**Azure Active Directory**

**What is Azure Active Directory?**

Azure Active Directory (Azure AD) is a cloud-based identity and access management service. Azure AD enables your employees access external resources, such as Microsoft 365, the Azure portal, and thousands of other SaaS applications. Azure Active Directory also helps them access internal resources like apps on your corporate intranet, and any cloud apps developed for your own organization

**Who uses Azure AD?**

IT admins use Azure AD to control access to apps and app resources, based on business requirements. For example, as an IT admin, you can use Azure AD to require multi-factor authentication when accessing important organizational resources. You could also use Azure AD to automate user provisioning between your existing Windows Server AD and your cloud apps, including Microsoft 365. Finally, Azure AD gives you powerful tools to automatically help protect user identities and credentials and to meet your access governance requirements.

App developers can use Azure AD as a standards-based authentication provider that helps them add single sign-on (SSO) to apps that works with a user's existing credentials. Developers can also use Azure AD APIs to build personalized experiences using organizational data.

**What are the Azure AD licenses?**

Microsoft Online business services, such as Microsoft 365 or Microsoft Azure, use Azure AD for sign-in activities and to help protect your identities. If you subscribe to any Microsoft Online business service, you automatically get access to Azure AD free.

To enhance your Azure AD implementation, you can also add paid features by upgrading to Azure Active Directory Premium P1 or Premium P2 licenses. Azure AD paid licenses are built on top of your existing free directory. The licenses provide self-service, enhanced monitoring, security reporting, and secure access for your mobile users.

**Azure AD Core Concepts**

**Azure AD Tenants**

An Azure AD tenant is a dedicated instance of Azure AD that represents an organization. It is a distinct identity and access management environment with its own set of users, groups, applications, and configuration settings. Each Azure AD tenant has a globally unique domain name (e.g., yourcompany.onmicrosoft.com) associated with it.

**Users and Groups**

**Users** in Azure AD represent individuals within an organization and can have various roles and permissions. Azure AD supports user management features like self-service password reset, group-based access management, and user provisioning.

**Groups** in Azure AD are used to organize and manage users and provide a convenient way to assign permissions and access rights to multiple users simultaneously. Groups can be synchronized from on-premises Active Directory or created directly in Azure AD.

**Applications and Service Principals**

In Azure AD, applications represent software services that can be accessed and used by users. Azure AD supports various types of applications, including web applications, native applications, and single-page applications.

When an application is registered in Azure AD, it is assigned a service principal. The service principal represents the application's identity within Azure AD and defines its permissions, authentication settings, and access control.

**Authentication Methods**

Azure AD supports multiple authentication methods, including:

**Password-Based Authentication:** Users can sign in to Azure AD using their username and password.

**Multi-Factor Authentication (MFA):** Azure AD offers MFA options such as SMS, phone call, mobile app notification, or hardware token verification to provide an additional layer of security.

**Federation:** Azure AD supports federation with on-premises Active Directory or other identity providers, allowing users to use their existing credentials to access Azure AD-integrated resources.

**Role-Based Access Control (RBAC):** RBAC in Azure AD enables fine-grained access management by assigning roles to users or groups, granting them specific permissions to Azure resources. This allows organizations to implement the principle of least privilege and enforce access controls based on job functions and responsibilities.

**Azure AD Authentication and Authorization**

**Overview of Authentication in Azure AD**

Azure AD offers various authentication options to secure access to resources. It supports authentication protocols like OAuth 2.0 and OpenID Connect, enabling secure sign-in and user authentication across applications. Azure AD authentication can be integrated with on-premises Active Directory through Azure AD Connect for a hybrid identity solution.

**Azure AD Connect for Hybrid Environments**

Azure AD Connect is a tool that facilitates synchronization of on-premises Active Directory with Azure AD. It ensures a unified identity experience for users, enabling them to use their existing on-premises credentials to access cloud resources. Azure AD Connect also supports password hash synchronization, pass-through authentication, and federation with Active Directory Federation Services (AD FS).

**Configuring Single Sign-On (SSO)**

Azure AD enables single sign-on, allowing users to access multiple applications and services with a single set of credentials. You can configure SSO for cloud applications using Azure AD's pre-integrated application gallery or by adding custom applications. Azure AD supports different SSO protocols such as SAML, WS-Federation, and OpenID Connect.

**Multi-Factor Authentication (MFA)**

Azure AD provides robust multi-factor authentication capabilities to enhance security. With MFA, users are required to provide additional verification, such as a phone call, SMS, mobile app notification, or biometric authentication, along with their password. This adds an extra layer of protection against unauthorized access.

