SC-300T00: Microsoft Identity and Access Administrator

Course Details

Course Code: SC-300T00

Duration: 4 days

Notes:

- This course syllabus should be used to determine whether the course is appropriate for the students, based on their current skills and technical training needs.
- Course content, prices, and availability are subject to change without notice.
- Terms and Conditions apply

Academy IT Pty Ltd
Level 4, 45 Grenfell Street
ADELAIDE 5000

Email: sales@academyit.com.au
Web: www.academyit.com.au

Phone: 08 7324 9800
Brian: 0400 112 083

Elements of this syllabus are subject to change.

About this course

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.

Explore identity in Microsoft Entra ID

This module covers definitions and available services for identity provided in Microsoft Entra ID and to Microsoft 365. You start with authentication, authorization, and access tokens then build into full identity solutions.

Learning objectives

By the end of this module, you'll 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

Implement initial configuration of Microsoft Entra ID

Learn to create an initial Azure Active Directory configuration to ensure all the identity solutions available in Azure are ready to use. This module explores how to build and configure an Azure AD system.

Learning objectives

By the end of this module, you will be able to:

- Implement initial configuration of Azure Active Directory
- Create, configure, and manage identities
- Implement and manage external identities (excluding B2C scenarios)
- Implement and manage hybrid identity

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.

Learning objectives

At the end of this module, you'll be able to:

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

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.

Learning objectives

By the end of this module, you 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)

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.

Learning objectives

By the end of this module, you 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

Secure Microsoft Entra users with multifactor authentication

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

Learning objectives

In this module, you will:

- Learn about Microsoft Entra multifactor authentication (Microsoft Entra multifactor authentication)

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

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.

Learning objectives

By the end of this module, you 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

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.

Learning objectives

By the end of this module, you 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.

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.

Learning objectives

By the end of this module, you are 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

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.

Learning objectives

By the end of this module, you 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

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.

Learning objectives

By the end of this module, you're 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.

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.

Learning objectives

By the end of this module, you 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

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.

Learning objectives

By the end of this module, you 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

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.

Learning objectives

By the end of this module, you 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.

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.

Learning objectives

By the end of this module, you 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

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.

Learning objectives

By the end of this module, you 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

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.

Learning objectives

By the end of this module, you'll 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