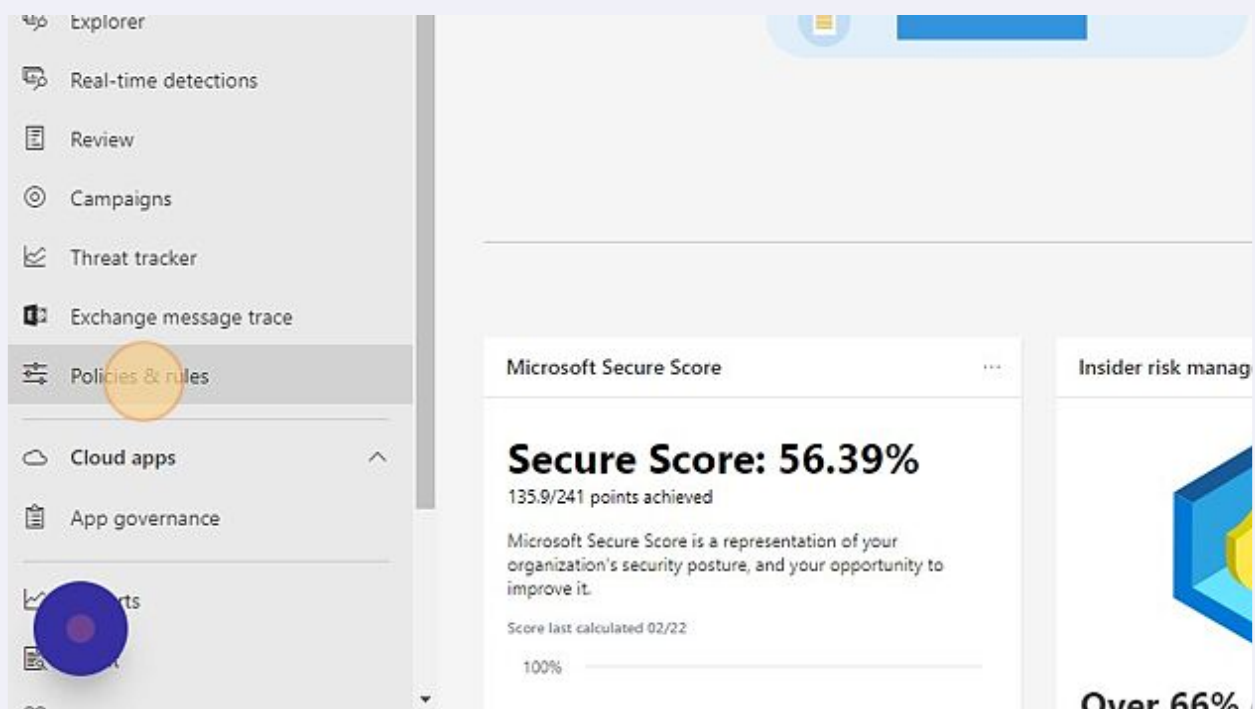


How to Configure an Anti-Malware Policy in Microsoft 365

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 va

Name
Threat policies
Alert policy
Manage advanced alerts
Activity alerts

4 Click "Anti-malware"

Policies

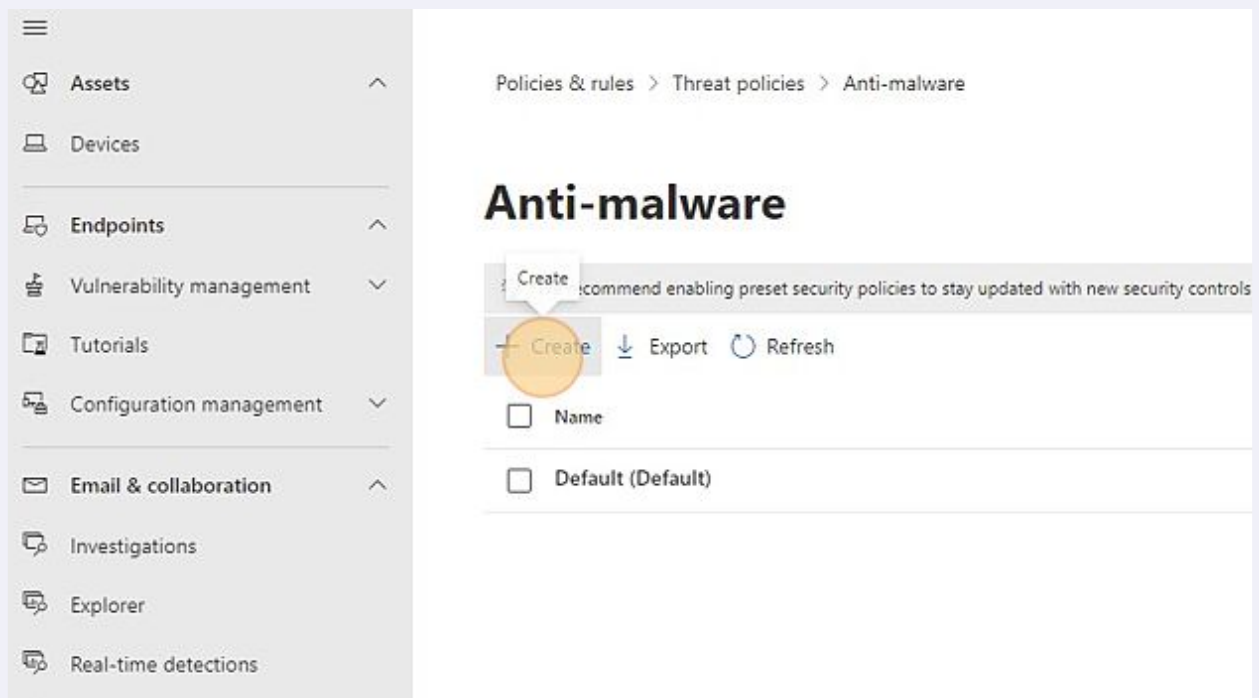
Configuration analyzer

- Anti-phishing
- Anti-spam
- [Anti-malware](#)
- Safe Attachments
- Safe Links

Rules

- Tenant Allow/Block Lists

