Microsoft 365 Certified: Enterprise Administrator Expert (MCEAE)

This module covers MD-100-Windows, MD-101-Managing Modern Desktops, MS-100-Microsoft 365 Identity and Services and MS-101-Microsoft 365 Mobility and Security. Microsoft 365 Enterprise Administrators evaluate, plan, migrate, deploy and manage Microsoft 365 services, Installing the Windows 10 OS. Students will learn the different editions of Windows Server 2016, Windows 10 requirements and new features introduced. This module covers how to install the OS, as well as methods for migrations and upgrading. Students will also learn about common tools used in the deployment process.

Course Outline

☞ **Earning this certification will validate you are able to:**

- Design and implement Microsoft 365 services
- Manage user identity and roles
- Manage access and authentication
- Plan Office 365 workloads and applications
- Implement modern device services
- Implement Microsoft 365 security and threat management
- Manage Microsoft 365 governance and compliance

MD-100: Windows 10 and MD-101: Managing Modern Desktops

Network Essentials
- Networking Concepts, History of Server OS
- Introduction to Windows Server 2012 and 2016
- Features of Windows 2016
- Introduction to Windows 10
- Windows 10 Editions and Requirements
- Installation of Windows Server 2016 and Windows 10
- Upgrading to Windows 10 / In-place upgrade of Win7 to Win 10
- Introduction and Creation of Users accounts
- Migrating User Settings using USMT

Active Directory - Domain Services
- IP Addressing and Configuring Networking
- Logical Topologies - Peer-Peer & Domain Models
- Introduction to Directory Services
- Evolution of Active Directory Services
- Features of Active Directory
- Installing Active Directory – Domain Controller

Member Servers, Clients, User Configuration
- Configuring Member Servers and Clients - Joining a Domain
- Creating Users in AD-DS
- User Logon policies
- Password policies
- Account Lockout policies
- User properties

Configuring Networking
- Configure IP Network Connectivity
- Implement Name Resolution
- Implement Wireless Network Connectivity
- Remote Access Overview
- Remote Management

Permissions / Access Control Lists / Configuring Data Access and Usage
- File Systems
- Security and Sharing Permissions - Folders & Files
- Access Based Enumeration

Configuring Authorization & Authentication
- Configuring User Account Control
- Implementing Device Registration
- Configure Windows Hello.
- Configure user account control

Configuring Storage
- Overview of storage options
- Managing Local Storage
- Maintaining Disks and Volumes
- Configure local disk partitions and volumes.
- Managing Storage Spaces / Managing Storage
- Compressing Folders
- Enabling Disk Quotas / Creating a Storage Space
- Configure OneDrive / Synchronizing files with OneDrive

Managing Apps in Windows 10
- Providing Apps to Users
- Managing Universal Windows Apps
- Web Browsers in Windows 10
- Install applications manually and using automated methods
- Manage application deployment using the Windows Store

Planning an Operating System Deployment Strategy
- The Enterprise Desktop
- Assessing Deployment Readiness
- Deployment Tools & Strategies
- Planning Windows 10 deployment

Implementing Windows 10
- Upgrading Devices to Windows 10
- Deploying New Devices and Refreshing
- Migrating Devices to Windows 10
- Alternate Deployment Methods
- Imaging Considerations
- Creating and deploying provisioning package
- Migrating user settings
- Deploying Windows 10 with Autopilot

Managing Updates for Windows 10
- Updating Windows 10
- Windows Update for Business
- Introduction to Windows Analytics
- Practice Lab - Managing Updates for Windows 10
- Manually configuring Windows Update settings
- Describe updating Windows using WSUS
- Configuring Windows Update by using GPOs

Device Enrollment
- Cover Azure AD join and will be introduced to Microsoft Intune
- Device management options
- Microsoft Intune Overview
- Manage Intune device enrollment and inventory
- Managing devices with Intune
- Practice Lab - Device Enrollment and Management

Configuring Profiles
- Configuring device profiles
- Managing user profiles
- Monitoring devices
- Managing profiles

Managing Authentication in Azure AD
- Azure AD Overview
- Differences between Azure AD and Active Directory DS
- Managing identities in Azure AD
- Protecting identities in Azure AD
- Managing device authentication
- Managing objects and authentication in Azure AD

