



Deep Secure Gateway eXtension uses ICAP to receive data from McAfee Web Gateway. This means a on premises McAfee Web Gateway will be required to push the ICAP configuration to MVISION.

- 1. Download the Deep Secure GX ICAP Client.zip
- 2. Unzip the Deep_Secure_GX_ICAP_Client.zip to extract the Deep Secure GX ICAP Client.xml
- 3. Connect to the McAfee Web Management page and import the Deep_Secure_GX_ICAP_Client file. To do this navigate to Policy -> Rule Set -> Media Type Filtering and click Add -> Rule Sets from Library, click Import from File and select the Deep_Secure_GX_ICAP_Client.xml file.
 - If the Media Type rule has not been unlocked, unlock this and import the Deep Secure GX ICAP Client Rule
- 4. Verify the import was successful by navigating to:
 - a. Policy -> Media Type -> GX Media Types



b. Policy -> ICAP Server -> ReqMod Server & RespMod Server





c. Policy -> Rule Sets -> Media Type Filtering -> Deep Secure GX ICAP Client.

Server: mwgappl Server Time: 2020-09-16 09:53 UTC UI Version 9.2.2	(39635) User: admin Role: Super Administrator	1 <u>Us</u>	er Preferences Logout 🕐
McAfee McAfee Web Gateway Dashboar	Policy Configuration Accounts Troubleshoating	Q Sear	rch Save Changes 🔻
Rule Sets Lists Settings Templates			
Add E Add E Add C C Add C C	Edit PEnable Enable in Cloud Criteria: Connection.Protocol.ISIM equal ** MD Applies to: Pequests (and IM) Pesponses Enabedded Objects Pules in 'Deep Secure GX ICAP Client': Add Pule Pedit X Deltet Move up Move up Move up Move up Move up Paste Shov details		
 ☐ Global Whitelist ← Common Rules ← URL Filtering ← Media Type Filtering ← Deep Secure GN ICAP Client ← Reybdd ← Budad Media Type ← Download Media Types ← Gateway Anti-Makare ← Dynamic Content Classification 	Enabled Name/Criteria	Action	Events
	CX Hedia Types	Stop Rule Set	

To test the before and after Deep Secure Policy change:

- 1. Navigate to <u>http://demo.deep-secure.com/poc/Restricted/index.html</u> and sign in with the Username and Password provided by Deep Secure.
- Using a browser that is not being protected by Deep Secure navigate to Scripted Malware → Trade Price List.
- 3. Download and open the PDF hover over the top left corner of the document. A pop up will appear saying hacked!



Using a browser that is being protected by McAfee and Deep Secure navigate to the same URL as shown in *step 1* and download the same PDF (Trade Price List). This time when the PDF is view it will look the same as the original, however the hacked pop up will no longer appear.