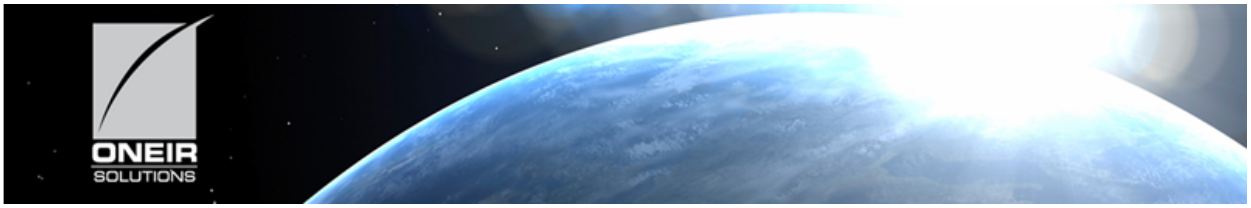
Oneir Email System



Emailing with Oneir

Last Edit: December 23rd, 2025

Emails created by Oneir Accounting system go through Perfect Mail and are forwarded to your email service used by your domain.

What the new Email problem is:

Things started to change in late 2024 / early 2025. In the last year, large mail providers (Google, Microsoft, Outlook and many others) have implemented new standards to verify and authenticate all e-mail transactions. To this end, they have mandated the use of 2 additional technologies DKIM and DMARC.

Systems that do not implement DKIM and DMARC or systems that incorrectly implement DKIM and DMARC often **have their e-mails rejected outright or redirected into Spam / Junk folders – thereby reducing the effective delivery rate of their e-mails.**

1. **DKIM**, or DomainKeys Identified Mail, is an email authentication method that allows the owner of a domain to sign their emails with a digital signature. This signature helps verify that the email was sent by the legitimate domain owner and that its content has not been altered during transmission

2. **DMARC**, or Domain-based Message Authentication, Reporting, and Conformance, is an email authentication protocol that helps protect email domains from unauthorized use, such as spoofing and phishing attacks. It allows domain owners to specify how receiving email servers should handle messages that fail authentication checks, improving email security and deliverability.

How do emails go from Oneir to End Recipients:

1. When a current Oneir client sends an e-mail, it goes through the Perfect Mail relay service.

2. Perfect Mail then delivers that e-mail through the Oneir client's e-mail service using the latest standards for e-mail authentication and verification including SPF, DMARC and DKIM

3. The Oneir client's mail server then forwards Perfect Mail e-mail to their customer through their e-mail service. This is where the problem is occurring; the Oneir client mail server is configured by their local technician and / or service provider, who may or may not be fully up to date on e-mail standards (SPF, DKIM, DMARC) for acceptable mail delivery.

4. Oneir can provide documentation on how to assist an Oneir client to create Sender Policy Framework (SPF) DNS records so that their customers can verify that the e-mail originates with Oneir customer's mail server (and isn't being spoofed by a spammer).

   SPF records must be created by the client, in their own domain DNS records, to specify which mail servers (by IP address) are permitted to send e-mail on behalf of the client's domain. This does a good job of shutting down spoofing by allowing peer mail servers to reject all e-mail from the client's domain that doesn't come from mail server(s) identified by a DNS SPF record.

The issue is that Perfect Mail accepts e-mail from Oneir VMs and send it directly to the client's mail server using correct SPF, DKIM and DMARC records, but the client's mail server then forwards e-mail to their customers often with missing or mis-configured SPF, DMARC or DKIM records. This results in the receiving mail server rejecting or spam quarantining e-mail from your customer's mail server to their customer's mail server.

There is nothing Perfect Mail can do directly that can change this because they have no control over what Oneir's clients do to manage their local mail services. Furthermore, we have no ability to add DMARC and DKIM functionality to Oneir client's mail server.

Oneir has partnered with a 3rd party provider to provide solutions for these email issues:

Oneir had a 3rd party provider write a program to address these issues and have them automatically integrated with Oneir.

There is a small fee of $495.00 for this service.

We have installed this in dozens of Oneir clients and it solved their issues immediately.

If you are interested in this solution, please reach out to Steve Lowe and Professional Services, slowe@oneirsolutions.com

Additional papers written by Perfect Mail on this topic:

1. *https://perfectmail.com/learn/authentication*,
2. *https://perfectmail.com/learn/spf*,
3. *https://perfectmail.com/learn/dkim*,
4. *https://perfectmail.com/learn/dmarc*
5. https://perfectmail.com/learn/ip-rev

Step by Step how to resolve the email blocking issues

One of Oneir's clients has an in-house tech department; they provided us with the below document after they had resolved all their email blocking issues .

SPF, DKIM, and DMARC: Enhancing Email Security

Introduction

Email security is crucial for protecting organizations from phishing, spoofing, and other malicious activities. Three key email authentication protocols—SPF, DKIM, and DMARC—play a vital role in ensuring the integrity and authenticity of email communications.

SPF (Sender Policy Framework)

SPF is an email validation system designed to prevent email spoofing. It allows domain owners to specify which mail servers are permitted to send emails on behalf of their domain.

- **How it works**: Domain owners publish SPF records in their DNS settings, listing authorized mail servers. When an email is received, the recipient's mail server checks the SPF record to verify the sender's IP address.
- **Significance**: SPF helps prevent unauthorized emails from being sent from your domain, reducing the risk of spam and phishing attacks.

DKIM (DomainKeys Identified Mail)

DKIM adds a digital signature to outgoing emails, allowing the recipient to verify that the email was indeed sent by the domain owner and that it hasn't been altered during transit.

- **How it works**: The sending mail server generates a unique cryptographic signature for each email, which is embedded in the email header. The recipient's mail server retrieves the DKIM signature and verifies it against the public key stored in the sender's DNS records.
- **Significance**: DKIM ensures the integrity of the email content and enhances the sender's reputation, leading to better email deliverability.

DMARC (Domain-based Message Authentication, Reporting, and Conformance)

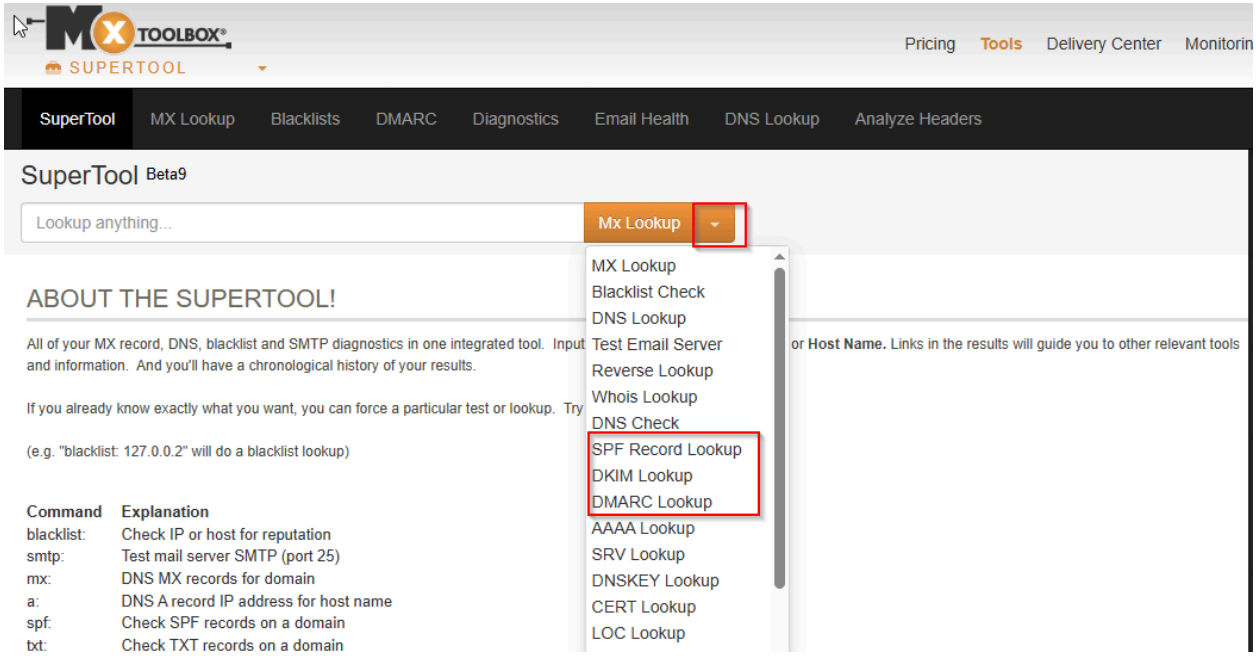
DMARC builds on SPF and DKIM by providing a framework for handling unauthenticated emails. It allows domain owners to specify how emails that fail SPF or DKIM checks should be treated.

