# Attachment Protection in Mimecast

Last Modified on 23/01/2020 9:59 am GMT

Part of the Targeted Threat Protection (TTP) policies, Attachment Protection is designed to provide additional protection against malicious attachments in emails. The policies provide two different services, including a hybrid between them, of:

- **Attachment Sandboxing:** Mimecast will open the attachment files in a sandbox environment, checking for malicious activity before passing it onto the user.
- **Attachment Transcribing**: Converts supported file types to a 'safer' version of the file. This can include converting word documents to PDF or a plain DOCX file to remove potentially malicious content, such as Macros. Users can request the original files if enabled.

If your Mimecast licencing includes Internal Email Protect (IEP), you will be able to configure these policies for your internal and outbound emails. Otherwise you will only have the options for inbound emails.

The Attachment Protection policies work alongside the Attachment Management policies. If troubleshooting issues with attachments, you should check both policies if they are both enabled.

## User Experience

With Attachment Protection, users will generally only see the policy in action when Transcribing is being used. The Sandbox service will run before users receive the email, with the option to notify users if an attachment is held.

Below are the experiences users will have under the different settings.

**Safe File**: Users will receive a 'safe' version of attachments that have been converted by the Transcribing service. The file type received will be determined by the definition.

**Safe File with On-Demand Sandbox**: Users will receive a 'safe' version of attachments that have been converted by the Transcribing service. The file type received will be determined by the definition. Alongside the transcribed attachment will be a notification that allows the user to request the original. If the original is requested by the user, it will be scanned by the Attachment Sandbox service before the original email, with the original attachments will be delivered to the user. Emails with potentially malicious content in attachments will be held by Mimecast.

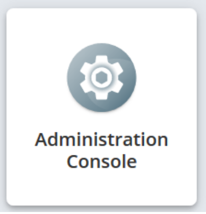
**Preemptive Sandbox:** Attachments will be sent to the Attachment Sandbox service on arrival. Emails with potentially malicious content in attachments will be held by Mimecast.

**Dynamic Configuration:** Users will receive a 'safe' version of attachments that have been converted by the Transcribing service. The file type received will be determined by the definition. Alongside the transcribed attachment will be a notification that allows the user to request the original. If the original is requested by the user, it will be scanned by the Attachment Sandbox service before the original email, with the original attachments will be delivered to the user. Emails with potentially malicious content in attachments will be held by Mimecast. Users can opt to 'trust' a sender, so that attachments from that sender go straight to the Attachment Sandbox, rather than transcribed.

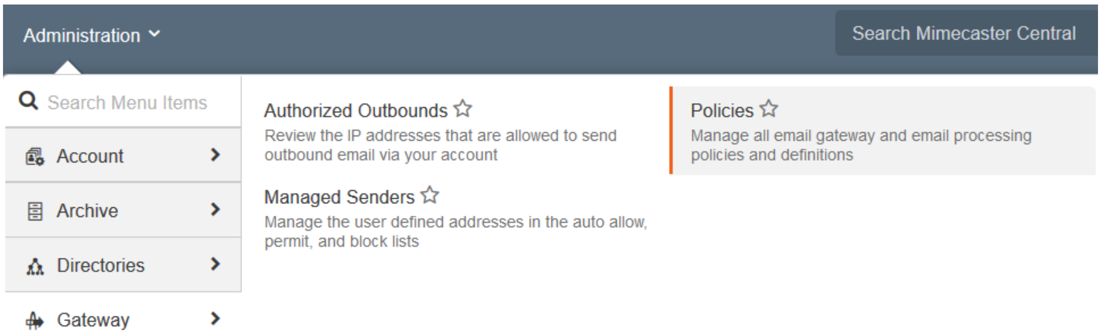
## Definition

New Mimecast accounts will have a definition for this service already in place. This can be used to get started, or you can create your own definition.

