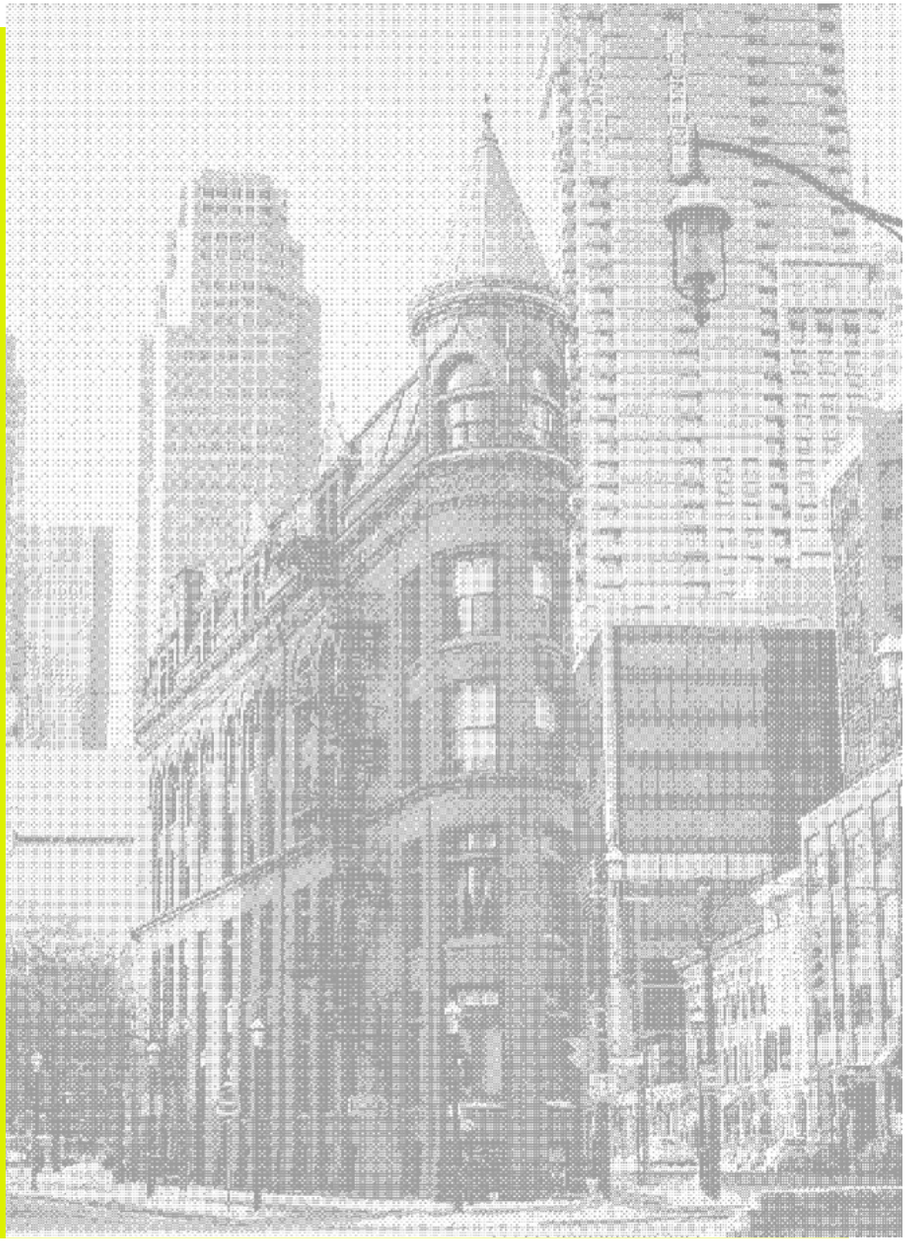


Azure Administrator Associate

AZ 104

Presenter

Mohammed Arif, PhD

GenAI Architect & Data Scientist

Mohammed Arif has more than eighteen (18+) years of working experience in Information Communication and Technology (ICT) industry. The highlights of his career are more than nine (9) years of holding various senior management and/or C-Level and had six (6) years of international ICT consultancy exposure in various countries (APAC and Australia), specially on Big Data, Data Engineering, Machine Learning and AI arena.

He is also Certified Trainer for Microsoft & Cloudera.

/arifmazumder

Microsoft

AZ-104
Administer Identity

© Copyright Microsoft Corporation. All rights reserved.

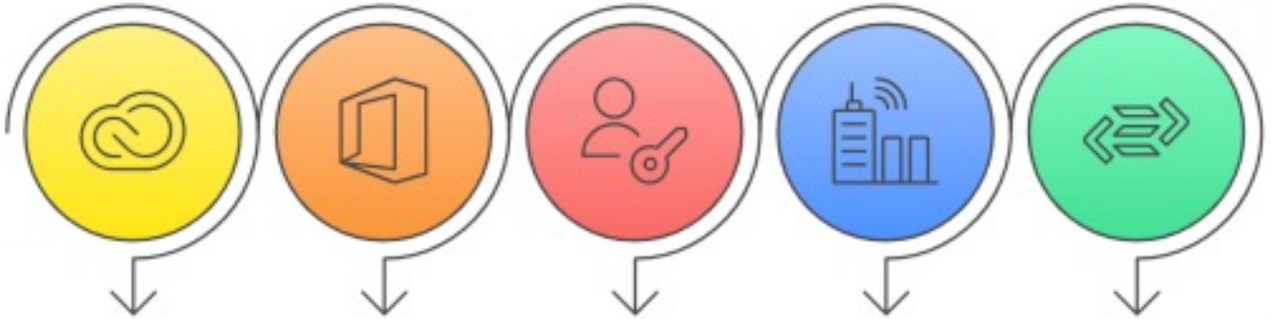
Learning Objectives

- Understand Microsoft Entra ID
- Create, configure, and manage identities
- Lab 01 - Manage Microsoft Entra ID Identities

© Copyright Microsoft Corporation. All rights reserved.

