

File Rules

File Rules allow you to create rules containing either block or allow actions for file extensions, file types or file expressions. File rules are assigned to Spam/Virus/File Policies which in turn are assigned to Internal Recipients.

Hermes SEG file rules are processed from the top down fashion. In other words, as a file rule gets processed, block/allow actions on the top of the rule get processed first. If a match is found then the action is taken and all further processing of the rule stops.

Default System File Rule

Hermes SEG already comes pre-configured with a **Default** System File Rule which is assigned to all the system Spam/Virus/File Policies. The Default System File Rule cannot be edited, it can only be viewed or copied in order to be used as a starting point in creating custom file rules (**Figure 1**).

Figure 1

File Rules

System File Rules

Rule Name	System Rule	Actions
Default	Yes	 

View Default File Rule

Note: You cannot make any changes to the Default file rule.


1. Under the **System File Rules** section click on the  icon under the **Actions** column of the **Default** file rule.
2. On the **View File Rule** page, you will see a listing of file types and corresponding actions for those file types (**Figure 2**).

Figure 2

View File Rule

Policy Name

Default

File Types and Actions

Double Extensions in File Name (exe,vbs,pif,scr,bat,cmd,com,cpl,dll,rtf) --> ban
Windows Class IDs --> ban
(application/x-msdownload) Windows DLL and EXE --> ban
(application/x-msdos-program) MS DOS application and executable --> ban
(application/hta) Microsoft HTML Application --> ban

Back to File Rules

3. Click on the **Back to File Rules** button on the bottom of the page to return to the File Rules page (**Figure 3**).

Figure 3

Back to File Rules

Create Custom File Rule by copying Default File Rule or any Custom File Rule

This method will allow you to copy the **Default** File Rule or any **Custom File Rule** (assuming there are existing custom file rules) and using it as a starting point for a new custom file rule.


1. Under the **System File Rules** section or the **Custom File Rules** (if there are already existing custom file rules) section, click on the  icon under the **Actions** column of the file rule you wish to copy. You will be redirected to the **Copy File Rule** page in order to create and customize a new file rule based on the file rule you choose (**Figure 4**).

Figure 4

Copy File Rule

Select File Type from the drop-down list below, select the Action to take and then click the ADD button. Add as many File Types as you need along with their associated actions. Once finished adding the File Types, enter a name for the rule you are creating on the bottom of the page and click ADD RULE button. If you make a mistake, click on the CANCEL ALL button below. File rules are processed from the top down fashion and once a match is found for a particular file type the assigned action is taken and processing of the rule stops. So the order the File Types and assigned Actions appear in a rule is important. For instance, if you wish to ban (.exe) Executable file types but you want to allow them within a (.zip) Zip Archive, you would add file type (.zip) Zip Archive first with an Allow action and then add (.exe) Executable file types with a Ban action.

