


# PHASE 18: Windows 365 Cloud PC (Cloud VDI) Deployment

Deploy a secure, fully cloud-managed Windows 365 Cloud PC using the Microsoft 365 E5 Developer Tenant. The goal is to simulate enterprise-grade virtual desktop infrastructure (VDI) with integration into Microsoft Intune and Entra ID (Azure AD), without needing on-premises hardware.

## Environment Used:

- Microsoft 365 E5 Developer Tenant: dipeshcorp.onmicrosoft.com
  - Intune + Entra ID (Cloud-only)
  - Admin User: admin@dipeshcorp.onmicrosoft.com
  - Target User: user1@dipeshcorp.onmicrosoft.com
  - Windows 365 License: Windows 365 Business Trial (2 vCPU, 8GB RAM)
  - Endpoint Manager Access: 
  - Entra ID Security Group: CloudPC Users
- 


## I. Assign Windows 365 License


### Actions Completed:

1. Navigated to <https://admin.microsoft.com>
2. Opened: Users → Active Users → user1@dipeshcorp...
3. Selected: Licenses and Apps → Assigned
4. Searched and selected: Windows 365 Business (Trial) – 2 vCPU | 8GB RAM
5. Saved the assignment

 Outcome: License successfully assigned and visible under the user's license tab

 Error: "Cloud PC provisioning failed"

 Cause: License not fully applied or delay in syncing

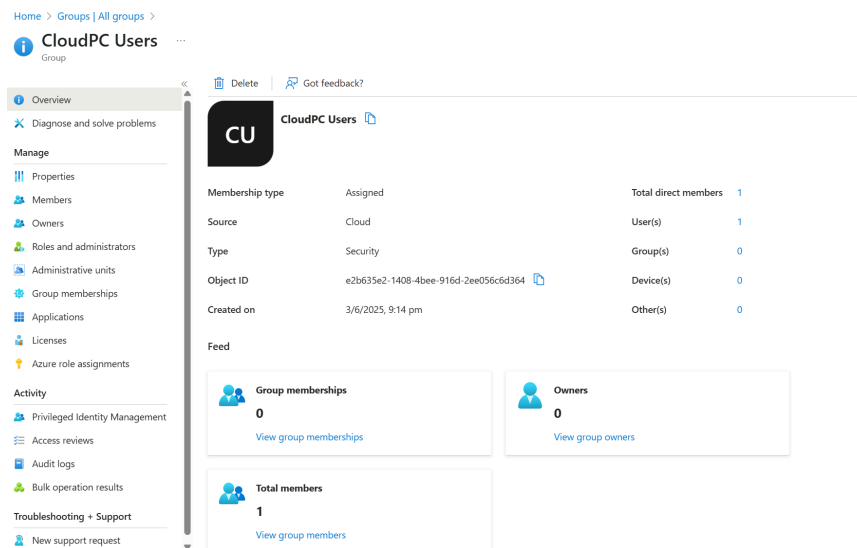
 Fix: Recheck license assignment and allow up to 15–30 minutes for propagation. Reassign if necessary.

---

## II. Create Entra ID Security Group

Actions Completed:

1. Opened: <https://entra.microsoft.com>
2. Went to: Identity → Groups → + New Group
3. Selected:
  - Group Type: Security
  - Name: CloudPC Users
  - Membership Type: Assigned
4. Added Member: device1@dipeshcorp.onmicrosoft.com
5. Created the group



✅ Outcome: Group created and verified in Entra ID → Members tab

❌ Error: "User is not a member of any provisioning group" during Cloud PC setup

✅ Fix: Ensure user is added to the exact security group linked to the provisioning policy. Wait 10–15 minutes after adding user.

### III. Configure Provisioning Policy in Intune

Actions Completed:

1. Opened: <https://endpoint.microsoft.com>
2. Navigated to: Devices → Windows 365 → Provisioning Policies
3. Clicked: + Create Policy

Policy Details Entered:

- Name: DipeshCorp Cloud PC
  - Join Type: Microsoft Entra Join
  - Network: Microsoft-hosted network
  - Image: Windows 11 Enterprise + Microsoft 365 Apps
  - Language: English (Canada)
  - Assigned Group: CloudPC Users
4. Completed policy creation and confirmed in the policy list

✅ Outcome: Policy created and active in Endpoint Manager

❌ Error: "Image not found"

⚠️ Cause: You chose a custom image or none selected

✅ Fix: Always choose the built-in Microsoft-hosted Windows 11 image when simulating

---

### IV. Automatic Provisioning Triggered

Actions Completed:

1. System automatically detected the group membership and began provisioning
2. Monitored status at: Devices → Windows 365 → All Cloud PCs
3. Status:
  - Initially: Provisioning...

- After ~35–45 minutes: Provisioned – Ready
- Device Name: CP-W365-01

✅ Outcome: Cloud PC was provisioned, joined to Entra, and managed by Intune.

❌ Error: "Provisioning Failed"

⚠️ Cause: User license issue or group not assigned to provisioning policy

✅ Fix: Remove user from group, reassign, or check policy group linkage

---

## V. End-User Login (Test Experience)

Actions Completed:

1. Opened browser → <https://windows365.microsoft.com>
2. Signed in as: device1@dipeshcorp.onmicrosoft.com
3. Clicked: Cloud PC tile → "Open in Browser"
4. Waited for the desktop session to load

✅ Outcome: Cloud PC desktop loaded successfully. Verified access to desktop, OneDrive, and pre-installed Office apps.

❌ Error: "Can't connect to Cloud PC"

⚠️ Cause: Conditional Access policy or device non-compliance

✅ Fix: Modify CA policy to allow access from browser or test group. Confirm compliance status in Intune.

---

## VI. Outcome

I successfully deployed a Windows 365 Cloud PC in a cloud-only enterprise environment using Microsoft 365 Developer Tenant. The Cloud PC was provisioned via Intune, Entra ID joined, assigned to a dedicated security group, and made accessible to the user from a browser. This environment simulated real-world enterprise VDI deployment scenarios, complete with group-based provisioning, policy enforcement, and user access testing.