5 Click "Create"

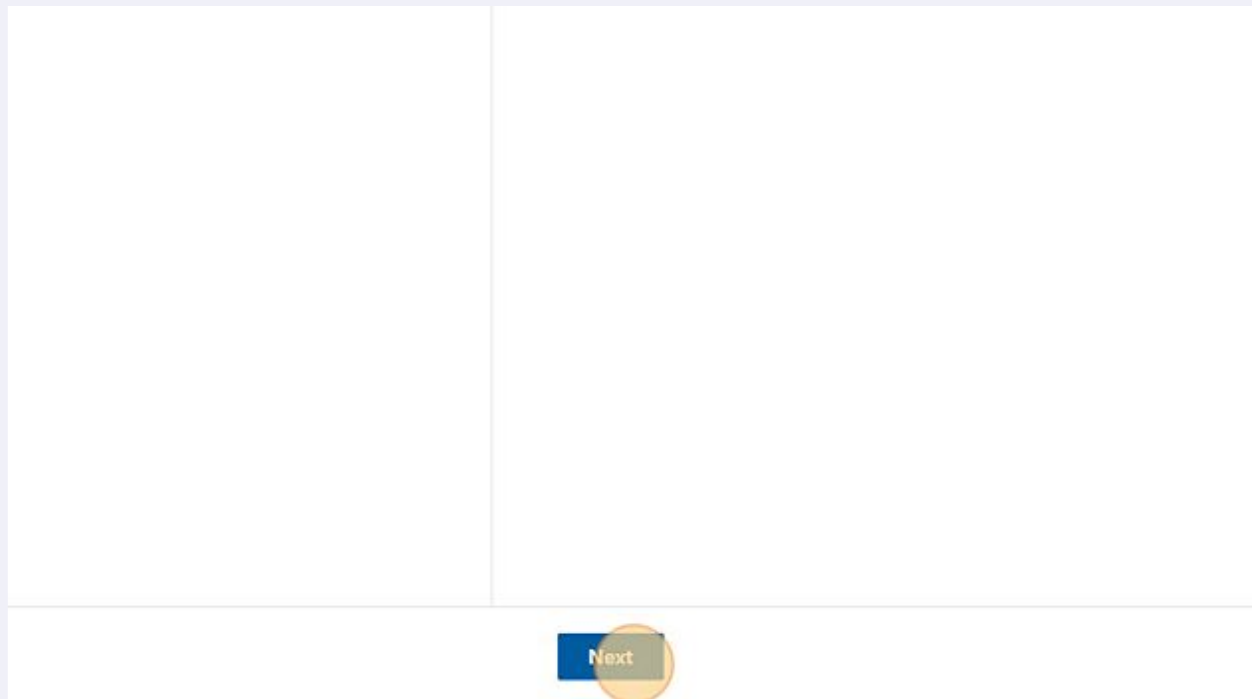


6 Enter "Default-AntiMalware-Policy" in the "Name" field.

The screenshot shows a form titled 'Name your policy'. It has two main fields: 'Name *' and 'Description'. The 'Name *' field contains the text 'Default-AntiMalware-Policy'. The 'Description' field is empty and has a yellow circle highlighting its start. The form is set against a light gray background.