The Multiple ways to Manage Identities

- Azure Portal (portal.azure.com)
- Microsoft 365 Admin Center (admin.microsoft.com)
- Entra Portal (entra.Microsoft.com)
- On-Premise Active Directory Domain Services with account sync through Azure AD Connect
- PowerShell / Azure CLI (Bash)



Azure Portal

Web-based interface for managing Azure resources.

Microsoft 365 Admin Center

Centralized platform for managing Microsoft 365 services.

Entra Portal

Microsoft Entra admin center for identity management.

On-Premise AD

Managing identities through local Active Directory.

PowerShell/Azure CLI

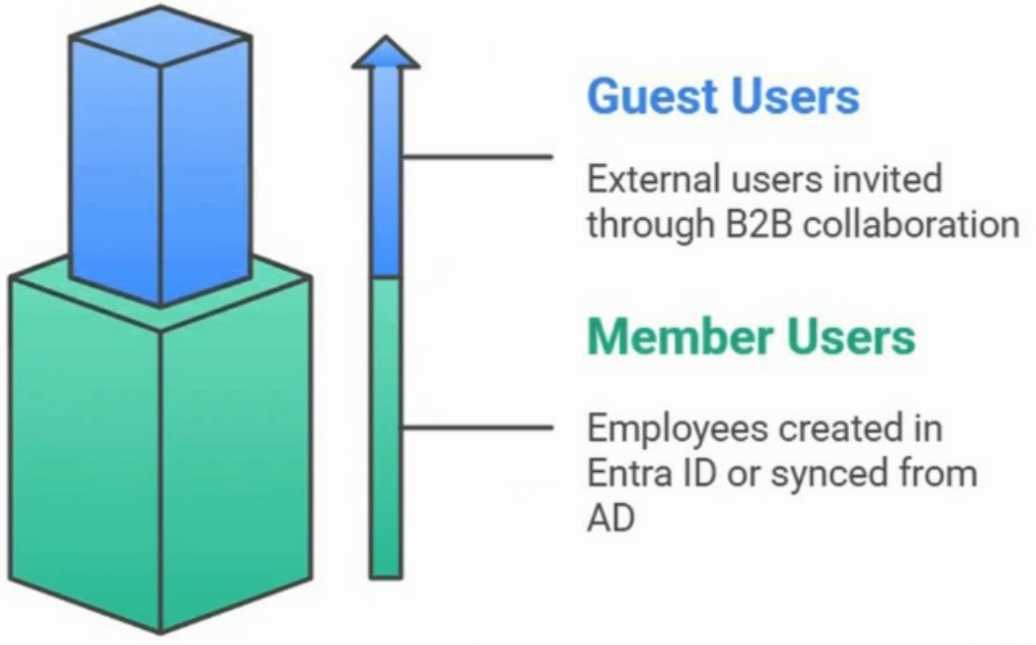
Command-line tools for managing Azure resources.

© Copyright Microsoft Corporation. All rights reserved.

User Identities

These are human users who access Microsoft services.

- **Member users**: Typically, employees created directly in Entra ID or synced from on-premises Active Directory.
- **Guest users**: External users invited through B2B collaboration. Their identity is managed in their home directory but granted limited access.



© Copyright Microsoft Corporation. All rights reserved.

Service Principals

These represent applications or services that need to authenticate and access resources.

- Created automatically when an app is registered in Entra ID.
- Used for assigning permissions, running automation, or secure access without human interaction.

Example: A web app that needs to read/write from Microsoft Graph or access Azure Key Vault.

Application Authentication

Ensures secure access for applications and services

Automated Permissions

Facilitates permission assignments without human intervention

Secure Access

Provides secure resource access without human interaction

© Copyright Microsoft Corporation. All rights reserved.

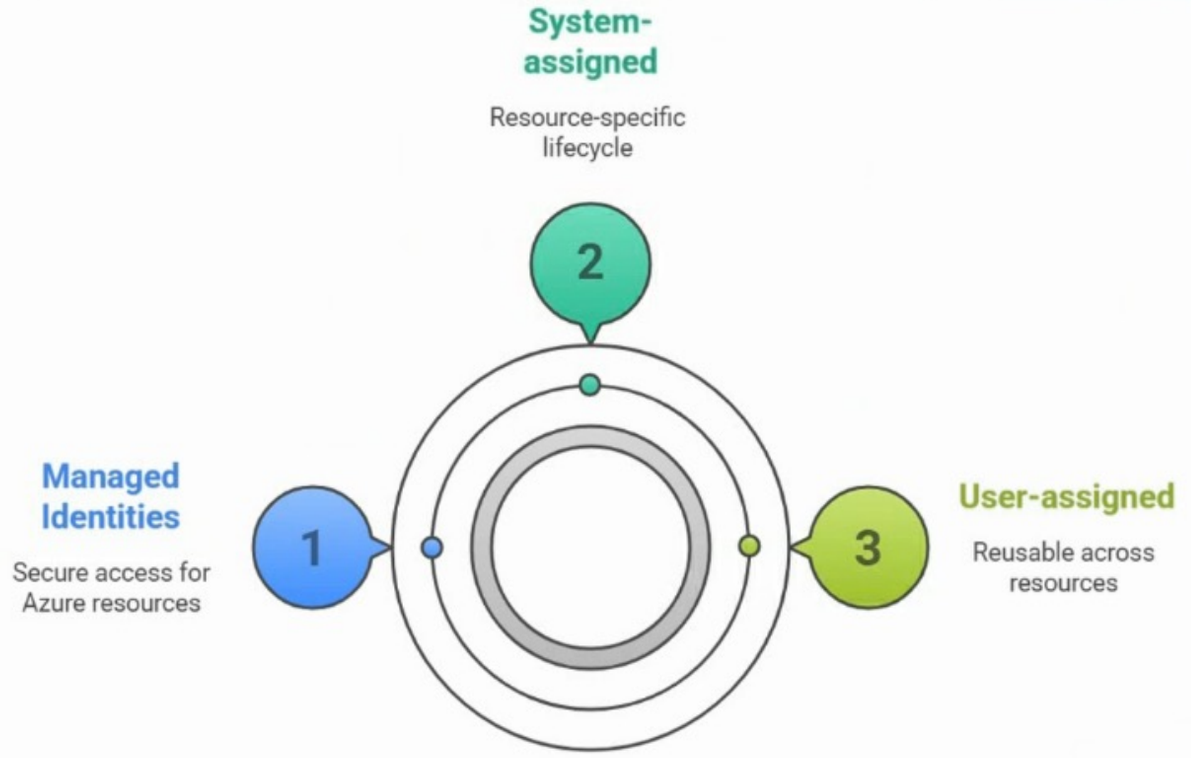
Managed Identities

These are special identities for Azure resources (like VMs or Function Apps) to access other Azure services securely — without storing credentials.

