedHTTPChanged <reqmod></reqmod>	Selected Operator:	Compare with true	Value - Boolean	~	
Filter: <none> - Type to filter properties</none>]				
ICAP.RespMod.EncapsulatedHTTPChanged Will be true if ICAP server changes the HTTP state of the response. Extinos: RespMod v ICAP.RespMod.ResponseHeader.Exists(String)	does not equal equals	false true			
Will be true if RespMod server response contains a specified header. ICAP.RespMod.ResponseHeader.ExistsMatching() Will be true if RespMod server response contains header with					
given name, which matches the wildcard expression. List.OfApplicationControl.Exists(String) Returns true if list with given name exists.					
List.OfApplicationControl.IsEmpty(List of n Name) Returns true if list is empty					
List.OfCategory.Exists(String) Returns true if list with given name exists.					
Returns true if list is empty					
Returns true if list with given name exists.]				
]		0	ОК	Cancel

Figure 3.10 Example RespMod Rule Criteria

- Action Continue
- Events Leave Blank

3.4 Configure ICAP Media Type Rule Set

The final stage of McAfee configuration is to configure an ICAP Client Rule Set. To do this navigate to Policy -> Rule Set -> Media Type Filtering -> ICAP Client and right click selecting Add Rule.

- Name Choose a meaningful name
- Rule Criteria Click the Add button and select Media Type Criteria. Select the following
 properties for the Media Type Criteria: Selected Property MediaType.EnsureTypes;
 Selected Operator none in list; Compare with GX FileTypes (MediaType).



DEEP SECURE

Figure 3.8 Example Rule Criteria

- Action Stop Rule Set
- Events Leave Blank



4 Enhanced configuration

- 4.1 Configure McAfee Web Gateway to convert HTTP/2.0 Requests to HTTP/1.1 (Only for GX 1.6.0 or Older)
 - A To ensure correct operation, GX 1.6.0 or older requires MWG to be configured to support HTTP/1.1.

In order to do this, you must add a new rule to the 'rule set' to the common rules within the policy tab on the Web Gateway Appliance. Please choose an appropriate name, set 'rule criteria' to always, and ensure that 'action' is set to 'stop rule set'. Please also ensure that the 'events' section is set to modify the variables 'Set Response.ProtocolAndVersion' and 'Set Request.ProtocolAndVersion' is using the strings 'HTTP/1.1' as below.

1. Name	Events:
	🔘 Add 👻 🥜 Edit 💢 Delete 🕆 Move up 🕹 Move down
2. Rule Criteria	Set Response.ProtocolAndVersion = "HTTP/1.1"
3. Action	Set Request.ProtocolAndVersion = "HTTP/1.1"
4. Events	
5 Summon	
5. Summary	

Figure 3.1 Configure MWG to convert HTTP/2.0 Requests to HTTP/1.1

4.2 Configurating McAfee WGW ICAP to fail open

The following steps will detail how the McAfee WGW can be configured to fail open when an ICAP error is displayed. A reason for doing this might be to improve the user experience as it will ensure minimal disruption to the web traffic if an ICAP service becomes unavailable.

With this rule enabled it will mean content downloaded while the ICAP service is unavailable will be downloaded without transformation bypassing the Deep Secure security.

To create the rule:

• Log into the McAfee WGW GUI and navigate to Policy → Error Handler → Block on All Errors



Security Veb Gateway	Dashbo	ard Policy Configuration Accounts Troubleshooting		Search Save Changes
ule Sets Lists Settings Templates	2 Edit			
Default	Rules in 'Blo	k on Al Errors': e ∕ Edit X Delet ↑ Move up ↓ Move down Copy Paste Show det	tais	
Long Running Connections (Based on Volume)	Enabled	Name/Criteria	Action	Events
		Ignore Mail Bomb Warning	Nop Rule Set	
Block on Anti-Malware Engine Errors		Send Email on Internal Errors	Stop Rule Set	1 Event
Block on URL Hiter Errors DLP Filter Errors		Always Block	Block	
Rule Sets				
Rule Sets Cog Handler Error Handler				

