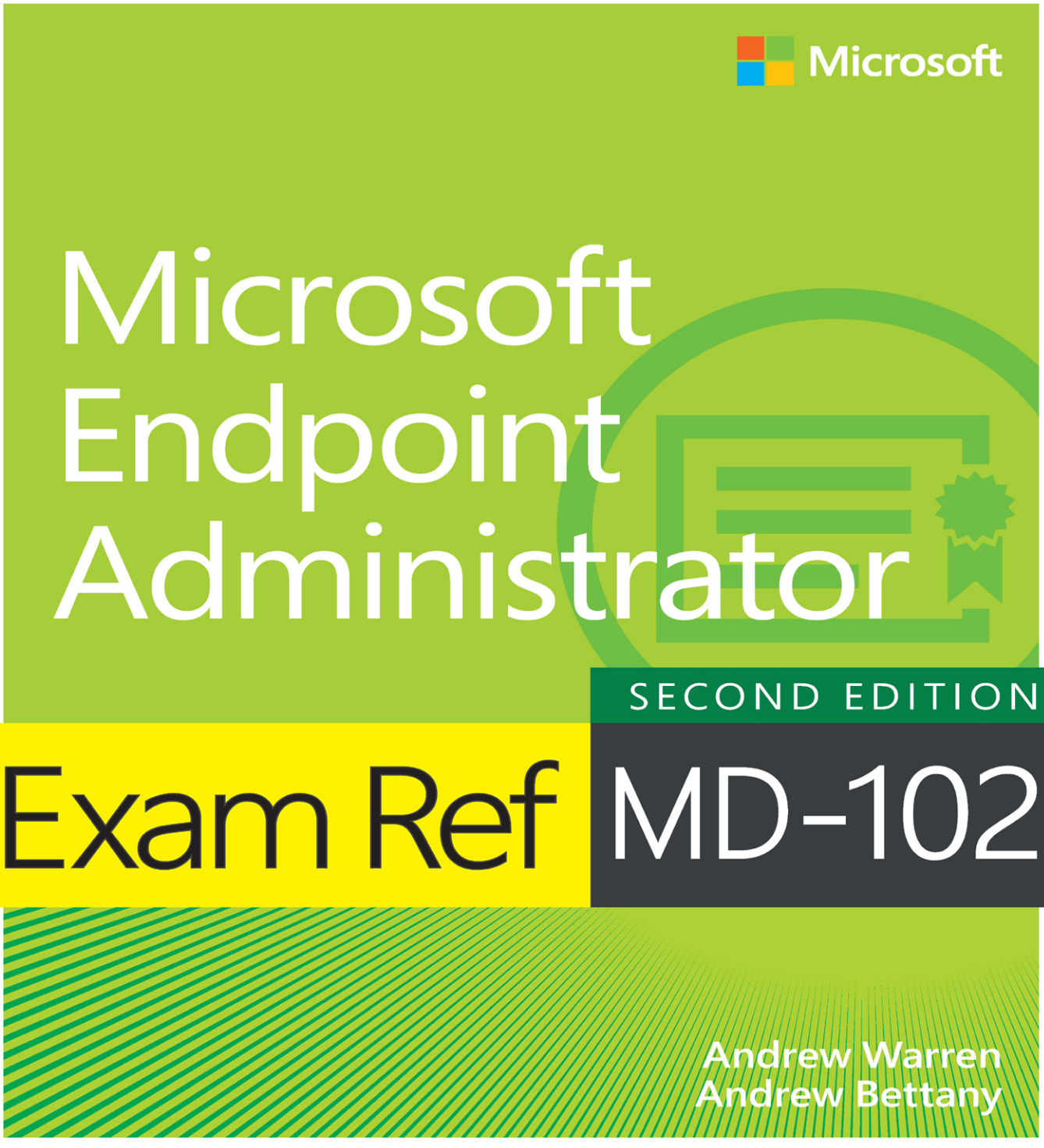

FREE SAMPLE CHAPTER |

Microsoft

Exam Ref MD-102 Microsoft Endpoint Administrator

Second Edition

Andrew Warren
Andrew Bettany

Exam Ref MD-102 Microsoft Endpoint Administrator Second Edition

Published with the authorization of Microsoft Corporation by:
Pearson Education, Inc.

