KodeKloud

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

Administer Identity

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

Learning Objectives

A Configure Microsoft Entra ID

B Configure User and Group Accounts

Learning Objectives

A 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

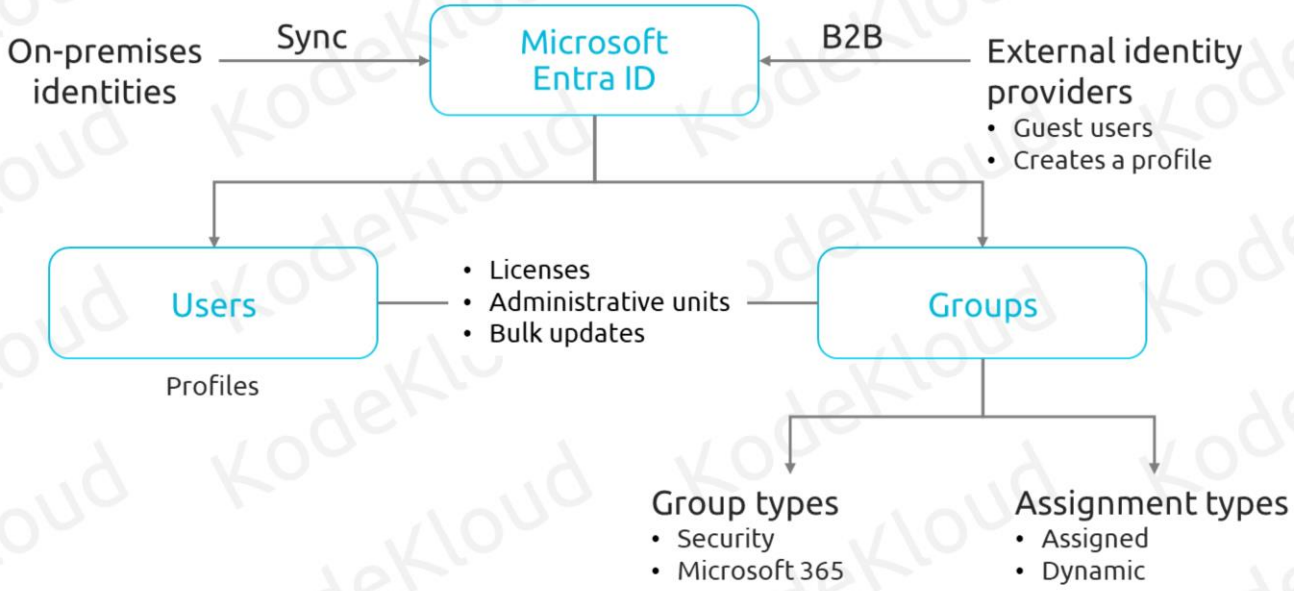
02 Bulk Operations

03 Group Accounts

04 Self-service password reset (SSPR)

05 Multi-tenant environments

Administer Identity – Overview



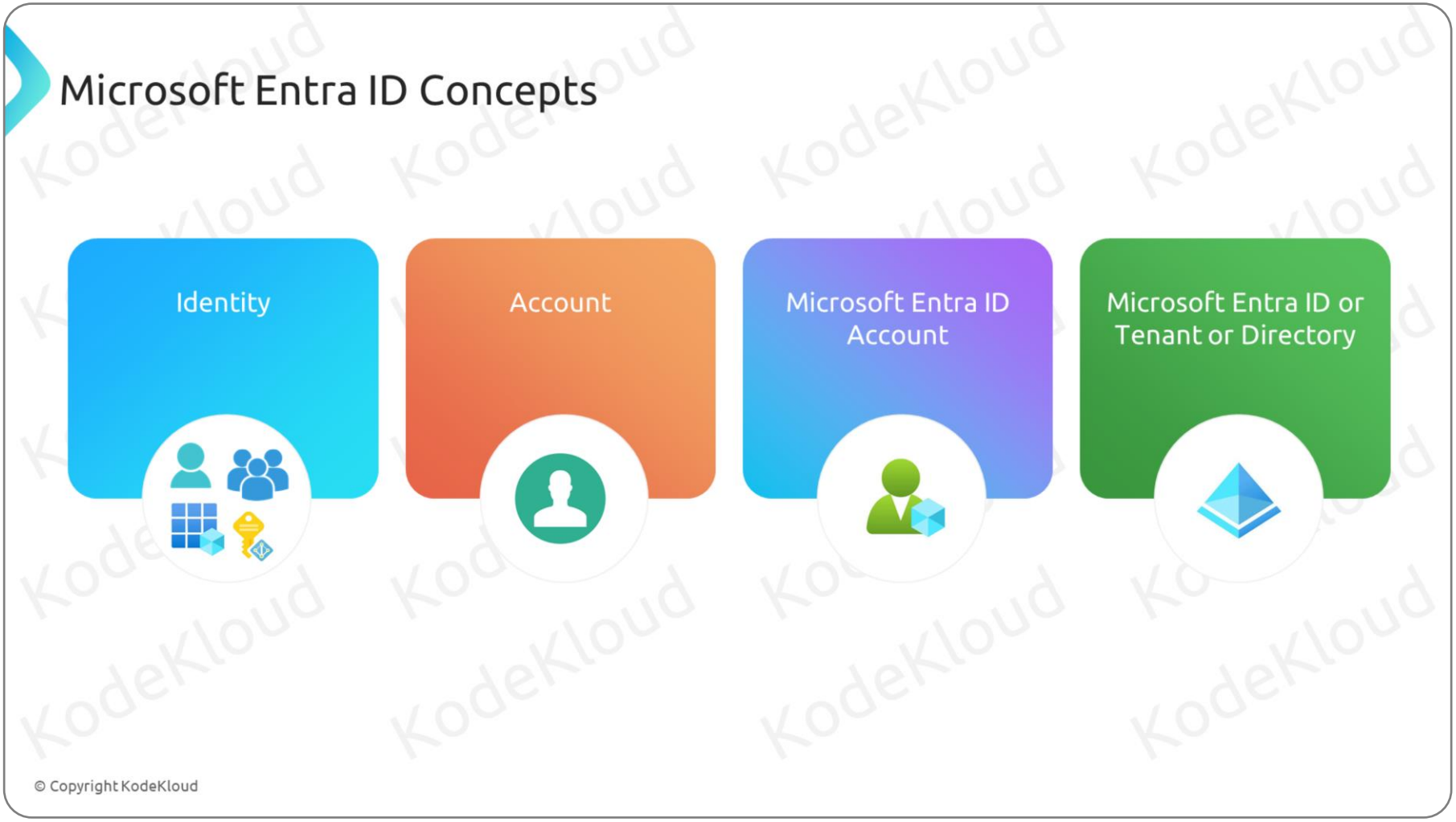
