



---

# GX integration with McAfee Web Gateway Application Note

---

## Table of Contents

1	Introduction .....	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	Integration Steps.....	6
3.1	Initial Configuration of ICAP .....	6
3.2	Configure the new Reqmod .....	7
3.3	Configure the new Respmo d .....	9
3.4	Configure ICAP Media Type Rule Set.....	10
4	Enhanced configuration .....	12
4.1	Configure McAfee Web Gateway to convert HTTP/2.0 Requests to HTTP/1.1 (Only for GX 1.6.0 or Older).....	12
4.2	Configuring McAfee WGW ICAP to fail open .....	12
4.3	Configure McAfee Web Gateway to implement GX profile switching based on Active Directory 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	Troubleshooting.....	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	Supported Data Types.....	27
7	References .....	28
8	Appendix 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.

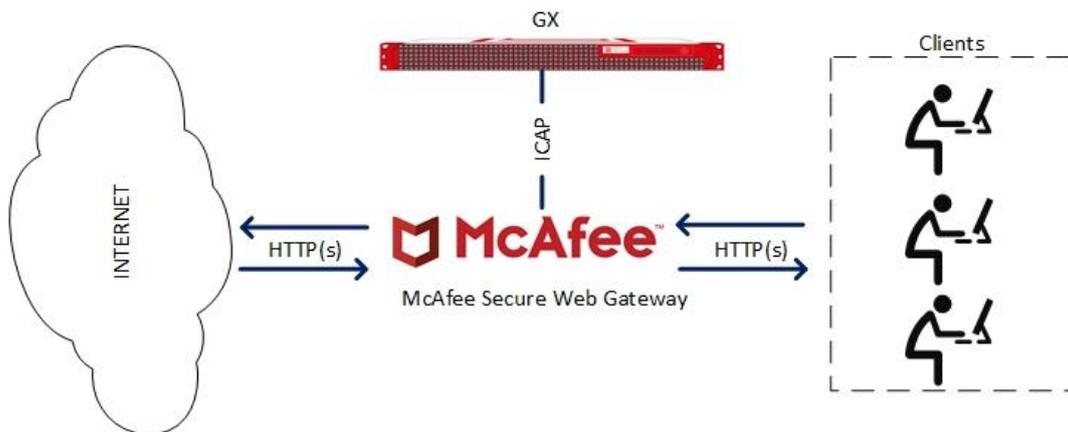


Figure 1-1: GX and McAfee deployment

### 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
<b>Emphasis</b>	Terms in a definition list or emphasis for important introductory words in a paragraph.
<b>Options</b>	Menu names, options, buttons, keys and other items from the user interface or the keyboard.
<i>Italics</i>	Cross-reference to related information in another document.
<variable>	A value you must supply, for example in a command line.
[<variable>]	An optional value you can supply, for example, in a command line.
	<b>Important information that emphasises or supplements points in the text, or that may apply only in special cases.</b>
	<b>A caution that alerts you that failure to take or avoid a specified action could result in the loss of data.</b>
<small>Tip</small>	<b>A tip that suggests an alternative method for applying a technique or procedure or helps you to understand the benefits and capability of the product.</b>

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 pre-requisites 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.

**Tip** 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

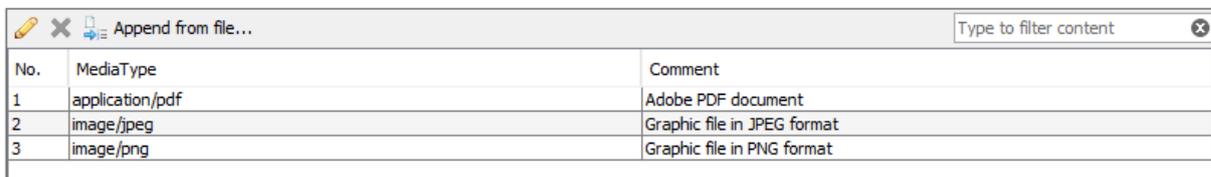
#### 3.1 Initial Configuration of ICAP

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

- ⚠ 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 Media Type 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.



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.

