Microsoft Endpoint Administrator

SECOND EDITION

Exam Ref MD-102

Andrew Warren
Andrew Bettany

Microsoft

Exam Ref MD-102 Microsoft Endpoint Administrator

Second Edition

Andrew Warren
Andrew Bettany

Chapter summary

- Windows computers can be Entra ID-joined or Entra ID-registered. However, other operating systems can only be registered.
- You can configure Windows Hello for Business settings using either GPOs or Microsoft Intune.
- You create custom RBAC roles in Microsoft Entra but can assign roles in Microsoft Entra or Microsoft Intune.
- LAPS enables you to manage your Windows devices' local administrator passwords. You use Intune to configure the settings using an Account protection policy.
- Automatic enrollment lets you enroll Windows devices when they register with or join Azure AD.
- Device Enrollment Manager Accounts enable a specified account to enroll up to 1,000 devices.
- There are a number of ways to enroll Windows devices:
  - Add a Work Or School account
  - Enroll In MDM Only (user-driven)
  - Entra ID Join during OOBE
  - Entra ID Join using Windows Autopilot
  - Enroll In MDM only (using a Device Enrollment Manager)
  - Entra ID Join using bulk enrollment
- To enroll Android and iOS devices, you can download the Company Portal app from the relevant device store and sign in to the app using an organizational or school account.
- Compliance policies ensure devices meet compliance requirements, such as being encrypted, not being jailbroken, and using a password for device access.
- Noncompliant devices can be blocked from accessing resources or offered help to become compliant.
- When multiple device compliance policies are assigned to a device, Intune calculates a compliance status based on the highest severity level of all the policies assigned to the device.
- Devices will periodically check with Intune to determine the device's compliance status; this will be every six hours for Apple devices and every eight hours for Android and Windows devices.
- A conditional access policy in Entra ID can be configured to require device compliance before access to corporate apps and data is granted.

Thought experiment

In this thought experiment, demonstrate your skills and knowledge of the topics covered in this chapter. You can find the answers in the section that follows.

Scenario 1

Contoso has a significant on-premises infrastructure. However, their IT department is in the process of planning the migration to the Microsoft cloud. For a significant period, Contoso's computer needed to be hybrid-joined. As an IT consultant for Contoso, answer the following question:

How can the IT department enable the hybrid joining of existing computers?

Scenario 2

Your organization has 500 employees and has implemented a bring-your-own-device (BYOD) strategy that enables users to use their personal mobile phones and tablets for corporate purposes as long as they comply with company policy regarding security and management features. After consulting an employee survey, you find that the users in your organization have iOS, Android, or Windows 11 devices.

1. What technology should you use to manage the devices?
2. You want to simplify enrollment for your Windows device users. What should you do?
3. To support your iOS devices, what additional step is required to enable MDM?

Thought experiment answers

This section contains the solution to the thought experiment. Each answer explains why the answer choice is correct.

Scenario 1

IT staff have two choices for the hybrid joining of existing computers. They could implement Entra ID Cloud Sync or Entra ID Connect Sync. With Entra ID Cloud Sync, an agent is installed on an on-premises computer. Then, synchronization settings are configured and managed in Intune. With Entra ID Connect Sync, the Entra ID Connect program is downloaded and installed on an on-premises server computer. Then, synchronization settings are configured and managed within the Entra ID Connect program in the on-premises context.

Scenario 2

1. Microsoft Intune with Mobile Device Management enabled.
2. Enable and configure Windows Autoenrollment.
3. You require an Apple MDM Push Certificate for your organization.

CHAPTER 2

Manage and maintain devices

The content in this chapter accounts for around 30–35 percent of the MD-102 exam. Therefore, understanding how to deploy and provision Windows using cloud tools and how to manage and maintain devices in your organization using Intune is critical—not only to pass the exam but also so you can manage your organization's devices efficiently.

A good chunk of the exam focuses on efficiently deploying Windows 11 with the least administrative effort and using modern tools and technologies. You must understand how to plan and implement the deployment of Windows 11 and be able to choose the most appropriate tools and methods. It's also important that you know how to create and assign configuration profiles in order to provision organizational devices running both Windows and other operating systems.

Skills covered in this chapter:

- Skill 2.1: Deploy and upgrade Windows clients by using cloud-based tools
- Skill 2.2: Plan and implement device configuration profiles
- Skill 2.3: Implement Intune Suite add-on capabilities
- Skill 2.4: Perform remote actions on devices

Skill 2.1: Deploy and upgrade Windows clients by using cloud-based tools

Within a domain-based environment, deploying new devices to users has become increasingly complex. There are many different options and numerous components, and each needs to work precisely to ensure that your devices are compliant, secure, and usable. The complexity arises partly because of the granular nature of the tooling used to ensure that devices comply with strict organizational security requirements. Windows Autopilot is a solution that radically changes this approach while allowing you to deploy secure and compliant devices.

Windows 11 offers new and exciting methods for organizations to deploy the operating system to users. For many years, large organizations have resisted adopting modern dynamic deployment methods and utilized legacy on-premises tools to deploy Windows.

However, for the MD-102 exam, you must understand when the newer methods are used and how to implement them over more traditional methods. By nudging the audience, we can see Microsoft shift the adoption of the new dynamic deployment methods, which will gain traction in the modern workplace.

You must understand how to plan and implement Windows 11 within an organization using Windows Autopilot. This skill explores the planning, example scenarios, and installation requirements for the application of Windows Autopilot and other cloud-based deployment tools.

