Study guide for Exam MS-101: Microsoft 365 Mobility and Security

Purpose of this document

This study guide should help you understand what to expect on the exam and includes a summary of the topics the exam might cover and links to additional resources. The information and materials in this document should help you focus your studies as you prepare for the exam.

Useful links	Description
Review the skills measured as of November 2, 2022	This list represents the skills measured AFTER the date provided. Study this list if you plan to take the exam AFTER that date.
Review the skills measured prior to November 2, 2022	Study this list of skills if you take your exam PRIOR to the date provided.
Change log	You can go directly to the change log if you want to see the changes that will be made on the date provided.
How to earn the certification	Some certifications only require passing one exam, while others require passing multiple exams.
Certification renewal	Microsoft associate, expert, and specialty certifications expire annually. You can renew by passing a free online assessment on Microsoft Learn.
Your Microsoft Learn profile	Connecting your certification profile to Learn allows you to schedule and renew exams and share and print certificates.
Passing score	A score of 700 or greater is required to pass.
Exam sandbox	You can explore the exam environment by visiting our exam sandbox.
Request accommodations	If you use assistive devices, require extra time, or need modification to any part of the exam experience, you can request an accommodation.

Useful links	Description
Take a practice test	Are you ready to take the exam or do you need to study a bit more?

Updates to the exam

Our exams are updated periodically to reflect skills that are required to perform a role. We have included two versions of the Skills Measured objectives depending on when you are taking the exam.

We always update the English language version of the exam first. Some exams are localized into other languages, and those are updated approximately eight weeks after the English version is updated. Other available languages are listed in the **Schedule Exam** section of the **Exam Details** webpage. If the exam isn't available in your preferred language, you can request an additional 30 minutes to complete the exam.

Note

The bullets that follow each of the skills measured are intended to illustrate how we are assessing that skill. Related topics may be covered in the exam.

Note

Most questions cover features that are general availability (GA). The exam may contain questions on Preview features if those features are commonly used.

Skills measured as of November 2, 2022

Audience Profile

Candidates for this exam are Microsoft 365 enterprise administrators who have expert-level skills in evaluating, planning, migrating, deploying, and managing Microsoft 365. They perform Microsoft 365 tenant-level planning, implementation, and administration of cloud and hybrid enterprise environments. Candidates for this exam have subject matter expertise in Microsoft 365 endpoints, security, and compliance.

The enterprise administrator functions as the integrating hub for all Microsoft 365 workloads. This role coordinates across multiple Microsoft 365 workloads and advises the architects and workload administrators.

Candidates for this exam have functional experience with all Microsoft 365 workloads and Microsoft Azure Active Directory (Azure AD), part of Microsoft Entra and have administered at least one of these. They also have a working knowledge of networking, server administration, DNS, and PowerShell.

- Plan and implement device services (35–40%)
- Manage security and threats by using Microsoft 365 Defender (25–30%)
- Manage Microsoft 365 compliance (30–35%)

Plan and implement device services (35–40%)

Plan and implement device management by using Microsoft Endpoint Manager

- Plan co-management between Endpoint Configuration Manager and Intune
- Plan and implement configuration profiles for Windows and MacOS clients
- Plan and implement configuration profiles for iOS and Android
- Review and respond to issues identified in Microsoft Endpoint Manager

Plan and implement device security and compliance by using Microsoft Endpoint Manager

- Plan and implement device compliance policies
- Plan and implement attack surface reduction policies
- Implement and manage security baselines
- Plan and configure conditional access policies for device compliance

Deploy and manage applications by using Microsoft Endpoint Manager

- Plan and implement application deployment
- Publish public and private applications by using Microsoft Endpoint Manager
- Plan and implement application protection policies
- Plan and implement application configuration policies
- Monitor and troubleshoot application deployment

Plan for Windows client deployment and management

- Choose Windows client deployment methods and tools based on requirements, including Windows Autopilot, USMT, Microsoft Deployment Toolkit, and Windows Deployment Services
- Plan and implement Windows subscription-based activation
- Plan for Windows updates
- Plan and implement additional Windows client security features

Plan and implement device enrollment

- Plan and implement device join or hybrid join to Azure AD
- Plan and implement device registration to Azure AD
- Plan and implement manual and automated device enrollment into Intune

Manage security and threats by using Microsoft 365 Defender (25–30%)

Manage security reports and alerts by using the Microsoft 365 Defender portal

- Review and respond to the Microsoft 365 Secure Score
- Review and respond to security alerts in Microsoft 365 Defender