ISBN-13: 978-0-13-541709-6
ISBN-10: 0-13-541709-0

Library of Congress Control Number: 2024951939

$PrintCode

EDITOR-IN-CHIEF
Brett Bartow

EXECUTIVE EDITOR
Loretta Yates

ASSOCIATE EDITOR
Shourav Bose

DEVELOPMENT EDITOR
Rick Kughen

MANAGING EDITOR
Sandra Schroeder

SENIOR PROJECT EDITOR
Tracey Croom

COPY EDITOR
Rick Kughen

INDEXER
Timothy Wright

PROOFREADER
Barbara Mack

TECHNICAL EDITOR
Tommy B. Kobberøe

EDITORIAL ASSISTANT
Cindy Teeters

COVER DESIGNER
Twist Creative, Seattle

COMPOSITOR
codeMantra

Contents at a glance

Contents

Acknowledgments

Writing a book is a challenge. There are many words, and some of them are quite long. But just like a journey starts with a single step, so writing a book starts with a single sip; in this case, of espresso. And then you take another sip, another step, and the book takes shape. I'm thankful as ever for the team at Pearson who helped keep me on the straight and narrow while I crafted what is, I think, my eleventh Microsoft Press title. I am also, as ever, grateful for coffee.

—Andrew Warren

Thank you to the team at Pearson, who helped make the book production process efficient and painless. I'm dedicating this book to Annette and Tommy for being supportive and encouraging. This book is also for the reader. I hope this book helps you proficiently manage Microsoft Windows within a modern cloud environment. The world of IT changes often, and we should all strive to stay up-to-date and use the most appropriate tools. I hope this book helps you to achieve success!

—Andrew Bettany

About the authors

ANDREW WARREN has been writing for Microsoft for many years, helping to develop its official curriculum of instructor-led training material. He has served as a subject matter expert on many Windows Server courses, was technical lead on several Windows client titles, and was involved in Microsoft 365, Azure, and Intune course development. When not writing about Microsoft technologies, he can be found in the classroom, teaching other IT professionals what they need to know to manage their organization's IT infrastructure.

ANDREW BETTANY has been honored as a Microsoft Most Valuable Professional (MVP) in two categories—Microsoft AI and Windows and Devices for IT—for 12 years. In 2020, he joined Microsoft for a couple of years to assist the Education team in promoting cloud skills. Currently, he helps students worldwide achieve cloud and AI skills and certifications through his Cloud Ready Skills programs.

Andrew is a dedicated father, IT enthusiast, training mentor, consultant, entrepreneur, and author. He is renowned for his expertise in AI and Windows and has authored numerous publications, including several Windows exam certification prep guides and official Microsoft training materials. He has also developed video training content for LinkedIn Learning and Pluralsight.

As a Microsoft Certified Trainer for 20 years, Andrew provides training and consultancy to businesses in various technical areas, including Microsoft 365, AI, Azure, and Windows. He is active on social media and can be found on LinkedIn, Facebook, and Twitter. Andrew resides in a village near the picturesque city of York in Yorkshire, England.

Introduction

With the Microsoft 365 Certified: Endpoint Administrator Associate certification, Microsoft has changed how IT Pro certifications work. Rather than being based on a technology area, they are focused on a specific job role. The Microsoft MD-102: Endpoint Administrator exam provides the foundation of this Microsoft 365 Certified: Endpoint Administrator Associate certification.

This book covers every major topic area on the exam but does not cover every exam question. Only the Microsoft exam team has access to the exam questions, and Microsoft regularly adds new questions to the exam, making it impossible to cover specific questions. You should consider this book a supplement to your relevant real-world experience and other study materials. If you encounter a topic in this book that you do not feel completely comfortable with, use the "Need more review?" links you'll find in the text to find more information and take the time to research and study the topic. Great information is available on the Microsoft website at *docs.microsoft.com*.

Organization of this book

This book is organized by the "Skills measured" list published for the exam. The "Skills measured" list is available for each exam on the Microsoft Learn website: *microsoft.com/learn*. Each chapter in this book corresponds to a major topic area in the list, and the technical tasks in each topic area determine a chapter's organization. For example, if an exam covers four major topic areas, the book will contain four chapters.

Preparing for the exam

Microsoft certification exams are a great way to build your resume and let the world know about your level of expertise. Certification exams validate your on-the-job experience and product knowledge. Although there is no substitute for on-the-job experience, preparation through study and hands-on practice can help you prepare for the exam.

