

# 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.

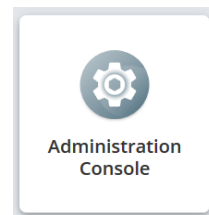
## Inbound Definition

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

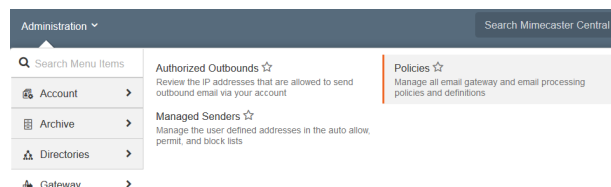
1. Log into your Mimecast Account at

<https://login.mimecast.com>

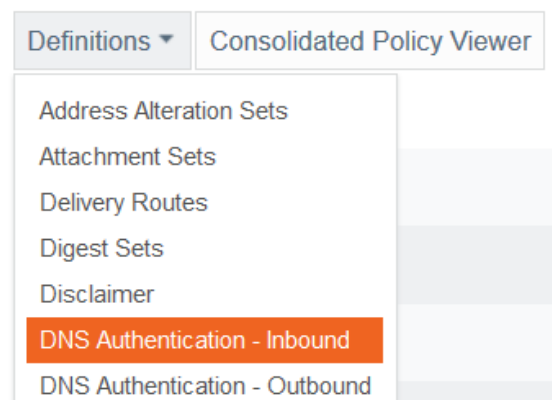
2. Select **Administration Console**



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



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



5. Select **New DNS Authentication -**

## Inbound Checks

### New DNS Authentication - Inbound Checks

- Set the name (**Description**) for the Definition
- Tick the checkbox next to each check to take place.
- 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

Description	DNS Auth Inbound
Verify SPF for inbound mail	<input checked="" type="checkbox"/> ?
SPF None	Take No Action ?
SPF Neutral	Take No Action ?
SPF Soft Fail	Take No Action ?
SPF Hard Fail	Ignore Managed/Permitted Sender Entries ?
SPF PermError	Take No Action ?
SPF TempError	Take No Action ?
Verify DKIM for inbound mail	<input checked="" type="checkbox"/> ?
DKIM None	Take No Action ?
DKIM Fail	Ignore Managed/Permitted Sender Entries ?
DKIM PermError	Take No Action ?
DKIM TempError	Take No Action ?
Verify DMARC for inbound mail	<input checked="" type="checkbox"/> ?
DMARC None	Take No Action ?
DMARC Fail	Honor DMARC Record ?
DMARC PermError	Take No Action ?
DMARC TempError	Take No Action ?

- Press **Save & Exit**

Save and Exit

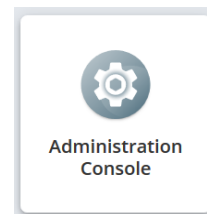
# Inbound Policy

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

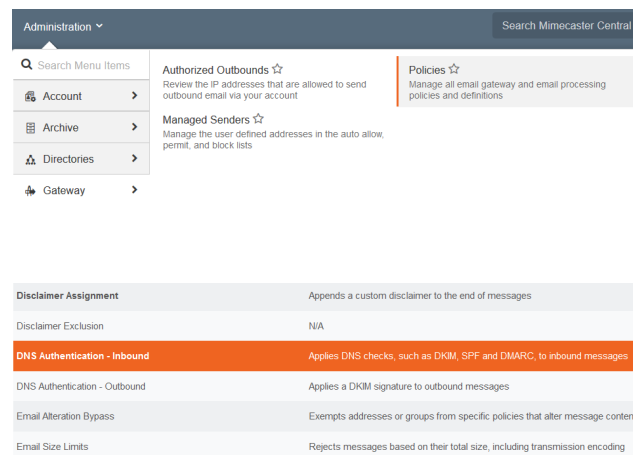
1. Log into your Mimecast Account at

<https://login.mimecast.com>

2. Select Administration Console

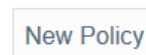


3. Go to 'Administration > Gateway > Policies'



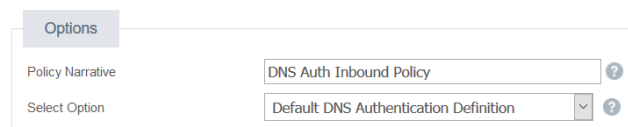
4. Click into DNS Authentication - Inbound

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

Emails From	
Addresses Based On	The Return Address (Email Envelope From) ?
Applies From	Everyone ?
Specifically	Applies to all Senders ?

Emails To	
Applies To	Everyone ?
Specifically	Applies to all Recipients ?

