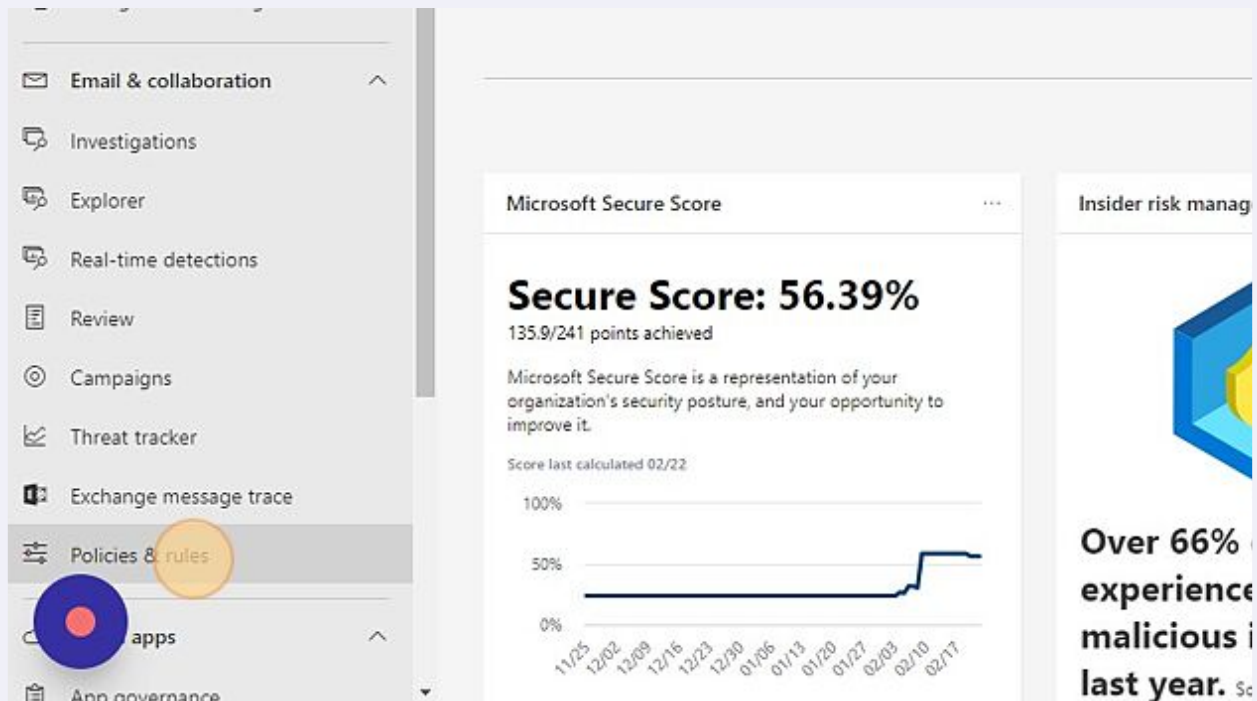


How to Configure an Anti-Spam Policy in Microsoft 365

1 Navigate to security.microsoft.com

2 Click "Policies & rules"



3 Click "Threat policies"

Policies & rules

Set up policies to manage devices, protect against threats, and receive alerts about vari

Name
<u>Threat policies</u>
Alert policy
Manage advanced alerts
Activity alerts

4 Click "Anti-spam"

Policies

Preset Security Policies

Configuration analyzer

- Anti-phishing
- Anti-spam
- Anti-malware
- Safe Attachments
- Safe Links

Rules

5 Click "Create policy"

Policies & rules > Threat policies > Anti-spam policies

Anti-spam policies

We recommend enabling preset security policies to stay updated with new security controls. Use this page to configure policies that are included in anti-spam protection. These policies are included in the anti-spam protection.

+ Create policy Refresh

Name
<input type="checkbox"/> Anti-spam inbound policy (Default)
<input type="checkbox"/> Connection filter policy (Default)
<input type="checkbox"/> Anti-spam outbound policy (Default)

6 Click "Inbound"

Policies & rules > Threat policies > Anti-spam policies

Anti-spam policies

We recommend enabling preset security policies to stay updated with new security controls. Use this page to configure policies that are included in anti-spam protection. These policies are included in the anti-spam protection.