Two types:

- System-assigned: Tied to one resource; lifecycle matches the resource.
- User-assigned: Standalone identity reusable across multiple resources

Example: An Azure VM accessing a storage account using a system-assigned identity.

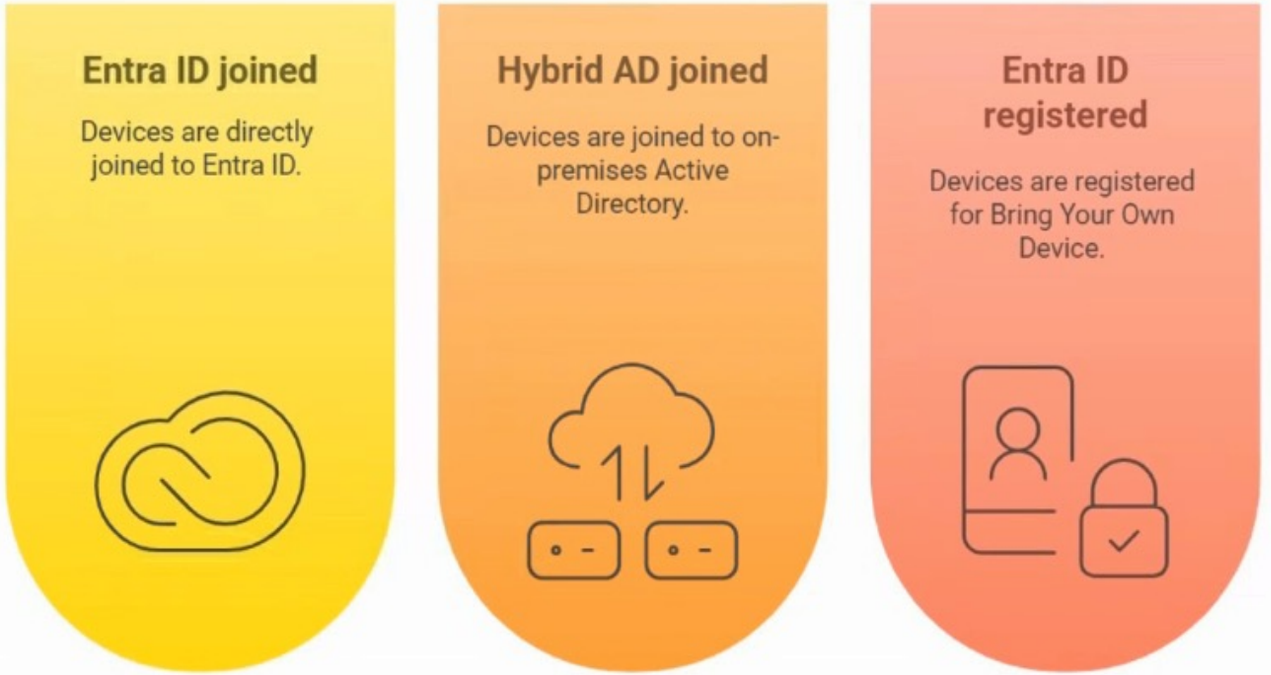


© Copyright Microsoft Corporation. All rights reserved.

Device Identities

Each device that joins Microsoft Entra ID (or is hybrid-joined) gets an identity.

- Used for Conditional Access, compliance, and Intune management.
- Devices can be:
  - Entra ID joined
  - Hybrid AD joined
  - Entra ID registered (BYOD)



© Copyright Microsoft Corporation. All rights reserved.

Understand Microsoft Entra ID

© Copyright Microsoft Corporation. All rights reserved.

Learning Objectives – Understand Microsoft Entra ID

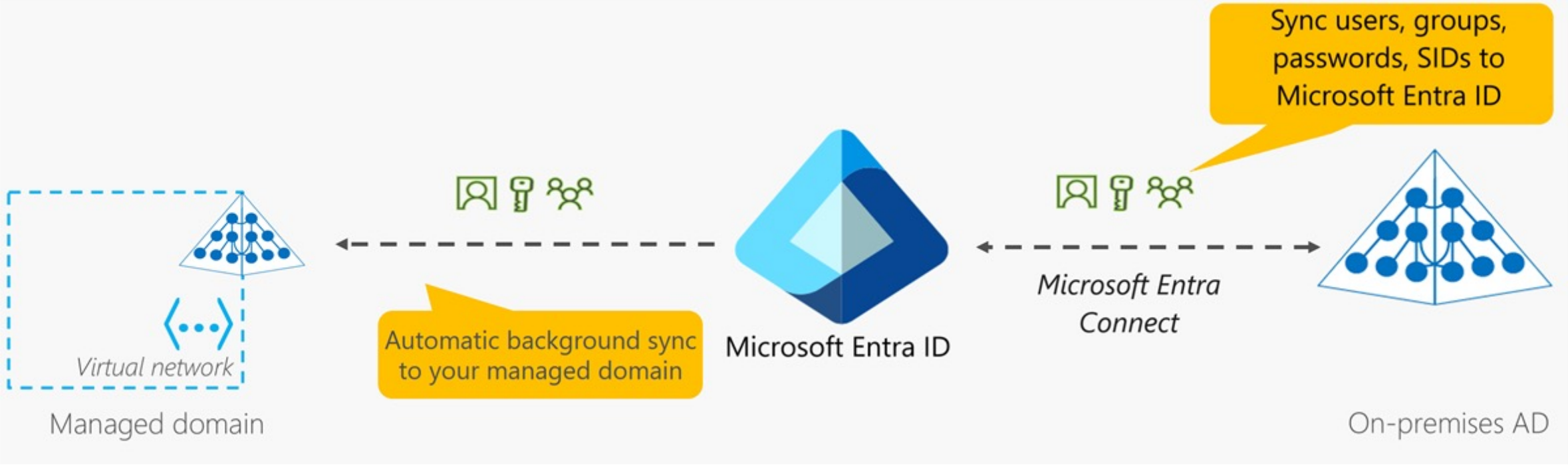
- Examine Microsoft Entra ID
- Describe Microsoft Entra ID Concepts
- Compare Microsoft Entra ID to Active Directory Domain Services
- Compare Microsoft Entra ID P1 and P2 plans
- Implement Self-Service Password Reset
- Learning Recap

Manage Azure identities and governance (20–25%): Manage Microsoft Entra ID users and groups

- Manage licenses in Microsoft Entra ID
- Configure self-service password reset (SSPR)

© Copyright Microsoft Corporation. All rights reserved.

