

# Permitted Senders in Mimecast

Last Modified on 23/01/2020 9:57 am GMT

Permitted Senders policies define criteria for automatically allowing an email through spam checks. By default, you will automatically have a policy scoped for the default Permitted Senders Profile Group. If you simply need to allow through another address or domain for your whole account, you should add it to that Profile Group.

Permitted Sender policies can be bypassed by Domain Authentication Policies. It also does not permit emails through Anti-Malware, Anti-Spoofing or Content Examination policies.

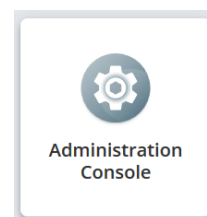
Permitted Sender policies are admin-controlled policies. Permitted Senders added by Users are managed through the Auto Allow policy.

## Policy

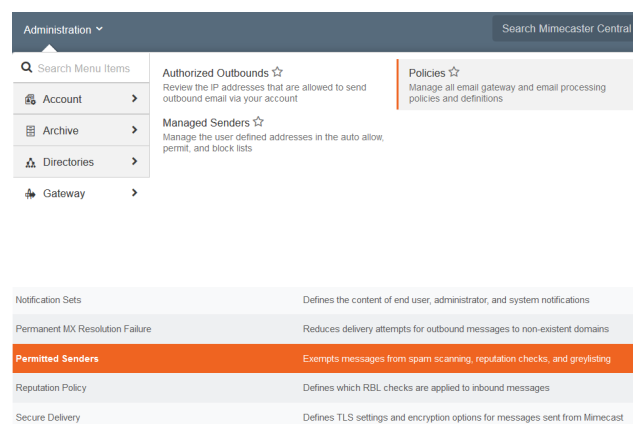
1. Log into your Mimecast Account at

<https://login.mimecast.com>

2. Select **Administration Console**

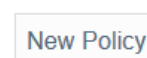


3. Go to '**Administration > Gateway > Policies**'



4. Click into **Permitted Senders**

5. Select **New Policy**



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

7. Set Permitted Sender Policy to Permit Sender

**Options**

Policy Narrative  ?

Permitted Sender Policy  ?

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

**Emails From**

Addresses Based On  ?

Applies From  ?

Specifically  ?

**Emails To**

Applies To  ?

Specifically  ?

9. If you want to scope the policy to permit emails only when connecting from certain IP Ranges, enter the IPs under Source IP Ranges

**Note:** You must enter the IP Ranges in CIDR format (For single IPs add /32 at the end)

**Validity**

Enable / Disable  ?

Set policy as perpetual  ?

Date Range  ?

Policy Override  ?

Bi Directional  ?

Source IP Ranges (n.n.n.n/x)  ?

10. Press Save & Exit

Save and Exit