

PHASE 4: Exchange Online Setup & Email Infrastructure Deployment

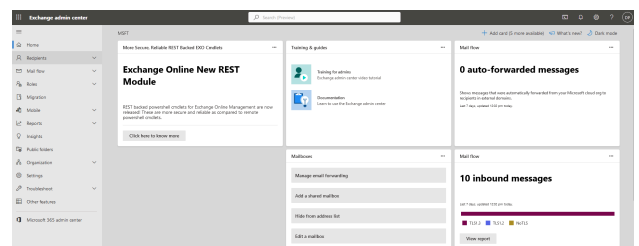
This phase outlines the configuration of Exchange Online within the Microsoft 365 tenant for DipeshCorp (alias: **nxhz**). It includes the setup of user mailboxes, shared mailboxes, distribution groups, transport (mail flow) rules, retention policies, and baseline security measures to simulate a real-world enterprise email infrastructure. These configurations lay the foundation for secure collaboration and regulatory compliance in a hybrid cloud environment.

I. Access and Initialize Exchange Admin Center (EAC)

Gain administrative access to Exchange Online and familiarize with core configuration areas.

Actions Completed:

- Navigated to the Exchange Admin Center (EAC):
URL: <https://admin.exchange.microsoft.com>
- Signed in using: **admin@dipeshcorp.onmicrosoft.com**
- Explored primary EAC modules:
 - Recipients: Manage user and shared mailboxes, groups
 - Mail Flow: Transport rules, accepted domains, connectors
 - Protection: Anti-spam and anti-phishing settings
 - Compliance Management: Retention and litigation policies
 - Organization: Address book policies and calendar sharing



II. Shared Mailbox Configuration

Set up a shared mailbox to simulate help desk functionality accessible by multiple IT team members.

Actions Completed:

1. Navigated to EAC → Recipients > Shared
2. Clicked: + Add a shared mailbox
3. Entered:
 - Name: IT Helpdesk
 - Email: ithelpdesk@dipeshcorp.onmicrosoft.com
4. Added members: Test Device, Dipesh Patel, Dipesh HR
 - These users now have permission to send/receive as this mailbox.
 - It might take up to 60 minutes for the change to be effective in Outlook and OWA.

Validation:




1. Logged into Test Device's Outlook → Confirmed shared mailbox auto-mapped
2. Sent/Received test emails from ithelpdesk@dipeshcorp.onmicrosoft.com

Important Note:

To ensure that on-premises Active Directory (AD) users appear in the Exchange Admin Center and can be assigned to shared mailboxes or distribution groups, the following conditions must be met:

-  The user must be synchronized to Microsoft Entra ID (Azure AD) using Azure AD Connect.
-  The synchronized user must be assigned a Microsoft 365 license that includes Exchange Online.

If either condition is not met:

-  The user will not be mail-enabled in the cloud
-  The user will not appear in the Exchange Admin Center
-  You will be unable to add them to shared mailboxes, groups, or apply mail flow policies

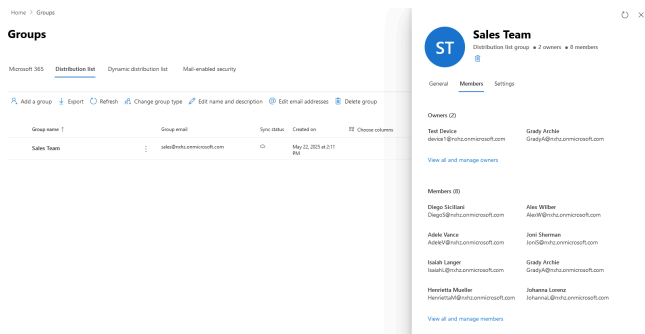
Always verify synchronization status in Entra Admin Center and assign appropriate licenses through the Microsoft 365 Admin Center.

III. Distribution Group Setup

Enable group-based communication by creating a distribution list for multi-user email delivery.

Actions Completed:

1. Navigated to EAC → Recipients > Groups
2. Clicked: + Add a group
3. Type: Distribution
4. Configured:
 - Name: Sales Team
5. Added Owners: Test Device, Grady Archie
6. Added members: Adele, Alex, Diego, etc.
7. Group Email: sales@dipeshcorp.onmicrosoft.com
 - Uncheck Communication
 - Joining the group: Owner approval
 - Leaving the group: Closed (Only owner can remove)



Validation:

- Sent test email to sales@dipeshcorp.onmicrosoft.com
 - Confirmed receipt by all group members
-

IV. Mail Flow Rules (Transport Rules)

Define organization-wide email governance policies using conditional mail rules.

Actions Completed:

Use Case 1: Block Executable Attachments

1. EAC → Mail Flow > Rules > Add a rule
2. Rule Name: Block EXE Attachments
3. Apply this rule if:
 - Any attachment | file extension includes these words > “exe”
4. Do the following:
 - Block the message | Reject the message with explanation: “Executable attachments are not allowed.”

