Microsoft Identity and Access Administrator

Course SC-300 4 Day Instructor-led, Hands-on

Introduction

The Microsoft Identity and Access Administrator course explores how to design, implement, and operate an organization's identity and access management systems by using Microsoft Entra ID. Learn to manage tasks such as providing secure authentication and authorization access to enterprise applications. You will also learn to provide seamless experiences and self-service management capabilities for all users. Finally, learn to create adaptive access and governance of your identity and access management solutions ensuring you can troubleshoot, monitor, and report on your environment. The Identity and Access Administrator may be a single individual or a member of a larger team. Learn how this role collaborates with many other roles in the organization to drive strategic identity projects. The end goal is to provide you knowledge to modernize identity solutions, to implement hybrid identity solutions, and to implement identity governance.

Who Should Attend?

This course is for the Identity and Access Administrators who are planning to take the associated certification exam, or who are performing identity and access administration tasks in their day-to-day job. This course would also be helpful to an administrator or engineer that wants to specialize in providing identity solutions and access management systems for Azure-based solutions; playing an integral role in protecting an organization.

At Course Completion

Upon successful completion of this course, students will have the following skills and knowledge:

- Explain how Microsoft Defender for Endpoint can remediate risks in your environment
- Administer a Microsoft Defender for Endpoint environment
- Configure Attack Surface Reduction rules on Windows devices

Prerequisites

Before attending this course, you should have attended the following courses:

- SC-900 - Microsoft Security, Compliance, and Identity Fundamentals
- AZ-104 - Microsoft Azure Administrator

Contact ISInc for more information at 916.920.1700 or by visiting our website at http://www.isinc.com

Outline

Module 1: Explore identity in Microsoft Entra ID

- Explain the identity landscape
- Explore zero trust with identity
- Discuss identity as a control plane
- Explore why we have identity
- Define identity administration
- Contrast decentralized identity with central identity systems
- Discuss identity management solutions
- Explain Microsoft Entra Business to Business
- Compare Microsoft identity providers
- Define identity licensing
- Explore authentication
- Discuss authorization
- Explain auditing in identity

Module 2: Implement initial configuration of Microsoft Entra ID

- Configure company brand
- Configure and manage Microsoft Entra roles
- Configure delegation by using administrative units
- Analyze Microsoft Entra role permissions
- Configure and manage custom domains
- Configure tenant-wide setting

Module 3: Create, configure, and manage identities

- Create, configure, and manage users
- Create, configure, and manage groups
- Configure and manage device registration
- Manage licenses
- Create custom security attributes

Explore automatic user creation

Module 4: Implement and manage external identities

- Describe guest access and Business to Business accounts
- Manage external collaboration
- Invite external users - individually and in bulk
- Demo - manage guest users in Microsoft Entra ID
- Manage external user accounts in Microsoft Entra ID
- Manage external users in Microsoft 365 workloads
- Implement and manage Microsoft Entra Verified ID
- Configure identity providers

- Implement cross-tenant access controls

Module 5: Implement and manage hybrid identity

- Plan, design, and implement Microsoft Entra Connect
- Implement manage password hash synchronization (PHS)
- Implement manage pass-through authentication (PTA)
- Demo - Manage pass-through authentication and seamless single sign-on (SSO)
- Implement and manage federation
- Trouble-shoot synchronization errors
- Implement Microsoft Entra Connect Health
- Manage Microsoft Entra Health

Module 6: Secure Microsoft Entra users with multifactor authentication

- What is Microsoft Entra multifactor authentication?
- Plan your multifactor authentication deployment
- Configure multifactor authentication methods

Module 7: Manage user authentication

- Administer FIDO2 and passwordless authentication methods
- Explore Authenticator app and OATH tokens
- Implement an authentication solution based on Windows Hello for Business
- Deploy and manage password protection
- Configure smart lockout thresholds
- Implement Kerberos and certificate-based authentication in Microsoft Entra ID
- Configure Microsoft Entra user authentication for virtual machines