9. Press **Save & Exit**

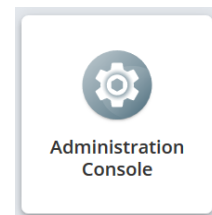
Save and Exit

## Outbound Definition

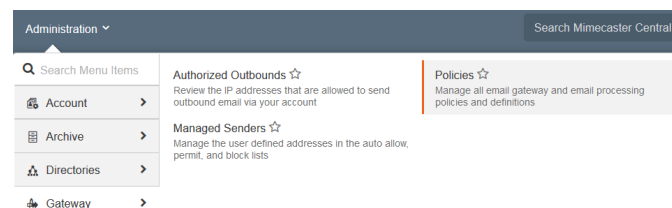
The Definition for Outbound DNS Authentication determines the DKIM signing settings to use.

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

2. Select **Administration Console**

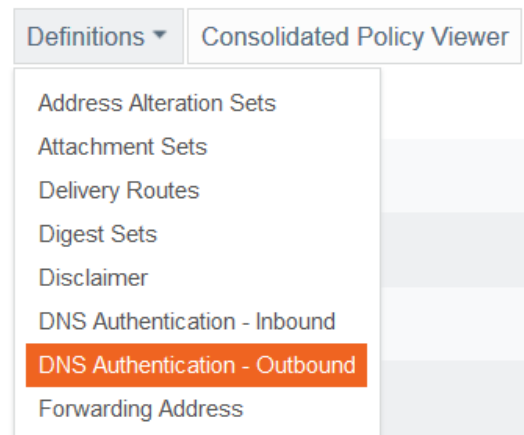


3. Go to **'Administration > Gateway > Policies'**

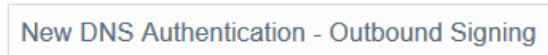


4. From the **Definitions** dropdown, select **DNS Authentication -**

## 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**

Description	New DNS Authentication Definition
Sign outbound mail with DKIM	<input checked="" type="checkbox"/>
DKIM Key Length	1024 bits
Domain	cobwebnoc.me.uk
Selector	mimecastdkim
DNS Address	mimecastdkim._domainkey.cobwebnoc.me.uk
Public Key	<pre>v=DKIM1; k=rsa; p=MTGFMA0GCSqSIlb3DQEBAQUAA4GNADCBiQKBgQCeTr Hud31aMviQN3kN7CGHbpPAcyG36uBA01/AD1bJE+Bga9 bVH7Jkehfou8V9xKf5MF49WHWROqQi2uKLyFLg+VUzyX zAKOAF7zA1srtGhvbo0KJyVXc /OYX6M7yba9xvEfB2TqB7WXBRSeBz4mnqSUFjXn1H+W FdtT5GdD7+wIDAQAB</pre>
	<input type="button" value="Check DNS"/>

13. Press Save & Exit

Save and Exit

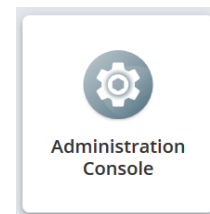
## Outbound Policy

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

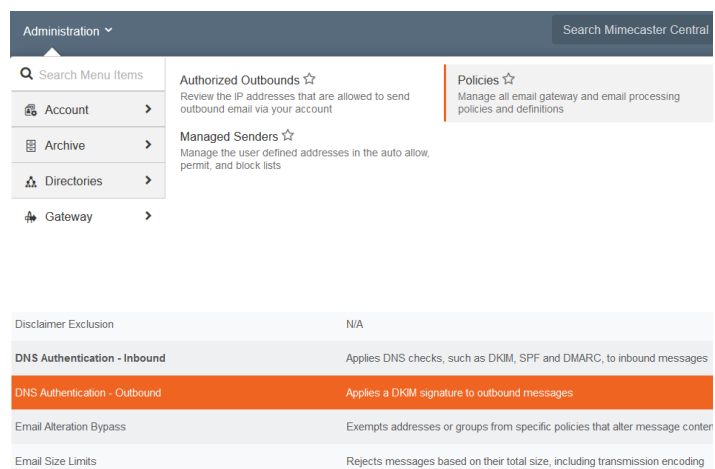
Account at

<https://login.mimecast.com>



2. Select Administration Console

3. Go to 'Administration > Gateway > Policies'



4. Click into DNS Authentication - Outbound

5. Select New Policy

New Policy

6. Give the policy a name (Policy Narrative)

7. Set Select Option to definition you created

A screenshot of the "Options" form in the Mimecast interface. The form has a grey header with the word "Options". Below the header are two input fields. The first field is labeled "Policy Narrative" and contains the text "DNS Auth Outbound Policy". The second field is labeled "Select Option" and contains a dropdown menu with the text "New DNS Authentication Definition". Both fields have a question mark icon to their right.

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

Emails From	
Addresses Based On	The Return Address (Email Envelope From) ?
Applies From	Email Domain ?
Specifically	domain.com ?

Emails To	
Applies To	Everyone ?
Specifically	Applies to all Recipients ?

9. Press **Save & Exit**

Save and Exit

---