**Step by Step instructions for setting up ATP - SPF, DKIM, and DMARC**

**SPF or Anti-Spoofing**

To set up SPF you’ll need to update DNS so you can use Sender Policy Framework with your custom domain.

1. Log into O365 and go into Admin Center
2. Once inside the Microsoft 365 admin center, go to the Setup --> Domains page. Click the domain name you wish to send emails from.
3. Add New Custom Record, Select TXT
4. If you are fully hosted by O365 with nothing on prem, enter “v=spf1 include:spf.protection.outlook.com -all” This SPF record handles protection for most O365 deployments
5. If you still have on prem email services you need to enter “v=spf1 and below options”  
   ip4:< *IP address*>

ip6:< *IP address*>

include:< *domain name*>

Where the value for < *IP address*> is the IP address of the other mail system and < *domain name*> is the domain name of the other mail system that sends mail on behalf of your domain.

1. If you send from a 3rd party mail system you’ll have to get the spf information domain information from them and add in “v=spf1 include: and the below information from your 3rd party email system.

include:<domain name>

Where domain name is the domain name of the third party email system.

**DKIM - Adding a Domain Keys Identified Mail encryption signature to your email system**

To set up DKIM you’ll need to set up 2 cnames for each domain in your external DNS you want to send emails from. For O365 the selectors will always be selector 1 and selector2. Also, your intial domain is the domain you used to signed up for office 365 with the onmicrosoft.com. In this example of CNAMES we’ll use xyz.com

1. Create CNAME for Selector1 should look like this.  
   selector1.\_domainkey

Points to address or value: \*\*selector1-xyz-com\*\*.\_domainkey.xyz.onmicrosoft.com

TTL: 3600

1. Create CNAME for Selector2 which is basically the same as 1 except you replace the 1 with a 2.

selector2.\_domainkey

Points to address or value: \*\*selector2-xyz-com\*\*.\_domainkey.xyz.onmicrosoft.com

TTL: 3600

Your DNS record should look like this (replace the 1 with a 2 for the second one)

DNS type - CNAME

host name - selector1.\_domainkey

Address/value - selector1-YourDomain-com.\_domainkey.YourDomain.onmicrosoft.com

3. Next you have to enable DKIM by either the GUI or PowerShell. I’ll use Powershell for this example since I think it’s faster and easier.

4. Run the following Commands

1. $credential = Get-credential
2. $exchange - newpssession -configurationname microsoft.eschange -connectionuri “<https://outlook.office365.com/powershell-liveid>[/](https://outlook.office365.com/powershell-liveid/)“ -credential $credential -autnentication “basic” -allowredirection
3. import-pssession $exchange
4. New-DkimSigningConfig -DomainName xyz.com -Enabled $true

**DMARC - Validating outbound emails**

Once you have SPF and DKIM running, DMARC is just 1 DNS record.

1. Same as SPF - for each domain enter a txt record named DMARC. This is the most commonly used setting for DMARC although you can customize it if you’d like. For customizing this, go to Microsoft.com and look up how to modify the settings.

Your text record should look like this.

DNS type - TXT

Host name - \_dmarc.whaever-the-domainname-is.com

Address or value - v=DMARC1; p=none; pct=100; rua=mailto:d@rua.agari.com; ruf=mailto:d@ruf.agari.com; fo=1

*See Setting up ATP Policies - Step by step for setting up ATP Anti-phishing, Safelinks, Safe Attachments*