Figure 4.1 Rule Location

- Click the Add rule button and create a new rule with the following set:
 - a. Name Relevant name
 - b. Rule Criteria Add \rightarrow Advanced Criteria \rightarrow Filter on Error.ID, Selected Operator equals and Compare with ICAP error ID 16000

Selected Property: Selected Operator: Compare with Value - Number Error.ID equals 16000 Filter: <none> error.id</none>	
Error.ID equals 16000 Filter: <none> • •</none>	4.2 Rule
Filter: <none></none>	Critoria
error.id	Citteria
error.id	example
Recommended does not equal 16000	
equals equals	
greater than a same	
greater than or equais	
less than	
less than or equals	
& Add 'Number' User Defined Property	
OK Cancel	



c. Repeat step b until all ICAP errors you wish to fail open on have been added to the list. You may wish to only add certain error codes to the fail open list, see the ICAP error ID table in section 4.2. Once complete it will look like this:

Steps	Appr	r this rule: (Aiways	critoria is matched		
. Name	Crite	ria:		3 Add - Z Edit X Di	elete 🕇 Move up 👢 Mo	ove down
. Rule Criteria	ID	AND/OR	Property	Operator	Operand	
. Action	a		Error.ID	equals	16000	
	b	OR 🔍	Error.ID	equals	16001	
. Events	с	OR 🔍	Error.ID	equals	16002	
	d	OR 🔍	Error.ID	equals	16003	
. Summary	e	OR 🔍	Error.ID	equals	16004	
	f	OR 🔨	Error.ID	equals	16005	
	Crite	ria Combinat	tion: a OR b OR c	OR d OR e OR f	Example: (a OR	b) AND c
						0

Figure 4.3 Rule Criteria complete example

- d. Acton Stop Rule Set
- e. Events Blank
- b. Once complete you will have a rule like the one shown in Figure 4.4. It will need to be placed above the *Always Block* rule, if it is not above this rule the service will not fail open.

(intel) Security Web Gateway	Dasht	Sard Policy Configuration Accounts Troubleshooting		Search Save Changes			
Rule Sets Lists Settings Templates							
 Add ▼ □ Add ▼ □ A t → □ A Default B Long Running Connections (Based on Time) E Long Running Connections (Based on Time) 	C Edi Rules in 'E						
Long Running Connections (based on volume)	Enabled	Enabled Name/Oriteria Action Events					
Even Hontoning Hontoning Hontoning Logine Indents Logine Indents Logine Indents Bodo n Anti-Mahare Engine Errors Bodo n URL Filter Errors Du Philer Errors External List Indents Application Control Filter Errors		Ignore Hail Bomb Warning 🚟 Stop Rule Set					
		Send Email on Internal Errors List.OfString.Sze (<u>Default Email Recipients</u> #) greater than 0	Stop Rule Set	Email.Send (List.OfString.ToString (Default Email Recipients ^A , ⁺ ; ⁺), ⁻ (Internal "There are internal errors, please examine mwg-core.errors.log file for more information. ⁻) < <u>Error Messages</u> >			
Block on SSO Errors Incident Notifications Block on All Errors	V	ICAP Fail Open Error. Ib equals 16000 CR Error. Ib equals 16001 CR Error. Ib equals 16002 CR Error. Ib equals 16003 CR Error. Ib equals 16004 CR Error. Ib equals 16004 CR	🚰 Stop Rule Set				
		Always Block Always	Block < <u>Internal Error</u> >				
_							
Rule Sets							
🔂 Log Handler							
0 Error Handler							
User Defined Properties							





4.3 Configure McAfee Web Gateway to implement GX profile switching based on Active Directory User Group:

The GX can have multiple data type profiles that allow it to implement different restrictions depending on which profile is called. Using ICAP headers the McAfee WGW can specify which profile it would like the GX to use, allowing for threat removal to be customised on a per user group basis.

