Microsoft 365 Certified: Enterprise Administrator Expert – Skills Measured

This document contains the skills measured on the exams associated with this certification. It does not include any upcoming or recent changes that have been made to those skills. For more information about upcoming or recent changes, see the associated exam details page(s).

NOTE: The bullets that follow each of the skills measured are intended to illustrate how we are assessing that skill. This list is not definitive or exhaustive.

NOTE: Most questions cover features that are General Availability (GA). The exam may contain questions on Preview features if those features are commonly used.

Exam MS-100: Microsoft 365 Identity and Services

Design and implement Microsoft 365 services (25-30%)

Plan architecture

- plan integration of Microsoft 365 and on-premises environments
- plan an identity and authentication solution
- plan enterprise application modernization

Deploy a Microsoft 365 tenant

- manage domains
- configure organizational settings
- complete the organizational profile
- add a Microsoft partner or work with Microsoft FastTrack
- 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 Power BI, Azure Monitor logs, Log Analytics workspaces, 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 (25-30%)

Design identity strategy

- evaluate requirements and solutions for synchronization
- evaluate requirements and solutions for identity management
- evaluate requirements and solutions for authentication

Plan identity synchronization Design directory synchronization

- design directory synchronization
- implement directory synchronization with directory services, federation services, and azure endpoints by using Azure AD Connect sync
- plan for directory synchronization using Azure AD cloud sync

Manage identity synchronization with Azure Active Directory (Azure AD)

- configure and manage directory synchronization by using Azure AD cloud sync
- configure directory synchronization by using Azure AD Connect
- monitor Azure AD Connect Health
- manage Azure AD Connect synchronization
- configure object filters
- configure password hash 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

Manage access and authentication (15-20%)

Manage authentication

- design an authentication method
- configure authentication
- implement an authentication method
- manage authentication
- monitor authentication

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
- get and manage Integrated apps from the Microsoft 365 admin center

Plan Microsoft Office 365 workloads and applications (25-30%)

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 Microsoft 365 apps deployment and software downloads
- plan for Microsoft 365 apps updates
- plan Microsoft telemetry and reporting
- plan for and manage policy settings using the Office cloud policy service
- manage security recommendations using the Security Policy Advisor

Plan for messaging deployments

- plan migration strategy
- plan messaging deployment
- identify hybrid requirements
- plan for connectivity
- plan for mail routing
- plan email domains

Plan for Microsoft SharePoint Online and OneDrive for Business

- plan migration strategy
- plan external share settings
- identify hybrid requirements
- manage access configurations
- manage Microsoft groups
- manage SharePoint tenant and site settings

Plan for Microsoft Teams infrastructure

- plan for communication and call quality and capacity
- plan for Phone System
- plan Microsoft Teams deployment
- plan Microsoft Teams organizational settings
- plan for guest and external access
- plan for Microsoft Teams hybrid connectivity and co-existence

Plan Microsoft Power Platform integration

- implement Microsoft Power Platform Center of Excellence (CoE) starter kit
- plan for Power Platform workload deployments
- plan resource deployment
- plan for connectivity (and data flow)
- manage environments
- manage resources

Exam MS-101: Microsoft 365 Mobility and Security

Implement modern device services (40-45%)

Plan device management

- plan device monitoring
- plan Microsoft Endpoint Manager implementation and integration with Azure AD
- plan co-management between Endpoint Configuration Manager and Intune
- 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 for apps

- create and configure Microsoft Store for Business
- plan app deployment
- plan for mobile application management (MAM)

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

Enroll devices

- plan for device join or device registration to Azure Active Directory (Azure AD)
- plan for manual and automated device enrollment into Intune
- enable device enrollment into Intune

Implement Microsoft 365 security and threat management (20-25%)

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 365 Defender

- plan Microsoft Defender for Endpoint
- design Microsoft Defender for Office 365 policies
- implement Microsoft Defender for Identity

Plan Microsoft Defender for Cloud Apps

- plan information protection by using Microsoft Defender for Cloud Apps
- plan policies to manage access to cloud apps
- plan for application connectors
- configure Cloud App Security policies
- review and respond to Cloud App Security alerts
- monitor for unauthorized cloud applications

Manage Microsoft 365 governance and compliance (35-40%)

Plan for compliance requirements

- plan compliance solutions
- assess compliance
- plan for and implement privileged access management
- plan for legislative and regional or industry requirements and drive implementation

Manage information governance

- plan data classification
- plan for classification labeling
- plan for restoring deleted content
- implement records management
- design data retention labels and policies in Microsoft 365

Implement Information protection

- plan an information protection solution
- plan and implement sensitivity labels and policies
- monitor label alerts and analytics
- deploy Azure Information Protection unified labels clients
- configure Information Rights Management (IRM) for workloads
- plan for Windows information Protection (WIP) implementation

Plan and implement data loss prevention (DLP)

- plan for DLP
- configure DLP policies
- monitor DLP

Manage search and investigation

- plan and configure auditing
- plan and configure eDiscovery
- implement and manage insider risk management
- design a Content Search solution