

NS-M365-001

Exchange Online Administration, Shared Mailbox Troubleshooting & Permission Auditing

NOCTURNE SYSTEMS / WAYNE ENTERPRISE SYSTEMS / CONTROLLED MICROSOFT 365 LAB

Executive summary

This lab documented an end-to-end Exchange Online support workflow: reviewing an existing Security shared mailbox, configuring delegated access, investigating Outlook access failures, validating mailbox functionality, examining message-trace evidence, and using PowerShell to audit and export permissions. The work was performed in a controlled Microsoft 365 Business Premium tenant using fictional lab identities.

Environment and scope

Platform	Microsoft 365 Business Premium; Exchange Online; Microsoft Entra ID
Tools	Exchange Admin Center; Outlook on the web; Windows PowerShell 5.1; ExchangeOnlineManagement 3.10.1; VS Code
Target resource	Security shared mailbox (lab tenant)
Principal	Bruce Wayne test user, distinct from the lab administrator account
Scope	Single-mailbox delegation, functional verification, mail-flow investigation, read-only audit and CSV export

1 | Access request and baseline

Scenario: An authorized employee needed to open Security mailbox contents and send replies that appear to originate from Security. The existing shared mailbox and its recipient type were confirmed in Exchange Admin Center. The delegated Full Access and Send As assignments were checked before the controlled configuration step.

Least-privilege decision: assign Read and manage (Full Access) for mailbox contents, and Send As for sender identity; do not grant the Exchange Administrator role. Send on behalf was not required.

The baseline was captured after a test delegation had been removed and before the subsequent controlled reassignment. It should not be presented as the first-ever configuration of this mailbox.

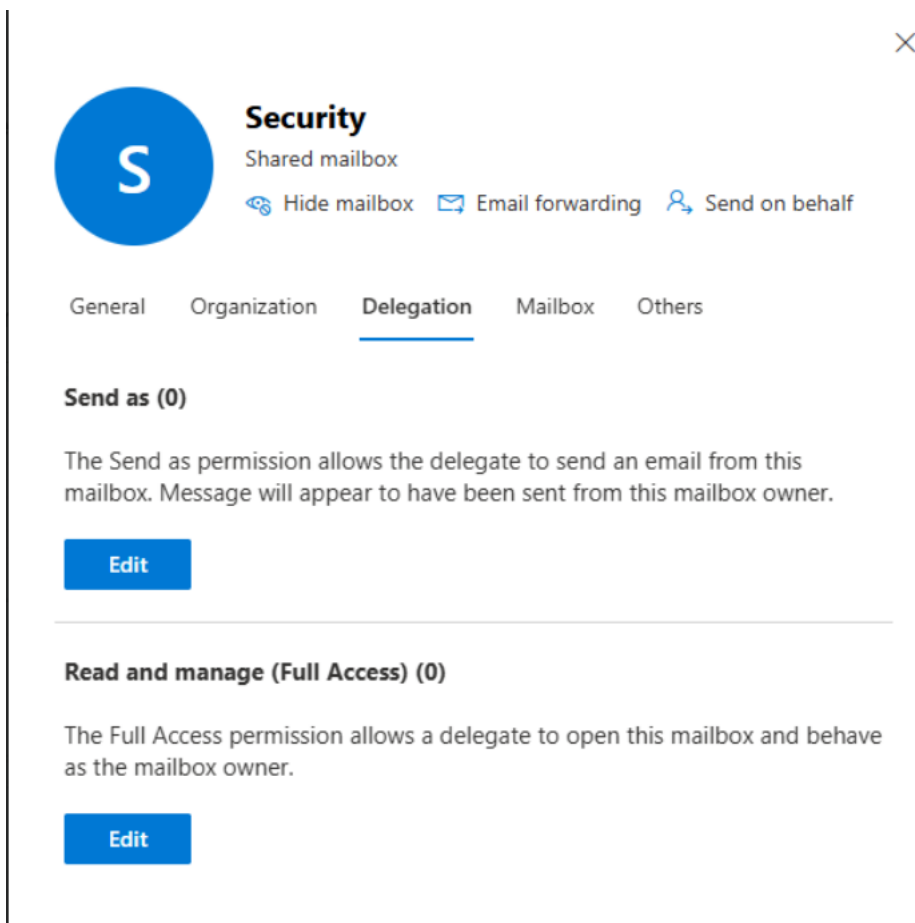


Figure 1. Controlled baseline showing no named delegate under Full Access and Send As.