+ Create policy Refresh

Inbound Outbound

<input type="checkbox"/> Anti-spam inbound policy (Default)
<input type="checkbox"/> Connection filter policy (Default)
<input type="checkbox"/> Anti-spam outbound policy (Default)

7 Click the "Name" field.

threat policies > Create anti-spam inbound policy

by

d domains

old & spam properties

Name your policy

Add a name and description for your custom anti-spam policy.

Name *

Description

8 Enter "Default-Inbound-Spam-Policy" and click "Next"

Add a name and description for your custom anti-spam policy.

Name *

Description

9 Target your domain and click "Next"

Domains

imperionllc.com

☐ Exclude these users, groups and domains

Back Next

10 Set the bulk email threshold to "7"

i-spam inbound policy

Bulk email threshold & spam properties

Set your anti-spam bulk email threshold and properties for this policy.

Bulk email threshold ⓘ

7 (Default)

A higher bulk email threshold means more bulk email will be delivered

Spam properties

✓ Increase spam score

Specify whether to increase the spam score for messages that include these types of links or U

Image links to remote websites

Off

11 Turn "Image links to remote websites" to ON

A higher bulk email threshold means more bulk email will be delivered

Spam properties

✓ Increase spam score

Specify whether to increase the spam score for messages that include these types of links

Image links to remote websites

Off

Off

On

Test

URL redirect to other port

Off

Links to .biz or .info websites

Off

✓ Mark as spam

Specify whether to mark messages that include these properties as spam.

Empty messages

12 Turn "Numeric IP address in URL" to ON

Specify whether to increase the spam score for messages that include these types of

Image links to remote websites

On

Numeric IP address in URL

Off

Off

On

Test

Links to .biz or .info websites

Off

✓ Mark as spam

Specify whether to mark messages that include these properties as spam.

Empty messages

13 Turn "Image links to remote websites" to ON

Image links to remote websites

On

Numeric IP address in URL

On

URL redirect to other port

Off

Off

On

Test

Mark as spam

Specify whether to mark messages that include these properties as spam.

Empty messages

Back Next

14 Turn "Links to .biz or .info websites" to ON

On

URL redirect to other port

On

Links to .biz or .info websites

Off

Off

On

Test

Empty messages

Off

Embedded tags in HTML

Off

Back Next

15 Turn "Empty messages" to ON

properties

On

▼

▼ Mark as spam

Specify whether to mark messages that include these properties as spam.

Empty messages

Off

▼

Off

On

Test

javascript or vbscript in html

Off

▼

Form tags in HTML

Off

▼

Frame or iframe tags in HTML

Off

▼

16 Turn "Embedded tags in HTML" to ON

Specify whether to mark messages that include these properties as spam.