Block EXE Attachments

[Edit rule conditions](#) [Edit rule settings](#)

Status: Enabled

Enable or disable rule: ☒ Enabled

Rule settings

Rule name	Block EXE Attachments	Mode	Enforce
Severity	High	Set date range	Specific date range is not set
Senders address	Matching Header	Priority	0
For rule processing errors	Ignore		

Rule description

Apply this rule if

has an attachment with a file extension that matches one of these values: 'exe'

Do the following

Set audit severity level to 'High' and reject the message and include the explanation 'Executable attachments are not allowed.' with the status code: 5.7.1

Rule comments

Use Case 2: External Email Disclaimer

1. Rule Name: External Email Disclaimer
2. Apply this rule if:
 - The Sender | is external/internal > “Outside the organization”
3. Do the following:
 - Apply a disclaimer to the message | Append a disclaimer > Select text: “This is an external email. Please exercise caution.”

External Email Disclaimer

[Edit rule conditions](#) [Edit rule settings](#)

Status: Disabled

Enable or disable rule: ☒ Enabled

Updating the rule status, please wait...

Rule settings

Rule name	External Email Disclaimer	Mode	Enforce
Severity	High	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

Is received from 'Outside the organization'

Do the following

Set audit severity level to 'High' and Append the message with the disclaimer 'This is an external email. Please exercise caution.'. If the disclaimer can't be applied, attach the message to a new disclaimer message.

Rule comments

Validation:

1. Attempted sending .exe attachment → Rejection confirmed
2. Sent email from external Gmail account → Disclaimer appended in received email

V. Retention and Security Policies

Apply governance to email retention and implement security controls against spam and phishing threats.

Actions Completed:

1. Retention Policy Implementation

- Accessed Microsoft Purview Compliance Center: <https://purview.microsoft.com>
- Navigated to: Data lifecycle management > Microsoft

365 > Retention policies

- Created new policy:
 - Name: 5-Year Retention Policy
 - Policy Scope: Default
 - Type of Retention Policy: Static
 - Applied to: Exchange mailboxes and Microsoft 365 Group mailboxes & sites
- Retention Settings:
 - Retain items for 5 years
 - Action: Delete automatically after retention period

5-Year Retention Policy

Status
Enabled (Pending)

Admin units (preview)
Full directory

Applies to content in these locations
Exchange mailboxes
Microsoft 365 Group mailboxes & sites

Settings

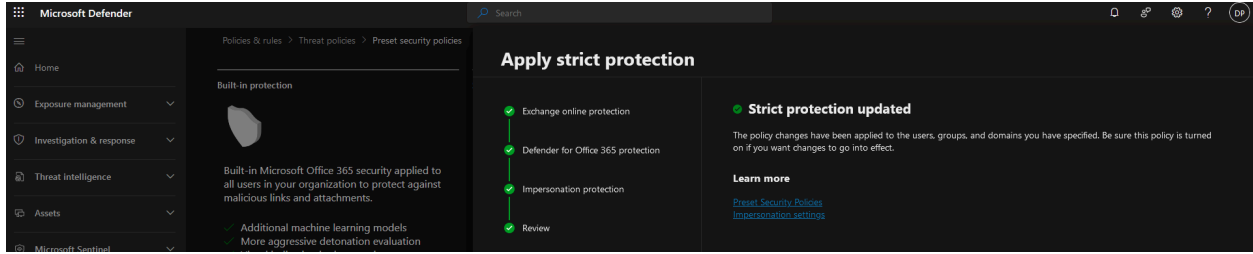
Retention period
Keep content, and delete it if it's older than 5 years

Preservation lock
No

2. Anti-Spam and Anti-Phishing Setup

- Accessed Microsoft 365 Defender Portal: <https://security.microsoft.com>
- Navigated to: Email & Collaboration → Policies & Rules → Threat Policy
- Select Preset security policy > Turn on Strict protection by Manage protection settings
- Assigned policies to all user mailboxes
- Auto-Configured:
 - Anti-Spam
 - Anti-Phishing

Optional Note: SPF, DKIM, and DMARC records will be implemented when a custom domain is added.



VI. Testing and Verification

Validate email functionality, mailbox access, and policy effectiveness.

Actions Completed:

Validation Performed:

1. User: Test Device → Dipesh IT email: Delivered
 2. Outside Organisation Gmail → device1@dipeshcorp.onmicrosoft.com: Received with disclaimer
 3. ithelpdesk@dipeshcorp.onmicrosoft.com: Accessible by Test Device and Dipesh Patel
 4. sales@dipeshcorp.onmicrosoft.com: Delivered to group members
 5. .exe attachment blocked as expected
 6. Retention policy confirmed in Compliance Center (applied to Test Device)
-

V. Completion Outcome:

With Exchange Online successfully configured for DipeshCorp, Phase 4 established a complete and secure cloud-hosted email environment. This includes collaborative features such as shared mailboxes and distribution lists, enforced security rules, and compliance controls — replicating real-world enterprise messaging standards in Microsoft 365.