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

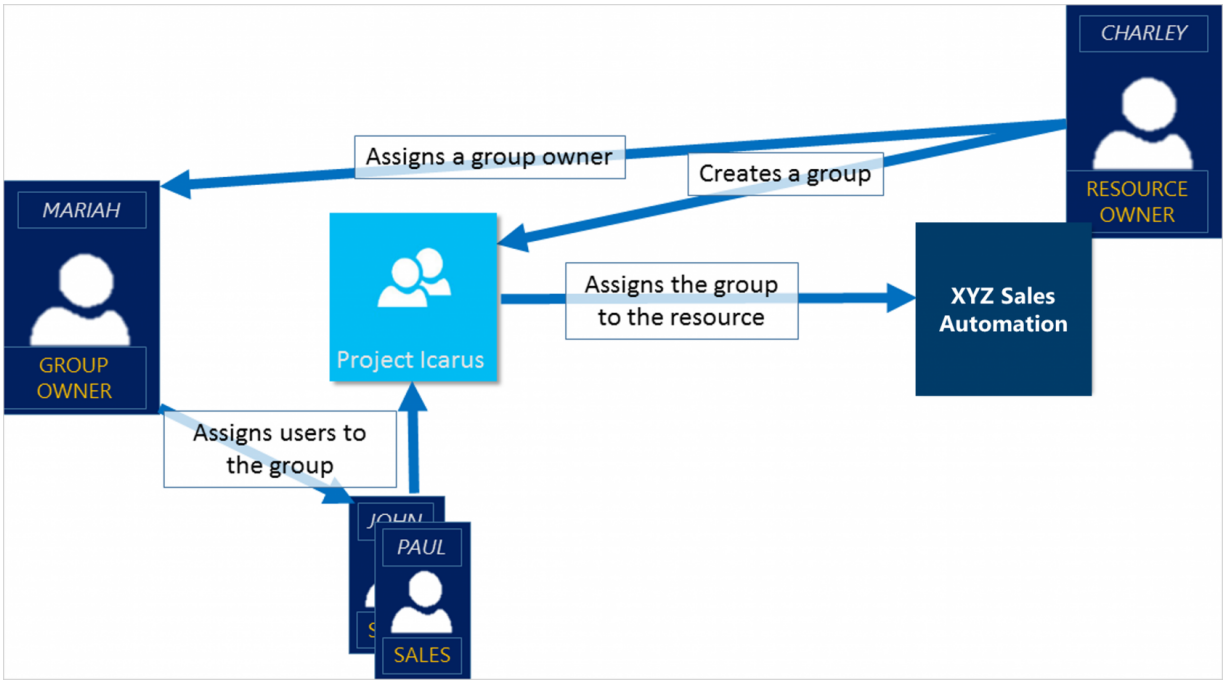
- Resource owner assigns a Microsoft Entra group to the resource, which automatically gives all group members access to the resource
- Group membership is managed by both the group owner and the resource owner

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

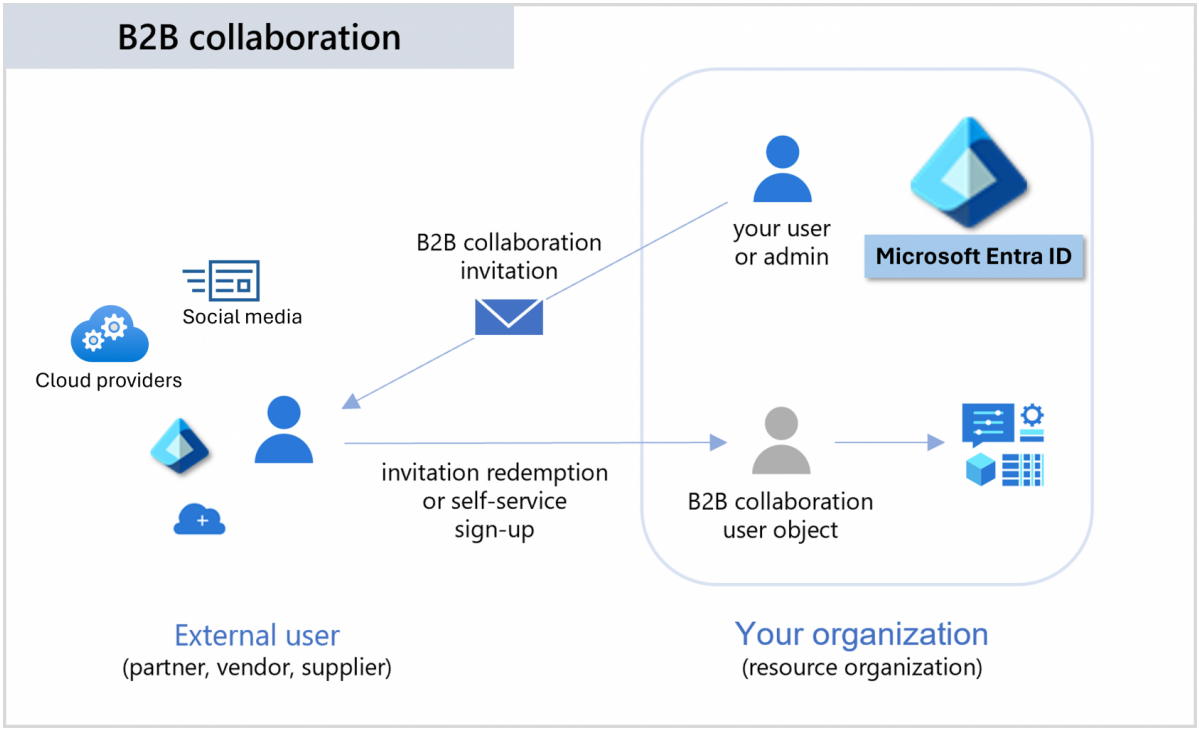
External Authority Assignment

- 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"

Revision #3
Created 2024-03-30 00:53:52 UTC by Austin
Updated 2024-04-02 00:36:45 UTC by Austin