



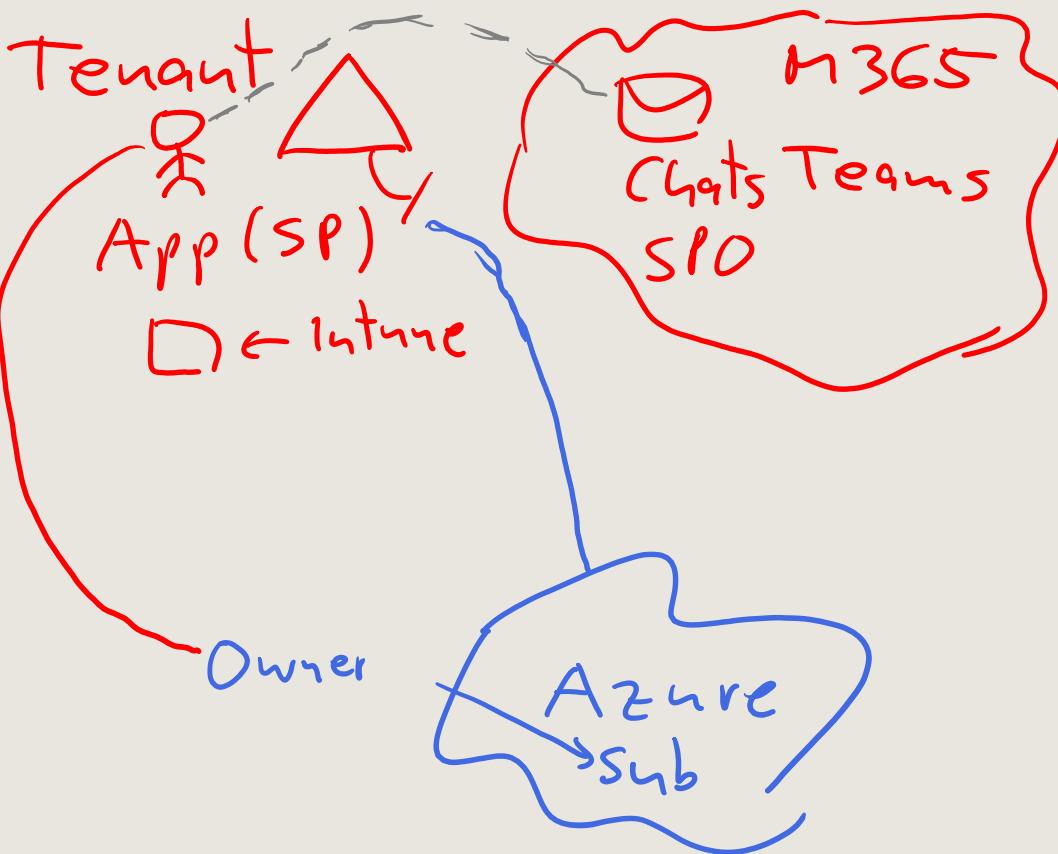
AZ-104

# Administer Identity



# AZ-104 Agenda

- 01: Administer Identity ← Entra ID
- 02: Administer Governance and Compliance
- 03: Administer Azure Resources
- 04: Administer Virtual Networking
- 05: Administer Intersite Connectivity
- 06: Administer Network Traffic Management
- 07: Administer Azure Storage
- 08: Administer Azure Virtual Machines
- 09: Administer PaaS Compute Options
- 10: Administer Data Protection
- 11: Administer Monitoring



