

What is DKIM ?

DKIM stands for = DomainKeys Identified Mail

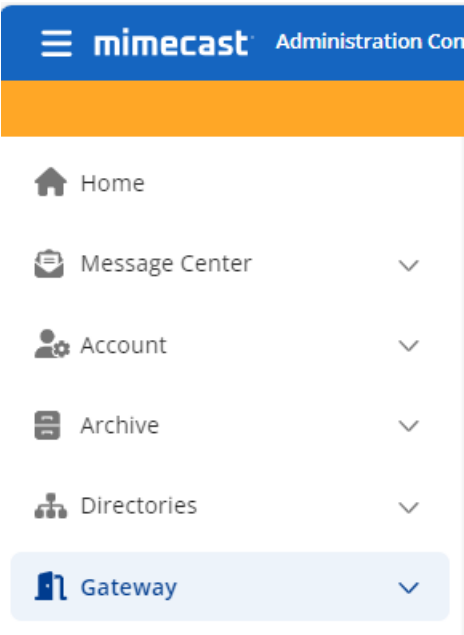
DKIM is another type of email authentication which is used to detect forged sender email addresses. This is a technique that is used in phishing emails and spam emails.

This is also a method that is uses a digital signature to let the recipient know that the email was sent and authorized by the domain owner

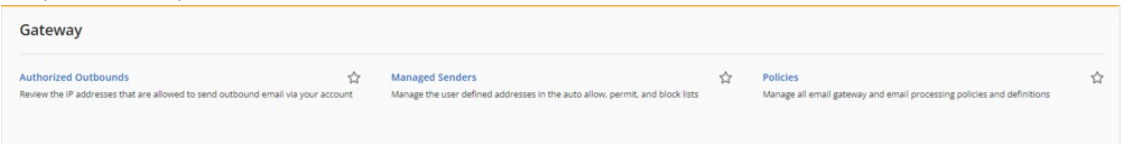
How to configure DKIM ?

To configure DKIM in Mimecast you need to do the following:

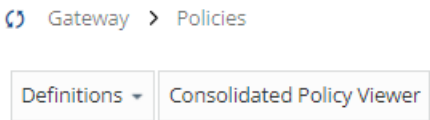
- 1. go to [Partner Portal \(mimecast.com\)](#) and log in
- 2. Once logged in go to [Partner Portal \(mimecast.com\)](#) and find the client e.g. International Precision Casting Supplies Limited
- 3. Once you have found the client's portal go to the admin console
- 4. Once in the admin console on the left sidebar menu look for "Gateway"



- 5. Once your in the Gateway menu select "Policies"




- 6. From here at the top you will see a dropdown button called "Definitions"



Select that and you will get this menu appear


Address Alteration Sets
Attachment Protection
Attachment Sets
Auto Response Notification
Content Definitions
Delivery Routes
Digest Sets
DNS Authentication - Inbound
DNS Authentication - Outbound
Document Services
External Recipient Limiting
Forwarding Address
Geographical Restrictions
Impersonation Protection
Notification Sets
Reputation Definition
Scan Definitions
Secure Delivery Definitions
Stationery
Suspected Malware
URL Protection

7. From here you will want to select "DNS Authentication - Outbound"
8. when you get to this page you will then see these two buttons

 Gateway > Policies


Go Back New DNS Authentication - Outbound Signing

- Select "New DNS Authentication - Outbound Signing"
9. you will then get this page

 Gateway > Policies

Go Back Save Save and Exit

Description New DNS Authentication Definition

Sign outbound mail with DKIM ☐ 

10. From here put the description e.g. "IPCS DKIM Authentication"
then tick the "sign outbound mail with DKIM"
Once you have ticked that you will then get this screen

Go Back Save Save and Exit

Description New DNS Authentication Definition

Sign outbound mail with DKIM ☒ ?

Is External Domain ☐ ?

Domain Select a Domain ✕ Lookup

Selector mimecast20240430 ?

11. From there you will need to select the "Lookup" button to search for the domain

Gateway > Policies

Go Back

Search ?