- **How it works**: Domain owners publish DMARC records in their DNS settings, specifying their desired policy (e.g., "none," "quarantine," or "reject"). DMARC also enables domain owners to receive reports on email authentication failures.
- **Significance**: DMARC ensures consistent email authentication across domains, helps prevent phishing attacks, and improves overall email security.

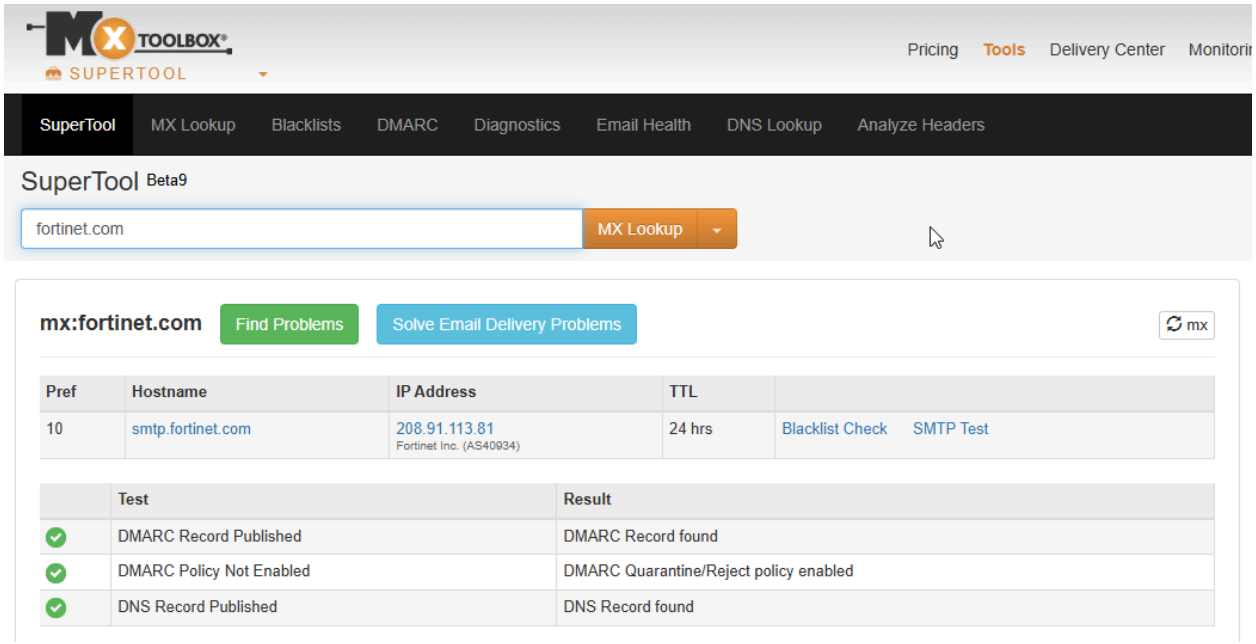
Verification of Records

Before initiating the setup of email security protocols, it is essential to assess the current configuration using MXToolbox. This evaluation will help determine whether existing email security measures are in place or if modifications are required.

These records can be verified at **https://mxtoolbox.com/SuperTool.aspx**



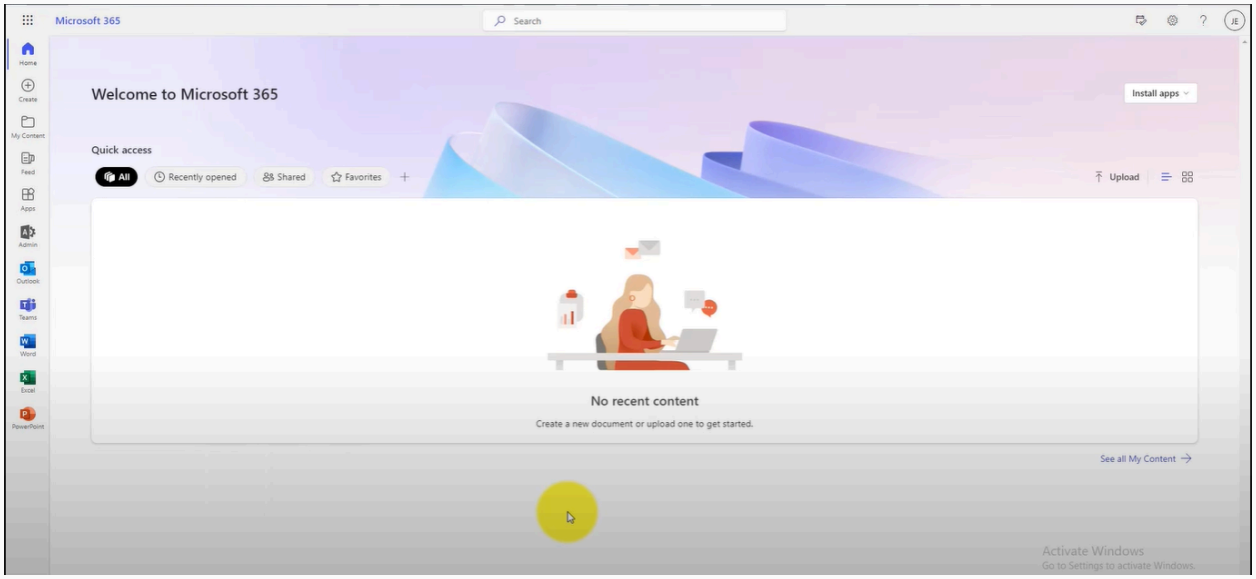
Enter your domain name and check all three records and their values configured.



