DNS Authentication in Mimecast

Last Modified on 23/01/2020 9:56 am GMT

DNS Authentication in Mimecast is handled by two separate policies.

DNS Authentication Inbound – Handles whether SPF, DKIM & DMARC checks should apply and what to do when a check if failed.
DNS Authentication Outbound – Handles DKIM signing your outbound emails through Mimecast.

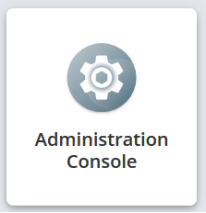
Both policies require a Definition to be configured first.

Inbound Definition

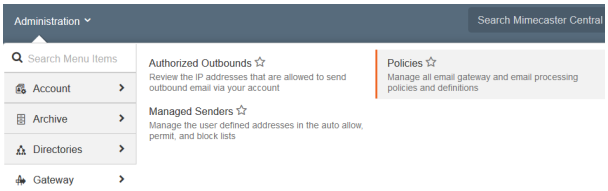
The Definition for Inbound DNS Authentication determines what to do when an SPF, DKIM or DMARC check fails.

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

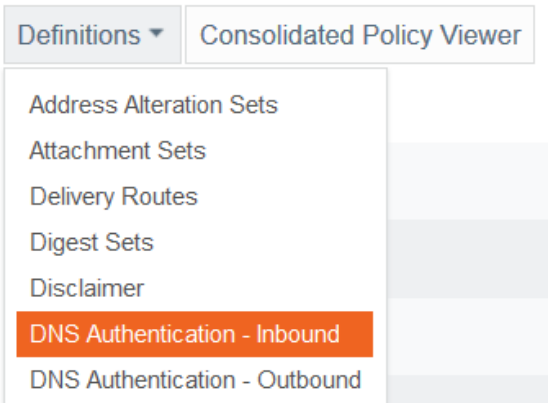
2. Select **Administration Console**



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



4. From the **Definitions** dropdown, select **DNS Authentication Inbound**



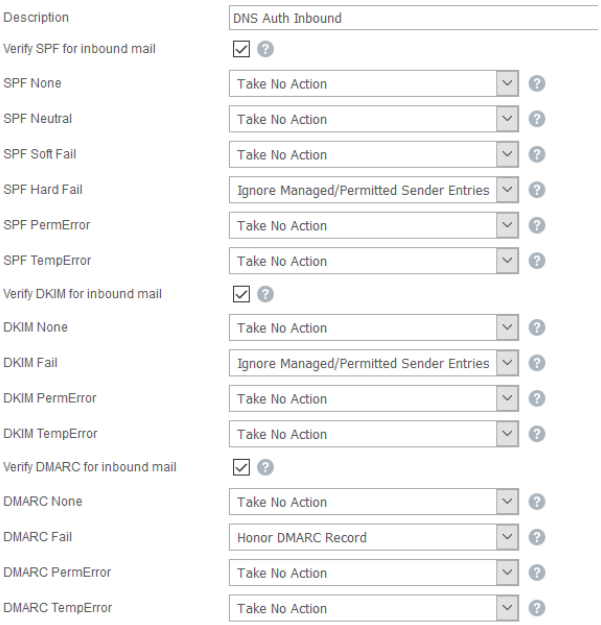
5. Select **New DNS Authentication -**

Inbound Checks

6. Set the name (**Description**) for the Definition

7. Tick the checkbox next to each check to take place.

8. For each possible result, select the action to take place:



Take No Action: The email will continue to spam checks as normal

Ignore Managed/Permitted Sender Entries: Any Permitted Sender or Auto Allow policies applying to this email will be ignored.

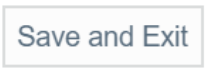
Reject: The email is blocked and deleted by Mimecast.