We recommend augmenting your exam preparation plan by using a combination of available study materials and courses. For example, you might use the Exam Ref and another study guide for your "at-home" preparation and take a Microsoft Official Curriculum course for the classroom experience. Choose the combination that you think works best for you. Learn more about available classroom training, online courses, and live events at *microsoft.com/learn*.

Note that this Exam Ref is based on publicly available information about the exam and the author's experience. To safeguard the integrity of the exam, authors do not have access to the live exam.

Microsoft certifications

Microsoft certifications distinguish you by proving your command of a broad set of skills and experience with current Microsoft products and technologies. The exams and corresponding certifications are developed to validate your mastery of critical competencies as you design and develop, or implement and support, solutions with Microsoft products and technologies, both on-premises and in the cloud. Certification brings various benefits to the individual, employers, and organizations.

MORE INFO **ALL MICROSOFT CERTIFICATIONS**

For information about Microsoft certifications, including a full list of available certifications, go to *microsoft.com/learn*.

Access the exam updates chapter and online references

The final chapter of this book, "MD-102 Endpoint Administrator updates," will be used to provide information about new content per new exam topics, content that has been removed from the exam objectives, and revised mapping of exam objectives to chapter content. The chapter will be made available from the link below as exam updates are released.

This book contains webpage addresses that the author has recommended you visit for more information. Some of these links can be very long and painstaking to type, so we've shortened them for you to make them easier to visit. We've also compiled them into a single list that readers of the print edition can refer to while they read.

The URLs are organized by chapter and heading. Every time you come across a URL in the book, find the hyperlink in the list to go directly to the webpage.

Download the Exam Updates chapter and the URL list at *MicrosoftPressStore.com/ERMD102/downloads*.

Errata, updates, & book support

We've made every effort to ensure the accuracy of this book and its companion content. You can access updates to this book—in the form of a list of submitted errata and their related corrections—at:

MicrosoftPressStore.com/ERMD102/errata

If you discover an error that is not already listed, please submit it to us at the same page.

For additional book support and information, please visit *MicrosoftPressStore.com/Support*.

Please note that product support for Microsoft software and hardware is not offered through the previous addresses. For help with Microsoft software or hardware, go to *support.microsoft.com*.

Stay in touch

Let's keep the conversation going! We're on Twitter: *twitter.com/MicrosoftPress*.

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.

The types of transformations that are currently available using dynamic provisioning include the following:

- **Provisioning packages** A provisioning package is created using the Windows Configuration Designer and can send one or more configurations to apps and settings on a device.
- **Entra ID join with automatic MDM enrollment** A device can be joined to Entra ID and automatically enrolled into the organizational MDM solution by having users enter their work or school account details. Once enrolled, MDM will configure the device to the organization's policies.
- **Subscription Activation** Windows 11 Subscription Activation allows you to automatically upgrade devices from Windows 11 Pro to Windows 11 Enterprise without entering a product key or performing a restart.

Use provisioning packages

Using provisioning packages to transform a device can apply tailored settings and configurations to a device, including:

- Transform the edition of Windows that is in use.
- Apply configuration and settings to the device, including:
- Security settings
- Device restrictions
- Policies
- WiFi and VPN profiles
- Certificates
- Install apps
- Language packs
- Windows updates
- Enroll the device in a management solution such as Intune

After the device has been configured, it can then be managed via the management solution for further configuration and ongoing management.

Larger enterprises will choose to use more robust and scalable tools, including one or more of the following:

- Entra ID join and automatic MDM enrollment
- Windows Autopilot

Implement Entra ID Join with automatic MDM enrollment

You can dynamically provision Windows 11 devices using Entra ID and an MDM solution, such as Microsoft Intune. Once a device is enrolled into management, Microsoft Intune can deploy compliance and corporate security policies to the device in a similar way (but not the same) as Group Policy objects are used within a domain-based environment to configure computers.

MDM can be used to add or remove apps, restrict device features, and more. Through the application of MDM policies, Entra ID can block or allow access to corporate resources or applications based on the status of the device compliance.

To benefit from the cloud-based dynamic provisioning, you need the following requirements:

- Windows 11 Pro or Windows 11 Enterprise
- Entra ID for identity management
- A mobile device management solution, such as Microsoft Intune

Implement subscription-based activation

Windows 11 requires activation to unlock all the operating system's features and comply with the licensing requirements.

