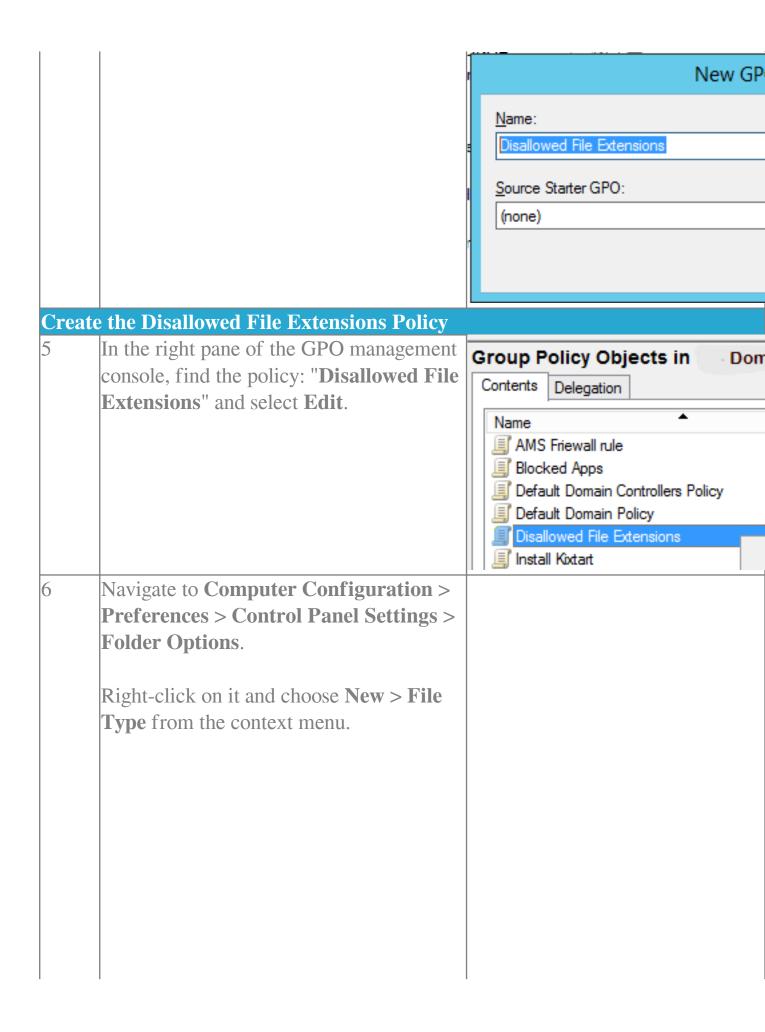
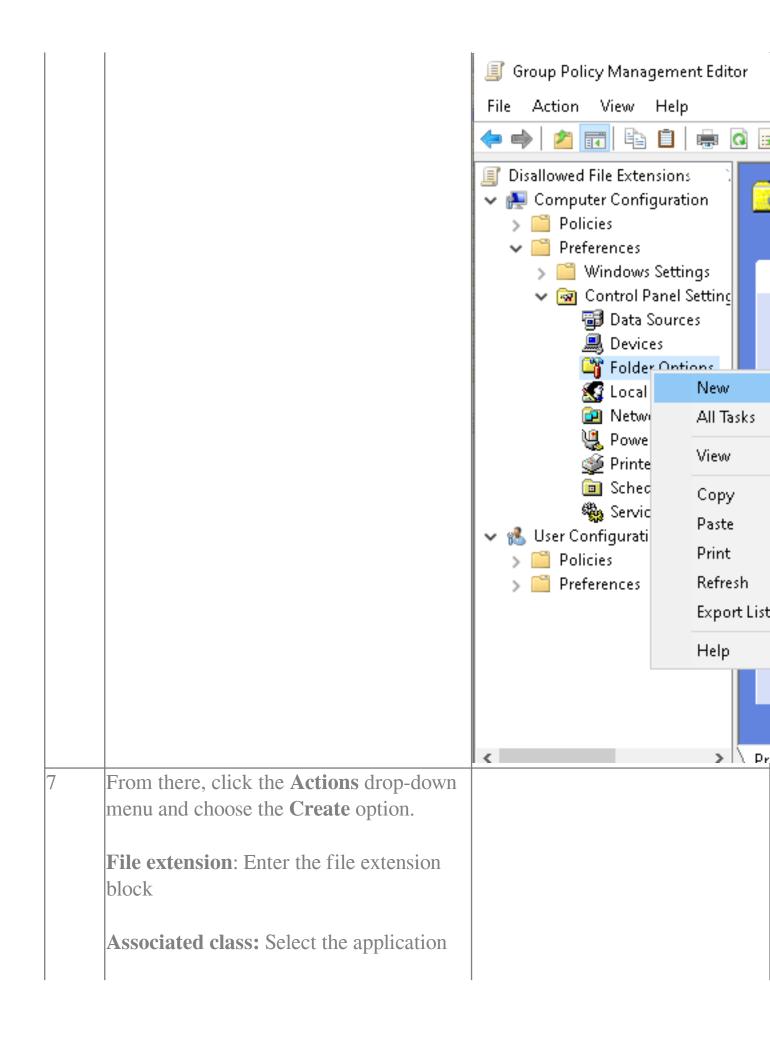
## How to Restrict File Types Recognized as Possible Crypto Threats with Group Policy

Step #	Task	Screenshot	
1	Log in to a PC that has <b>The Application That File Extension Uses</b> and <b>Domain Administrative Tools</b> installed.		
2	From the <b>Server Manager</b> Screen:		Serv
	Select Tools > Group Policy Management	Dashboard Local Server All Servers AD DS DHCP DNS File and Storage Services	QUICK START  WHAT'S NEW  LEARN MORE
			ROLES AND SERV Roles: 4   Server gro
3	Right-click on <b>Group Policy Projects</b> and select <b>New</b> .	<ul> <li>▶ ☐ Group Policy Obje</li> <li>▶ ☐ WMI Filters</li> <li>▶ ☐ Starter GPOs</li> <li>Sites</li> </ul>	<u>N</u> ew <u>B</u> ack Up Al Manage Ba
4	Name the new GPO Disallowed File Extensions and then, click OK.		





	that uses this file.	New File Type Properties	
	Click <b>OK</b> to Save.	File Type Common	
	Repeat Steps 5 and 6 for each extension that needs to be entered.  Note: application must be installed on the device you are creating the GPO on or else it will not be available in the list.	Action: Create	
		File extension: iqy	
		Associated class: Excel	
		Configure class settings	
		Icon file path:	
		Icon Index:	
		Actions:	
		Confirm open after download Always show extension Browse in same window  OK  Cancel	
8	Apply the rule to the top of the domain	-	
	infrastructure so it will apply to every		
	device on the domain.		
	-	· · · · · · · · · · · · · · · · · · ·	

Online URL: <a href="https://kb.naturalnetworks.com/article.php?id=509">https://kb.naturalnetworks.com/article.php?id=509</a>