File Type

=== HIGH RISK FILE EXTENSIONS ===

Action

☒

Ban

☐

Allow

Add

File Types and Actions to be added

Double Extensions in File Name (exe,vbs,pif,scr,bat,cmd,com,cpl,dll,rtf) --> ban

Windows Class IDs --> ban

(application/x-msdownload) Windows DLL and EXE --> ban

(application/x-msdos-program) MS DOS application and executable --> ban

(application/hta) Microsoft HTML Application --> ban

Delete

Move Up

Move Down

Cancel All

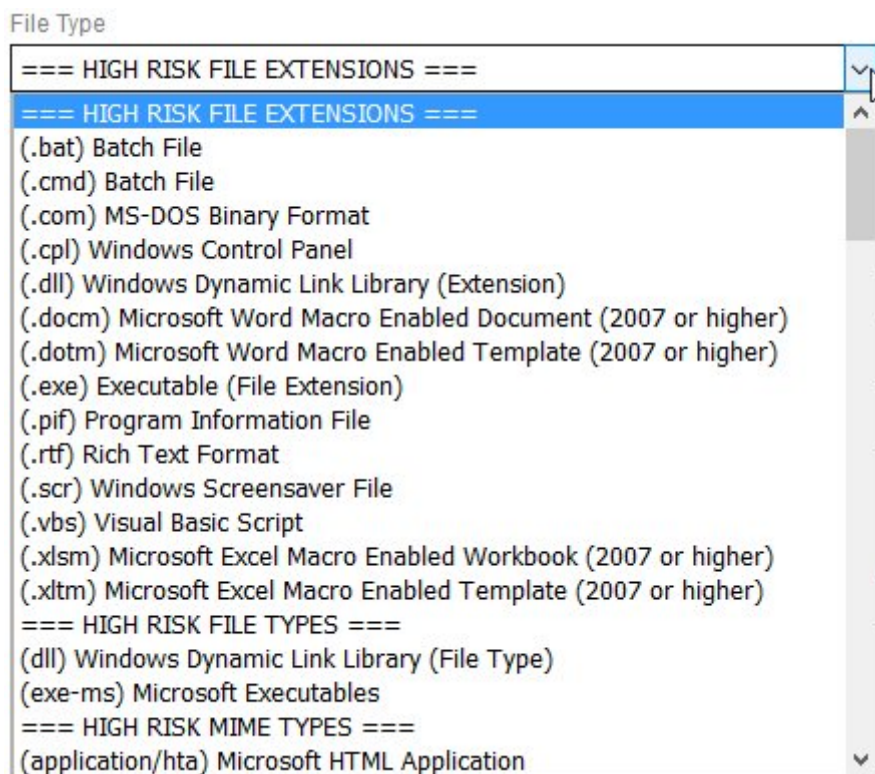
Enter a name for this File Rule

Add Rule

Add File Types

2. On the **Copy File Rule** page, under the **File Type** drop-down field, select a file type. Note that the **File Type** drop-down is organized in sections of HIGH-RISK FILE EXTENSIONS, HIGH RISK FILE TYPES, HIGH RISK MIME TYPES, FILE EXTENSIONS, FILE TYPES, MIME TYPES, OTHER TYPES and CUSTOM-EXPRESSIONS (**Figure 5**).

Figure 5



- Under the **Action** field, select either a **Ban** or **Allow** action and then click on the **Add** button (**Figure 6**).

Figure 6

The screenshot shows the 'File Type' dropdown menu set to '(xism) Microsoft Excel Macro Enabled Workbook (2007 or higher)'. Below it, the 'Action' field has two radio buttons: 'Ban' (selected) and 'Allow'. To the right of these fields is an 'Add' button.

- As you add File Types and their associated actions, they show up on the bottom of the **File Types and Actions** to be added section (**Figure 7**).

Figure 7

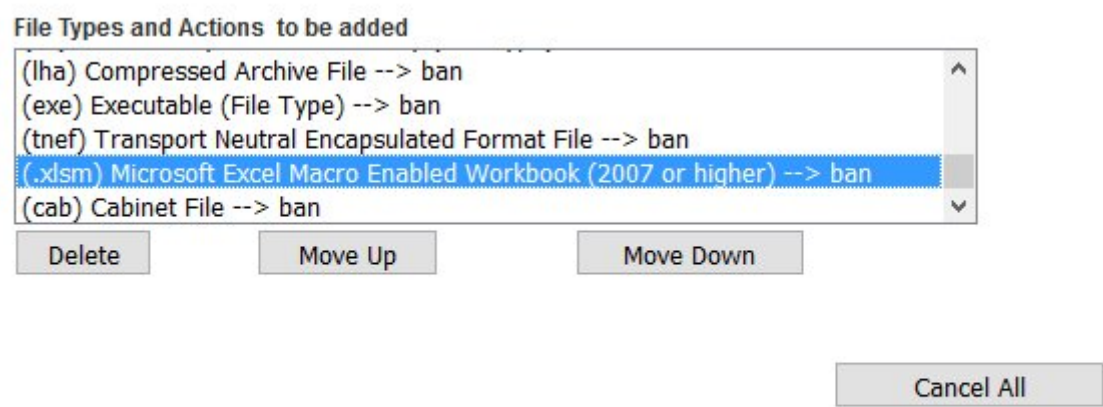
The screenshot shows a list titled 'File Types and Actions to be added'. The list contains four entries: (lha) Compressed Archive File --> ban, (exe) Executable (File Type) --> ban, (tnef) Transport Neutral Encapsulated Format File --> ban, and (cab) Cabinet File --> ban. The last entry, '(xism) Microsoft Excel Macro Enabled Workbook (2007 or higher) --> ban', is highlighted in blue. Below the list are three buttons: 'Delete', 'Move Up', and 'Move Down'.