Honor DMARC Record: Only available for DMARC Fail. Performs the action specified in the sender's DMARC record:

Quarantine: The email is held for an Admin to release

Reject: The email is blocked and deleted by Mimecast

9. Press **Save & Exit**

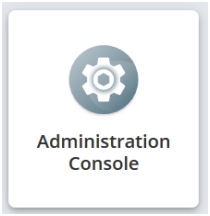


Inbound Policy

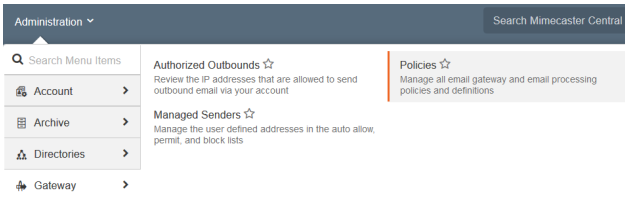
Once you have created your definition, you will need to create an accompanying policy to determine when it is applied.

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

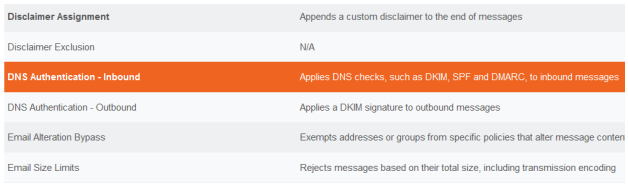
2. Select **Administration Console**



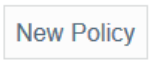
3. Go to **'Administration > Gateway > Policies'**



4. Click into **DNS Authentication - Inbound**

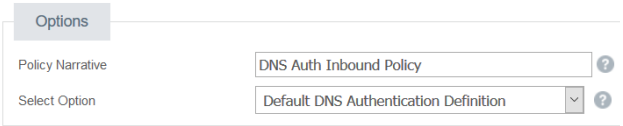


5. Select **New Policy**



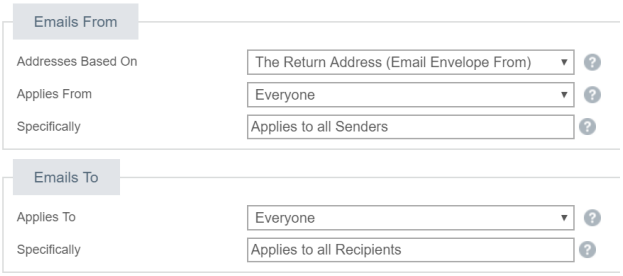
6. Give the policy a name (**Policy Narrative**)

7. Set **Select Option** to definition you created

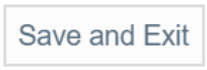


8. Set the scope for the policy under

Emails From and **Emails To**



9. Press **Save & Exit**

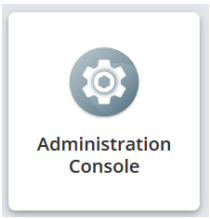


Outbound Definition

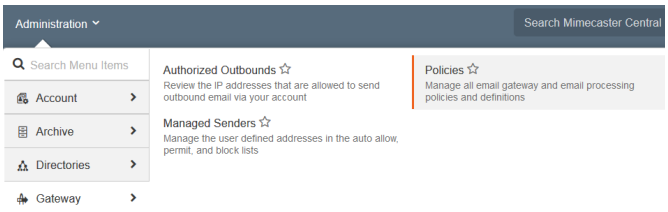
The Definition for Outbound DNS Authentication determines the DKIM signing settings to use.