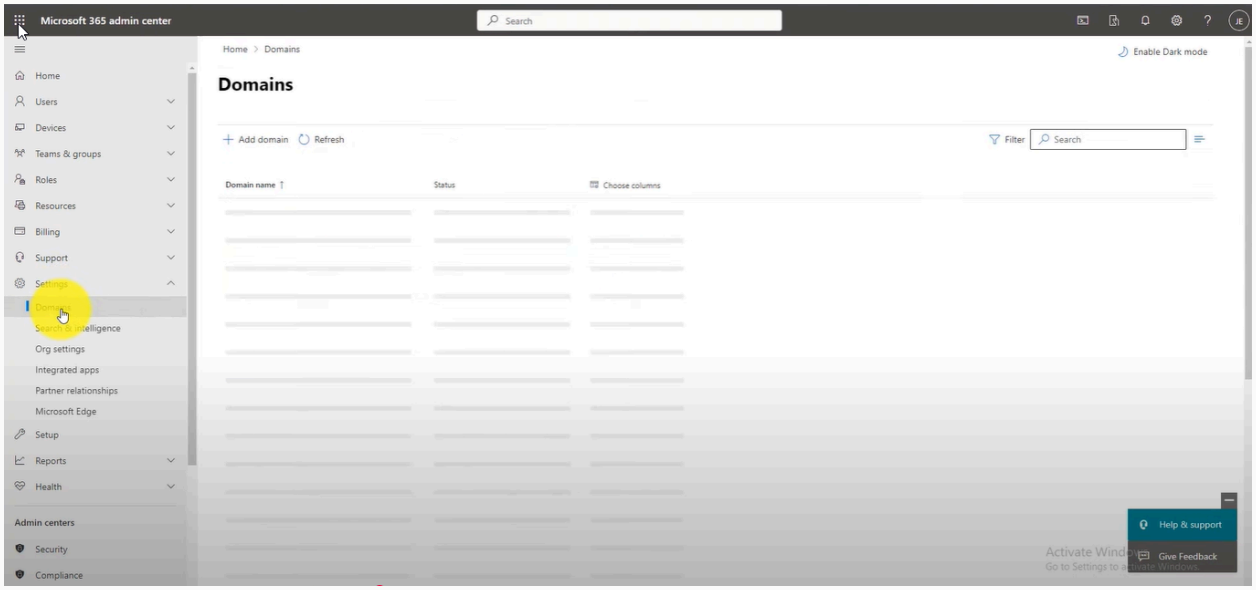
SPF record:

Login to Microsoft admin panel

admin.microsft.com

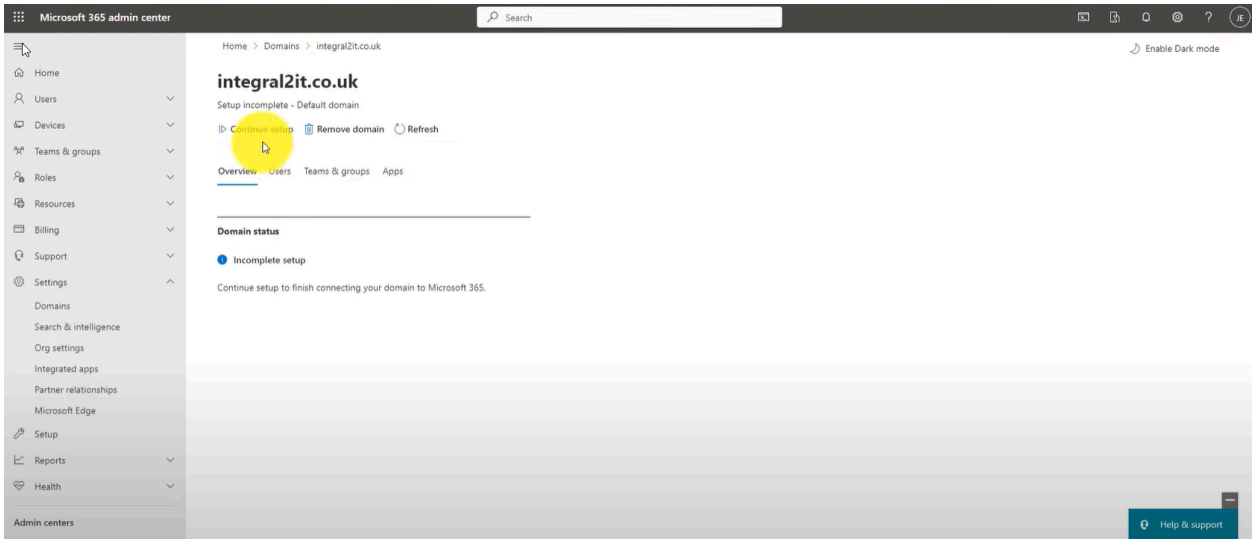


Settings □ Domain

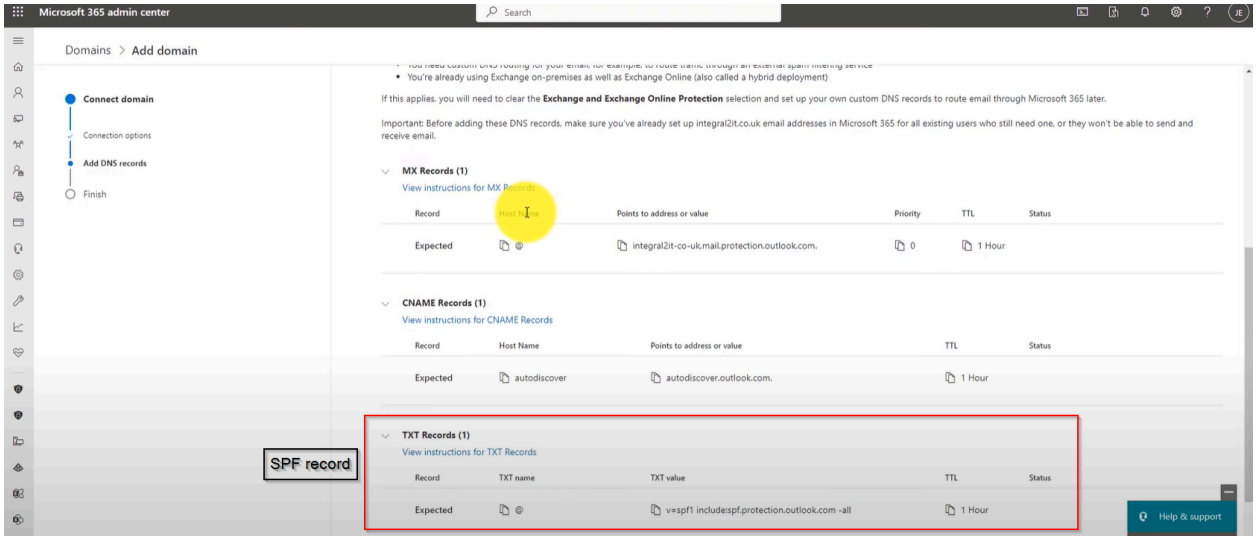


Click on your domain continue setup

Note: you might see incomplete setup at the bottom



Continue setup



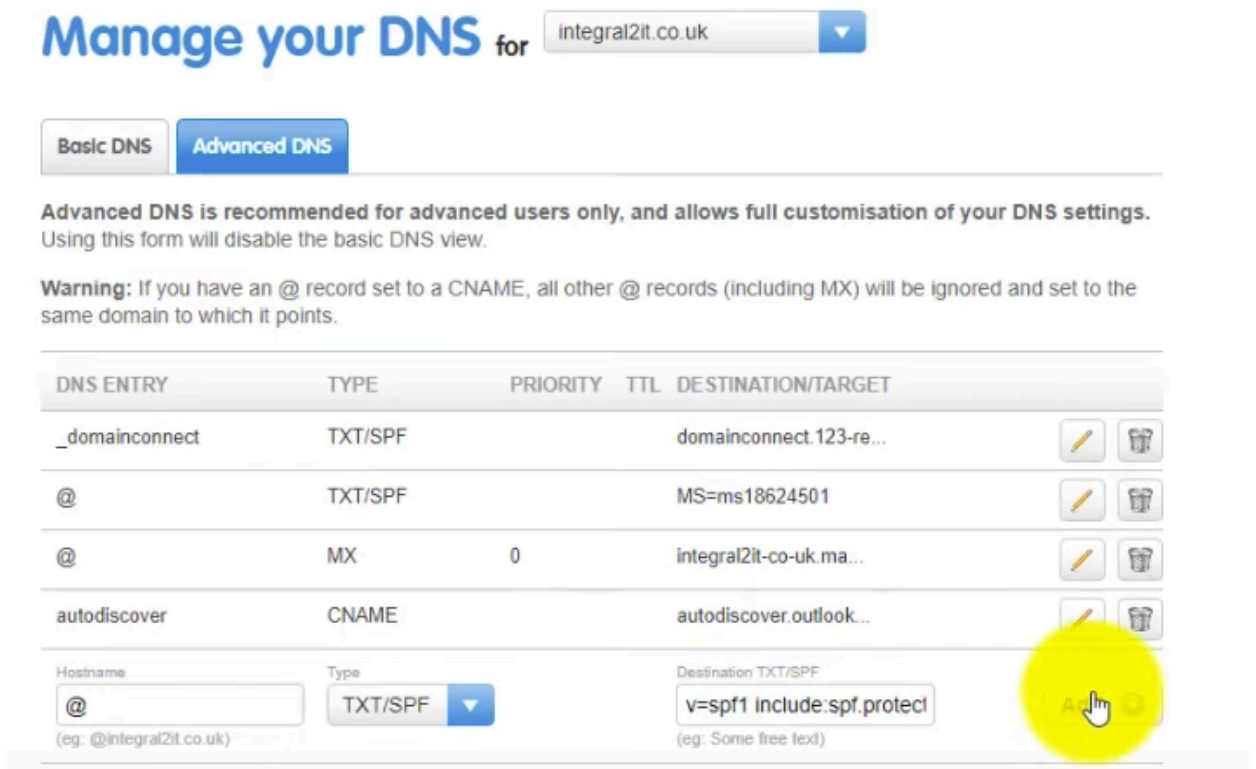
Make sure to ass this record on your hosting DNS panel

Hostname: @

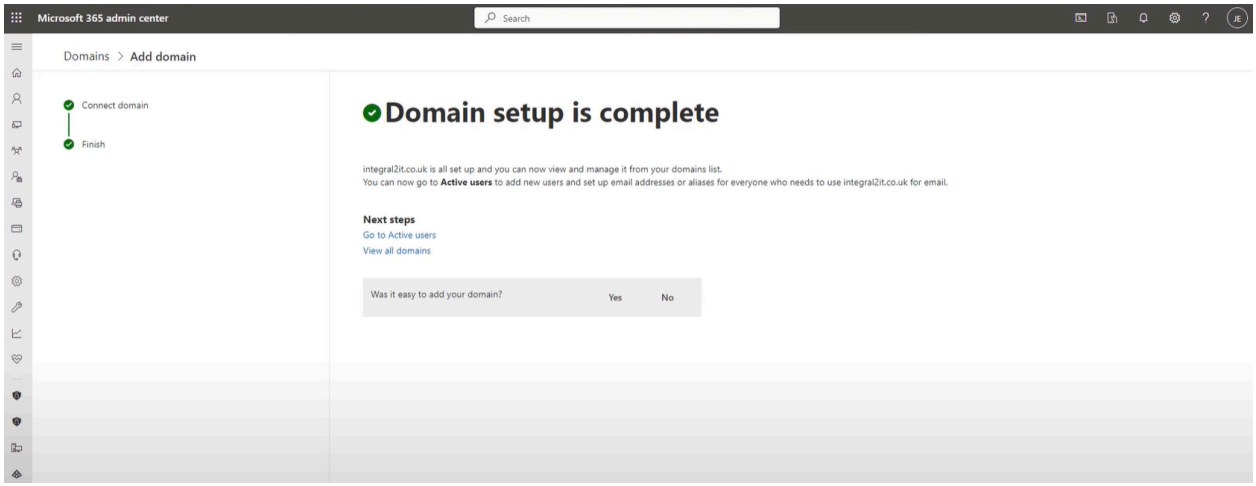
Type: TXT

Value: v=spf1 include:spf.protection.outlook.com

Click on save and continue.