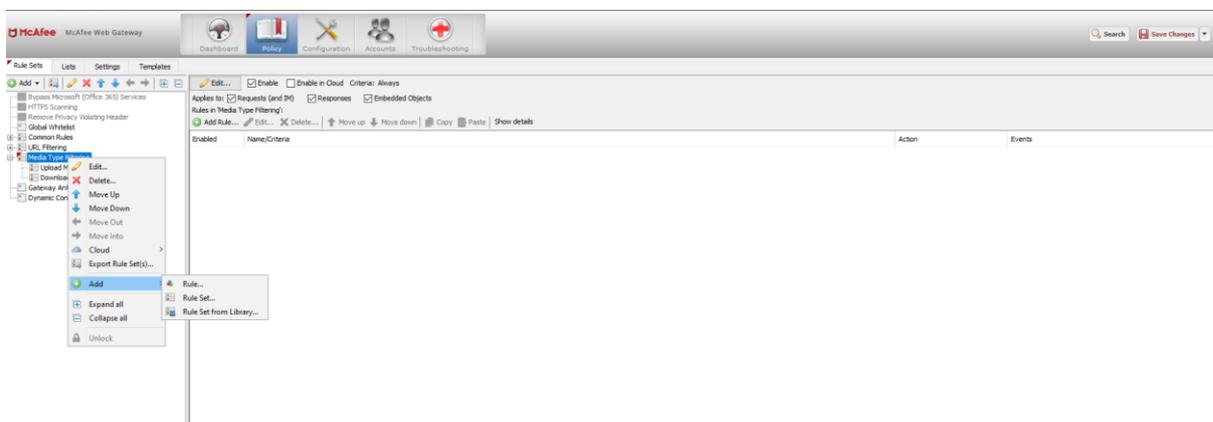


Figure 3.3 Example creation of new Rule Set

**Tip** 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.

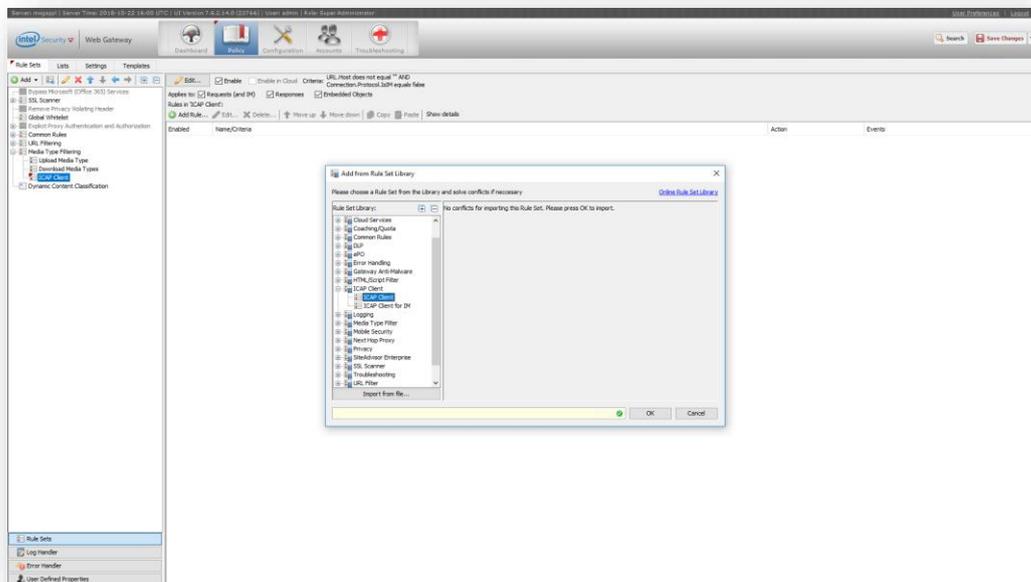


Figure 3.5 Example of ICAP Client Rule Set Library

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
```

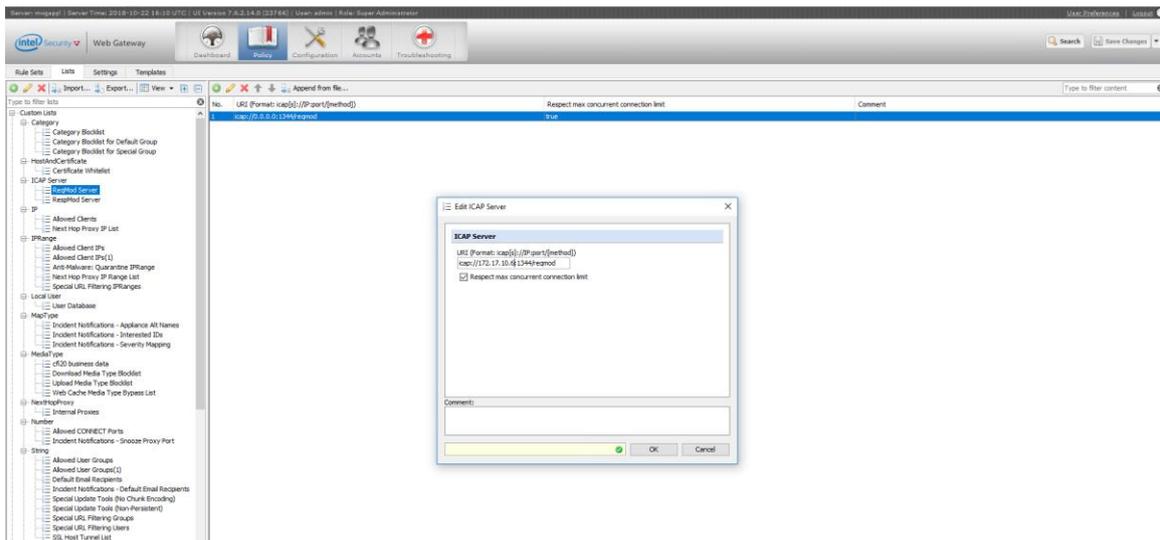


Figure 3.6 Example ICAP Server Configuration

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`.

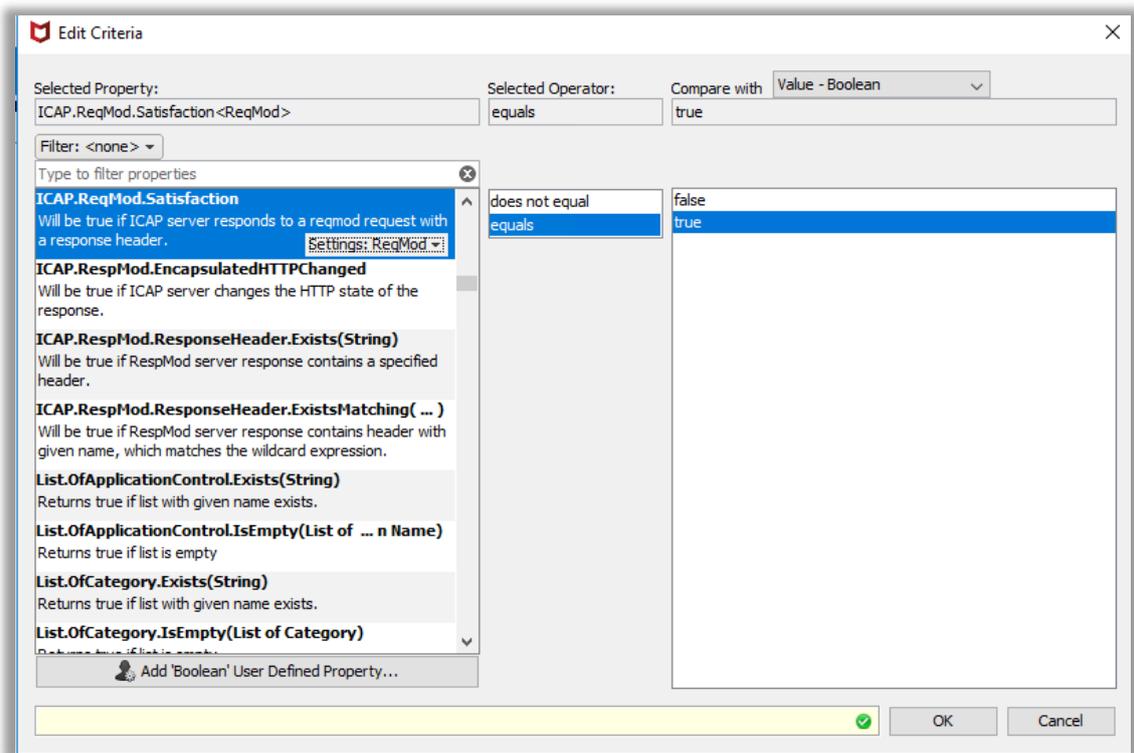


Figure 3.9 Example ReqMod Rule Criteria

- Action – Continue
- Events – Leave Blank

### 3.3 Configure the new Respmo

To configure the newly created ReqMod navigate to Policy -> Lists -> ICAP Servers -> Respmo 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/respmo
```

Finally configure the Respmo Rule set. To do this for the Respmo navigate to Policy -> Rule Set -> Media Type Filtering -> ICAP Client -> Respmo 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`.

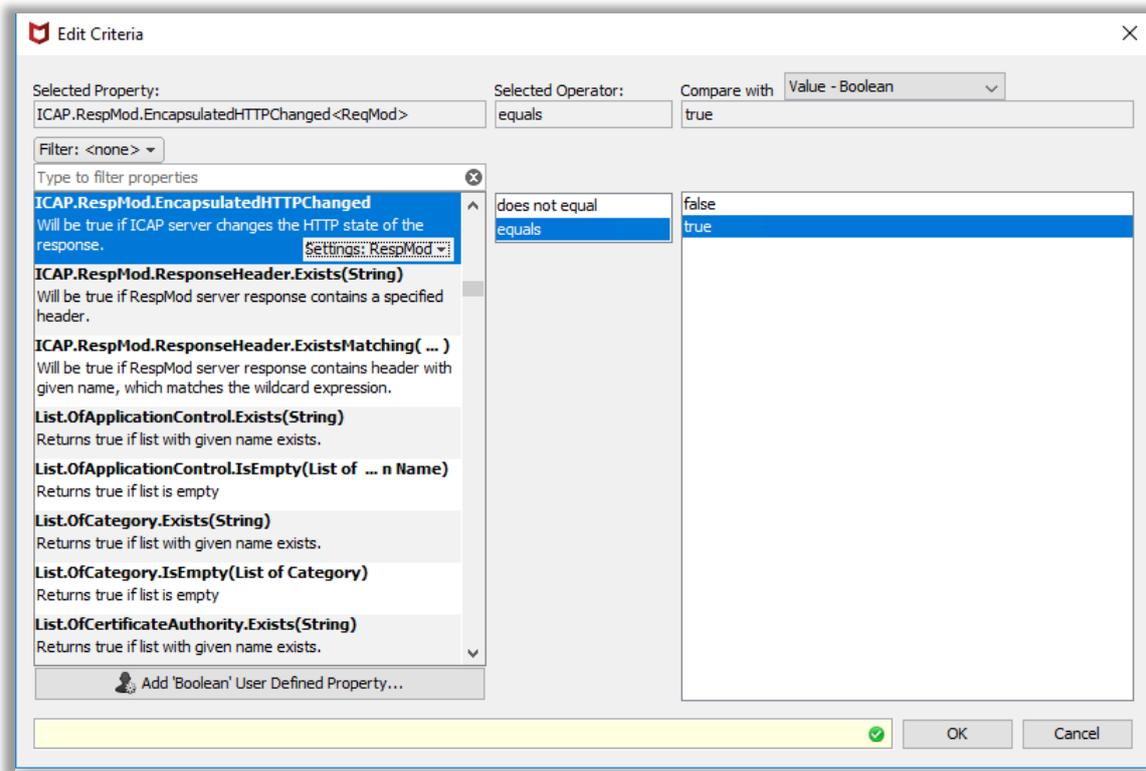


Figure 3.10 Example RespMod Rule Criteria

- 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).