- A For the following configuration steps, it is assumed that the MWG is already configured correctly to perform user authentication through Windows Active Directory. Users will need to be part of a User Group as the names of those groups are used as a criterion in MWG rule configuration. If not, please refer to the appropriate MWG configuration documentation to complete these steps.
- A For the following configuration steps, it is assumed that the GX is already configured to have the desired data type profile(s). The names of those profiles are referenced in ICAP headers in the MGW configuration steps. If not, please refer to the GX Configuration Guide to complete these steps.
 - For this example, I will be using the Active Directory user groups Students, Teachers, Staff and Headmaster, alongside their matching name GX data type profiles.
 Only ASCII characters are supported in GX profile naming.

4.3.1 Enabling GX User Profile Support

- Log into the GX GUI and navigate to Components → ICAP Server → Enable Default Profile Override → Toggle to Yes
 - Take note of the Parsing Profile Header and Rendering Profile Headers as these are used in the ICAP request information later. They can be configured to alternatives names as desired.

				Logge	d In: admin	GX / 2.0.0	Ti
G DEEP	\rightarrow		Activate Deactivate	Maintenance	Shutdown	Reboot Lo	oç
SECUF	RE -			Save Undo	Update	Import E:	xp
Monitoring System Information Diagnostic Log Diagnostics		erver					
Dashboards	Default Parsing	Basic 🗸					
Platform	Default Rendering	Basic 🗸					
Content	Enable Default Profile Override	o Yes					
Steganography Analysis	Parsing Profile Header	X-Parsing-Profile					
Network	Rendering Profile Header	X-Rendering-Profile					
Settings Peers List	Use Process Isolation	o No					
Management Interface	ICAP						
Components	Enable	o Yes					
ICAP Server	Network Interface	Data 🗸					
HTTP Server	Listen Port	1344					
Monitor Indexing							
Servers	Enable	o No					
Indexing	Network Interface						
Storage	Listen Port	11344					
Schemas	TLS Profile						
CSV Schemas	SSL Verification Mode	Mutual Server-side					
Fixed Format Schemas	Private Key						
HTML Schemas	Certificate						
JSON/Swagger Schemas	Concert National Optimized						
Protocol Buffers Schemas	General Network Settings						
XDSX Schemas	Buffer Size	65535					



Figure 4.5 GX Profile override location

4.3.2 Configure the McAfee WGW to use the ICAP headers

 Log into the McAfee WGW GUI and navigate to Policy → Rule Sets → Media Type Filtering → ICAP Client → RespMod

Server: megaggi Server Time: 2021-02-08 12:22 GMT UI Version 8.2.4	(32545) Usar: admin Role: Super Administrator		UserFreiferences Lagout 📀
CMCAfee McAfee Web Gateway	er Configuration Accurts Trackleboting		🔍 Search 🛛 🔛 Save Changes 💌
Rule Sets Lists Settings Templates			
🔾 Add - 🔛 🥒 🗙 🛊 🔸 💠 🕀 🖻	Edit 🗹 Enable 🗌 Enable in Cloud Criteria: Always		
Explicit Proxy Authentication and Authorization Authentication Server Bypass Microsoft (Office 365) Services DitTes Scanning	Apples to: Requests (and IM) Image: Respective Section 2014 Rules in: Respective Section 2014 Image: Respective Section 2014 Ø Add Rules X Edfs		
Remove Privacy Violating Header	Enabled Name/Criteria	Action	Events
 Global Whitelist Common Rules 	Skip RespMod Server for Responses Without a Body	Stop Rule Set	
General Content of the second se	Add X-Server-IP header	- Continue	1 Event
Download Media Types	Call RespMod Server	🚳 Stop Cycle	
S BegMod	RespModRuleSet	🐥 Continue	
C Pule Sets			
Dog Handler			
B Error Handler			
Loser Defined Properties			

Figure 4.6 Rule location

- Click the Add rule button and create a new rule with the following set:
 - Name Relevant name
 - Rule Criteria Click Add.. → Choose Advanced Criteria → The Selected Property -Authentication.UserGroups, Selected Operator - Contains, Compare with - Value – String and [<Active Directory User Group Name>] (E.g. Students)
 - Acton Continue