- Continue adding File Types as needed.

Re-order File Types

- 6. Under the **File Types and Actions to be added** section, adjust the order the File Types that appear in the file rule by selecting each file type at a time the clicking on the **Move Up** or **Move Down** buttons as necessary to adjust the order (**Figure 8**).

Figure 8



✔ Success! File Type Moved Up

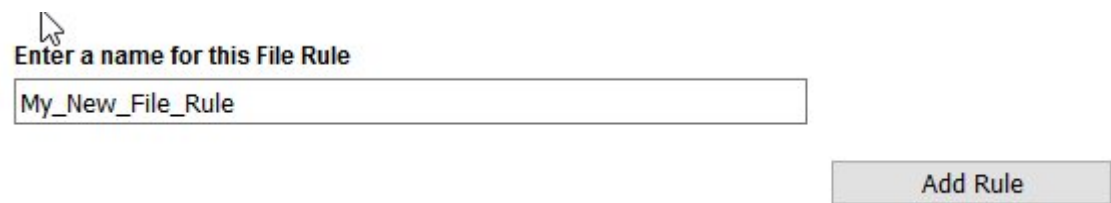
Delete File Types

- 7. Under the **File Types and Actions to be added** section, delete file types by selecting each file type at a time the clicking on delete button (**Figure 8**).

Create File Rule Name

















- 8. Under the **Enter a name for this File Rule** field, enter a unique name for this rule and click the **Add Rule** button below (**Figure 9**). You will be redirected back to the **File Rules** page.

Figure 9



- 9. Back at the **File Rules** page, the new rule will appear under the **Custom File Rules** section (**Figure 10**).

Figure 10

Custom File Rules		
Rule Name	System Rule	Actions
ban_old_office_files_ban_macro_enabled_new_office	No	  
Default-3-2-2010	No	  
...	No	  
...	No	  
My_New_File_Rule	No	  
...	No	  

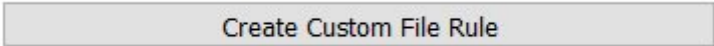
Create Custom File Rule

Create Custom File Rule

This method will allow you to create a new blank Custom File Rule.

- Under the **Custom File Rules** section, click on Create Custom File Rule button (**Figure 11**).

Figure 11



- You will be redirected to the **Create File Rule** page in order to create and customize a new file rule (**Figure 12**).

Figure 12

Create File Rule

Select File Type from the drop-down list below, select the Action to take and then click the ADD button. Add as many File Types as you need along with their associated actions. Once finished adding the File Types, enter a name for the rule you are creating on the bottom of the page and click ADD RULE button. If you make a mistake, click on the CANCEL ALL button below. File rules are processed from the top down fashion and once a match is found for a particular file type the assigned action is taken and processing of the rule stops. So the order the File Types and assigned Actions appear in a rule is important. For instance, if you wish to ban (.exe) Executable file types but you want to allow them within a (.zip) Zip Archive, you would add file type (.zip) Zip Archive first with an Allow action and then add (.exe) Executable file types with a Ban action.

File Type

=== HIGH RISK FILE EXTENSIONS ===

Action

☒ Ban

☐ Allow

Add

File Types and Actions to be added

No file type(s) found to be added..

Cancel All

Enter a name for this File Rule

Add Rule

Add File Types

3. On the **Create File Rule** page, under the **File Type** drop-down field, select a file type.
Note that the **File Type** drop-down is organized in sections of HIGH-RISK FILE EXTENSIONS, HIGH RISK FILE TYPES, HIGH RISK MIME TYPES, FILE EXTENSIONS, FILE TYPES, MIME TYPES, OTHER TYPES and CUSTOM-EXPRESSIONS (**Figure 13**).