Optional whiteboard slide to introduce the module or review the content. Use the whiteboard diagram directly or recreate the image during the class.

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



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

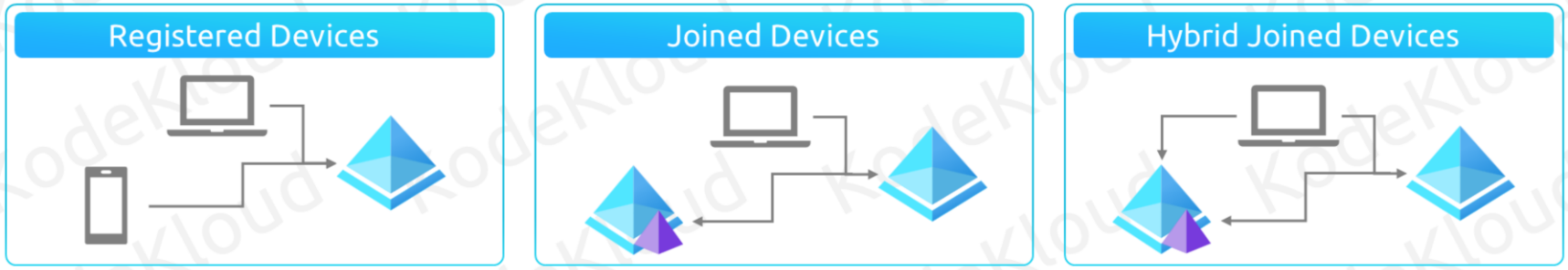
Microsoft Entra ID Editions

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



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

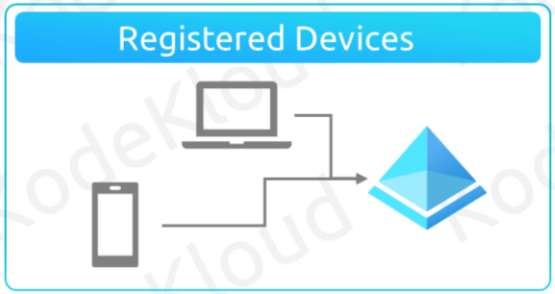
Microsoft Entra joined devices - https://docs.microsoft.com/azure/active-directory/devices/concept-azure-ad-join