Empty messages

On

▼

Embedded tags in HTML

Off

▼

Off

On

Test

form tags in HTML

Off

▼

Frame or iframe tags in HTML

Off

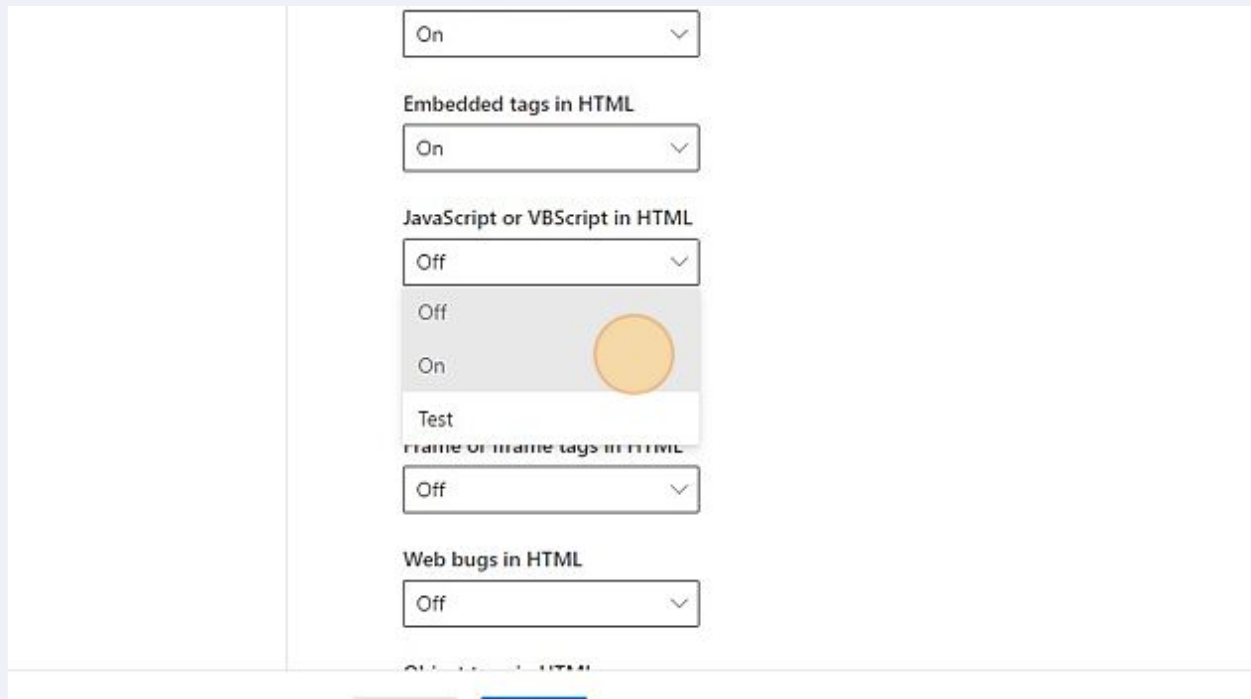
▼

Web bugs in HTML

Off

▼

17 Turn "JavaScript or VBScript in HTML" to ON



On

Embedded tags in HTML

On

JavaScript or VBScript in HTML

Off

Off

On

Test

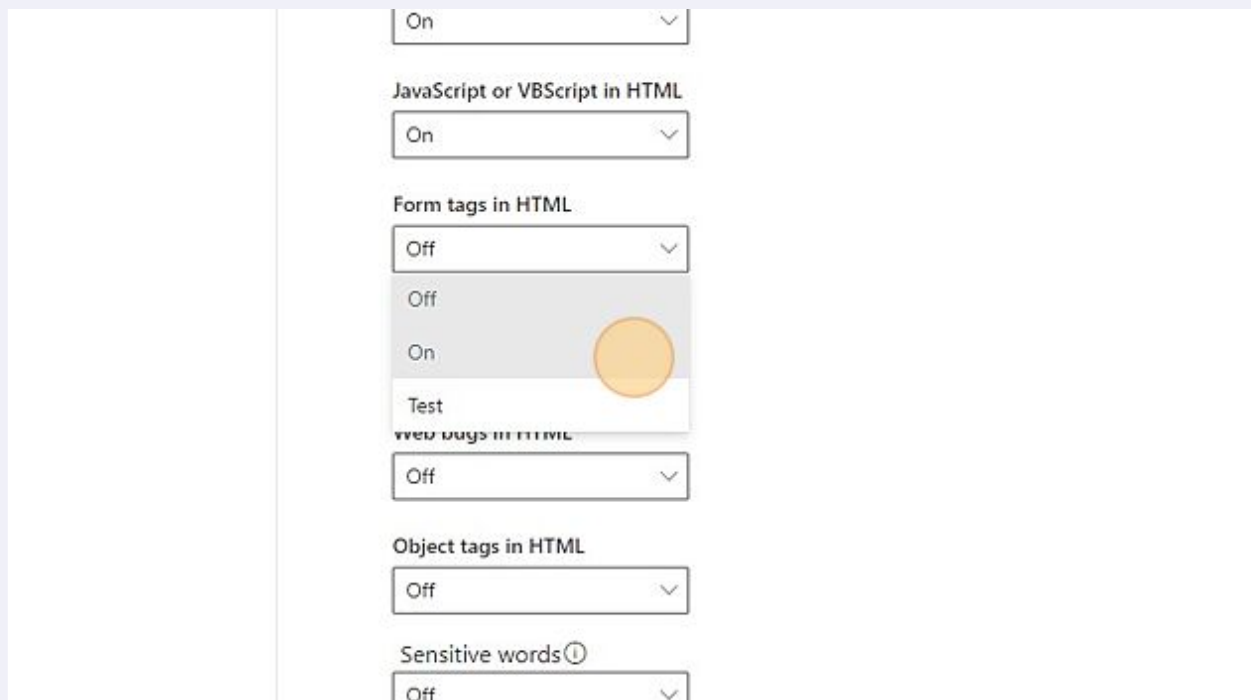
Frame or frame tags in HTML

Off

Web bugs in HTML

Off

18 Turn "Form tags in HTML" to ON



On

JavaScript or VBScript in HTML

On

Form tags in HTML

Off

Off

On

Test

Web bugs in HTML

Off

Object tags in HTML

Off

Sensitive words ⓘ

Off

19 Turn "Frame or iFrame tags in HTML" to ON

On

Form tags in HTML

On

Frame or iFrame tags in HTML

Off

Off

On

Test

Object tags in HTML

Off

Sensitive words ⓘ

Off

SPF record: hard fail ⓘ

Off

20 Turn "Web bugs in HTML" to ON

On

Frame or iFrame tags in HTML

On

Web bugs in HTML

Off

Off

On

Test

Sensitive words ⓘ

