Managing Identities in Entra ID

Key Terms

- Azure Tenant
  - A dedicated and trusted instance of Entra ID. Automatically created when an organization signs up for MS Cloud Services.
- Single Tenant
  - Azure Tenants that access other services in a dedicated environment.
- Multitenant
  - Azure tenants that access other services in a shared environment, across multiple organizations.
-

ENTRA ID - Licenses and Features

Licenses

FREE

Provides user and group management, on prem directory synchronization and cloud resources, basic reports, self-service password change for cloud users, and SSO across Azure, MS 365, and other SaaS applications.

P1 - Everything in Free plus:

Hybrid user access both on-prem and cloud resources, advanced administration such as dynamic groups, self-service group management, MS Identity Manager, and Cloud-write back capabilities.

P2 - Everything in P1 plus:

ENTRA ID Protection for risk-based conditional access to apps, company data, and Privileged Identity Management. PIM allows for discovering, restricting, and monitoring administrators and their access to resources - "just in time" access when needed.

Pay as You Go

Self-Explanatory. Pay for features and services with various factors being used to determine cost.

User Types & Creation

Always try and enforce the concept of least privilege: Users should only have the level of access required for them to perform their work tasks. Nothing more.

User Types

Internal Member

- These users are most likely full time employees in your organization.

Internal Guest

- These users have access in your tenant but have guest level privileges. Possible they were created within your tenant prior to the availability of a B2B collaboration.

External Members

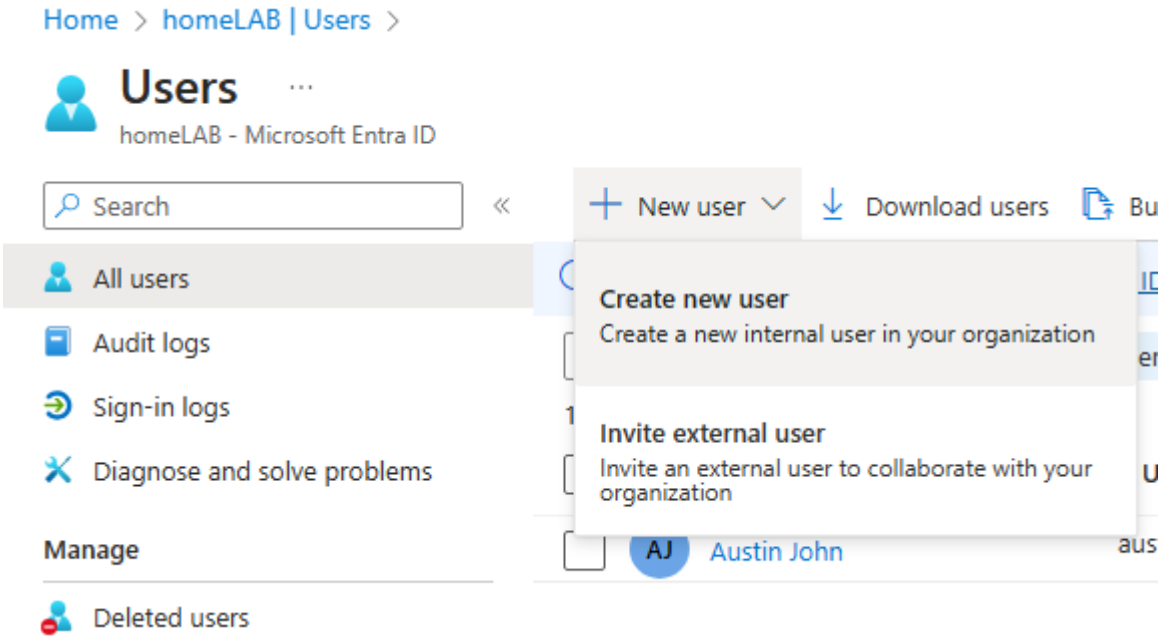
- These users authenticate using an external account, but have member access to your tenant. These are common in multitenant organizations.

External Guest

- These users are true guest of your tenant who authenticate using an external method and who have guest level privileges.