Security

Shared mailbox

 Hide mailbox  Email forwarding  Send on behalf

General

Organization

Delegation

Mailbox

Others

Send as (1)

The Send as permission allows the delegate to send an email from this mailbox. Message will appear to have been sent from this mailbox owner.

Edit

Read and manage (Full Access) (1)

The Full Access permission allows a delegate to open this mailbox and behave as the mailbox owner.

Edit

Figure 2. Bruce Wayne explicitly assigned Full Access and Send As.

2 | Outlook access investigation

Following the delegation changes, Bruce could access his own primary Outlook mailbox, but attempts to open the Security mailbox initially failed. The “Open another mailbox” workflow returned an access-denied startup error; adding the shared mailbox to Outlook navigation also produced a permission-related message.

The permission assignments were confirmed in Exchange Admin Center and no repeated permission changes were made during the later retest. After additional time elapsed, Bruce successfully accessed the shared mailbox. Permission propagation delay was a plausible explanation, but the exact cause was not conclusively established.

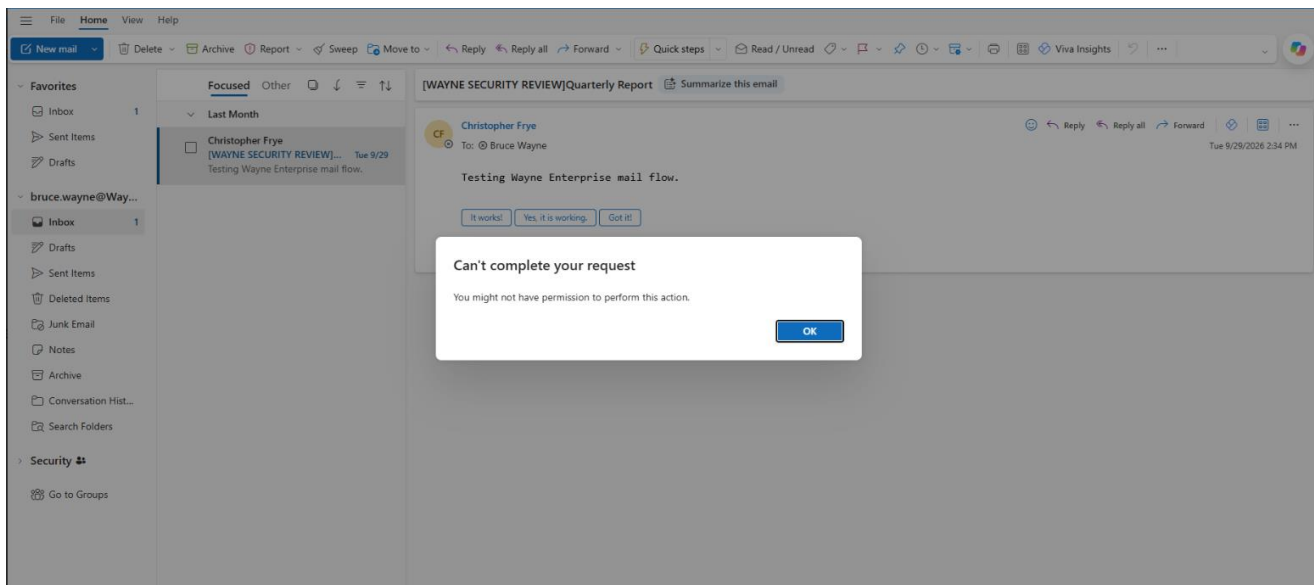


Figure 3. Initial failure opening the Security shared mailbox in Outlook.

Access verification: the test user later opened Security successfully. This result was observed in the lab; the dedicated success screenshot can be retained in the private evidence set if desired.

3 | Functional Send As validation

A harmless test email was sent from the Security identity, and the received message showed Security as its sender. This confirmed functional Send As behavior in the test. The message body used a humorous fictional example; use a neutral or cropped version for public presentation.