Module 8: Plan, implement, and administer Conditional Access

- Plan security defaults
- Plan Conditional Access policies
- Implement Conditional Access policy controls and assignments
- Test and troubleshoot Conditional Access policies
- Implement application controls
- Implement session management
- Implement continuous access evaluation

Module 9: Manage Microsoft Entra Identity Protection

- Review identity protection basics
- Implement and manage user risk policy
- Monitor, investigate, and remediate elevated risky users
- Implement security for workload identities

Contact ISInc for more information at 916.920.1700 or by visiting our website at http://www.isinc.com

- Explore Microsoft Defender for Identity

Module 10: Implement access management for Azure resources

- Assign Azure roles
- Configure custom Azure roles
- Create and configure managed identities
- Access Azure resources with managed identities
- Analyze Azure role permissions
- Configure Azure Key Vault RBAC policies
- Retrieve objects from Azure Key Vault
- Explore Microsoft Entra Permissions Management

Module 11: Deploy and Configure Microsoft Entra Global Secure Access

- Explore Global Secure Access
- Deploy and configure Microsoft Entra Internet Access
- Deploy and configure Microsoft Entra Private Access
- Explore how to use the Dashboard to drive Global Secure Access
- Create remote networks for use with Global Secure Access
- Use Conditional Access with Global Secure Access
- Explore logs and monitoring options with Global Secure Access

Module 12: Plan and design the integration of enterprise apps for SSO

- Discover apps by using Microsoft Defender for Cloud Apps and Active Directory Federation Services app report
- Configure connectors to apps
- Design and implement app management roles
- Configure preintegrated gallery SaaS apps
- Implement and manage policies for OAuth apps

Module 13: Implement and monitor the integration of enterprise apps for SSO

- Implement token customizations
- Implement and configure consent settings
- Integrate on-premises apps with Microsoft Entra application proxy
- Integrate custom SaaS apps for single sign-on
- Implement application-based user provisioning
- Monitor and audit access to Microsoft Entra integrated enterprise applications
- Create and manage application collections

Contact ISInc for more information at 916.920.1700 or by visiting our website at http://www.isinc.com

Module 14: Implement app registration

- Plan your line of business application registration strategy
- Implement application registration
- Register an application
- Configure permission for an application
- Grant tenant-wide admin consent to applications
- Implement application authorization
- Manage and monitor application by using app governance

Module 15: Register apps using Microsoft Entra ID

- Plan for app registration
- Explore application objects and service principals
- Create app registrations
- Configure app authentication
- Configure API permissions
- Create app roles

Module 16: Plan and implement entitlement management

- Define access packages
- Configure entitlement management
- Configure and manage connected organizations
- Review per-user entitlements

Module 17: Plan, implement, and manage access review

- Plan for access reviews
- Create access reviews for groups and apps
- Create and configure access review programs
- Monitor access review findings
- Automate access review management tasks
- Configure recurring access reviews

Module 18: Plan and implement privileged access

- Define a privileged access strategy for administrative users
- Configure Privileged Identity Management for Azure resources
- Plan and configure Privileged Access Groups
- Analyze Privileged Identity Management audit history and reports
- Create and manage emergency access accounts

Module 19: Monitor and maintain Microsoft Entra ID

- Analyze and investigate sign-in logs to troubleshoot access issues
- Review and monitor Microsoft Entra audit logs

- Export logs to third-party security information and event management system
- Analyze Microsoft Entra workbooks and reporting
- Monitor security posture with Identity Secure Score

Module 20: Explore the many features of Microsoft Entra Permissions Management

- A comprehensive experience for all cloud environments
- Get high level insights in the Permissions Management dashboard
- Dive deeper with the Analytics tab
- Develop a better understanding of your environment with reports
- Analyze historical data with the Audit tab
- Act on your findings with the Permissions Management Remediation tab
- Take a more proactive approach to managing with continuous monitoring
- Manage access to Microsoft Entra Permissions Management
- Putting it all together