



AZ-104: Entra ID Users, Groups and Licences

AZ-104 domain 1 (identities and governance), part 1 | Microsoft Entra ID tenants, users, groups, dynamic membership, licences, external (B2B) users, administrative units, SSPR, devices; az CLI, Microsoft Graph PowerShell

AZ-104 Domain 1 Microsoft Entra ID

Tenant, directory objects and where AZ-104 stops

Microsoft Entra ID for an Azure administrator

In one sentence
●○○

The phone book and the bouncer of Azure: it holds who exists (users, groups, apps, devices) and proves who they are before Azure RBAC decides what they may touch.

Practitioner
●●○

One tenant, many subscriptions:

- a subscription trusts exactly one tenant; moving it to another tenant deletes its role assignments
- the same user can be a member in one tenant and a guest in others
- Entra roles manage the directory; Azure roles (sheet 02) manage resources

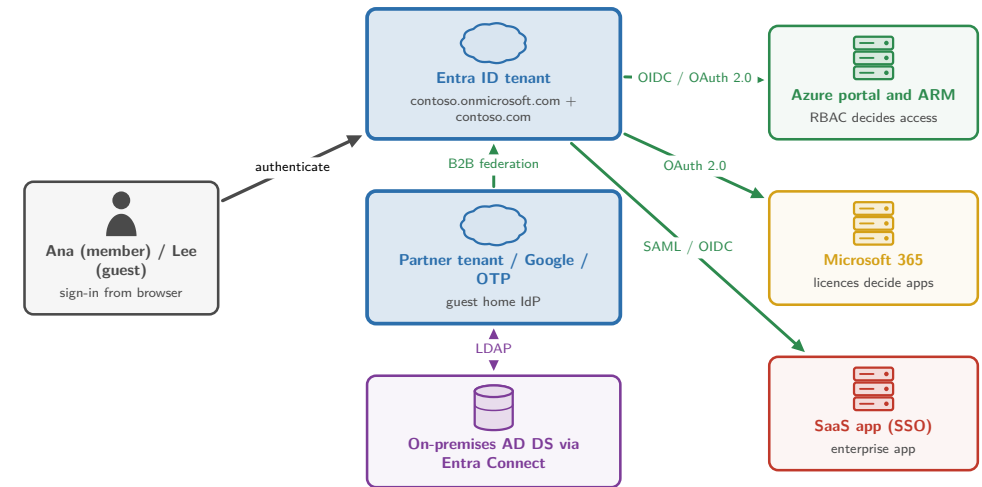
Expert
●●●

Editions decide features (as of 2026):

- Free: users, groups, basic SSO, security defaults
- P1: dynamic groups, group-based licensing, Conditional Access, SSPR writeback, Entra Connect Health
- P2: PIM, ID Protection (risk-based policies), access reviews
- Entra ID Governance add-on: lifecycle workflows, entitlement management at scale

Analogy

A company badge office: it prints and revokes badges (identity); each building's guard list (RBAC) decides which doors a badge opens.



One tenant authenticates members and guests for Azure, Microsoft 365 and SaaS apps

Object	Created by	Key attributes the exam uses	Gotcha
Member user	admin, Entra Connect sync, HR provisioning	UPN, usageLocation, accountEnabled, department, manager	no licence assignable until usageLocation (country) is set
Guest user	B2B invitation or self-service sign-up	UserType Guest, externalUserState (PendingAcceptance, Accepted)	default guest permissions are restricted; change in External collaboration settings
Security group	admin, user (if allowed), dynamic rule	membership type Assigned, Dynamic user, Dynamic device	a dynamic group cannot have manual members
Microsoft 365 group	admin, Teams, Outlook	owners, expiration policy, naming policy	cannot contain devices or other groups
Device	Entra registered, Entra joined, hybrid joined	trust type, compliance (Intune), owner	device settings cap how many devices a user may join (default 50)
Administrative unit	Privileged Role Administrator or Global Administrator	members (static or dynamic), scoped role assignments	restricted management AUs block even tenant-level admins

☀ Users and groups in practice

Command	What it does
az ad user create --display-name Ana --user-principal-name ana@contoso.com --password '<pw>' --force-change-password- next-sign-in true	create a cloud-only member user
az ad group create --display-name sg-app-readers --mail-nickname sg-app-readers	create a security group (assigned membership)
az ad group member add --group sg-app-readers --member-id <objectId>	add a member by object ID
az ad signed-in-user show --query id -o tsv	your own object ID (for role assignments)
Connect-MgGraph -Scopes User.ReadWrite. All,Group.ReadWrite.All	Graph PowerShell sign-in with consented scopes
New-MgUser -DisplayName Ana -UserPrincipalName ana@contoso.com -AccountEnabled -MailNickname ana -PasswordProfile @{Password='<pw>'}	same user in PowerShell
Update-MgUser -UserId ana@contoso.com -UsageLocation FR	set usage location before licensing
Restore-MgDirectoryDeletedItem -DirectoryObjectId <id>	restore a user or M365 group deleted less than 30 days ago

Which group type and membership?

