Course duration

- 4 days

Course Benefits

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

Microsoft Certified Partner

Webucator is a Microsoft Certified Partner for Learning Solutions (CPLS). This class uses official Microsoft courseware and will be delivered by a Microsoft Certified Trainer (MCT).

Course Outline

1. Implement an identity management solution
    1. Implement Initial configuration of Azure AD
    2. Create, configure, and manage identities
    3. Implement and manage external identities
    4. Implement and manage hybrid identity
    5. Lab: Manage user roles
    6. Lab: Setting tenant-wide properties
    7. Lab: Assign licenses to users
2. Implement an authentication and access management solution
    1. Secure Azure AD user with MFA
    2. Manage user authentication
    3. Plan, implement, and administer conditional access
    4. Manage Azure AD identity protection
    5. Lab: Enable Azure AD MFA
    6. Lab: Configure and deploy self-service password reset (SSPR)
    7. Lab: Work with security defaults
    8. Lab: Implement conditional access policies, roles, and assignments
    9. Lab: Configure authentication session controls
    10. Lab: Manage Azure AD smart lockout values
    11. Lab: Enable sign-in risk policy
    12. Lab: Configure Azure AD MFA authentication registration policy
3. Implement access management for Apps

    1. Plan and design the integration of enterprise for SSO
    2. Implement and monitor the integration of enterprise apps for SSO
    3. Implement app registration
    4. Lab: Implement access management for apps
    5. Lab: Create a custom role to management app registration
    6. Lab: Register an application
    7. Lab: Grant tenant-wide admin consent to an application
    8. Lab: Add app roles to applications and receive tokens
4. Plan and implement an identity governancy strategy
    1. Plan and implement entitlement management
    2. Plan, implement, and manage access reviews
    3. Plan and implement privileged access
    4. Monitor and maintain Azure AD
    5. Lab: Create and manage a resource catalog with Azure AD entitlement
    6. Lab: Add terms of use acceptance report
    7. Lab: Manage the lifecycle of external users with Azure AD identity governance
    8. Lab: Create access reviews for groups and apps
    9. Lab: Configure PIM for Azure AD roles
    10. Lab: Assign Azure AD role in PIM
    11. Lab: Assign Azure resource roles in PIM
    12. Lab: Connect data from Azure AD to Azure Sentinel

Class Materials

Each student will receive a comprehensive set of materials, including course notes and all the class examples.

Class Prerequisites

Experience in the following *is required* for this Microsoft Security class:

- 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.