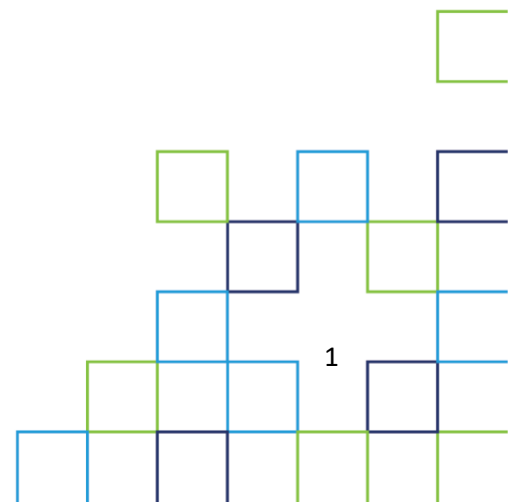


## Office 365 Connector– *aacn.org*



*Prepared By:*  
*--Shivam Shah*  
*--Vatsal Patel*



Issues and requirement of connector:

a) "aacn.org" is using google mail service and same domain is white-listed in office365, so any emails sent or files shared via OneDrive from office365 will remain there due to working of mail service is defined i.e. if the domain is found in local server it won't go to search remote servers.

-→ Due to that connector is required to show directions to the mail i.e. if any emails sent from matching domain then this connector will show the directions of landing that mail.

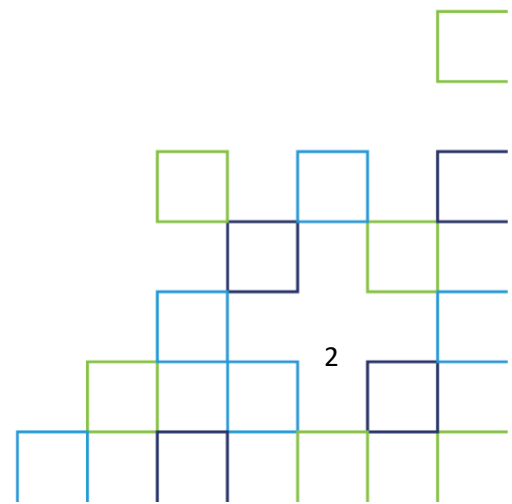
b) After creating connector, mails sent from this domain from office365 were received at google workspace end, but identical username (email address) were not getting emails as it was found at both ends (O365 and Google workspace) and it was getting failed at office365 end as the connector was getting confused.

→ To resolve this we had created connector with transport rule, this will forcefully go to connector without searching locally and then connector will show direction where to land.

c) The connector verifies by sending test mail to remote server user, but it was getting failed because of security.

→ We had whitelisted, office365 exchange IP addresses at Mimecast and Google workspace. Also, sender domains were added in SPF record.

Please check below steps followed in office365 Admin to create a connector successfully.



1. Office365 admin -> Exchange admin center -> mail flow-> connectors -> create a connector.

With From and To settings as below:

**Add a connector**

**New connector**

Specify your mail flow scenario, and we'll let you know if you need to set up a connector.

