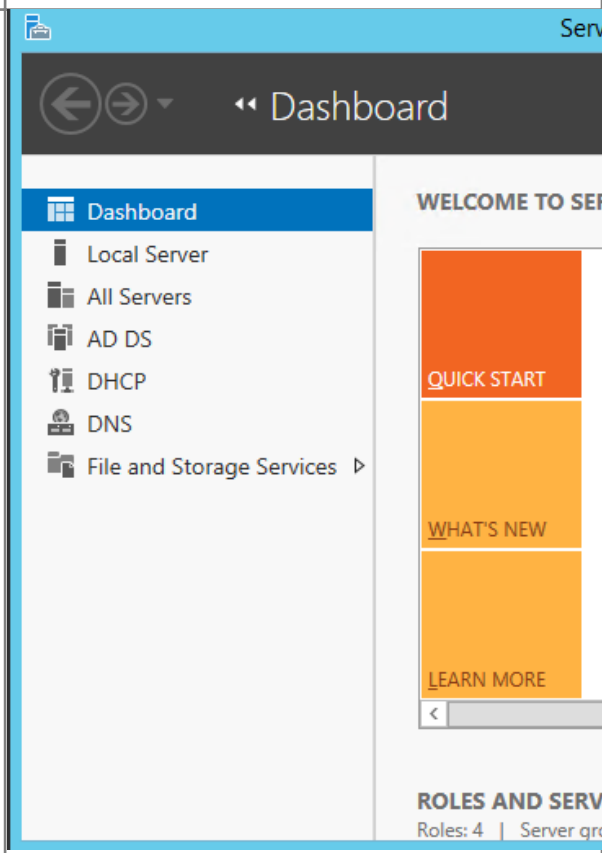
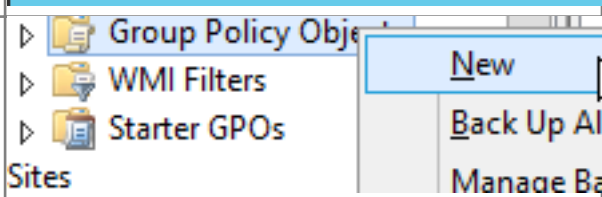
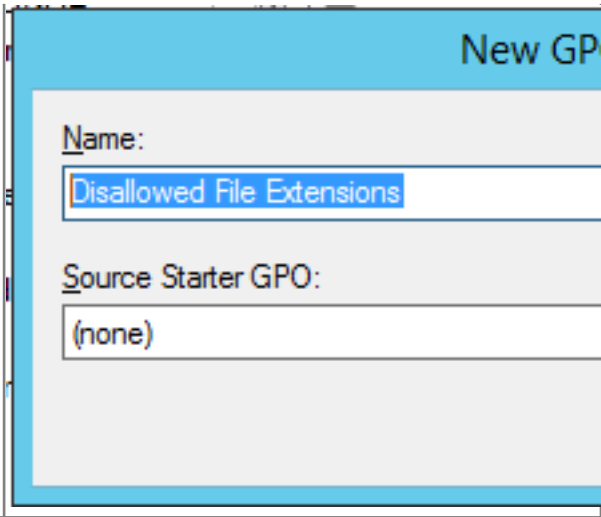
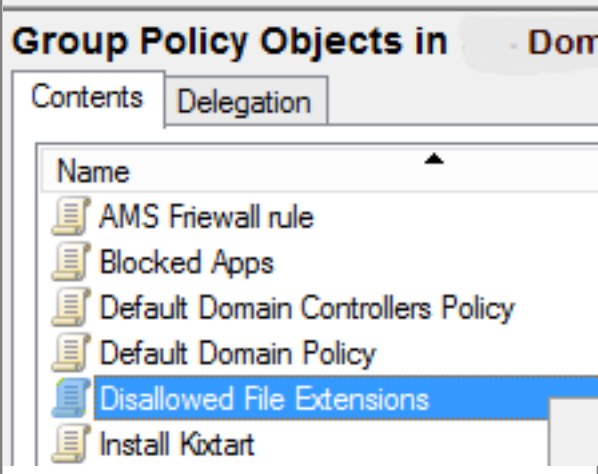
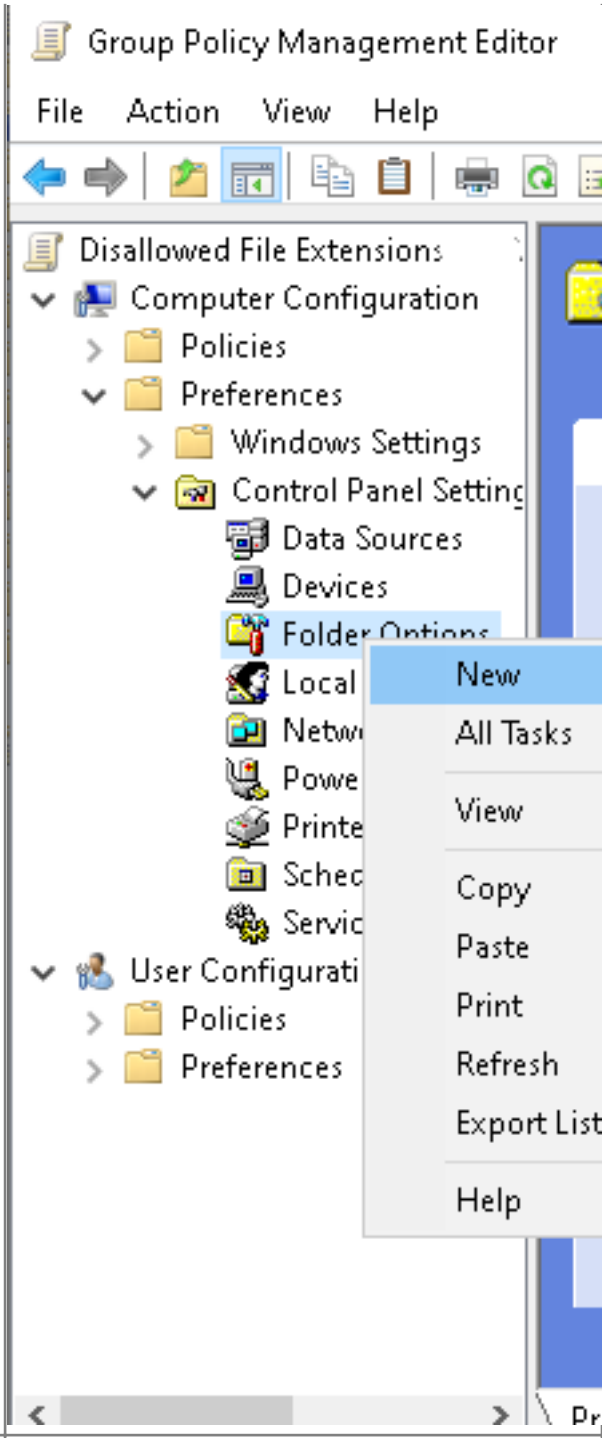
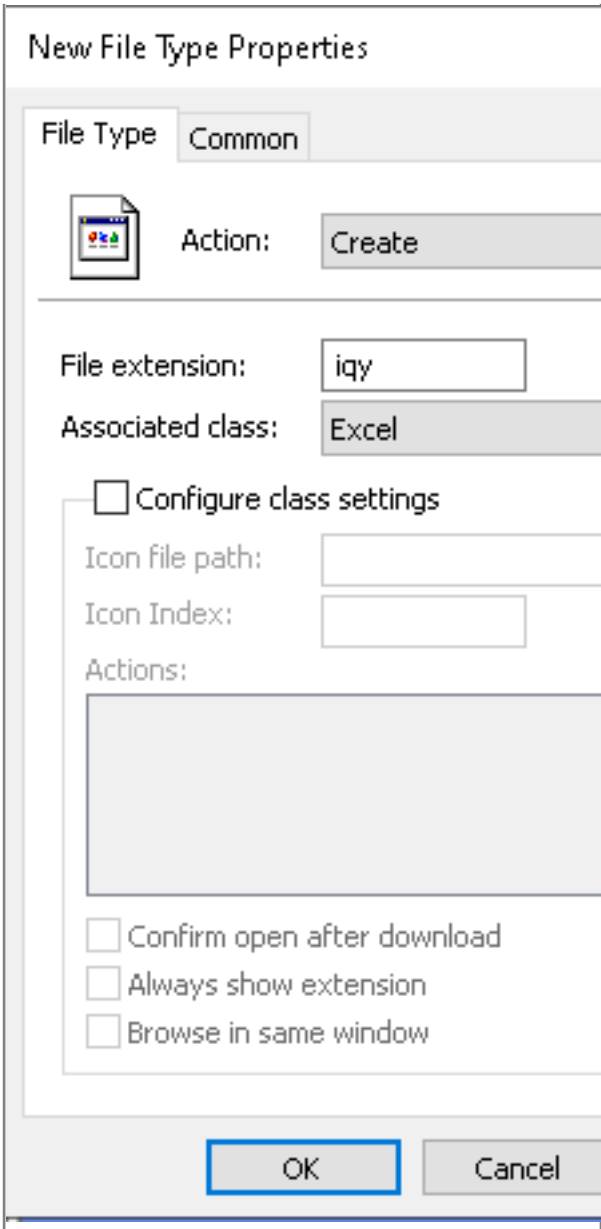
How to Restrict File Types Recognized as Possible Crypto Threats with Group Policy

Step #	Task	Screenshot
1	Log in to a PC that has **The Application That File Extension Uses** and **Domain Administrative Tools** installed.	
2	From the **Server Manager** Screen: Select **Tools > Group Policy Management**	
3	Right-click on **Group Policy Projects** and select **New**.	
4	Name the new GPO **Disallowed File Extensions** and then, click **OK**.	

		
Create the Disallowed File Extensions Policy		
5	In the right pane of the GPO management console, find the policy: "**Disallowed File Extensions**" and select **Edit**.	
6	Navigate to **Computer Configuration > Preferences > Control Panel Settings > Folder Options**. Right-click on it and choose **New > File Type** from the context menu.	

		
7	From there, click the **Actions** drop-down menu and choose the **Create** option. **File extension**: Enter the file extension block **Associated class:** Select the application	

	that uses this file. Click **OK** to Save. **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.***	
8	Apply the rule to the top of the domain infrastructure so it will apply to every device on the domain.	

Online URL: https://kb.naturalnetworks.com/article.php?id=509