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

hybrid

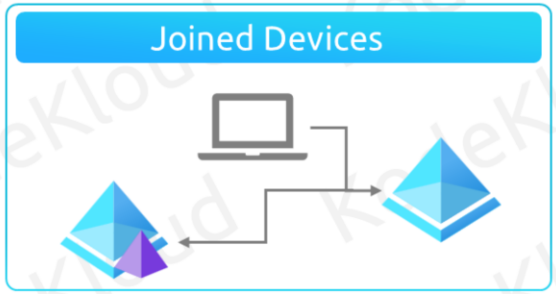
Configure Device Identities

Registered Devices



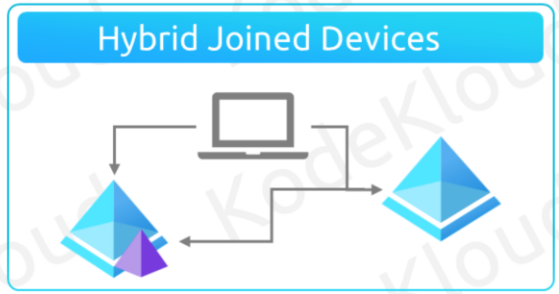
- Permit personal device use
- Login via individual Microsoft accounts
- Link to user account for resource access
- Managed by Microsoft Intune
- Support Windows 10, iOS, Android, and macOS

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

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

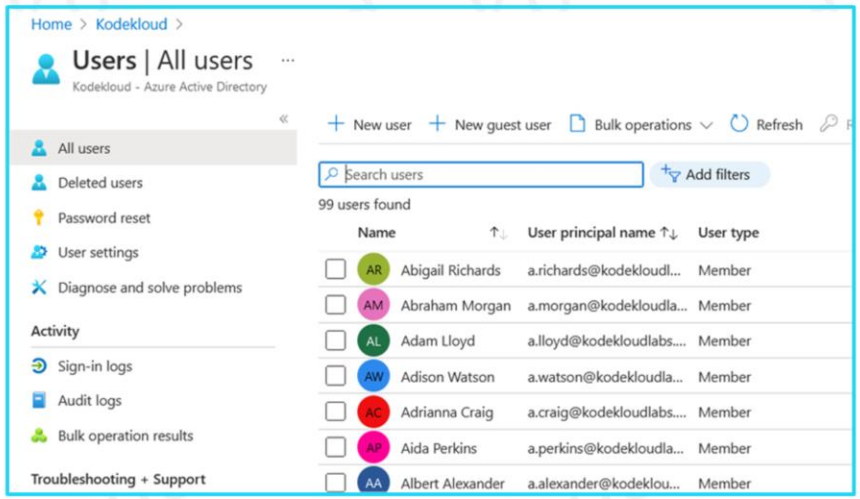
Microsoft Entra joined devices - https://docs.microsoft.com/azure/active-directory/devices/concept-azure-ad-join