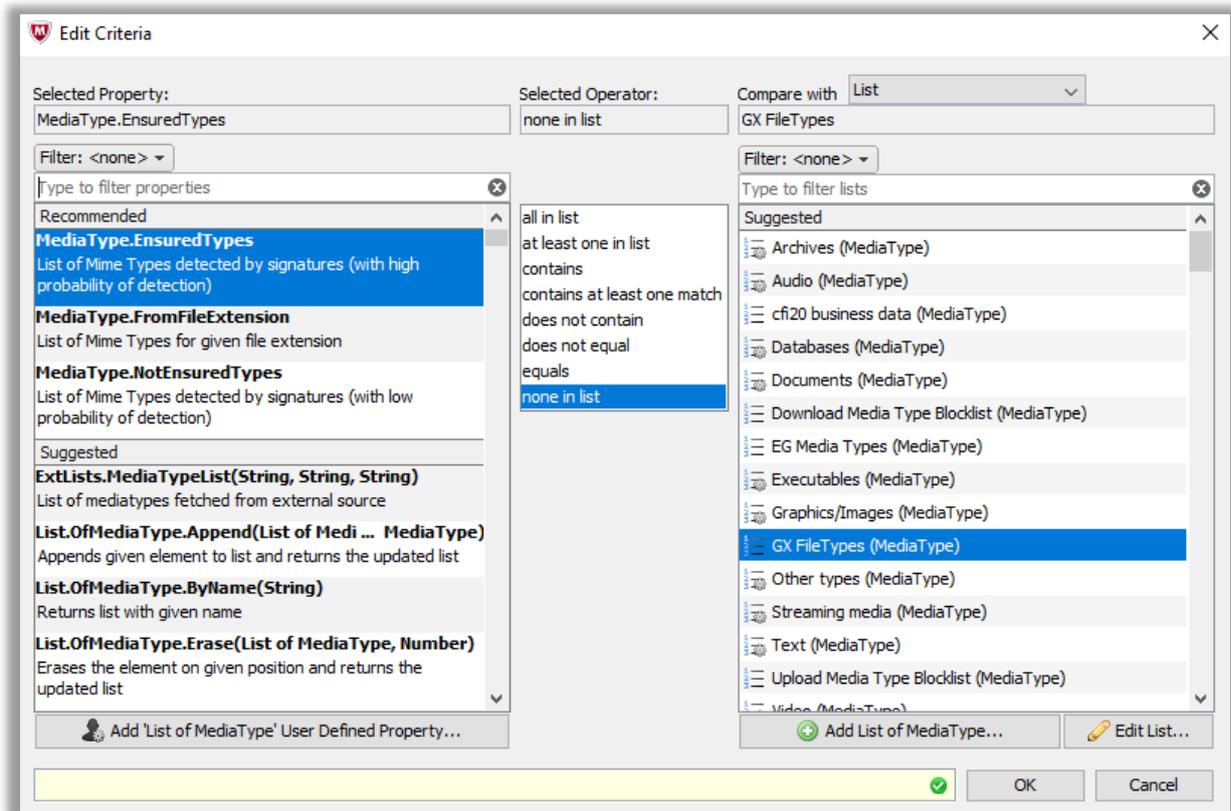


Figure 3.8 Example Rule Criteria

- 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)

- ⚠ 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.

