

Region 9 IT Follow-Up Task

Verify SPF, DKIM, and DMARC for Microsoft 365 Email Domains

Purpose. During the Region 9 discussion, it was noted that some offices may not have SPF, DKIM, and DMARC fully configured. This follow-up provides a simple verification process for offices using Microsoft 365. The initial DNS checks are read-only and do not change your environment.

Important distinction: A message can show SPF, DKIM, and DMARC as PASS while DKIM is still signing with the Microsoft tenant domain (for example, `yourdomain.onmicrosoft.com`) instead of the office's custom domain (`yourdomain.com`). The Gmail test in Step 5 is included specifically to identify that condition.

Before You Begin

Replace **yourdomain.com** in the examples with the domain after the @ in your office email address. Example: if your email is `name@example.org`, use `example.org`.

Checks 1-3	Require only PowerShell plus Internet/DNS access. No Microsoft 365 sign-in is required.
Check 4	Requires the Exchange Online PowerShell module, Internet access to Microsoft 365, and an authorized Microsoft 365/E
Check 5	Requires sending a new message to an external Gmail mailbox and viewing the original message headers.

1. Verify SPF

Open Windows PowerShell and run:

```
Resolve-DnsName yourdomain.com -Type TXT -Server 8.8.8.8
```

Find the TXT record beginning with `v=spf1`. For an office sending through Microsoft 365, the SPF record commonly includes:

```
include:spf.protection.outlook.com
```

Your SPF record may legitimately include other mail services, gateways, or sending IP addresses. There should normally be only one SPF record beginning with `v=spf1`. Do not modify SPF simply because your result differs from another office.

2. Verify the Microsoft 365 DKIM DNS Selectors

Run both commands:

```
Resolve-DnsName selector1._domainkey.yourdomain.com -Type CNAME -Server 8.8.8.8  
Resolve-DnsName selector2._domainkey.yourdomain.com -Type CNAME -Server 8.8.8.8
```

For a Microsoft 365 custom-domain DKIM configuration, both names should resolve to Microsoft-provided CNAME targets. If either returns **DNS name does not exist**, the custom-domain DKIM configuration should be reviewed by the office's Microsoft 365/DNS administrator.

3. Verify DMARC

Run:

```
Resolve-DnsName _dmarc.yourdomain.com -Type TXT -Server 8.8.8.8
```

Look for a TXT record beginning with `v=DMARC1`. The policy may contain `p=none`, `p=quarantine`, or `p=reject`. Finding a DMARC record confirms publication; determining the appropriate enforcement policy requires knowledge of all legitimate systems that send mail for the domain.

4. Verify DKIM Inside Microsoft 365

This is the Microsoft 365-specific portion. The computer running PowerShell must be able to reach Microsoft 365. You also need the Exchange Online PowerShell module and an account with sufficient Exchange Online permissions.

If the Exchange Online module is not installed:

```
Install-Module ExchangeOnlineManagement
```

Then load the module and connect:

```
Import-Module ExchangeOnlineManagement Connect-ExchangeOnline
```

Sign in when prompted using an authorized Microsoft 365 account. Then run:

```
Get-DkimSigningConfig -Identity yourdomain.com | Format-List  
Domain, Enabled, Status, Selector1CNAME, Selector2CNAME
```

For an enabled custom-domain Microsoft 365 DKIM configuration, the desired result is:

```
Enabled : True Status : Valid
```

If Microsoft reports CnameMissing, compare the Selector1CNAME and Selector2CNAME values returned by Microsoft with the public DNS results from Step 2. Coordinate corrections with whoever manages your DNS. Do not guess the Microsoft CNAME targets.

5. Perform the External Gmail Test - Do Not Skip This

This verifies what an external recipient actually sees after the message leaves your environment.

1. Send a **new** email from your office Microsoft 365 account to an external Gmail account.
2. In Gmail, open the message.
3. Select the three-dot **More** menu and choose **Show original**.
4. Confirm that Gmail reports **SPF: PASS, DKIM: PASS, and DMARC: PASS**.
5. Then inspect the DKIM signing domain. This is the important extra check.

A fully aligned custom-domain result should show DKIM associated with your office domain, for example:

```
dkim=pass header.i=@yourdomain.com header.s=selector1
```

You may instead see DKIM pass using a Microsoft tenant identity such as:

```
d=yourdomain.onmicrosoft.com
```

That is an important distinction: a PASS result by itself does not prove that custom-domain DKIM is enabled. Microsoft 365 can sign using an onmicrosoft.com identity. For this follow-up task, verify that DKIM is signing with your organization's actual custom email domain whenever custom-domain DKIM is expected.

6. Record Your Results

Item	What to Record
SPF	Published? Microsoft 365 included? PASS in Gmail?
DKIM DNS	Selector 1 resolves? Selector 2 resolves?
M365 DKIM	Enabled = True? Status = Valid?
Gmail DKIM	PASS? Signing domain = your custom domain or onmicrosoft.com?
DMARC	Published? Policy (none/quarantine/reject)? PASS in Gmail?

Safety / Change Control

This document is intended primarily for verification. Do not change SPF, DKIM, or DMARC records solely because one test fails. Mail authentication settings can affect delivery for Microsoft 365, security gateways, scanners, applications, vendors, and other systems that send mail using your domain. Coordinate remediation with your Microsoft 365 administrator and DNS provider.

Region 9 follow-up objective: Each office should be able to identify whether SPF, DKIM, and DMARC are present, verify Microsoft 365 DKIM status where applicable, and confirm through an external Gmail test whether the custom domain is actually being used for DKIM signing.