

M365□□

- [M365□□□](#)

- 設定規則條件
- 設定規則設定
- 檢閱並完成

設定規則條件

傳輸規則的名稱與設定條件

您離開預設規則模式。您現在可以看到所有規則條件

名稱 *

若為以下情況，套用這個規則 *

寄件者 選取一個

執行下列動作 *

轉寄要核准的電子郵件 選取一個

除非 選取一個 選取一個

M365 admin center

Entra

Microsoft Defender



Microsoft Defender

原則與規則 > 威脅原則 > 反垃圾郵件原則

反垃圾郵件原則

我們建議啟用預先設定的安全性原則，以使用新的安全性控制項和我們建議的設定來保持最新狀態。 [檢視預設安全性原則](#)

使用此頁面來設定包含在反垃圾郵件保護的原則。這些原則包含垃圾郵件過濾、垃圾郵件篩選、以及輸出垃圾郵件篩選。 [深入了解](#)

建立原則 重新整理

4個項目

搜尋

名稱	狀態	優先順序	類型
<input type="checkbox"/> 使用者24小時內發超過300封信件則封鎖	● 開啟	0	自訂輸出垃圾郵件原則
<input type="checkbox"/> 反垃圾郵件輸入原則 (預設)	● 一律開啟	最低	
<input type="checkbox"/> 垃圾郵件過濾原則 (預設)	● 一律開啟	最低	
<input type="checkbox"/> 反垃圾郵件輸出原則 (預設)	● 一律開啟	最低	



Microsoft Defender

搜尋

身分識別

儀表板

健康情況問題

工具

電子郵件與共同作業

調查

總管

檢閱

行銷活動

威脅追蹤程式

Exchange 訊息追蹤

攻擊模擬訓練

原則與規則

檢閱

控制中心

!

追蹤目標為您使用者的網路釣魚與惡意程式碼活動，並採取適當的動作。

隔離

☒

檢閱隔離的郵件，並決定是否要將其釋出給一或多個預定收件者。

受限制的實體

解除封鎖因傳送過多被標示為垃圾郵件/大量郵件的郵件而遭到封鎖的實體。

解除封鎖因傳送過多被標示為垃圾郵件/大量郵件的郵件而遭到封鎖的實體。

惡意程式碼趨勢

未偵測到任何惡意程式碼