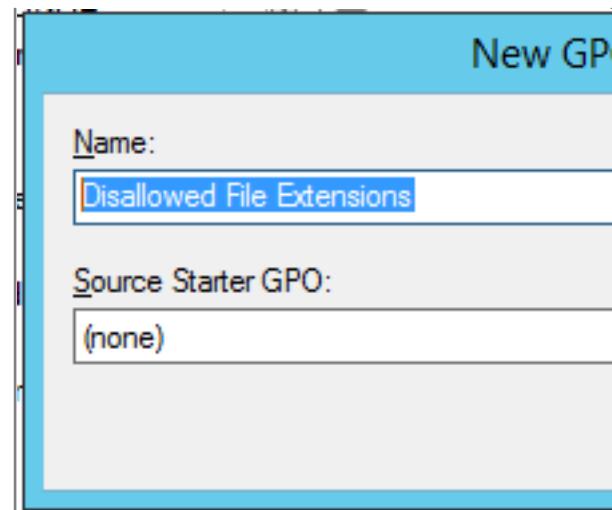


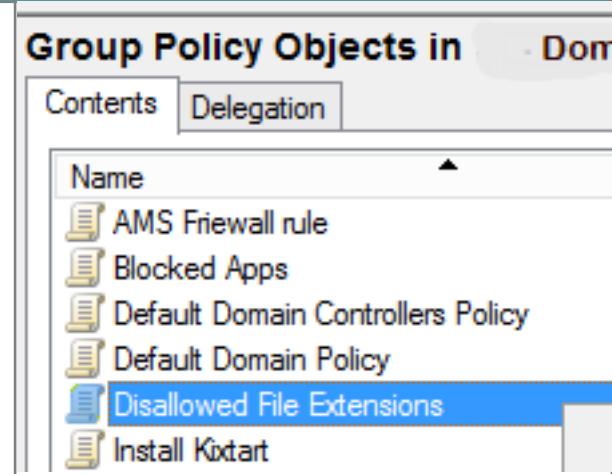
# How to Restrict File Types Recognized as Possible Crypto Threats with Group Policy

| 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:<br><br><b>Select Tools &gt; Group Policy Management</b>                            |            |
| 3      | Right-click on <b>Group Policy Projects</b> and select <b>New</b> .   |            |
| 4      | Name the new GPO <b>Disallowed File Extensions</b> and then, click <b>OK</b> .  |            |



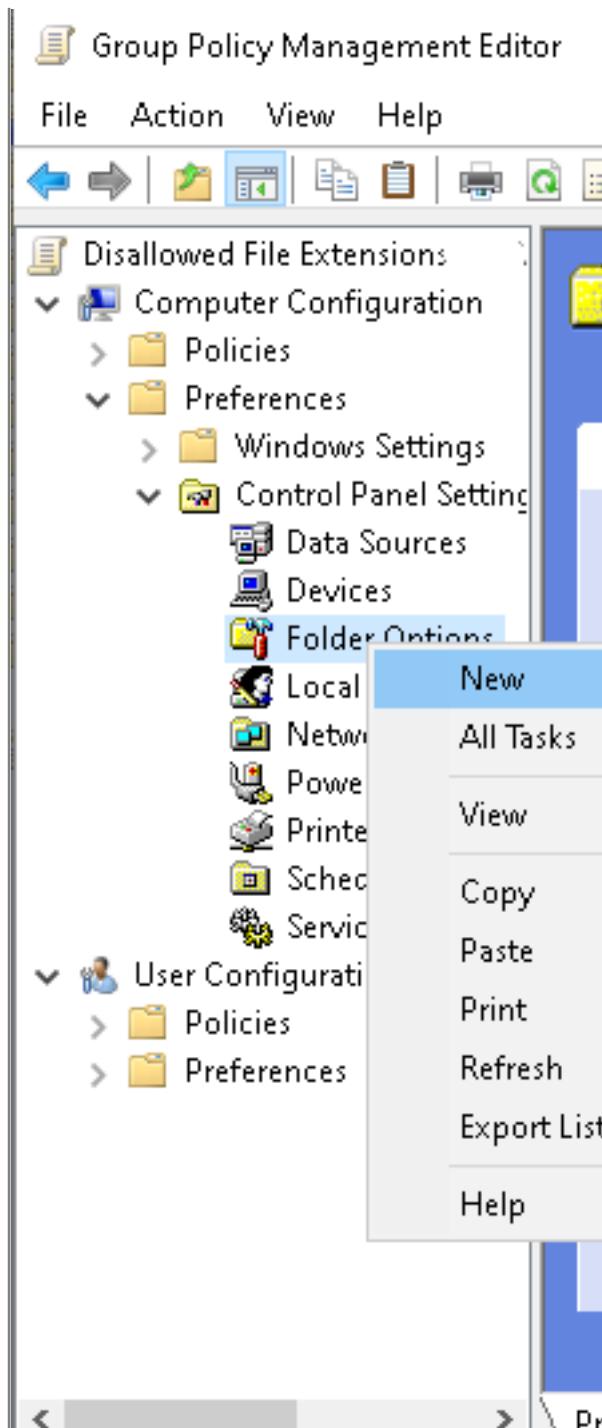
## Create the Disallowed File Extensions Policy

