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.

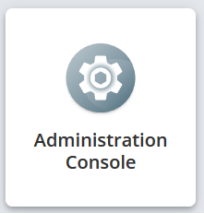
The Anti-Spoofing policy is a strict allow or reject policy. When you add a domain, the policy that is automatically created will reject all emails from your domain that are not from your connected email service, i.e. Office 365. If you utilise other email platforms outside of this, you will need to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

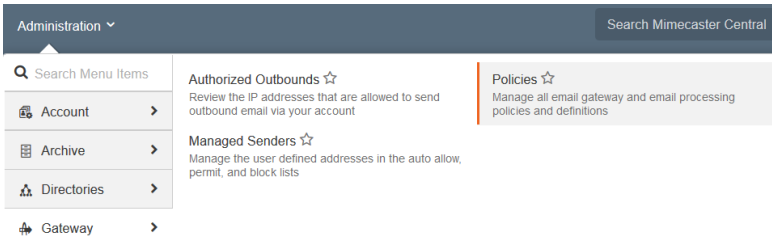
If you didn't create the Anti-Spoofing policy when adding your domain, you can create this at a later date in your Administration Console.

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

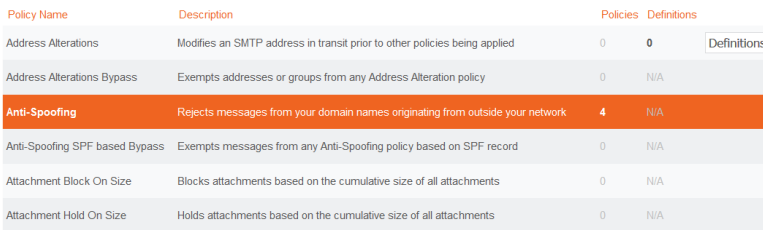


2. Select **Administration Console**

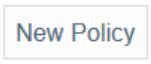
3. Go to **'Administration > Gateway > Policies'**



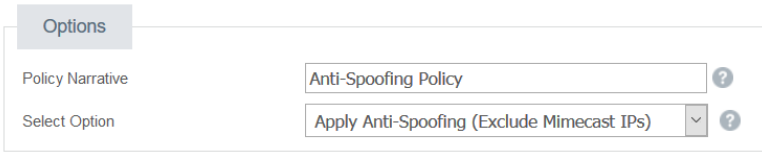
4. Click into **Anti-Spoofing**



5. Select **New Policy**

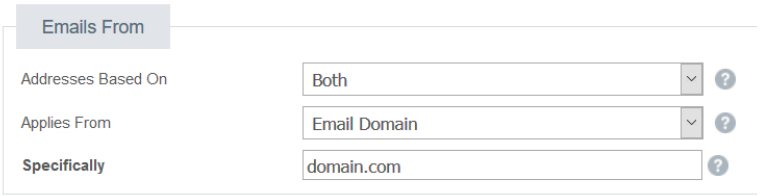


6. Give the policy a name (**Policy Narrative**)



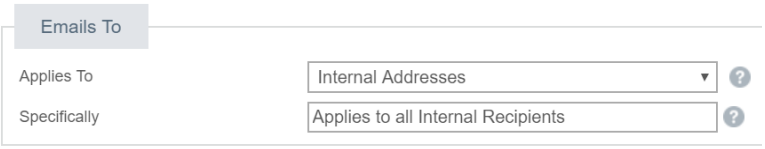
7. Set the **Select Option** to **Apply Anti-Spoofing (Exclude Mimecast IPs)**

8. Under Emails From, set the following:



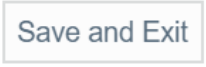
Addresses Based On: Both
Applies From: Email Domain
Specifically: Your email domain

9. Under Emails From, set the following:



Applies To: Internal Addresses

10. Press **Save & Exit**

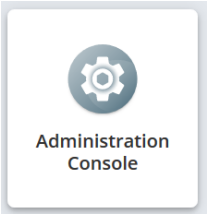


IP-based Bypass Policy

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.

