

MODULE-2-Implement an identity management □

קישור למודול :

[/https://learn.microsoft.com/en-us/training/paths/implement-identity-management-solution](https://learn.microsoft.com/en-us/training/paths/implement-identity-management-solution)

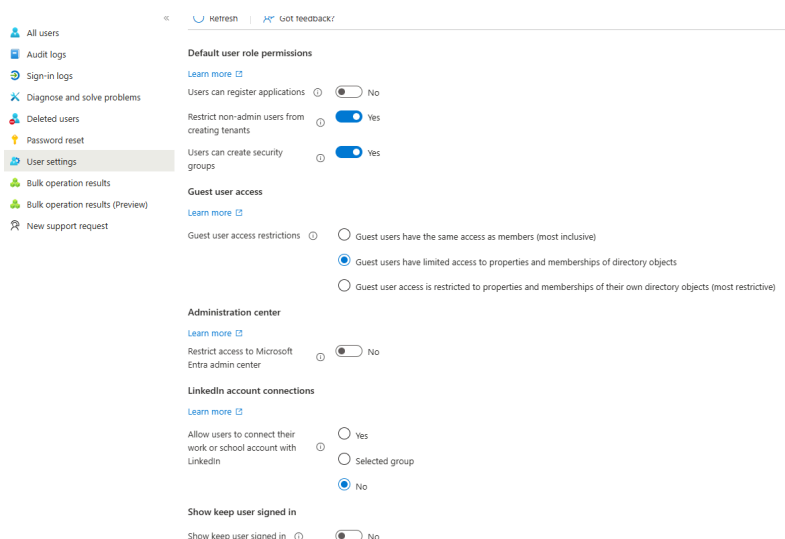
הסדר במצגת שונה :

חשוב להכיר את ההגדרות הכלליות ל TENNAT :

<https://learn.microsoft.com/en-us/training/modules/implement-initial-configuration-of-azure-active-directory/8-configure-tenant-wide-options?ns-enrollment-type=learningpath&ns-enrollment-id=learn.www.implement-identity-management-solution>

התחלנו עם זהויות : <https://learn.microsoft.com/en-us/training/modules/create-configure-manage-/identities>

חשוב להכיר סוגי משתמשים : ולהבין את הגדרות ברירת המחדל עבור משתמשים



סוגי משתמשים ב-Entra ID

מאפיינים	הסבר	סוג משתמש
מנוהל בענן בלבד	נוצר ישירות ב-Entra	Cloud-only

סוג משתמש	הסבר	מאפיינים
Synced (Hybrid)	מגיע מ-AD On-Prem דרך Cloud / Entra Connect Sync	Master Attributes ב-On-Prem
Guest (B2B)	משתמש חיצוני מארגון אחר	בעל סוג UserType=Guest
External Member	משתמש B2B שנראה כרגיל (תצורה מתקדמת) -	דומה ל-Member

Property / Concept	Member	Guest
UserType	Member	Guest
Owner of identity	מנוהל אצלך (ב-tenant שלך)	מנוהל אצל הארגון/IdP המקורי
UPN	בד"כ user@yourdomain	בד"כ user@otherdomain או onmicrosoft.com. אוטומטי
Authentication	מנוהל אצלך (MFA, SSPR, Passkeys, CBA)	לפי IdP של המשתמש (Microsoft/Google/ADFS)
ExternalUserState	לא קיים	Pending / Accepted
ExternalTenantId	לא קיים	מצביע על ה-Tenant של המשתמש
CreationType	LocalAccount / Synchronized	Invitation / External
Editable Attributes	ניתן לערוך כמעט הכל	חלק מהשדות נעולים כי מגיעים מהטננט המקורי
Group Membership	מלא, כולל Dynamic Groups לפי User Attributes	מוגבל – משתנים של Guest לא תמיד זמינים ל-Dynamic
Directory Role Assignment	אפשר לתת Roles	אפשר לתת Roles
Access Reviews	לא חובה	נפוץ מאוד – מנגנון ניהול מחזור חיים
Lifecycle (Soft Delete)	מחיקה → 30 יום שחזור	אותו דבר
Login Frequency	מנוהל אצלך	תלוי ב-IdP שלהם
Licensing	ניתן להקצות רשיונות	ניתן להקצות, אך לרוב לא נהוג