Off

SPF record: hard fail ⓘ

Off

Sender ID filtering hard fail ⓘ

21 Turn "Object tags in HTML" to ON

Frame or iframe tags in HTML

On

Web bugs in HTML

On

Object tags in HTML

Off

Off

On

Test

Off

Sender ID filtering hard fail ⓘ

Back Next

22 Turn "SPF record: hard fail" to ON

Object tags in HTML

On

Sensitive words ⓘ

Off

SPF record: hard fail ⓘ

Off

On

Off

Backscatter ⓘ

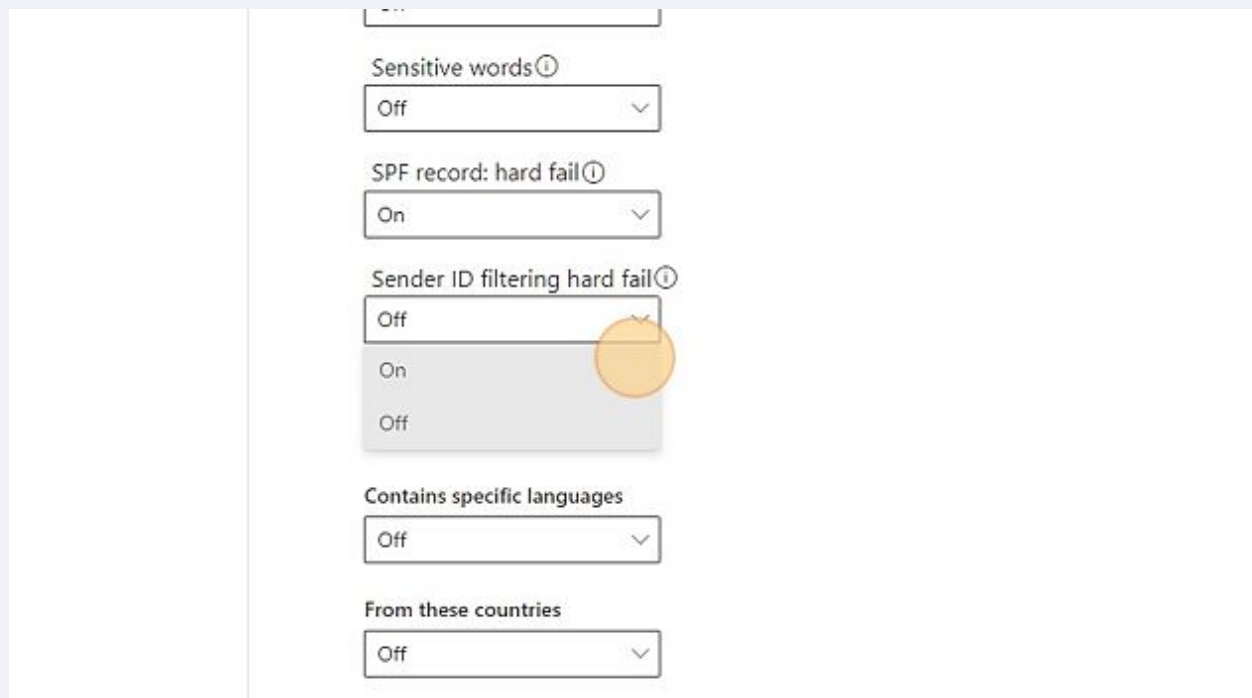
Off

Contains specific languages

Off

From these countries

23 Turn "Sender ID filtering hard fail" to ON



The screenshot shows a configuration page with several dropdown menus. The 'Sender ID filtering hard fail' dropdown is open, showing 'Off' as the selected option and 'On' as an available option. An orange circle highlights the 'On' option. Other visible options include 'Sensitive words' (Off), 'SPF record: hard fail' (On), 'Contains specific languages' (Off), and 'From these countries' (Off).