7

Click "Next"



8

Target your domain and click "Next"

A screenshot of a web form with a light gray border. The form is divided into two main sections by a vertical line. The left section is empty. The right section contains a "Domains" label above a text input field. The input field contains the text "imperionllc.com". Below the input field, there is a checkbox labeled "Exclude these users, groups and domains". At the bottom of the form, there are two buttons: a gray "Back" button and a blue "Next" button. A yellow circle is drawn around the "Next" button.

9 Ensure that "Quarantine the message" is the action taken.

Configure the settings for this anti-malware policy

Protection settings

☒ Enable the common attachments filter ⓘ
.ace, .apk, .app, .appx, .ani, .arj, .bat, .cab, .cmd, .com and 43 other types

Select file types

When these file types are found:

☒ Reject the message with a non-delivery receipt (NDR) ⓘ

☐ Quarantine the message

☒ Enable zero-hour auto purge for malware (Recommended) ⓘ

Quarantine policy

Default Quarantine Policy

Permission to release quarantined messages will be ignored for messages with malware detected and we will fall back to release request instead

Notification

10 Click "Enable zero-hour auto purge for malware"

Protection settings

☒ Enable the common attachments filter ⓘ
.ace, .apk, .app, .appx, .ani, .arj, .bat, .cab, .cmd, .com and 43

Select file types

When these file types are found:

☒ Reject the message with a non-delivery receipt (NDR) ⓘ

☐ Quarantine the message

☒ Enable zero-hour auto purge for malware (Recommended) ⓘ

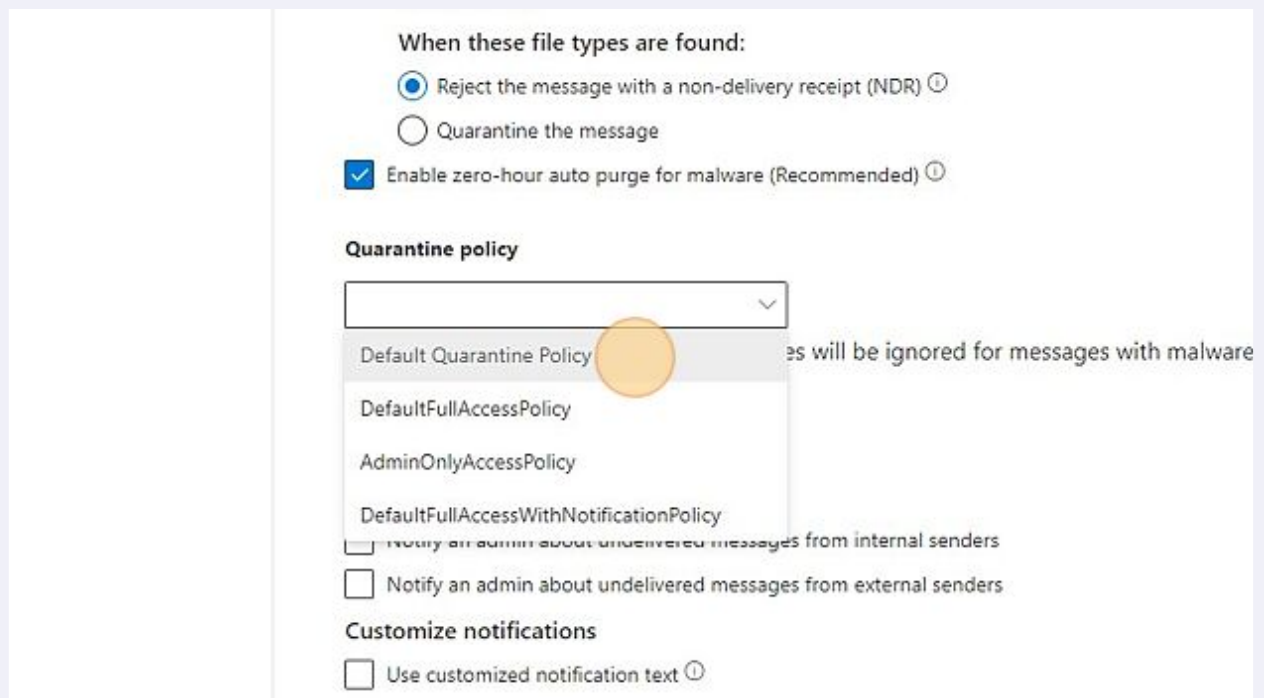
Quarantine policy

Permission to release quarantined messages will be ignored for messages with malware detected and we will fall back to release request instead

Notification

Admin notifications

11 Click "Default Quarantine Policy"



When these file types are found:

- ☒ Reject the message with a non-delivery receipt (NDR) ⓘ
- ☐ Quarantine the message
- ☒ Enable zero-hour auto purge for malware (Recommended) ⓘ