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

hybrid

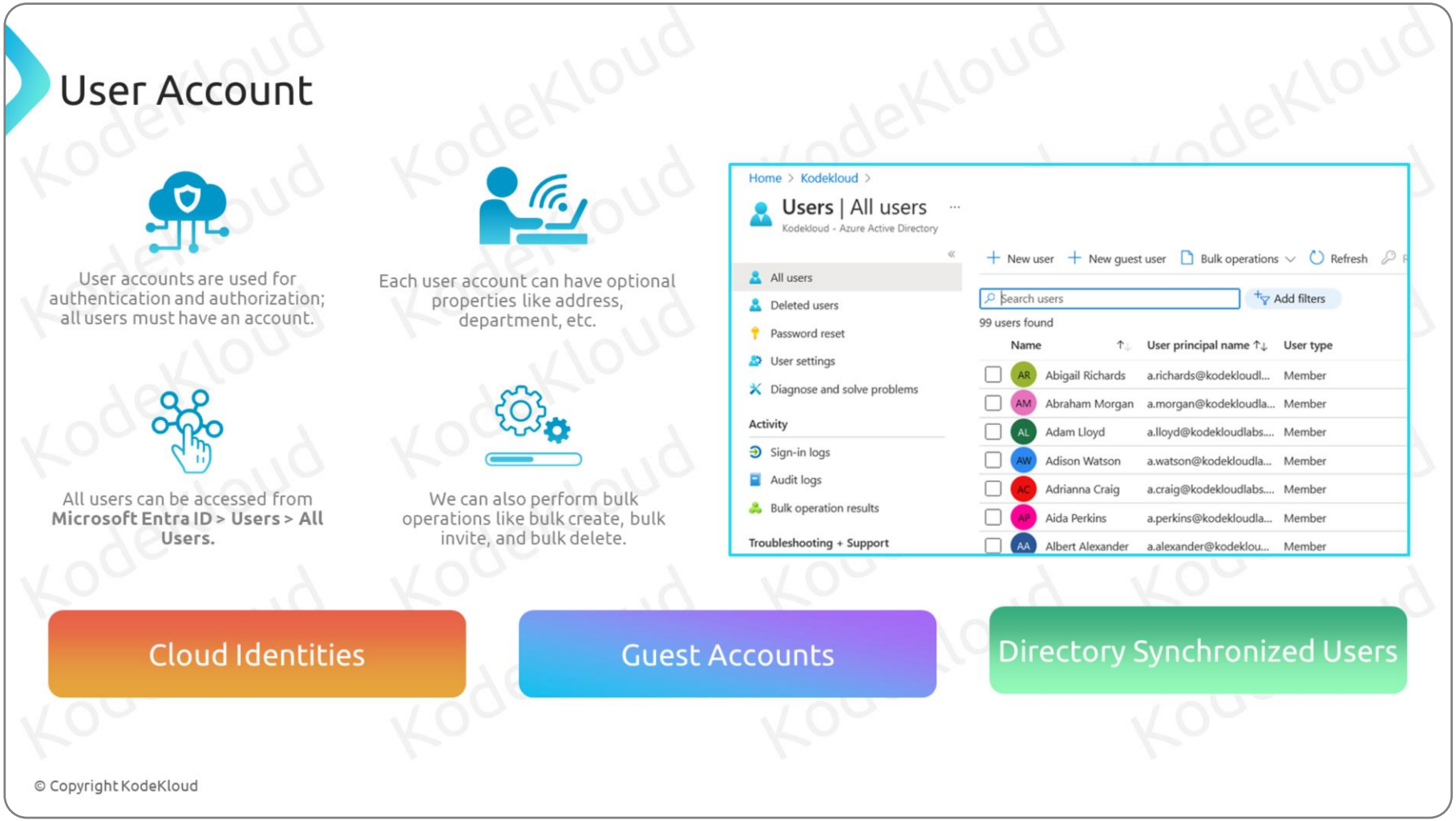
Configure User Accounts

User Account



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.



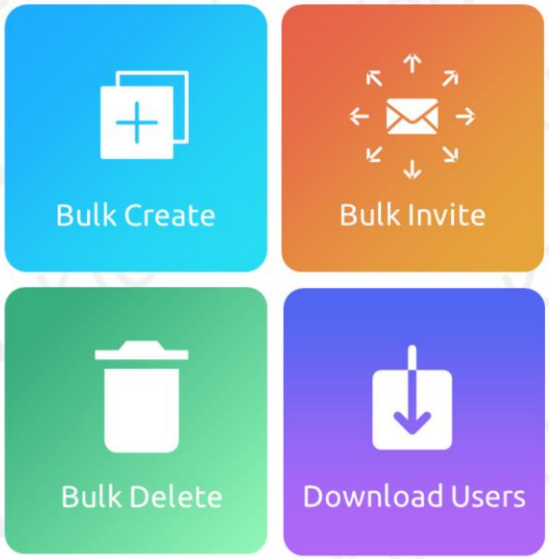
Cloud Identities
These users exist only in Microsoft Entra ID. Can be Microsoft Entra ID or external Microsoft Entra ID as well.
Guest Accounts
These users exist outside of Azure and they are invited for collaboration. Microsoft accounts, Live accounts, etc.
Directory synchronized users
These users are synchronized from your on-premises Windows AD. We cannot create directory synchronized users; they