OAuth 2.0

# Learning Objectives

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

# Understand Microsoft Entra ID

# Learning Objectives – Understand Microsoft Entra ID

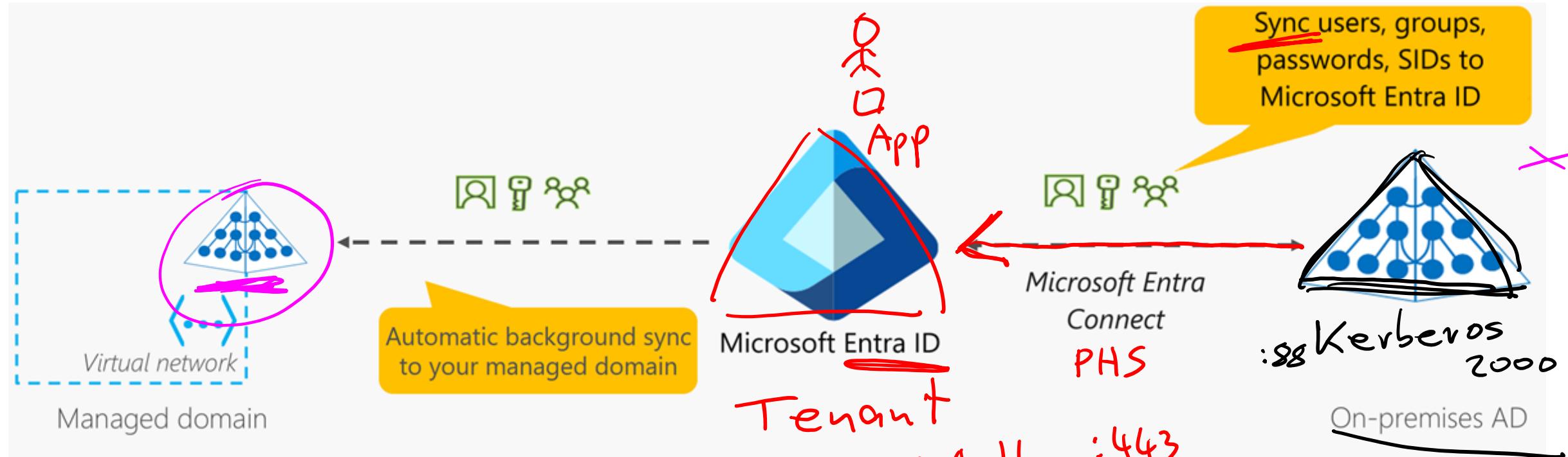
- Examine Microsoft Entra ID
- Describe Microsoft Entra ID Concepts
- Compare Microsoft Entra ID to Active Directory Domain Services
- Compare Microsoft Entra ID P1 and P2 plans
- Implement Self-Service Password Reset
- Learning Recap

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)

AAA

# Examine Microsoft Entra ID



- Configure access to applications, including single sign-on **OAuth :443** **Open ID Connect**
- Manage and provision users and groups
- Providing an identity management solution, including federation
- Implement security features like multi-factor authentication and conditional access

# 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. <ul style="list-style-type: none"><li>Additional instances can be created</li><li>Microsoft Entra ID is the underlying product providing the identity service</li><li>The term <i>Tenant</i> means a single instance representing a single organization</li><li>The terms <i>Tenant</i> and <i>Directory</i> are often used interchangeably</li></ul>
Azure subscription	Used to pay for Azure cloud services

EXO  
SPO

# Compare Microsoft Entra ID to Active Directory Domain Services



Microsoft Entra ID is primarily an identity solution

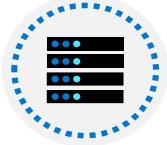


Queried using the REST API over HTTP and HTTPS

Microsoft Graph API  
M365



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)

SKU

# 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				✓

Access  
Packages

# 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)

**Password reset - Authentication methods**  
mitaric (Default Directory)

Save Discard

Number of methods required to reset 1

Methods available to users

- Mobile app notification
- Mobile app code
- Email
- Mobile phone
- Office phone
- Security questions

Number of questions required to register 5

Number of questions required to reset 5

Select security questions  
5 security questions selected

Diagnose and solve problems

Manage

Properties

Authentication methods

Registration

Notifications

Customization

On-premises integration

Audit logs

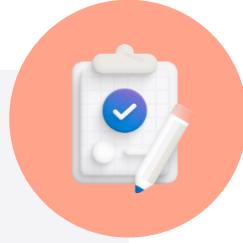
Usage & insights

Troubleshooting + Support

New support request

# 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](#)

# Create, configure, and manage identities



# 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

# Create User Accounts

All users	Name	User principal name	User type	Directory synced
<a href="#">All users</a>	Retail Crisis Notifications	@microsoft.com	Member	Yes
<a href="#">Deleted users</a>	Rumon Sinha	@microsoft.onmicrosoft.com	Guest	No
<a href="#">Password reset</a>	Momir Radojkovic	@microsoft.onmicrosoft.com	Guest	No
<a href="#">User settings</a>	Mika Robertson	@microsoft.onmicrosoft.com	Member	No
<a href="#">Diagnose and solve problems</a>				

All users must have an account

The account is used for authentication and authorization

Each user account has additional properties

# Manage User Accounts

+ New user + New guest user ↑ Bulk create ↑ Bulk invite ↑ Bulk delete ↓ Download users ⏪ Refresh 🗑️ Reset password 🛡️ Multi-Factor Authentication ⋮

## New user

Microsoft



### Create user

Create a new user in your organization. This user will have a user name like alice@Microsoft.onmicrosoft.com.