Examine Microsoft Entra ID



- Configure access to applications, including single sign-on
- Manage and provision users and groups
- Providing an identity management solution, including federation
- Implement security features like multi-factor authentication and conditional access

© Copyright Microsoft Corporation. All rights reserved.

Describe Microsoft Entra ID Concepts

Concept	Description
Identity	An object that can be authenticated
Account	An identity that has data associated with it
Microsoft Entra ID account	An identity created through Microsoft Entra ID or another Microsoft cloud service
Tenant/directory	A dedicated and trusted instance. A tenant is automatically created when your organization signs up for a Microsoft cloud service subscription. • Additional instances can be created • Microsoft Entra ID is the underlying product providing the identity service • The term *Tenant* means a single instance representing a single organization • The terms *Tenant* and *Directory* are often used interchangeably
Azure subscription	Used to pay for Azure cloud services

© Copyright Microsoft Corporation. All rights reserved.

Compare Microsoft Entra ID to Active Directory Domain Services

Microsoft Entra ID is primarily an identity solution

Queried using the REST API over HTTP and HTTPS

Uses HTTP and HTTPS protocols such as SAML, WS-Federation, and OpenID Connect for authentication (and OAuth for authorization)

Includes federation services, and many third-party services (such as Facebook)

Microsoft Entra ID users and groups are created in a flat structure, and there are no Organizational Units (OUs) or Group Policy Objects (GPOs)

© Copyright Microsoft Corporation. All rights reserved.

Compare Microsoft Entra ID plans

Feature	Free	Microsoft ID P1	Microsoft ID P2	Microsoft Entra Suite
Single Sign-On (unlimited)	✓	✓	✓	
Cloud and Federated authentication	✓	✓	✓	
Advanced group management		✓	✓	
Self-service account management portal	✓	✓	✓	
Multifactor authentication (MFA)	✓	✓	✓	
Conditional access		✓	✓	
Risk-based Conditional Access (sign-in risk, user risk)			✓	
Automated user and group provisioning to apps		✓	✓	✓
Privileged identity management (PIM)			✓	✓
Advanced identity governance				✓

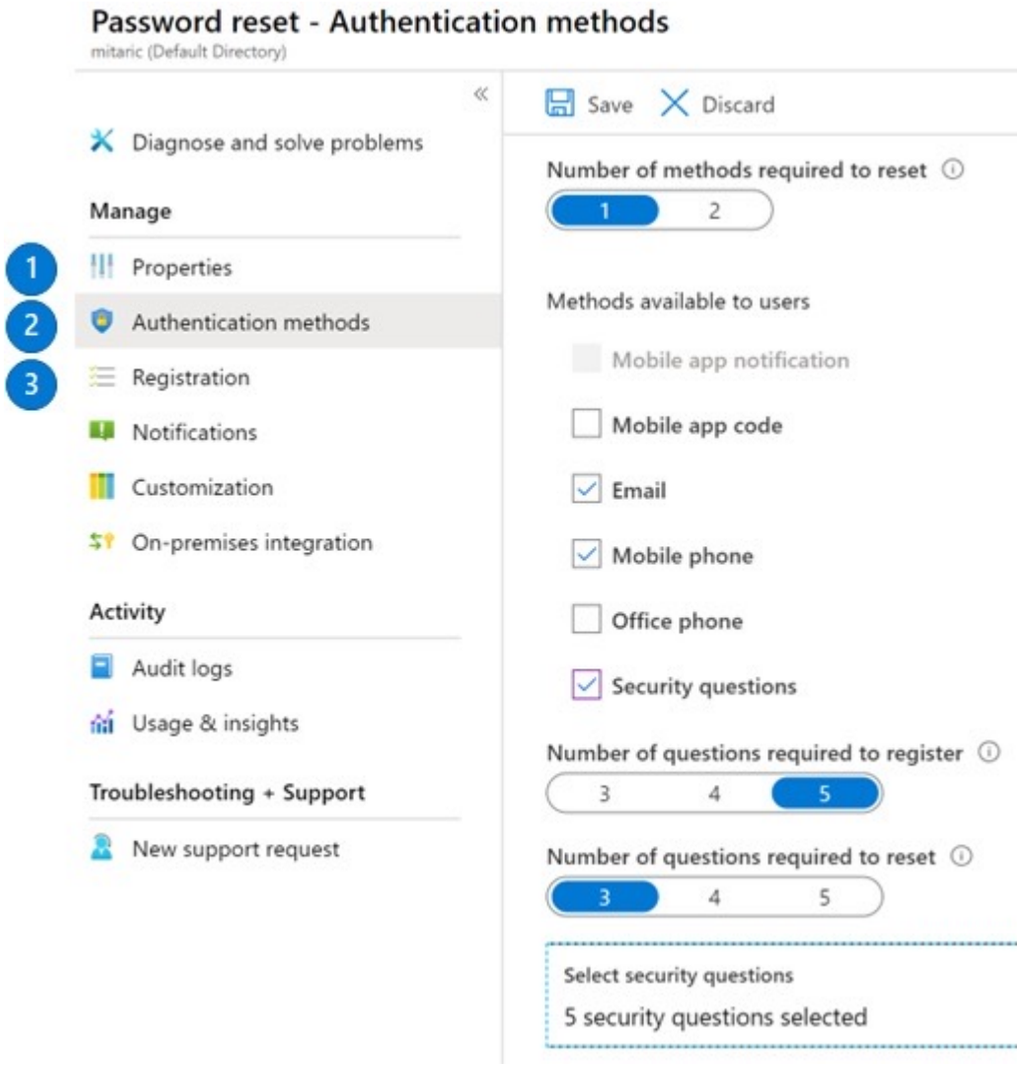
© Copyright Microsoft Corporation. All rights reserved.