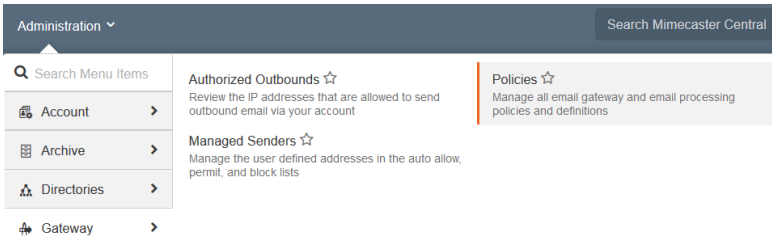
In most cases, you will want to scope the bypass policy for the IP Address of the sending server.

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

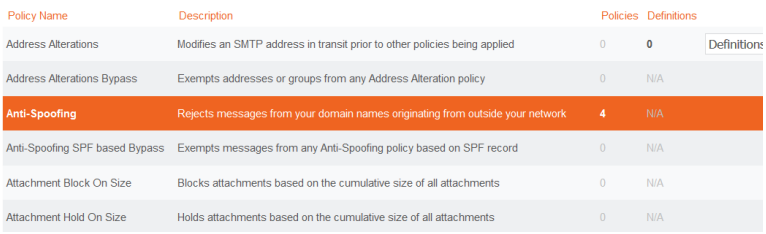


2. Select **Administration Console**

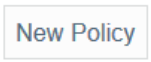
3. Go to **'Administration > Gateway > Policies'**



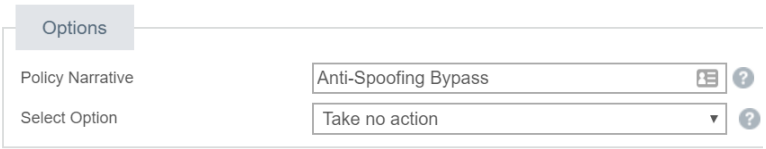
4. Click into **Anti-Spoofing**



5. Select **New Policy**

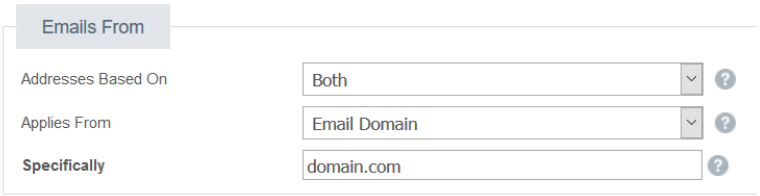


6. Give the policy a name (**Policy Narrative**)



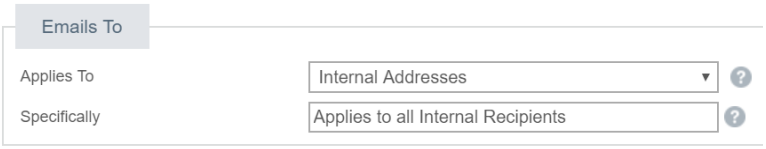
7. Set the **Select Option** to **Take No Action**

8. Under Emails From, set the following:



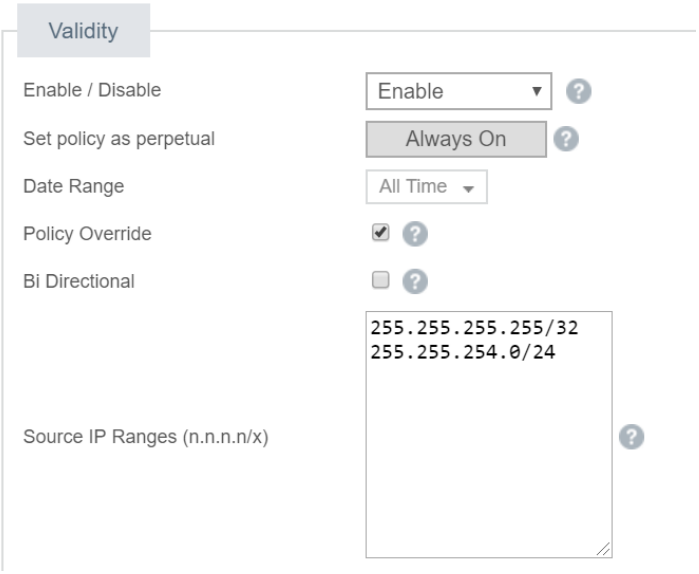
Addresses Based On: Both
Applies From: Email Domain
Specifically: Your email domain