Selected Property:	Selected Operator:	Compare with	Value - String
Authentication.UserGroups	contains	"Students"	
Filter: <none> -</none>			
Type to filter properties 🛛 😵			
Recommended	all in list	Students	
Action.Names 📃	at least one in list		
List of Actions performed.	contains		
Antimalware.VirusNames	contains at least one match		
List of names of found viruses	does not contain		
Authentication.GetUserAzureGroups()	does not equal		
Get user groups from Azure AD	equals		
Authentication GetUserGroups	none in list		
Get user groups only, no authentication. Can be used only with LDAP or User Database methods.			
Authentication.ICEToken.Audiences Audiences that are stored in/loaded from ICEToken			
Authentication.UserGroups			
contains the groups of the last authenticated user.			
Command.Categories			
Stores a list of categories that apply to the			
list of String' User Defined Property			
		,	
			OK Cancel

Figure 4.7 Rule criteria example

 Events – Add → Event → ICAP.AddRequestInformation → Settings: RespMod → Parameters: Header Name – [<Parsing Profile Header from GX as shown in Figure 4.5>] (e.g. if the default GX header values have been used set this to X-Parsing-Profile) and Header Value - [<Active Directory user group>] (E.g Students).

Event:	Settings:
Type to filter events	RespMod 🗸
HTTP.SetStatus (Number)	
Header.Add (String, String)	😳 Add 🥜 Edit
Header.AddMultiple (String, List of String)	
Header.Block.Add (String, String)	Para and a second
Header.Block.AddMultiple (String, List of Strin	Parameters
Header.Block.RemoveAll (String)	
Header.Block.RemoveAllMatching (String, Stri	
Header.ICAP.Response.Add (String, String)	
Header.ICAP.Response.AddMultiple (String, Li	
Header.ICAP.Response.RemoveAll (String)	
Header.ICAP.Response.RemoveAllMatching (S	
Header.RemoveAll (String)	
Header.RemoveAllMatching (String, String)	
Header.Response.Add (String, String)	
ICAP.AddRequestInformation (String, String) 🚽	
	OK Cancel



Figure 4.8 Rule criteria example

• Repeat the previous step and create a second Event for the Rendering Profile. Once completed the following event will be listed as shown in Figure 4.8.

Steps	Optional: Select one or more events to take effect immediately.
l. Name	Events:
2. Rule Criteria	💽 ICAP.AddRequestInformation ("X-Parsing-Profile", "Students") <respmod< td=""></respmod<>
3. Action	ICAP.AddRequestInformation ("X-Rendering-Profile", "Students") <respm< p=""></respm<>
4. Events	
5. Summary	
	Sack Next > Finish Cancel

Figure 4.9 Rule criteria example

• You will now have a rule like the one shown in Figure 4.9. It will need to be placed above the *Call RespMod Server* rule, if it is not above this rule the ICAP based profile switching will fail.

Server: mwgappi Server Time: 2021-02-09 11:18 GMT UI Version 8.2.4 (1545) User	admin Role: Super Administrator		UserPreferences Logout 🕐
McAfee McAfee Web Gateway	Pos	y Configuration Accusts Trablehooting		🔍 Search 🔛 Save Changes 💌
Rule Sets Lists Settings Templates				
Rule sets Luss settings tempares Ø Add + 0 Q M and tempares Compares Beplick Proxy Authentication and Authorization Authentication Server Bypass Microsoft (Office 355) Services Common Phases Violating Header Benova Phases Violating Header Common Nules Upload Media Types Dominal Media Despite Aleval Common Nules BespMed Gateway Anti-Malware Dynamic Content Classification	Constant of the second	Parable in Cloud Criteria: Always Parable in Cloud Criteria: Always Pacuests (and M) Responses Parable in Cloud Criteria: Always Name/Criteria Skip RespMod Server for Responses Without a Body Add X-Server-IP header CX profile switch using "Students" User Group CX profile switch using "Staff" User Group CX profile switch using "Staff" User Group CX profile switch using "Headmaster" User Group CAI RespMod Server RespModRuleSet	Action Stop Rule Set Continue Continue Continue Continue Continue Continue Stop Cycle Continue Continue Continue	Events 1 Event 2 Events 2 Events 2 Events 2 Events
뒤 Rule Sets				
log Handler				
An Error Handler				
& User Defined Properties				





Each rule is only able to cover a single user group so multiple will be required if switching between more than two Active Directory and GX profiles as shown by the rules for Students, Teachers, Staff and Headmaster in Figure 4.9
 The order of the rules matters if users are in more than one of the users groups in use, the lowest one in the list will take precedence.