Conditions	R1	R2	R3	R4
Needs mailbox, Teams, SharePoint	Y	N	N	N
Members follow HR attributes	--	Y	N	N
Holds devices	--	--	Y	N
Must be assignable to an Entra role	--	N	N	Y
Actions				
Microsoft 365 group	X			
Security group, dynamic user rule		X		
Security group, dynamic device rule			X	
Security group, assigned, isAssignableToRole				X
Notes	M365 groups can also be dynamic	P1 per member in scope	rule on device.* attributes	flag set at creation only; static membership

Dynamic membership rules (rule builder syntax)

```
# all enabled Sales users in France
(user.department -eq "Sales") -and
(user.country -eq "France") -and
(user.accountEnabled -eq true)
```

```
# all Windows devices
(device.deviceOSType -eq "Windows")
```

```
# direct reports of a manager (special rule)
Direct Reports for "<manager objectId>"
```

```
# every user (all users group)
user.objectId -ne null
```

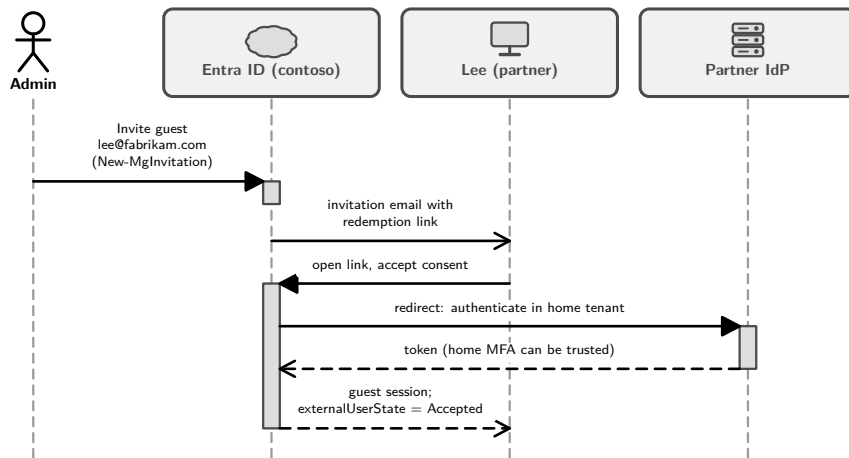
⚠ Dynamic groups are not instant

Membership is re-evaluated asynchronously after an attribute change: minutes in a small tenant, longer in a large one. Validate a rule with Validate Rules before saving; pausing processing is possible per group. You cannot add members by hand to a dynamic group, and a group cannot switch to dynamic if it is role-assignable.

- **Group owners** can manage membership without an admin role; set at least two owners per important group
- **Nested groups** a security group may contain security groups for RBAC, but group-based licensing and some apps ignore nested members
- **Deleted objects** users and M365 groups are soft-deleted for 30 days (restorable); security groups are deleted permanently
- **Bulk operations** portal Bulk create / invite / delete with a CSV template; async, check the bulk operation results page
- **Expiration policy** M365 groups only: owners must renew every N days or the group is soft-deleted

📄 Licences, external users and administrative units

- 1 **Set usageLocation on users** licence assignment fails with a usage location error otherwise
- 2 **Assign the licence to a security group** Entra admin centre > Billing > Licenses > product > Assign; choose service plans to disable
- 3 **Check for errors** group > Licenses: CountViolation (not enough seats), MutuallyExclusive Violation, DependencyViolation
- 4 **Remove direct assignments** users keep the licence while any path (direct or group) grants it
Group-based licensing, the order that works



B2B collaboration: the guest keeps its home credentials

External collaboration settings (tenant)	Cross-tenant access settings
guest user access: same as members / limited (default) / most restricted	inbound and outbound defaults, per-organisation overrides
who can invite: everyone incl. guests, members and admins, only admins with Guest Inviter, nobody	trust partner MFA and compliant-device claims (avoids double MFA)
collaboration restrictions: allow or deny list of domains	B2B direct connect: Teams shared channels without a guest object
email one-time passcode for guests without a supported IdP (on by default)	cross-tenant sync: provision users into a partner tenant automatically

Administrative unit — Scope for Entra roles: assign User Administrator or Helpdesk Administrator on AU 'Paris' and the admin manages only Paris users and groups. Membership can be dynamic (P1).

Restricted management AU — An AU whose members can only be changed by admins scoped to that AU, protecting executives' accounts from tenant-wide User Administrators.

EXAM TIP

Trap: 'the helpdesk of the Paris office must reset passwords only for Paris users' → administrative unit + Helpdesk Administrator scoped to the AU, not an Azure RBAC role and not a separate tenant. 'Licence assignment fails for new users' → usageLocation is empty.