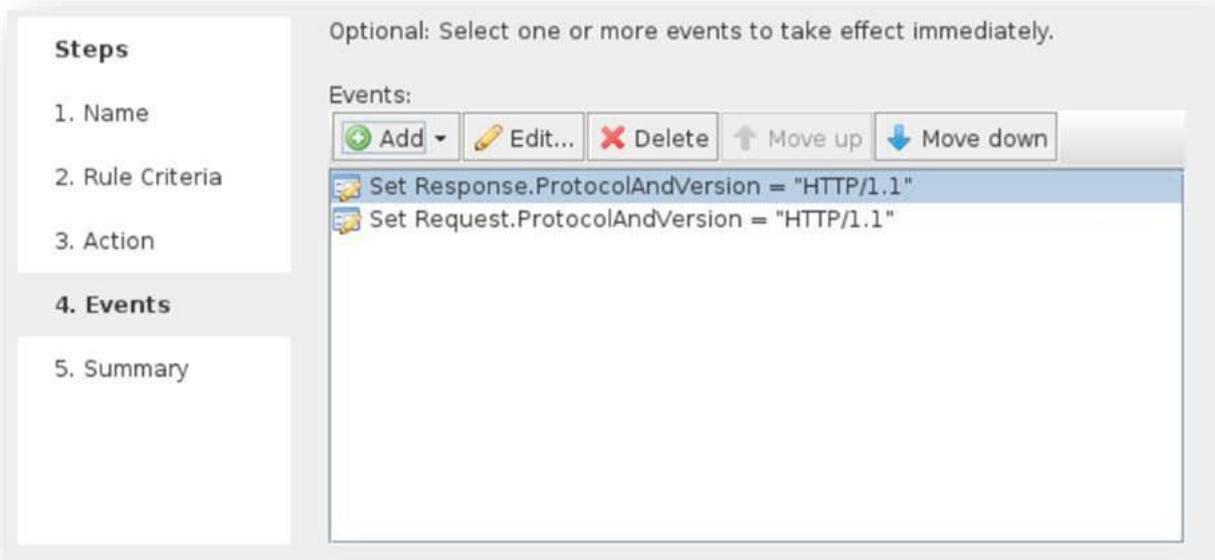


Figure 3.1 Configure MWG to convert HTTP/2.0 Requests to HTTP/1.1

### 4.2 Configuring 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

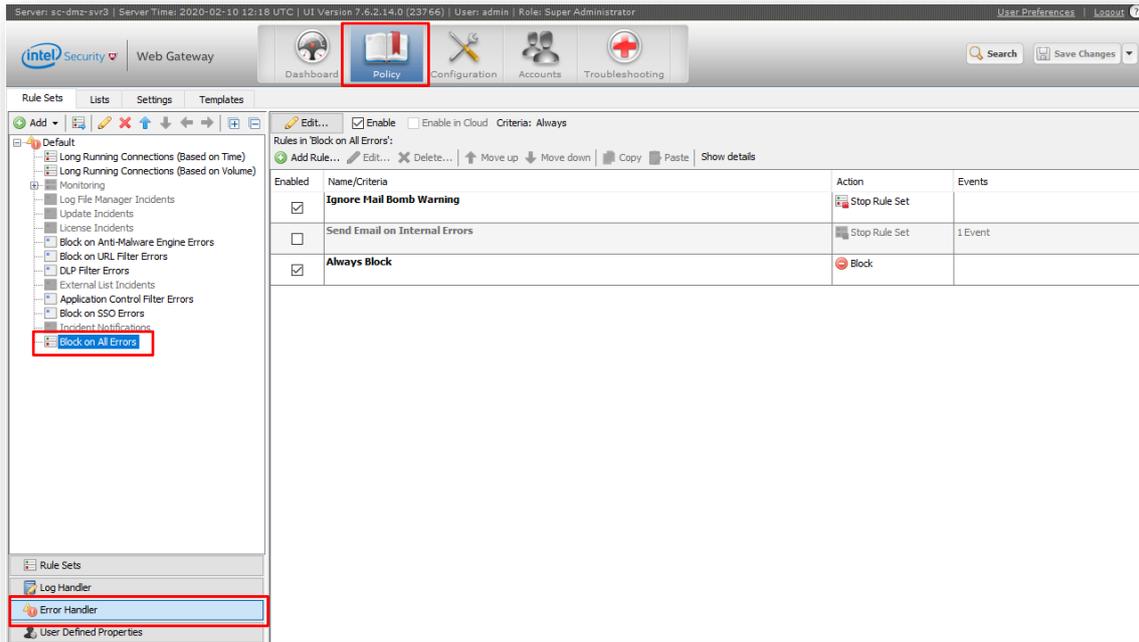


Figure 4.1 Rule Location

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

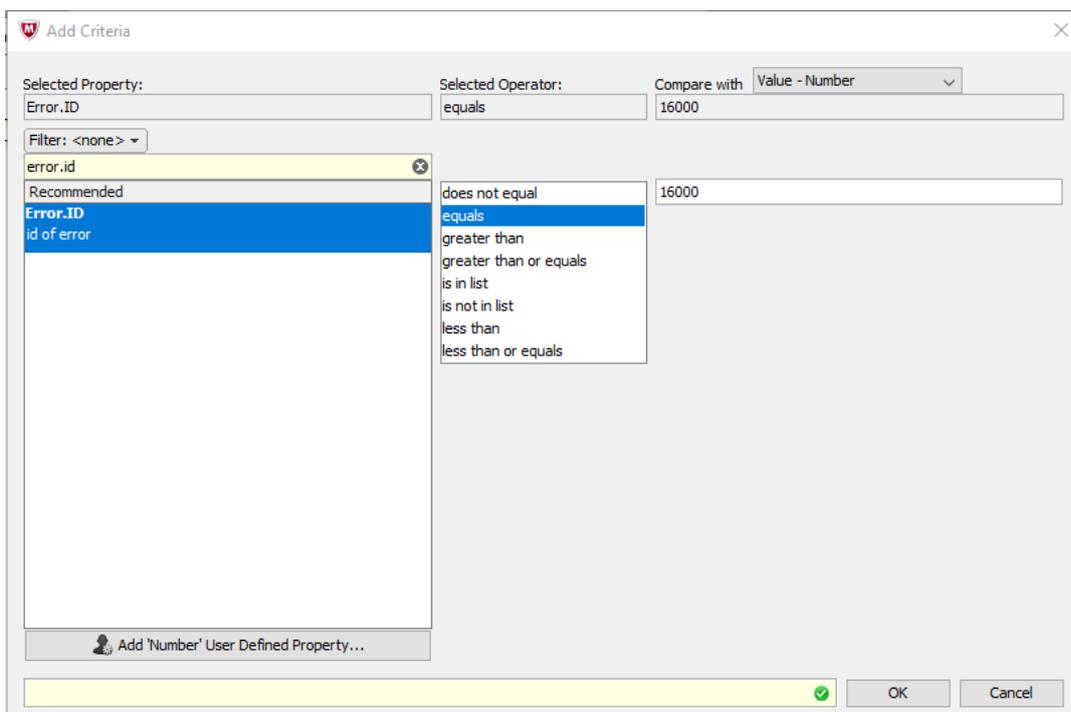


Figure 4.2 Rule Criteria example

- 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:

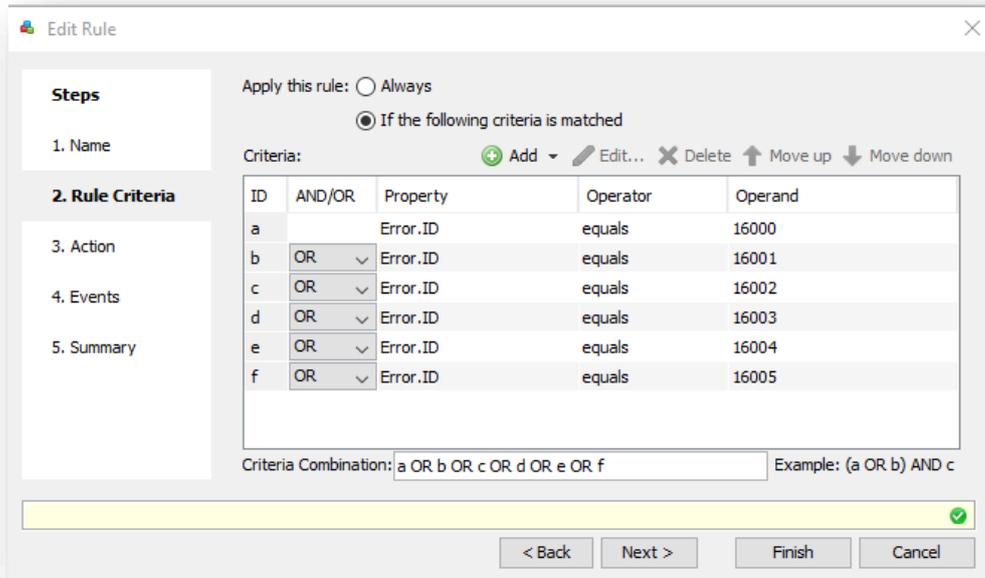


Figure 4.3 Rule Criteria complete example

- 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.

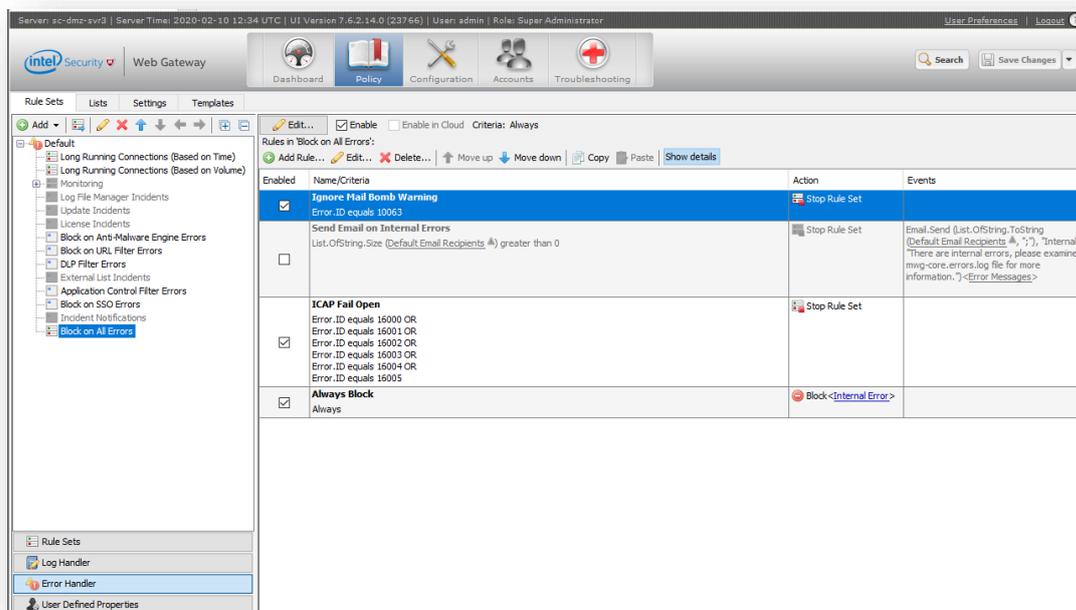


Figure 4.4 Completed rule location

### 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.

- ⚠ 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.
- ⚠ 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.