Figure 13

File Type

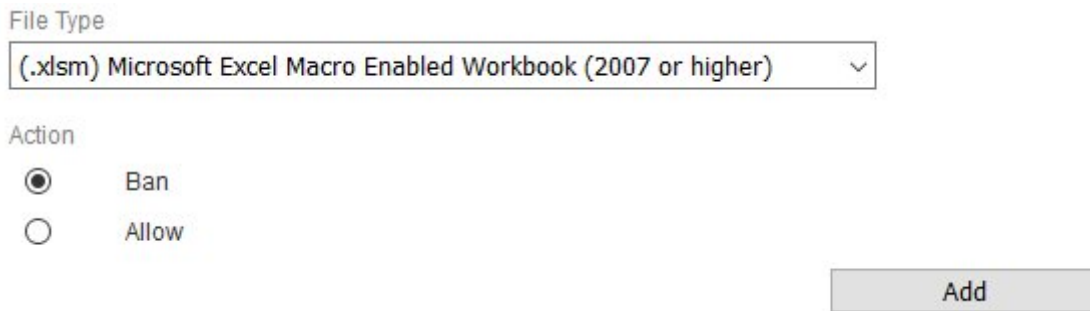
=== HIGH RISK FILE EXTENSIONS ===

=== HIGH RISK FILE EXTENSIONS ===

(.bat) Batch File
(.cmd) Batch File
(.com) MS-DOS Binary Format
(.cpl) Windows Control Panel
(.dll) Windows Dynamic Link Library (Extension)
(.docm) Microsoft Word Macro Enabled Document (2007 or higher)
(.dotm) Microsoft Word Macro Enabled Template (2007 or higher)
(.exe) Executable (File Extension)
(.pif) Program Information File
(.rtf) Rich Text Format
(.scr) Windows Screensaver File
(.vbs) Visual Basic Script
(.xlsm) Microsoft Excel Macro Enabled Workbook (2007 or higher)
(.xltm) Microsoft Excel Macro Enabled Template (2007 or higher)
=== HIGH RISK FILE TYPES ===
(dll) Windows Dynamic Link Library (File Type)
(exe-ms) Microsoft Executables
=== HIGH RISK MIME TYPES ===
(application/hta) Microsoft HTML Application

- Under the **Action** field, select either a **Ban** or **Allow** action and then click on the **Add** button (**Figure 14**).

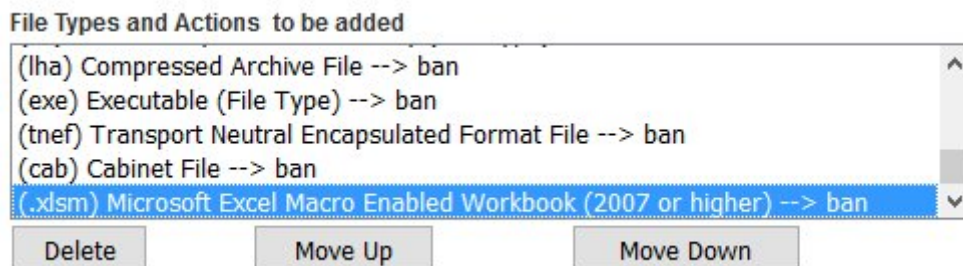
Figure 14



The screenshot shows a configuration window with two main sections. The first section, labeled 'File Type', contains a dropdown menu with the text '(.xism) Microsoft Excel Macro Enabled Workbook (2007 or higher)' and a downward arrow. The second section, labeled 'Action', contains two radio buttons: the first is selected and labeled 'Ban', and the second is unselected and labeled 'Allow'. To the right of these sections is a rectangular button labeled 'Add'.

- As you add File Types and their associated actions, they show up on the bottom of the **File Types and Actions to be added** section (**Figure 15**).

Figure 15



The screenshot shows a list titled 'File Types and Actions to be added'. The list contains five entries, each with a file extension in parentheses, a file name, and an action: '(lha) Compressed Archive File --> ban', '(exe) Executable (File Type) --> ban', '(tnef) Transport Neutral Encapsulated Format File --> ban', '(cab) Cabinet File --> ban', and '(.xism) Microsoft Excel Macro Enabled Workbook (2007 or higher) --> ban'. The last entry is highlighted in blue. Below the list are three buttons: 'Delete', 'Move Up', and 'Move Down'.

