

Phase 1: Microsoft 365 Developer Tenant Deployment

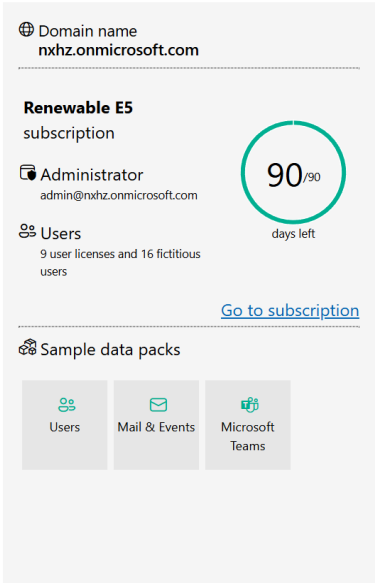
This report details the procedural execution and validation of a Microsoft 365 E5 Developer Tenant for DipeshCorp (*Alias of **nxhz***), designed to emulate an enterprise-grade, cloud-native infrastructure. The initiative was undertaken to establish a foundational identity and productivity services environment in preparation for a hybrid cloud deployment. Phase 1 encompasses tenant provisioning, identity setup, license management, baseline security configuration, and service validation.

I. Enrollment in the Microsoft 365 Developer Program

The initial step involved registering for the Microsoft 365 Developer Program, which grants access to a fully licensed, time-limited E5 sandbox tenant. This environment is essential for configuring and testing enterprise services without incurring licensing costs.

Actions Completed:

1. Accessed the [Microsoft 365 Developer Program Portal](#).
2. Initiated enrollment under the "Individual Developer" category.
3. Designated the organization name as "DipeshCorp."
4. Selected the Instant Sandbox option to provision an E5 tenant with preconfigured services.
5. Received tenant domain: **dipeshcorp.onmicrosoft.com**.
6. Created administrative account: **admin@dipeshcorp.onmicrosoft.com**.
7. Stored all credentials securely in an encrypted vault.
8. Completed verification and confirmed tenant activation within approximately 5 minutes.

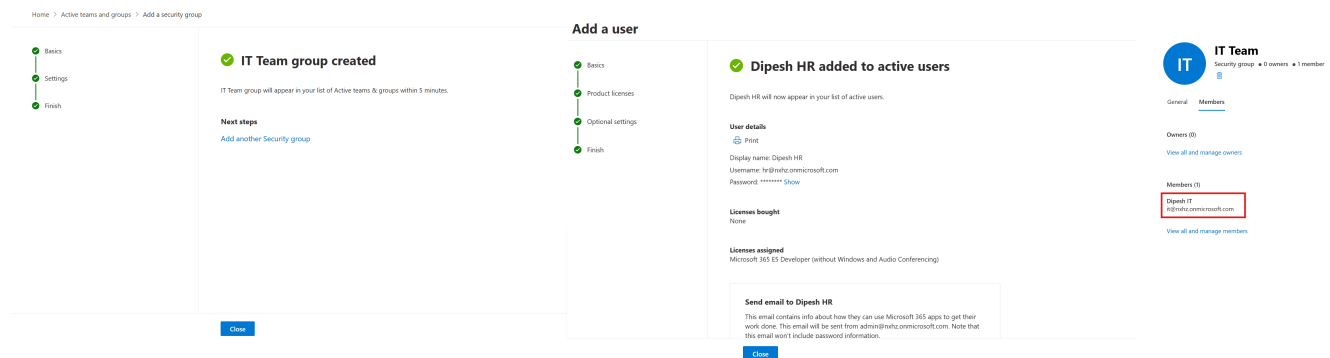


II. Directory Initialization and Organizational Setup

With tenant provisioning completed, directory initialization was conducted using the Microsoft 365 Admin Center. This involved the creation of users and security groups, as well as license assignments required for access to M365 services.