Managing Device Access and Compliance
- Microsoft Intune Overview
- Implement device compliance policies
- Managing Access and Compliance

Managing Security
- Implement device data protection
- Managing Windows Defender Advanced Threat Protection
- Managing Windows Defender in Windows 10
- Practice Lab - Managing Security in Windows 10

MS-100: Microsoft 365 Identity & Services & MS-101: Microsoft 365 Mobility & Security

Plan architecture
- Plan integration of Microsoft 365 and on-premises environments
- Identify deployment workloads team
- Plan an identity and authentication solution
- Plan enterprise application modernization

Deploy a Microsoft 365 tenant
- Manage domains
- Configure organizational settings
- Complete the organizational profile
- Complete the subscription setup wizard
- Plan and create a tenant
- Edit an organizational profile
- Plan and create subscription(s)
- Configure tenant-wide workload settings

Manage Microsoft 365 subscription and tenant health
- Manage service health alerts
- Create and manage service requests
- Create internal service health response plan
- Monitor service health
- Monitor license allocations
- Configure and review reports, including BI, Operations Management Suite (OMS), and Microsoft 365 reporting
- Schedule and review security and compliance reports
- Schedule and review usage metrics

Plan migration of users and data
- Identify data to be migrated and migration methods
- Identify users and mailboxes to be migrated and migration methods
- Plan migration of on-premises users and groups
- Import PST files

Manage User Identity and Roles
- Design identity strategy
- Evaluate requirements and solutions for synchronization
- Evaluate requirements and solutions for identity management
- Evaluate requirements and solutions for authentication

Manage identity synchronization with Azure Active Directory (Azure AD)
- Configure directory synchronization by using Azure AD Connect
- Monitor Azure AD Connect Health
- Manage Azure AD Connect synchronization
- Configure object filters•configure password synchronization
- Implement multi-forest AD Connect scenarios

Manage Azure AD identities
- Plan Azure AD identities
- Implement and manage self-service password reset (SSPR)
- Manage access reviews
- Manage groups
- Manage passwords
- Manage product licenses
- Manage users
- Perform bulk user management

Manage roles
- Plan user roles
- Manage admin roles
- Allocate roles for workloads
- Manage role allocations by using Azure AD

Plan and implement secure access
- Design a conditional access solution
- Implement entitlement packages
- Implement Azure AD Identity Protection
- Manage identity protection
- Implement conditional access
- Manage conditional access
- Implement and secure access for guest and external users

Configure application access
- Configure application registration in Azure AD
- Configure Azure AD Application Proxy
- Publish enterprise apps in Azure AD

Plan Office 365 Workloads and Applications
- Plan for Microsoft 365 Apps deployment
- Plan for Microsoft connectivity
- Manage Microsoft 365 Apps
- Plan for Office online
- Assess readiness using Microsoft analytics
- Plan Microsoft 365 App compatibility
- Manage Office 365 software downloads
- Plan for Microsoft apps updates
- Plan Microsoft telemetry and reporting

Implement Modern Device Services / Plan device management
- Plan device monitoring
- Plan Microsoft Endpoint Manager implementation and integration with Azure AD
- Plan for configuration profiles

Manage device compliance
- Plan for device compliance
- Plan for attack surface reduction
- Configure security baselines
- Configure device compliance policy
- Plan and configure conditional access policies

Plan Windows 10 deployment
- Plan for Windows as a Service (waas)
- Plan for managing Windows quality and feature updates
- Plan Windows 10 Enterprise deployment methods
- Analyze upgrade readiness for Windows 10 by using services such as Desktop Analytics
- Evaluate and deploy additional Windows 10 Enterprise security features

Implement Microsoft 365 Security and Threat Management
- Manage security reports and alerts
- Evaluate and manage Microsoft Office 365 tenant security by using Secure Score
- Manage incident investigation
- Review and manage Microsoft 365 security alerts

Plan and implement threat protection with Microsoft Defender
- Plan Microsoft Defender for Endpoint
- Design Microsoft Defender for Office 365 policies
- Implement Microsoft Defender for Identity

Plan and implement data loss prevention (DLP)
- Plan for DLP
- Configure DLP policies
- Monitor DLP

Manage search and investigation
- Plan for auditing
- Plan for ediscovery
- Implement insider risk management
- Design a content search solution