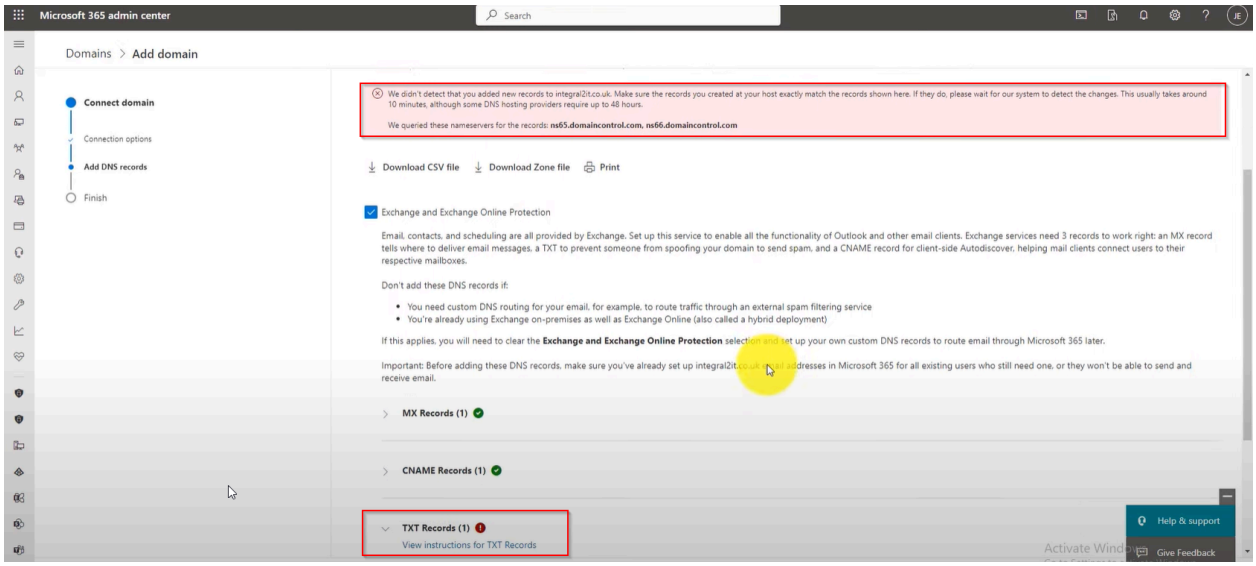


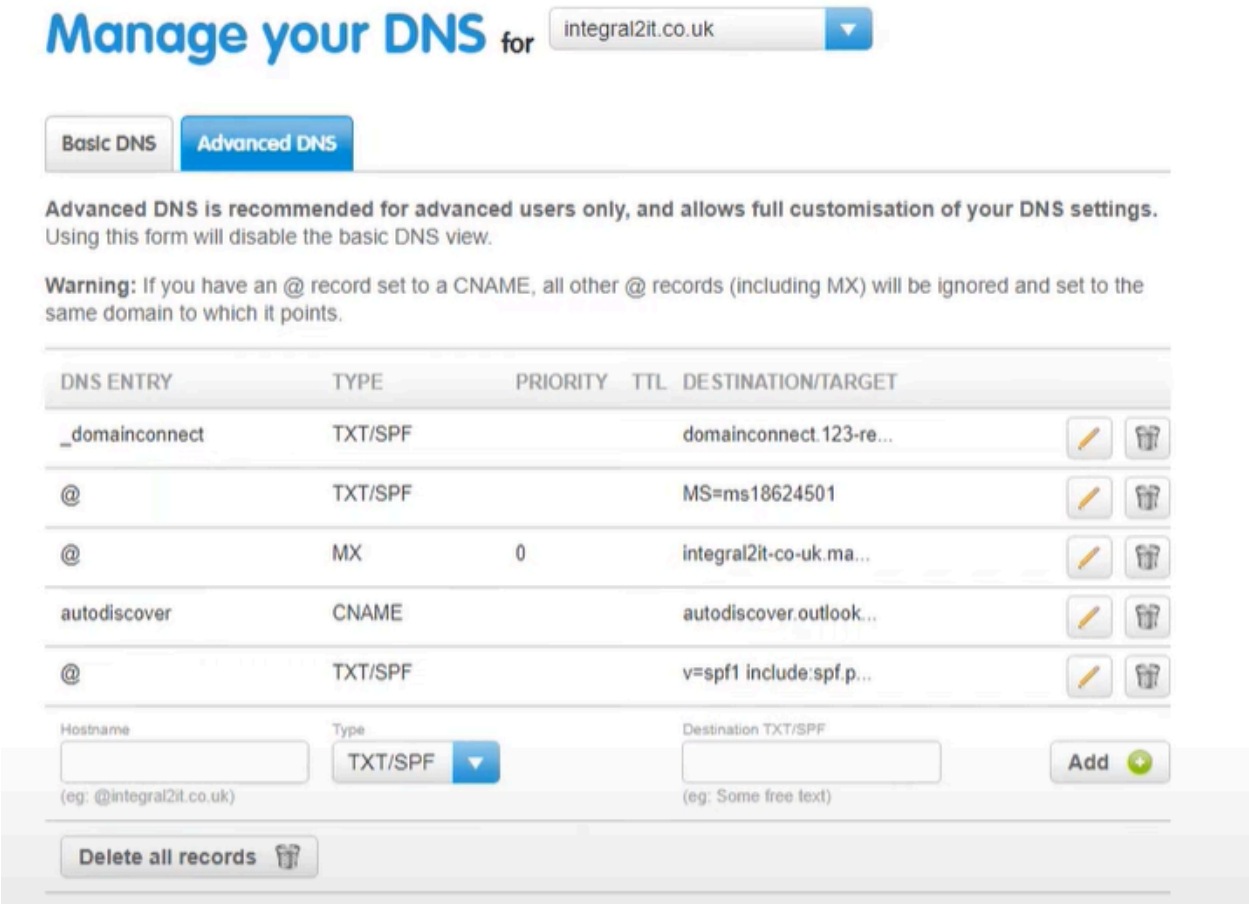
If the values are successfully added go back to the Microsoft admin panel and click on verify.



This might take from a few minutes to a few hours to complete, but if you receive any error check for accuracy and retry to verify the domain again.

Error message attached.