Guest	Member	Property / Concept
מבוסס דומיין של המשתמש	לא קיים	Home Realm Discovery
מתבצע בטננט של המשתמש	מנוהל ב-Entra של הארגון שלך	MFA
לא רלוונטי — סיסמה לא אצלך	זמין (אם מופעל בארגון)	SSPR
מלאים, אבל Authentication Details מגיעים מה-IdP של המשתמש	מלאים	Sign-in Logs
בענן המקורי של המשתמש	בענן שלך	User Principal Location

קבוצות :

פרמטר	Security Group	Microsoft 365 Group (Unified)	Distribution List	Mail-Enabled Security Group
מטרה	הרשאות, RBAC, גישה לאפליקציות	קולבורציה: Teams, SharePoint, Planner	דיוור בלבד	הרשאות + דיוור
Email Enabled	לא	כן	כן	כן
מתאים להרשאות	כן	לא	לא	כן
משאבים שיוצר	אין	כן — Teams, SharePoint, Planner, Mailbox	אין	אין
Dynamic Membership	נתמך	נתמך	לא נתמך	לא נתמך
Nesting (קיבון)	נתמך	לא נתמך	לא נתמך	נתמך
Role Assignment	נתמך	לא נתמך	לא נתמך	נתמך
Group-based Licensing	נתמך	נתמך	לא נתמך	נתמך
Guests Allowed	כן	כן	כן	כן

פרמטר	Security Group	Microsoft 365 Group (Unified)	Distribution List	Mail-Enabled Security Group
Creation Location	Cloud או AD	Cloud בלבד	AD או Cloud	Cloud או AD
Sync from AD	נתמך	לא נתמך	נתמך	נתמך
כלי ניהול	Entra / AD / Graph	Entra / M365 Admin / Graph	Exchange / AD	Exchange / AD
הערות Nesting על	עובד גם בהרשאות וגם בגישה לאפליקציות	לא תומך קיבול כלל	לא תומך קיבול	תומך בקיבול מלא
תרחיש שימוש	הרשאות מערכתיות ואפליקציות	צוותים ופרויקטים	רשימות מייל בלבד	הרשאות + כתובת דיוור

להכיר מאפייני קבוצות והגדרות כלליות לקבוצות + קבוצות דינמיות

Groups | General

« Save Discard Got feedback?

Self Service Group Management

Owners can manage group membership requests in My Groups [?](#) Yes No

Restrict user ability to access groups features in My Groups. Group and User Admin will have read-only access when the value of this setting is 'Yes'. [?](#) Yes No

Information Restrict user ability to access groups features in My Groups' setting - originally planned for June 2024 - deferred. New date will be shared later this year. [Learn more.](#)

