Microsoft Identity and Access Administrator (SC-300T00)

COURSE OVERVIEW

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 the knowledge to modernize identity solutions, to implement hybrid identity solutions, and to implement identity governance.

WHO WILL BENEFIT FROM THIS COURSE?

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 who 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 an understanding of:

- Security best practices and industry security requirements such as defense in depth, least privileged access, shared responsibility, and zero trust model.
- Be familiar with identity concepts such as authentication, authorization, and active directory.
- Have some 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.
- Some 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

Students will learn to:

- Explore identity in Microsoft Entra ID
- Implement initial configuration of Microsoft Entra ID
- Create, configure, and manage identities
- Implement and manage external identities
- Implement and manage hybrid identity
- 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
- Plan and design the integration of enterprise apps for SSO
- Implement and monitor the integration of enterprise apps for SSO
- Implement app registration
- Plan and implement entitlement management
- Plan, implement, and manage access review
- Plan and implement privileged access
- Monitor and maintain Microsoft Entra ID

COURSE 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: Implement initial configuration of Microsoft Entra ID

- 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

Module 3: Create, configure, and manage identities

- 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

- 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

- 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 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

- 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

- 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

- 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

- Configure and use Azure roles within Microsoft Entra ID
- Configure and manage 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: Plan and design the integration of enterprise apps for SSO

- 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 12: Implement and monitor the integration of enterprise apps for SSO

- 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 13: Implement app registration

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

Module 14: Plan and implement entitlement management

- 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 15: Plan, implement, and manage access review

- 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 16: Plan and implement privileged access

- 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 17: Monitor and maintain Microsoft Entra ID

- 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

WHY TRAIN WITH SUNSET LEARNING INSTITUTE?

Sunset Learning Institute (SLI) has been an innovative leader in developing and delivering authorized technical training since 1996. Our goal is to help our customers optimize their technology Investments by providing convenient, high quality technical training that our customers can rely on. We empower students to master their desired technologies for their unique environments.

What sets SLI apart is not only our immense selection of trainings options, but our convenient and consistent delivery system. No matter how complex your environment is or where you are located, SLI is sure to have a training solution that you can count on!

Premiere World Class Instruction Team

- All SLI instructors have a four-year technical degree, instructor level certifications and field consulting work experience
- Sunset Learning has won numerous Instructor Excellence and Instructor Quality Distinction awards since 2012

Enhanced Learning Experience

- The goal of our instructors during class is ensure students understand the material, guide them through our labs and encourage questions and interactive discussions.

Convenient and Reliable Training Experience

- You have the option to attend classes live with the instructor, at any of our established training facilities, or from the convenience of your home or office
- All Sunset Learning Institute classes are guaranteed to run – you can count on us to deliver the training you need when you need it!

Outstanding Customer Service

- You will work with a dedicated account manager to suggest the optimal learning path for you and/or your team
- An enthusiastic student services team is available to answer any questions and ensure a quality training experience

Interested in Private Group Training?

Contact Us