Microsoft Domain and IP Whitelist Instructions

Domain Whitelist Instructions:

- 1. Login to https://portal.microsoftonline.com
- 2. Click on the Admin icon
- 3. Click the "Admin centers" drop down in the side navigation and then click on "Exchange"
- 4. Once the new window has loaded, click the "mail flow" button in the side navigation bar
- 5. Click the plus sign and select "Bypass spam filtering" from the drop down

Exchange admin center

dashboard	rules	message trace	accepted domains	remote domains	connectors
recipients					
permissions	+-	'≞ _ ↑ ↓ [- ~ <i>C</i>		

- 6. In the name field add "Whitelist Spectruminc.com"
- 7. Click the drop down in the "*Apply this rule if..." field and hover over "The Sender..." and select "domain is" from the drop down that appears
 - In the "specify domain" window that appears add the following without quotes: "spectruminc.com"

×

Click the plus button to add the domain to the list and click "OK"

specify domain		
/ -		
spectruminc.com		+
spectruminc.com		
	OK	Cancel

8. Make sure the "Stop processing more rules" checkbox is checked

9. The window should look like the following:

new rule

Name:		
Whitelist Spectruminc.com		
Apply this rule if		
The sender's domain is	-	'spectruminc.com'
add condition		
Do the following		
Set the spam confidence level (SCL) to	·	Bypass spam filtering You don't need to create a transport rul to bypass spam filtering or mark email a spam for a sender or domain. Click here to use an allow or block list in the spam filter.
add action		
Except if		
add exception		
Properties of this rule:		
Audit this rule with severity level:		
Not specified		
Choose a mode for this rule:		
Enforce		
Test with Policy Tips		
Test without Policy Tips		
Activate this rule on the following date:		
Tue 7/16/2019 v 3:30 PM v		
Deactivate this rule on the following date:		
Tue 7/16/2019 👻 3:30 PM 🔻		
✓ Stop processing more rules		
Defer the message if rule processing doesn't complete		
Match sender address in message:		
Header 👻		
Comments:		

10. You can now click "save" on the current window

11. The new rule should automatically be turned on in the rules list

IP Address Whitelist Instructions:

Part 1: Adding IP to Allow list

- 1. Login to https://portal.microsoftonline.com
- 2. Click on the Admin icon
- 3. Click the "Admin centers" drop down in the side navigation and then click on "Exchange"
- 4. Once the new window has loaded, click the "connection filter" button under the "protection" section
- 5. Click the pencil icon to edit the connection filter policy

Exchange admin c	renter
dashboard	malware filter connection filter spam filter outbound spam quarantine action center dkim
recipients	
permissions	
compliance management	NAME
organization	Default
protection	
mail flow	
mobile	
public folders	
unified messaging	
hybrid	

6. In the window that appears, select the "connection filtering" button in the side navigation and then select the plus sign icon under the "IP Allow list" section"

Default

general • connection filtering	connection filtering IP Allow list Always accept messages from the following IP addresses.
	2321.109212 Select connection filtering then click the + icon to add an IP address to the Allowed List
	Blocked IP Address

- 7. In the window that appears add the following without quotations and click "OK": "**142.0.186.64**"
- 8. Save the changes made

Part 2: Whitelisting Spectruminc.com IP address

- 1. Login to https://portal.microsoftonline.com
- 2. Click on the Admin icon
- 3. Click the "Admin centers" drop down in the side navigation and then click on "Exchange"
- 4. Once the new window has loaded, click the "mail flow" button in the side navigation bar
- 5. Click the plus sign and select "Bypass spam filtering" from the drop down

Exchange admin center

dashboard	rules message trace	accepted domains	remote domains	connectors
recipients				
permissions	+- 🖍 🖻 🗰 🛧 🗸	<u>□</u> - 2 S		

- 6. In the name field add "Whitelist Spectruminc.com IP"
- 7. Click the drop down in the "*Apply this rule if..." field and hover over "The Sender..." and select "IP address is in any of these ranges or exactly matches"

Name:	
Bypass Clutter & Spam Filtering by IP Address	
Apply this rule if	
Sender's IP address is in the range	•
Select one	
The sender	is this person
The recipient	is external/internal
The subject or body	is a member of this group
Any attachment	 address includes any of these words
Any recipient	address matches any of these text patterns
The message	is on a recipient's supervision list
The sender and the recipient	has specific properties including any of these words specific
The message properties	has specific properties matching these text patterns
A message header	 has overridden the Policy Tip
[Apply to all messages]	IP address is in any of these ranges or exactly matches
add action	domain is

Except	if
	add exception

	au	IG.	ex.	Ç,	:pu	OU.
-	_	_			_	

Save Cance	1
------------	---

8. In the "specify IP address ranges" window add the following without quotes: "142.0.186.64"

×

specify IP addres	ss ranges	
<u>/</u> -		
142.0.186.64		+
142.0.186.64		
	OK	Cancel

- 9. Click the "OK" button
- 10. Set the "*Do the following..." field to "set a message header"

Sender's IP address is in the range	•
add condition	
Do the following	
Set the message header to this value	 Set the message header <u>'X-MS-Exchange-Organization-</u>
Select one	BypassClutter' to the value 'true'
Forward the message for approval	* Denne man Obering
Redirect the message to	 Bypass spam filtering You don't need to create a transport rule to bypass span
Block the message	 filtering or mark email as spam for a sender or domain.
Add recipients	Click here to use an allow or block list in the spam
Apply a disclaimer to the message	 filter.
Modify the message properties	remove a message header
Modify the message security	set a message header
Prepend the subject of the message with	apply a message classification
Generate incident report and send it to	set the spam confidence level (SCL)
Notify the recipient with a message	

11. Set the message header to the following without quotes: "X-MS-Exchange-Organization-BypassClutter"

	*Apply this rule if									
	Sender's IP address is in the range									
	add condition									
	"Do the following	message header			×					
×	Set the message header to						e-Organization-			
	and	X-MS-Exchange-Organiz	ation-BypassClutter			rue'				
×	Set the spam confidence le		OK	Cancel	_	m for a set	e to bypass spam nder or domain.			
			filter.							
	add action									
	Except if									
	add exception									
					Save	e	Cancel			

- 12. Set the value to "true"
- 13. Add an additional action beneath "*Do the following..." to "Modify the message properties"
- 14. Click on "Set the spam confidence level (SCL) to..." and select "Bypass Spam Filtering"

Sender's IP address is in the range	×			
	×			
add condition	552			
*Do the following specify SCL				
Set the message header to this valu	ader 'X-MS-Exchange-Organizati	on-		
Bypass spam filtering and Bypass spam filtering	value <u>'true'</u>			
Set the spam confidence level (SCL)	g reate a transport rule to bypass ail as spam for a sender or doma	g reate a transport rule to bypass spam ail as spam for a sender or domain. allow or block list in the spam		
add action 6				
Except if 8				
add exception				
	Save Cancel			

15. Click save