- Review and respond to issues identified in security and compliance reports in Microsoft 365 Defender

Plan, implement, and manage email and collaboration protection by using Microsoft Defender for Office 365

- Plan and implement policies and rules in Microsoft Defender for Office 365
- Review and respond to issues identified in Microsoft Defender for Office 365, including threats, investigations, and campaigns
- Unblock users

Plan, implement, and manage endpoint protection by using Microsoft Defender for Endpoint

- Plan Microsoft Defender for Endpoint
- Onboard devices to Microsoft Defender for Endpoint
- Configure Microsoft Defender for Endpoint settings
- Review and respond to endpoint vulnerabilities
- Review and respond to risks on devices
- Review and respond to exposure score

Plan, implement, and manage Microsoft Defender for Cloud Apps

- Configure the application connector for Office 365
- Plan and configure Microsoft Defender for Cloud Apps policies
- Review and respond to Microsoft Defender for Cloud Apps alerts
- Review and respond to activity log
- Configure Cloud App Discovery
- Review and respond to issues identified in Cloud App Discovery

Manage Microsoft 365 compliance (30–35%)

Plan and implement information governance

- Plan and implement retention labels and label policies
- Recover deleted data in Exchange Online and SharePoint Online
- Implement records management

Plan and implement information protection

- Plan and implement data classification
- Plan and implement sensitivity labels and policies
- Optimize label usage by using Content explorer, Activity explorer, and label reports

Plan and implement data loss prevention (DLP)

- Plan and implement DLP for workloads
- Plan and implement Microsoft 365 Endpoint DLP

- Review and respond to DLP alerts, events, and reports

Manage search and investigation

- Configure auditing in Azure AD, including diagnostic settings
- Plan and configure audit retention policies for Microsoft 365
- Retrieve and interpret audit logs for workloads
- Plan and configure eDiscovery and Advanced eDiscovery
- Specify a Content Search based on requirements

Study resources

We recommend that you train and get hands-on experience before you take the exam. We offer self-study options and classroom training as well as links to documentation, community sites, and videos.

Study resources	Links to learning and documentation
Get trained	Choose from self-paced learning paths and modules or take an instructor-led course
Find documentation	Microsoft 365 documentation Microsoft 365 admin center help Microsoft Endpoint Configuration Manager documentation Microsoft Defender products and services Microsoft Purview compliance documentation
Ask a question	Microsoft Q&A | Microsoft Docs
Get community support	Microsoft 365 - Microsoft Tech Community
Follow Microsoft Learn	Microsoft Learn - Microsoft Tech Community
Find a video	Exam Readiness Zone Browse other Microsoft Learn shows

Change log

Key to understanding the table: The topic groups (also known as functional groups) are in bold typeface followed by the objectives within each group. The table is a comparison between the two versions of the exam skills measured and the third column describes the extent of the changes.

Skill area prior to November 2, 2022	Skill area as of November 2, 2022	Change
Audience profile		Minor
Plan and implement device services	**Plan and implement device services**	No change
Plan and implement device management by using Microsoft Endpoint Manager	Plan and implement device management by using Microsoft Endpoint Manager	No change
Plan and implement device security and compliance by using Microsoft Endpoint Manager	Plan and implement device security and compliance by using Microsoft Endpoint Manager	No change
Deploy and manage applications by using Microsoft Endpoint Manager	Deploy and manage applications by using Microsoft Endpoint Manager	No change
Plan for Windows client deployment and management	Plan for Windows client deployment and management	No change
Plan and implement device enrollment	Plan and implement device enrollment	Minor
Manage security and threats by using Microsoft 365 Defender	**Manage security and threats by using Microsoft 365 Defender**	No change
Manage security reports and alerts by using the Microsoft 365 Defender portal	Manage security reports and alerts by using the Microsoft 365 Defender portal	No change
Plan, implement, and manage email and collaboration protection by using Microsoft Defender for Office 365	Plan, implement, and manage email and collaboration protection by using Microsoft Defender for Office 365	No change
Plan, implement, and manage endpoint protection by using Microsoft Defender for Endpoint	Plan, implement, and manage endpoint protection by using Microsoft Defender for Endpoint	No change
Plan, implement, and manage Microsoft Defender for Cloud Apps	Plan, implement, and manage Microsoft Defender for Cloud Apps	No change
Manage Microsoft 365 compliance	**Manage Microsoft 365 compliance**	No change

Skill area prior to November 2, 2022	Skill area as of November 2, 2022	Change
Plan and implement information governance	Plan and implement information governance	No change
Plan and implement information protection	Plan and implement information protection	Minor
Plan and implement data loss prevention (DLP)	Plan and implement data loss prevention (DLP)	No change
Manage search and investigation	Manage search and investigation	No change

Skills measured prior to November 2, 2022

Audience Profile

Candidates for this exam are Microsoft 365 enterprise administrators who have expert-level skills in evaluating, planning, migrating, deploying, and managing Microsoft 365. They perform Microsoft 365 tenant-level planning, implementation, and administration of cloud and hybrid enterprise environments. Candidates for this exam have subject matter expertise in Microsoft 365 endpoints, security, and compliance.