- Continue adding File Types as needed.

Re-order File Types

- Under the **File Types and Actions to be added** section, adjust the order the File Types that appear in the file rule by selecting each file type at a time the clicking on the **Move Up** or **Move Down** buttons as necessary to adjust the order (**Figure 16**).

Figure 16

File Types and Actions to be added

(lha) Compressed Archive File --> ban

(exe) Executable (File Type) --> ban

(tnef) Transport Neutral Encapsulated Format File --> ban

(.xlsm) Microsoft Excel Macro Enabled Workbook (2007 or higher) --> ban

(cab) Cabinet File --> ban

Delete

Move Up

Move Down

Cancel All

✔ Success! File Type Moved Up

Delete File Types

8. Under the **File Types and Actions to be added** section, delete file types by selecting each file type at a time the clicking on delete button (**Figure 16**).

Create File Rule Name

9. Under the **Enter a name for this File Rule** field, enter a unique name for this rule and click the **Add Rule** button below (**Figure 17**). You will be redirected back to the **File Rules** page.

Figure 17

Enter a name for this File Rule



















My_New_File_Rule

Add Rule

10. Back at the **File Rules** page, the new rule will appear under the **Custom File Rules** section (**Figure 18**).

Figure 18

Custom File Rules

Rule Name	System Rule	Actions
ban_old_office_files_ban_macro_enabled_new_office	No	  
Default-3-2-2010	No	  
...file-rule	No	  
...file-rule	No	  
My_New_File_Rule	No	  
...	No	  

Create Custom File Rule

Edit Custom File Rule

Note: ONLY Custom File Rules can be edited.


1. Under the **Custom File Rules** section, click on the  icon of the Custom File Rule you wish to edit.
2. You will be redirected to the **Edit File Rule** page in order to customize the file rule (**Figure 19**).

Figure 19

Edit File Rule

Select File Type from the drop-down list below, select the Action to take and then click the ADD button. Add as many File Types as you need along with their associated actions. Once finished adding the File Types, enter a name for the rule you are creating on the bottom of the page and click ADD RULE button. If you make a mistake, click on the CANCEL ALL button below. File rules are processed from the top down fashion and once a match is found for a particular file type the assigned action is taken and processing of the rule stops. So the order the File Types and assigned Actions appear in a rule is important. For instance, if you wish to ban (.exe) Executable file types but you want to allow them within a (.zip) Zip Archive, you would add file type (.zip) Zip Archive first with an Allow action and then add (.exe) Executable file types with a Ban action.

