



KodeKloud

© Copyright KodeKloud

Follow us on <https://kodekloud.com/> to learn more about us.

Administer Identity

© Copyright KodeKloud

These Learn modules are part of the AZ-104: Manage identities and governance in Azure (<https://docs.microsoft.com/learn/patterns/az-104-manage-identities-governance/>) path.

Learning Objectives



A

Configure Microsoft Entra ID



B

Configure User and Group Accounts

Learning Objectives



Configure Microsoft Entra ID

01

Introduction to Microsoft Entra ID

02

Microsoft Entra ID concepts

03

Microsoft Entra ID Editions

04

Configure device identities

Learning Objectives



B Configure User and Group Accounts

01 User Accounts

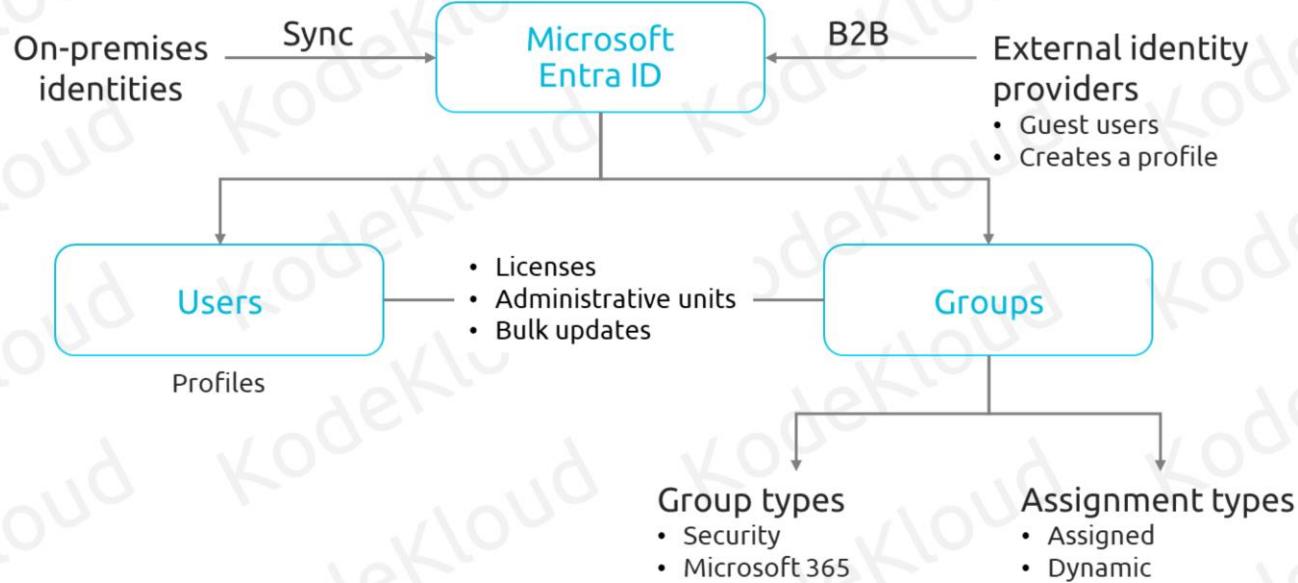
02 Bulk Operations

03 Group Accounts

04 Self-service password reset (SSPR)

05 Multi-tenant environments

Administer Identity – Overview



© Copyright KodeKloud

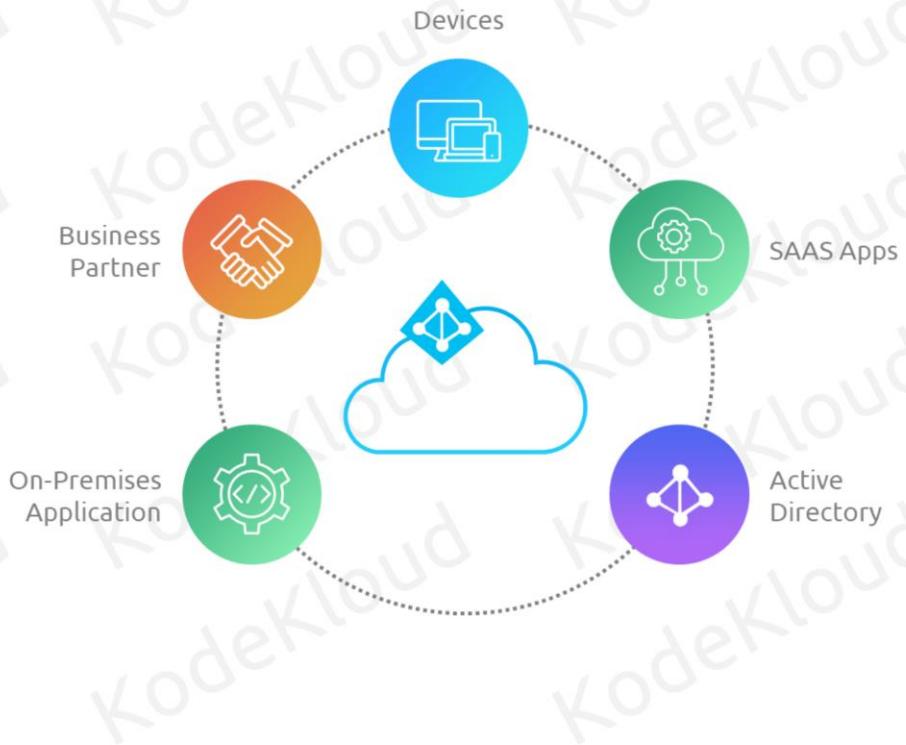
Optional whiteboard slide to introduce the module or review the content. Use the whiteboard diagram directly or recreate the image during the class.



