MS-SC300T00: MICROSOFT IDENTITY AND ACCESS ADMINISTRATOR

DURATION	LEVEL	TECHNOLOGY	DELIVERY METHOD	TRAINING CREDITS
4 Days	Intermediate	Security	Instructor-led	NA

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.

AUDIENCE PROFILE

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.

PREREQUISITES

Before attending this course, students should have:

- Security best practices and industry security requirements such as defence in depth, least privileged access, shared responsibility, and zero trust model.
- Familiarity with identity concepts such as authentication, authorization, and active directory.
- Experience deploying Azure workloads. This course does not cover the basics of Azure administration, instead the course content builds on that knowledge by adding security specific information.
- Experience with Windows and Linux operating systems and scripting languages is helpful but not required. Course labs may use PowerShell and the CLI.

COURSE OBJECTIVES

After completing this course, students will be able to:

- Implement an identity management solution
- Implement an authentication and access management solutions
- Implement access management for apps
- Plan and implement an identity governancy strategy

COURSE CONTENT

Module 1: Explore identity in Microsoft Entra ID

This module covers definitions and available services for identity, provided in Microsoft Entra ID. Explore authentication, authorization, and access tokens, then build into full identity solutions.

Lessons

- Introduction
- 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
- Knowledge check
- Summary

After completing this module, students will be able to:

- Define common identity terms and explain how they're used in the Microsoft Cloud
- Explore the common management tools and needs of an identity solution
- Review the goal of Zero Trust and how it's applied in the Microsoft Cloud
- Explore the available identity services in the Microsoft Cloud

Module 2: Implement initial configuration of Microsoft Entra ID

Learn to create an initial Microsoft Entra ID configuration to ensure all the identity solutions available in Azure are ready to use. This module explores how to build and configure a Microsoft Entra system.

Lessons

- Introduction
- Configure company brand
- Configure and manage Microsoft Entra roles

- Exercise manage users roles
- Configure delegation by using administrative units
- Analyze Microsoft Entra role permissions
- Configure and manage custom domains
- Configure tenant-wide setting
- Exercise - setting tenant-wide properties
- Knowledge check
- Summary and resources

After completing this module, students will be able to:

- Implement initial configuration of Microsoft Entra ID.
- Create, configure, and manage identities.
- Implement and manage external identities (excluding B2C scenarios).
- Implement and manage hybrid identity.

Module 3: Create, configure, and manage identities

Access to cloud-based workloads needs to be controlled centrally by providing a definitive identity for each user and resource. You can ensure employees and vendors have just enough access to do their job.

- Introduction
- Create, configure, and manage users
- Exercise - assign licenses to users
- Exercise - restore or remove deleted users
- Create, configure, and manage groups
- Exercise - add groups in Microsoft Entra ID
- Configure and manage device registration
- Manage licenses
- Exercise - change group license assignments
- Exercise - change user license assignments
- Create custom security attributes
- Explore automatic user creation
- Knowledge check
- Summary and resources

After completing this module, students will be able to:

- Create, configure, and manage users
- Create, configure, and manage groups
- Manage licenses
- Explain custom security attributes and automatic user provisioning

Module 4: Implement and manage external identities

Inviting external users to use company Azure resources is a great benefit, but you want to do it in a secure way. Explore how to enable secure external collaboration.

Lessons

- Introduction
- Describe guest access and Business to Business accounts
- Manage external collaboration
- Exercise - configure external collaboration
- Invite external users - individually and in bulk
- Exercise - add guest users to directory
- Exercise - invite guest user's bulk
- Demo - manage guest users in Microsoft Entra ID
- Manage external user accounts in Microsoft Entra ID
- Manage external users in Microsoft 365 workloads
- Exercise - explore dynamic groups
- Implement and manage Microsoft Entra Verified ID
- Configure identity providers
- Implement cross-tenant access controls
- Knowledge check
- Summary and resources

After completing this module, students will be able to:

- Manage external collaboration settings in Microsoft Entra ID
- Invite external users (individually or in bulk)
- Manage external user accounts in Microsoft Entra ID
- Configure identity providers (social and SAML/WS-fed)

Module 5: Implement and manage hybrid identity

Creating a hybrid-identity solution to use your on-premises active directory can be challenging. Explore how to implement a secure hybrid-identity solution.

Lessons

- Introduction
- 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
- Knowledge check
- Summary and resources

After completing this module, students will be able to:

- Plan, design, and implement Microsoft Entra Connect
- Manage Microsoft Entra Connect
- Manage password hash synchronization (PHS)
- Manage pass-through authentication (PTA)
- Manage seamless single sign-on (seamless SSO)
- Manage federation excluding manual ADFS deployments
- Troubleshoot synchronization errors
- Implement and manage Microsoft Entra Connect Health

Module 6: Secure Microsoft Entra users with multifactor authentication

Learn how to use multifactor authentication with Microsoft Entra ID to harden your user accounts.