1. Log into your Mimecast Account at https://login.mimecast.com
2. Select **Administration Console**



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



Administration

Search Mimecaster Central

Search Menu Items

Account

Archive

Directories

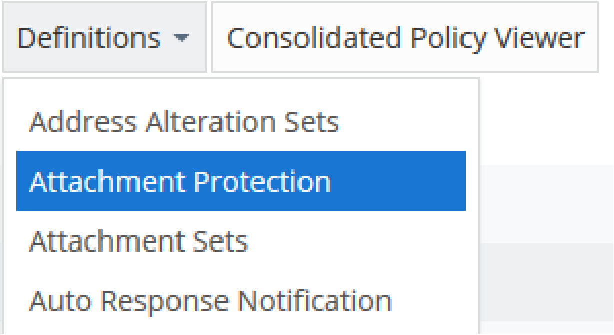
Gateway

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. From the **Definitions** dropdown, select **Attachment Protection**



Definitions ▾

Consolidated Policy Viewer

Address Alteration Sets

Attachment Protection

Attachment Sets

Auto Response Notification

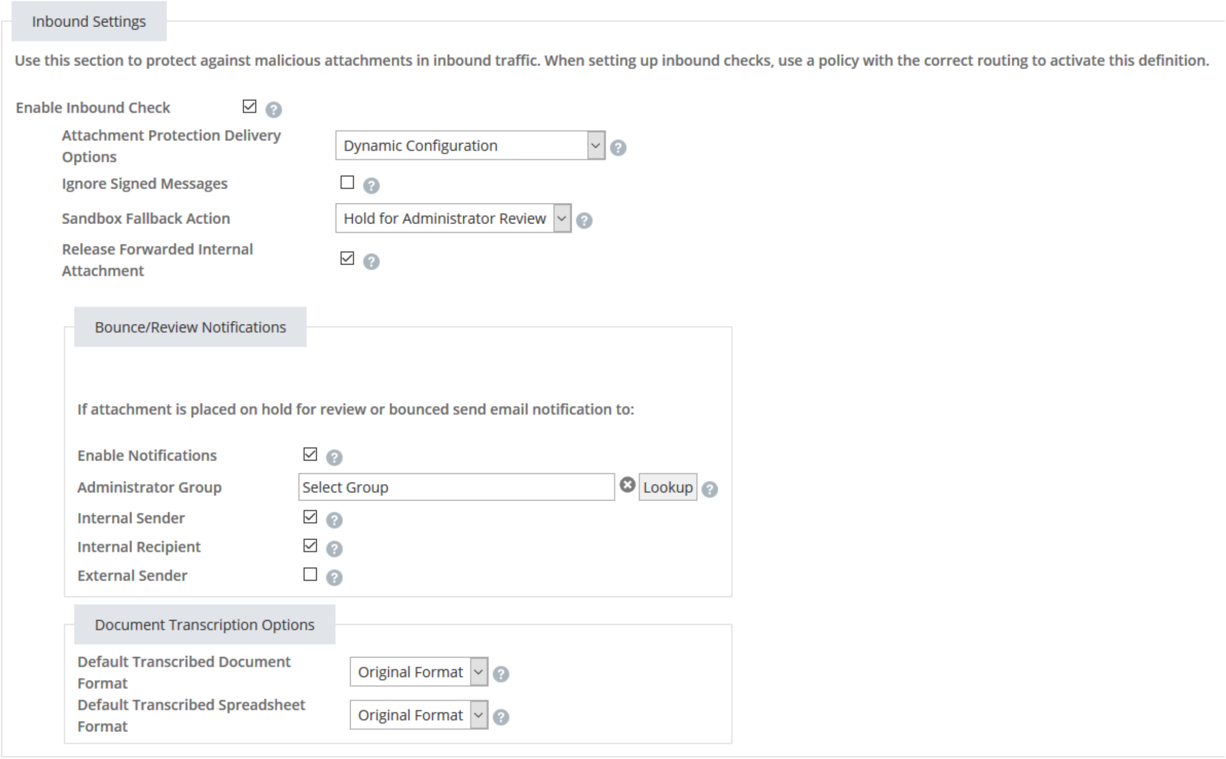
5. Select **New Definition** or click into the Default policy
6. Set the Name (**Definition Narrative**) for the Definition
7. Select the option to use for this Definition (see User Experience)
8. Enable Notifications if you want a particular group or the Sender/Recipient to be notified when an inbound email is held or rejected by this policy.

