Attachment Management in Mimecast

Last Modified on 23/01/2020 9:54 am GMT

Attachment Management is the set of policies that determine which file types are allowed through by email.

Mimecast provides you with a default definition for determining what attachment types should be handled. This covers the most common file types you will encounter.

You can choose to have Mimecast perform one of the following actions for attachments:

Allow – The attachment is delivered as normal.
Link – The attachment is removed from the email and replaced with a link to download the file.
Hold – The email is held by Mimecast, requiring it to be released before them email is delivered to the recipient
Block – The email is delivered without the attachment

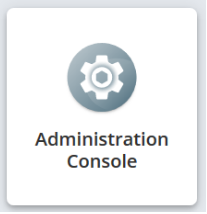
You can also have an action performed based on the size of the file. For example blocking PDF files over 10MB.

Detections for Attachment Management can be set on both file extension and MIME type.

Definition

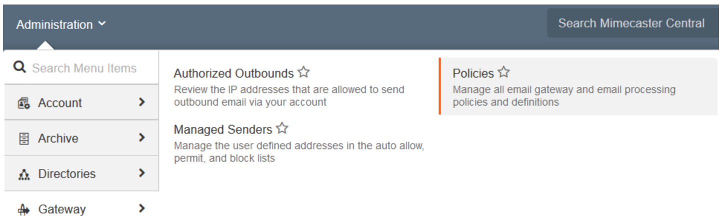
The Attachment Definition is the settings that will be applied when a policy is triggered. You must configure the Definition first.

1. Log into your Mimecast Account at https://login.mimecast.com



2. Select **Administration Console**

3. Go to **'Administration > Gateway > Policies'**

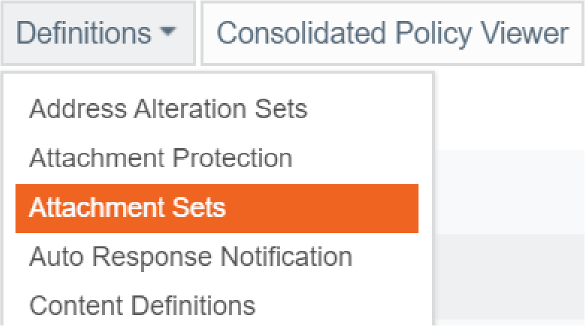


Review the IP addresses that are allowed to send outbound email via your account

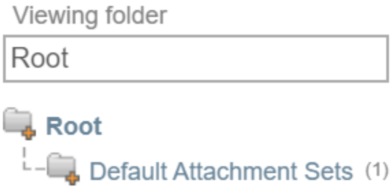
Manage the user defined addresses in the auto allow, permit, and block lists

Manage all email gateway and email processing policies and definitions

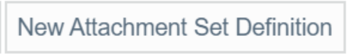
4. From the **Definitions** dropdown, select **Attachment Sets**



5. Select the **Default Attachment Sets** folder



6. Select New Attachment Set Definition



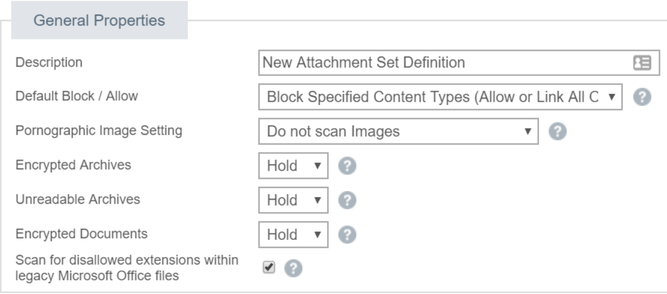
7. Set the name (**Description**) for the Definition

8. Set the General Properties for the definition:

Default Block / Allow:
Determines if the definition actions as a Blacklist (allow all but selected items) or a Whitelist (allow only selected items)

Pornographic Image Setting:
Determines if images should be scanned for pornographic

content and at what certainty it will be triggered. These will be held if detected when enabled.



General Properties

Description	New Attachment Set Definition
Default Block / Allow	Block Specified Content Types (Allow or Link All C
Pornographic Image Setting	Do not scan Images
Encrypted Archives	Hold
Unreadable Archives	Hold
Encrypted Documents	Hold
Scan for disallowed extensions within legacy Microsoft Office files	☑

Encrypted Archives: How to handle password protected archive (.zip, .rar etc.) files.

Unreadable Archives: How to handle archive files that could not be read.

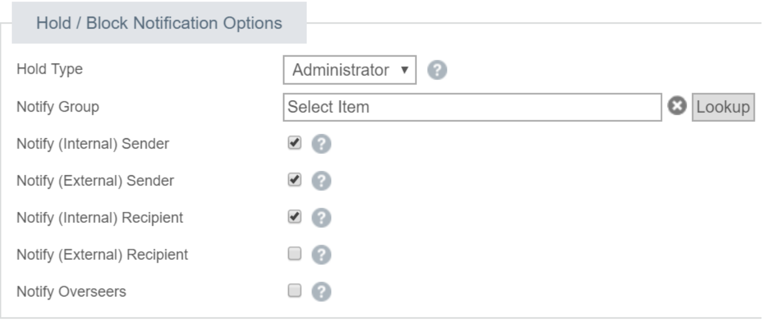
Encrypted Documents: How to handle password protected Office files

Scan for disallowed extensions within legacy Microsoft Office files: Determines if legacy Microsoft Office embedded files should be checked

9. Set the Hold / Block Notification Options:

   Hold Type: Determines who can release emails that have been held by this definition (Hold options applied in General Properties will always be an Admin Hold)

   Moderator Group: The group of users who can release emails held by this definition when the Hold Type is set to Moderator or User



Hold / Block Notification Options

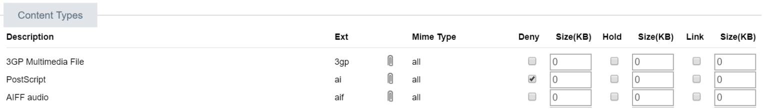
Hold Type	Administrator ▾
Notify Group	Select Item
Notify (Internal) Sender	☑
Notify (External) Sender	☑
Notify (Internal) Recipient	☑
Notify (External) Recipient	□
Notify Overseers	□

Notify Group: The group of users who will receive a notification when this definition is used (in addition to the below options)

Notify (Internal/External) Sender/Recipient: Determines if who should receive a notification when this definition is triggered

10. Set the actions for Content Types

Note: If a Size is set of more than zero, that action will only apply if the file size of the attachment exceeds that size.