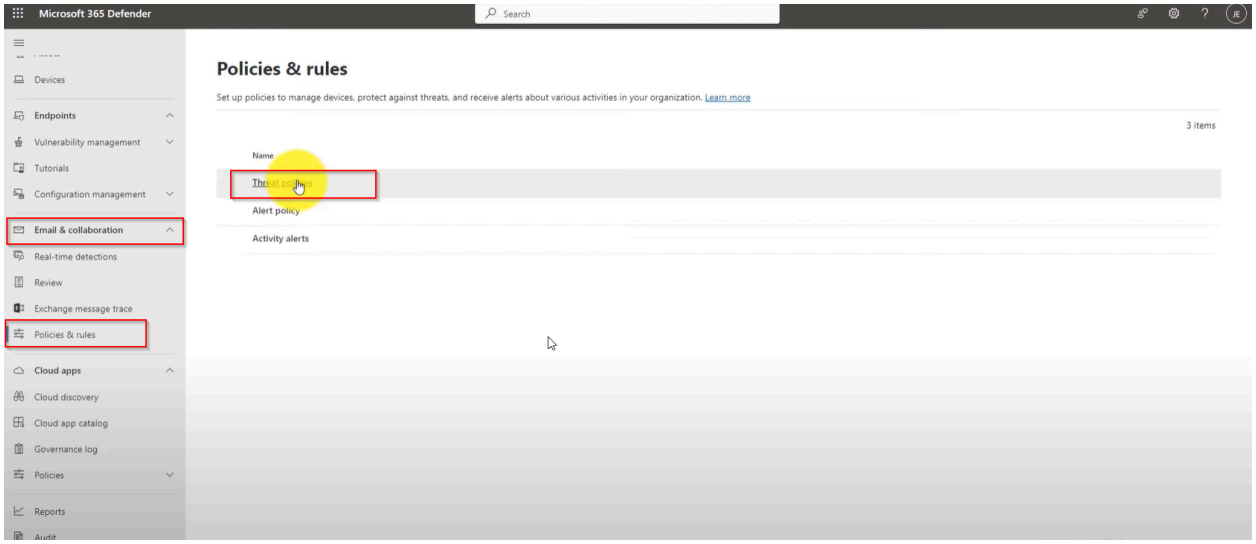


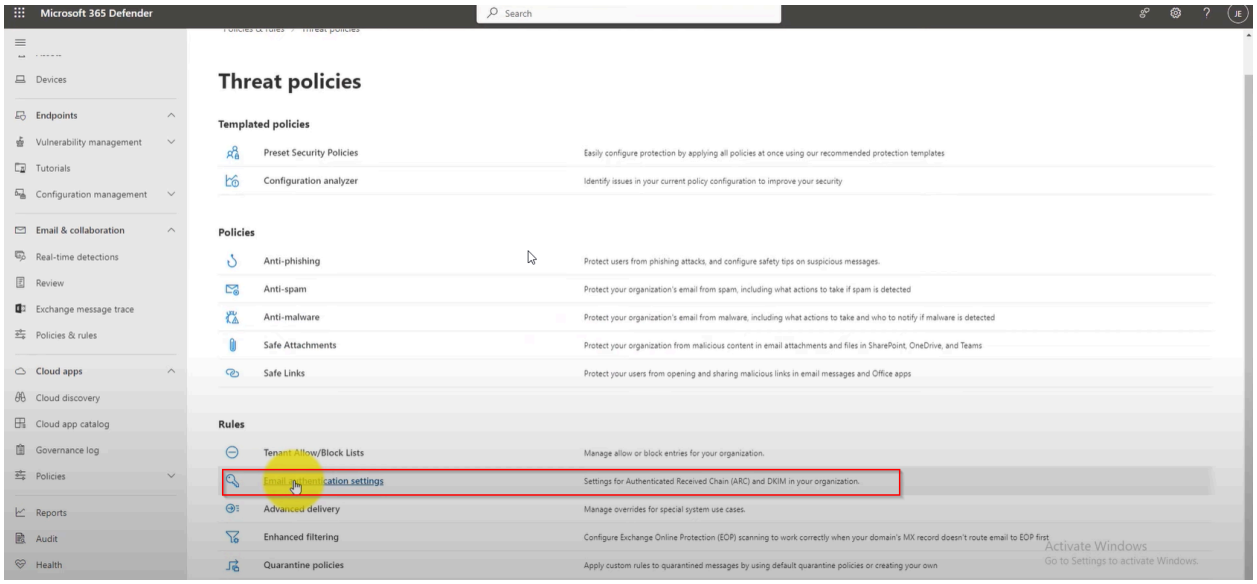


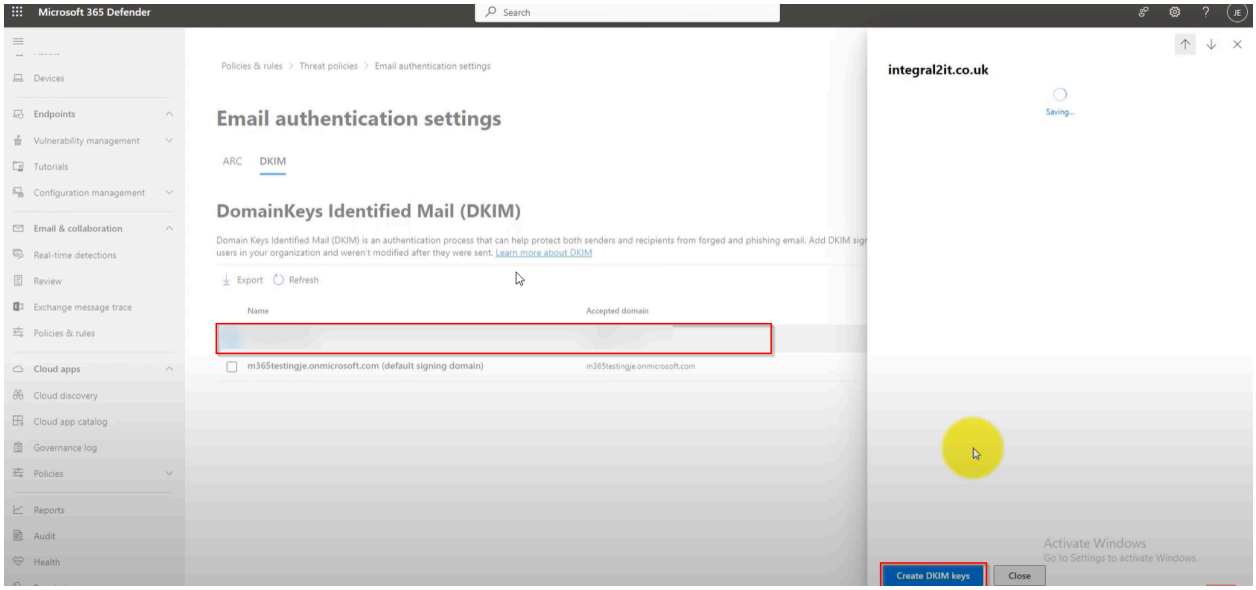
DKIM record:

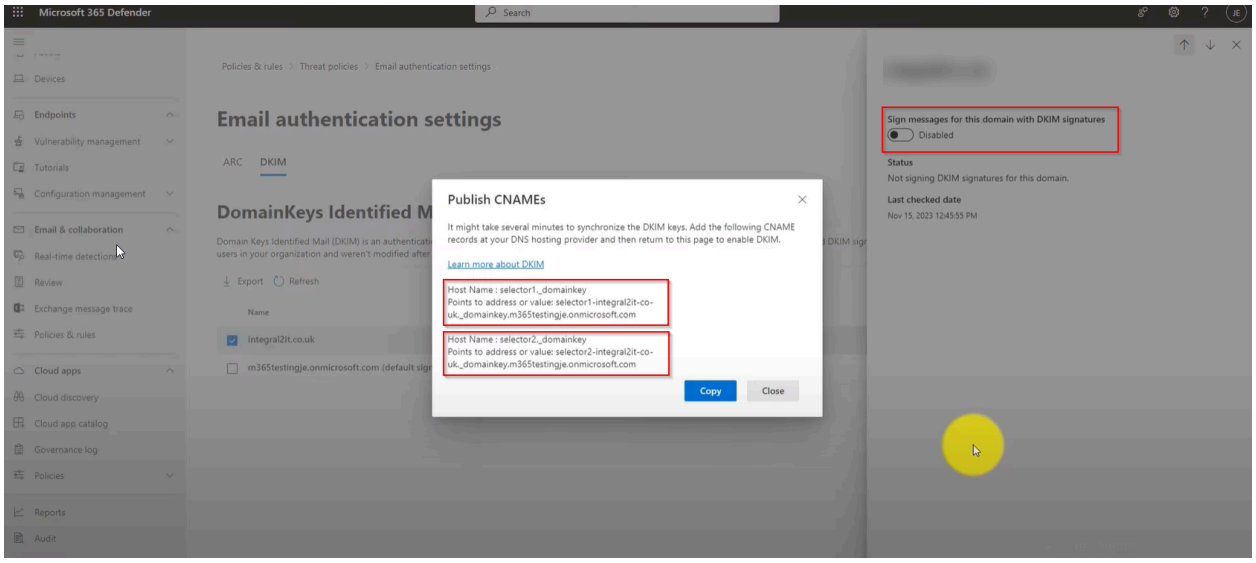
Navigate to admin center Security tab or http://security.microsoft.com.

Email and collaboration exchange message trace DKIM Domain name Create DKIM keys.


Microsoft 365 Defender
Search
Devices
Endpoints
Vulnerability management
Tutorials
Configuration management
Email & collaboration
Real-time detections
Review
Exchange message trace
Policies & rules
Cloud apps
Cloud discovery
Cloud app catalog
Governance log
Policies
Reports
Audit
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
Alert policy
Activity alerts


Microsoft 365 Defender
Search
Devices
Endpoints
Vulnerability management
Tutorials
Configuration management
Email & collaboration
Real-time detections
Review
Exchange message trace
Policies & rules
Cloud apps
Cloud discovery
Cloud app catalog
Governance log
Policies
Reports
Audit
Health
Threat policies
Templated policies
Preset Security Policies
Easily configure protection by applying all policies at once using our recommended protection templates
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 notify if malware is detected
Safe Attachments
Protect your organization from malicious content in email attachments and files in SharePoint, OneDrive, and Teams
Safe Links
Protect your users from opening and sharing malicious links in email messages and Office apps
Rules
Tenant Allow/Block Lists
Manage allow or block entries for your organization.
Settings for Authenticated Received Chain (ARC) and DKIM in your organization.
Advanced delivery
Manage overrides for special system use cases.
Enhanced filtering
Configure Exchange Online Protection (EOP) scanning to work correctly when your domain's MX record doesn't route email to EOP first
Quarantine policies
Apply custom rules to quarantined messages by using default quarantine policies or creating your own
Activate Windows
Go to Settings to activate Windows.





