Exam MD-101: Managing Modern Desktops – Skills Measured

This exam was updated on November 24, 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 were made to the exam on that date.

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

Audience Profile

Candidates for this exam are administrators who deploy, configure, secure, manage, and monitor devices and client applications in an enterprise environment. Candidates manage identity, access, policies, updates, and apps.

As an administrator, candidates typically collaborate with the M365 Enterprise Administrator to design and implement a device strategy that meets the business needs of a modern organization.

Candidates must be familiar with M365 workloads and must be proficient and experienced in deploying, configuring, and maintaining Windows 10 and non-Windows devices and technologies.

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.

Deploy and upgrade operating Systems (25-30%)

Plan a Windows 10 deployment

- assess infrastructure readiness
- evaluate and select appropriate deployment options (Autopilot, MDT, Configuration Manager)
- plan upgrade and downgrade paths
- plan app compatibility
- plan for user state

Plan and implement Windows 10 by using Windows Autopilot

- choose method based on requirements
- create, validate, and assign deployment profile
- extract device HW information to CSV file
- import device HW information to cloud service
- deploy Windows 10
- troubleshoot deployment

Plan and implement Windows 10 using MDT

- choose configuration options based on requirements
- create and manage images
- deploy images (may include WDS)
- create and use task sequences
- manage application and driver deployment
- monitor and troubleshoot deployment

Manage accounts, VPN connections, and certificates on Windows 10

- secure privileged accounts on Windows 10
- configure VPN client
- configure and manage certificates on client devices
- configure Microsoft Tunnel for Microsoft Intune

Manage policies and profiles (20-25%)

Implement compliance policies for devices

- implement device compliance policies
- manage device compliance policies
- plan device compliance policies

Configure device profiles

- implement device profiles
- manage device profiles
- plan device profiles
- control policy conflicts
- configure and implement assigned access or public devices
- configure filters for configuration profiles

Manage user profiles

- configure user profiles
- configure Enterprise State Roaming in Azure AD

- configure sync settings

Manage and protect devices (30-35%)

Implement and manage device, application, and threat protection

- implement and manage Microsoft Defender Application Guard
- implement and manage Windows Defender Credential Guard
- implement and manage Exploit protection
- plan and Implement Microsoft Defender Advanced for Endpoint for Windows 10
- integrate Windows Defender Application Control
- protect devices using Endpoint Security
- manage enterprise-level disk encryption
- implement and manage security baselines in Microsoft Intune

Manage devices enrolled in Microsoft Intune

- configure enrollment settings in Microsoft Intune
- configure Microsoft Intune automatic and bulk enrollment
- enroll non-Windows devices
- enroll Windows devices
- review device inventory

Monitor devices

- monitor devices using Azure Monitor and Desktop Analytics
- monitor device inventory reports using Endpoint Manger Admin Center

Manage updates

- configure Windows 10 delivery optimization
- deploy Windows updates using Microsoft Intune
- monitor Windows 10 updates

Manage apps and data (10-15%)

Deploy and update applications

- assign apps to users or groups
- deploy apps by using Microsoft Intune
- deploy apps by using Microsoft Store for Business/iTunes/Google Play
- deploy Microsoft 365 Apps for enterprise (by using Office Deployment Tool, Intune, or Microsoft 365)

- create and Modify Office deployment configurations (using ODT or Microsoft 365 Apps Admin Center/Office Customization Tool)
- gather Microsoft 365 Apps readiness data

Implement Mobile Application Management (MAM)

- implement App Protection policies
- manage App Protection policies
- plan App Protection Policies
- plan and implement App Configuration Policies (Windows Information Protection)

The exam guide below shows the changes that were implemented on November 24, 2021.

Audience Profile

Candidates for this exam are administrators who deploy, configure, secure, manage, and monitor devices and client applications in an enterprise environment. Candidates manage identity, access, policies, updates, and apps.

As an administrator, candidates typically collaborate with the M365 Enterprise Administrator to design and implement a device strategy that meets the business needs of a modern organization.

Candidates must be familiar with M365 workloads and must be proficient and experienced in deploying, configuring, and maintaining Windows 10 and non-Windows devices and technologies.

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.

Deploy and upgrade operating Systems (25-30%)

Plan a Windows 10 deployment

- assess infrastructure readiness
- evaluate and select appropriate deployment options (~~Endpoint Manager~~Autopilot, MDT, Configuration Manager)

- plan upgrade and downgrade paths
- plan app compatibility
- plan for user state

Plan and implement Windows 10 by using Windows Autopilot

- choose method based on requirements
- create, validate, and assign deployment profile
- extract device HW information to CSV file
- import device HW information to cloud service
- deploy Windows 10
- troubleshoot deployment

Plan and implement Windows 10 using MDT

- choose configuration options based on requirements
- create and manage images
- deploy images (may include WDS)
- create and use task sequences
- manage application and driver deployment
- monitor and troubleshoot deployment

Manage accounts, VPN connections, and certificates on Windows 10

- secure privileged accounts on Windows 10
- configure VPN client
- configure and manage certificates on client devices
- configure Microsoft Tunnel for Microsoft Intune

Manage policies and profiles (20-25%)

Implement compliance policies for devices

- implement device compliance policies
- manage device compliance policies
- plan device compliance policies

Configure device profiles

- implement device profiles
- manage device profiles
- plan device profiles
- control policy conflicts
- configure and implement assigned access or public devices

- configure filters for configuration profiles

Manage user profiles

- configure user profiles
- configure Enterprise State Roaming in Azure AD
- configure sync settings

Manage and protect devices (30-35%)

Implement and manage device, application, and threat protection

- implement and manage Microsoft Defender Application Guard
- implement and manage Windows Defender Credential Guard
- implement and manage Exploit protection
- plan and Implement Microsoft Defender Advanced for Endpoint for Windows 10
- integrate Windows Defender Application Control
- protect devices using Endpoint Security
- manage enterprise-level disk encryption
- implement and manage security baselines in Microsoft Intune

Manage devices enrolled in Microsoft Intune

- configure enrollment settings in Microsoft Intune
- configure Microsoft Intune automatic and bulk enrollment
- enroll non-Windows devices
- enroll Windows devices
- review device inventory

Monitor devices

- monitor devices using Azure Monitor and Desktop Analytics
- monitor device inventory reports using Endpoint Manger Admin Center

Manage updates

- configure Windows 10 delivery optimization
- deploy Windows updates using Microsoft Intune
- monitor Windows 10 updates

Manage apps and data (10-15%)

Deploy and update applications

- assign apps to users or groups
- deploy apps by using Microsoft Intune
- deploy apps by using Microsoft Store for Business/iTunes/Google Play
- deploy Microsoft 365 Apps for enterprise (by using Office Deployment Tool, Intune, or Microsoft 365)
- create and Modify Office deployment configurations (using ODT or Microsoft 365 Apps Admin Center/Office Customization Tool)
- gather Microsoft 365 Apps readiness data

Implement Mobile Application Management (MAM)

- implement App Protection policies
- manage App Protection policies
- plan App Protection Policies
- plan and implement App Configuration Policies (Windows Information Protection)