## Sandbox Settings

9. Select a **Sandbox Fallback Action** for when the attachment cannot be processed by the Sandbox service:
   a. **Hold for Administrator Review**: The email is held by Mimecast. It must be released by a Mimecast admin.
   b. **Bounce**: The email is rejected.
10. Set the option for **Release Forwarded Internal Attachment.** This allows an email to be forwarded to another internal recipient and still allow the attachment to be released by the new recipient.

## Transcribing Settings

11. Select if you want to **Ignore Signed Messages**
    1. If this is enabled, emails with digital signatures will not have the definition apply in order to maintain the digital signature.
12. Select the file type to convert Documents and Spreadsheets to



Inbound Settings

Use this section to protect against malicious attachments in inbound traffic. When setting up inbound checks, use a policy with the correct routing to activate this definition.

Enable Inbound Check ☑

Attachment Protection Delivery Options: Dynamic Configuration

Ignore Signed Messages ☐

Sandbox Fallback Action: Hold for Administrator Review

Release Forwarded Internal Attachment ☑

Bounce/Review Notifications

If attachment is placed on hold for review or bounced send email notification to:

Enable Notifications ☑

Administrator Group: Select Group

Internal Sender ☑

Internal Recipient ☑

External Sender ☐

Document Transcription Options

Default Transcribed Document Format: Original Format

Default Transcribed Spreadsheet Format: Original Format

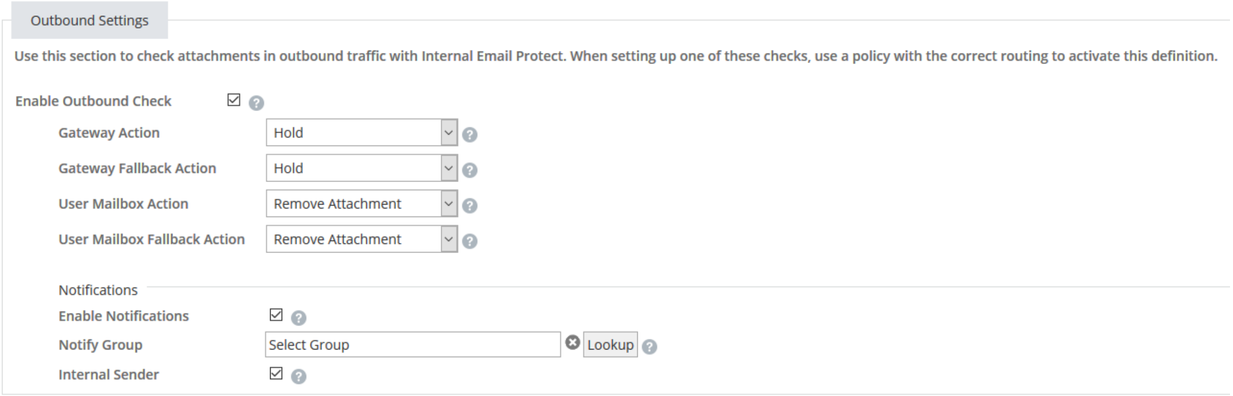
## Outbound Settings

This section will not appear if you don't have Internal Email Protect. User Mailbox Actions require a Server Connection to be configure to process the action.

13. Select to **Enable Outbound Check**
14. Select the settings to use for outbound checks
    a. **Gateway Action**: The action performed by Mimecast to the email in transit when malicious content is detected.
    b. **Gateway Fallback Action**: The action performed by Mimecast to the email in transit when it can't be processed.
    c. **User Mailbox Action**: The action performed by Mimecast to the email in the user's mailbox when malicious content is detected.
    d. **User Mailbox Fallback Action**: The action performed by Mimecast to the

email in the user’s mailbox when it can’t be processed.

15. Enable Notifications if you want a group or the Sender/Recipient to be notified when an outbound email is held or rejected by this policy.



