

Study guide for Exam MD-101: Managing Modern Desktops

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 February 3, 2023	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 February 3, 2023	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 February 3, 2023

Audience profile

Candidates for this exam are IT professionals who have subject matter expertise in installing, configuring, and maintaining Windows clients within a domain infrastructure. Responsibilities include protecting and maintaining the reliability of the Windows device and the data stored on the device. Candidates for this exam administer Windows clients in an Active Directory environment. Candidates for this exam may collaborate with the Microsoft 365 enterprise administrator, the Microsoft 365 security administrator, and Windows Server administrators to implement a modern desktop and device strategy that meets the business needs of an organization.

Candidates for this exam must be familiar with device management, client computer networking, policy-based management, and cloud-based solutions.

- Deploy Windows client (25–30%)
- Manage identity and access (10–15%)
- Manage compliance policies and configuration profiles (10–15%)
- Manage, maintain, and protect devices (25–30%)
- Manage apps (10–15%)

Deploy Windows client (25–30%)

Plan a Windows client deployment

- Assess infrastructure readiness by using Endpoint Analytics
- Select a deployment tool based on requirements
- Choose between migrate and rebuild
- Choose an imaging and/or provisioning strategy
- Plan and implement changes to Windows edition by using subscription activation or MAK license management

Plan and implement Windows client provisioning by using Windows Autopilot

- Choose an Autopilot deployment method based on requirements, including user-driven mode, self-deploying mode, autopilot reset, and pre-provisioning
- Configure device registration for Autopilot
- Create, validate, and assign deployment profiles
- Set up the Enrollment Status Page
- Provision Windows devices by using Autopilot
- Troubleshoot an Autopilot deployment

Plan and implement Windows client deployment by using Microsoft Deployment Toolkit (MDT)

- Plan and implement an MDT deployment infrastructure
- Choose configuration options based on requirements, such as boot images, OS images, upgrade packages, task sequences, and drivers
- Create, manage, and deploy images
- Plan and implement PXE boot by using Windows Deployment Services (WDS)
- Create and use task sequences
- Manage application and driver deployment
- Customize an MDT deployment by using customsettings.ini and bootstrap.ini
- Monitor and troubleshoot deployment
- Plan and configure user state migration

Manage identity and access (10–15%)

Manage identity

- Register devices in and join devices to Microsoft Azure Active Directory (Azure AD), part of Microsoft Entra
- Enable users and groups from Azure AD to access Windows client
- Manage AD DS and Azure AD groups
- Manage AD DS and Azure AD users
- Configure Enterprise State Roaming in Azure AD

Plan and implement conditional access policies

- Plan conditional access
- Set up conditional access policies
- Determine which users are affected by a conditional access policy
- Troubleshoot conditional access

Manage compliance policies and configuration profiles (10–15%)

Implement device compliance policies

- Plan device compliance policies
- Implement device compliance policies
- Manage notifications for device compliance policies
- Monitor device compliance
- Troubleshoot device compliance policies

Plan and implement device configuration profiles

- Plan device configuration profiles
- Implement device configuration profiles
- Monitor and troubleshoot device configuration profiles
- Configure and implement assigned access on public devices, including kiosks and dedicated devices

Manage, maintain, and protect devices (25–30%)

Manage device lifecycle

- Configure enrollment settings in Intune
- Configure automatic and bulk enrollment in Intune
- Configure policy sets
- Restart, retire, or wipe devices

Monitor devices

- Monitor devices by using Azure Monitor
- Monitor device hardware and software inventory by using Endpoint Manager Admin Center
- Monitor devices by using Endpoint Analytics

Manage device updates

- Plan for device updates
- Create and manage quality update policies by using Intune
- Create and manage feature update policies by using Intune
- Create and manage iOS/iPadOS update policies by using Intune
- Manage Android updates by using device configuration profiles

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

Plan and implement endpoint protection

- Plan endpoint security
- Implement and manage security baselines in Intune
- Create and manage configuration policies for Endpoint Security including antivirus, encryption, firewall, endpoint detection and response, and attack surface reduction
- Onboard devices into Microsoft Defender for Endpoint
- Monitor Microsoft Defender for Endpoint
- Investigate and respond to threats

Manage apps (10–15%)

Deploy and update applications

- Deploy apps by using Intune
- Configure Microsoft 365 Apps deployment by using Office Deployment Toolkit or Office Customization Tool
- Manage Microsoft 365 Apps by using Microsoft 365 Apps Admin Center
- Deploy Microsoft 365 Apps by using Intune
- Manage Office app settings by using group policy or Intune
- Deploy apps by using Microsoft Store for Business, Apple store, and Google store

Implement app protection and app configuration policies

- Plan app protection policies
- Plan app configuration policies for iOS and Android
- Implement app protection policies
- Implement app configuration policies for iOS and Android
- Manage app protection policies
- Manage app configuration policies

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	Windows Documentation Windows client documentation for IT Pros Windows client deployment resources and documentation Windows Autopilot documentation Windows application management Microsoft Intune documentation Manage Windows client Windows security Microsoft Endpoint Manager documentation
Ask a question	Microsoft Q&A Microsoft Docs
Get community support	Windows - 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 February 3, 2023	Skill area as of February 3, 2023	Change
Audience profile	Audience profile	No change

