MICROSOFT IDENTITY AND ACCESS ADMINISTRATOR (SC-300T00)

Course Code: 821304

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.

What You'll Learn

Students will learn to,

- Explore identity in Microsoft Entra ID
- SC-300: Implement an identity management solution
- SC-300: Implement an Authentication and Access Management solution
- SC-300: Implement Access Management for Apps
- SC-300: Plan and implement an identity governance strategy

Who Needs to 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.

skillsoft global knowledge™

MICROSOFT IDENTITY AND ACCESS ADMINISTRATOR (SC-300T00)

Course Code: 821304

CLASSROOM LIVE	$2,595 CAD	4 Day

Classroom Live Outline

Module 1 : Explore identity in Microsoft Entra ID

- 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 : SC-300: Implement an identity management solution

- Implement initial configuration of Microsoft Entra ID
- Create, configure, and manage identities
- Implement and manage external identities
- Implement and manage hybrid identity

Module 3: SC-300: Implement an Authentication and Access Management solution

- Secure Microsoft Entra users with multifactor authentication
- Manage user authentication
- Plan, implement, and administer Conditional Access
- Manage Microsoft Entra Identity Protection
- Implement access management for Azure resources
- Deploy and Configure Microsoft Entra Global Secure Access

Module 4: SC-300: Implement Access Management for Apps

- Plan and design the integration of enterprise apps for SSO
- Implement and monitor the integration of enterprise apps for SSO
- Implement app registration
- Register apps using Microsoft Entra ID

Module 5: SC-300: Plan and implement an identity governance strategy

- Plan and implement entitlement management
- Plan, implement, and manage access review
- Plan and implement privileged access
- Monitor and maintain Microsoft Entra ID
- Explore the many features of Microsoft Entra Permissions Management

Classroom Live Labs

- Lab : Manage user roles
- Lab : Working with tenant properties
- Lab : Assigning license using group membership
- Lab : Configure external collaboration settings
- Lab : Add guest users to the directory
- Lab : Add a federated identity provider
- Lab : Add hybrid identity with Azure AD Connect
- Lab : Enable sign-in and user-risk policies
- Lab : Configure an Azure AD Multi-factor Authentication registration policy
- Lab : Use Azure Key Vault for managed identities
- Lab : Implement and test a conditional access policy
- Lab : Manage Azure AD smart lockout values
- Lab : Assign Azure resource roles in Privileged Identity Management
- Lab : Azure AD authentication for Windows and Linux virtual machines
- Lab : Enable Azure AD self-service password reset
- Lab : Enable Azure AD Multi-factor Authentication
- Lab : Defender for Cloud Apps access policies
- Lab : Register an application
- Lab : Implement access management for apps
- Lab : Grant tenant-wide admin consent to an application
- Lab : Create access reviews for internal and external users
- Lab : Manage the lifecycle of external users in Azure AD Identity Governance settings
- Lab : Add terms of use and acceptance reporting
- Lab : Create and manage a catalog of resources in Azure AD entitlement management
- Lab : Configure Privileged Identity Management (PIM) for Azure AD roles
- Lab : Explore Microsoft Sentinel and use Kusto Queries for reviewing Azure AD data sources
- Lab : Monitor and manage your security posture with Identity Secure Score

skillsoft global knowledge™

MICROSOFT IDENTITY AND ACCESS ADMINISTRATOR (SC-300T00)

Course Code: 821304

VIRTUAL CLASSROOM LIVE	$2,595 CAD	4 Day

Virtual Classroom Live Outline

Module 1 : Explore identity in Microsoft Entra ID

- 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 : SC-300: Implement an identity management solution

- Implement initial configuration of Microsoft Entra ID
- Create, configure, and manage identities
- Implement and manage external identities
- Implement and manage hybrid identity

Module 3: SC-300: Implement an Authentication and Access Management solution

- Secure Microsoft Entra users with multifactor authentication
- Manage user authentication
- Plan, implement, and administer Conditional Access
- Manage Microsoft Entra Identity Protection
- Implement access management for Azure resources
- Deploy and Configure Microsoft Entra Global Secure Access

Module 4: SC-300: Implement Access Management for Apps

- Plan and design the integration of enterprise apps for SSO
- Implement and monitor the integration of enterprise apps for SSO
- Implement app registration
- Register apps using Microsoft Entra ID

Module 5: SC-300: Plan and implement an identity governance strategy

- Plan and implement entitlement management
- Plan, implement, and manage access review
- Plan and implement privileged access
- Monitor and maintain Microsoft Entra ID
- Explore the many features of Microsoft Entra Permissions Management

Virtual Classroom Live Labs

- Lab : Manage user roles
- Lab : Working with tenant properties
- Lab : Assigning license using group membership
- Lab : Configure external collaboration settings
- Lab : Add guest users to the directory
- Lab : Add a federated identity provider
- Lab : Add hybrid identity with Azure AD Connect
- Lab : Enable sign-in and user-risk policies
- Lab : Configure an Azure AD Multi-factor Authentication registration policy
- Lab : Use Azure Key Vault for managed identities
- Lab : Implement and test a conditional access policy
- Lab : Manage Azure AD smart lockout values
- Lab : Assign Azure resource roles in Privileged Identity Management
- Lab : Azure AD authentication for Windows and Linux virtual machines
- Lab : Enable Azure AD self-service password reset
- Lab : Enable Azure AD Multi-factor Authentication
- Lab : Defender for Cloud Apps access policies
- Lab : Register an application
- Lab : Implement access management for apps
- Lab : Grant tenant-wide admin consent to an application
- Lab : Create access reviews for internal and external users
- Lab : Manage the lifecycle of external users in Azure AD Identity Governance settings
- Lab : Add terms of use and acceptance reporting
- Lab : Create and manage a catalog of resources in Azure AD entitlement management
- Lab : Configure Privileged Identity Management (PIM) for Azure AD roles
- Lab : Explore Microsoft Sentinel and use Kusto Queries for reviewing Azure AD data sources
- Lab : Monitor and manage your security posture with Identity Secure Score

May 27 - 30, 2025 | 9:00 AM - 5:00 PM EDT

Jun 2 - 5, 2025 | 9:00 AM - 5:00 PM EDT

Jun 23 - 26, 2025 | 9:00 AM - 5:00 PM EDT

Jul 7 - 10, 2025 | 9:00 AM - 5:00 PM EDT

Aug 4 - 7, 2025 | 9:00 AM - 5:00 PM EDT

Sep 15 - 18, 2025 | 9:00 AM - 5:00 PM EDT

Oct 13 - 16, 2025 | 9:00 AM - 5:00 PM EDT

Nov 17 - 20, 2025 | 9:00 AM - 5:00 PM EST

Dec 1 - 4, 2025 | 12:00 - 8:00 PM EST

Dec 8 - 11, 2025 | 9:00 AM - 5:00 PM EST

MICROSOFT IDENTITY AND ACCESS ADMINISTRATOR (SC-300T00)

Course Code: 821304

PRIVATE GROUP TRAINING	4 Day

Visit us at www.globalknowledge.com or call us at 1-866-716-6688.

Date created: 4/24/2025 10:29:02 PM