File Type

=== HIGH RISK FILE EXTENSIONS ===

Action

☒ Ban

☐ Allow

Add

File Types and Actions to be updated

Double Extensions in File Name (exe,vbs,pif,scr,bat,cmd,com,cpl,dll,rtf) --> ban

Windows Class IDs --> ban

(application/x-msdownload) Windows DLL and EXE --> ban

(application/x-msdos-program) MS DOS application and executable --> ban

(application/hta) Microsoft HTML Application --> ban

Delete

Move Up

Move Down

Cancel All

Name of the File Rule

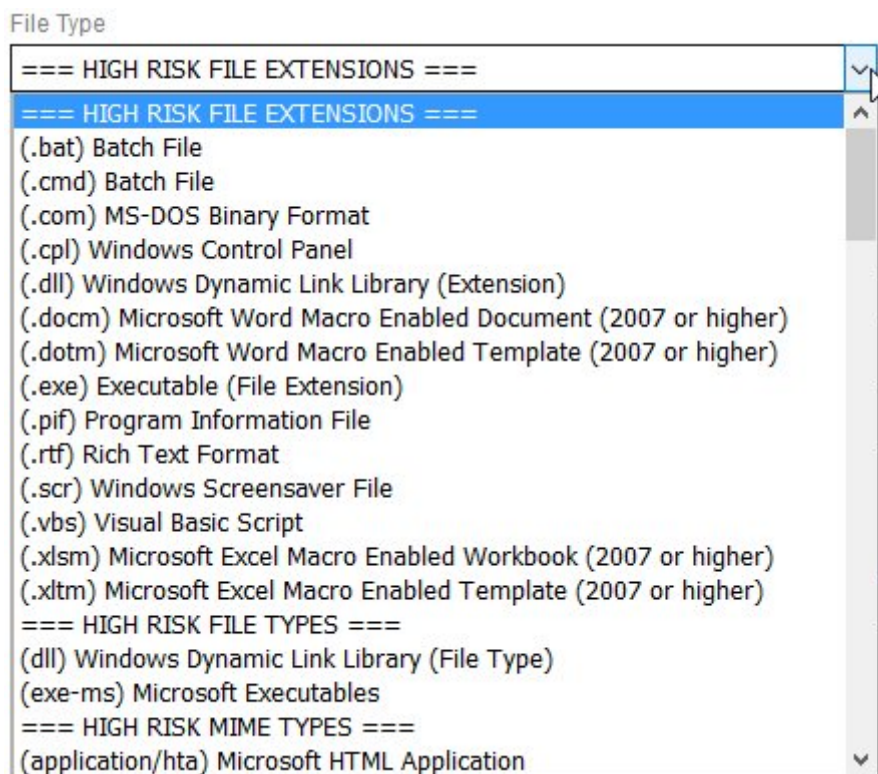
My_New_File_Rule

Save Rule

Add File Types

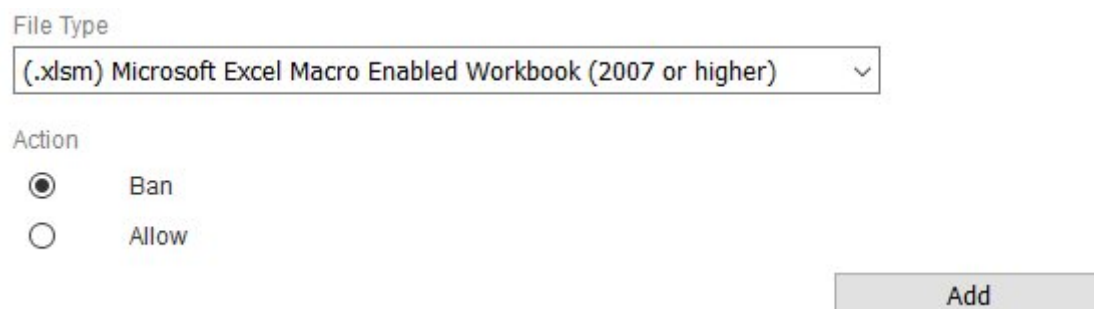
3. On the **Edit File Rule** page, under the **File Type** drop-down field, select a file type. Note that the **File Type** drop-down is organized in sections of HIGH-RISK FILE EXTENSIONS, HIGH RISK FILE TYPES, HIGH RISK MIME TYPES, FILE EXTENSIONS, FILE TYPES, MIME TYPES, OTHER TYPES and CUSTOM-EXPRESSIONS (**Figure 20**).

Figure 20



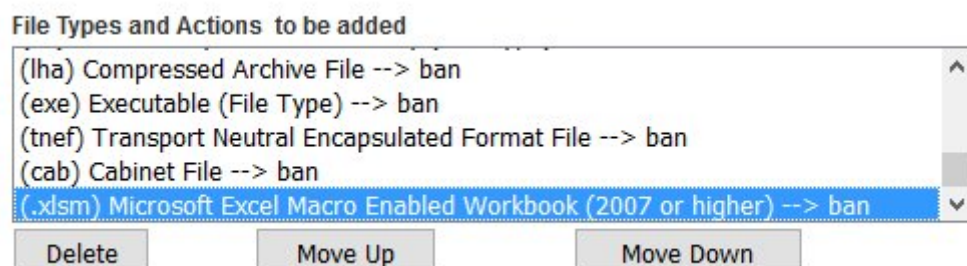
4. Under the **Action** field, select either a **Ban** or **Allow** action and then click on the **Add** button (**Figure 21**).

Figure 21



5. As you add File Types and their associated actions, they show up on the bottom of the **File Types and Actions** to be added section (**Figure 22**).