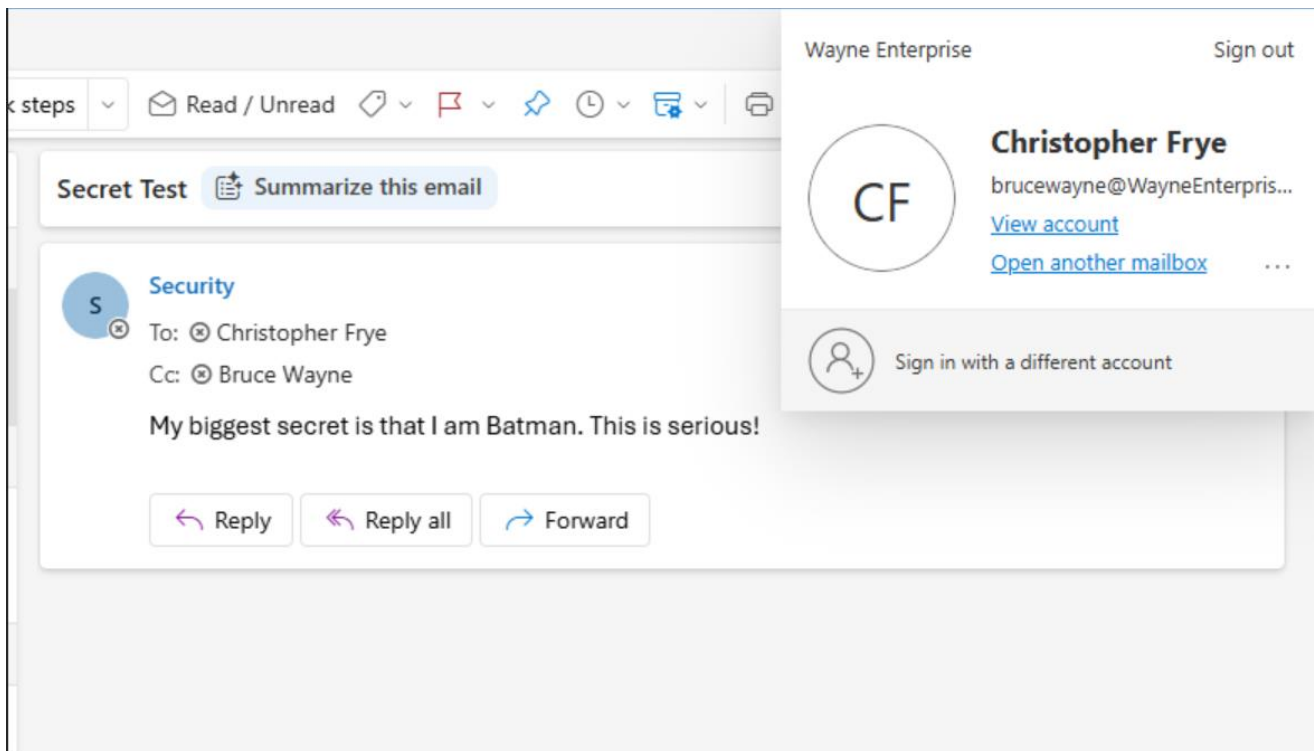


Figure 4. Successful Send As verification using the delegated test identity.

4 | Message trace and delivery analysis

The Exchange Admin Center message-trace feature was used to search for the Security test email. Search results and message details were captured for review. Message trace helps establish Exchange delivery processing, but “Delivered” alone does not prove the recipient read the email or saw it in their Inbox.

The precise result shown in the saved trace has not yet been reviewed for this case study. Record the final status and relevant events from the screenshot before publishing; do not assume a specific outcome.