**Tip** 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.

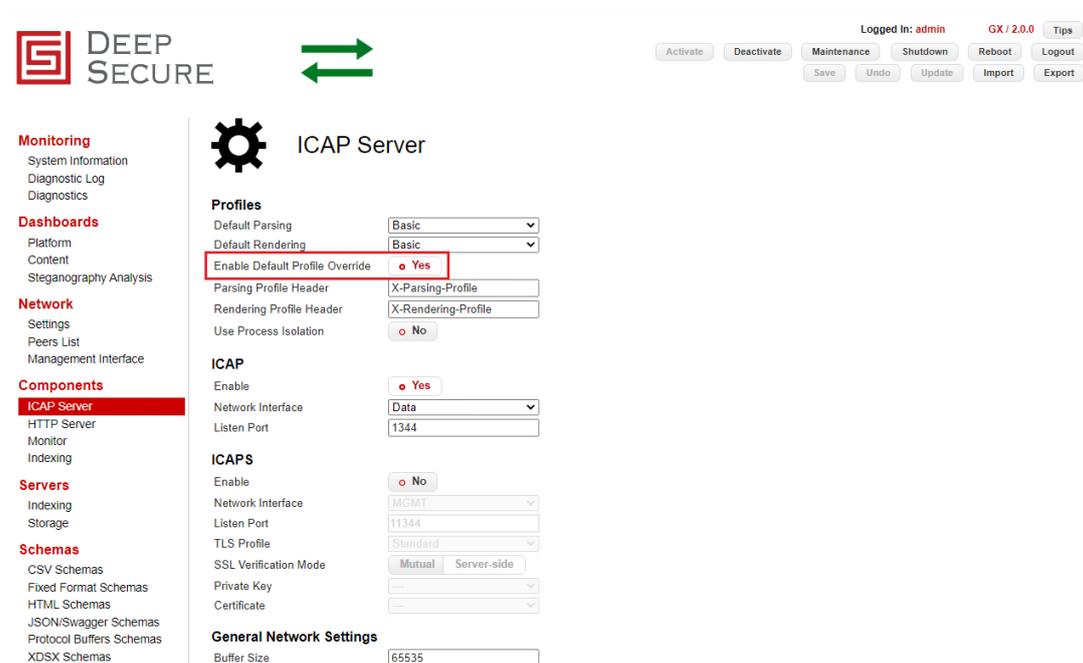


Figure 4.5 GX Profile override location

#### 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

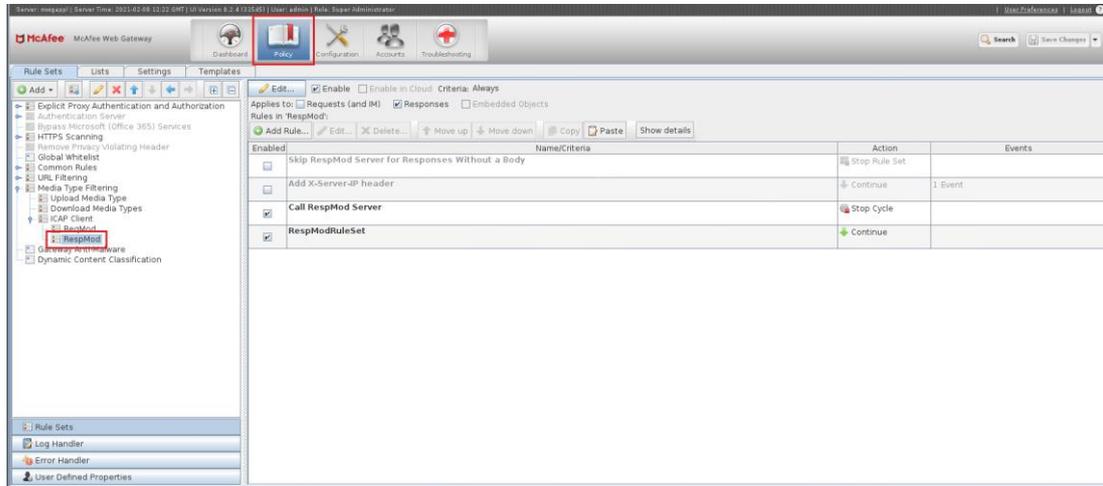


Figure 4.6 Rule location

- 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

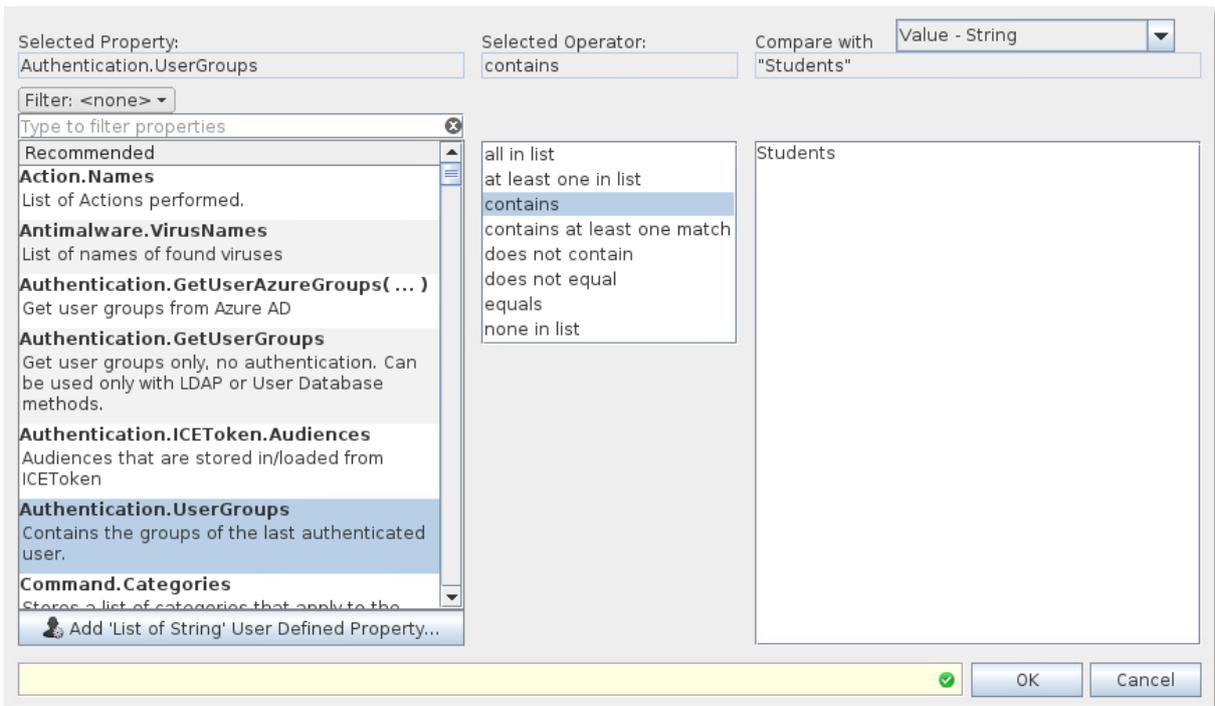


Figure 4.7 Rule criteria example

- 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) .

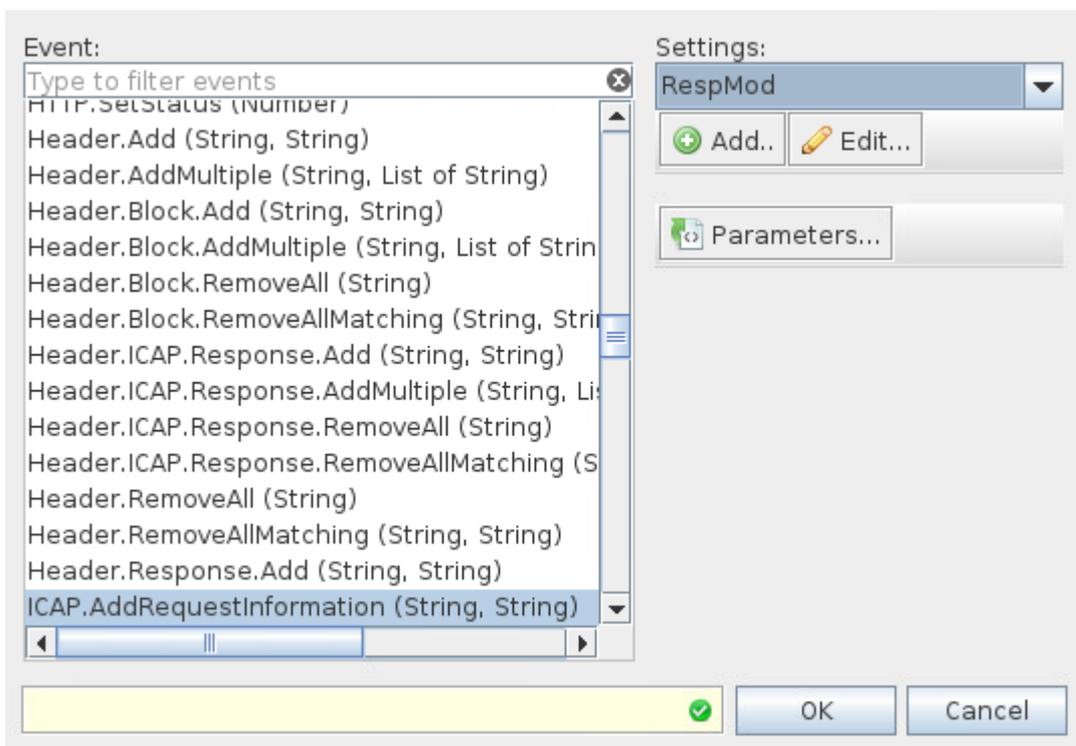


Figure 4.8 Rule criteria example

- 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.

