

Blocking or Allowing Emails in Exchange Online Protection

Last Modified on 23/01/2020 2:29 pm GMT

With the Exchange Online service, you have access to the Exchange Online Protection service for anti-spam and anti-malware functions.

At times, you may find a legitimate email has been marked as Junk (a false positive) and want to allow this through for future emails. Alternatively, you may have received an email that should be blocked or handled as spam (a false negative).

The Exchange Online Protection service allows you to block emails based on the address they come from and the IP address of the sending server.

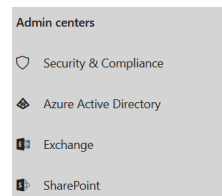
It is not recommended to configure Allow policies for free-mail domains such as outlook.com or yahoo.com.

Block or Allow by Email Address

1. Log into the Microsoft 365 Admin Center using global admin credentials for the tenant:

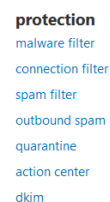
<https://admin.microsoft.com>

2. Under **Admin Centers**, select **Exchange**



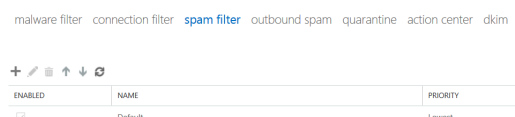
Note: If you don't see the Admin Centers section, press **Show More**

3. Go to 'Protection > Spam Filter'

A screenshot of the Microsoft 365 Admin Center interface. The 'protection' section is expanded, showing a list of options: malware filter, connection filter, spam filter, outbound spam, quarantine, action center, and dkim. The 'spam filter' option is highlighted with a blue selection bar.

malware filter
connection filter
spam filter
outbound spam
quarantine
action center
dkim

4. Double click on the Default spam configuration

A screenshot of the Microsoft 365 Admin Center interface showing the 'spam filter' configuration table. The table has columns for 'ENABLED', 'NAME', and 'PRIORITY'. There is one row with a checked checkbox in the 'ENABLED' column, the name 'Default' in the 'NAME' column, and 'Lowest' in the 'PRIORITY' column. Above the table, there are navigation icons and a breadcrumb trail: 'malware filter > connection filter > spam filter > outbound spam > quarantine > action center > dkim'.

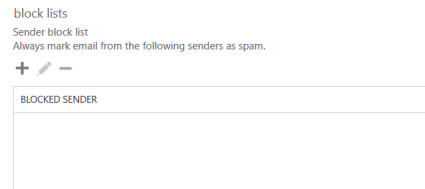
ENABLED	NAME	PRIORITY
<input checked="" type="checkbox"/>	Default	Lowest

5. Select either **Allow lists** or **Block lists**

Default

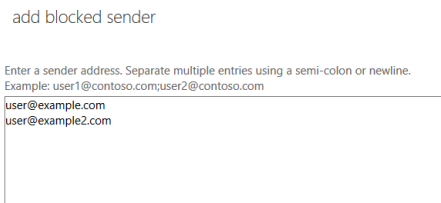
- general
- spam and bulk actions
- ▶ **block lists**
- allow lists
- international spam
- advanced options

6. Under **Sender block/allow list**, select the + icon



7. Enter the address to block with one-per line

Note: You can also add multiple entries per line separated by a semicolon.

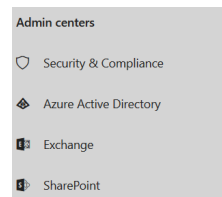


8. Select **OK**

9. Select **Save**

Block or Allow by Domain

1. Log into the Microsoft 365 Admin Center using global admin credentials for the tenant:
<https://admin.microsoft.com>
2. Under **Admin Centers**, select **Exchange**

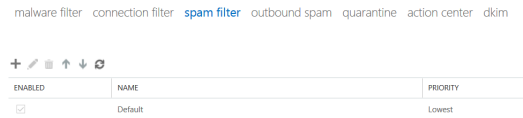


Note: If you don't see the Admin Centers section, press **Show More**

3. Go to 'Protection > Spam Filter'

- protection
- malware filter
- connection filter
- spam filter
- outbound spam
- quarantine
- action center
- dkim

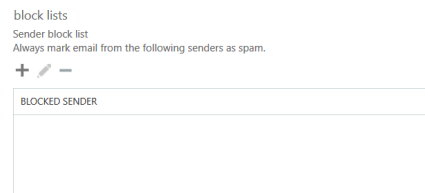
4. Double click on the Default spam configuration



5. Select either **Allow lists** or **Block lists**

- Default
- general
- spam and bulk actions
- ▶ **block lists**
- allow lists
- international spam
- advanced options

6. Under **Domain block/allow list**, select the + icon



7. Enter the domain to block with one-per line



Note: You can also add multiple entries per line separated by a semicolon.

8. Select **OK**

9. Select **Save**

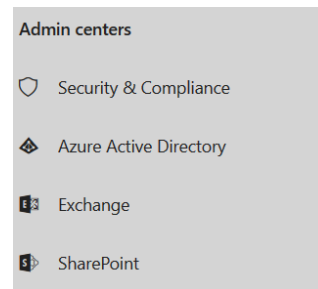
Block or Allow by IP Address

1. Log into the Microsoft 365 Admin Center using global admin credentials for the tenant:

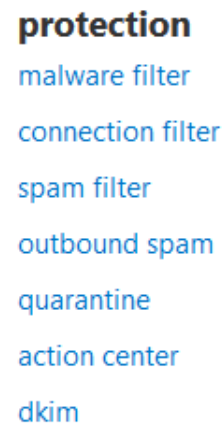
<https://admin.microsoft.com>

2. Under **Admin Centers**, select **Exchange**

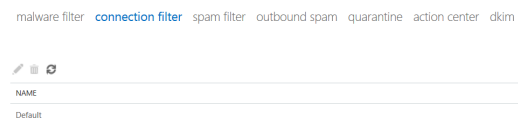
Note: If you don't see the Admin Centers section, press **Show More**



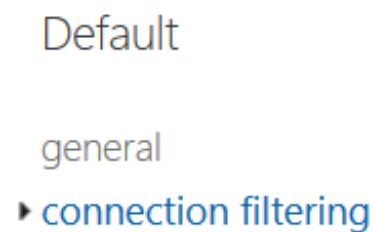
3. Go to 'Protection > Connection Filter'



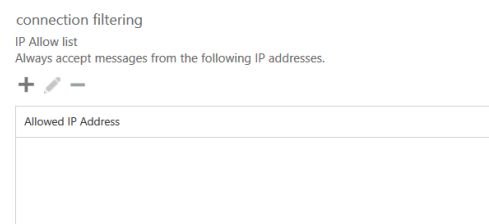
4. Double click on the Default Connection Filter



5. Select **Connection Filtering**



6. Under **IP block/allow list**, select the + icon



7. Enter the IP address you want to block

Note: You can block ranges of IPs by entering them in CIDR format (Only /24 & /32 are supported)

8. Press **OK**

9. Press **Save**

add allowed IP address

Address or address range:
Example: 192.168.180.0/26

255.255.255.0/24