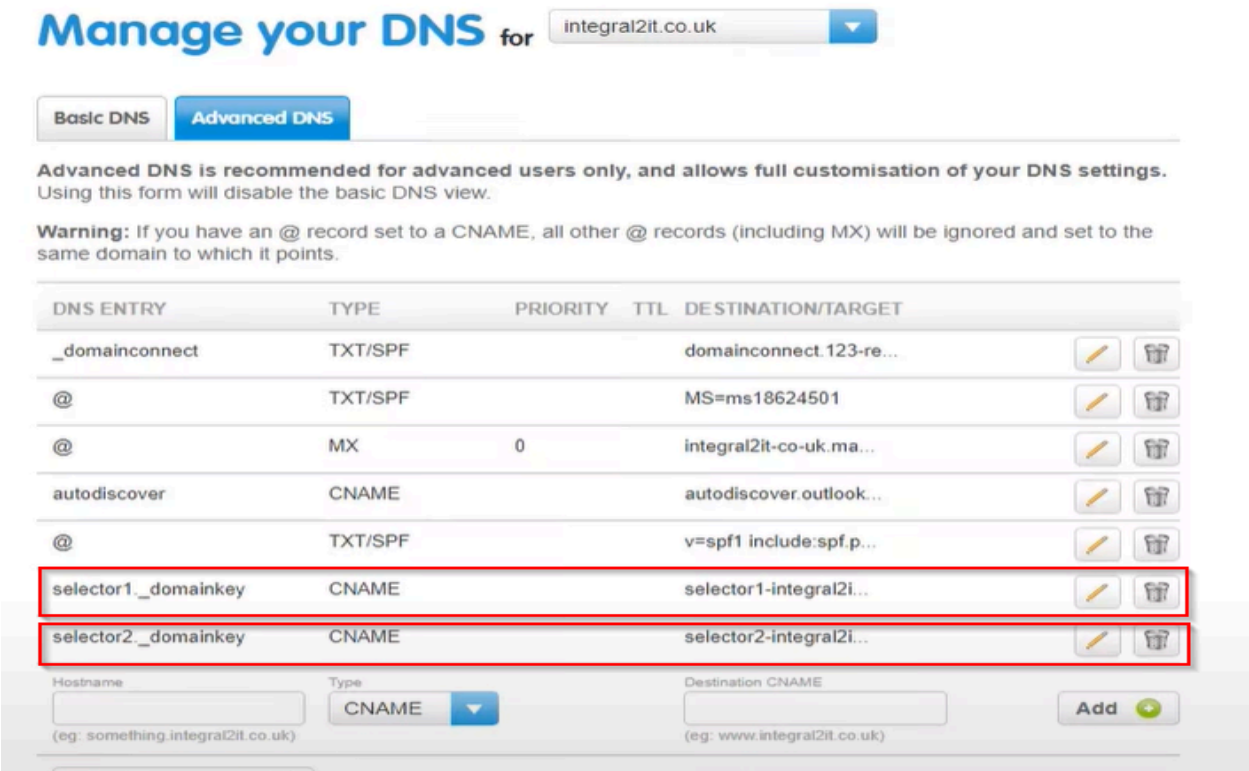
Microsoft provides you with values to be added to your DNS panel.

Add all the provided values and click verify on the Microsoft admin panel.

Example:

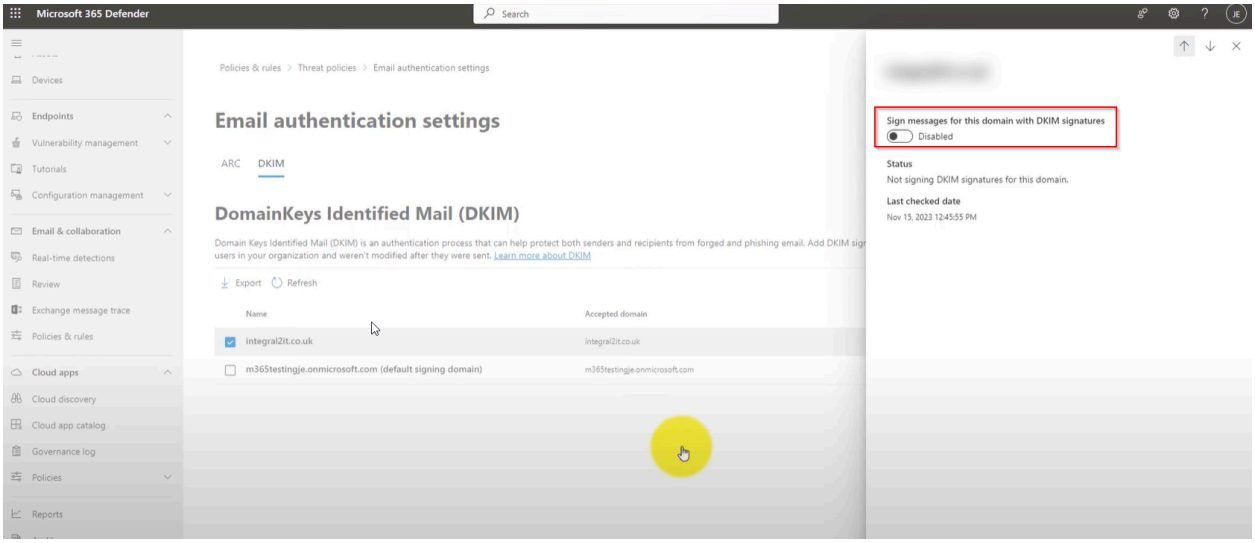
Hostname: selector1._domainkey

Value: selector1-your_domain._domainkey.365testings.com

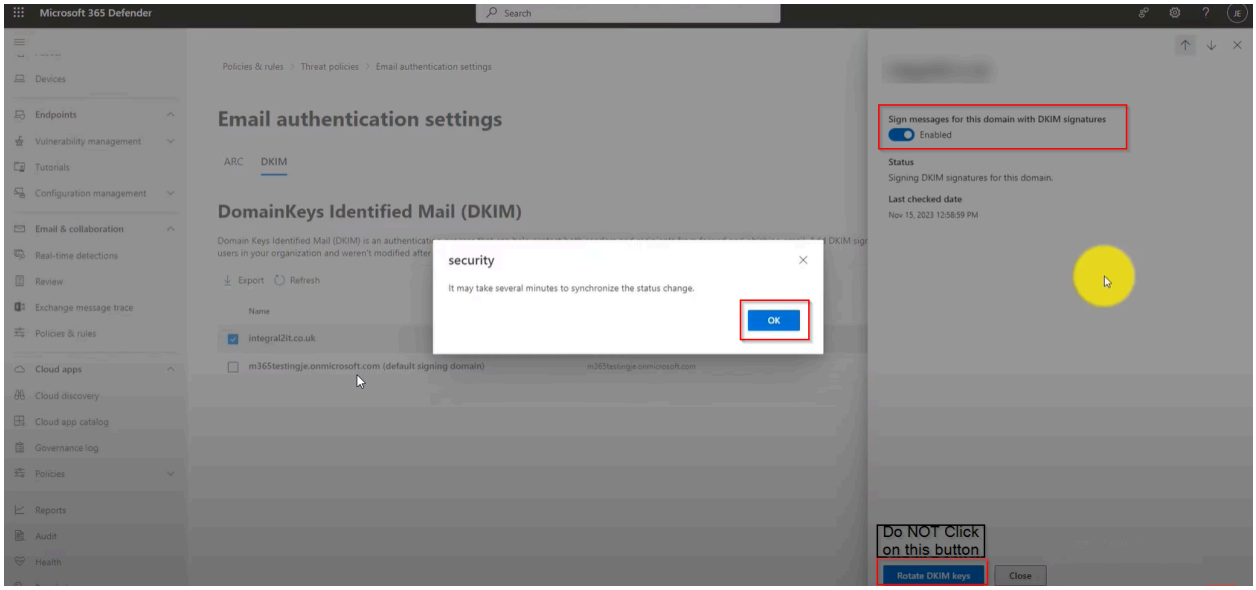


Click on enable toggle to verify the records.