User Creation

1. Navigate to Entra ID ---> Users ---> All Users
2. Select the +*New User* icon and select *Create New User*

1. 
Home > homeLAB | Users >
Users
homeLAB - Microsoft Entra ID
Search
New user
Download users
Bu
All users
Audit logs
Sign-in logs
Diagnose and solve problems
Manage
Deleted users
Create new user
Create a new internal user in your organization
Invite external user
Invite an external user to collaborate with your organization
AJ
Austin John

Groups, Memberships, Access Management

Group Types

Security Groups

- Used to manage user and computer access to shared resources
- Can consist of:
  - Users
  - Devices
  - Service Principles
  - Nested Groups
- SGs are owned by Users and/or Service Principals

Microsoft 365 Group

- Provides collaboration opportunities between group members, providing access to shared services:
  - Mailboxes
  - Calendars
  - Files
  - SharePoint sites
- Also allows for users outside of the organization to be granted access. Members of an MS 365 Group can only be Users.
- MS365 groups are owned by Users and/or Service Principals

Membership Types

Assigned

- Allows you to add specific users as members of a group and have unique permissions

Dynamic User

- Allows use of dynamic membership rules to automatically add or remove members
- If a User's attributes change, the system will determine if the new attributes meet the Dynamic Group rules for the directory

Dynamic Device

- Allows use of dynamic group rules to automatically add or remove devices
- If a device's attributes change, the system looks at the dynamic group rules and determines if the device meets requirements for the directory

Ways to Assign Access Rights

Direct Assignment

- Resource owner directly assigns the user to the resource

Group Assignment

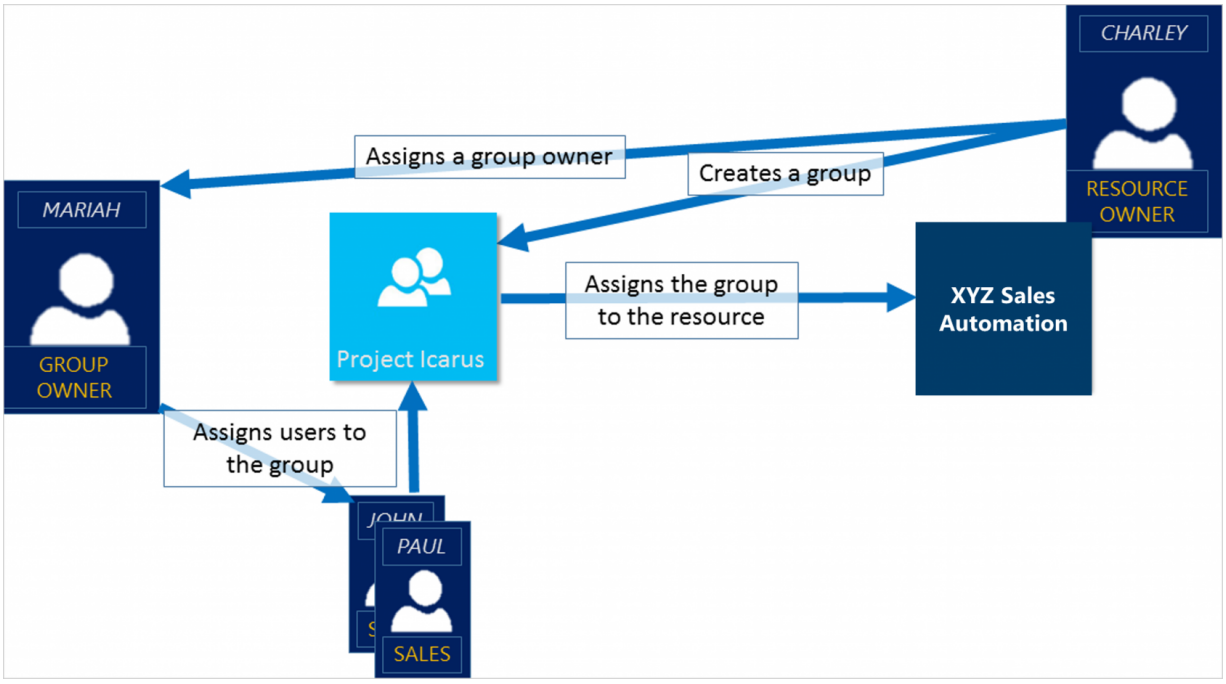
- Resource owner assigns a Microsoft Entra group to the resource, which automatically gives all group members access to the resource
- Group membership is managed by both the group owner and the resource owner