Self-service password reset and devices

SSPR setting	Options	Recommended
Enabled for	None, Selected (one group), All	pilot group first, then All
Methods required	1 or 2	2 for admins (enforced by default for admin roles)

Methods available	Authenticator app (notification or code), SMS, office or mobile call, email, security questions	Authenticator first; security questions only for users, never admins
Registration	require users to register at sign-in; re-confirm every N days (default 180)	on, combined MFA + SSPR registration
Notifications	notify users on reset; notify all admins when another admin resets	both on
Password writeback	via Entra Connect Sync or Cloud Sync to on-premises AD	on for hybrid users (P1)

SSPR

Self-service password reset
user resets own password after verifying methods
NOT
MFA: proves identity at every sign-in

AU

Administrative unit
scopes Entra admin roles to a subset of objects
NOT
management group: scopes Azure resources

UPN

User principal name
sign-in name, verified domain suffix
NOT
mail address (can differ)

B2B

Business-to-business collaboration
external users as guests in your tenant
NOT
B2C / External ID for customers: consumer identities in a separate tenant

PIM

Privileged Identity Management
just-in-time, time-bound, approved role activation (P2)
NOT
PAM on-premises jump servers

MDM

Mobile device management
Intune enrolment of Entra-joined devices
NOT
MAM: app protection without device enrolment

	Entra registered	Recommended Entra joined	Hybrid joined
Device owner	personal (BYOD)	organisation	organisation
Sign-in account	local or Microsoft account + work account added	Entra ID work account	AD DS account synced to Entra
Typical OS	Windows, iOS, Android, macOS	Windows 10/11, Windows Server 2019+ VMs in Azure	Windows
Needs on-premises AD	✗	✗	yes (Entra Connect or Cloud Sync)

💡 Sign in to Azure VMs with Entra ID

Install the AADLoginForWindows (or AADSSHLoginForLinux) VM extension, then grant **Virtual Machine Administrator Login** or **Virtual Machine User Login** on the VM: the RBAC role, not local accounts, decides who logs on.

Recap and self-test

MYTH

✗ Owner on a subscription can create Entra users

✗ Deleting a security group can be undone for 30 days

✗ Guests need a new password in my tenant

✗ Dynamic groups are part of the Free edition

FACT

✓ **Azure roles do not grant directory rights**
Creating users needs an Entra role such as User Administrator; the two role systems are separate.

✓ **Only users and Microsoft 365 groups are soft-deleted**
Security groups are hard-deleted; recreate them and their role assignments.

✓ **Guests authenticate at their home identity provider**
Microsoft Entra, Microsoft account, Google, SAML/WS-Fed IdP or email one-time passcode.

✓ **Dynamic membership needs Entra ID P1**
Licence every user who is a member of a dynamic group.

PROBLEM How many Entra ID P1 licences does the dynamic group plan need?

GIVEN

- Tenant of 1,200 users; 300 in Sales, 150 in Finance, 40 users in both via a project attribute
- Dynamic groups planned: Sales users, Finance users
- Licensing rule: every unique user who is a member of a dynamic group needs P1

1 Add the two group sizes

$300 + 150 = 450$ memberships

Why: a user can be counted in both groups

2 Remove double counting

$450 - 40 = 410$ unique users

Why: a licence is per user, not per membership

3 Compare with the tenant

410 of 1,200 = 34 %

Why: if Conditional Access or SSPR writeback is also planned for all, licence everyone instead

ANSWER 410 P1 licences (or 1,200 if other P1 features target all users)

CHECK ✓ $410 = |\text{Sales} \cup \text{Finance}| = 300 + 150 - 40$

Key takeaways

01

One tenant, two role systems

Entra roles for the directory, Azure RBAC for resources

02

usageLocation before licences

group-based licensing for scale

03

Dynamic groups need P1

no manual members, asynchronous updates

04

Guests keep home credentials

control invitations and cross-tenant trust

05

AUs scope admin roles

helpdesk per office or country

Q1 A new user cannot receive a Microsoft 365 licence. First thing to check?

A The usageLocation attribute: licences require a country; set it with Update-MgUser -UsageLocation.

Q2 Which group type can hold devices?

A A security group (assigned or dynamic device rule); Microsoft 365 groups hold users only.

Q3 Which Entra edition is required for dynamic groups and group-based licensing?

A Microsoft Entra ID P1 (or P2, which includes P1).

Q4 How long can a deleted user be restored?

A 30 days from the Deleted users blade (soft delete), then it is purged.

Q5 Restrict a helpdesk admin to the users of one country?

A Create an administrative unit for that country and assign Helpdesk Administrator scoped to it.

Q6 Which setting stops members from inviting guests?

A External collaboration settings > Guest invite restrictions: only users assigned to specific admin roles (Guest Inviter).

Q7 Which property shows that a guest has not accepted the invitation yet?

A externalUserState = PendingAcceptance (Accepted after redemption).

Q8 Hybrid users reset their password with SSPR but on-premises logon fails. Missing piece?

A Password writeback in Entra Connect Sync or Cloud Sync (P1).

Q9 Which PowerShell module replaces AzureAD and MSOnline?

A Microsoft Graph PowerShell SDK (`Microsoft.Graph`, `Connect-MgGraph`).

Q10 A group must be assignable to Entra roles. When do you decide?

A At creation (`isAssignableToRole = true`); it cannot be changed later and membership must be assigned.