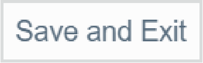
Content Types

Description	Ext		Mime Type	Deny	Size(KB)	Hold	Size(KB)	Link	Size(KB)
3GP Multimedia File	3gp		all	□	0	□	0	□	0
PostScript	ai		all	☑	0	□	0	□	0
AIFF audio	aif		all	□	0	□	0	□	0

Note: You can search for a specific file type using the search option at the top right of the page.

Note: You can change which items show in the list using the **View** dropdown at the top of the page.

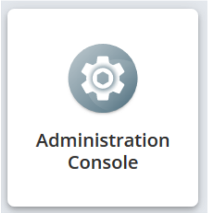
11. Press **Save & Exit**



Policy

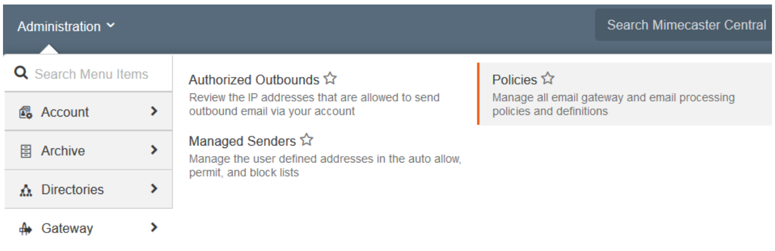
Once you have created your definition, you will need to create an accompanying policy to determine when it is applied.

1. Log into your Mimecast Account at https://login.mimecast.com



2. Select **Administration Console**

3. Go to **'Administration > Gateway > Policies'**

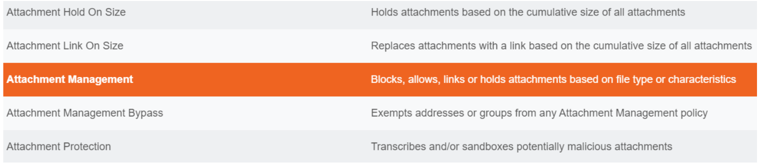


Authorized Outbounds: Review the IP addresses that are allowed to send outbound email via your account

Managed Senders: Manage the user defined addresses in the auto allow, permit, and block lists

Policies: Manage all email gateway and email processing policies and definitions

4. Click into **Attachment Management**

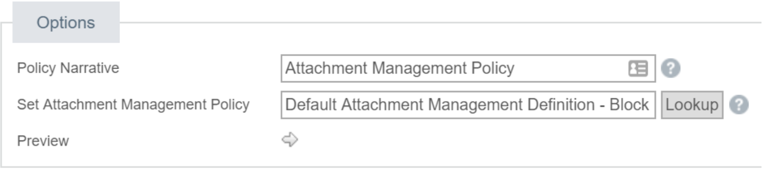


Attachment Hold On Size	Holds attachments based on the cumulative size of all attachments
Attachment Link On Size	Replaces attachments with a link based on the cumulative size of all attachments
Attachment Management	**Blocks, allows, links or holds attachments based on file type or characteristics**
Attachment Management Bypass	Exempts addresses or groups from any Attachment Management policy
Attachment Protection	Transcribes and/or sandboxes potentially malicious attachments

5. Select **New Policy**

6. Give the policy a name **(Policy Narrative)**

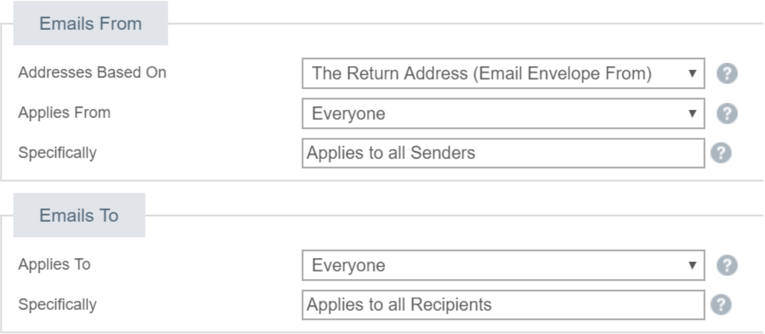
7. Set **Set Attachment Management Policy** to definition you created using the **Lookup** button



Policy Narrative	Attachment Management Policy
Set Attachment Management Policy	Default Attachment Management Definition - Block
Preview	

Note: When using the definition lookup, you will need to select the folder the definition is located in and use the Select option. Clicking into the definition on this screen will take you to the editing screen for it.

8. Set the scope for the policy under **Emails From** and **Emails To**



Addresses Based On	The Return Address (Email Envelope From)
Applies From	Everyone
Specifically	Applies to all Senders

Applies To	Everyone
Specifically	Applies to all Recipients

9. Press **Save & Exit**

Only one Attachment Management Policy will apply to an email. If you need to ensure a particular policy is picked, you should enable the **Policy Override** option within the policy.