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

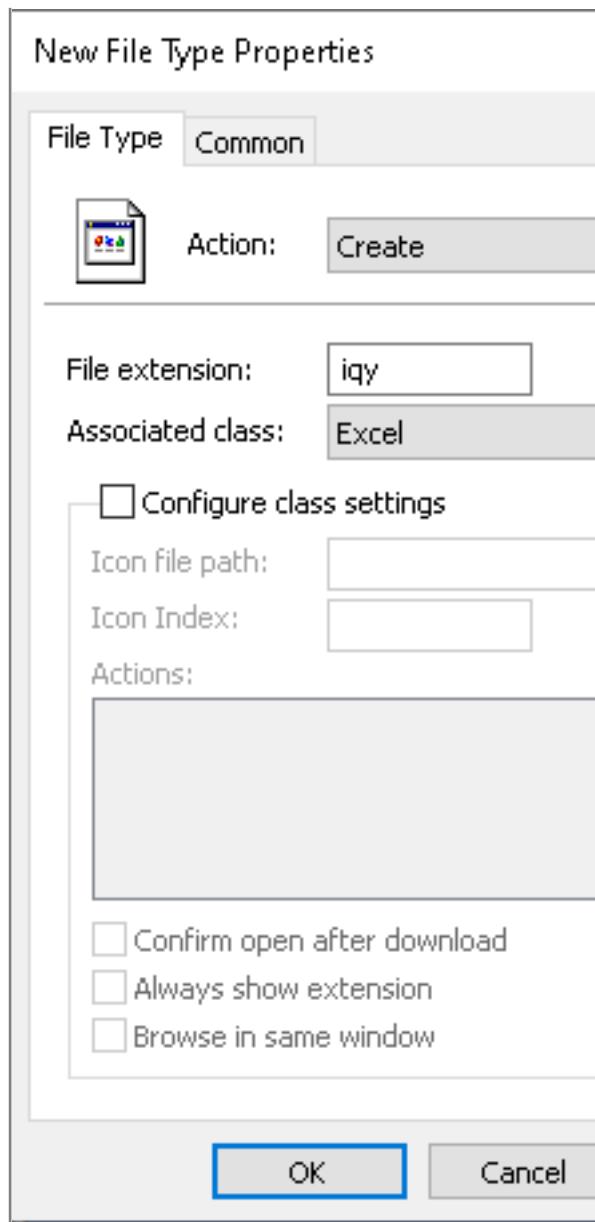
**Associated class:** Select the application

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>