5 Troubleshooting

5.1 Missing Images on Websites

5.1.1 McAfee Web Gateway Timeout

When a user is browsing the internet images can be missing from websites:



Figure 5.1 Example of a missing image on website

This can be caused due to the Progress page Delay setting. This setting can be found within the McAfee WGW under Policy \rightarrow Settings \rightarrow Progress Page \rightarrow Delay for redirects to progress page. To confirm this is the setting being invoked view the network settings in the console of the browser. If any of the images being loaded by the browser have a 307 returned and url contains MWG, this confirms that the *Delay for redirects to progress page* setting is being invoked.



● ◎ ♥ Q, Ш Preserve log 🗹 Disable cache Online 🔹 :	1 1 V
Filter UI Hide data URLs 🔛 XHR JS CSS Img N	fedia Font Doc WS Manifest Other 🗉 Only show requests with SameSite issues
500 ms 1000 ms 1500 ms 2500 ms 3500 ms	200 m 201 m 200 m 1000 m 1000 m 1000 m
Name	* Headers Preview Response Initiator Timing Cookies
e flow_045.jpg	* v General
ie flow_046.jpg	Request URL: https://www.apple.com/uk/ipad-pro/images/overview/display_bardware romend cells2vidifada large.ong
■ flow_048.jpg	Request Method: 6ET
■ flow_049.jpg	
■ flow_050.jpg	Remote Address: 172.17.16.149/1000
H flow_052.jpg	Referrer Policy: no-referrer-when-downgrade
m flow_053.jpg	T Response Headers
m now_054.jpg	- Independent Federald - English and former Laborated Card Anti-Anti-Anti-Anti-Anti-Anti-Anti-Anti-
(= flow_056.jpg	<pre>iodcamon: https://www.appie.com/mg-internal/des/signu/jos/progressig-ocaku/wagkrsu_grestsposgillaysregaw/cn_dg,</pre>
in now_us/.jpg	statuc 307
Env 060 inc	* Request Headers
Env 051 inc	sauthority: www.apple.com
- few 052 inc	imethodi 6ET
E flow 054.ico	spath: /uk/ipad-pro/images/ov_ex/display hardware zoomed_cg6k2vi0fa6a large.ong
- flow.065.jpg	scheme: https://Response Headers
flow_066.jpg	accept: inage/ Hold Children S
- flow_068.jpg	accept-encodim location: https://www.apple.com/mwg-internal/_e5fs23hu73ds/progress?id=bCawOP4kgknSG_OYEFtspbfSgZ114vShfguwPvCn_gg.
E flow_069.jpg	accept-languag
fiow_070.jpg	cache-control: no-cache
flow_072.jpg	cookie: s_fid=68700020f8F87594-328F320C3F820152; s_vi=[CS]v1]2F364C78851587CC-600006FCE0552000[CE]; geo=68; ccl=9v/0TV/HbTvkTUH7IPR2Zg==; s_cc=true; s_sq=85885088508
- flow_073.jpg	D
flow_074jpg	progma: no-cache
- flow_076.jpg	referer: https://www.apple.com/wk/ipad-pro/styles/overview.css
flow_077.jpg	sec-fetch-dest: inage
E flow_078.jpg	sec-fetch-mode: no-cons
- flow_080.jpg	sec-feldv-site: same-origin
E flow_081.jpg	user-agent Hozilla/5.0 (Windows NT 18.0; Wind4; x64) AppleHebtilt/537.36 (KHTML, 11ke Gecko) Chrome/80.0.3987.149 Safari/537.36
favicon.ico	

Figure 5.2 Example console view of website with 307s

By default, the *Delay for redirects to progress page* setting is set to 5 seconds. This setting will need to be increased if images are being lost on websites.