Outbound Settings

Use this section to check attachments in outbound traffic with Internal Email Protect. When setting up one of these checks, use a policy with the correct routing to activate this definition.

| | |
|---|---|
| Enable Outbound Check | ☑ |
| Gateway Action | Hold |
| Gateway Fallback Action | Hold |
| User Mailbox Action | Remove Attachment |
| User Mailbox Fallback Action | Remove Attachment |

Notifications

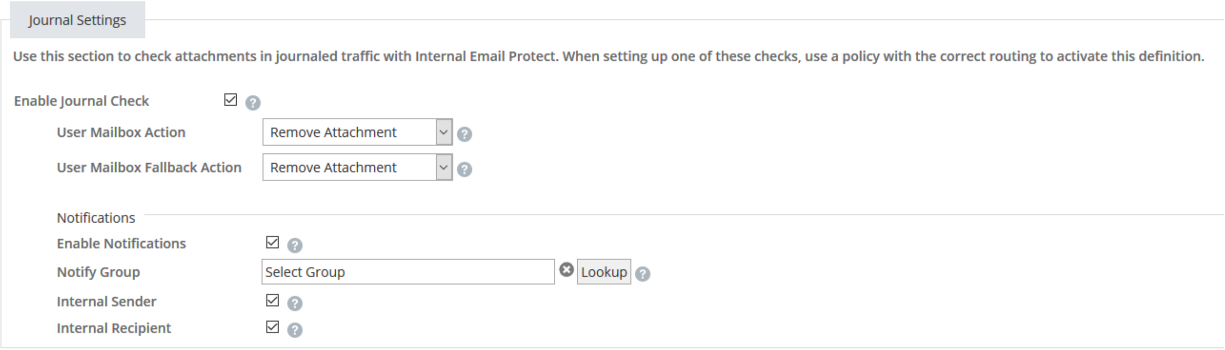
| | |
|---|---|
| Enable Notifications | ☑ |
| Notify Group | Select Group |
| Internal Sender | ☑ |

## Journal Settings

This section will not appear if you don’t have Internal Email Protect. User Mailbox Actions require a Server Connection to be configure to process the action. You must have a Journal Rule configured to send emails to Mimecast for this to apply.

These settings will apply to internal email that does not normally route outside of your email infrastructure.

16. Select to **Enable Journal Check**
17. Select the settings to use for internal checks
    a. **User Mailbox Action:** The action performed by Mimecast to the email in the user’s mailbox when malicious content is detected.
    b. **User Mailbox Fallback Action:** The action performed by Mimecast to the email in the user’s mailbox when it can’t be processed.
18. Enable Notifications if you want a group or the Sender/Recipient to be notified when an internal email is held or rejected by this policy.



Journal Settings

Use this section to check attachments in journaled traffic with Internal Email Protect. When setting up one of these checks, use a policy with the correct routing to activate this definition.

Enable Journal Check ☑

User Mailbox Action: Remove Attachment

User Mailbox Fallback Action: Remove Attachment

Notifications

Enable Notifications ☑

Notify Group: Select Group

Internal Sender ☑

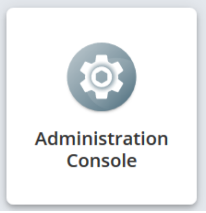
Internal Recipient ☑

19. Press **Save and Exit**

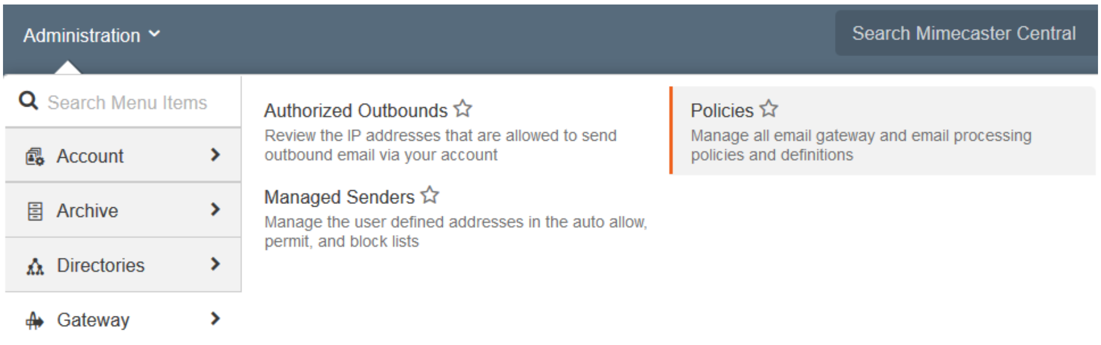
# Policy

Once you have your definition, you will need to set a policy for when Attachment Protection applies.

