

Anti-Spoofing Policies in Mimecast

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

The Anti-Spoofing service is designed to protect your users against spoofing attacks where your own domain is being spoofed, i.e. your domains appear in the From address.

The Anti-Spoofing policy is a strict allow or reject policy. When you add a domain, the policy that is automatically created will reject all emails from your domain that are not from your connected email service, i.e. Office 365. If you utilise other email platforms outside of this, you will need to ensure your Anti-Spoofing Policies allow through those emails.

By default, Anti-Spoofing will not look at your SPF record, instead you must configure this separately.

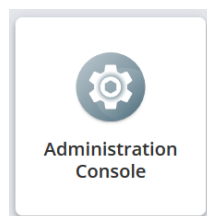
Anti-Spoofing Policy

If you didn't create the Anti-Spoofing policy when adding your domain, you can create this at a later date in your Administration Console.

1. Log into your Mimecast

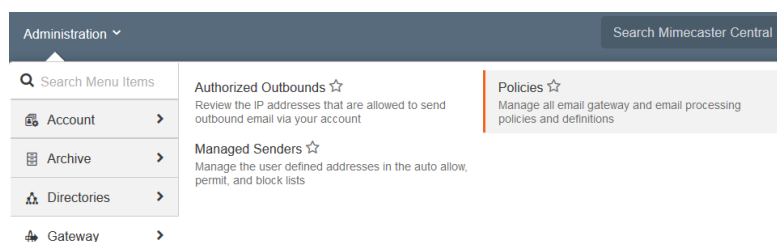
Account at

<https://login.mimecast.com>



2. Select **Administration Console**

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



4. Click into **Anti-Spoofing**

Policy Name	Description	Policies	Definitions	
Address Alterations	Modifies an SMTP address in transit prior to other policies being applied	0	0	Definitions
Address Alterations Bypass	Exempts addresses or groups from any Address Alteration policy	0	N/A	
Anti-Spoofing	Rejects messages from your domain names originating from outside your network	4	N/A	
Anti-Spoofing SPF based Bypass	Exempts messages from any Anti-Spoofing policy based on SPF record	0	N/A	
Attachment Block On Size	Blocks attachments based on the cumulative size of all attachments	0	N/A	
Attachment Hold On Size	Holds attachments based on the cumulative size of all attachments	0	N/A	

5. Select New Policy

New Policy

6. Give the policy a name
(Policy Narrative)

Options

Policy Narrative ?

Select Option ?

7. Set the Select Option to
Apply Anti-Spoofing
(Exclude Mimecast IPs)

8. Under Emails From, set the
following:

Emails From

Addresses Based On ?

Applies From ?

Specifically ?

Addresses Based On: Both
Applies From: Email Domain
Specifically: Your email domain

9. Under Emails From, set the
following:

Emails To

Applies To ?

Specifically ?

Applies To: Internal Addresses

10. Press Save & Exit

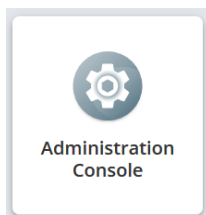
Save and Exit

IP-based Bypass Policy

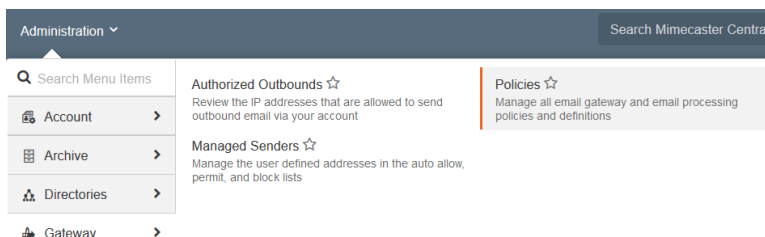
If you do have a legitimate email service outside of Mimecast that sends as your email domain, you will need to configure a bypass policy to skip Anti-Spoofing for those emails. A bypass policy should be scoped as specific as possible.

In most cases, you will want to scope the bypass policy for the IP Address of the sending server.

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



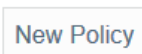
2. Select Administration Console
3. Go to 'Administration > Gateway > Policies'



4. Click into Anti-Spoofing

Policy Name	Description	Policies	Definitions
Address Alterations	Modifies an SMTP address in transit prior to other policies being applied	0	0
Address Alterations Bypass	Exempts addresses or groups from any Address Alteration policy	0	N/A
Anti-Spoofing	Rejects messages from your domain names originating from outside your network	4	N/A
Anti-Spoofing SPF based Bypass	Exempts messages from any Anti-Spoofing policy based on SPF record	0	N/A
Attachment Block On Size	Blocks attachments based on the cumulative size of all attachments	0	N/A
Attachment Hold On Size	Holds attachments based on the cumulative size of all attachments	0	N/A

5. Select New Policy



6. Give the policy a name (Policy Narrative)

A screenshot of the "Options" form for a new policy. The form has a light grey header with the word "Options". Below the header are two fields: "Policy Narrative" with a text input field containing "Anti-Spoofing Bypass" and a help icon; and "Select Option" with a dropdown menu showing "Take no action" and a help icon.