What is self-service password reset in Microsoft Entra ID?

1. Determine who can use self-service password reset

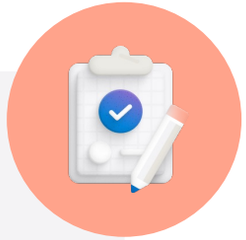
2. Choose the number of authentication methods required and the methods available (email, phone, questions)

3. You can require users to register for SSPR (same process as MFA)



© Copyright Microsoft Corporation. All rights reserved.

Learning Recap – Understand Microsoft Entra ID



Check your knowledge questions and additional study

Reference modules

- Understand Microsoft Entra ID
- Allow users to reset their password with self-service password reset
- Implement and manage hybrid identity

© Copyright Microsoft Corporation. All rights reserved.

Create, configure, and manage identities

© Copyright Microsoft Corporation. All rights reserved.

Learning Objectives - User and Group Accounts

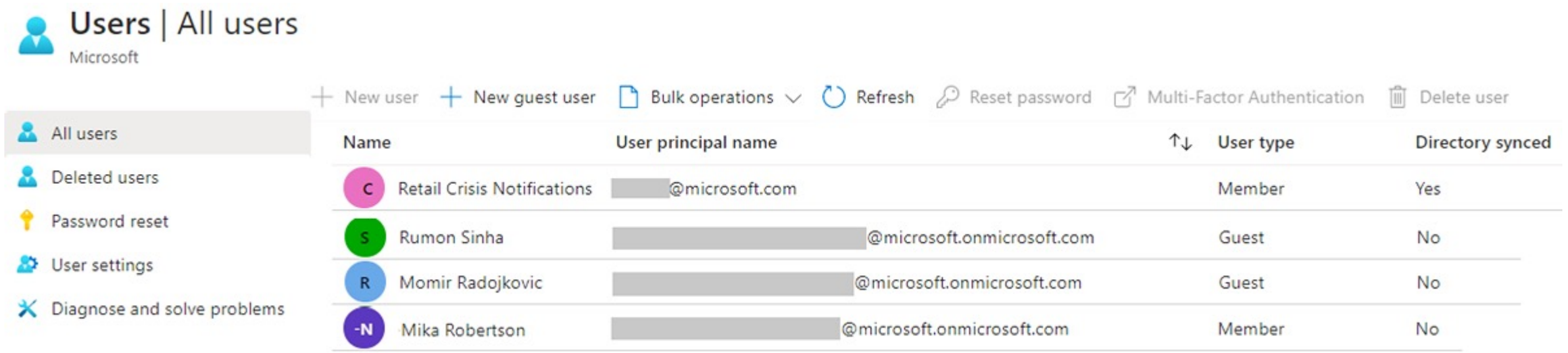
- Create User Accounts
- Manage User Accounts
- Create Group Accounts
- Assign Licenses to Users and Groups (extra topic)
- Demonstration – Users and Groups
- Summary and Resources

Manage Azure identities and governance (20–25%): Manage Microsoft Entra ID users and groups

- Create users and groups
- Manage user and group properties
- Manage external users
- Manage licenses in Microsoft Entra ID

© Copyright Microsoft Corporation. All rights reserved.

Create User Accounts



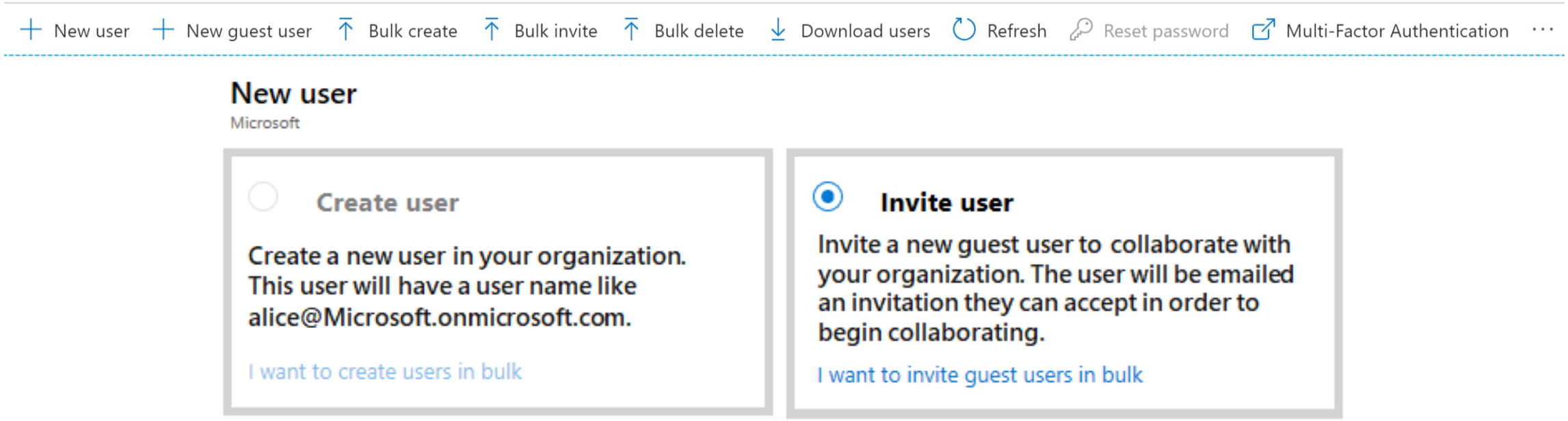
All users must have an account

The account is used for authentication and authorization

Each user account has additional properties

© Copyright Microsoft Corporation. All rights reserved.