- Introduction
- What is Microsoft Entra multifactor authentication?
- Plan your multifactor authentication deployment
- Exercise - Enable Microsoft Entra multifactor authentication
- Configure multi-factor authentication methods
- Summary

After completing this module, students will be able to:

- Learn about Microsoft Entra multifactor authentication
- Create a plan to deploy Microsoft Entra multifactor authentication
- Turn on Microsoft Entra multifactor authentication for users and specific apps

Module 7: Manage user authentication

There are multiple options for authentication in Microsoft Entra ID. Learn how to implement and manage the right authentications for users based on business needs.

Lessons

- Introduction
- Administer FIDO2 and passwordless authentication methods
- Explore Authenticator app and OATH tokens
- Implement an authentication solution based on Windows Hello for Business
- Exercise configure and deploy self-service password reset
- Deploy and manage password protection
- Configure smart lockout thresholds
- Exercise - Manage Microsoft Entra smart lockout values
- Implement Kerberos and certificate-based

authentication in Microsoft Entra ID
- Configure Microsoft Entra user authentication for virtual machines
- Knowledge check
- Summary and resources

After completing this module, students will be able to:
- Administer authentication methods (FIDO2 / Passwordless)
- Implement an authentication solution based on Windows Hello for Business
- Configure and deploy self-service password reset
- Deploy and manage password protection
- Implement and manage tenant restrictions

Module 8: Plan, implement, and administer Conditional Access

Conditional Access gives a fine granularity of control over which users can do specific activities, access which resources, and how to ensure data and systems are safe.

Lessons
- Introduction
- Plan security defaults
- Exercise - Work with security defaults
- Plan Conditional Access policies
- Implement Conditional Access policy controls and assignments
- Exercise - Implement Conditional Access policies roles and assignments
- Test and troubleshoot Conditional Access policies
- Implement application controls
- Implement session management
- Exercise - Configure authentication session controls
- Implement continuous access evaluation
- Knowledge check
- Summary and resources

After completing this module, students will be able to:
- Plan and implement security defaults.
- Plan conditional access policies.
- Implement conditional access policy controls and assignments (targeting, applications, and conditions).
- Test and troubleshoot conditional access policies.
- Implement application controls.
- Implement session management.
- Configure smart lockout thresholds.

Module 9: Manage Microsoft Entra Identity Protection

Protecting a user's identity by monitoring their usage and sign-in patterns ensure a secure cloud solution. Explore how to design and implement Microsoft Entra Identity protection.
- Introduction
- Review identity protection basics
- Implement and manage user risk policy
- Exercise enable sign-in risk policy
- Exercise configure Microsoft Entra multifactor authentication registration policy
- Monitor, investigate, and remediate elevated risky users
- Implement security for workload identities
- Explore Microsoft Defender for Identity
- Knowledge check
- Summary and resources

After completing this module, students will be able to:
- Implement and manage a user risk policy.
- Implement and manage sign-in risk policies.
- Implement and manage MFA registration policy.
- Monitor, investigate, and remediate elevated risky users.

Module 10: Implement access management for Azure resources

Explore how to use built-in Azure roles, managed identities, and RBAC-policy to control access to Azure resources. Identity is the key to secure solutions.

Lessons
- Introduction
- 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
- Knowledge check
- Summary and resources

After completing this module, students will be able to:
- Configure and use Azure roles within Microsoft Entra ID
- Configure and managed identity and assign it to Azure resources
- Analyze the role permissions granted to or inherited by a user
- Configure access to data in Azure Key Vault using RBAC-policy

Module 11: Deploy and Configure Microsoft Entra Global Secure Access

Global Secure Access lets you put identity as the gatekeeper to your network access. Use Zero Trust principles to protect your data and apps.

Lessons
- Introduction
- 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
- Knowledge check
- Summary and resources

After completing this module, students will be able to:
- Define Global Secure Access and its components.
- Explore deployment and configuration of Microsoft Entra Internet Access.
- Explore deployment and configuration of Microsoft Entra Private Access.
- Use the Global Secure Access Dashboard to monitor your systems.
- Configure Remote Networks.
- Create Conditional Access policies to protect your networks, data, and applications.

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

Enterprise app deployment enables control over which users can access the apps, easily log into apps with single-sign-on, and provide integrated usage reports.

Lessons
- Introduction
- Discover apps by using Microsoft Defender for Cloud Apps and Active Directory
- Federation Services app report
- Configure connectors to apps
- Exercise implement access management for apps

- Design and implement app management roles
- Exercise create a custom role to manage app registration
- Configure preintegrated gallery SaaS apps
- Implement and manage policies for OAuth apps
- Knowledge check
- Summary and resources

After completing this module, students will be able to:

- Discover apps by using Defender for Cloud Apps or ADFS app report.
- Design and implement access management for apps.
- Design and implement app management roles.
- Configure preintegrated (gallery) SaaS apps.