[I want to create users in bulk](#)



### Invite user

Invite a new guest user to collaborate with your organization. The user will be emailed an invitation they can accept in order to begin collaborating.

[I want to invite guest users in bulk](#)

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

# Create Group Accounts

Name		Group Type	Membership Type
<input type="checkbox"/>	MA	Managers	Security Assigned
<input type="checkbox"/>	VM	Virtual Machine Administrators	Security Assigned
<input type="checkbox"/>	VN	Virtual Network Administrators	Security <u>Assigned</u> M365 Dynamic

**Group Types**

- Security groups
- Microsoft 365 groups

**Membership Types**

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

# 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

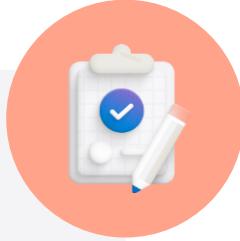
Additional Services (like O365 are paid cloud services)

- 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

# Learning Recap – Create, configure, and manage identities

Check your knowledge questions and additional study

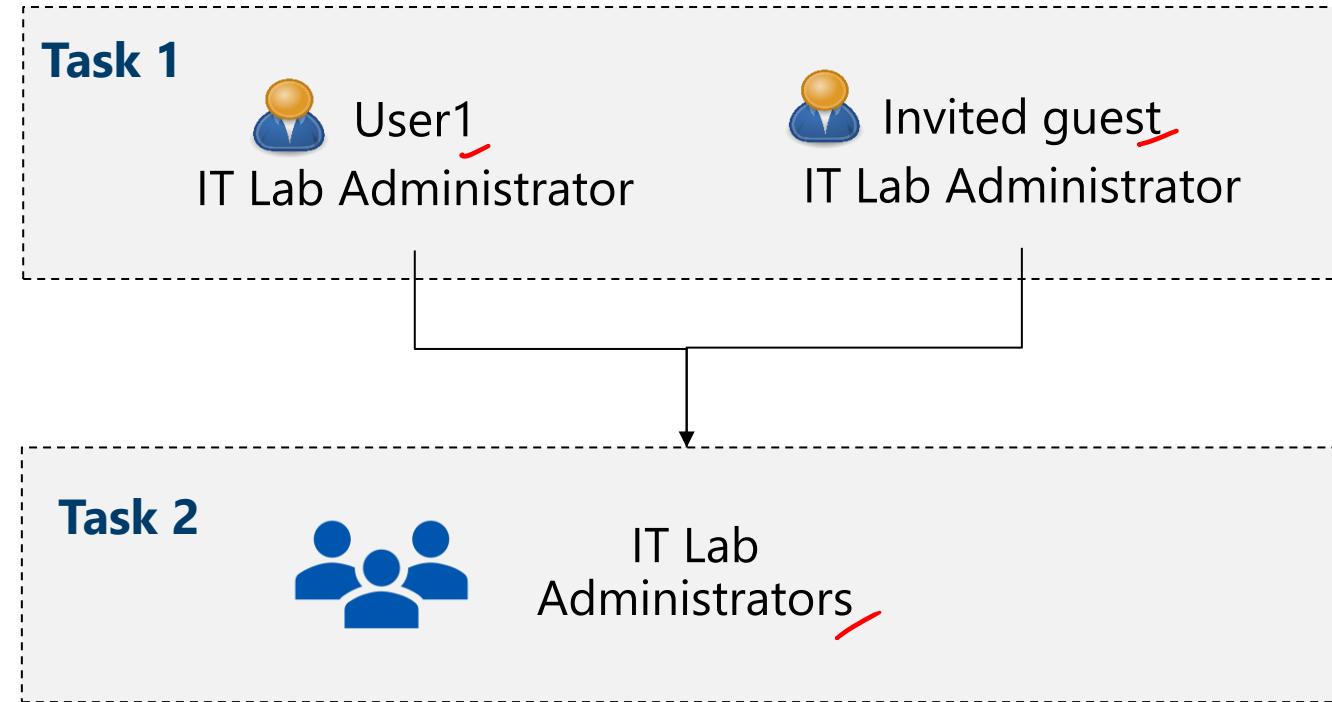


## Reference modules

- [Create, configure, and manage identities](#)
- [Manage users and groups in Microsoft Entra ID](#)

# Lab – Manage Entra ID Identities

# Lab 01 – Manage Entra ID Identities (architecture diagram)



New Tenant  
MFA

# End of presentation