Once activated, Windows 11 devices can:

- Receive updates
- Access all Windows 11 features
- Access support

Several types of activation register the installation of Windows on a device with a standalone or corporate Windows 11 product key. The three main methods of activation are:

- Retail
- OEM
- Microsoft Volume Licensing (volume activation)

Organizations with Enterprise Agreements (EA) can use volume activation methods, which provide tools and services that allow activation to be automated and deployed at scale. These tools and services include:

- **Active Directory–based activation** This is an automated service that, once installed, uses Active Directory Directory Services (AD DS) to store activation objects. This simplifies the maintenance of volume activation services for an enterprise. Activation requests are automatically processed as devices authenticate to the Active Directory domain.
- **Key Management Service (KMS)** This automated service is hosted on a computer within your domain-based network. All volume editions of Windows 11 periodically connect to the KMS host to request activation.
- **Multiple activation key (MAK)** Enterprises purchase product keys that allow a specific number of Windows 11 devices to be activated using the Microsoft activation servers on the Internet.

All the above enterprise activation methods utilize services found within traditional on-premises, domain-based environments. An alternative activation method is required to meet the needs of devices registered to cloud-based authentication and identity services, such as Entra ID.

Subscription Activation allows your organization's Entra ID tenant to be associated with an existing Enterprise Agreement; all valid devices connected to that tenant will be automatically activated.

Eligible licenses that can use Subscription Activation include

- Windows 11 Enterprise E3 or E5 licenses obtained as part of an Enterprise Agreement
- Devices containing a firmware-embedded activation key
- Windows 11 Enterprise E3 in CSP (Cloud Solution Provider), which is offered as a subscription for small- and medium-sized organizations—from one to hundreds of users

NOTE **FIRMWARE-EMBEDDED ACTIVATION KEY**

Most OEM-provided devices designed to run Windows 8 or later will have a firmware-embedded key. You can read more information about firmware-embedded activation key licensing on the Microsoft website at *https://learn.microsoft.com/windows/deployment/deploy-enterprise-licenses*.

Organizations must meet the following requirements to implement Subscription Activation:

- Enterprise Agreement or a Microsoft Products and Services Agreement (MPSA) associated with the organization's Entra ID tenant.
- Windows 11 Pro or Windows 11 Enterprise is installed on the devices you want to upgrade.
- Entra ID for identity management.
- All devices are either Entra ID–joined or are members of an AD DS domain synchronized to Entra ID using Entra ID Connect.

If all the requirements are met, when a licensed user signs in using their Entra ID credentials using a device, the operating system switches from Windows 11 Pro to Windows 11 Enterprise, and all Windows 11 Enterprise features are then available. This process takes place without entering a product key and without requiring that users restart their computers.

EXAM TIP

Devices that have been upgraded using Subscription Activation must be able to connect to the Entra ID tenant at least every 90 days to remain licensed. If the Entra ID tenant expires or the user license is unassigned, the device will revert to Windows 11 Pro.

Using the Subscription activation for Enterprise feature, you can deploy Windows Enterprise to your devices without requiring software license keys. If you have used the Windows 11 Enterprise Subscription Activation to step up from Windows Pro edition to Enterprise or Education edition (or from Windows Pro Education edition to Education edition), you should ensure that the device remains licensed with an *Enterprise Agreement (EA)* or by using a Windows Enterprise E3 or E5 license. Each user that has an enterprise license can upgrade up to 5 devices.

Devices that have been upgraded will attempt to renew licenses about every 30 days. If the license expires, devices will automatically revert to the original edition after the 90-day grace period. For example, if you originally upgraded to Windows 11 Enterprise from Windows 11 Pro, the device will revert to Windows 11 Pro.

If you want to downgrade from Windows 11 Enterprise to Windows 11 Pro for Workstations, Pro Education, or Education editions, you must obtain an additional activation key, which will supersede the original firmware-embedded Windows 11 Pro key.

If an organization uses Windows virtual machines, these can automatically inherit the activation state from the Windows client host. The host computer must meet the following conditions for this feature to be supported:

- Run Windows 10 or Windows 11.
- The user must have a Windows Enterprise E3 or E5 license assigned.
- The Hypervisor platform must be Windows Hyper-V.
- The user signs in to the VM with a local or Entra ID account.

NOTE **SOFTWARE ACTIVATION CHANGES THE EDITION NOT THE VERSION**

Subscription activation doesn't upgrade a device from Windows 10 to Windows 11. Only the edition is updated.