Manage User Accounts



Must be Global Administrator or User Administrator to manage users

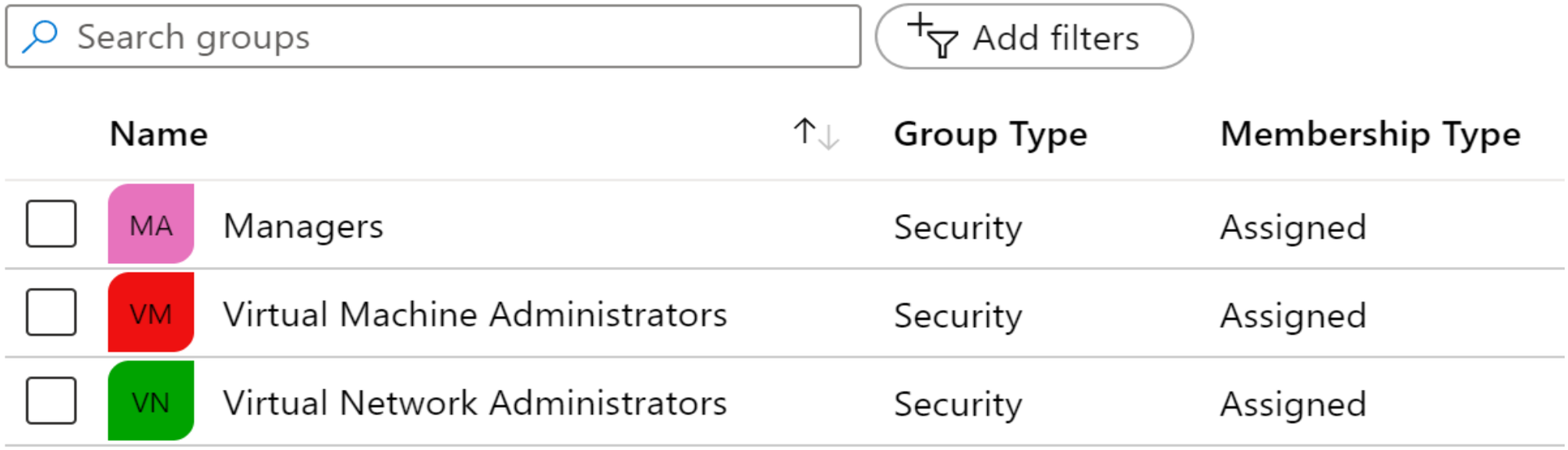
User profile (picture, job, contact info) is optional

Deleted users can be restored for 30 days

Sign in and audit log information is available

© Copyright Microsoft Corporation. All rights reserved.

Create Group Accounts



Group Types

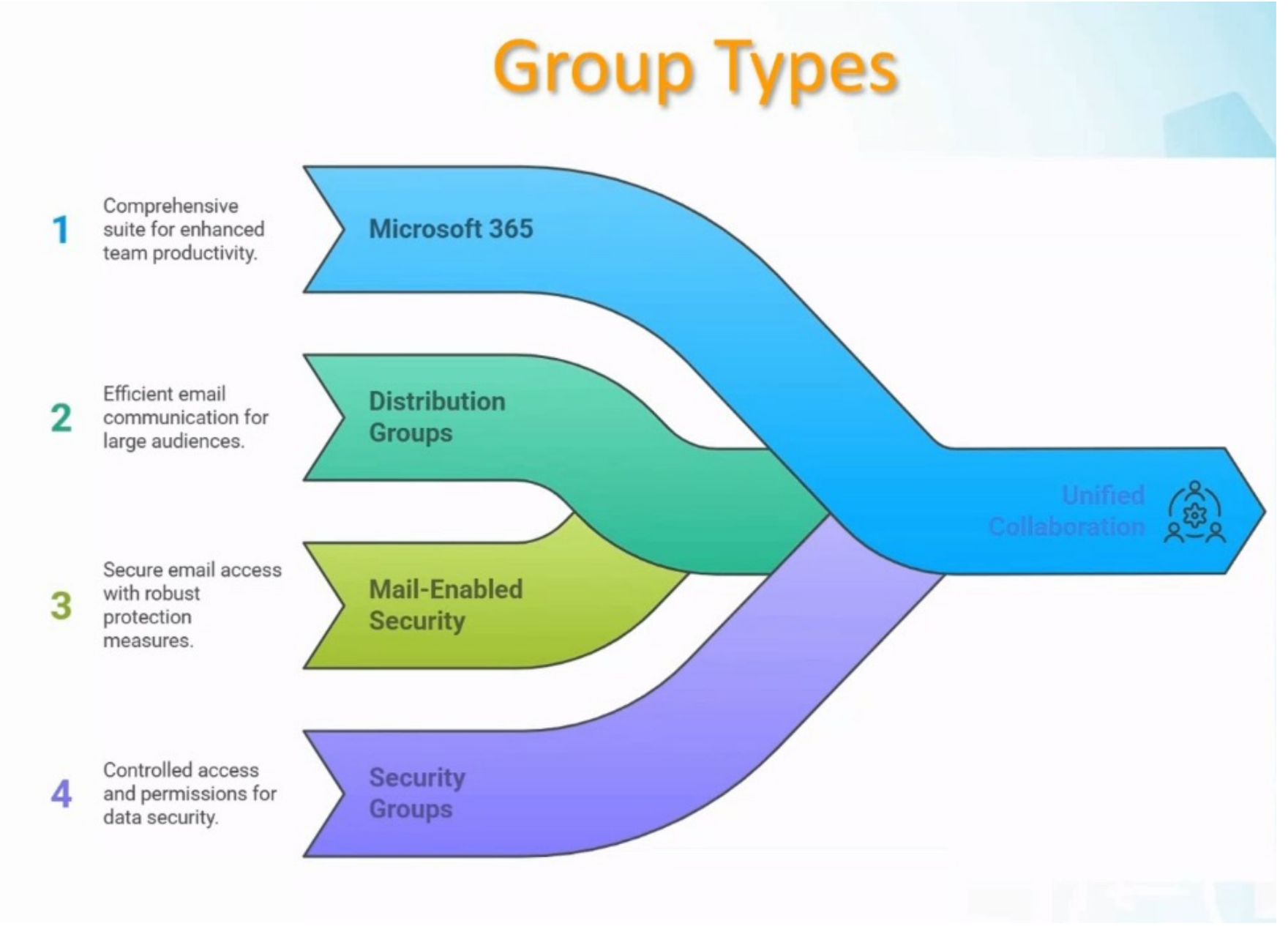
- Security groups
- Microsoft 365 groups

Membership Types

- Assigned
- Dynamic User
- Dynamic Device (Security groups only)

© Copyright Microsoft Corporation. All rights reserved.