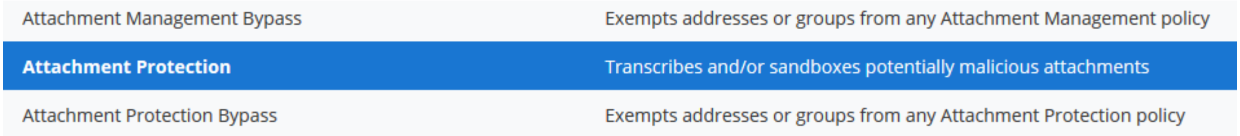
1. Log into your Mimecast Account at https://login.mimecast.com
2. Select **Administration Console**



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

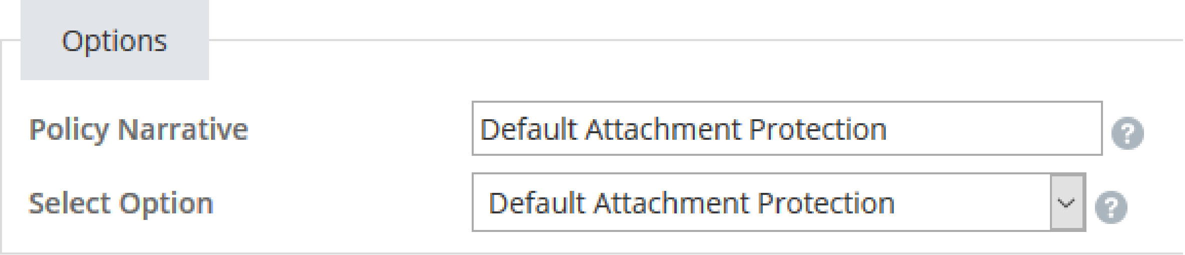

Administration
Search Mimecaster Central
Search Menu Items
Account
Archive
Directories
Gateway
Authorized Outbounds
Review the IP addresses that are allowed to send outbound email via your account
Managed Senders
Manage the user defined addresses in the auto allow, permit, and block lists
Policies
Manage all email gateway and email processing policies and definitions

4. Select **Attachment Protection** from the policies list



| | |
|---|---|
| Attachment Management Bypass | Exempts addresses or groups from any Attachment Management policy |
| **Attachment Protection** | Transcribes and/or sandboxes potentially malicious attachments |
| Attachment Protection Bypass | Exempts addresses or groups from any Attachment Protection policy |

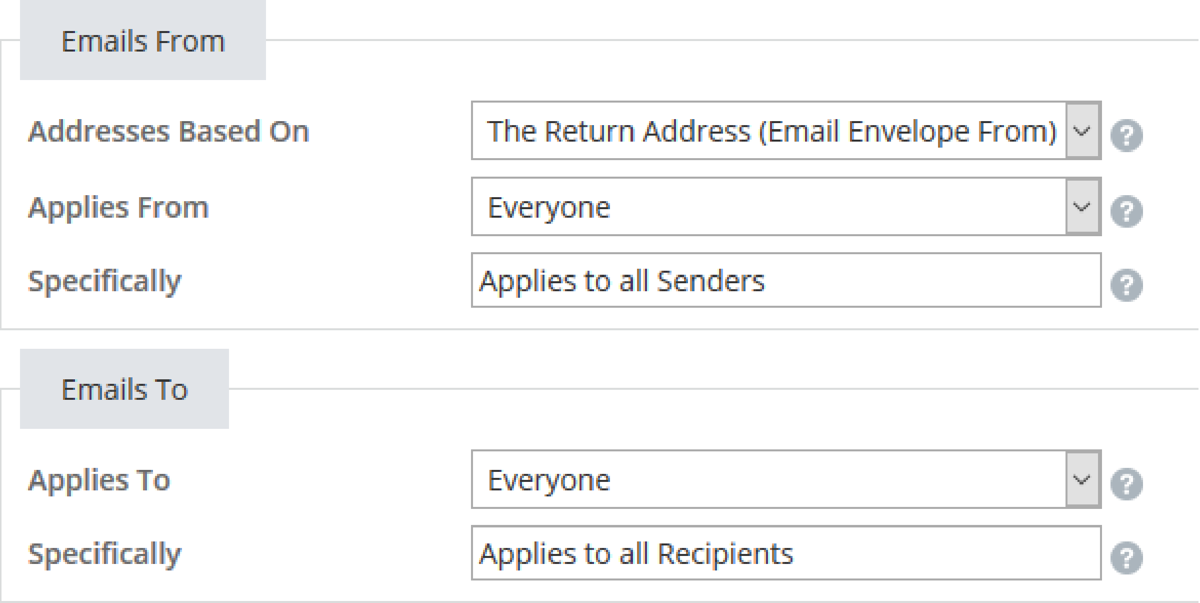
5. Select **New Policy**
6. Give the policy a name (**Policy Narrative**)
7. Set the Definition you created



