

## Module-2-Implement and manage external ident □

סוגי משתמשים והיחסים בניהם :

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

סוג משתמש	מקור חשבון	רמת גישה	מתי משתמשים?	UserType ב- Entra
External Guest	חשבון מארגון חיצוני או IdP חיצוני (Google/Facebook/Ent ra אחר)	גישה ברמת Guest – מוגבלת	B2B Collaboration רגילה: ספקים, שותפים, משתתפים חיצוניים	Guest
External Member	חשבון מארגון חיצוני או IdP חיצוני	רמת גישה של Member – רחבה	תרחיש של ארגונים מרובי-טננטים (multi-tenant organization) שבהם משתמשים נחשבים "חלק מהארגון הגדול"	Member
Internal Guest	חשבון פנימי שנוצר ידנית עבור ספק/שותף (בעבר, לפני B2B)	גישה ברמת Guest	תצורה מיושנת — לפני B2B. מומלץ להחליף ל-B2B כדי שישתמשו בחשבון האמיתי שלהם	Guest
Internal Member	עובד אמיתי של הארגון, מחובר ישירות ב-Entra	רמת גישה של Member מלאה	המשתמשים הפנימיים / העובדים של הארגון	Member

הגדרות ברירת מחדל :

Search

Save Discard

Email one-time passcode for guests has been moved to All Identity Providers. →

Overview

Cross-tenant access settings

All identity providers

External collaboration settings

Diagnose and solve problems

Self-service sign up

Custom user attributes

All API connectors

Custom authentication extensions

User flows

Subscriptions

Linked subscriptions

Lifecycle management

Terms of use

Access reviews

Troubleshooting + Support

New support request

Guest user access

Guest user access restrictions ⓘ

Learn more

☐ 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

Guest invite restrictions ⓘ

Learn more

☒ 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 ⓘ

Learn more

Yes No

External user leave settings

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

Learn more

Yes No

Collaboration restrictions

☒ Cross-tenant access settings are also evaluated when sending an invitation to determine whether the invite should be allowed or blocked. [Learn more.](#)

☒ Allow invitations to be sent to any domain (most inclusive)

## לשים לב שיש ל GUESTS הרשאות שונות ב -365 Guest לעומת Member ב-Microsoft 365

תחום	Guest	Member
גישה ל-Microsoft 365 Apps	רק אם הוקצתה הרשאה מפורשת לאפליקציה/קבוצה	מלא
Teams	יכול להצטרף לצוות/ערוץ שאליו הוזמן	יוצר צוותים, מצטרף חופשי
SharePoint	גישה רק לאתרים / ספריות / קבצים שהורשו לו במפורש	גישה לפי היררכיית אתר / קבוצה
OneDrive	לא מקבל OneDrive משלו	כן
Mailbox (Exchange Online)	אין תיבת דואר	כן
Planner / To Do	לא	כן

תחום	Guest	Member
<b>PowerApps / Power Automate</b>	רק אם הוקצו לו רשיונות והרשאות	כן
<b>Azure AD Directory Read</b>	רואה כמעט כלום — רק את עצמו ואת קבוצות שהוא חבר בהן (בהתאם ל-GAR)	רואה את רוב האובייקטים לפי Tenant settings
<b>Join Devices / MDM</b>	לא יכול לרשום מכשירים	כן
<b>SSPR (איפוס סיסמה)</b>	לא (הסיסמה מנוהלת בטננט שלו)	כן
<b>MFA</b>	מתבצע דרך הטננט המקורי שלו	דרך Entra ID של הארגון
<b>גישה ל-Graph API</b>	מאוד מוגבל, רק עם Delegated permissions שהאפליקציה מאפשרת	מלא
<b>עמידה במדיניות Conditional Access</b>	כן, מופעלים עליו CA של הארגון המארח	כן