9. Under Emails From, set the following:



Applies To: Internal Addresses

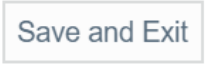
10. Under Validity, set the following:



Policy Override: True

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

11. Press **Save & Exit**

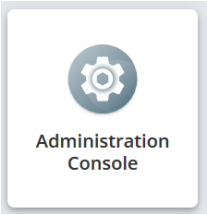


Sender-based Bypass Policy

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.

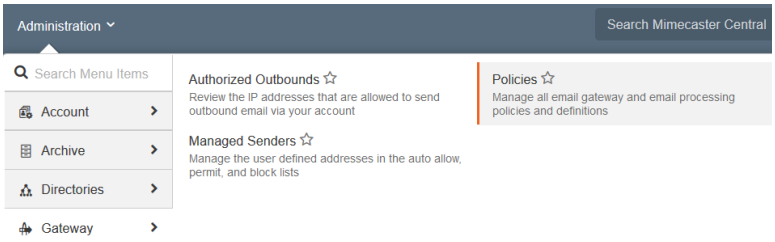
When you don't have the details for the sending servers, you can use the From address of the email to bypass Anti-Spoofing. Take care when creating this bypass policy, as Mimecast will accept all emails from this From address, regardless of where they come from.

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

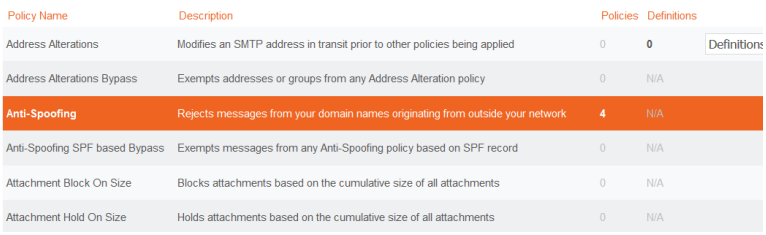


2. Select **Administration Console**

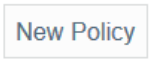
3. Go to **'Administration > Gateway > Policies'**



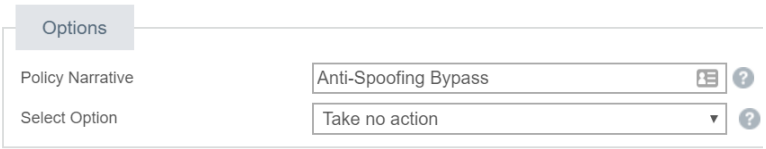
4. Click into **Anti-Spoofing**



5. Select **New Policy**

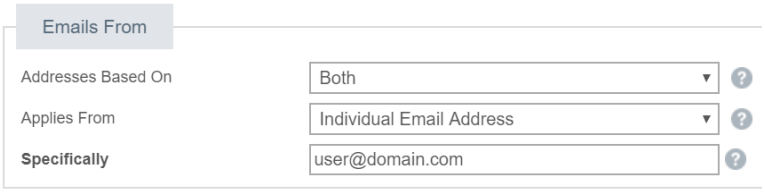


6. Give the policy a name (**Policy Narrative**)



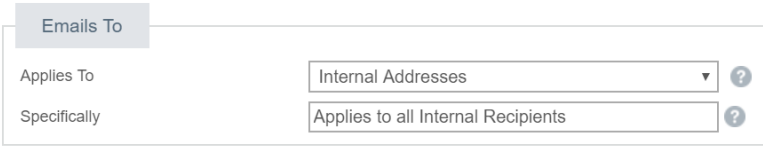
7. Set the **Select Option** to **Take No Action**

8. Under Emails From, set the following:



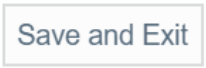
Addresses Based On: Both
Applies From: Individual Email Address
Specifically: The From address of the emails

9. Under Emails From, set the following:



Applies To: Internal Addresses

10. Press **Save & Exit**



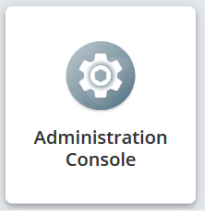
SPF-based Bypass Policy

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.