**Connection from**

☒ Office 365

☐ Your organization's email server

☐ Partner organization

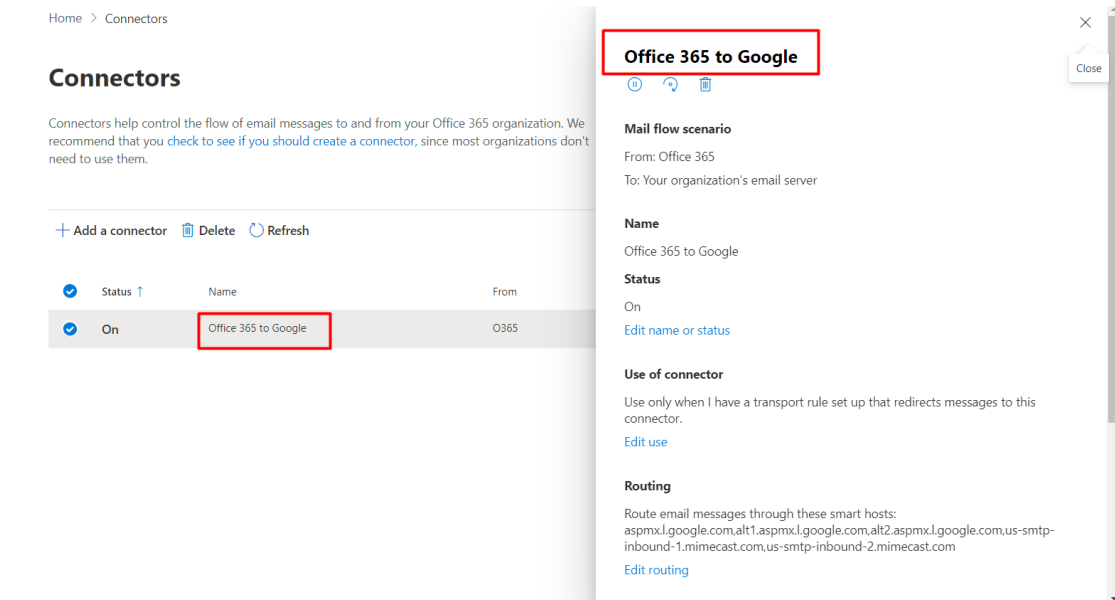
**Connection to**

☒ Your organization's email server

☐ Partner organization

**Next**

## 2. Name the connector:



The screenshot shows the 'Connectors' page in Office 365. A table lists the connectors, with 'Office 365 to Google' highlighted. A side panel for this connector is open, showing details like 'Mail flow scenario', 'Name', 'Status', 'Use of connector', and 'Routing'.