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

2. Select **Administration Console**

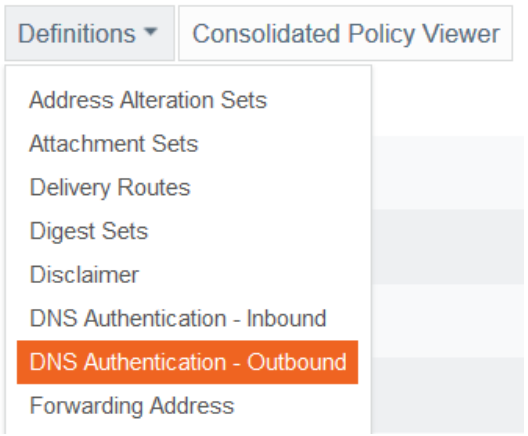


3. Go to **'Administration > Gateway > Policies'**

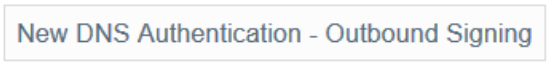


4. From the **Definitions** dropdown, select **DNS Authentication -**

Outbound



5. Select **New DNS Authentication – Outbound Signing**

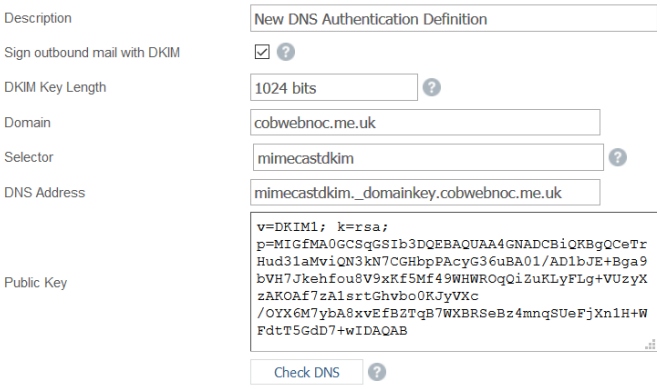


6. Set the name (**Description**) for the Definition

7. Tick the checkbox next to **Sign outbound email with DKIM**

8. Use the Lookup option to select the Domain to use

9. Enter the name for the DKIM Selector

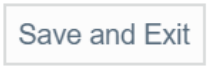


10. Press **Generate**

11. Add the Public Key as a TXT record with your domain host at the DNS Address

12. Press **Check DNS**

13. Press **Save & Exit**

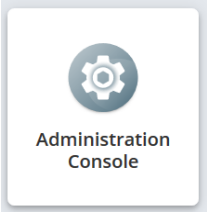


Outbound Policy

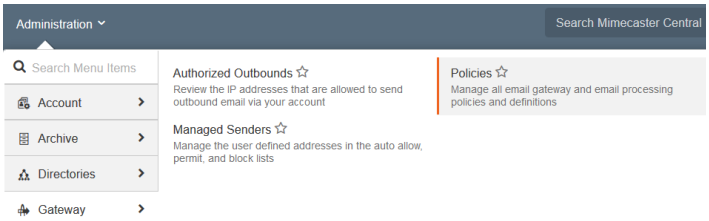
Once you have created your definition, you will need to create an accompanying policy to determine when it is applied.

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

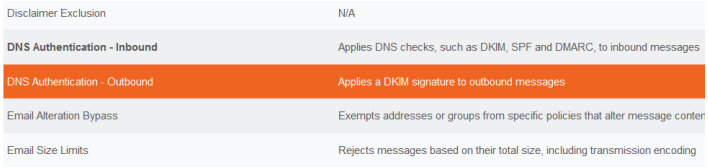
2. Select **Administration Console**



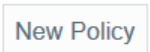
3. Go to **'Administration > Gateway > Policies'**



4. Click into **DNS Authentication - Outbound**

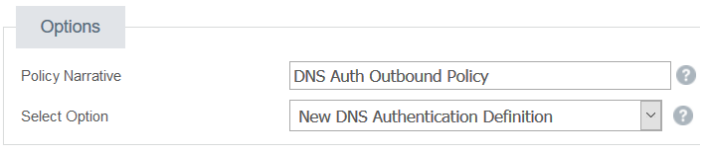


5. Select **New Policy**

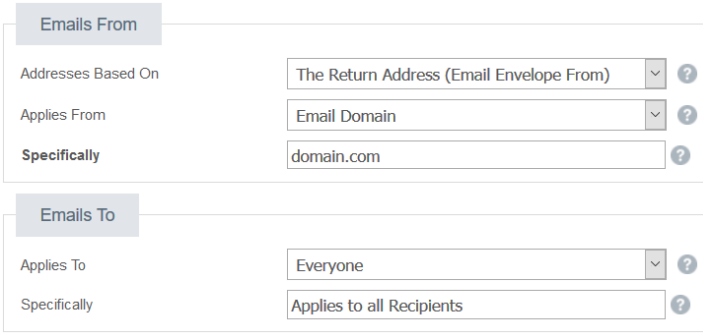


6. Give the policy a name (**Policy Narrative**)

7. Set **Select Option** to definition you created



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



9. Press **Save & Exit**