

Geographical Restrictions in Mimecast

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

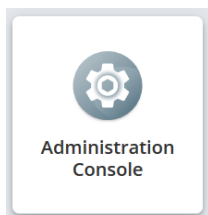
Geographical Restriction policies allow you to operate a country-based whitelist or blacklist to limit which countries your Mimecast account allows emails from. Emails outside of the allowed country list are rejected.

You can use these policies to automatically reject emails from high spam sending countries.

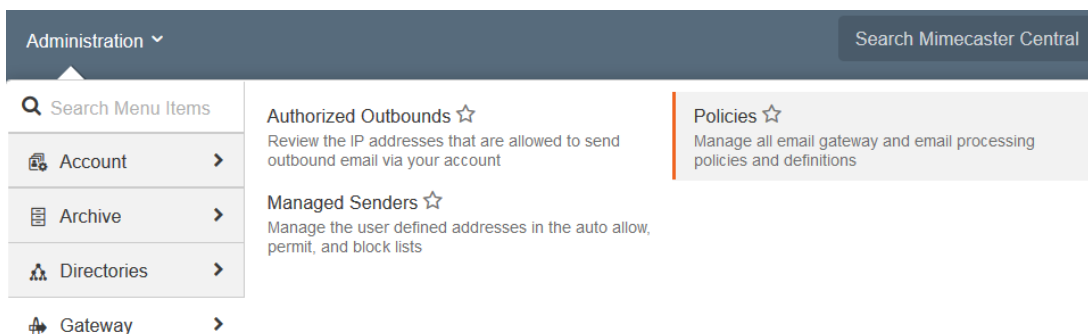
Definition

You will need to first configure a definition to determine which countries to use as a blacklist or whitelist.

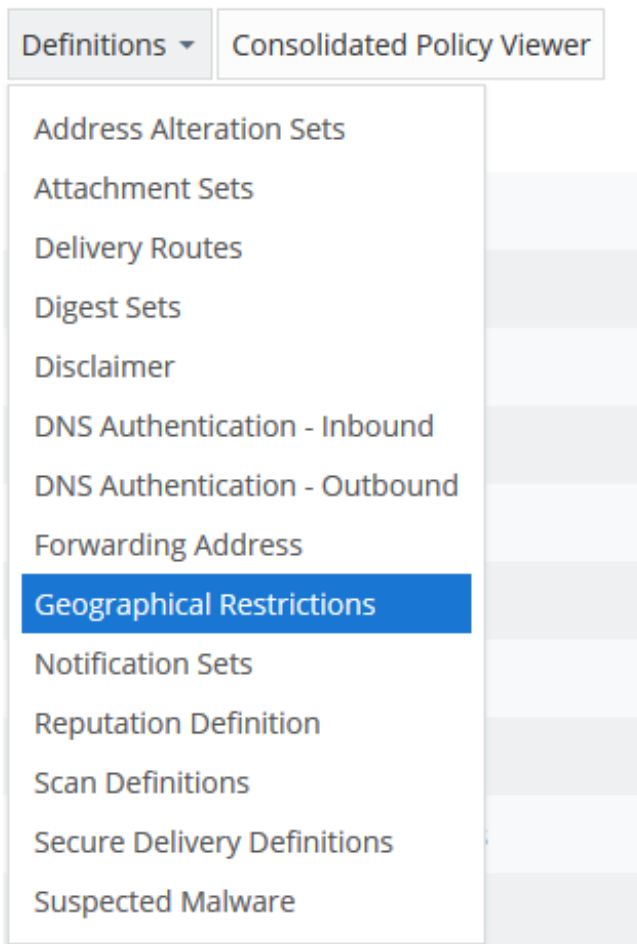
1. Log into your Mimecast Account at <https://login.mimecast.com>
2. Select **Administration Console**



3. Go to 'Administration > Gateway > Policies'



4. From the **Definitions** dropdown, select **Geographical Restrictions**



5. Select **New Geographical Restrictions**
6. Set the **Name** for the Definition
7. Select to Block or Permit the country list
 - a. **Block**: Operates a blacklist. Any country on this list will be rejected.
 - b. **Permit**: Operates a whitelist. Any country not on this list will be rejected.
8. Add countries to the Select Countries list by selecting them and using the **Add & Remove** buttons
9. Press **Save and Exit**

Geographical Settings

Name:

Type:

- Block
Block inbound messages from selected countries
- Permit
Permit inbound messages from selected countries.

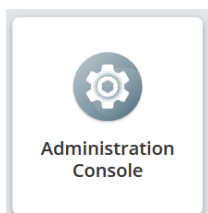
Countries

Available		Selected
TUNISIA(TN)	Add »» «« Remove	United Kingdom(GB)
Turkey(TR)		
Turkmenistan(TM)		
Turks And Caicos Islands(TC)		
Tuvalu(TV)		
U.S. Virgin Islands(VI)		
Uganda(UG)		
Ukraine(UA)		
United Arab Emirates(AE)		
United States Minor Outlying Islands(UM)		
United States(US)		
Uruguay(UY)		
Uzbekistan(UZ)		
Vanuatu(VU)		
Venezuela(VZ)		

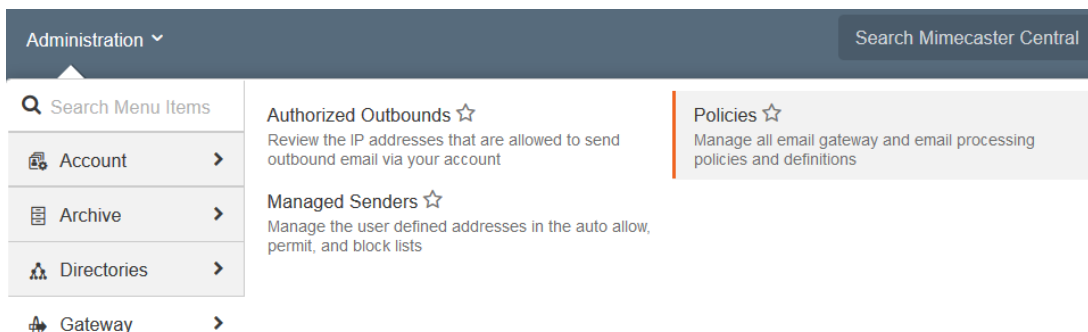
Policy

Once a definition is created, a policy will determine when the restrictions apply.

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



3. Go to 'Administration > Gateway > Policies'



4. Select **Geographical Restrictions** from the policies list

Forwarding Address	Forwards messages to another individual recipient address
Geographical Restrictions	Block or permit inbound messages from selected countries
Greylisting	Requires previously unknown senders to retry messages to verify RFC compliance

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

Note: Use the Lookup button to browse your definitions, then use the **Select** option next to the definition to use.

Options

Policy Narrative	<input style="width: 95%;" type="text" value="UK Only"/>	?	
Select Definition	<input style="width: 95%;" type="text" value="UK Only"/>	?	<input style="border: 1px solid #ccc; padding: 2px 5px;" type="button" value="Lookup"/> ?
Preview	↔		

8. Set the scope for the policy under **Emails From** and **Emails To**
9. Press **Save and Exit**

Emails From

Addresses Based On	<input type="text" value="The Return Address (Email Envelope From)"/>	?	
Applies From	<input type="text" value="Everyone"/>	?	
Specifically	<input type="text" value="Applies to all Senders"/>	?	

Emails To

Applies To	<input type="text" value="Internal Addresses"/>	?	
Specifically	<input type="text" value="Applies to all Internal Recipients"/>	?	

Only one Geographical Restrictions 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.