Exam MS-100: Microsoft 365 Identity and Services – Skills Measured

This exam will be updated on November 30, 2021. Following the current exam guide, we have included a version of the exam guide with Track Changes set to "On," showing the changes that will be made to the exam on that date.

NOTE: Passing score: 700. Learn more about exam scores here.

Audience Profile

Candidates for this exam are Microsoft 365 Enterprise Administrators who take part in evaluating, planning, migrating, deploying, and managing Microsoft 365 services. They perform Microsoft 365 tenant management tasks for an enterprise, including its identities, security, compliance, Power Platform, and supporting technologies.

Candidates have a working knowledge of Microsoft 365 workloads and should have been an administrator for at least one Exchange, SharePoint, Teams, or Windows 10 deployment. Candidates also have a working knowledge of networking, server administration, and IT fundamentals such as DNS, Active Directory, and PowerShell.

Skills Measured

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.

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
- 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 Office 365 software downloads
- plan for Microsoft apps updates
- plan Microsoft telemetry and reporting

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

The exam guide below shows the changes that will be implemented on November 30, 2021.

Audience Profile

Candidates for this exam are Microsoft 365 Enterprise Administrators who take part in evaluating, planning, migrating, deploying, and managing Microsoft 365 services. They perform Microsoft 365 tenant management tasks for an enterprise, including its identities, security, compliance, Power Platform, and supporting technologies.

Candidates have a working knowledge of Microsoft 365 workloads and should have been an administrator for at least one Exchange, SharePoint, Teams, or Windows 10 deployment. Candidates also have a working knowledge of networking, server administration, and IT fundamentals such as DNS, Active Directory, and PowerShell.

Skills Measured

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.

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
- 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 ~~Office~~ 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