This page is in **lookup** mode - please select an item

Select Domain Name	Inbound Checks
Select @cuk101a221.mimecast.connect	Known Recipients Only
Select @ipcsadmin.onmicrosoft.com	Accept Any Address
Select @ipcs-uk.com	Directory Users Only

select the domain you want to proceed with e.g. ipcs-uk.com
you will then get this page here

Go Back Save Save and Exit

Description New DNS Authentication Definition

Sign outbound mail with DKIM ☒ ?

Is External Domain ☐ ?

DKIM Key Length 1024 bits ?

Domain ipcs-uk.com ✕ Lookup

Selector mimecast20240430 ?

Generate ?

12. once you have selected the domain you want to proceed with (Make sure to change the DKIM Key Length) this must be 2048

DKIM Key Length 1024 bits ?

Domain 1024 bits - this is so that the DKIM key has higher security

Selector 2048 bits

13. Once changed press generate
You will now get this page here

Go BackSaveSave and Exit

Description

New DNS Authentication Definition

Sign outbound mail with DKIM

☒

Is External Domain

☐

DKIM Key Length

2048 bits

Domain

ipcs-uk.com

Selector

mimecast20240430

DNS Address

mimecast20240430_domainkey.ipcs-uk.com

DKIM Public Key

v=DKIM1; k=rsa;
p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA526KVSih9okhkd3FW2FngRr+11b+9slqfw0Mehaeu6+vi6WGGQI2
KNU1SHwxYWXbSXGICo5ZA9HVN0YvEtyssOuhRzmahdxde8fH9mpPeWdhOc4oyPy9eHDnL5QthTOYNfmBEsoY/xmfrs6qfLs
OghoBzrMwXgdLHR6xZakB22/xYNSdRoaed2xjifiReBDyqzvKMsIN3/q77BoDWzAxKcobEI44T2Ya7B3AzHNwpxy34Vgbp+12I/
AhDFO/NU/XdGF+6MV4qYKKA9z6fQ/siv7VB5BWGgOMI5jqTgvdCbSshdAs47/uvFkxRbRG4zQdeITCCLQd4aLPTZf50fkswIDAQ
AB

Check DNS

Alert Message

Public Key Is generated successfully.

Publish the Public Key as the DNS TXT record for mimecast20240430_domainkey.ipcs-uk.com

OK

14. Now its time to configure the DNS record for this

How to configure DNS record for DKIM - Using Mimecast

To configure DKIM DNS record you need to do the following:

1. Login to the companies DNS hosting provider e.g. [IPCS-UK.com domain login — IT Glue](#)
2. Once you are logged in go to the DNS settings
The type of record for a DKIM (using Mimecast) record is a TXT record.
3. To add this to the DNS settings the record should look something like this:

name of record:

mimecast20240430

Value of record:

DKIM Public Key

v=DKIM1; k=rsa;
p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA526KVSih9okhkd3FW2FngRr+11b+9slqfw0Mehaeu6+vi6WGGQI2
KNU1SHwxYWXbSXGICo5ZA9HVN0YvEtyssOuhRzmahdxde8fH9mpPeWdhOc4oyPy9eHDnL5QthTOYNfmBEsoY/xmfrs6qfLs
OghoBzrMwXgdLHR6xZakB22/xYNSdRoaed2xjifiReBDyqzvKMsIN3/q77BoDWzAxKcobEI44T2Ya7B3AzHNwpxy34Vgbp+12I/
AhDFO/NU/XdGF+6MV4qYKKA9z6fQ/siv7VB5BWGgOMI5jqTgvdCbSshdAs47/uvFkxRbRG4zQdeITCCLQd4aLPTZf50fkswIDAQ
AB

4. you will then have something like this on the DNS hosting provider DNS settings

21

mimecast20210430

.domain

TXT

v=DKIM1; k=rsa; p=MIGfMA0GCS

What to do after you have configured the DNS

You will now need to go back to the Mimecast portal where you created the DKIM Key and validate the record once you have done this you will get a message like this

Check DNS Status **Successfully Validated**

Press "Save & Exit" and your record has been completed