This skill covers how to:

- Choose between Windows Autopilot and provisioning packages
- Plan and implement provisioning packages
- Plan and implement device upgrades for Windows 11
- Choose a Windows Autopilot deployment mode
- Apply a device name template
- Create an Enrollment Status Page
- Implement Windows client deployment by using Windows Autopilot
- Implement a Windows 365 cloud PC deployment

Choose between Windows Autopilot and provisioning packages

Deploying Windows 11 within an enterprise environment should be carefully planned so the delivery has every chance to succeed. This is especially applicable when faced with choosing from numerous tools and methods.

Technologies evolve and modernize, so your deployment process should evolve, too. You should follow best practices and current guidance to utilize the productivity advancements to ensure that your deployment is delivered with minimal issues and delivered on schedule.

Windows 11 is released using a continuous delivery model, sometimes known as Windows as a Service, with a new version of Windows 11 available annually, usually in the fall. Therefore, the skills you learn in deploying Windows 11 to your users will be reused again and often.

It is recommended that administrators choose a group of users and deploy Windows 11 into focused pilot projects to test each version of Windows 11 within their organizations before rolling out the operating system to larger cohorts of users.

You must explore each of the available deployment and provisioning options. These options include technology such as Windows Autopilot and Windows Configuration Designer, Microsoft Deployment Toolkit (MDT), and Configuration Manager.

NOTE **MDT AND CONFIGURATION MANAGER**

The MD-102 exam no longer includes specific requirements for the understanding and use of either MDT or Configuration Manager, both of which are on-premises-focused tools. However, these tools and their methods are briefly referenced throughout this content.

Table 2-1 lists many different methods to deploy and configure Windows 11. You must understand when to use each deployment method.

TABLE 2-1 Methods for deploying and configuring Windows

Method	Description
Windows Autopilot	Transform an existing Windows 11 installation, join the device to Entra ID, and enroll it into a Mobile Device Management solution to complete the configuration. Deploy Windows 11 on an existing Windows 10 device.
Windows 11 subscription activation	Upgrade the Windows edition seamlessly without requiring user intervention or restarting the device.
Entra ID / MDM	Cloud-based identity and management solution offering device, app, and security configuration.
Provisioning packages	Small distributable `.appx` files that securely transform devices to meet organizational requirements. Can be used alone or in combination with other deployment techniques and tools.
In-place upgrade	Upgrade an earlier version of Windows to Windows 11 while retaining all apps, user data, and settings.
Bare metal	Deploy Windows 11 to newly built devices or wipe existing devices and deploy fresh Windows 11 images to them.
Refresh (wipe and load)	Re-use existing devices. Retain user state (user data, Windows, and app settings). Wipe devices, deploy Windows 11 images to them, and finally, restore the user state.
Replace	Purchase new devices. Back up the user state from the current device. Transform or wipe a pre-installed Windows 11 installation and restore the user state.

Dynamic provisioning uses modern tools, including mobile device management solutions, to deploy devices. Many of these options were unavailable when deploying previous Windows versions using traditional deployment methods. Table 2-2 compares modern dynamic provisioning and traditional deployment methods (which can also incorporate image creation).

TABLE 2-2 Provisioning methods

Dynamic provisioning methods	Traditional deployment methods
Enrollment into Entra ID and MDM (such as Microsoft Intune)	On-premises deployment tools using Windows Assessment and Deployment Kit (Windows ADK), Windows Deployment Services, Microsoft Deployment Toolkit, or Configuration Manager
Provisioning packages using Windows Configuration Designer	Bare-metal install
Subscription activation	In-place upgrade
Windows Autopilot	Wipe-and-load upgrade

The deployment choices available to an organization might be skewed by its investment in traditional deployment methods and infrastructure. This might include reliance upon on-premises tools and procedures, such as MDT and Endpoint Configuration Manager. These tools continue to be supported and can be used to support on-premises deployment methods, such as bare metal, refresh, and replace scenarios. You should understand the modern alternatives to the traditional on-premises methods.

Deploying Windows 11 using modern cloud-based deployment and dynamic provisioning methods includes subscription activation, Windows Autopilot, and Entra ID join. Ongoing management of Windows 11 is then undertaken using Microsoft Intune.

You should see a theme throughout this book, which is to recommend an alternative method of provisioning client devices to the traditional approach, which would typically include the following stages:

- Purchase or reprovision a device
- Wipe the device
- Replace the preinstalled operating system with a customized image using MDT or Configuration Manager
- Join an on-premises Active Directory domain
- Apply Group Policy settings to configure the device
- Manage apps using Configuration Manager

With a cloud-based deployment approach, the stages are simplified to the following:

- Purchase or re-provision a device
- Apply a transformation to the preinstalled operating system
- Join Entra ID and enroll in MDM
- Use MDM to configure the device, enforce compliance with corporate policies, and add, remove, and configure apps

There is a significant difference between the two approaches. Dynamic provisioning seeks to avoid the requirement for significant on-premises infrastructure and resource-intensive reimaging procedures.

> ***NOTE*** **REQUIRED ON-PREMISES INFRASTRUCTURE**
>
> **Although you can reduce the requirement for on-premises infrastructure, you cannot remove it entirely. During dynamic provisioning, for example, with Windows Autopilot, a device must be able to access specific internet-based resources. This means that the device must have an IP configuration and be able to resolve internet names using Dynamic Name System (DNS). These important requirements must be met by your on-premises infrastructure.**

Because Windows 11 is updated once a year to a newer version—with each new version supported for a maximum of 24 months (36 months for Enterprise and Education editions)—maintaining customized deployment images can become a costly and burdensome process for the IT department.