Actions Completed:

1. Logged in to the [Microsoft 365 Admin Center](#) using the global admin account.
2. Navigated to Users > Active Users to create standard user accounts:
 - [hr@dipeshcorp.onmicrosoft.com](#)
 - [it@dipeshcorp.onmicrosoft.com](#)
 - [device1@dipeshcorp.onmicrosoft.com](#)
3. Assigned Microsoft 365 E5 licenses to all users.
4. Proceeded to Groups > Active Groups to configure organizational security groups:
 - IT Team
 - HR Department
5. Added users to their respective groups to enable role-based service access.



III. Validation of Microsoft 365 Core Services

Following user and license provisioning, the availability and administrative access to primary Microsoft 365 services were verified.

Services Accessed and Validated:

- [Exchange Online Admin Center](#)
- [Microsoft Intune Endpoint Manager](#)
- [Microsoft Teams Admin Center](#)

IV. Security Configuration and Compliance Enablement

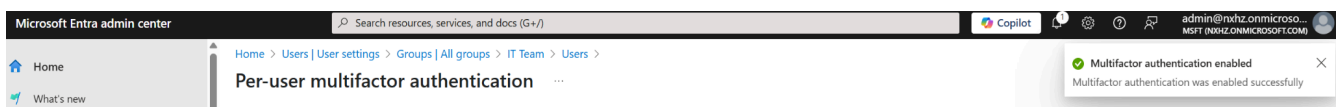
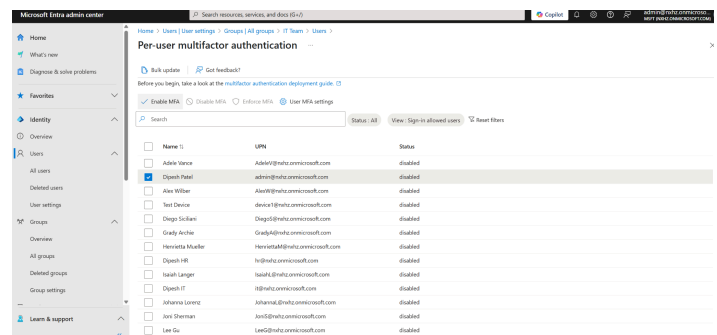
To reinforce access control and enable traceability, two core security configurations were executed: enabling Multi-Factor Authentication (MFA) and activating audit logging.

4.1 Multi-Factor Authentication (MFA)

Objective: To mitigate the risk of unauthorized access to administrative accounts by requiring a secondary authentication mechanism.

Actions Completed:

1. Accessed the [Microsoft Entra Admin Center](#).
2. Navigated to Users > Per-user MFA.
3. Enabled MFA for the global administrator:
`admin@dipeshcorp.onmicrosoft.com`.



4.2 Audit Logging Enablement

Objective: To activate unified audit logs across Microsoft 365 services to monitor privileged activity and enforce regulatory compliance.

Actions Completed:

1. Logged in to the [Microsoft 365 Compliance Center](#).
2. Navigated to Solutions > Audit, or used the search function to locate the "Audit" module.
3. Clicked Start recording user and admin activity.

4.2.1 PowerShell-Based Exception Handling

Error Encountered: Attempting to enable audit logs triggered the following error:

Microsoft.Exchange.Configuration.Tasks.InvalidOperationInDehydratedContextException: The command you tried to run isn't currently allowed in your organization.

Root Cause: This exception is common in newly provisioned tenants where Exchange Online has not yet been fully initialized.

Resolution Process:


1. # Enable PowerShell script execution for the current session
2. Set-ExecutionPolicy -Scope Process -ExecutionPolicy RemoteSigned
- 3.
4. # Import Exchange Online module
5. Import-Module ExchangeOnlineManagement
- 6.
7. # Authenticate with Exchange Online
8. Connect-ExchangeOnline -UserPrincipalName admin@dipeshcorp.onmicrosoft.com
- 9.
10. # Enable organization-wide Exchange customization

Enable-OrganizationCustomization

Following successful execution, audit logging was reinitiated through the Compliance Center.

Screenshot Recommendation:

- Confirmation message indicating that audit log recording has been activated.

 It may take up to 24 hours for audit logs to appear in the compliance search results.