Figure 5.3 McAfee Configuration example

With this setting increased and configuration saved the images will be transformed successfully and displayed on the website.





Figure 5.4 Website being displayed after McAfee setting updated

5.2 Formatting on webpages ruined and content missing

As it is possible for unsupported media to be passed to the GX from MWG, it is possible for this to cause formatting issues with some websites (See Figure 5.5).



(←)→ ♂ ₪	🛛 🔒 https://www.bbc.co.uk/news	 ▽ ☆	III\ 🗉 📽
• Three			
Search			
Search the BBC Search	Search the BBC		
NEWS			
News Navigation			
Sections			
BBC News Hon	ne		
Latest Stories Most ReadSkip to most read Latest Stories Most Read			
The BBC is bet	ter when you sign in 🗙		
Start by setting your nation for news	and sign		
<u>Sign in</u> or <u>Register</u>	up for		
O Find out more about signing up for	a BBC account BBC		
You're now seeing more stories from	the UK account later		
Change your nation DFind out more about changing your	nations nation		
Top Stories			

Figure 5.5 Website being incorrectly displayed

The cause of this is the GX media transformation rules, if a piece of content is sent to the GX and no suitable rule can be found for its processing the GX will block that piece of content. To circumvent this issue a new type mapping will need to be configured to allow any unsupported content to be returned.

To add this new type mapping to a GX profile:



• On the GX appliance navigate to Data Types \rightarrow Profiles.

Servers		Bitman				
Indexing	bmp	(File)	bmp	Disabled	1	-
Storage	application/vnd.openxmlformats- officedocument.wordprocessingml.document	DOCX	application/vnd.openxmlformats- officedocument.wordprocessingml.document	Enabled	-	-
schemas	docx	DOCX (File)	docx	Enabled	-	-
CSV Schemas	image/emf	EMF	image/emf	Enabled	-	_
Fixed Format Schemas	emf	EMF (File)	emf	Enabled	-	-
HTML Schemas	application/emf	EMF	application/emf	Enabled	-	-
DSON/Swagger Schemas	image/gif	GIF	image/gif	Disabled	-	-
XDSX Schemas	gif	GIF (File)	gif	Enabled	-	-
XSD Schemas	text/html	HTML	text/html	Enabled	-	
	html	HTML (File)	html	Enabled	-	-
Input Data Types	htm	HTML (File MS)	htm	Enabled	-	_
Output Data Types	text/calendar	ICAL	text/calendar	Enabled	-	-
Type Mappings	ics	ICAL (ICS)	ics	Enabled	-	-
Promes	VCS	ICAL (VCS)	vcs	Enabled	-	-
ettings	image/ipeg	JPEG	image/ipeg	Disabled	-	_
Diagnostic Logging	ipeg	JPEG (File)	ipeg	Disabled	-	
Audit Logging Regular Expressions	Bai	JPEG (File MS)	jpg	Enabled	-	_
TLS Profiles	image/jp2	JPEG2K	image/jp2	Enabled	-	-
Metrics Date & Time	jp2	JPEG2K (File)	jp2	Enabled	-	-
Keys & Certificates	application/json	JSON	application/json	Enabled	-	
Remote Management	mime	MIME	mime	Enabled	-	-
Account	message/rfc822	MIME (RFC822)	message/rfc822	Enabled	-	-
Links	application/x-mimearchive	MIME (Archive)	application/x-mimearchive	Enabled	-	-
, 100ar	emi	MIME (EML)	emi	Enabled	-	

Figure 5.6 Data Types \rightarrow Profiles location

• Head to the bottom of your chosen profile and choose add.

Figure 5.7 Location of Add button near the bottom of a profile.