Rule-Based Assignment

- Resource owner creates a group and uses a rule to define which users are assigned to a specific resource
- Rule is based on attirbuted that are assigned to individual users
- Resource owner manages the rule, determining which attributes and values are required to gain access

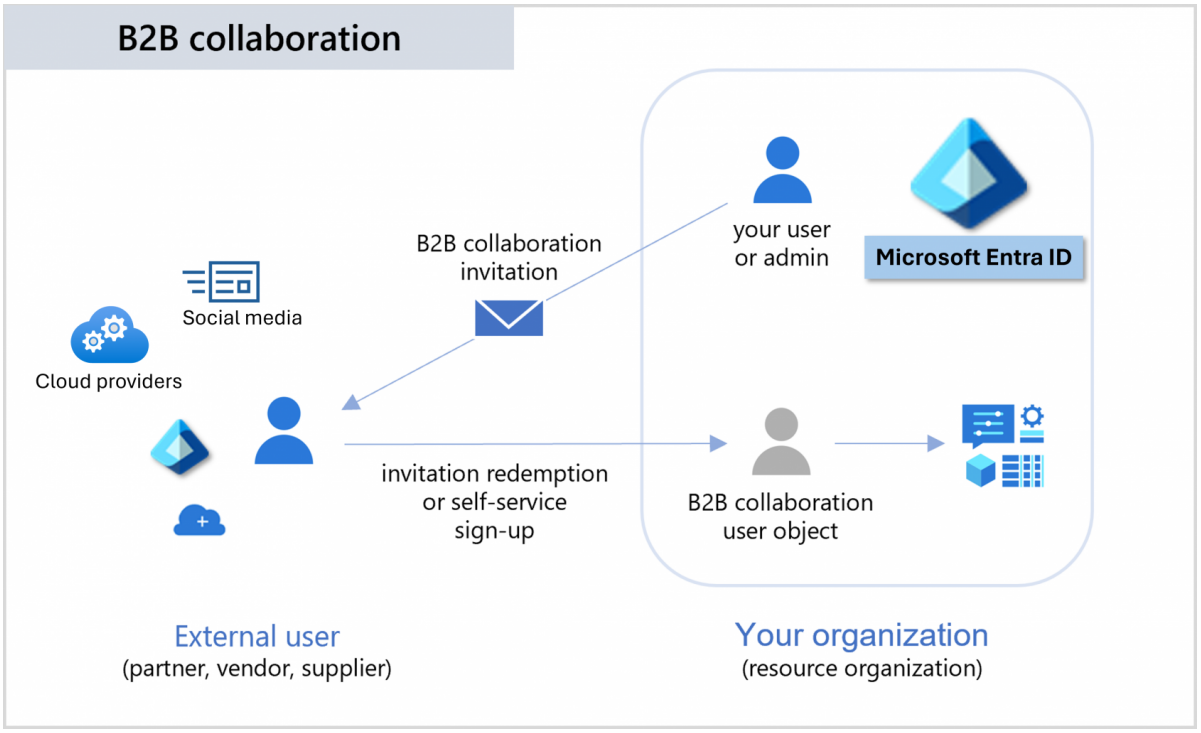
External Authority Assignment

- Access comes from an external resource, such as an on-premises directory or a SaaS application
- In this situation, the resource owner assigns a groupo to provide access to the resource, and the external source manages the group members



When to use External Identities

B2B collaboration is the most common use of this method. It allows you to securely share company applications and services with external users, while maintaining control over your own corporate data.



MS Entra B2B

Entra B2B allows fore partners to use their own identity management solution

- Results in zero overhead for your organization
- Guest users can sign in to your apps and services with their own work, school, or social identities
- User type for B2B collaboration is typically set to "Guest"