Sensitive words ⓘ
Off

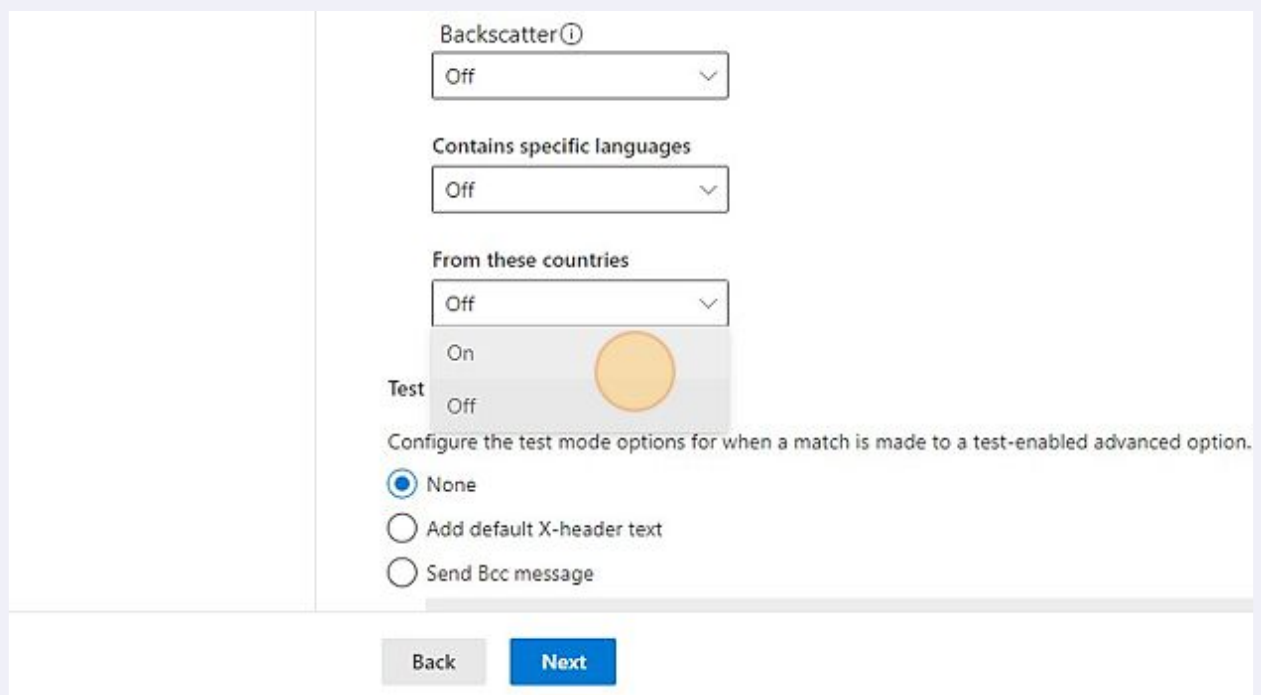
SPF record: hard fail ⓘ
On

Sender ID filtering hard fail ⓘ
Off
On
Off

Contains specific languages
Off

From these countries
Off

24 Turn "From these countries" to ON



The screenshot shows a configuration page with several dropdown menus. The 'From these countries' dropdown is open, showing 'Off' as the selected option and 'On' as an available option. An orange circle highlights the 'On' option. Other visible options include 'Backscatter' (Off), 'Contains specific languages' (Off), and 'Test' (Off). Below the dropdowns, there are radio button options for 'Test mode': 'None' (selected), 'Add default X-header text', and 'Send Bcc message'. At the bottom, there are 'Back' and 'Next' buttons.

Backscatter ⓘ
Off

Contains specific languages
Off

From these countries
Off
On
Off

Test
Off

Configure the test mode options for when a match is made to a test-enabled advanced option.