- Now configure the following settings:
 - Input Content Type \rightarrow #Unidentified
 - Type Mapping → Binary (Anything)**
 - Output Content Type \rightarrow #Unidentified
 - Status \rightarrow Enabled

Add	×
Input Content Type: #Unidentified	
Type Mapping: Binary (Anything)	
Output Content Type: #Unidentified	
Status: Enabled	
1	Add Cancel

Figure 5.8 Example of the new #Unidentified Type Mapping



• The new type mapping should now be in place at the bottom of the list as shown in Figure 5.9. To make sure this now remains save the GX settings.

	application/x-www-form-urlencoded	URL Encoded (Forms)	application/x-www-form-urlencoded	Enabled	
	image/wmf	WMF	image/wmf	Enabled	
	application/wmf	WMF	application/wmf	Enabled	/
	wmf	WMF (File)	wmf	Enabled	/
	application/vnd.openxmlformats- officedocument.spreadsheetml.sheet	XLSX	application/vnd.openxmlformats- officedocument.spreadsheetml.sheet	Enabled	
	xlsx	XLSX (File)	xlsx	Enabled	/
	embedded/xml	XML (Embedded)	embedded/xml	Enabled	
	application/xml	XML	application/xml	Enabled	
	xml	XML (File)	xml	Enabled	/
	text/csv	CSV	text/csv	Enabled	/
	csv	CSV (File)	csv	Enabled	/
	text/plain	Text	text/plain	Enabled	-
	txt	Text (File)	txt	Enabled	/
	application/zip	ZIP	application/zip	Enabled	/
	application/x-zip-compressed	ZIPx	application/x-zip-compressed	Enabled	-
	zip	ZIP (File)	zip	Enabled	/
	#Unidentified	Binary (Anything)	#Unidentified	Enabled	
	+ Add				
Actions Clone	e Profile				
eset Profi	les				

Figure 5.9 Example of the new type mapping now at the bottom of the list.



6 Supported Data Types

The following data types are currently supported by the Deep Secure GX appliance:

Data Type	Content Type	
BMP	Image/bmp Image/x-ms-bmp	
	Bmp	
CSV	Text/csv	
	CSV	
DOCX	Application/vnd.openxmlformats-	
	officedocument.wordprocessingml.document	
	docx Deplication (and	
EMF	Application/emi	
	Fmf	
CIE	Image/gif	
GIF	Gif	
	Text /html	
HINL	H+m]	
	Htm	
IPEG	Image/jpeg	
	Jpeg	
	Jpg	
JPEG2K	Image/jp2	
	Jp2	
JSON	Application/json	
MIME	Mime	
	Message/rfc822	
	Application/x-mimearchive	
	Eml	
	Mht	
PDF	Application/pdf	
PNG	Image/png	
	Png	
PPTX	Application/vnd.openxmlformats-	
	officedocument.presentationml.presentation	
ртг	ppux Text /rtf	
KIF	Rt f	
	Application/msword	
тхт	Text/plain	
	Txt	
TIFF	Image/tiff	
	Tiff	
	Tif	
WMF	Application/wmf	
	Image/wmf	
	Wmf	
XML	Embedded/xml	
ZIP	Application/zip	
	Application/x-zip-compressed	
	Zlp	



7 References

GX Configuration Guide.



8 Appendix A

8.1 ICAP Error IDs

Error ID	Error Message	Error Description
16000	NoICAPServerAvailable	No ICAP server available from list: \$list\$.
16001	NoRespModPropInReqMod	Property \$propName\$ cannot be calculated in
		request cycle.
16002	ICAPBadResponse	ICAP client filter error: ICAP server sent bad
		response.
16003	ICAPMaxConnectionLimit	ICAP client filter error: Maximum number of
		connections reached.
16004	ICAPCannotConnectToServer	ICAP client filter error: Cannot connect to ICAP
		server.
16005	ICAPCommunicationFailure	ICAP client filter error: Failure in
		communication with ICAP server.

Url to McAfee Error ID List - <u>https://docs.mcafee.com/bundle/web-gateway-7.8.0-interface-</u>reference-guide-unmanaged/page/GUID-5151C504-39F7-45E2-8C13-1C9E85D1990A.html