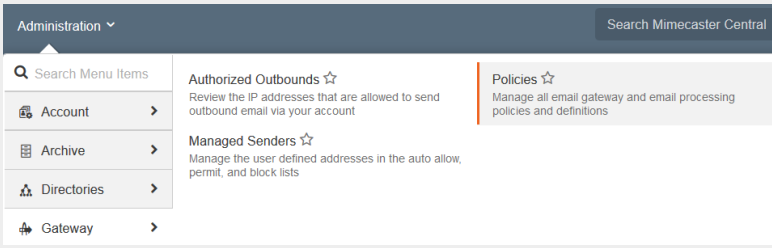
1. Log into your Mimecast Account at

https://login.mimecast.com

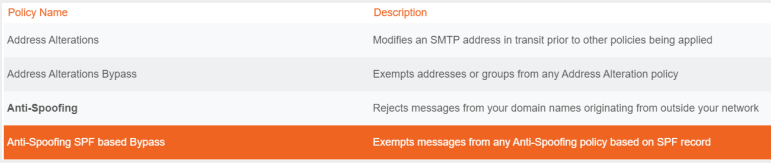


2. Select **Administration Console**

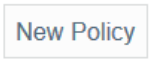
3. Go to **'Administration > Gateway > Policies'**



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

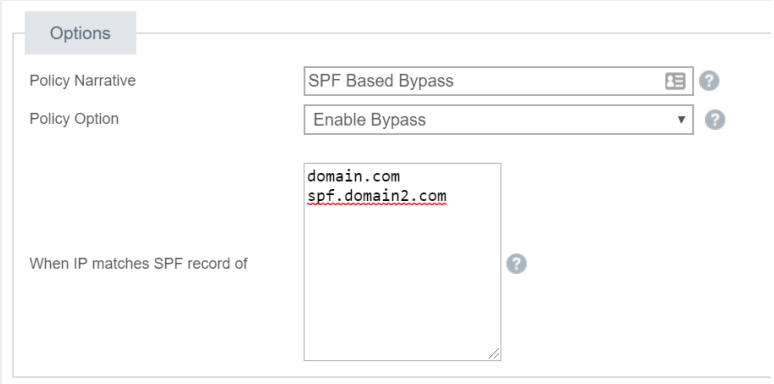


5. Select **New Policy**



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

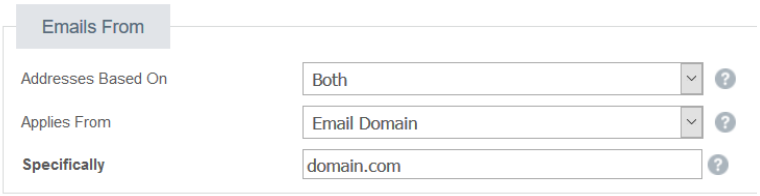
7. Set the **Policy Option** to **Enable Bypass**



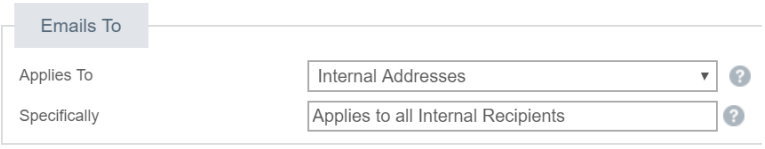
8. Enter the domains where the SPF records are hosted

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:



Applies To: Internal Addresses

11. Press **Save & Exit**