☒ None
☐ Add default X-header text
☐ Send Bcc message

Back Next

25

Set these countries and click "Next":

- Russia
- China
- Iran
- Turkey
- Bangladesh
- Brazil
- Estonia
- Iraq
- Latvia
- Lebanon
- North Korea
- Romania
- Syria
- Ukraine
- Vietnam

Russia × China × Iran × Turkey ×

Bangladesh × Brazil × Estonia × Iraq ×

Latvia × Lebanon × North Korea × Romania ×

Syria × Ukraine × Vietnam ×

Test mode

Configure the test mode options for when a match is made to a test-enabled advanced

☒ None

☐ Add default X-header text

☐ Send Bcc message

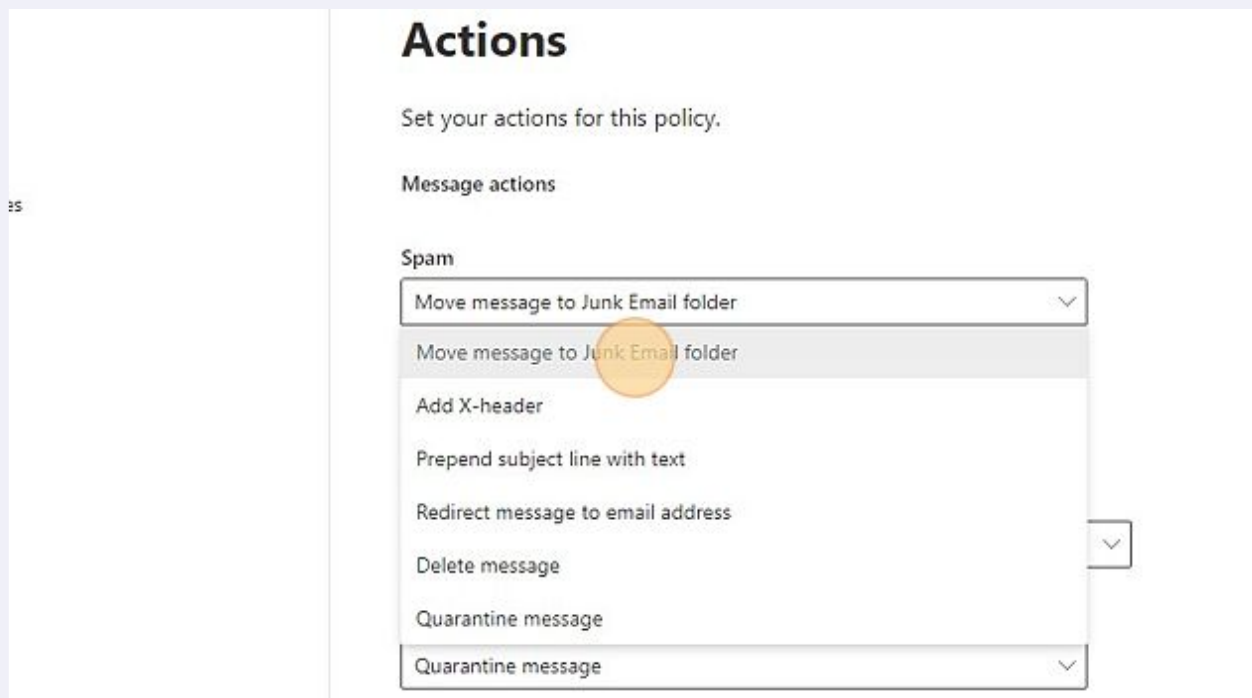
Back Next



Alert!

If you have a business need to allow one of these countries, do not include them in this list.