Microsoft Entra ID – Introduction

Microsoft Entra ID

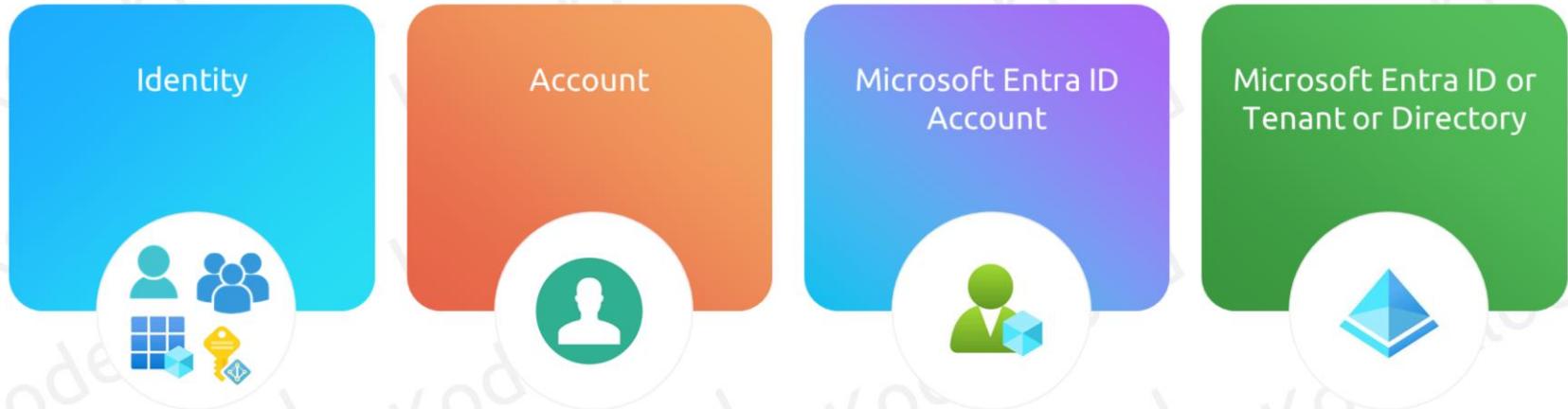
- Cloud-based identity and directory management service enabling access to Azure services and other SaaS solutions like Microsoft 365, DropBox, Concur, Salesforce, etc.
- Cloud offers self-service options including password reset, authentication, device management, hybrid identities, and single sign-on.





Microsoft Entra ID Concepts

Microsoft Entra ID Concepts



© Copyright KodeKloud

Identity

Any object that can be authenticated is considered as an identity. It could be a user, group, managed identity, or service principals.

Account

When we associate data attributes to an identity, we call it an account. For example, a user will have multiple attributes like location, department, manager, phone number, etc.

Microsoft Entra ID account

An account that is created in Microsoft Entra ID or another Microsoft cloud service is known as Microsoft Entra ID account.

Microsoft Entra ID or tenant or directory

Dedicated instance of Microsoft Entra ID that is created during the sign-up of any Microsoft cloud service subscription. Tenant and directory mean the same and you can use the two words interchangeably.



