

# 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)

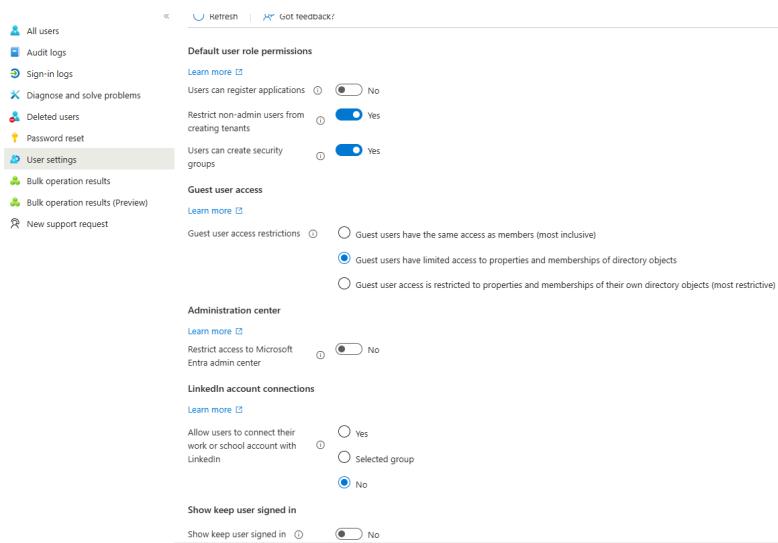
הסדר במצגת שונה :

חשוב להכיר את הגדרות 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.wwl.implement-identity-management-solution>

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

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



## סוגי משתמשים ב-ID Entra

מאפיינים	הסבר	סוג משתמש
מנהל בען בלבד	ນutzer יישור ב-ID	Cloud-only

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

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

<b>Guest</b>	<b>Member</b>	<b>Property / Concept</b>
mboso דומיין של המשתמש	לא קיימ	<b>Home Realm Discovery</b>
מתבצע בטננט של המשתמש	מנהל ב-Entra של הארגון שלו	<b>MFA</b>
לא רלוונטי — סיסמה לא אצלך	זמן (אם מופעל בארגון)	<b>SSPR</b>
מלאים, אבל Authentication Details מגייעים מה-PId של המשתמש	מלאים	<b>Sign-in Logs</b>
בען המקורי של המשתמש	בען שלו	<b>User Principal Location</b>

**קבעות :**

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

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

להכיר מאפייני קבוצות והגדרות כלליות לקבוצות + קבוצות דינמיות

The screenshot displays the 'Groups | General' settings page. On the left, a sidebar lists navigation options: Overview, All groups, Deleted groups, Diagnose and solve problems, Settings (with General selected), Expiration, Naming policy, Activity (with Privileged Identity Management, Access reviews, Audit logs, Bulk operation results, Troubleshooting + Support, and New support request listed), and Help. The main content area contains several configuration sections:

- Self Service Group Management:** Owners can manage group membership. Options: Yes (selected) or No.
- Restrict user ability to access groups:** Restricts users from accessing group features in My Groups. Options: Yes (selected) or No.
- Security Groups:** Users can create security groups in Azure portals, API or PowerShell. Options: Yes (selected) or No.
- Microsoft 365 Groups:** Users can create Microsoft 365 groups in Azure portals, API or PowerShell. Options: Yes (selected) or No.
- Directory-wide Groups:** A note states: "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

The screenshot shows the 'All Company' group page in the Azure portal. At the top, there are navigation links: Home > Users > Groups | All groups >. Below that is the group name 'All Company' with a blue icon. To the right are 'Delete' and 'Got feedback?' buttons. The main area has tabs: Overview (which is selected), Basic information, and Manage. Under Manage, several options are listed: Properties (highlighted with a red box), Members, Owners, Roles and administrators, Administrative units (highlighted with a red box), Group memberships (highlighted with a red box), Applications, Azure role assignments, Activity, Privileged Identity Management, and Access reviews. On the right side, there's a summary card for 'All Company' with a blue background and white text. It says 'This is the default group for everyone in the network'. Below the card is a table with details like Membership type (Assigned), Source (Cloud), Type (Microsoft 365), Object ID, Created on (4/24/2022, 7:51 AM), and Email (allcompany).

## - CUSTOM ATTRIBUTES יצירת 属性

<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 לקובץ :

<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>

MAM Only	Intune Managed	Azure AD Registered	Hybrid Azure AD Joined	Azure AD Joined	פרמטר
אישית	ארגוני/אישי	ארגוני	ארגוני	ארגוני	בעלויות
חשבון באפליקציה	תלי Join	עובד	חשבון בלבד	Domain AD	Envelope ID

MAM Only	Intune Managed	Azure AD Registered	Hybrid Azure AD Joined	Azure AD Joined	פרמטר
אפליקציה בלבד	Intune MDM	המשתמש	AD + Sync	ען בלבד	ווצר מכשיר
לא Device	כן	כן	כן	כן	גראות ב-Entra
App Protection בלבד באמצעות Compliant	מלאה (t)	בינוי	גבוהה	גבוהה	תמיכה ב- Conditional Access
לא	כן	כן	כן	כן	מתאים ל-Intune MDM
מוגבל	מלא	חלקי	מלא	מלא	SSO
BYOD לא מנהל	ארגוני מנהל	BYOD	Hybrid	Cloud-first	תרחיש

חשוב להבין שאות הרישיון משנים בפורטל 365 - המלצה לעבוד עם קבוצות רישיון

<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>

הסבר	נושא
חלוקת ליחידות ניהול מבודדות בתוך ID	מה זה?
لتת הרשות ניהול מוגבלות ולא טננט מלא	למה?
Users, Groups, Devices	מה ניתן להכין?
ארגוני גדולים, מבזרים, אוניברסיטאות, בנקים	למי מתאים?
Scope = Administrative Unit Role Assignment	איך נקבעים הרשותות?
גבוהה — מונע זליגת הרשותות בין מחלקות	רמת אבטחה

נושא	הסביר
שילוב עם MIM	נתמך — DOJ רק על AU-AU
מגבלות	חלק מהרולים אינם "scopable" ל-AU