## Course duration

- 4 days

## Course Benefits

- Learn to administer user and group access in Microsoft 365.
- Learn to explain and manage Azure Identity Protection.
- Learn to plan and implement Azure AD Connect.
- Learn to manage synchronized user identities.
- Learn to explain and use conditional access.
- Learn to describe cyber-attack threat vectors.
- Learn to explain security solutions for Microsoft 365.
- Learn to use Microsoft Secure Score to evaluate and improve your security posture.
- Learn to configure various advanced threat protection services for Microsoft 365.
- Learn to plan for and deploy secure mobile devices.
- Learn to implement information rights management.
- Learn to secure messages in Office 365.
- Learn to configure Data Loss Prevention policies.
- Learn to deploy and manage Cloud App Security.
- Learn to implement Windows information protection for devices.
- Learn to plan and deploy a data archiving and retention system.
- Learn to create and manage an eDiscovery investigation.
- Learn to manage GDPR data subject requests.
- Learn to explain and use sensitivity labels.

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. User and Group Management
    1. Identity and Access Management concepts
    2. The Zero Trust model
    3. Plan your identity and authentication solution
    4. User accounts and roles
    5. Password Management
    6. Lab: Initialize your tenant - users and groups

      1. Set up your Microsoft 365 tenant
      2. Manage users and groups
   7. Lab: Password management
      1. Configure Self-service password reset (SSPR) for user accounts in Azure AD
      2. Deploy Azure AD Smart Lockout
2. Identity Synchronization and Protection
   1. Plan directory synchronization
   2. Configure and manage synchronized identities
   3. Azure AD Identity Protection
   4. Lab: Implement Identity Synchronization
      1. Set up your organization for identity synchronization
3. Identity and Access Management
   1. Application Management
   2. Identity Governance
   3. Manage device access
   4. Role Based Access Control (RBAC)
   5. Solutions for external access
   6. Privileged Identity Management
   7. Lab: Use Conditional Access to enable MFA
      1. MFA Authentication Pilot (require MFA for specific apps)
      2. MFA Conditional Access (complete an MFA roll out)
   8. Lab: Configure Privileged Identity Management
      1. Manage Azure resources
      2. Assign directory roles
      3. Activate and deactivate PIM roles
      4. Directory roles
      5. PIM resource workflows
      6. View audit history for Azure AD roles in PIM
4. Security in Microsoft 365
   1. Threat vectors and data breaches
   2. Security strategy and principles
   3. Microsoft security solutions
   4. Secure Score
   5. Lab: Use Microsoft Secure Score
      1. Improve your secure score in the Microsoft 365 Security Center
5. Threat Protection
   1. Exchange Online Protection (EOP)
   2. Microsoft Defender for Office 365
   3. Manage Safe Attachments
   4. Manage Safe Links
   5. Microsoft Defender for Identity
   6. Microsoft Defender for Endpoint
   7. Lab: Manage Microsoft 365 Security Services
      1. Implement Microsoft Defender Policies
6. Threat Management
   1. Security dashboard

   2. Threat investigation and response
   3. Azure Sentinel
   4. Advanced Threat Analytics
   5. Lab: Using Attack Simulator
      1. Conduct a simulated Spear phishing attack
      2. Conduct simulated password attacks
7. Microsoft Cloud Application Security
   1. Deploy Cloud Application Security
   2. Use cloud application security information
8. Mobility
   1. Mobile Application Management (MAM)
   2. Mobile Device Management (MDM)
   3. Deploy mobile device services
   4. Enroll devices to Mobile Device Management
   5. Lab: Device Management
      1. Enable Device Management
      2. Configure Azure AD for Intune
      3. Create compliance and conditional access policies
9. Information Protection and Governance
   1. Information protection concepts
   2. Governance and Records Management
   3. Sensitivity labels
   4. Archiving in Microsoft 365
   5. Retention in Microsoft 365
   6. Retention policies in the Microsoft 365 Compliance Center
   7. Archiving and retention in Exchange
   8. In-place records management in SharePoint
   9. Lab: Archiving and Retention
      1. Initialize compliance
      2. Configure retention tags and policies
10. Rights Management and Encryption
    1. Information Rights Management (IRM)
    2. Secure Multipurpose Internet Mail Extension (S-MIME)
    3. Office 365 Message Encryption
    4. Lab: Configure Office 365 Message Encryption
       1. Configure Office 365 Message Encryption
       2. Validate Information Rights Management
11. Data Loss Prevention
    1. Data loss prevention fundamentals
    2. Create a DLP policy
    3. Customize a DLP policy
    4. Create a DLP policy to protect documents
    5. Policy tips
    6. Lab: Implement Data Loss Prevention policies
       1. Manage DLP Policies
       2. Test MRM and DLP Policies
12. Compliance Management

    1. Compliance center
13. Insider Risk Management
    1. Insider Risk
    2. Privileged Access
    3. Information barriers
    4. Building ethical walls in Exchange Online
    5. Lab: Privileged Access Management
        1. Set up privileged access management and process a request
14. Discover and Respond
    1. Content Search
    2. Audit Log Investigations
    3. Advanced eDiscovery
    4. Lab: Manage Search and Investigation
        1. Investigate your Microsoft 365 Data
        2. Conduct a Data Subject Request

## 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 365 Administration class:

- Basic conceptual understanding of Microsoft Azure.
- Experience with Windows 10 devices.
- Experience with Office 365.
- Basic understanding of authorization and authentication.
- Basic understanding of computer networks.
- Working knowledge of managing mobile devices.