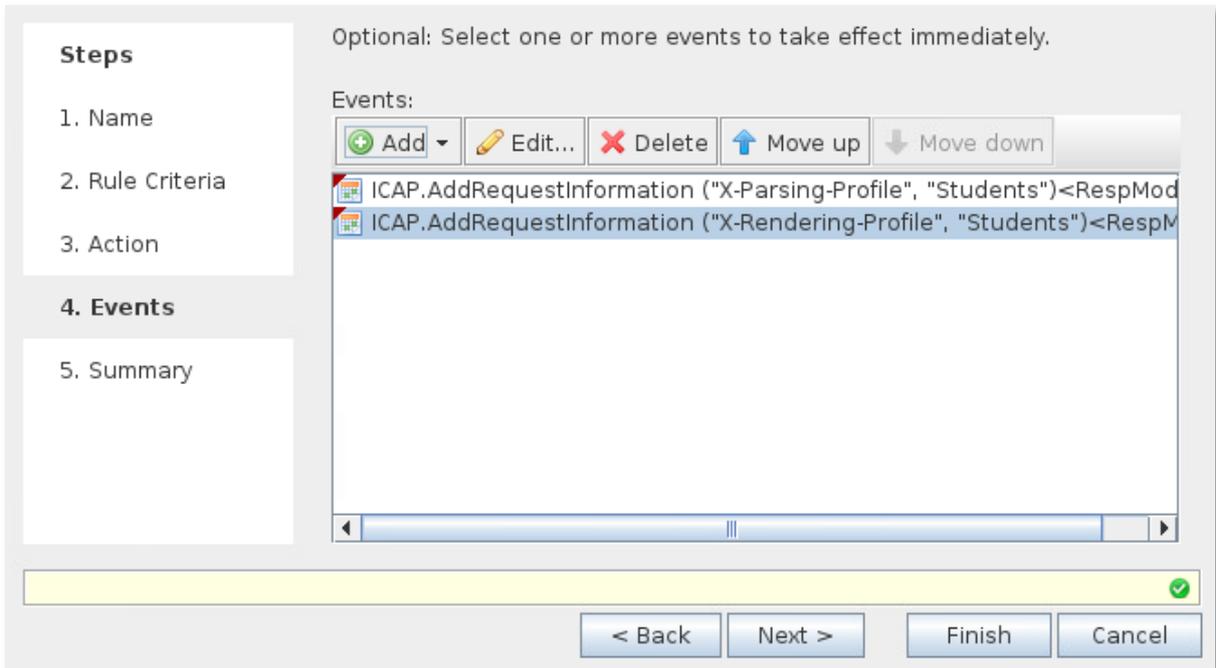


Figure 4.9 Rule criteria example

- 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.

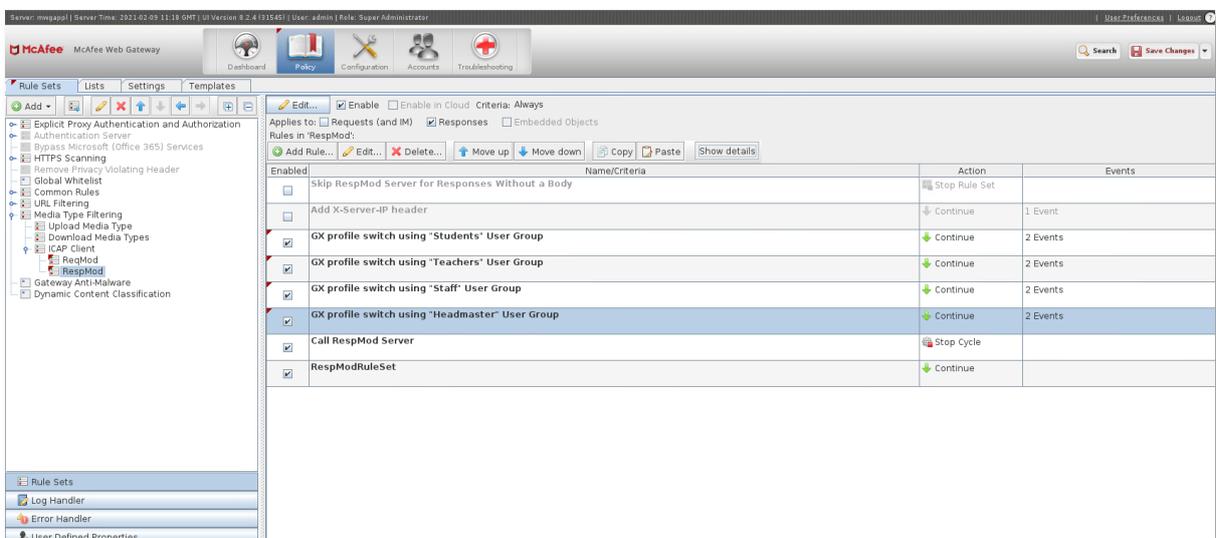


Figure 4.10 Complete rule location

**Tip** 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:

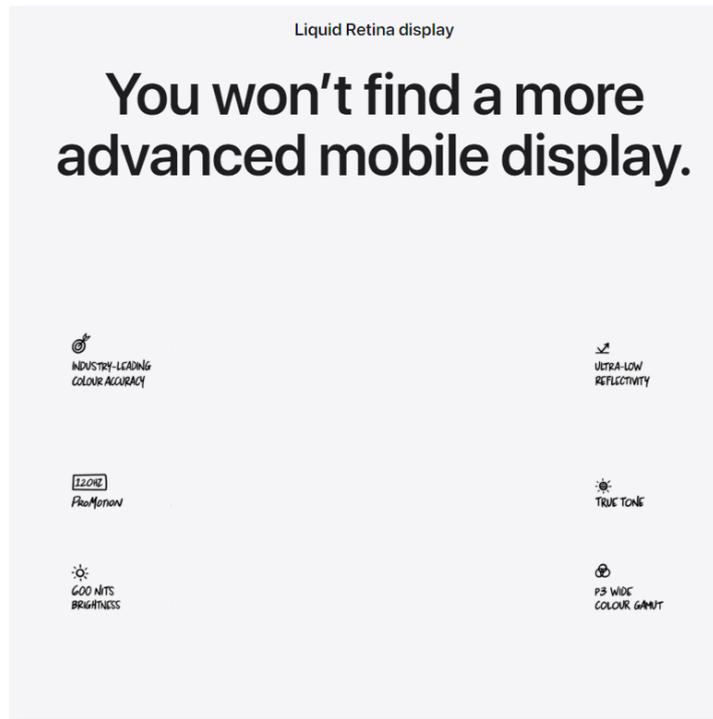


Figure 5.1 Example of a missing image on website

This can be caused due to the Progress page Delay setting. This setting can be found within the McAfee WGW under Policy → Settings → Progress Page → 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.