Options

| | |
|---|---|
| Policy Narrative | Default Attachment Protection |
| Select Option | Default Attachment Protection |

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



Emails From

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

Emails To

| | |
|---|---|
| Applies To | Everyone |
| Specifically | Applies to all Recipients |

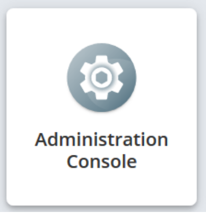
9. Press **Save and Exit**

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

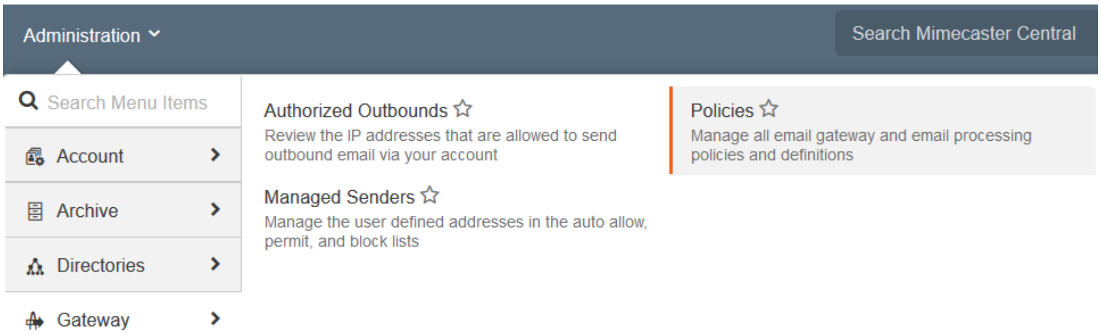
## Bypass Policy

You may have some users that need to be exempt from Attachment Protection, for example if you have emails being sent to a mailbox accessed by a CRM or ticketing system. You can configure an Attachment Protection Bypass policy to exempt users from Attachment Protection.

1. Log into your Mimecast Account at https://login.mimecast.com
2. Select **Administration Console**



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

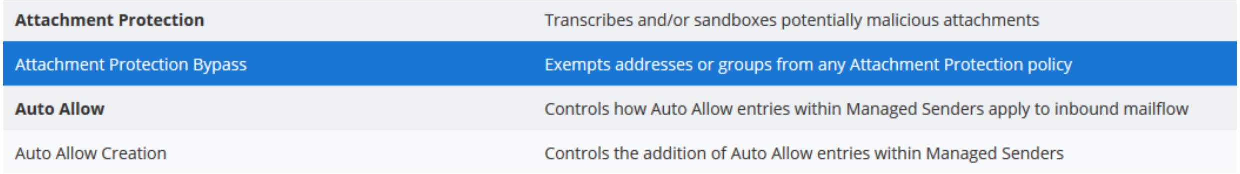


Authorized Outbounds ☆
Review the IP addresses that are allowed to send outbound email via your account

