Configure Secure Email Gateway to use Microsoft Quarantine and Microsoft Quarantine Notification

Contents

Introduction

This document describes the configuration steps required to integrate Cisco Secure Email (CES) with Microsoft 365 quarantine.

Overview

In modern email infrastructures, multiple security layers are often implemented, resulting in emails being quarantined by different systems. To streamline user experience and improve notification consistency, it is beneficial to centralize quarantine management in a single platform. This guide explains how to redirect unwanted messages—such as spam and graymail—identified by Cisco CES into the Microsoft 365 user quarantine.

Prerequisites

To complete this configuration, ensure you have the following:

1. An active tenant in **Cisco Secure Email Gateway**
2. An active tenant in **Microsoft Exchange online**.
3. Access to **Microsoft 365 (O365)** services
4. A **Microsoft 365 Defender** license (required to configure quarantine policies and notifications)

Configure Microsoft 365 (O365)

Start by setting up Microsoft 365 to receive and manage quarantined messages.

Enable Quarantine Notifications in Microsoft Exchange online

You can refer to the official Microsoft documentation to configure user notifications for quarantined

messages:
Microsoft Quarantine Notification configuration

Create a Mail Flow Rule

Once notifications are active, configure a rule that redirects messages marked by Cisco Secure Email Gateway to Microsoft's hosted quarantine.

1. Open the **Microsoft Exchange Admin Center**.
2. From the left-hand menu, go to **Mail Flow → Rules**.
3. Click **Add a rule**, and then select **Create a new rule**.
4. Set the rule name to: ***CSE Quarantine Rule***.
5. Under **Apply this rule if**, select **The message header**, then choose **matches text patterns**.
6. In the header name, enter: ***X-CSE-Quarantine***, and set the value to match: ***true***.
7. Under **Do the following**, choose **Redirect the message to**, and select **Hosted Quarantine**.
8. Save the configuration.
9. After saving, ensure the rule is **enabled**.

In the picture you can see how the rule looks like.

CSE Quarantine

Edit rule conditions Edit rule settings

Status: Disabled

Enable or disable rule

Enabled

Updating the rule status, please wait...

Rule settings

Rule name
CSE Quarantine

Mode
Enforce

Severity
Not specified

Set date range
Specific date range is not set

Senders address
Matching Header

Priority
1

For rule processing errors
Ignore

Rule description

Apply this rule if

'X-CSE-Quarantine' header matches the following patterns: 'true'

Do the following

Deliver the message to the hosted quarantine.

Rule comments

Microsoft Rule

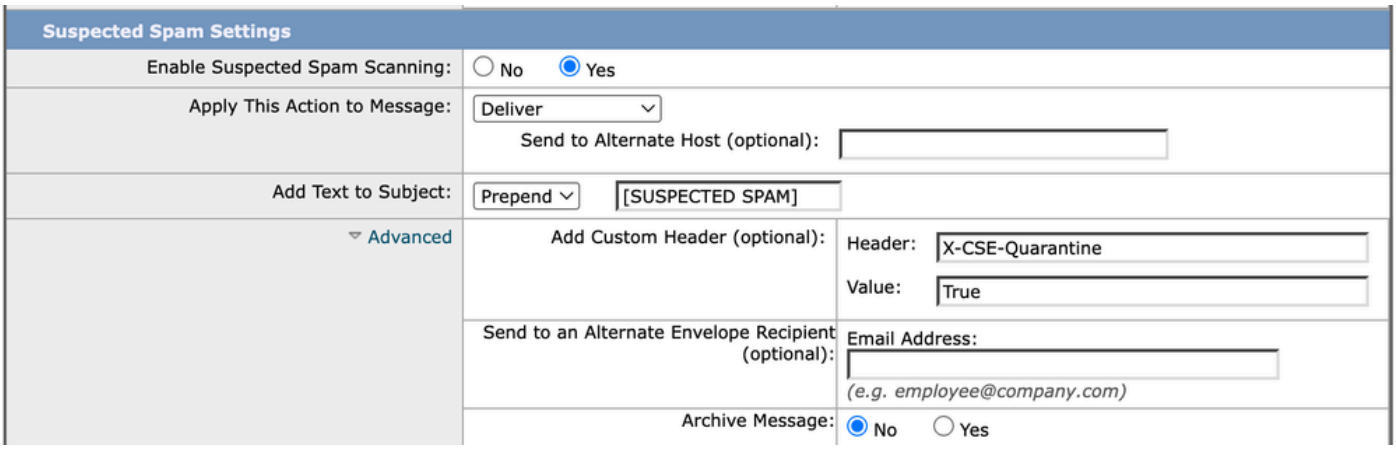
Configure Cisco Secure Email

In Cisco CES, you can add a custom header (***X-CSE-Quarantine: true***) to any message we want to redirect to Microsoft's quarantine.

These messages can be flagged by any content filter or engine in CES. In this example, we configure it for **Suspect Spam** messages.

1. Open the **Cisco Secure Email Management Console**.
2. Go to **Mail Policies → Incoming Mail Policies**.
3. Edit the policies you wish to modify (for example, select the **Default Policy**).
4. Click on the **Spam settings** for the selected policy.
5. Under **Suspect Spam**, change the action from **Quarantine** to **Deliver**.
6. Click on **Advanced** and add a custom header:
    - **Header name**: ***X-CSE-Quarantine***
    - **Value**: ***true*** (same value used in the Microsoft rule)
7. Click **Submit**, then **Commit Changes** to apply the configuration.

