Exam MS-101: Microsoft 365 Mobility and Security – Skills Measured

This exam was updated on November 24, 2020. Following the current exam guide, we have included a version of the exam guide with Track Changes set to "On," showing the changes that were made to the exam on that date.

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, and supporting technologies.

Candidates have a working knowledge of Microsoft 365 workloads and should have been an administrator for at least one Microsoft 365 workload (Exchange, SharePoint, Skype for Business, Windows as a Service). 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 appear below each of the skills measured are intended to illustrate how we are assessing that skill. This list is NOT definitive or exhaustive.

NOTE: In most cases, exams do NOT cover preview features, and some features will only be added to an exam when they are GA (General Availability).

Implement Modern Device Services (30-35%)

Implement Mobile Device Management (MDM)

- plan for MDM
- configure MDM integration with Azure AD
- set device enrollment limit for users

Manage device compliance

- plan for device compliance
- design Conditional Access Policies
- create Conditional Access Policies
- configure device compliance policy
- manage Conditional Access Policies

Plan for devices and apps

- create and configure Microsoft Store for Business
- plan app deployment
- plan device co-management
- plan device monitoring
- plan for device profiles
- plan for Mobile Application Management
- plan mobile device security

Plan Windows 10 deployment

- plan for Windows as a Service (WaaS)
- plan the appropriate Windows 10 Enterprise deployment method
- 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 (30-35%)

Implement Cloud App Security (CAS)

- configure Cloud App Security (CAS)
- configure Cloud App Security (CAS) policies
- configure Connected apps
- design a Cloud App Security (CAS) Solution
- manage Cloud App Security (CAS) alerts
- upload Cloud App Security (CAS) traffic logs

Implement threat management

- plan a threat management solution
- design Azure Advanced Threat Protection (ATP) implementation
- design Microsoft 365 ATP policies
- configure Azure ATP
- configure Microsoft 365 ATP policies
- monitor Advanced Threat Analytics (ATA) incidents

Implement Microsoft Defender Advanced Threat Protection (ATP)

- plan a Microsoft Defender ATP solution
- configure preferences
- implement Microsoft Defender ATP policies
- enable and configure security features of Windows 10 Enterprise

Manage security reports and alerts

- manage service assurance dashboard
- manage tracing and reporting on Azure AD Identity Protection
- configure and manage Microsoft 365 security alerts
- configure and manage Azure Identity Protection dashboard and alerts

Manage Microsoft 365 Governance and Compliance (35-40%)

Configure Data Loss Prevention (DLP)

- configure DLP policies
- design data retention policies in Microsoft 365
- manage DLP exceptions
- monitor DLP policy matches
- manage DLP policy matches

Implement sensitivity labels

- plan for sensitivity labels
- create and publish sensitivity labels
- use sensitivity labels on SharePoint and OneDrive
- plan for Windows information Protection (WIP) implementation

Manage data governance

- configure information retention
- plan for Microsoft 365 backup
- plan for restoring deleted content
- plan information retention policies

Manage auditing

- configure audit log retention
- configure audit policy
- monitor Unified Audit Logs

Manage eDiscovery

- search content by using Security & Compliance admin center
- plan for in-place and legal hold
- configure eDiscovery and create cases

The exam guide below shows the changes that were implemented on November 24, 2020.

Skills Measured

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

NOTE: In most cases, exams do NOT cover preview features, and some features will only be added to an exam when they are GA (General Availability).

Implement Modern Device Services (30-35%)

Implement Mobile Device Management (MDM)

- plan for MDM
- configure MDM integration with Azure AD
- set device enrollment limit for users

Manage device compliance

- plan for device compliance
- design Conditional Access Policies
- create Conditional Access Policies
- configure device compliance policy
- manage Conditional Access Policies

Plan for devices and apps

- create and configure Microsoft Store for Business
- plan app deployment
- plan device co-management
- plan device monitoring
- plan for device profiles
- plan for Mobile Application Management
- plan mobile device security

Plan Windows 10 deployment

- plan for Windows as a Service (WaaS)
- plan the appropriate Windows 10 Enterprise deployment method
- 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 (30-35%)

Implement Cloud App Security (CAS)

- configure Cloud App Security (CAS)
- configure Cloud App Security (CAS) policies
- configure Connected apps
- design a Cloud App Security (CAS) Solution
- manage Cloud App Security (CAS) alerts
- upload Cloud App Security (CAS) traffic logs

Implement threat management

- plan a threat management solution
- design Azure Advanced Threat Protection (ATP) implementation
- design Microsoft 365 ATP policies
- configure Azure ATP
- configure Microsoft 365 ATP policies
- monitor Advanced Threat Analytics (ATA) incidents

Implement Microsoft Defender Advanced Threat Protection (ATP)

- plan a Microsoft Defender ATP solution
- configure preferences
- implement Microsoft Defender ATP policies
- enable and configure security features of Windows 10 Enterprise

Manage security reports and alerts

- manage service assurance dashboard
- manage tracing and reporting on Azure AD Identity Protection
- configure and manage Microsoft 365 security alerts
- configure and manage Azure Identity Protection dashboard and alerts

Manage Microsoft 365 Governance and Compliance (35-40%)

Configure Data Loss Prevention (DLP)

- configure DLP policies
- design data retention policies in Microsoft 365
- manage DLP exceptions
- monitor DLP policy matches
- manage DLP policy matches

Implement sensitivity labels

- plan for sensitivity labels
- create and publish sensitivity labels

- use sensitivity labels on SharePoint and OneDrive
- plan for Windows information Protection (WIP) implementation

Manage data governance

- configure information retention
- plan for Microsoft 365 backup
- plan for restoring deleted content
- plan information retention policies

Manage auditing

- configure audit log retention
- configure audit policy
- monitor Unified Audit Logs

Manage eDiscovery

- search content by using Security ~~&and~~ Compliance admin ~~C~~center
- plan for in-place and legal hold
- configure eDiscovery and create cases