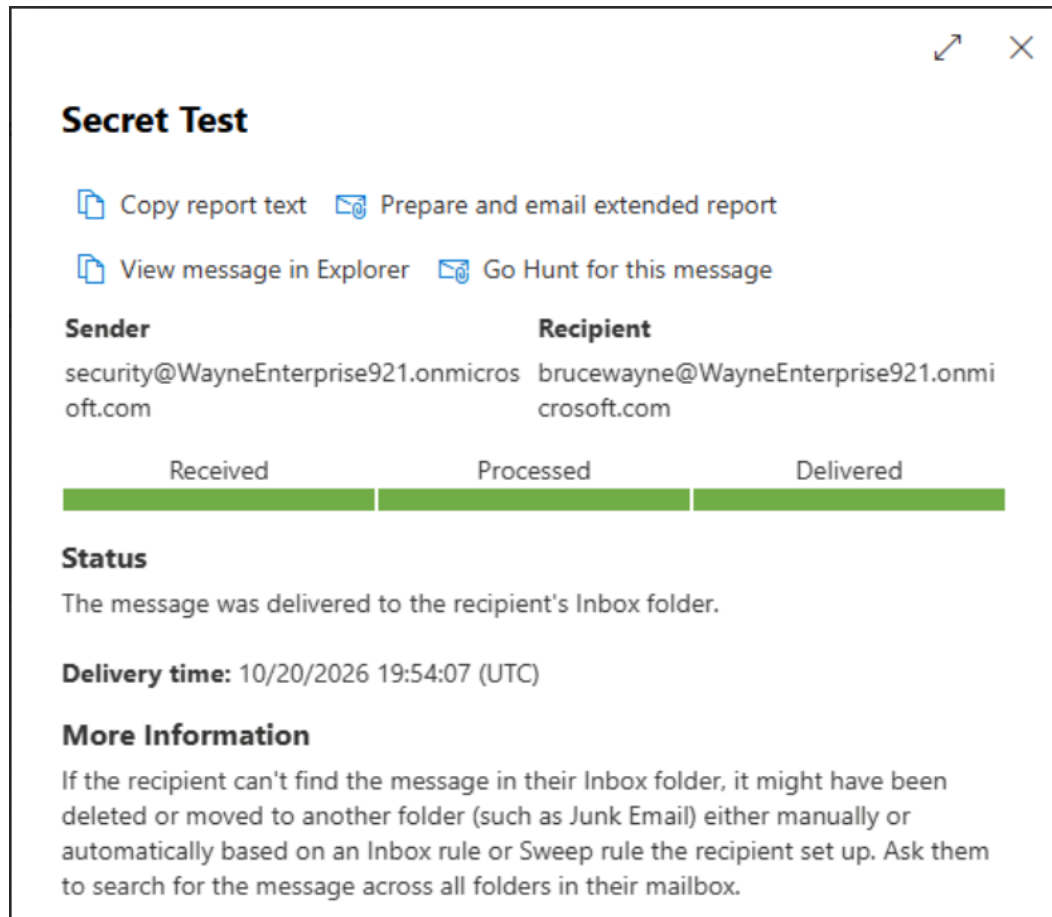


Figure 5. Message trace evidence for the Security test message; delivery status to be transcribed from source evidence.

5 | PowerShell audit and reporting

ExchangeOnlineManagement version 3.10.1 was installed and imported on Windows PowerShell 5.1. A local execution-policy restriction was resolved for the current PowerShell process using RemoteSigned. Authentication inside the VS Code terminal encountered difficulties; the audit was then run successfully in an authenticated Windows PowerShell session.

Get-EXOMailboxPermission returned an explicit FullAccess entry for the delegated Bruce Wayne user. Get-RecipientPermission separately returned an explicit SendAs entry. Built-in NT AUTHORITY\SELF entries were excluded from the concise delegate view. Another similarly named account was checked with Get-EXORecipient and confirmed to be a separate directory object.

A saved script, MailboxPermissionAudit.ps1, reproduced the two read-only permission queries and exported a MailboxPermissionReport.csv. The report contained two access records: FullAccess and SendAs. The script was tested against one mailbox; it is not a tenant-wide access certification workflow.

```

PS C:\Users\domin\OneDrive\Documents\NS-M365-001> cd "$HOME\OneDrive\Documents\NS-M365-001"
PS C:\Users\domin\OneDrive\Documents\NS-M365-001> .\MailboxPermissionAudit.ps1
Starting mailbox permission audit...
Target mailbox: security@WayneEnterprise921.onmicrosoft.com

=== FULL ACCESS PERMISSIONS ===

User                                AccessRights IsInherited Deny
----                                -
bruce.wayne@WayneEnterprise921.onmicrosoft.com {FullAccess}      False False

=== SEND AS PERMISSIONS ===

Trustee                                AccessRights IsInherited Deny
-----                                -
bruce.wayne@WayneEnterprise921.onmicrosoft.com {SendAs}          False

CSV report saved to: C:\Users\domin\OneDrive\Documents\NS-M365-001\MailboxPermissionReport.csv
PS C:\Users\domin\OneDrive\Documents\NS-M365-001> |

```

Figure 6. Reusable PowerShell permission audit run successfully with CSV export.

Results and significance

- Confirmed least-privilege mailbox delegation and verified the two distinct capabilities: access to contents and sender identity.
- Isolated a shared-mailbox-specific Outlook error from successful primary mailbox access; documented failure and successful retest without overclaiming root cause.
- Performed a mail-flow investigation and distinguished delivery status from message readership.
- Verified explicit access assignments using two Exchange Online PowerShell interfaces, then generated a reusable CSV report.
- Practiced identity disambiguation by comparing distinct Entra directory object identifiers behind similar account addresses.

Limitations and lessons learned

This was a controlled, non-production tenant with a single shared mailbox and lab user. The automation reports permission assignments; it does not evaluate business justification, query all mailboxes, or remediate access. The exact message trace status remains to be copied from the saved evidence. Technical commands were developed with AI assistance, then executed, troubleshooted, reviewed, and tested in the lab.