7. Set the **Select Option** to **Take No Action**

8. Under **Emails From**, set the following:

Emails From

Addresses Based On: Both

Applies From: Email Domain

Specifically: domain.com

Addresses Based On: Both
Applies From: Email Domain
Specifically: Your email domain

9. Under **Emails From**, set the following:

Emails To

Applies To: Internal Addresses

Specifically: Applies to all Internal Recipients

Applies To: Internal Addresses

10. Under **Validity**, set the following:

Validity

Enable / Disable: Enable

Set policy as perpetual: Always On

Date Range: All Time

Policy Override:

Bi Directional:

Source IP Ranges (n.n.n.n/x): 255.255.255.255/32, 255.255.254.0/24

Policy Override: True

Source IP Ranges: The IP Ranges in CIDR format (For single IPs add /32 at the end)

11. Press **Save & Exit**

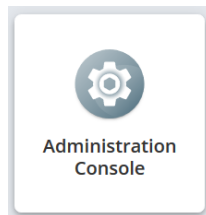
Save and Exit

Sender-based Bypass Policy

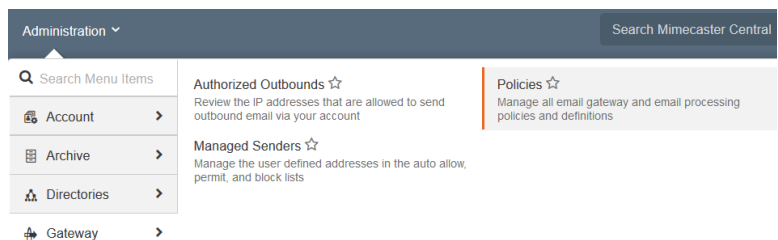
If you do have a legitimate email service outside of Mimecast that sends as your email domain, you will need to configure a bypass policy to skip Anti-Spoofing for those emails. A bypass policy should be scoped as specific as possible.

When you don't have the details for the sending servers, you can use the From address of the email to bypass Anti-Spoofing. Take care when creating this bypass policy, as Mimecast will accept all emails from this From address, regardless of where they come from.

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



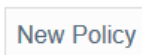
2. Select Administration Console
3. Go to 'Administration > Gateway > Policies'



4. Click into Anti-Spoofing

Policy Name	Description	Policies	Definitions
Address Alterations	Modifies an SMTP address in transit prior to other policies being applied	0	0
Address Alterations Bypass	Exempts addresses or groups from any Address Alteration policy	0	N/A
Anti-Spoofing	Rejects messages from your domain names originating from outside your network	4	N/A
Anti-Spoofing SPF based Bypass	Exempts messages from any Anti-Spoofing policy based on SPF record	0	N/A
Attachment Block On Size	Blocks attachments based on the cumulative size of all attachments	0	N/A
Attachment Hold On Size	Holds attachments based on the cumulative size of all attachments	0	N/A

5. Select New Policy



6. Give the policy a name (Policy Narrative)

Options

Policy Narrative:

Select Option:

7. Set the **Select Option** to **Take No Action**

8. Under **Emails From**, set the following:

Emails From	
Addresses Based On	Both
Applies From	Individual Email Address
Specifically	user@domain.com

Addresses Based On: Both
Applies From: Individual Email Address
Specifically: The From address of the emails

9. Under **Emails From**, set the following:

Emails To	
Applies To	Internal Addresses
Specifically	Applies to all Internal Recipients

Applies To: Internal Addresses

10. Press **Save & Exit**

Save and Exit

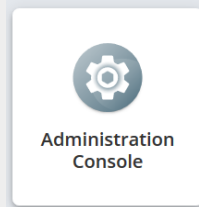
SPF-based Bypass Policy

If you do have a legitimate email service outside of Mimecast that sends as your email domain, you will need to configure a bypass policy to skip Anti-Spoofing for those emails. A bypass policy should be scoped as specific as possible.

If the provider for your other email platform publishes their IP addresses into an SPF record, you can scope the bypass to that SPF record. This can also be used to automatically create bypasses for services in your own SPF record.

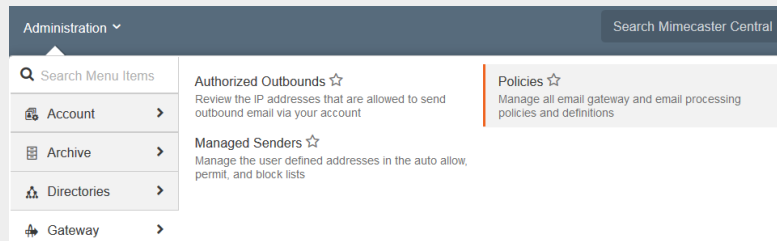
1. Log into your Mimecast Account at

<https://login.mimecast.com>



2. Select **Administration Console**

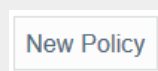
3. Go to **'Administration > Gateway > Policies'**



4. Click into **Anti-Spoofing SPF based Bypass**

Policy Name	Description
Address Alterations	Modifies an SMTP address in transit prior to other policies being applied
Address Alterations Bypass	Exempts addresses or groups from any Address Alteration policy
Anti-Spoofing	Rejects messages from your domain names originating from outside your network
Anti-Spoofing SPF based Bypass	Exempts messages from any Anti-Spoofing policy based on SPF record

5. Select **New Policy**



6. Give the policy a name
(Policy Narrative)

A screenshot of the "Options" section in the Mimecast console. It contains three fields: "Policy Narrative" with the value "SPF Based Bypass", "Policy Option" with a dropdown menu set to "Enable Bypass", and a text area labeled "When IP matches SPF record of" containing the text "domain.com" and "spf.domain2.com".

7. Set the **Policy Option** to **Enable Bypass**

8. Enter the domains where
the SPF records are hosted

9. Under **Emails From**, set the
following:

Addresses Based On: Both
Applies From: Email Domain
Specifically: Your email domain

10. Under Emails From, set the following:

Emails From	
Addresses Based On	Both ?
Applies From	Email Domain ?
Specifically	domain.com ?

Applies To: Internal Addresses

11. Press **Save & Exit**

Emails To	
Applies To	Internal Addresses ?
Specifically	Applies to all Internal Recipients ?

Save and Exit