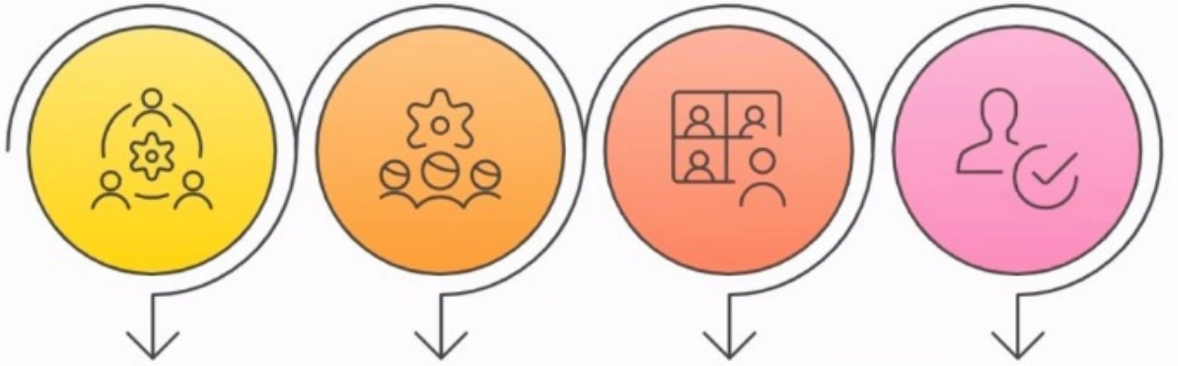
Group Types



© Copyright Microsoft Corporation. All rights reserved.

Microsoft 365 Groups

- **Collaboration-Ready:** Automatically includes a shared mailbox, calendar, SharePoint site, OneNote, and Planner.
- **Integrated with Teams:** Used as the backbone for Microsoft Teams, enabling chat, meetings, and file sharing.
- **Supports Guest Access:** External users can be added securely for collaboration.
- **Dynamic or Assigned:** Membership can be managed manually or based on user attributes using dynamic rules.



Collaboration-Ready

Includes shared mailbox, calendar, SharePoint, OneNote, and Planner.

Integrated with Teams

Backbone for Microsoft Teams, enabling chat, meetings, and file sharing.

Supports Guest Access

External users can be added securely for collaboration purposes.

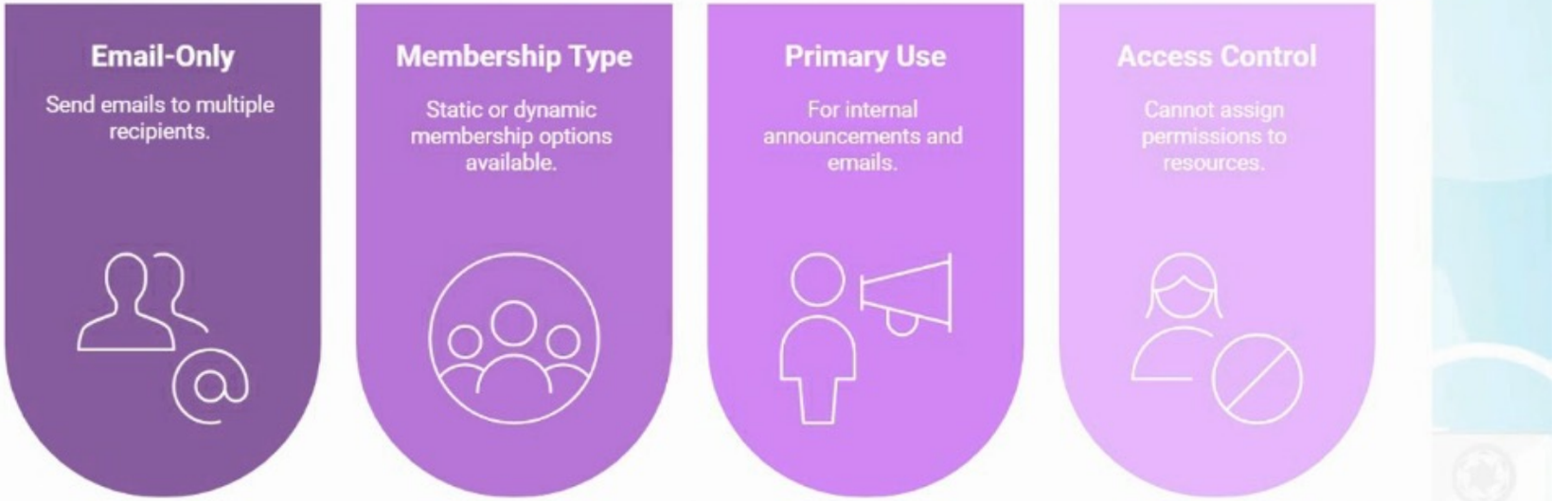
Dynamic or Assigned

Membership managed manually or based on user attributes using dynamic rules.

© Copyright Microsoft Corporation. All rights reserved.

Distribution Groups

- **Email-Only Functionality:** Used to send email messages to multiple recipients at once—no shared workspace or collaboration tools.
- **Manual or Dynamic:** Membership can be static or dynamic (via Exchange dynamic distribution groups based on filters).
- **Internal Communication:** Primarily intended for internal announcements or department-wide emails.
- **No Access Control:** Cannot be used to assign permissions to resources like SharePoint or Teams.



© Copyright Microsoft Corporation. All rights reserved.