Status	Name	From
On	Office 365 to Google	O365

**Office 365 to Google**

**Mail flow scenario**  
 From: Office 365  
 To: Your organization's email server

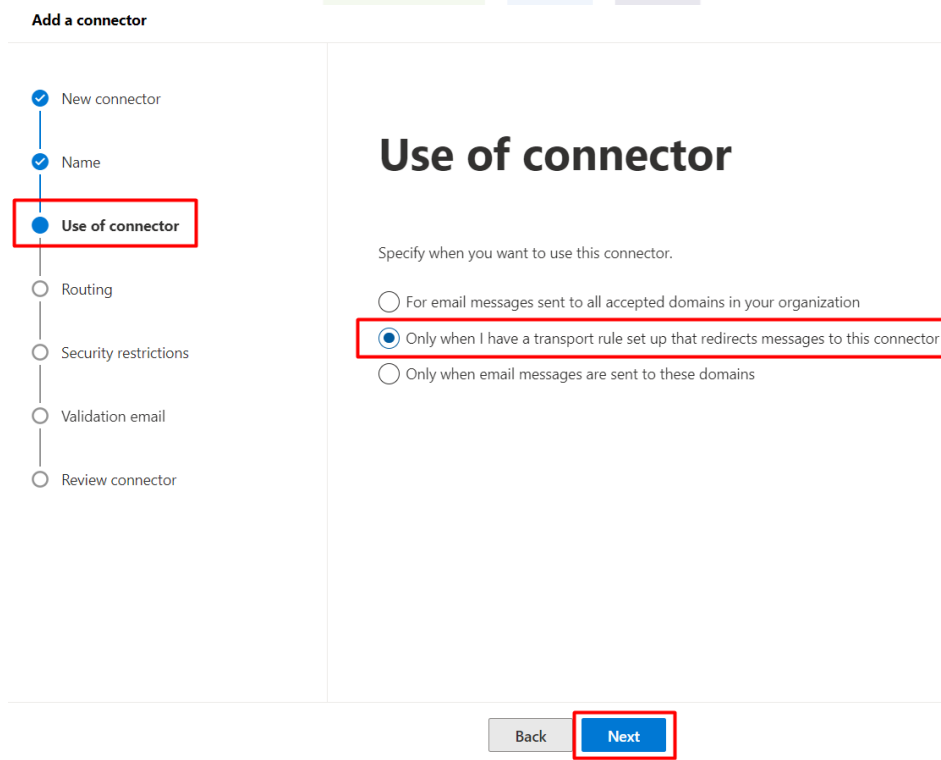
**Name**  
 Office 365 to Google

**Status**  
 On  
[Edit name or status](#)

**Use of connector**  
 Use only when I have a transport rule set up that redirects messages to this connector.  
[Edit use](#)

**Routing**  
 Route email messages through these smart hosts:  
 aspmx.l.google.com,alt1.aspmx.l.google.com,alt2.aspmx.l.google.com,us-smtp-inbound-1.mimecast.com,us-smtp-inbound-2.mimecast.com  
[Edit routing](#)

## 3. Select the usage with transport rule that will redirect the emails to connectors if rule conditions match.



The screenshot shows the 'Add a connector' wizard. The 'Use of connector' step is selected, and the 'Only when I have a transport rule set up that redirects messages to this connector' option is chosen.

**Add a connector**

- New connector
- Name
- Use of connector**
- Routing
- Security restrictions
- Validation email
- Review connector

### Use of connector

Specify when you want to use this connector.

☐ For email messages sent to all accepted domains in your organization  
☒ Only when I have a transport rule set up that redirects messages to this connector  
☐ Only when email messages are sent to these domains

[Back](#) [Next](#)

4. Add remote mail server addresses that can be mx records, domain names or IP addresses depending on mail service provider, in our case it is as below:

## Routing

How do you want to route email messages?

Specify one or more smart hosts to which Office 365 will deliver email messages. A smart host is an alternative server and can be identified by using a fully qualified domain name (FQDN) or an IP address.

Example: myhost.contoso.com or 192.168.3.2



aspmx.l.google.com



alt1.aspmx.l.google.com



alt2.aspmx.l.google.com



us-smtp-inbound-1.mimecast.com



us-smtp-inbound-2.mimecast.com



Next

5. Select the security restrictions settings as below:

### Security restrictions

How should Office 365 connect to your email server?

☒ Always use Transport Layer Security (TLS) to secure the connection (recommended)

Connect only if the recipient's email server certificate matches this criteria

☒ Any digital certificate, including self-signed certificates

☐ Issued by a trusted certificate authority (CA)

☐ Add the subject name or subject alternative name (SAN) matches this domain name:

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

Next

6. Add an email address of remote mail server to validate and test the connection.  
(Please note that validation needs to be done which is not identical)

### Validation email

Specify an email address for an active mailbox that's on your email server. You can add multiple addresses if your organization has more than one domain.

Example: user@contoso.com

+

meet.shah@aacn.org

Validate

Save

7. Validation results should be successful:

←

×

### Validation email

Specify an email address for an active mailbox that's on your email server. You can add multiple addresses if your organization has more than one domain.

Example: user@contoso.com

+

meet.shah@aacn.org

🗑️

Validate

✓ Validation successful

>	Task	Status
>	Check connectivity to 'aspmx.l.google.com'	Succeed
>	Check connectivity to 'alt1.aspmx.l.google.com'	Succeed
>	Check connectivity to 'alt2.aspmx.l.google.com'	Succeed
>	Check connectivity to 'us-smtp-inbound-1.mimecast.com'	Succeed
>	Check connectivity to 'us-smtp-inbound-2.mimecast.com'	Succeed
>	Send test email	Succeed

Save



8. Need to create transport rule to redirect mails to connector:  
Check below settings highlighted:

Exchange admin-> Mail flow -> Rules -> create a rule:

←

✕

### O365toGoogleWorkspaceRule\_Connector

Conditions Settings

Name \*

O365toGoogleWorkspaceRule\_Connector

Apply this rule if \*

The recipient

domain is

+

A recipient's domain is 'aacn.org'