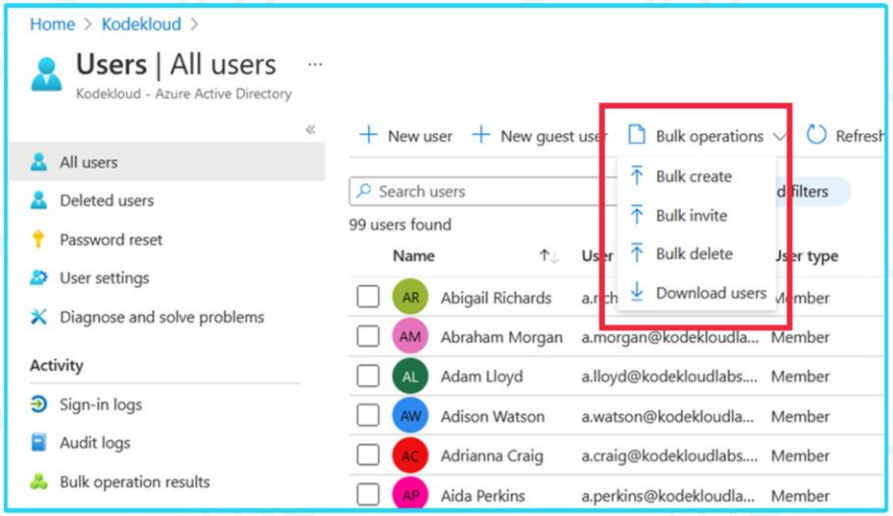
need to be synchronized.

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.