Figure 22

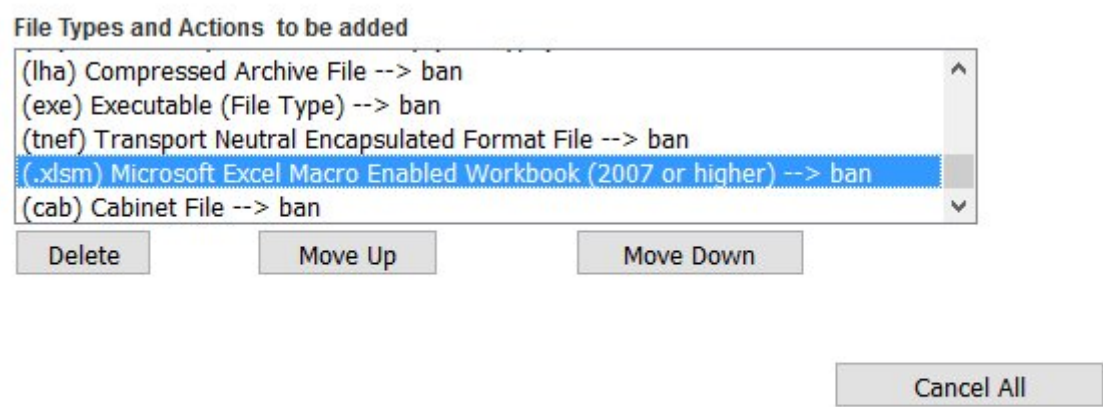


6. Continue adding File Types as needed.

Re-order File Types

- 7. Under the **File Types and Actions to be added** section, adjust the order the File Types that appear in the file rule by selecting each file type at a time the clicking on the **Move Up** or **Move Down** buttons as necessary to adjust the order (**Figure 23**).

Figure 23



✔ Success! File Type Moved Up

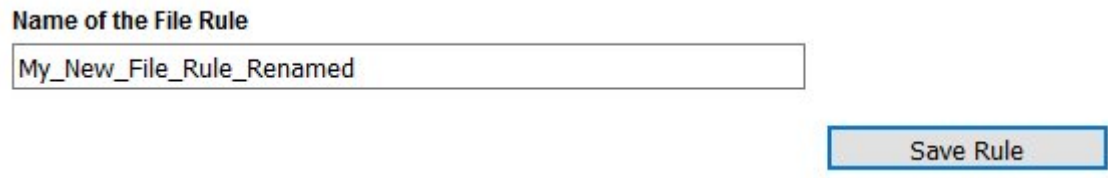
Delete File Types

- 8. Under the **File Types and Actions to be added** section, delete file types by selecting each file type at a time the clicking on delete button (**Figure 23**).

Edit File Rule Name

- 9. Under the **Name of the File Rule** field, enter a unique name for this rule and click the **Save Rule** button below (**Figure 24**). You will be redirected back to the **File Rules** page.


















Figure 24



- 10. Back at the **File Rules** page, the new rule will appear under the **Custom File Rules** section (**Figure 25**).

Figure 25

Custom File Rules

Rule Name	System Rule	Actions
ban_old_office_files_ban_macro_enabled_new_office	No	  
Default 2/2/2013	No	  
Custom file-rule	No	  
Custom file-rule	No	  
My_New_File_Rule_Renamed	No	  
Custom file-rule	No	  

Create Custom File Rule

Delete Custom File Rule

Note: ONLY Custom File Rules that are NOT associated with with a File/Virus/Spam Policy can be deleted. When deleting a Custom File Rule, the system will NOT prompt you to confirm, it will be deleted immediately.


1. Under the **Custom File Rules** section, click on the  icon of the Custom File Rule you wish to delete.
2. The system will delete the Custom File Rule and re-direct you back to the File Rules page (**Figure 26**)

Figure 26

File Rules

System File Rules

Rule Name	System Rule	Actions
Default	Yes	 

✓ File Rule Successfully Deleted!!

Revision #1

Created 2 January 2021 14:43:39 by Dino Edwards

Updated 20 May 2023 22:22:35 by Dino Edwards