Do the following \*

Redirect the message to

the following connector

+

route the message using the following connector 'Office 365 to Google'

Except if

Select one



Select one

+

Save

Cancel

## O365toGoogleWorkspaceRule\_Connector

 Edit rule conditions
  Edit rule settings

### Rule settings

Rule name	Mode
O365toGoogleWorkspaceRule_Connecto	Enforce
Severity	Set date range
High	Specific date range is not set
Senders address	Priority
Matching Header	0
For rule processing errors	
Ignore	

### Rule description

#### Apply this rule if

*recipients's address domain portion belongs to any of these domains: 'aacn.org'*

#### Do the following

*Route the message using the connector named 'Office 365 to Google'.  
and Set audit severity level to 'High'  
and Stop processina more rules*

9. Once the rule is created, test/verify by sending emails and sharing files:

Verification:

✕

Test Mail:09-jan-2024

Copy report text

Prepare and email extended report

View message in Explorer

Go Hunt for this message

Sender

vpatel@aacn.org

Recipient

robert.good@aacn.org

Received

Processed

Sent

Status

Office 365 used one of your organization's connectors to send the message to an external address. An admin in your organization set up a mail flow rule to route messages through that connector. Here are the details:

Connector name: TEST

External address: robert.good@aacn.org

Destination IP: 209.85.202.27

Destination smart host: alt1.aspmx.l.google.com

Mail flow rule: O365toGoogleWorkspaceRule\_Connector

More Information

You can view your organization's connector settings on the [connectors](#) page, and the mail flow rule settings on the [rules page](#).

Message events

⌵

Report Message

Vatsal Patel shared "TEST-vpatel-09012024 word" w...

Copy report text Prepare and email extended report

View message in Explorer Go Hunt for this message

**Sender**  
vpatel@aacn.org

**Recipient**  
robert.good@aacn.org

Received	Processed	Sent

**Status**

Office 365 used one of your organization's connectors to send the message to an external address. An admin in your organization set up a mail flow rule to route messages through that connector. Here are the details:

**Connector name:** TEST

**External address:** robert.good@aacn.org

**Destination IP:** 209.85.202.26

**Destination smart host:** alt1.aspmx.l.google.com

**Mail flow rule:** O365toGoogleWorkspaceRule\_Connector

**More Information**

You can view your organization's connector settings on the [connectors](#) page, and the mail flow rule settings on the [rules page](#).

### Vatsal Patel shared "TEST-VPATEL\_09012024 excel" ...

[Copy report text](#)
[Prepare and email extended report](#)

[View message in Explorer](#)
[Go Hunt for this message](#)

**Sender**  
 vpatel@aacn.org

**Recipient**  
 robert.good@aacn.org

Received      Processed      Sent

#### Status

Office 365 used one of your organization's connectors to send the message to an external address. An admin in your organization set up a mail flow rule to route messages through that connector. Here are the details:

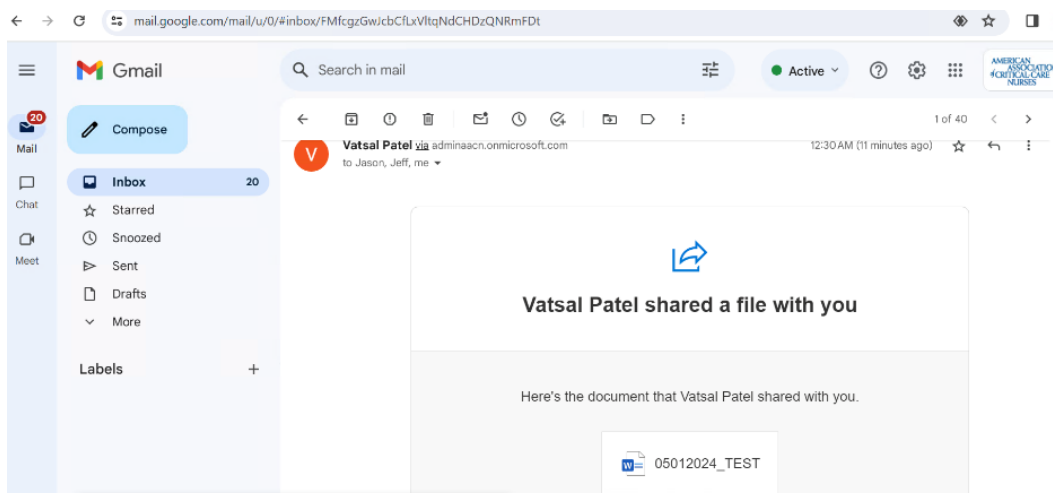
**Connector name:** TEST  
**External address:** robert.good@aacn.org  
**Destination IP:** 64.233.171.27  
**Destination smart host:** alt2.aspmx.l.google.com  
**Mail flow rule:** O365toGoogleWorkspaceRule\_Connector

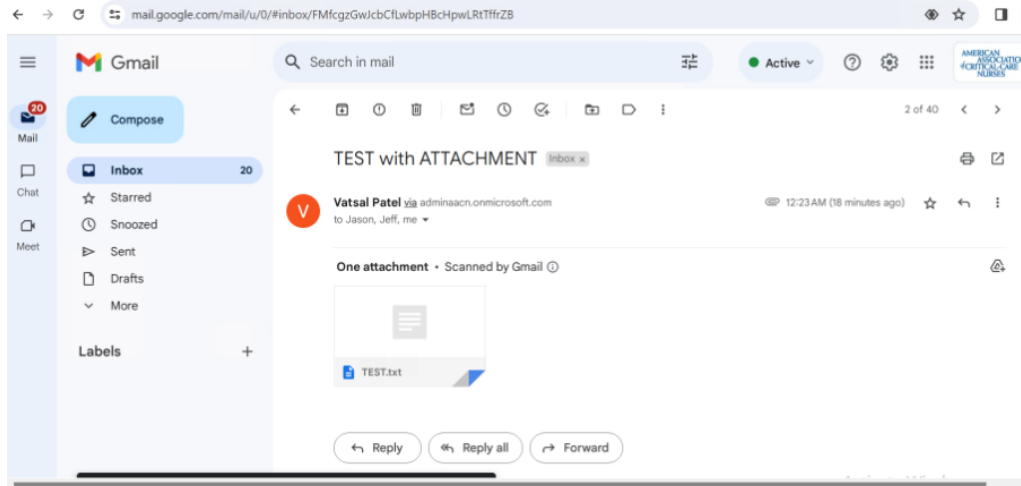
#### More Information

You can view your organization's connector settings on the [connectors](#) page, and the mail flow rule settings on the [rules page](#).

#### Message events

Recent Messages		
<input type="checkbox"/>	Vatsal Patel	Vatsal Patel shared "Test_shivam_visio_01042024" with you
<input type="checkbox"/>	Vatsal Patel	Vatsal Patel shared "TEST_Shivam_Doc_04012024" with you
<input type="checkbox"/>	Vatsal Patel	Vatsal Patel shared "Shivam-Test_04012024" with you
<input type="checkbox"/>	Vatsal Patel	TEST MAIL 2 - SHIVAM SHAH
<input type="checkbox"/>	Vatsal Patel	TEST FROM SHIVAM