Quarantine policy

Default Quarantine Policy ⓘ

DefaultFullAccessPolicy

AdminOnlyAccessPolicy

DefaultFullAccessWithNotificationPolicy

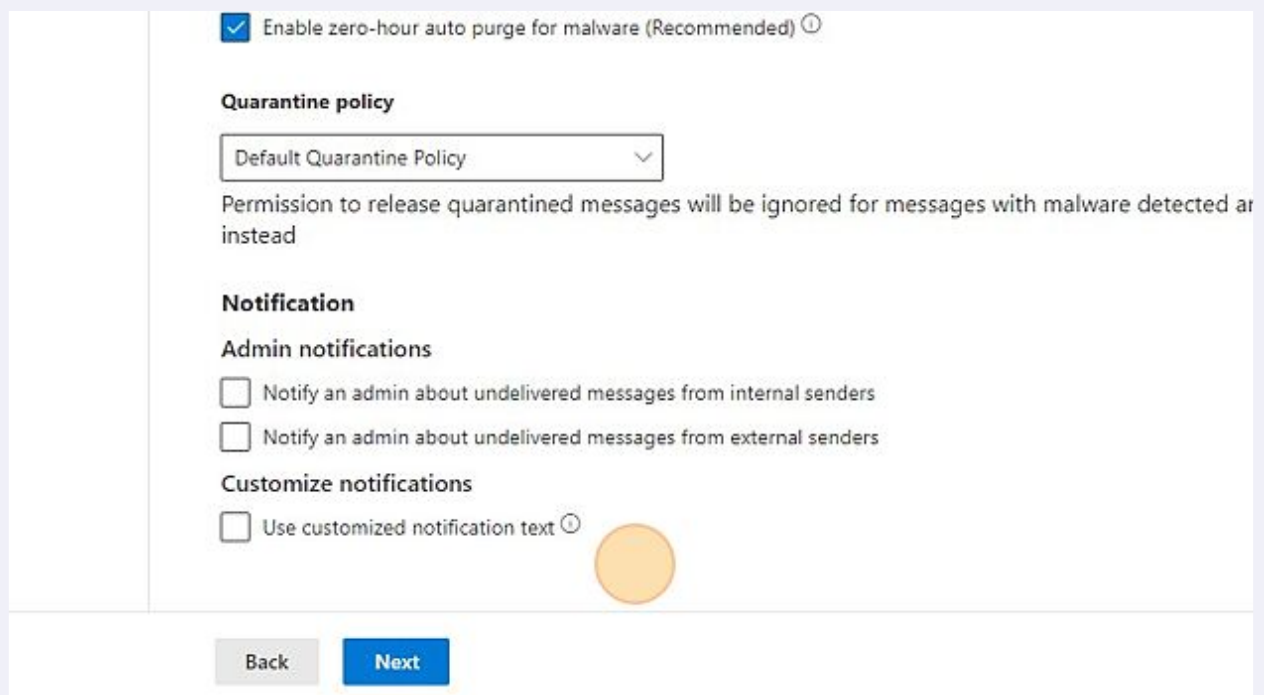
☐ Notify an admin about undelivered messages from internal senders

☐ Notify an admin about undelivered messages from external senders

Customize notifications

☐ Use customized notification text ⓘ

12 Turn on notifications if you like.



☒ Enable zero-hour auto purge for malware (Recommended) ⓘ

Quarantine policy

Default Quarantine Policy ⓘ

Permission to release quarantined messages will be ignored for messages with malware detected and instead

Notification

Admin notifications

☐ Notify an admin about undelivered messages from internal senders

☐ Notify an admin about undelivered messages from external senders

Customize notifications

☐ Use customized notification text ⓘ

Back Next

13 Click "Next"

	<div><input checked="" type="checkbox"/> Enable zero-hour auto purge for malware (Recommended) ⓘ</div> <div>Quarantine policy <div>Default Quarantine Policy ▼</div><p>Permission to release quarantined messages will be ignored for messages with this policy. Instead, the message will be released to the inbox.</p></div> <div>Notification Admin notifications <div><input type="checkbox"/> Notify an admin about undelivered messages from internal senders</div><div><input type="checkbox"/> Notify an admin about undelivered messages from external senders</div>Customize notifications <div><input type="checkbox"/> Use customized notification text ⓘ</div></div>
<div><div>Back</div><div>Next</div></div>	

14 Review the settings and click "Submit"

	<p>When these file types are found: Reject the message with a non-delivery receipt (NDR)</p> <div>Enable zero-hour auto purge for malware (Recommended) ● On</div> <div>Notify an admin about undelivered messages from internal senders ● Off</div> <div>Notify an admin about undelivered messages from external senders ● Off</div> <div>Customize notifications ● Off</div> <div>Quarantine policy Default Quarantine Policy</div> <div>Edit</div>
<div><div>Back</div><div>Submit</div></div>	

15

Click "Done"