Note: this might take anywhere between a couple of minutes to hours.



DO NOT click on the "Rotate DKIM keys" at the bottom (which renews the keys at random intervals and has to be manually updated on the DNS hosting panel.)



DKIM record (optional):

1. Ensure SPF and DKIM are Configured

Before setting up DMARC, make sure your domain has SPF and DKIM records configured.

2. Create a DMARC Record

Log in to your DNS hosting provider.

Navigate to the DNS management section.

Add a **new TXT record** with the following details:

Name: _dmarc.yourdomain.com

Type: TXT

Value: v=DMARC1; p=none; rua=mailto:dmarc-reports@yourdomain.com; ruf=mailto:dmarc-failures@yourdomain.com;

3. Define DMARC Policy

p=none: No action is taken on emails that fail DMARC checks.

p=quarantine: Emails that fail DMARC checks are marked as suspicious.

p=reject: Emails that fail DMARC checks are rejected outright.

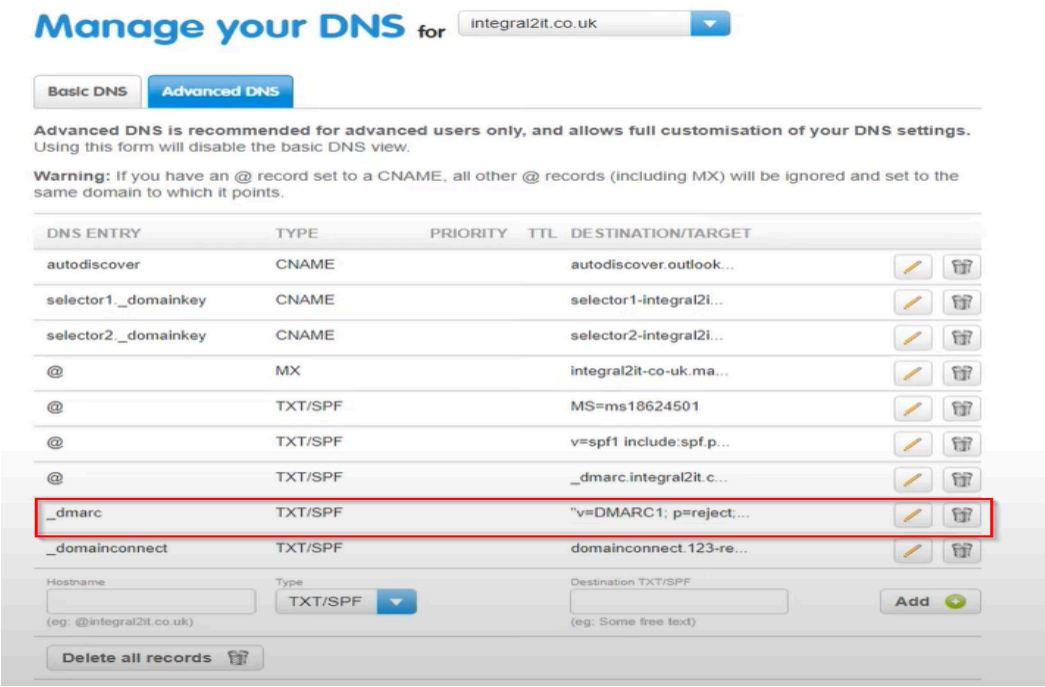
4. Specify Reporting Options

rua: Aggregate reports (summary of DMARC results).

ruf: Forensic reports (detailed reports on DMARC failures).

5. Publish the DMARC Record

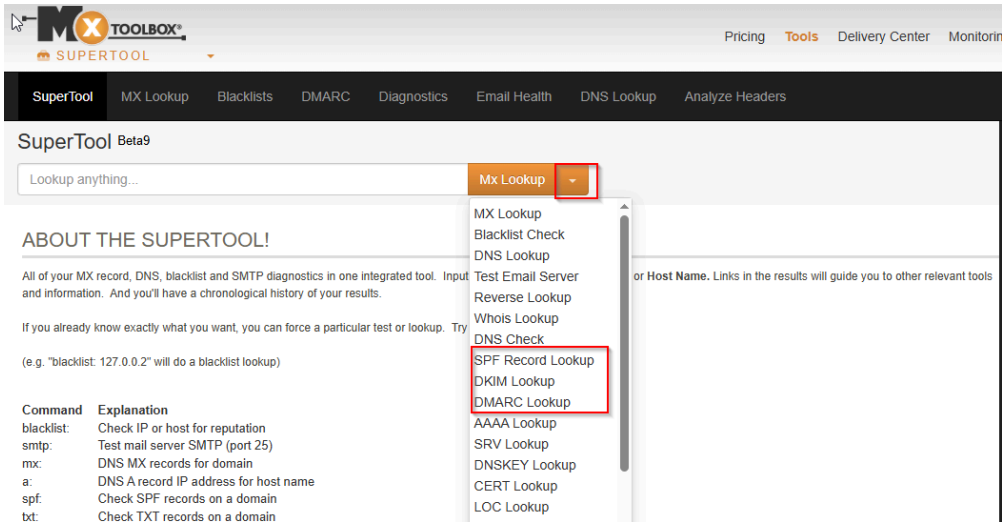
Save the TXT record in your DNS settings to publish the DMARC policy.



Validation of Records

Assess your records to make sure the updates have been published.

These records can be verified at **https://mxtoolbox.com/SuperTool.aspx**


MX TOOLBOX
SUPERTOOL
Pricing
Tools
Delivery Center
Monitorin
SuperTool
MX Lookup
Blacklists
DMARC
Diagnostics
Email Health
DNS Lookup
Analyze Headers
SuperTool Beta9
Lookup anything...
Mx Lookup
MX Lookup
Blacklist Check
DNS Lookup
Test Email Server
Reverse Lookup
Whois Lookup
DNS Check
SPF Record Lookup
DKIM Lookup
DMARC Lookup
AAAA Lookup
SRV Lookup
DNSKEY Lookup
CERT Lookup
LOC Lookup
ABOUT THE SUPERTOOL!
All of your MX record, DNS, blacklist and SMTP diagnostics in one integrated tool. Input
or Host Name. Links in the results will guide you to other relevant tools
and information. And you'll have a chronological history of your results.
If you already know exactly what you want, you can force a particular test or lookup. Try
(e.g. "blacklist: 127.0.0.2" will do a blacklist lookup)
Command
Explanation
blacklist:
Check IP or host for reputation
smtp:
Test mail server SMTP (port 25)
mx:
DNS MX records for domain
a:
DNS A record IP address for host name
spf:
Check SPF records on a domain
txt:
Check TXT records on a domain