Security Groups

Users can create security groups in Azure portals, API or PowerShell Yes No

Microsoft 365 Groups

Users can create Microsoft 365 groups in Azure portals, API or PowerShell Yes No

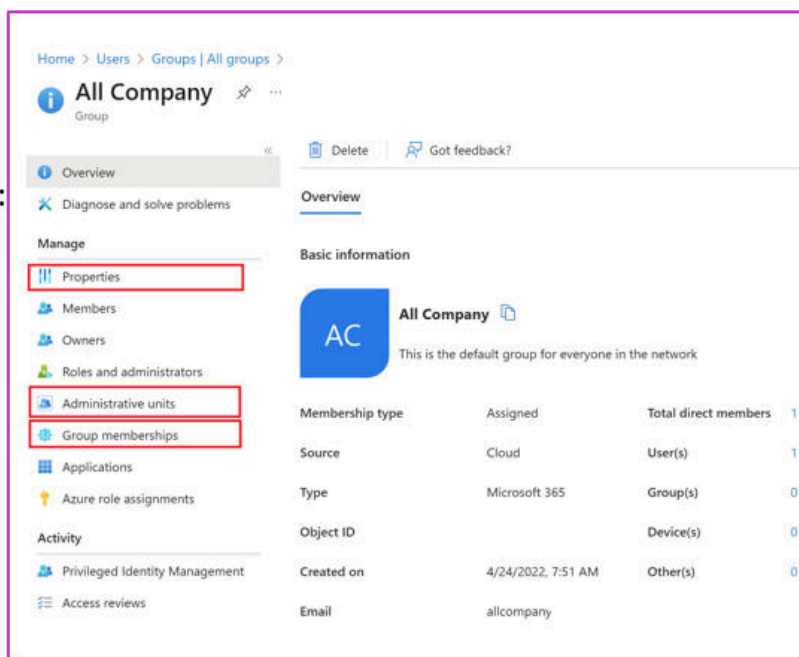
Directory-wide Groups

[Learn more about how to create "Direct reports", "All users", or "All devices" groups in other properties and common rules](#)

Group configuration options

Some configurable group settings:

- Properties
- Administrative units
- Group membership
- Roles and administrators



- **CUSTOM ATTRIBUTES** יצירת

<https://learn.microsoft.com/en-us/training/modules/create-configure-manage-identities/11-create-custom-security-attributes>

היכולת שלנו להשתמש בהם בקבוצות דינמיות או עבור ניהול משתמשים

קישור להסבר על ROLES לקבוצה :

<https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/groups-concept#group-assigned-roles-are-not-visible-in-the-groups-blade>

: **DEVICES** סוגי

<https://learn.microsoft.com/en-us/training/modules/create-configure-manage-identities/7-configure-manage-device-registration>

פרמטר	Azure AD Joined	Hybrid Azure AD Joined	Azure AD Registered	Intune Managed	MAM Only
בעלות	ארגונית	ארגונית	אישית	ארגונית/אישית	אישית
חשבון התחברות	Entra ID	Domain AD	חשבון עבודה בלבד	תלוי Join	חשבון באפליקציה

פרמטר	Azure AD Joined	Hybrid Azure AD Joined	Azure AD Registered	Intune Managed	MAM Only
יוצר מכשיר	ענן בלבד	AD + Sync	המשתמש	Intune MDM	אפליקציה בלבד
נראות ב-Entra	כן	כן	כן	כן	לא כ-Device
תמיכה ב-Conditional Access	גבוהה	גבוהה	בינונית	מלאה (Compliance)	באמצעות App Protection בלבד
מתאים ל-Intune MDM	כן	כן	כן	כן	לא
SSO	מלא	מלא	חלקי	מלא	מוגבל
תרחיש	Cloud-first	Hybrid	BYOD	ארגוני מנוהל	BYOD לא מנוהל

חשוב להבין שאת הרישוי משנים בפורטל 365 - המלצה לעבוד עם קבוצות רישוי

<https://learn.microsoft.com/en-us/training/modules/create-configure-manage-identities/8-manage-licenses>

Administrative Units

<https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/administrative-units>

נושא	הסבר
מה זה?	חלוקה ליחידות ניהול מבודדות בתוך Entra ID
למה?	לתת הרשאות ניהול מוגבלות ולא טננט מלא
מה ניתן להכניס?	Users, Groups, Devices
למי מתאים?	ארגונים גדולים, מבוזרים, אוניברסיטאות, בנקים
איך נותנים הרשאות?	Role Assignment עם Scope = Administrative Unit
רמת אבטחה	גבוהה — מונע זליגת הרשאות בין מחלקות

נושא	הסבר
שילוב עם PIM	נתמך — JIT רק על ה-AU
מגבלות	חלק מהרולים אינם "scopable" ל-AU