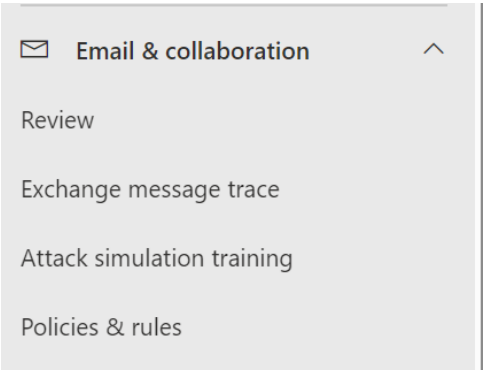


How to configure DKIM - using Microsoft 365

To configure DKIM you need to do the following:

- 1. Login to the companies Microsoft Office 365 Admin Console e.g. [Office 365 Admin \(IPCS\) — IT Glue](#)
- 2. Once you are logged in go to <https://admin.microsoft.com/>
- 3. Once in the admin console - from the left sidebar menu select the Security Admin center <https://security.microsoft.com/>
- 4. Once in the security admin console - from the left sidebar menu select the dropdown "Email & Collaboration"
you will then see this menu



- 5. From here select Policies & Rules
you will then get this page

Policies & rules

Set up policies to manage devices, protect against threats, and receive alerts about various activities in your organization. [Learn more](#)

3 items

Name ▾

Threat policies

Alert policy

Activity alerts

- 6. from here select Threat Policies
This page will then appear

Policies & rules > Threat policies

Threat policies

Templated policies

Preset Security Policies

Easily configure protection by applying all policies at once using our recommended protection

Configuration analyzer

Identify issues in your current policy configuration to improve your security

Policies

Anti-phishing

Protect users from phishing attacks, and configure safety tips on suspicious messages.

Anti-spam

Protect your organization's email from spam, including what actions to take if spam is detected

Anti-malware

Protect your organization's email from malware, including what actions to take and who to r

- 7. scroll down to the "Rules" section and select the option "Email Authentication Settings"
you will then get this page

Email authentication settings

ARC DKIM

Trusted ARC sealers

Authentication Received Chain (or ARC) is an authentication method that preserves authentication results across intervening devices and technologies. Its goal is to capture the full authentication story of the e-mail.

Add trusted ARC sealers below to trust and pass authentication using ARC seals. [Learn more about ARC](#)

+ Add Refresh

0 items Search

Trusted sealers

8. From here select the DKIM section

Email authentication settings

ARC DKIM

DomainKeys Identified Mail (DKIM)

Domain Keys Identified Mail (DKIM) is an authentication process that can help protect both senders and recipients from forged and phishing email. Add DKIM signatures to your domains so recipients know that email messages actually came from users in your organization and weren't modified after they were sent. [Learn more about DKIM](#)

Export Refresh

2 items Search

Name	Accepted domain	Domain Type
<input type="checkbox"/> ipcs-uk.com	ipcs-uk.com	Authoritative
<input type="checkbox"/> ipcsadmin.onmicrosoft.com (default signing domain)	ipcsadmin.onmicrosoft.com	Authoritative

9. Once here select the domain you want to configure
you will then get this pop up



ipcs-uk.com

Sign messages for this domain with DKIM signatures

☐ Disabled

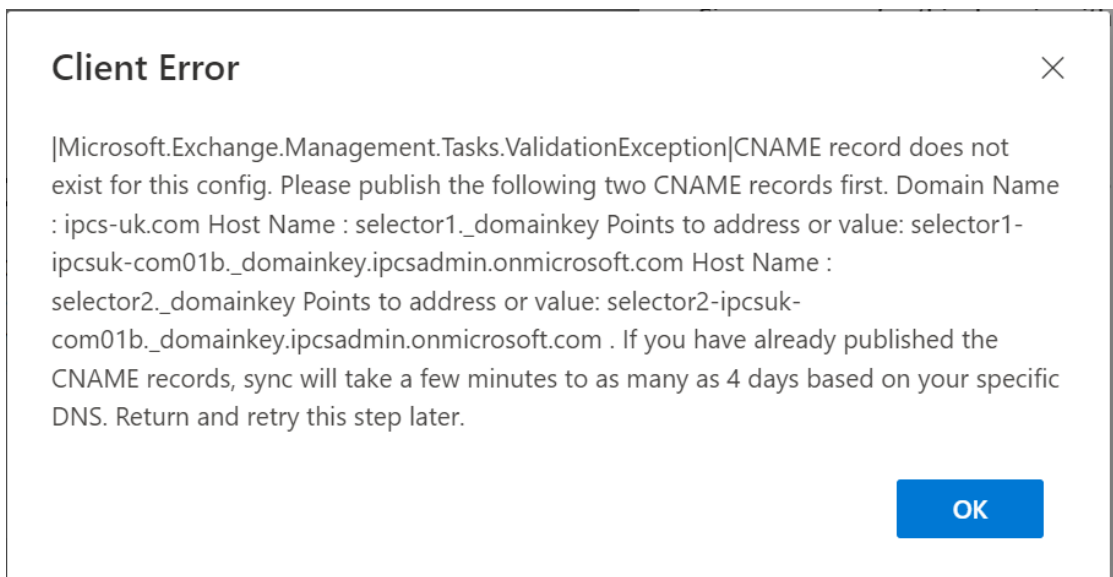
Status

Not signing DKIM signatures for this domain.

Last checked date

2 Jan 2016 23:29:40

10. turn the toggle on underneath the message "Sign messages for this domain with DKIM signatures"
you will then get this message pop up



11. this is where you have to configure the DNS settings

How to configure the DNS for DKIM - using M365

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 Microsoft) record is a CNAME record.
3. To add this to the DNS settings the record should look something like this:
there are two records that has to be completed
name1: selector1._domainkey
value: selector1-company-com01b._domainkey.companyadmin.onmicrosoft.com

name2: selector2._domainkey
value: selector2-company-com01b._domainkey.companyadmin.onmicrosoft.com

What do you do after you have edited the DNS records

Once you have entered the two x CNAME records go back to the O365 admin console where you got the two records from and after 10 minutes you can then enable the DKIM signing.

this depends on what DNS provider the company uses.