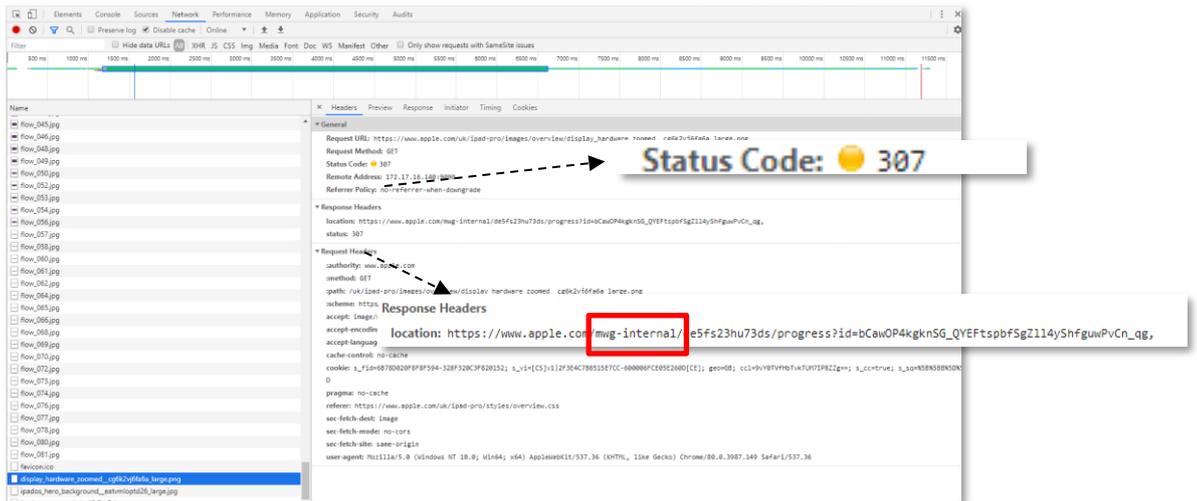


Figure 5.2 Example console view of website with 307s

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.

