



## CyberWarden MailAegis Setup Steps for Microsoft Office 365 customers

Go to <https://admin.exchange.microsoft.com/#/connectors>

Click on Add a connector

Select Partner organization then click Next

In the Name field type CyberWarden MailAegis Inbound

Optionally add a description

Ensure that the “Turn it on” checkbox is enabled. Click Next

Select the “By verifying that the IP address of the sending server...” radio button

Enter the following IP addresses into the text box, clicking the + button after entering each one:

- 109.228.60.118
- 85.215.201.235
- 212.227.232.71

← ×

### Authenticating sent email

How do you want Office 365 to identify your partner organization?  
Office 365 will only accept messages through this connector if your partner organization can be identified through one of the following two ways.

By verifying that the sender domain matches one of the following domains

By verifying that the IP address of the sending server matches one of the following IP addresses, which belong to your partner organization

Example: 10.5.3.2 or 10.3.1.5/24 +

109.228.60.118	🗑️
85.215.201.235	🗑️
212.227.232.71	🗑️

Save

Click Next



On the Security Restrictions page, ensure that only the “Reject email messages if they aren’t sent over TLS” checkbox is selected, then click Next

← ×

### Security restrictions

What security restrictions do you want to apply?

Reject email messages if they aren't sent over TLS

And require that the subject name on the certificate that the partner uses to authenticate with Office 365 matches this domain name

Example: contoso.com or \*.contoso.com

Save

On the Review Connector page, click the Create connector button, then click Done on the following page.

Go to <https://security.microsoft.com/skiplisting>  
Click on the Cyber Warden MailAegis Inbound connector  
Select the Automatically detect and skip the last IP address radio button  
Select the Apply to entire organization radio button  
Click Save

↑ ↓ ×

### Cyber Warden Mail Aegis

IP addresses to skip ^

Enhanced Filtering for Connector can either detect the IP address or you can define the list of IP addresses you want to skip.

Disable Enhanced Filtering for Connectors

Automatically detect and skip the last IP address

Skip these IP addresses that are associated with the connector: (If your messages pass through multiple gateways, you should include each gateway IP address)

Apply to these users ^

It is recommended that you start with a small subset of users in order to see if Enhanced Filtering is right for your organization.

Apply to entire organization

Apply to a small set of users

Save Close

Wait 10-15 minutes for the changes to propagate throughout the O365 platform, then send a test email from gmail or some other external mail system to your email address to check that everything is working.



In Outlook, view the headers of the received message. You should see no SPF fail or soft fail messages.

See an example of a soft fail below:

```
Authentication-Results: spf=softfail (sender IP is 74.208.88.228)
smtp.mailfrom=gmail.com; dkim=pass (signature was verified)
header.d=gmail.com; dmarc=pass action=none header.from=gmail.com; compauth=pass
reason=100
Received-SPF: SoftFail (protection.outlook.com: domain of transitioning
gmail.com discourages use of 74.208.88.228 as permitted sender)
Received: from mgw03.gdsvc.net (74.208.88.228) by
```

This is the result of the skiplisting configuration – No SPF fail.

```
Authentication-Results: spf=pass (sender IP is 209.85.128.48)
smtp.mailfrom=gmail.com; dkim=pass (signature was verified)
header.d=gmail.com; dmarc=pass action=none header.from=gmail.com; compauth=pass
reason=100
Received-SPF: Pass (protection.outlook.com: domain of gmail.com designates
209.85.128.48 as permitted sender) receiver=protection.outlook.com;
client-ip=209.85.128.48; helo=mail-wm1-f48.google.com; pr=C
Received: from mgw03.gdsvc.net (74.208.88.228) by
```