Mail-Enabled Security Groups

- **Dual Purpose:** Used for both email distribution and assigning permissions to Microsoft 365 resources.
- **Email Capable:** Has a shared email address, allowing group members to receive messages like a distribution list.
- **Access Control:** Can be used to manage access to SharePoint, OneDrive, Intune, and other resources.
- **No Collaboration Features:** Does not include Teams, shared calendar, or document libraries like Microsoft 365 Groups.

Mail-Enabled Security Groups

Manage access and email

Microsoft 365 Groups

Enhance collaboration and communication

© Copyright Microsoft Corporation. All rights reserved.

Security Groups

- **Access Management:** Primarily used to assign permissions to resources like SharePoint sites, apps, and Intune policies.
- **No Email Functionality:** Cannot send or receive email—strictly for access control.
- **Supports Devices and Users:** Can include users, devices, and service principals for flexible management.
- **Dynamic or Assigned:** Membership can be managed manually or through dynamic rules based on Entra ID attributes.

© Copyright Microsoft Corporation. All rights reserved.

Assigned vs Dynamic Groups

- **Assigned Groups**
  - Members are manually added or removed by an admin
  - Best for small teams or fixed memberships
  - Simple and controlled
- **Dynamic Groups**
  - Membership is based on rules (e.g., department = “HR”)
  - Users/devices automatically added/removed as attributes change
  - Ideal for large orgs and automated management

© Copyright Microsoft Corporation. All rights reserved.

Assign Licenses to Users and Groups

Azure is a cloud service that provides many built-in services for free.

- Microsoft Entra ID comes as a free service
- Gain additional functionality with a P1 or P2 license

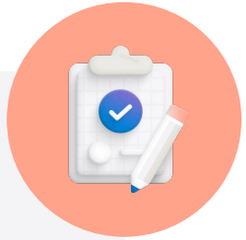
Additional Services (like O365 are paid cloud services)

- Microsoft paid cloud services require licenses
- Licenses are assigned to those who need access to the services
- Each user or group requires a separate paid license
- Administrators use the Microsoft 365 Admin portal and Microsoft Graph PowerShell cmdlets to manage licenses

- ❑ View license plans and plan details
- ❑ Set the Usage Location parameter
- ❑ Assign licenses to users and groups
- ❑ Change license plans for users and groups
- ❑ Remove a license

© Copyright Microsoft Corporation. All rights reserved.

Learning Recap – Create, configure, and manage identities



Reference modules

- Create, configure, and manage identities
- Manage users and groups in Microsoft Entra ID

Check your knowledge questions and additional study

© Copyright Microsoft Corporation. All rights reserved.

Lab – Manage Entra ID Identities

© Copyright Microsoft Corporation. All rights reserved.

Lab 01 – Manage Microsoft Entra ID Identities

In this lab, you learn about users and groups.

Users and groups are the basic building blocks for an identity solution.

You create a new user and invite a guest user.

You also create a group and add a member and owner.

Job Skills

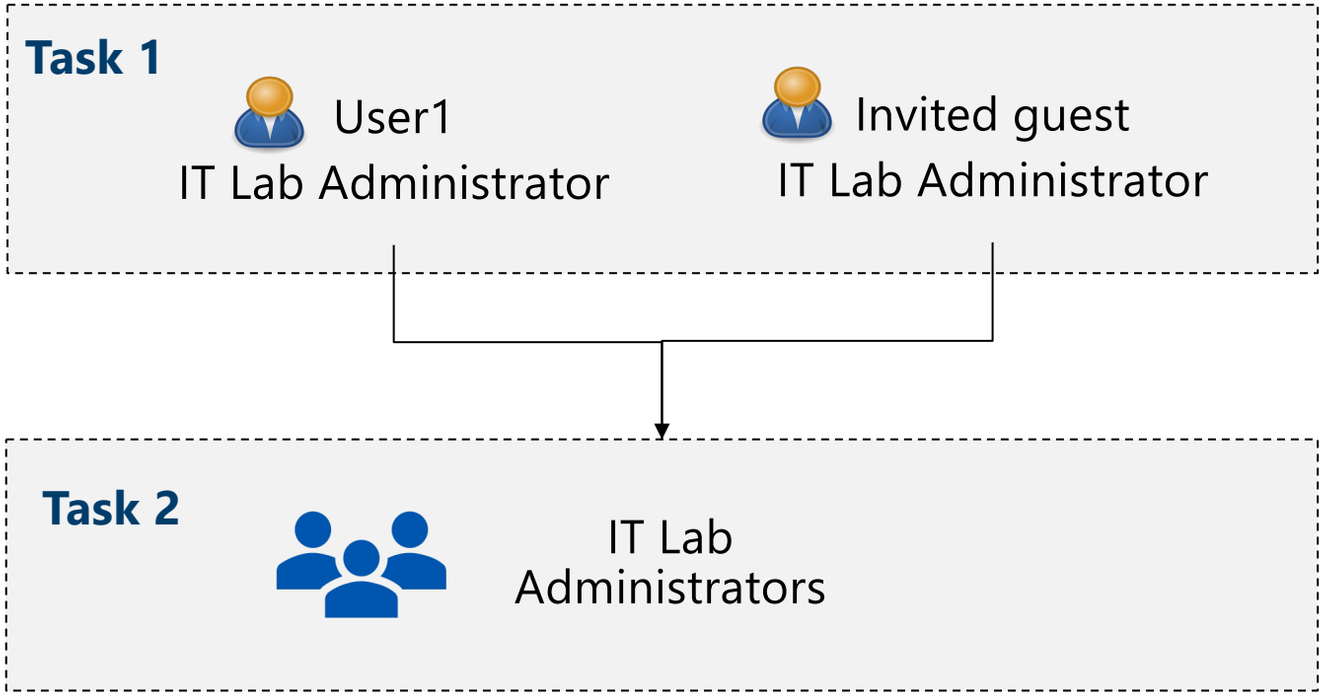
Task 1: Create and configure user accounts.

Task 2: Create groups and add members.

Next slide for an architecture diagram

© Copyright Microsoft Corporation. All rights reserved.

Lab 01 – Manage Entra ID Identities (architecture diagram)



© Copyright Microsoft Corporation. All rights reserved.

End of presentation

© Copyright Microsoft Corporation. All rights reserved.