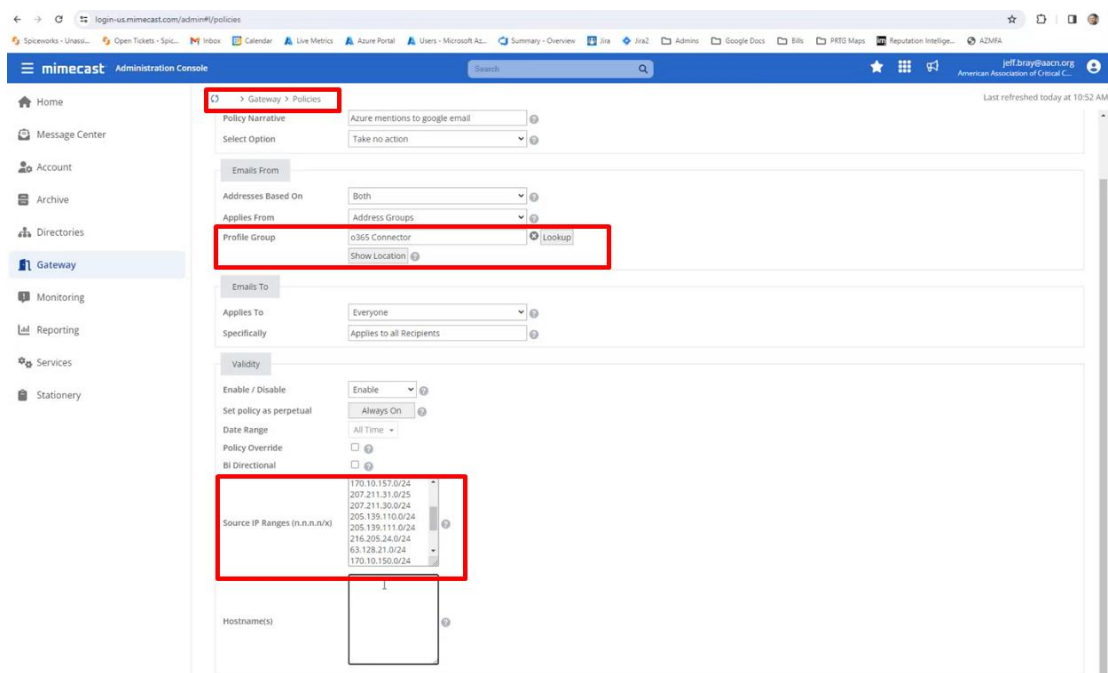
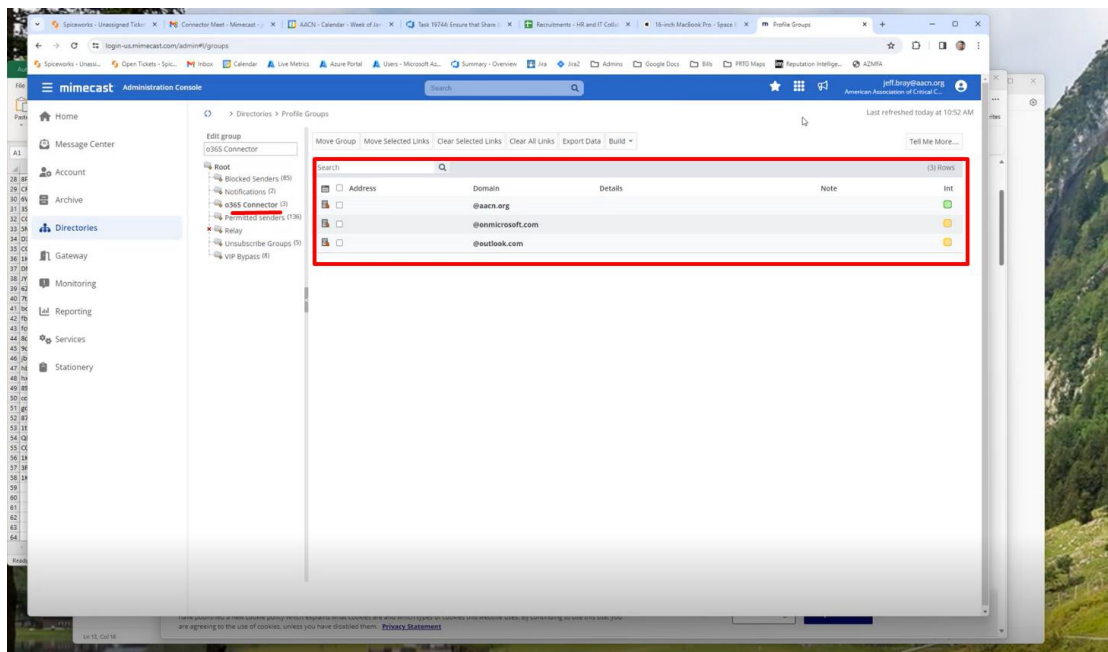