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

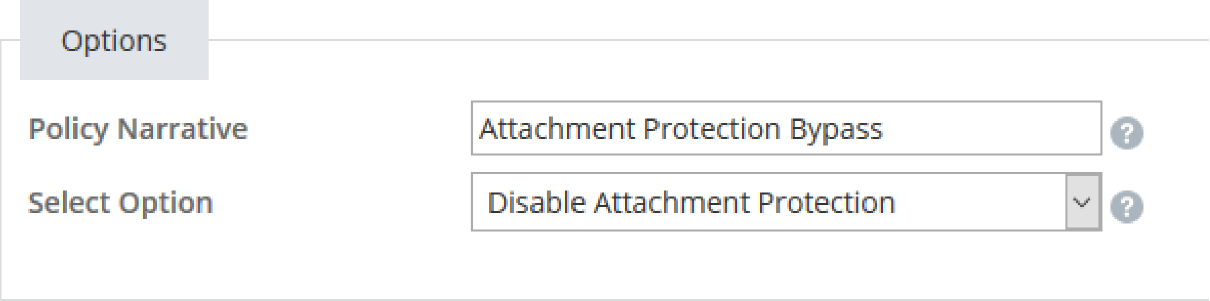
Policies ☆
Manage all email gateway and email processing policies and definitions

4. Select **Attachment Protection Bypass** from the policies list



| | |
|---|---|
| **Attachment Protection** | Transcribes and/or sandboxes potentially malicious attachments |
| Attachment Protection Bypass | Exempts addresses or groups from any Attachment Protection policy |
| **Auto Allow** | Controls how Auto Allow entries within Managed Senders apply to inbound mailflow |
| Auto Allow Creation | Controls the addition of Auto Allow entries within Managed Senders |

5. Select **New Policy**
6. Give the policy a name (**Policy Narrative**)
7. Select to **Disable Attachment Protection**

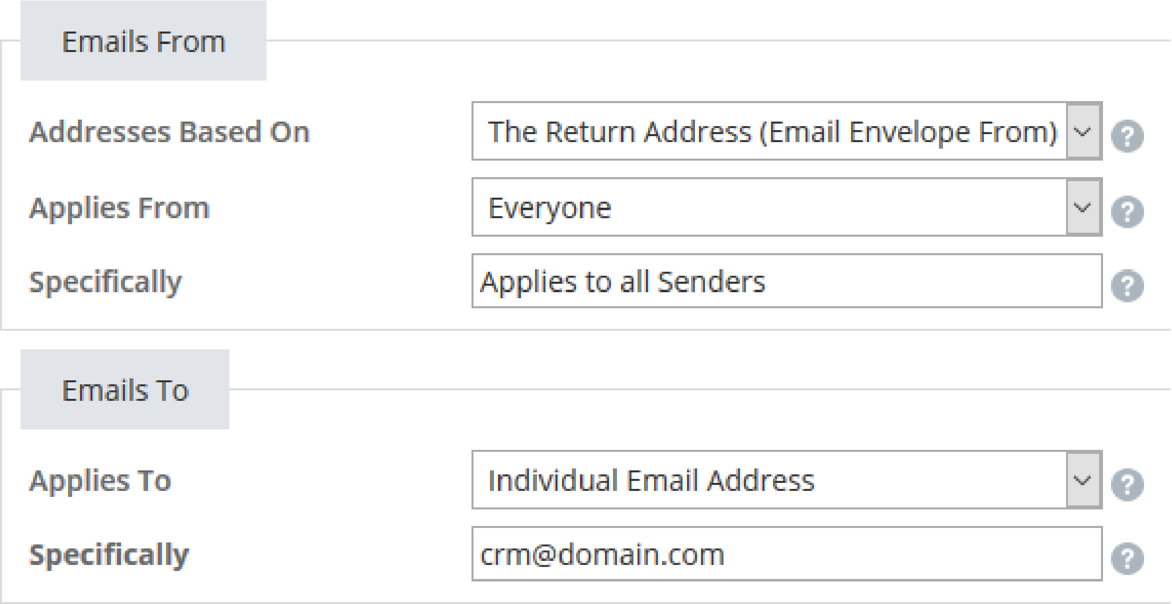


Options

Policy Narrative: Attachment Protection Bypass

Select Option: Disable Attachment Protection

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



Emails From

Addresses Based On: The Return Address (Email Envelope From)

Applies From: Everyone

Specifically: Applies to all Senders

Emails To

Applies To: Individual Email Address

Specifically: crm@domain.com

9. Press **Save and Exit**