Skill area prior to February 3, 2023	Skill area as of February 3, 2023	Change
Deploy Windows Client	Deploy Windows client	No change
Plan a Windows Client Deployment	Plan a Windows client deployment	No change
Plan and Implement Windows Client Provisioning by using Windows Autopilot	Plan and implement Windows client provisioning by using Windows Autopilot	Minor
Plan and Implement Windows 365 (temporarily removed)	Plan and implement Windows 365 (temporarily removed)	No change
Plan and Implement Windows Client Deployment by using Microsoft Deployment Toolkit (MDT)	Plan and Implement Windows client deployment by using Microsoft Deployment Toolkit (MDT)	No change
Manage Identity and Access	Manage identity and access	No change
Manage Identity	Manage identity	No change
Plan and Implement Conditional Access Policies	Plan and implement conditional access policies	No change
Manage Compliance Policies and Configuration Profiles	Manage compliance policies and configuration profiles	No change
Implement Device Compliance Policies	Implement device compliance policies	No change
Plan and Implement Device Configuration Profiles	Plan and implement device configuration profiles	No change
Manage, Maintain, and Protect Devices	Manage, maintain, and protect devices	No change
Manage Device Lifecycle	Manage device lifecycle	No change
Monitor Devices	Monitor devices	No change
Manage Device Updates	Manage device updates	No change
Plan and Implement Endpoint Protection	Plan and implement endpoint protection	No change
Manage Apps	Manage apps	No change
Deploy and Update Applications	Deploy and update applications	No change

Skill area prior to February 3, 2023	Skill area as of February 3, 2023	Change
Implement App Protection and App Configuration Policies	Implement app protection and app configuration policies	No change

Skills measured prior to February 3, 2023

- Deploy Windows client (25–30%)
- Manage identity and access (10–15%)
- Manage compliance policies and configuration profiles (10–15%)
- Manage, maintain, and protect devices (25–30%)
- Manage apps (10–15%)

Deploy Windows client (25–30%)

Plan a Windows client deployment

- Assess infrastructure readiness by using Endpoint Analytics
- Select a deployment tool based on requirements
- Choose between migrate and rebuild
- Choose an imaging and/or provisioning strategy
- Plan and implement changes to Windows edition by using subscription activation or MAK license management

Plan and implement Windows client provisioning by using Windows Autopilot

- Choose an Autopilot deployment method based on requirements, including user-driven mode, self-deploying mode, autopilot reset, and pre-provisioning
- Configure device registration for Autopilot
- Create, validate, and assign deployment profiles
- Provision Windows devices by using Autopilot
- Troubleshoot an Autopilot deployment

Plan and implement Windows client deployment by using Microsoft Deployment Toolkit (MDT)

- Plan and implement an MDT deployment infrastructure
- Choose configuration options based on requirements, such as boot images, OS images, upgrade packages, task sequences, and drivers
- Create, manage, and deploy images
- Plan and implement PXE boot by using Windows Deployment Services (WDS)
- Create and use task sequences
- Manage application and driver deployment
- Customize an MDT deployment by using customsettings.ini and bootstrap.ini

- Monitor and troubleshoot deployment
- Plan and configure user state migration

Manage identity and access (10–15%)

Manage identity

- Register devices in and join devices to Microsoft Azure Active Directory (Azure AD), part of Microsoft Entra
- Enable users and groups from Azure AD to access Windows client
- Manage AD DS and Azure AD groups
- Manage AD DS and Azure AD users
- Configure Enterprise State Roaming in Azure AD

Plan and implement conditional access policies

- Plan conditional access
- Set up conditional access policies
- Determine which users are affected by a conditional access policy
- Troubleshoot conditional access

Manage compliance policies and configuration profiles (10–15%)

Implement device compliance policies

- Plan device compliance policies
- Implement device compliance policies
- Manage notifications for device compliance policies
- Monitor device compliance
- Troubleshoot device compliance policies

Plan and implement device configuration profiles

- Plan device configuration profiles
- Implement device configuration profiles
- Monitor and troubleshoot device configuration profiles
- Configure and implement assigned access on public devices, including kiosks and dedicated devices

Manage, maintain, and protect devices (25–30%)

Manage device lifecycle

- Configure enrollment settings in Intune
- Configure automatic and bulk enrollment in Intune
- Configure policy sets
- Restart, retire, or wipe devices

Monitor devices

- Monitor devices by using Azure Monitor
- Monitor device hardware and software inventory by using Endpoint Manager Admin Center
- Monitor devices by using Endpoint Analytics

Manage device updates

- Plan for device updates
- Create and manage quality update policies by using Intune
- Create and manage feature update policies by using Intune
- Create and manage iOS/iPadOS update policies by using Intune
- Manage Android updates by using device configuration profiles
- Monitor updates
- Troubleshoot updates in Intune
- Configure Windows client delivery optimization by using Intune
- Create and manage update rings by using Intune

Plan and implement endpoint protection

- Plan endpoint security
- Implement and manage security baselines in Intune
- Create and manage configuration policies for Endpoint Security including antivirus, encryption, firewall, endpoint detection and response, and attack surface reduction
- Onboard devices into Microsoft Defender for Endpoint
- Monitor Microsoft Defender for Endpoint
- Investigate and respond to threats

Manage apps (10–15%)

Deploy and update applications

- Deploy apps by using Intune
- Configure Microsoft 365 Apps deployment by using Office Deployment Toolkit or Office Customization Tool
- Manage Microsoft 365 Apps by using Microsoft 365 Apps Admin Center
- Deploy Microsoft 365 Apps by using Intune
- Manage Office app settings by using group policy or Intune
- Deploy apps by using Microsoft Store for Business, Apple store, and Google store

Implement app protection and app configuration policies

- Plan app protection policies
- Plan app configuration policies for iOS and Android
- Implement app protection policies
- Implement app configuration policies for iOS and Android

- Manage app protection policies
- Manage app configuration policies