

Module-2-Implement and manage external ident ☐

סוגי משתמשים והיחסים בינם :

<https://learn.microsoft.com/en-us/entra/external-id/user-properties>

UserType ב- Entra	מתי משתמשים?	רמת גישה	מקור חשבון	סוג משתמש
Guest	B2B Collaboration שותפים, משתמשים חיצוניים	גישה ברמת Guest מוגבלת	חשבון מארגון חיצוני או IdP חיצוני Google/Facebook/(Ent) ר אחר)	External Guest
Member	תוך組織 של ארגונים מרובי-טננטים (multi-tenant organization) שבו משתמשים נחשבים "חלק מהארגון הגדל"	רמת גישה של Member רחבה	חשבון מארגון חיצוני או IdP חיצוני	External Member
Guest	תצורה מיושנת — לפני B2B. מומלץ להחילוף ל-B2B כדי לשימושו בחשבון האמייתי שליהם	גישה ברמת Guest	חשבון פנימי שנוצר ידנית בעור ספק/שותף (בעבר, לפני B2B)	Internal Guest
Member	המשתמשים הפנימיים / העובדים של הארגון	רמת גישה של Member מלאת	עובד אמייתי של הארגון, מחובר לשירות ב-Entra	Internal Member

הגדרות ברירת מחדל :

External Identities | External collaboration settings

Guest user access

- Guest users have the same access as members (most inclusive)
- Guest users have limited access to properties and memberships of directory objects
- Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)

Guest invite settings

- Anyone in the organization can invite guest users including guests and non-admins (most inclusive)
- Member users and users assigned to specific admin roles can invite guest users including guests with member permissions
- Only users assigned to specific admin roles can invite guest users
- No one in the organization can invite guest users including admins (most restrictive)

Enable guest self-service sign up via user flows

External user leave settings

Allow external users to remove themselves from your organization (recommended)

Collaboration restrictions

Microsoft 365 Member Guest

לשים לב שיש 7 הרשאות שונות ב-365 Microsoft 365 Member Guest

תחום	Guest	Member
Microsoft 365 Apps	רק אם הוקצתה הרשאה מפורשת לאפליקציה/קובוצה	מלא
Teams	יכול להצטרף לצוות/עורך שאליו הזמן	يُوزع قوائم، مصطفى حوضي
SharePoint	גישה רק לאתרים / ספריות / קבצים שהורשו לו בມפורש	גישה לפיקוח היררכית אתר / קבוצה
OneDrive	לא מקבל OneDrive משלה	כן
Mailbox (Exchange Online)	אין תיבת דואר	כן
Planner / To Do	לא	כן

Member	Guest	תחום
כן	רק אם הוקצו לו רשיות והרשות	PowerApps / Power Automate
ראוה כמעט כלום — רק את עצמו ואת קבוצות שהוא חבר בהן (בהתאם ל-GAR)	ראוה את רוב האובייקטים לפי Tenant settings	Azure AD Directory Read
כן	לא יכול לרשום מכשירים	Join Devices / MDM
כן	לא (הסימה מנהלת בטענת שלו)	SSPR (אייפוס סיסמה)
דרך ID Entra של הארגון	מתבצע דרך הטענת המקורי שלו	MFA
מלא	מואוד מוגבל, רק עם authorities שהאפשרות מאפשרת	גישה ל-API
כן	כן, מופעלים עליו CA של הארגון המארח	עמידה במדיניות Conditional Access