Microsoft 365 Administrator Expert

Duration: 40 Hours

Audience profile

As a candidate for this exam, you have subject matter expertise deploying, configuring, protecting, managing, and monitoring devices and client applications in a Microsoft 365 environment. You're responsible for:

- Managing identity, security, access, policies, updates, and apps for endpoints.
- Implementing solutions for efficient deployment and management of endpoints on various operating systems, platforms, and device types. Implementing and managing endpoints at scale by using Microsoft Intune, Windows 365, Windows Autopilot, Microsoft Defender for Endpoint, and Microsoft Entra ID.

As an endpoint administrator, you collaborate with architects, Microsoft 365 administrators, security administrators, and other workload administrators to plan and implement a modern workplace strategy that meets the business needs of an organization.

You must have experience with Microsoft Entra ID and Microsoft 365 technologies, including Intune, as well as strong skills and experience in deploying, configuring, and maintaining Windows client and non-Windows devices.

Skills at a glance

- Deploy Windows client
- Manage identity and compliance
- Manage, maintain, and protect devices
- Manage applications

Deploy Windows client

Prepare for a Windows client deployment

- Select a deployment tool based on requirements
- Choose between migrate and rebuild

- Choose an imaging and/or provisioning strategy
- Select a Windows edition based on requirements
- Implement subscription-based activation
- Deploy Windows 365

Plan and implement a Windows client deployment by using Windows Autopilot

- Configure device registration for Autopilot
- Create, validate, and assign deployment profiles
- Set up the Enrollment Status Page (ESP)
- Deploy Windows devices by using Autopilot □ Troubleshoot an Autopilot deployment

Configure remote management

- Configure Remote Help in Intune
- Configure Remote Desktop on a Windows client
- Configure the Windows Admin Center
- Configure PowerShell remoting and Windows Remote Management (WinRM)

Manage identity and compliance

Manage identity

- Implement user authentication on Windows devices, including Windows Hello for Business, passwordless, and tokens
- Manage role-based access control (RBAC) for Intune
- Register devices in and join devices to Microsoft Entra
- Implement the Intune Connector for Active Directory
- Manage the membership of local groups on Windows devices
- Implement and manage Local Administrative Passwords Solution (LAPS) for Microsoft Entra

Implement compliance policies for all supported device platforms by using Intune

- Specify compliance policies to meet requirements

- Implement compliance policies
- Implement Conditional Access policies that require a compliance status
- Manage notifications for compliance policies
- Monitor device compliance
- Troubleshoot compliance policies

Manage, maintain, and protect devices

Manage the device lifecycle in Intune

- Configure enrollment settings
- Configure automatic and bulk enrollment, including Windows, iOS, and Android
- Configure policy sets
- Restart, retire, or wipe devices

Manage device configuration for all supported device platforms by using Intune

- Specify configuration profiles to meet requirements
- Implement configuration profiles
- Monitor and troubleshoot configuration profiles
- Configure and implement Windows kiosk mode
- Configure and implement profiles on Android devices, including fully managed, dedicated, corporate owned, and work profile Plan and implement Microsoft Tunnel for Intune

Monitor devices

- Monitor devices by using Intune
- Monitor devices by using Azure Monitor
- Analyze and respond to issues identified in Endpoint analytics and Adoption Score

Manage device updates for all supported device platforms by using Intune

- Plan for device updates
- Create and manage update policies by using Intune

- Manage Android updates by using configuration profiles
- Monitor updates
- Troubleshoot updates in Intune
- Configure Windows client delivery optimization by using Intune
- Create and manage update rings by using Intune

Implement endpoint protection for all supported device platforms

- Implement and manage security baselines in Intune
- Create and manage configuration policies for Endpoint security including antivirus, encryption, firewall, endpoint detection and response (EDR), and attack surface reduction (ASR)
- Onboard devices to Microsoft Defender for Endpoint
- Implement automated response capabilities in Microsoft Defender for Endpoint
- Review and respond to device issues identified in the Microsoft Defender Vulnerability Management dashboard

Manage applications

Deploy and update apps for all supported device platforms

- Deploy apps by using Intune
- Configure Microsoft 365 Apps deployment by using the Microsoft Office Deployment Tool or Office Customization Tool (OCT)
- Manage Microsoft 365 Apps by using the Microsoft 365 Apps admin center
- Deploy Microsoft 365 Apps by using Intune
- Configure policies for Office apps by using Group Policy or Intune
- Deploy apps from platform-specific app stores by using Intune

Plan and implement app protection and app configuration policies

- Plan and implement app protection policies for iOS and Android
- Manage app protection policies
- Implement Conditional Access policies for app protection policies
- Plan and implement app configuration policies for managed apps and managed devices
- Manage app configuration policies

Deploy and manage a Microsoft 365 tenant

Implement and manage a Microsoft 365 tenant

- Create a tenant
- Implement and manage domains
- Configure org settings, including Security & privacy and Organizational profile
- Identify and respond to service health issues
- Configure notifications in service health
- Configure and review Network connectivity insights
- Monitor adoption and usage

Manage users and groups

- Create and manage users in Microsoft Entra, including external users and guests
- Create and manage contacts in the Microsoft 365 admin center
- Create and manage groups, including Microsoft 365 groups and shared mailboxes
- Manage and monitor Microsoft 365 licenses, including group-based licensing
- Perform bulk user management, including PowerShell

Manage compliance by using Microsoft Purview

Implement Microsoft Purview information protection and data lifecycle management

- Implement and manage sensitive information types by using keywords, keyword lists, or regular expressions
- Implement retention labels, retention label policies, and retention policies

- Implement sensitivity labels and sensitivity label policies
- Monitor label usage by using Content explorer, Activity explorer, and label reports

Implement Microsoft Purview data loss prevention (DLP)

- Configure DLP policies for Exchange, SharePoint, OneDrive, and Teams
- Configure Endpoint DLP
- Review and respond to DLP alerts, events, and reports