Microsoft Entra ID vs Active Directory Domain Services

Microsoft Entra ID vs Active Directory Domain Services



Microsoft Entra ID

- Queried using HTTP/HTTPS
- Protocols used for authentication include SAML, WS-Federation, and OpenID connect. OAuth is used for authorization
- Federation can be set up with third-party providers like Facebook
- A managed service offering



Active Directory

- Queried using LDAP
- Kerberos is used for AD DS authentication
- Federation is only to other domains; third-party services not supported
- ADDS will be running on VMs or physical servers



Microsoft Entra ID Editions

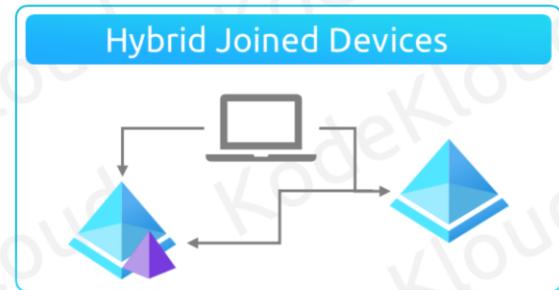
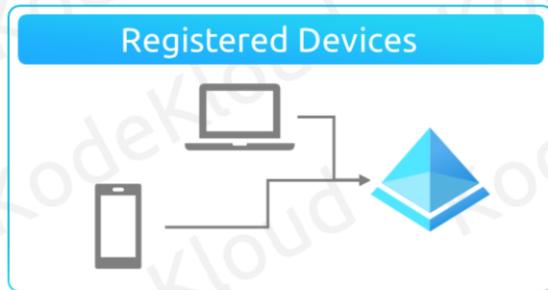
Microsoft Entra ID Editions

Premium P2	Self-service account management	Single Sign on & Core IAM	Cloud and Federated auth	Advanced group management	Automated user and group provisioning	Conditional access + MFA	Identity protection and governance	PIM
Premium P1	Self-service account management	Single Sign on & Core IAM	Cloud and Federated auth	Advanced group management	Automated user and group provisioning	Conditional access + MFA		
Governance	Identity Governance	PIM		Automated user and group provisioning				
Free	Self-service account management	Single Sign on & Core IAM	Cloud and Federated auth + MFA					



Configure Device Identities

Configure Device Identities



© Copyright KodeKloud

Microsoft Entra registered devices - <https://docs.microsoft.com/azure/active-directory/devices/concept-azure-ad-register>

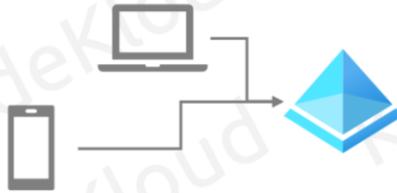
Microsoft Entra joined devices - <https://docs.microsoft.com/azure/active-directory/devices/concept-azure-ad-join>

Microsoft Entra hybrid joined devices - <https://docs.microsoft.com/azure/active-directory/devices/concept-azure-ad-join->

hybrid

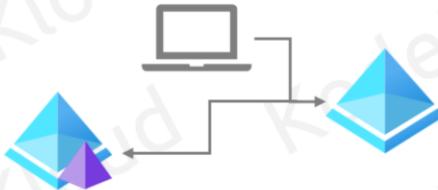
Configure Device Identities

Registered Devices



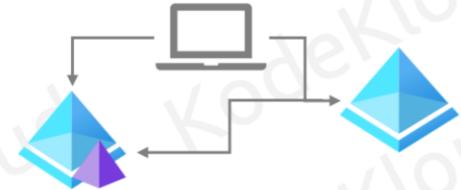
- Permit personal device use
- Login via individual Microsoft accounts
- Link to user account for resource access
- Managed by Microsoft Intune
- Support Windows 10, iOS, Android, and macOS

Joined Devices



- Ideal for cloud-centric organizations
- Company-owned, dedicated to organizational use
- Exclusively connects with Azure, requiring a company account
- Eligible for Conditional Access security measures
- Limited to Windows 10 and newer OS

Hybrid Joined Devices



- Designed for traditional desktop applications
- Managed through Group Policy settings
- Support deployment with pre-configured system images
- Compatible with Windows 7 and above

© Copyright KodeKloud

Microsoft Entra registered devices - <https://docs.microsoft.com/azure/active-directory/devices/concept-azure-ad-register>

Microsoft Entra joined devices - <https://docs.microsoft.com/azure/active-directory/devices/concept-azure-ad-join>

Microsoft Entra hybrid joined devices - <https://docs.microsoft.com/azure/active-directory/devices/concept-azure-ad-join-hybrid>

hybrid



Configure User Accounts

User Account

The screenshot shows the 'Users | All users' page in the Azure Active Directory portal. The left sidebar includes links for 'All users', 'Deleted users', 'Password reset', 'User settings', 'Diagnose and solve problems', 'Activity' (with 'Sign-in logs', 'Audit logs', and 'Bulk operation results'), and 'Troubleshooting + Support'. The main area displays a table with 99 users found, with columns for 'Name', 'User principal name', and 'User type'. Each user entry includes a checkbox and a small circular icon with initials. The users listed are: Abigail Richards (AR), Abraham Morgan (AM), Adam Lloyd (AL), Adison Watson (AW), Adrianna Craig (AC), Aida Perkins (AP), and Albert Alexander (AA).