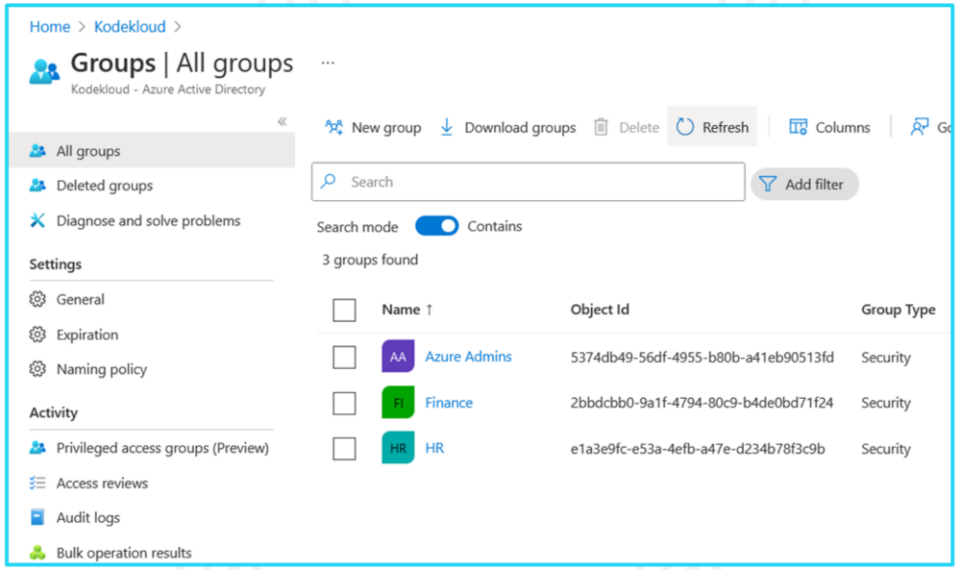




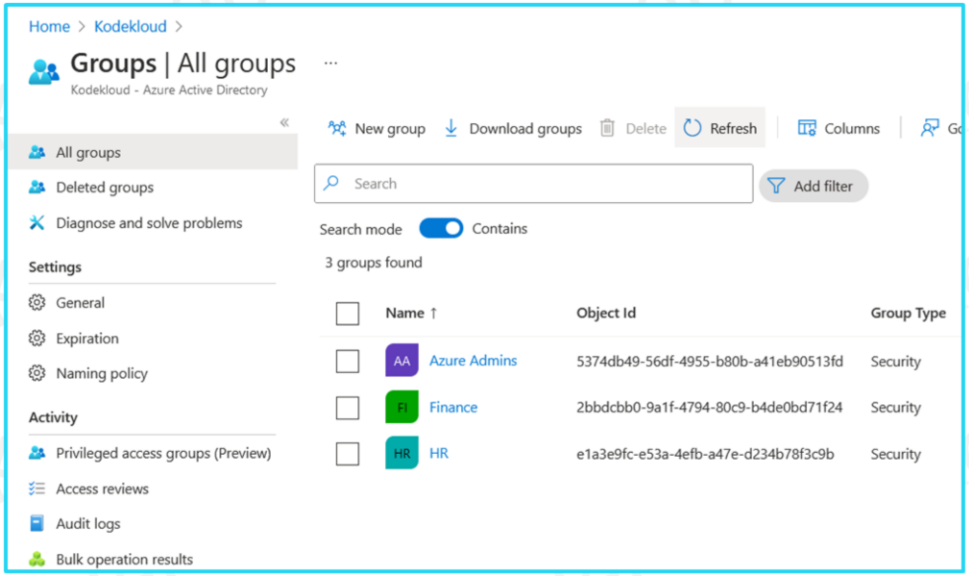
Bulk create: Create users in bulk
Bulk invite: Invite external users for collaboration in bulk
Bulk delete: Delete existing users in bulk
Download users: Creates export of all users in the directory

Group Account

Group Accounts



Group Accounts



Group Types

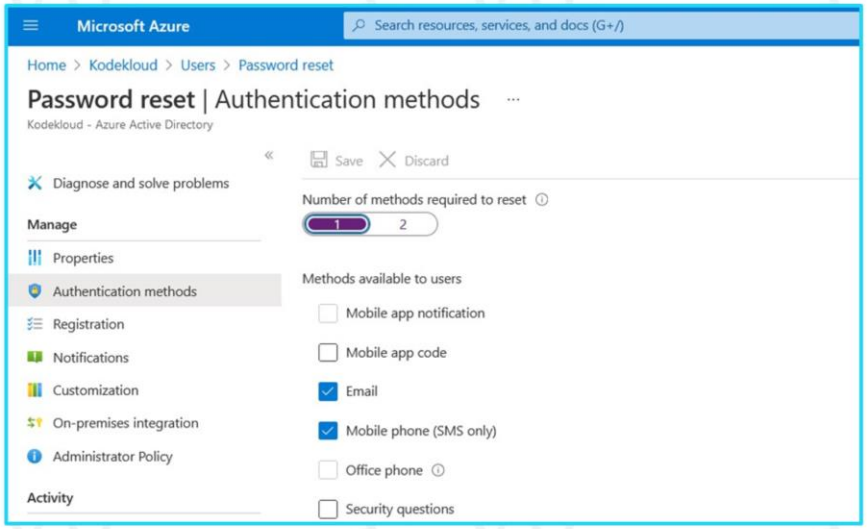
- Security groups
- Microsoft 365 groups

Assignment Types

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

Self-Service Password Reset (SSPR)

Self-Service Password Reset (SSPR)



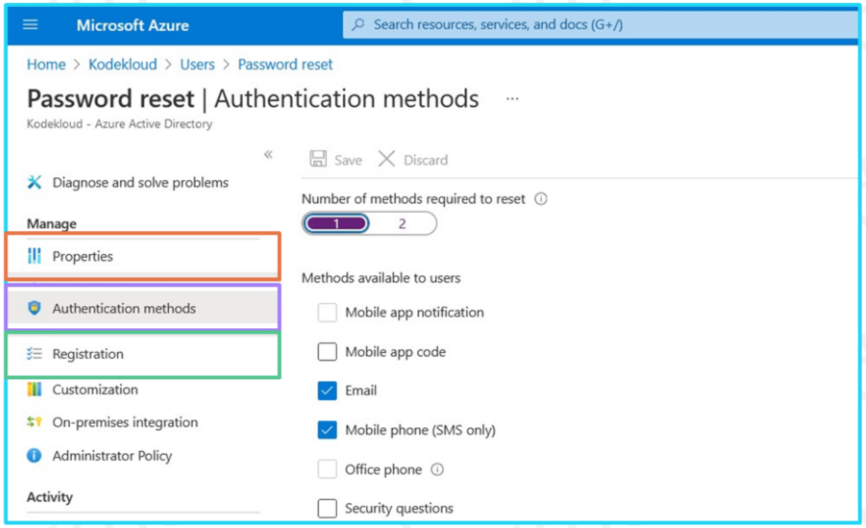
Self-Service Password Reset (SSPR)

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.



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

KodeKloud

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