September 2023

Microsoft Identity and Access Administrator

www.aka.ms/pathways

Getting started

The Microsoft Identity and Access Administrator designs, implements, and operates an organization's identity and access management systems by using Azure Active Directory (Azure AD).

Overview:

- Microsoft Security, Compliance, and Identity Fundamentals
- Microsoft Security Site
- Manage Identity and Access in Azure AD
- Zero Trust: Principals and Overview

YouTube

- Playlist: Configuration and Management
- Playlist: Secure Remote Work
- Playlist: Manage and Integrate Apps Securely
- Playlist: Identity and Access Management
- Azure AD Authentication Fundamentals
- Finding the Right Identity Strategy for Your Organization with Azure AD

Microsoft Security Technical Content Library

Microsoft is committed to helping build a safer world for all. Explore this library to find learning content relevant to your needs

ACCESS

Additional Study

Implement an identity management solution:

- Understand roles in Azure Active Directory
- Configure and manage Azure Active Directory roles
- Add custom domain name to Azure Active Directory
- Configure and manage custom domains
- Configure and manage device registration
- Administrative units in Azure Active Directory
- Configure delegation by using administrative units
- Configuration in a tenant
- Configure tenant-wide setting
- Create, configure, and manage users
- Create and manage users
- Create, configure, and manage groups
- Create and manage groups
- Manage licenses

Implement and Manage External Identities:

- Manage external collaboration
- Manage external collaboration settings
- Invite external users
- Manage external user accounts
- Configure identity providers

Implement and Manage Hybrid Identity:

- Plan, design, and implement Azure Active Directory Connect (AADC)
- Getting started with Azure AD Connect using express settings
- What is password hash synchronization with Azure AD?
- Implement manage password hash synchronization (PHS)
- What is Azure Active Directory Pass-through Authentication?
- Implement manage pass-through authentication (PTA)
- Azure Active Directory Seamless Single Sign-On
- Implement and manage federation

Implement an Authentication and Access Management Solution:

- What is Azure AD Multi-Factor Authentication?
- Plan your multi-factor authentication deployment
- Configure Azure AD Multi-Factor Authentication settings
- Manage user authentication methods for Azure AD Multi-Factor Authentication

Manage User Authentication:

- Passwordless authentication options
- Administer FIDO2 and passwordless authentication methods
- Windows Hello for Business and Authentication
- Implement an authentication solution based on Windows Hello for Business
- Deploy SSPR (Self-Service Password Reset)
- Plan and deploy on-premises Azure Active Directory Password Protection
- Deploy and manage password protection
- Use tenant restrictions to manage access to SaaS cloud applications
- Implement and manage tenant restrictions

Manage Azure AD Identity Protection:

- Implement and manage user risk policy
- Enable user risk policy
- How To: Configure the Azure AD Multi-Factor Authentication registration policy
- Monitor, investigate, and remediate elevated risky users

Implement access management for apps:

- Configure how end-users consent to applications
- Implement and configure consent settings
- Discover apps via MCAS and ADFS app report
- Design and implement app management roles
- Monitor and audit access to Azure Active Directory integrated applications
- Implement token customizations
- Integrate on-premises apps by using Azure Active Directory application proxy
- Integrate custom SaaS apps for single sign-on
- Configure pre-integrated gallery SaaS apps
- What is app provisioning in Azure Active Directory?
- Implement application user provisioning

Plan and Implement an Identity Governance Strategy:

- Define a privileged access strategy for administrative users
- Configure PIM for Azure Resources
- Approve or deny requests for AAD roles in PIM
- View audit history for Azure AD roles
- Manage emergency access accounts in AAD

Monitor and Maintain Azure Active Directory:

- Analyze and investigate sign-in logs
- Analyze Azure AD activity logs with Azure Monitor logs
- How to use Azure Monitor workbooks for Azure Active Directory reports
- Configure email notifications

Role Based Certification

Identity & Access Administrator

Exam SC-300: Microsoft Identity and Access Administrator

Skills measured:

- Implement identities in Azure AD
- Implement authentication and access management
- Implement access management for applications
- Plan and implement identity governance in Azure AD

Self-Guided Learning:

- Implement an identity management solution
- Implement an Authentication and Access Management solution
- Implement Access Management for Apps
- Plan and implement an identity governance strategy

Exam Study Guide | Course Page | Exam Page | Practice Assessment

Security Documentation

YouTube Microsoft Security

Entra ID Documentation