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

Deploying and monitoring enterprise applications to Azure solutions can ensure security. Explore how to deploy on-premises and cloud-based apps to users.

Lessons

- Introduction
- 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
- Knowledge check
- Summary and resources

After completing this module, students will be able to:

- Implement token customizations
- Implement and configure consent settings
- Integrate on-premises apps by using Microsoft Entra application proxy
- Integrate custom SaaS apps for SSO
- Implement application user provisioning
- Monitor and audit access/Sign-On to Microsoft Entra ID integrated enterprise applications

Module 14: Implement app registration

Line of business developed in-house need registration in Microsoft Entra ID and assigned to users for a secure Azure solution. Explore how to implement app registration.

Lessons

- Introduction
- 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
- Exercise add app roles to an application and receive tokens
- Manage and monitor application by using app governance
- Knowledge check
- Summary and resources

After completing this module, students will be able to:

- Plan your line of business application registration strategy
- Implement application registrations
- Configure application permissions
- Plan and configure multi-tier application permissions

Module 15: Register apps using Microsoft Entra ID

Explore the value and configuration options when registering an app in Microsoft Entra, to ensure your data and infrastructure is protected.

Lessons

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

After completing this module, students will be able to:

- Explain the benefits of registering apps in Microsoft Entra ID
- Compare and contrast single and multitenant apps
- Describe what happens and the primary settings when registering an app
- Describe the relationship between application objects and service principals

Module 16: Plan and implement entitlement management

When new users or external users join your site, quickly assigning them access to Azure solutions is a must. Explore how to entitle users to access your site and resources.

Lessons

- Introduction
- Define access packages
- Exercise create and manage a resource catalog with Microsoft Entra entitlement
- management
- Configure entitlement management
- Exercise add terms of use acceptance report
- Exercise manage the lifecycle of external users with Microsoft Entra identity governance
- Configure and manage connected organizations
- Review per-user entitlements
- Knowledge check
- Summary and resources

After completing this module, students will be able to:

- Define catalogs.
- Define access packages.
- Plan, implement and manage entitlements.
- Implement and manage terms of use.
- Manage the lifecycle of external users in Microsoft Entra Identity Governance settings.

Module 17: Plan, implement, and manage access review

Once identity is deployed, proper governance using access reviews is necessary for a secure solution. Explore how to plan for and implement access reviews.

Lessons

- Introduction
- 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
- Knowledge check
- Summary and resources

After completing this module, students will be able to:

- Plan for access reviews
- Create access reviews for groups and apps
- Monitor the access review findings
- Manage licenses for access reviews
- Automate management tasks for access review
- Configure recurring access reviews

Module 18: Plan and implement privileged access

Ensuring that administrative roles are protected and managed to increase your Azure solution security is a must. Explore how to use PIM to protect your data and resources.

Lessons

- Introduction
- Define a privileged access strategy for administrative users
- Configure Privileged Identity Management for Azure resources
- Exercise configure Privileged Identity Management for Microsoft Entra roles
- Exercise assign Microsoft Entra roles in Privileged Identity Management
- Exercise assign Azure resource roles in Privileged Identity Management
- Plan and configure Privileged Access Groups
- Analyze Privileged Identity Management audit history and reports
- Create and manage emergency access accounts
- Knowledge check
- Summary and resources

After completing this module, students will be able to:

- Define a privileged access strategy for administrative users (resources, roles, approvals, and thresholds)
- Configure Privileged Identity Management for Microsoft Entra roles
- Configure Privileged Identity Management for Azure resources
- Assign roles
- Manage PIM requests
- Analyze PIM audit history and reports
- Create and manage emergency access accounts

Module 19: Monitor and maintain Microsoft Entra ID

Audit and diagnostic logs within Microsoft Entra ID provide a rich view into how users are accessing your Azure solution. Learn to monitor, troubleshoot, and analyze sign-in data.

Lessons

- Introduction
- Analyze and investigate sign-in logs to troubleshoot access issues
- Review and monitor Microsoft Entra audit logs
- Exercise connect data from Microsoft Entra ID to Microsoft Sentinel
- Export logs to third-party security information and event management system
- Analyze Microsoft Entra workbooks and reporting
- Monitor security posture with Identity Secure Score
- Knowledge check
- Summary and resources

After completing this module, students will be able to:

- Analyze and investigate sign in logs to troubleshoot access issues
- Review and monitor Microsoft Entra audit logs
- Enable and integrate Microsoft Entra diagnostic logs with Log Analytics / Azure Sentinel
- Export sign in and audit logs to a third-party SIEM (security information and event management)
- Review Microsoft Entra activity by using Log Analytics / Azure Sentinel, excluding KQL (Kusto Query Language) use
- Analyze Microsoft Entra workbooks / reporting
- Configure notifications

ASSOCIATED CERTIFICATIONS & EXAM

This course will prepare delegates to write the Microsoft SC-300: Microsoft Identity and Access Administrator exam.