Name	User principal name	User type
Abigail Richards (AR)	a.richards@kodekloudl...	Member
Abraham Morgan (AM)	a.morgan@kodekloudl...	Member
Adam Lloyd (AL)	a.lloyd@kodekloudl...	Member
Adison Watson (AW)	a.watson@kodekloudl...	Member
Adrianna Craig (AC)	a.craig@kodekloudl...	Member
Aida Perkins (AP)	a.perkins@kodekloudl...	Member
Albert Alexander (AA)	a.alexander@kodeklou...	Member

© Copyright KodeKloud

Cloud Identities

These users exist only in Microsoft Entra ID. Can be Microsoft Entra ID or external Microsoft Entra ID as well.

Guest Accounts

These users exist outside of Azure and they are invited for collaboration. Microsoft accounts, Live accounts, etc.

Directory synchronized users

These users are synchronized from your on-premises Windows AD. We cannot create directory synchronized users; they

need to be synchronized.

User Account



User accounts are used for authentication and authorization; all users must have an account.



Each user account can have optional properties like address, department, etc.



All users can be accessed from **Microsoft Entra ID > Users > All Users**.



We can also perform bulk operations like bulk create, bulk invite, and bulk delete.

Name	User principal name	User type
AR	a.richards@kodekloudl...	Member
AM	a.morgan@kodekloudla...	Member
AL	a.lloyd@kodekloudl...	Member
AW	a.watson@kodekloudla...	Member
AC	a.craig@kodekloudl...	Member
AP	a.perkins@kodekloudl...	Member
AA	a.alexander@kodeklou...	Member

Cloud Identities

Guest Accounts

Directory Synchronized Users

© Copyright KodeKloud

Cloud Identities

These users exist only in Microsoft Entra ID. Can be Microsoft Entra ID or external Microsoft Entra ID as well.

Guest Accounts

These users exist outside of Azure and they are invited for collaboration. Microsoft accounts, Live accounts, etc.

Directory synchronized users

These users are synchronized from your on-premises Windows AD. We cannot create directory synchronized users; they

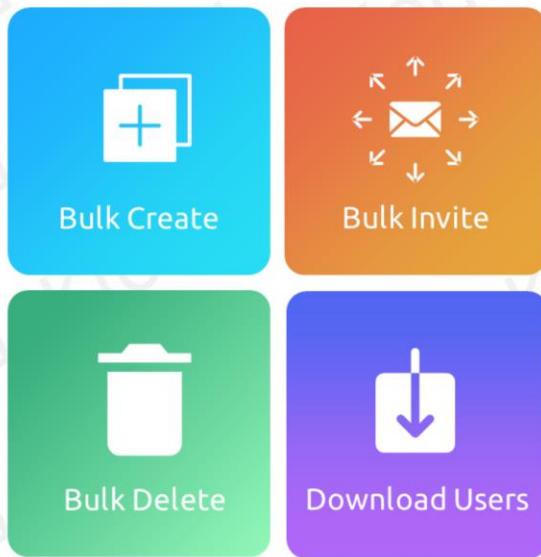
need to be synchronized.



Bulk Operations

User Accounts – Bulk Operations

Bulk operations will let you download a CSV template where you add users that you want to create, delete, or invite.
Using bulk operation, we can easily work on these operations rather than doing one by one.



The screenshot shows the 'Users | All users' page in the Azure Active Directory portal for the 'Kodekloud' tenant. The page lists 99 users found, with columns for Name, User principal name, and User type. On the right side, there is a toolbar with buttons for 'New user', 'New guest user', 'Bulk operations', 'Refresh', and 'filters'. A red box highlights the 'Bulk operations' dropdown menu, which contains four options: 'Bulk create', 'Bulk invite', 'Bulk delete', and 'Download users'. Below the toolbar, there are links for 'All users', 'Deleted users', 'Password reset', 'User settings', and 'Diagnose and solve problems'. The 'Activity' section includes links for 'Sign-in logs', 'Audit logs', and 'Bulk operation results'.