26 Set "Spam" to "Move message to Junk Email folder"



Actions

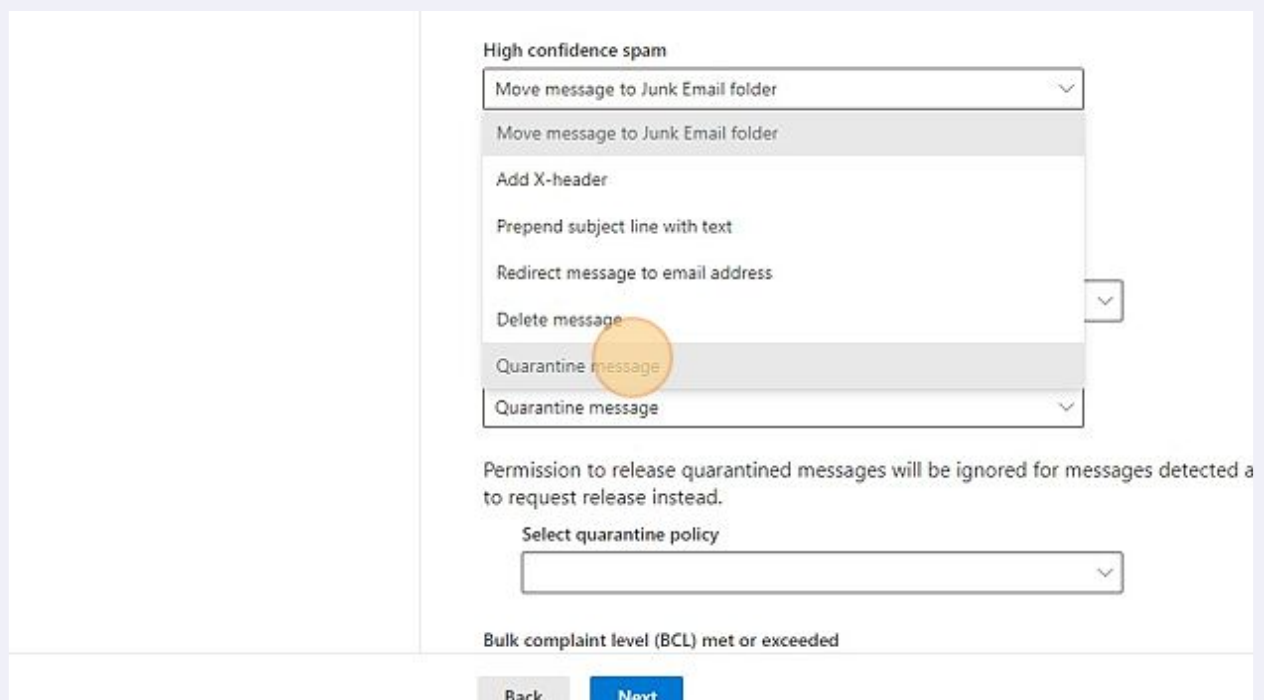
Set your actions for this policy.

Message actions

Spam

- Move message to Junk Email folder
- Move message to Junk Email folder
- Add X-header
- Prepend subject line with text
- Redirect message to email address
- Delete message
- Quarantine message
- Quarantine message

27 Set "High Confidence Spam" to "Quarantine message"



High confidence spam

- Move message to Junk Email folder
- Move message to Junk Email folder
- Add X-header
- Prepend subject line with text
- Redirect message to email address
- Delete message
- Quarantine message
- Quarantine message

Permission to release quarantined messages will be ignored for messages detected a to request release instead.

Select quarantine policy

Bulk complaint level (BCL) met or exceeded

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

28 Set "Default Quarantine Policy"

Spam

Move message to Junk Email folder

High confidence spam

Quarantine message

Select quarantine policy

Default Quarantine Policy

DefaultFullAccessPolicy

AdminOnlyAccessPolicy

DefaultFullAccessWithNotificationPolicy

Phishing

Quarantine message

High confidence phishing

Quarantine message

29 Set "Phishing" to "Quarantine message"

High confidence spam

Quarantine message

Select quarantine policy

Default Quarantine Policy

Phishing

Quarantine message

Select quarantine policy

High confidence phishing

Quarantine message

Permission to release quarantined messages will be ignored for message to request release instead

30 Set the "Default Quarantine Policy"

m properties

Select quarantine policy

Default Quarantine Policy

Phishing

Quarantine message

Select quarantine policy

Default Quarantine Policy

High confidence phishing

Quarantine message

DefaultFullAccessPolicy

AdminOnlyAccessPolicy

DefaultFullAccessWithNotificationPolicy

Select quarantine policy

Bulk complaint level (BCL) met or exceeded

31 Set "High confidence phishing" to "Quarantine message"

Phishing

Quarantine message

Select quarantine policy

Default Quarantine Policy

High confidence phishing

Quarantine message

Permission to release quarantined messages will be ignored for messages detected as high confidence phishing. Request release instead.

Select quarantine policy

Bulk complaint level (BCL) met or exceeded

Move message to Junk Email folder

32 Set the "Default Quarantine Policy"

High confidence phishing

Quarantine message

Permission to release quarantined messages will be ignored for messages to request release instead.