In the picture you can see how the configuration looks like.

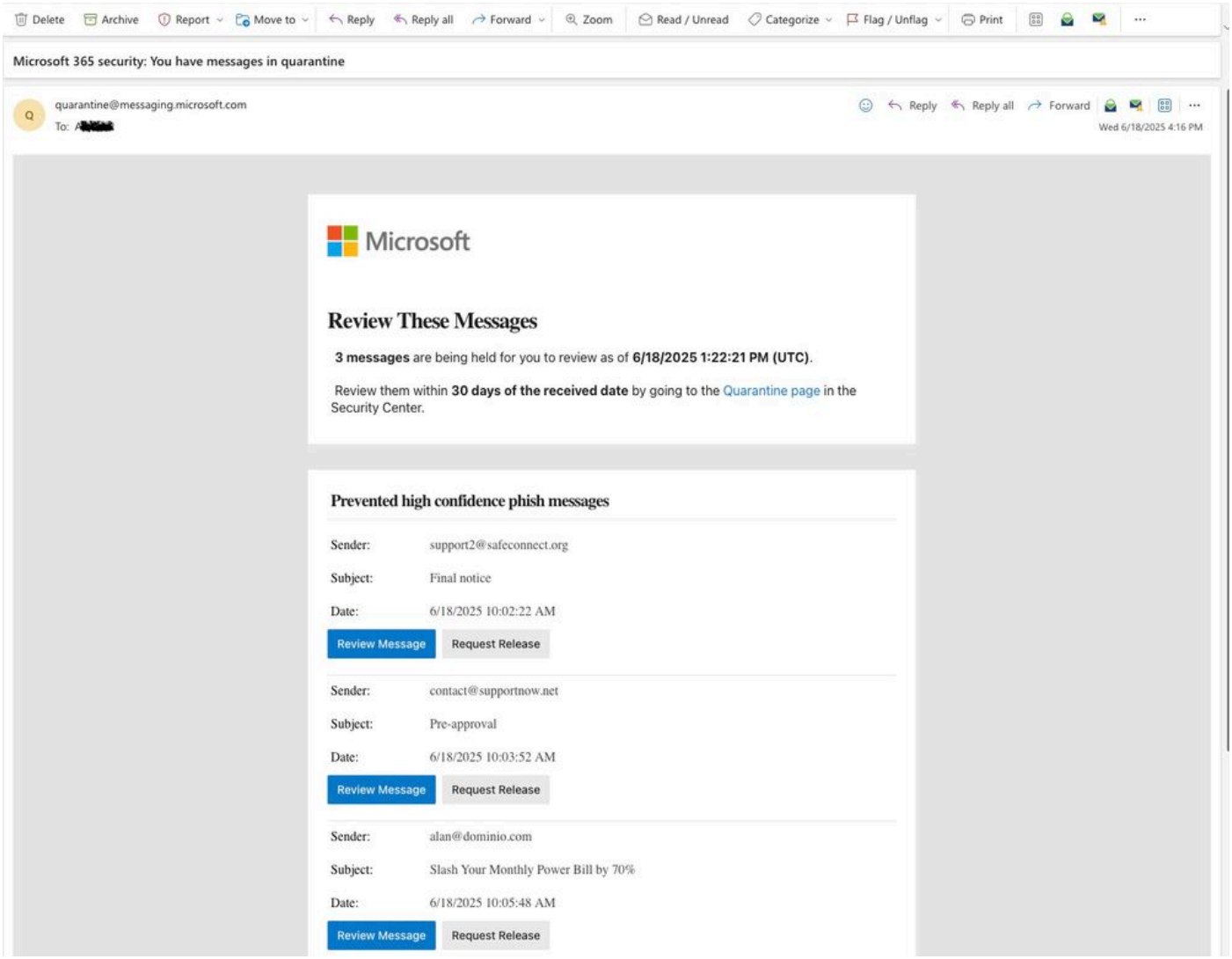


CES configuration

Verify

From this point on, emails identified by Cisco CES as potential spam are going to be tagged with the custom header. Microsoft 365 detects this tag and redirect the message to the user quarantine.

Users w¡are going receive quarantine notifications according to the Microsoft 365 configuration.


Delete
Archive
Report
Move to
Reply
Reply all
Forward
Zoom
Read / Unread
Categorize
Flag / Unflag
Print
Microsoft 365 security: You have messages in quarantine
quarantine@messaging.microsoft.com
To: A[redacted]
Reply
Reply all
Forward
Wed 6/18/2025 4:16 PM
Microsoft
Review These Messages
3 messages are being held for you to review as of 6/18/2025 1:22:21 PM (UTC).
Review them within 30 days of the received date by going to the Quarantine page in the Security Center.
Prevented high confidence phish messages
Sender: support2@safeconnect.org
Subject: Final notice
Date: 6/18/2025 10:02:22 AM
Review Message
Request Release
Sender: contact@supportnow.net
Subject: Pre-approval
Date: 6/18/2025 10:03:52 AM
Review Message
Request Release
Sender: alan@dominio.com
Subject: Slash Your Monthly Power Bill by 70%
Date: 6/18/2025 10:05:48 AM
Review Message
Request Release