Below is the reference of Microsoft to white-list there exchange online IP addresses and domain in anti-spam and anti-spoofing at google workspace and Mimecast:

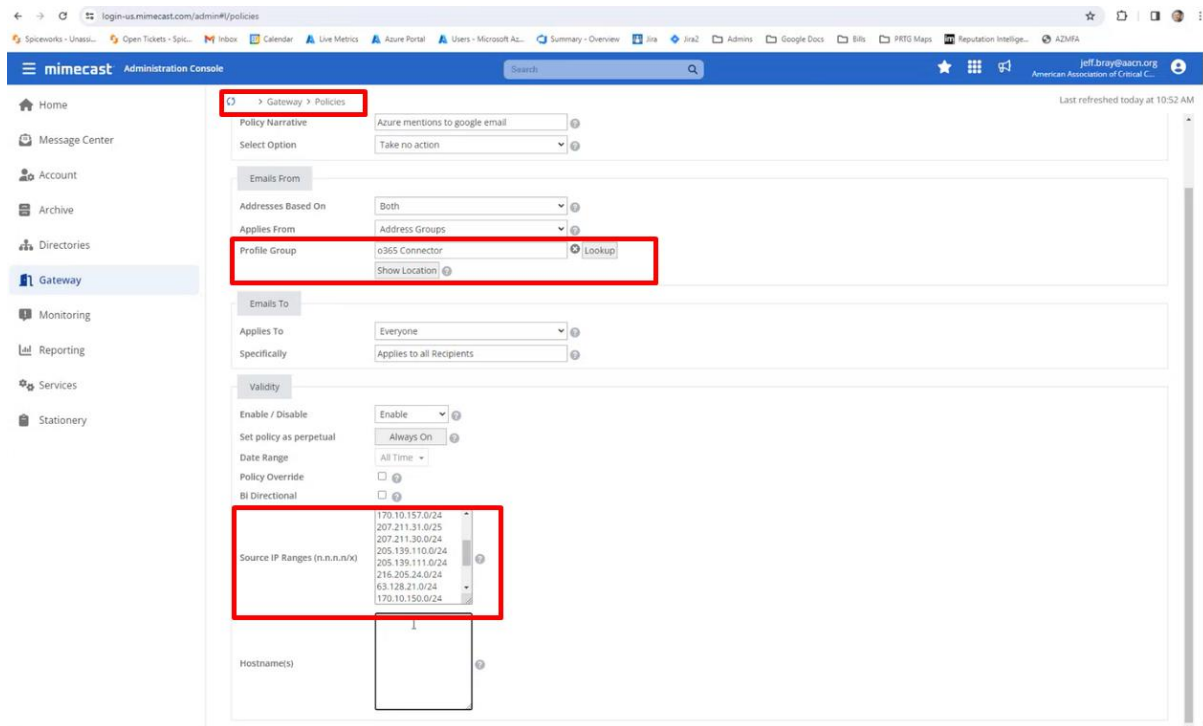
<https://learn.microsoft.com/en-us/microsoft-365/enterprise/urls-and-ip-address-ranges?view=o365-worldwide>

(Above reference is managed by Microsoft and there can be modifications in future)

Mimecast:

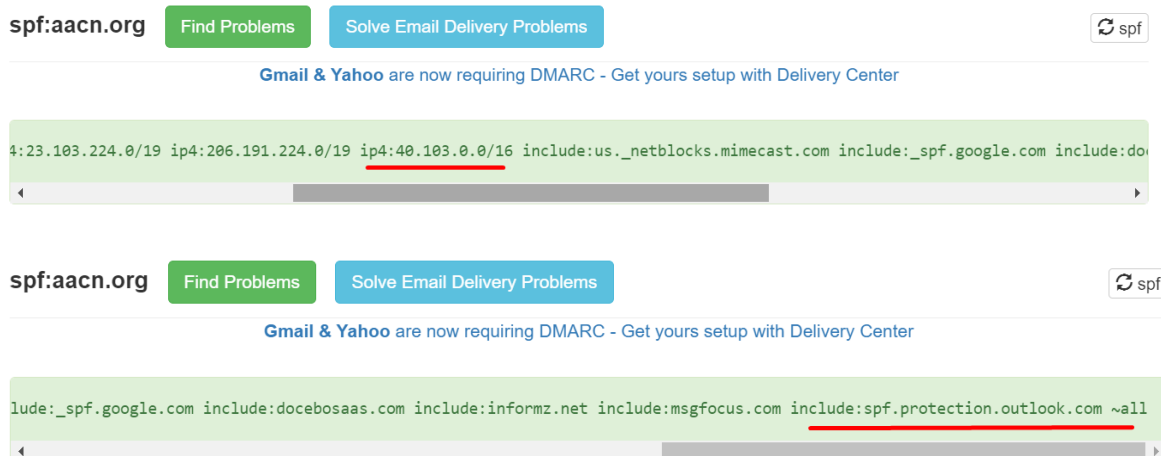


## Google Workspace:



The screenshot shows the Mimecast Administration Console interface. The left sidebar contains navigation links: Home, Message Center, Account, Archive, Directories, Gateway (selected), Monitoring, Reporting, Services, and Stationery. The main content area is titled 'Gateway > Policies'. A red box highlights the 'Gateway > Policies' breadcrumb. Below it, the 'Policy Narrative' is 'Azure mentions to google email'. The 'Select Option' is 'Take no action'. The 'Emails From' section has 'Addresses Based On' set to 'Both' and 'Applies From' set to 'Address Groups'. A red box highlights the 'Profile Group' dropdown, which is set to 'o365 Connector', with a 'Show Location' link and a 'Lookup' button. The 'Emails To' section has 'Applies To' set to 'Everyone' and 'Specifically' set to 'Applies to all Recipients'. The 'Validity' section has 'Enable / Disable' set to 'Enable', 'Set policy as perpetual' set to 'Always On', 'Date Range' set to 'All Time', and 'Policy Override' and 'BI Directional' checkboxes are unchecked. A red box highlights the 'Source IP Ranges (n.n.n.n/x)' list, which contains several IP ranges including 170.10.157.0/24, 207.211.31.0/25, 207.211.30.0/24, 205.139.110.0/24, 205.139.111.0/24, 216.205.24.0/24, 63.128.21.0/24, and 170.10.156.0/24. The 'Hostnames(s)' field is empty.

## SPF records changes:



The first screenshot shows the SPF record configuration for 'spf:aacn.org'. It includes buttons for 'Find Problems' and 'Solve Email Delivery Problems', and a 'spf' icon. Below the buttons, a message states: 'Gmail & Yahoo are now requiring DMARC - Get yours setup with Delivery Center'. The SPF record text is: '4:23.103.224.0/19 ip4:206.191.224.0/19 ip4:40.103.0.0/16 include:us.\_netblocks.mimecast.com include:\_spf.google.com include:do'. The second screenshot shows the same configuration for 'spf:aacn.org'. The SPF record text is: 'lude:\_spf.google.com include:docebosaas.com include:informz.net include:msgfocus.com include:\_spf.protection.outlook.com ~all'. Both screenshots have a red underline under the IP range 'ip4:40.103.0.0/16' in the first and 'include:\_spf.protection.outlook.com' in the second.