The enterprise administrator functions as the integrating hub for all Microsoft 365 workloads. This role coordinates across multiple Microsoft 365 workloads and advises the architects and workload administrators.

Candidates for this exam have functional experience with all Microsoft 365 workloads and Azure Active Directory and have administered at least one of these. They also have a working knowledge of networking, server administration, DNS, and PowerShell.

- Plan and implement device services (35–40%)
- Manage security and threats by using Microsoft 365 Defender (25–30%)
- Manage Microsoft 365 compliance (30–35%)

Plan and implement modern device services (35–40%)

Plan device management

- Plan co-management between Endpoint Configuration Manager and Intune
- Plan and implement configuration profiles for Windows and macOS clients
- Plan and implement configuration files for iOS and Android
- Review and respond to issues identified in Microsoft Endpoint Manager

Plan and implement device security and compliance by using Microsoft Endpoint Manager

- Plan and implement device compliance policies
- Plan and implement attack surface reduction policies
- Implement and manage security baselines
- Plan and configure conditional access policies for device compliance

Deploy and manage applications by using Microsoft Endpoint Manager

- Plan and implement application deployment
- Publish public and private applications by using Microsoft Endpoint Manager
- Plan and implement application protection policies
- Plan and implement application configuration policies
- Monitor and troubleshoot application deployment

Plan for Windows client deployment and management

- Choose Windows client deployment methods and tools based on requirements, including Windows Autopilot, USMT, Microsoft Deployment Toolkit, and Windows Deployment Services
- Plan and implement Windows subscription-based activation
- Plan for Windows updates
- Plan and implement additional Windows client security features

Plan and implement device enrollment

- Plan and implement device join or hybrid join to Azure Active Directory (Azure AD)
- Plan and implement device registration to Azure AD
- Plan and implement manual and automated device enrollment into Intune

Manage security and threats by using Microsoft 365 Defender (25–30%)

Manage security reports and alerts by using the Microsoft 365 Defender portal

- Review and respond to the Microsoft 365 Secure Score
- Review and respond to security alerts in Microsoft 365 Defender
- Review and respond to issues identified in security and compliance reports in Microsoft 365 Defender

Plan, implement, and manage email and collaboration protection by using Microsoft Defender for Office 365

- Plan and implement policies and rules in Microsoft Defender for Office 365
- Review and respond to issues identified in Microsoft Defender for Office 365, including threats, investigations, and campaigns
- Unblock users

Plan, implement, and manage endpoint protection by using Microsoft Defender for Endpoint

- Plan Microsoft Defender for Endpoint
- Onboard devices to Microsoft Defender for Endpoint
- Configure Microsoft Defender for Endpoint settings
- Review and respond to endpoint vulnerabilities
- Review and respond to risks on devices
- Review and respond to exposure score

Plan, implement, and manage Microsoft Defender for Cloud Apps

- Configure the application connector for Office 365
- Plan and configure Microsoft Defender for Cloud Apps policies
- Review and respond to Microsoft Defender for Cloud Apps alerts
- Review and respond to activity log
- Configure Cloud App Discovery
- Review and respond to issues identified in Cloud App Discovery

Manage Microsoft 365 compliance (30–35%)

Plan and implement information governance

- Plan and implement retention labels and label policies
- Recover deleted data in Exchange Online and SharePoint Online
- Implement records management

Plan and implement information protection

- Plan and implement data classification
- Plan and implement sensitivity labels and policies
- Optimize label usage by using Content Explorer, Activity Explorer, and label reports

Plan and implement data loss prevention (DLP)

- Plan and implement DLP for workloads
- Plan and implement Microsoft 365 Endpoint DLP
- Review and respond to DLP alerts, events, and reports

Manage search and investigation

- Configure auditing in Azure AD, including diagnostic settings
- Plan and configure audit retention policies for Microsoft 365
- Retrieve and interpret audit logs for workloads
- Specify a Content Search based on requirements