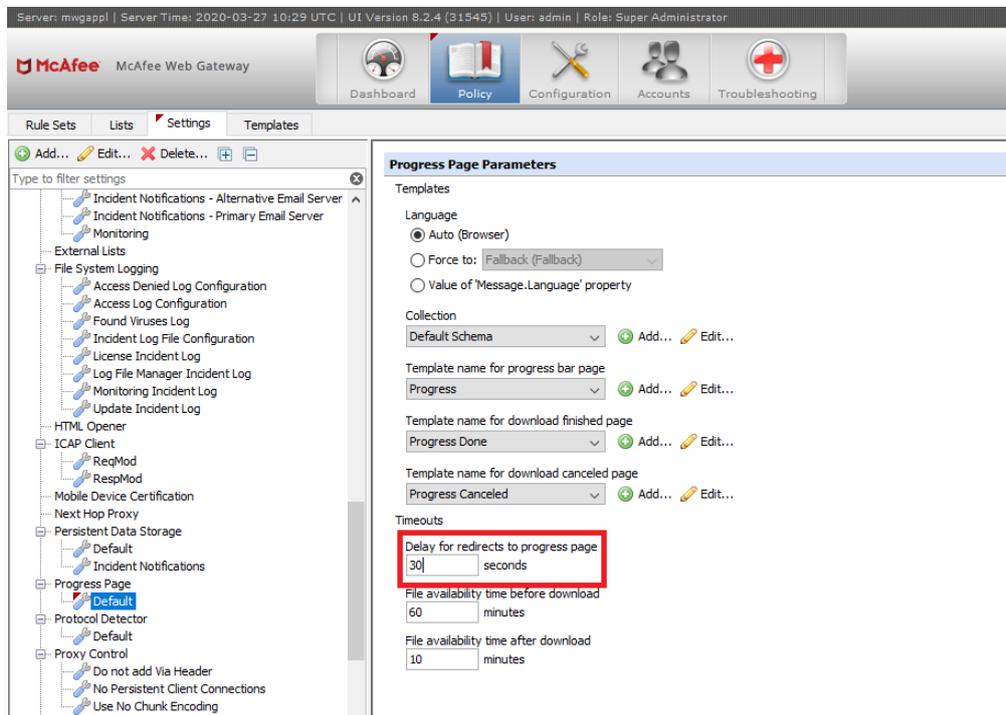


Figure 5.3 McAfee Configuration example

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

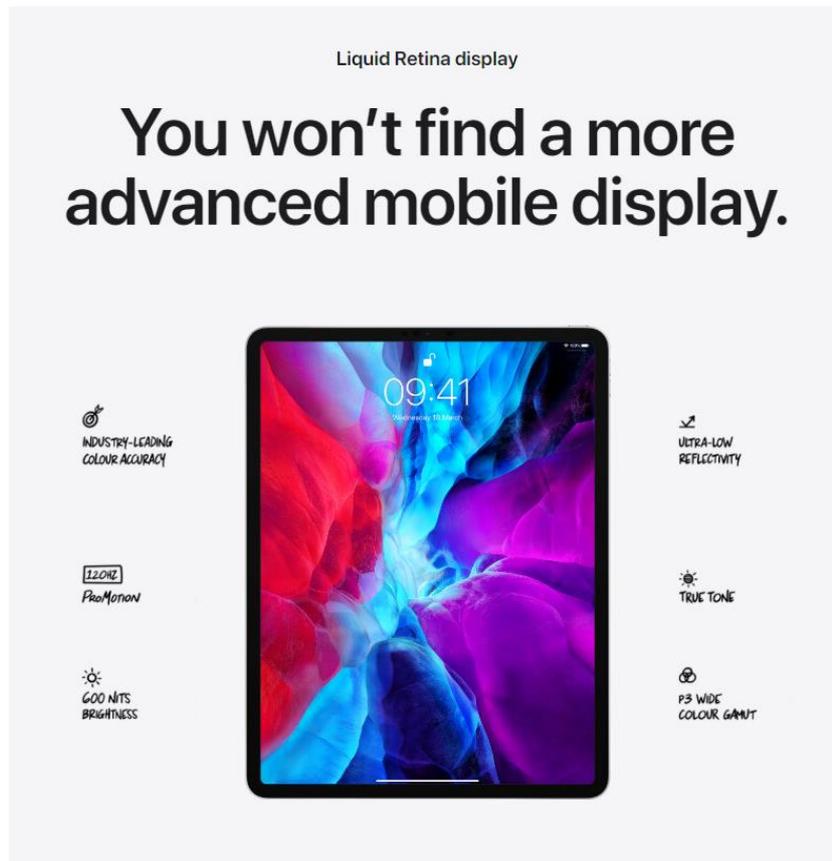


Figure 5.4 Website being displayed after McAfee setting updated

## 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).

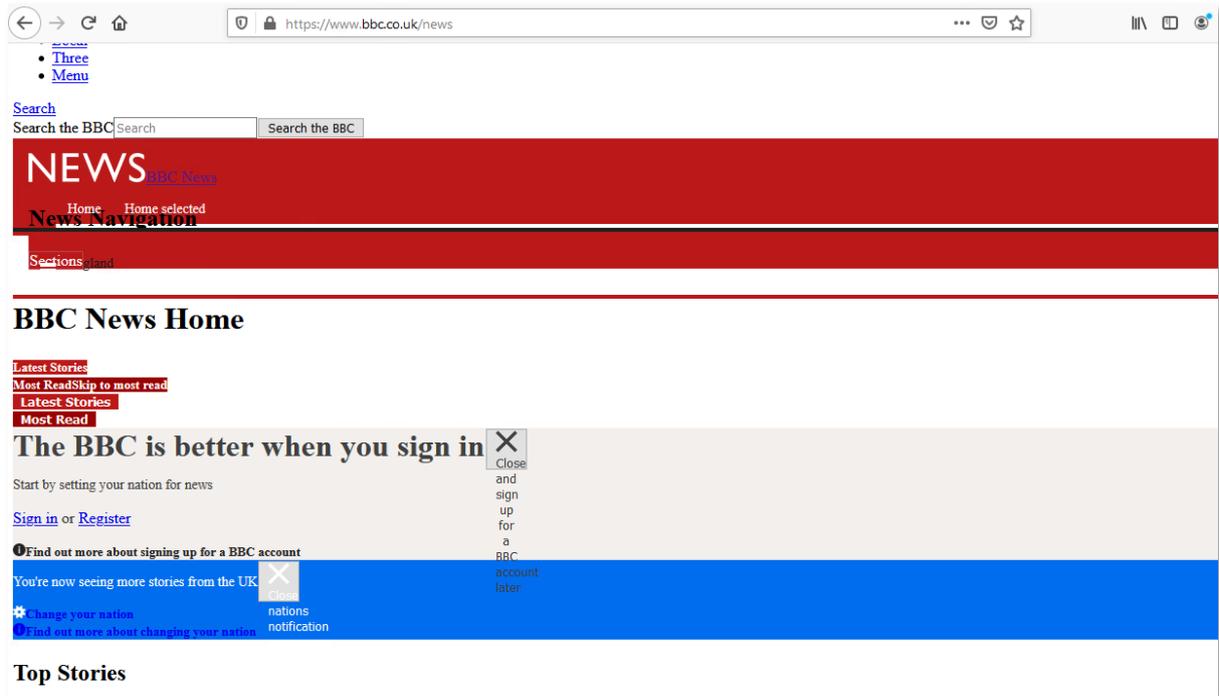


Figure 5.5 Website being incorrectly displayed

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 → Profiles.



Figure 5.6 Data Types → Profiles location

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

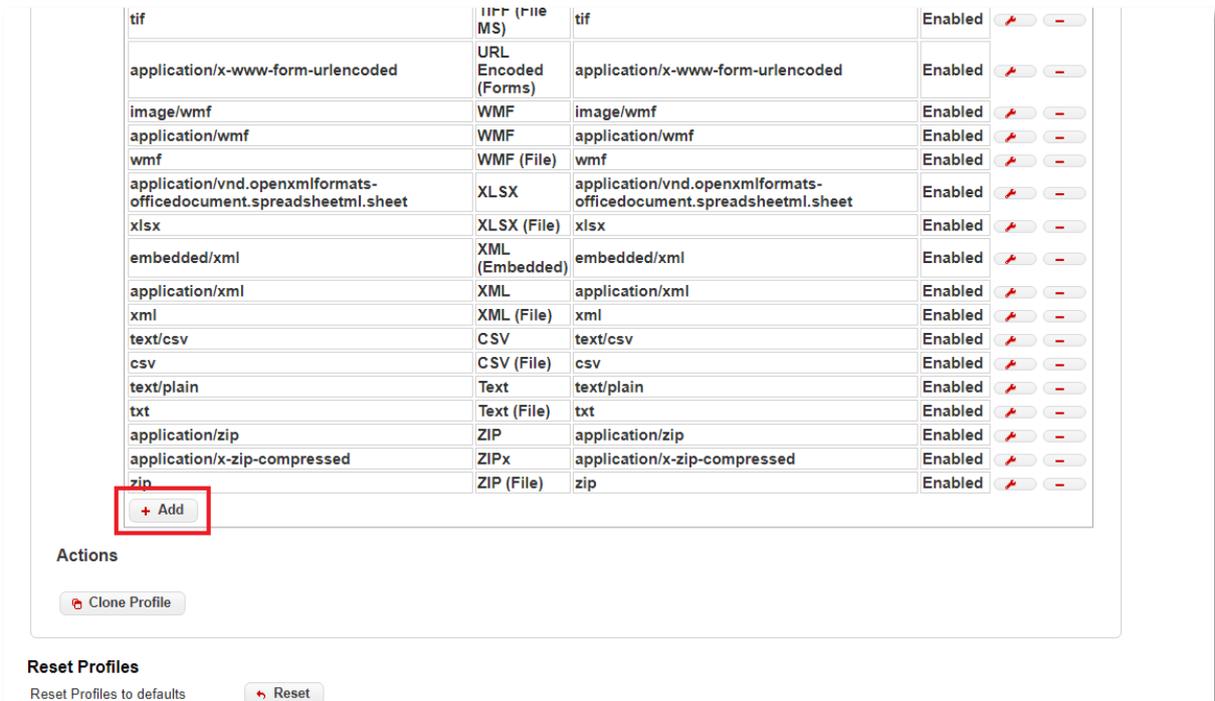
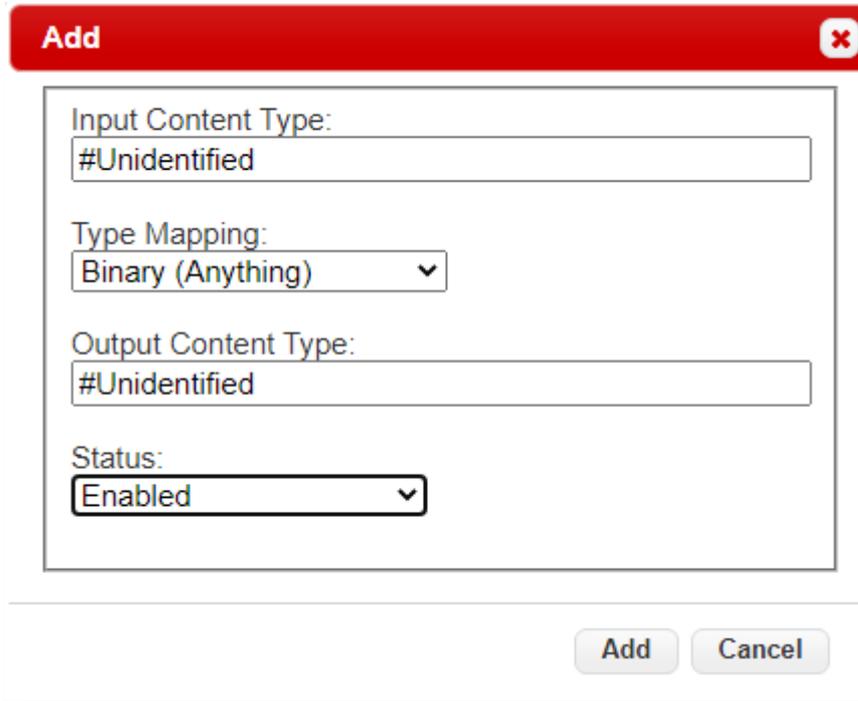


Figure 5.7 Location of Add button near the bottom of a profile.

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



The image shows a dialog box titled "Add" with a red header and a close button (X) in the top right corner. The dialog contains four configuration fields:

- Input Content Type:** A text input field containing "#Unidentified".
- Type Mapping:** A dropdown menu with "Binary (Anything)" selected and a downward arrow.
- Output Content Type:** A text input field containing "#Unidentified".
- Status:** A dropdown menu with "Enabled" selected and a downward arrow.

At the bottom right of the dialog, there are two buttons: "Add" and "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 Profile](#)

**Reset Profiles**

Reset Profiles to defaults [Reset](#)

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
EMF	Application/emf Image/emf Emf
GIF	Image/gif Gif
HTML	Text/html Html Htm
JPEG	Image/jpeg Jpeg Jpg
JPEG2K	Image/jp2 Jp2
JSON	Application/json
MIME	Mime Message/rfc822 Application/x-mimearchive Eml Mht
PDF	Application/pdf Pdf
PNG	Image/png Png
PPTX	Application/vnd.openxmlformats-officedocument.presentationml.presentation pptx
RTF	Text/rtf Rtf Application/msword
TXT	Text/plain Txt
TIFF	Image/tiff Tiff Tif
WMF	Application/wmf Image/wmf Wmf
XML	Embedded/xml
ZIP	Application/zip Application/x-zip-compressed Zip

## **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 - <https://docs.mcafee.com/bundle/web-gateway-7.8.0-interface-reference-guide-unmanaged/page/GUID-5151C504-39F7-45E2-8C13-1C9E85D1990A.html>