**Conditional Access Policies**

Conditional Access in Azure AD allows you to define access policies based on various conditions, including user location, device compliance, risk level, and application sensitivity. You can enforce specific authentication methods or require additional security measures, providing granular control over resource access based on contextual factors.

**Azure AD Application Integration**

**Overview of Application Integration Options**

Azure AD provides various options for integrating applications, enabling secure and streamlined access management. You can integrate applications through Azure AD's pre-integrated application gallery, which offers thousands of popular SaaS applications. Additionally, you can add custom applications and configure single sign-on (SSO) using standard protocols such as SAML, OAuth 2.0, and OpenID Connect.

**Configuring Enterprise Applications**

Azure AD allows you to configure and manage enterprise applications that require user authentication and access control. You can add applications from the Azure AD application gallery or register custom applications. Configuration options include specifying application properties, defining user assignment and access policies, and setting up single sign-on.

**Implementing OAuth 2.0 and OpenID Connect**

Azure AD supports OAuth 2.0 and OpenID Connect, industry-standard protocols for secure authentication and authorization. You can leverage these protocols to enable secure sign-in and access to your applications. Azure AD acts as an OAuth 2.0 authorization server and provides endpoints for authentication and token issuance.

**Integrating with Microsoft 365 Services**

Azure AD seamlessly integrates with Microsoft 365 services, such as Exchange Online, SharePoint Online, and Microsoft Teams. This integration enables users to sign in once to Azure AD and gain access to these services without the need for separate authentication. Azure AD provides SSO capabilities for Microsoft 365 services, enhancing user productivity and simplifying access management.

**Using Azure AD App Proxy**

Azure AD App Proxy enables secure remote access to on-premises web applications and APIs. It allows you to publish these resources through Azure AD, providing external users with access while maintaining security and control. With App Proxy, you can enable SSO, enforce multi-factor authentication, and apply fine-grained access policies for on-premises applications.

**Azure AD Security and Identity Protection**

**Identity Protection Overview**

Azure AD Identity Protection provides advanced threat detection and risk-based conditional access policies to protect user identities. It analyses user sign-in and usage patterns, detects suspicious activities, and helps organizations take appropriate actions to mitigate risks. Identity Protection offers insights and recommendations to enhance security posture.

**Enforcing Password Policies**

Azure AD allows you to enforce strong password policies to ensure secure user authentication. You can configure password complexity requirements, password expiration policies, and smart lockout settings to prevent unauthorized access through weak or compromised passwords.

**Risk-Based Conditional Access Policies**

Azure AD's risk-based conditional access policies enable organizations to make access decisions based on the risk level associated with user sign-in attempts. You can define policies that require additional authentication factors, block access, or trigger step-up authentication when unusual or high-risk activities are detected.

**Privileged Identity Management (PIM)**

Azure AD Privileged Identity Management (PIM) helps manage and monitor privileged roles within an organization. It allows organizations to control and audit access to sensitive resources by enabling just-in-time (JIT) access, time-bound access, and approval workflows for privileged roles. PIM helps reduce the attack surface and enforce the principle of least privilege.

**Azure AD Identity Governance**

Azure AD Identity Governance provides capabilities for managing and governing identities in Azure AD. It includes features such as access reviews, entitlement management, and lifecycle management. These capabilities enable organizations to streamline identity lifecycle processes, enforce access governance, and ensure compliance with regulatory requirements.

**Azure AD Developer's Guide**

**Authentication and Authorization Scenarios**

Azure AD offers various authentication and authorization scenarios for developers. This section covers topics such as integrating Azure AD authentication into your applications, implementing authorization using Azure AD roles and permissions, and handling consent and permissions for accessing user data.

**Azure AD Graph API**

Azure AD Graph API is a RESTful interface that allows developers to programmatically access and manage Azure AD resources. This section covers how to authenticate requests, perform CRUD operations on users, groups, applications, and other directory objects, and utilize query capabilities to retrieve specific information from Azure AD.

**Microsoft Graph API**

Microsoft Graph API is a unified API endpoint that provides access to a vast array of Microsoft 365 services, including Azure AD. This section covers authentication and authorization for Microsoft Graph, querying and modifying Azure AD resources using Microsoft Graph, and leveraging Microsoft Graph capabilities to enhance your applications.

**Azure AD SDKs and Libraries**

Azure AD provides SDKs and libraries for various programming languages and platforms, making it easier for developers to integrate Azure AD into their applications. This section covers the available SDKs and libraries, their features, and how to use them to implement authentication, authorization, and access control in your applications.

**Pricing:**