Name	User principal name	User type
AR	a.richards@kodekloudlab...	Member
AM	a.morgan@kodekloudlab...	Member
AL	a.lloyd@kodekloudlab...	Member
AW	a.watson@kodekloudlab...	Member
AC	a.craig@kodekloudlab...	Member
AP	a.perkins@kodekloudlab...	Member

© Copyright KodeKloud

Bulk create: Create users in bulk

Bulk invite: Invite external users for collaboration in bulk

Bulk delete: Delete existing users in bulk

Download users: Creates export of all users in the directory



Group Account

Group Accounts

The screenshot shows the 'Groups | All groups' page in the Azure Active Directory portal. The left sidebar includes links for 'All groups', 'Deleted groups', 'Diagnose and solve problems', 'Settings' (with options for General, Expiration, and Naming policy), and 'Activity' (with links for Privileged access groups (Preview), Access reviews, Audit logs, and Bulk operation results). The main area displays a table of groups with the following data:

	Name ↑	Object Id	Group Type
<input type="checkbox"/>	AA Azure Admins	5374db49-56df-4955-b80b-a41eb90513fd	Security
<input type="checkbox"/>	FI Finance	2bbdcbb0-9a1f-4794-80c9-b4de0bd71f24	Security
<input type="checkbox"/>	HR HR	e1a3e9fc-e53a-4efb-a47e-d234b78f3c9b	Security

Group Accounts

Home > KodeKloud

Groups | All groups

KodeKloud - Azure Active Directory

New group Download groups Delete Refresh Columns Go

All groups Deleted groups Diagnose and solve problems

Search Add filter

Search mode Contains

3 groups found

<input type="checkbox"/>	Name ↑	Object Id	Group Type
<input type="checkbox"/>	AA Azure Admins	5374db49-56df-4955-b80b-a41eb90513fd	Security
<input type="checkbox"/>	FI Finance	2bbdcbb0-9a1f-4794-80c9-b4de0bd71f24	Security
<input type="checkbox"/>	HR HR	e1a3e9fc-e53a-4efb-a47e-d234b78f3c9b	Security

General Expiration Naming policy

Privileged access groups (Preview) Access reviews Audit logs Bulk operation results

Group Types

- Security groups
- Microsoft 365 groups

Assignment Types

- Assigned
- Dynamic user
- Dynamic device (only for Security group type)



Self-Service Password Reset (SSPR)

Self-Service Password Reset (SSPR)

The screenshot shows the Microsoft Azure portal interface for managing password reset settings. The top navigation bar includes the Microsoft Azure logo, a search bar, and a user profile icon. The main title is "Password reset | Authentication methods". The left sidebar, titled "Manage", has several options: "Diagnose and solve problems", "Properties" (selected), "Authentication methods" (highlighted with a grey background), "Registration", "Notifications", "Customization", "On-premises integration", and "Administrator Policy". Below the sidebar, there's an "Activity" section. The main content area has a "Save" button and a "Discard" button. A slider labeled "Number of methods required to reset" is set to 1. Under "Methods available to users", several options are listed with checkboxes: "Mobile app notification" (unchecked), "Mobile app code" (unchecked), "Email" (checked), "Mobile phone (SMS only)" (checked), "Office phone" (unchecked), and "Security questions" (unchecked).

Self-Service Password Reset (SSPR)



Enables users to reset password without the need to call IT helpdesk.



Set up multiple methods for resetting the password.



Requires Premium P2 license as this a premium feature.



Target all users or a group of users and enable SSPR. For admin accounts, SSPR is enabled by default.

The screenshot shows the 'Password reset | Authentication methods' page in the Microsoft Azure portal. The 'Manage' sidebar on the left includes options like Properties (highlighted with a red border), Authentication methods (highlighted with a purple border), Registration (highlighted with a green border), Customization, On-premises integration, and Administrator Policy. The main area shows a slider for 'Number of methods required to reset' set to 1, and a list of 'Methods available to users' including: Mobile app notification (unchecked), Mobile app code (unchecked), Email (checked), Mobile phone (SMS only) (checked), Office phone (unchecked), and Security questions (unchecked).

1 | Enable SSPR for all users or for selected groups

2 | Set up the number of authentication methods required for reset and the available methods

3 | Users will be requested to register for SSPR during next sign-in where they can enable their reset method



Multi-Tenant Environments

Multi-Tenant Environments



Relationship



Resource
Independence



Administration
Independence



Synchronization
Independence



KodeKloud

© Copyright KodeKloud

Follow us on <https://kodekloud.com/> to learn more about us.