Select quarantine policy

Default Quarantine Policy

DefaultFullAccessPolicy

AdminOnlyAccessPolicy

DefaultFullAccessWithNotificationPolicy

Bulk

Mo

Retention

15

Back Next

33 Set "Bulk complaint level (BCL) met or exceeded" to "Quarantine message"

Bulk complaint level (BCL) met or exceeded

Move message to Junk Email folder

Move message to Junk Email folder

Add X-header

Prepend subject line with text

Redirect message to email address

Delete message

Quarantine message

No action

Redirect to this email address

Back Next

34 Set "Default Quarantine Policy"

Select quarantine policy

Default Quarantine Policy

Bulk complaint level (BCL) met or exceeded

Quarantine message

Select quarantine policy

Default Quarantine Policy

DefaultFullAccessPolicy

AdminOnlyAccessPolicy

DefaultFullAccessWithNotificationPolicy

Retain spam in quarantine for this many days

15

Prepend subject line with this text

35 Set "Retain spam in quarantine for this many days" to "30"

Bulk complaint level (BCL) met or exceeded

Quarantine message

Select quarantine policy

Default Quarantine Policy

Retain spam in quarantine for this many days

30

Add this X-header text

Prepend subject line with this text

Redirect to this email address

36 Enable "Spam safety tips"

	Prepend subject line with this text
	Redirect to this email address
	Safety tips
	<input checked="" type="checkbox"/> Enable spam safety tips ⓘ
	Zero-hour auto purge (ZAP)
	<input checked="" type="checkbox"/> Enable zero-hour auto purge (ZAP) ⓘ
	<input checked="" type="checkbox"/> Enable for phishing messages
	<input checked="" type="checkbox"/> Enable for spam messages
<div>BackNext</div>	

37 Enable "Zero-hour auto purge (ZAP)"

	Add this X-header text
	Prepend subject line with this text
	Redirect to this email address
	Safety tips
	<input checked="" type="checkbox"/> Enable spam safety tips ⓘ
	Zero-hour auto purge (ZAP)
	<input checked="" type="checkbox"/> Enable zero-hour auto purge (ZAP) ⓘ
<div>BackNext</div>	

38 Click "Enable for phishing messages"

	Prepend subject line with this text
	<input type="text"/>
	Redirect to this email address
	<input type="text"/>
	Safety tips
	<input checked="" type="checkbox"/> Enable spam safety tips ⓘ
	Zero-hour auto purge (ZAP)
	<input checked="" type="checkbox"/> Enable zero-hour auto purge (ZAP) ⓘ
	<input checked="" type="checkbox"/> Enable for phishing messages
	<input checked="" type="checkbox"/> Enable for spam messages
<div>BackNext</div>	

39 Click "Enable for spam messages"

	Prepend subject line with this text
	<input type="text"/>
	Redirect to this email address
	<input type="text"/>
	Safety tips
	<input checked="" type="checkbox"/> Enable spam safety tips ⓘ
	Zero-hour auto purge (ZAP)
	<input checked="" type="checkbox"/> Enable zero-hour auto purge (ZAP) ⓘ
	<input checked="" type="checkbox"/> Enable for phishing messages
	<input checked="" type="checkbox"/> Enable for spam messages
<div>BackNext</div>	

40 Click "Next"

Prepend subject line with this text

Redirect to this email address

Safety tips

☒ Enable spam safety tips ⓘ

Zero-hour auto purge (ZAP)

☒ Enable zero-hour auto purge (ZAP) ⓘ

☒ Enable for phishing messages

☒ Enable for spam messages

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

41 Add your whitelists and blacklists here.

Allow & block list

Choose which users, group and domains to allow or block in this policy. It also allows you to block messages that are marked as high confidence phishing.

Allowed

Senders (0)
Always deliver messages from these senders
[Manage 0 sender\(s\)](#)

Domains (0)
Always deliver messages from these domains
[Allow domains](#)

Blocked

Senders (0)
Always mark messages from these senders as spam
[Manage 0 sender\(s\)](#)

42 Click "Next"

	Allow domains Blocked Senders (0) Always mark messages from these senders as spam Manage 0 sender(s) Domains (0) Always mark messages from these domains as spam Block domains
<div>Back Next</div>	

43 Review the settings and click "Create"

	<p>Retain spam in quarantine for this many days 30</p> <p>Edit actions</p> <p>Allowed and blocked senders and domains</p> <p>Allowed senders -</p> <p>Allowed domains -</p> <p>Blocked senders -</p> <p>Blocked domains -</p> <p>Edit allowed and blocked senders and domains</p>
<div>Back Create</div>	

44

Click "Done"