Windows Autopilot deployment overview

We will cover Windows Autopilot in more detail later in this chapter, but it is useful to provide an overview of this new deployment solution here.

Devices deployed by Windows Autopilot can be traditional Windows computers or kiosk devices. Kiosk devices are regular devices dedicated to a specific task, such as a multi-app kiosk device like Surface Go, which displays a messaging app, or the Microsoft Edge browser in a corporate office lobby.

In addition to deploying devices, Autopilot allows you to remotely reset and repurpose devices. Therefore, IT departments can be further optimized and no longer need to process devices themselves—they can ship devices direct to the end user and allow the user to start the deployment configuration remotely. Because Autopilot runs as a cloud service, there's no infrastructure to manage. Administrators can manage and configure devices remotely from the Microsoft Endpoint Manager portal.

Windows Autopilot allows administrators to customize the out-of-the-box experience and reduce the time IT spends deploying and managing devices. Because devices are shipped directly to the end user, rather than via IT, and then transformed "while you wait," there is minimal delay in the deployment, and the user can be productive quickly.

All devices that are to be configured by Autopilot must first be known to the Windows Autopilot service. A hardware hash, or ID, is collected from each device. This can be done

within your organization for devices your organization already owns, or your hardware vendor can upload these hardware hashes on your behalf. Windows Autopilot requires Entra ID to provide the cloud identity for the user, and the hardware hash is associated with the cloud device identity. The overview of the Windows Autopilot device provisioning process can be seen in Figure 2-1. The flow diagram shows Windows Autopilot used to configure Entra-joined devices supplied by the hardware vendor directly to the user.

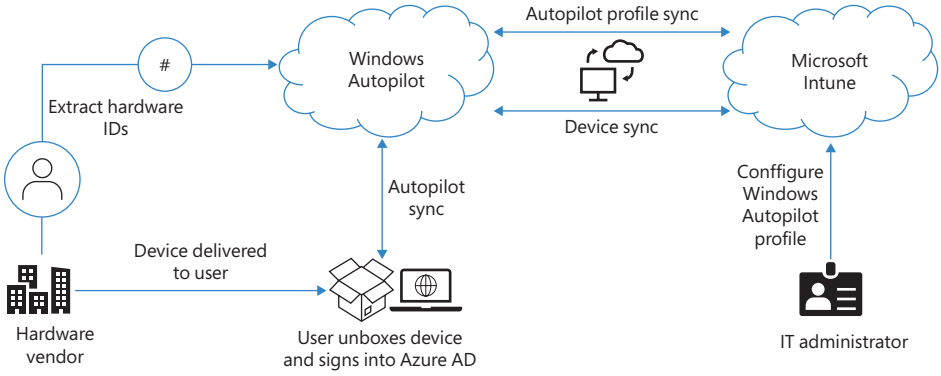

FIGURE 2-1 Windows Autopilot overview

Plan and implement provisioning packages

Provisioning packages are still a relatively new method for deploying changes to Windows clients. They are created using the Windows Configuration Designer included in the Windows ADK. You can also download the standalone Windows Configuration Designer app from the Microsoft Store. The Microsoft Store Windows Configuration Designer app will auto-update to the latest version available.

> ***NOTE*** **DOWNLOAD WINDOWS ADK**
>
> **You can download the Windows ADK from the Microsoft website at *https://learn.microsoft.com/windows-hardware/get-started/adk-install*. Make sure to download the version of Windows ADK that matches the Windows 11 version you intend to deploy.**

Provisioning packages use very small configuration files. These are used to modify existing Windows 11 installations and configure their runtime settings.

A provisioning package can perform a variety of functions, such as:

- Configure the computer name and user accounts
- Add the computer to a domain
- Upgrade the Windows 11 version, such as upgrading Windows 11 Home to Windows 11 Enterprise

- Configure the Windows user interface
- Add additional files or install apps
- Remove installed software
- Configure network connectivity settings
- Install certificates
- Implement security settings
- Reset Windows 11
- Run PowerShell scripts

To create a provisioning package, you should complete the Windows Configuration Designer installation process using either Windows ADK or the Microsoft Store. Once done, you can create and deploy your provisioning packages. Start by opening Windows Configuration Designer. On the **Start page** displayed in Figure 2-2, select the option that best describes the type of provisioning you want. If you're unsure, choose the **Advanced provisioning** tile.

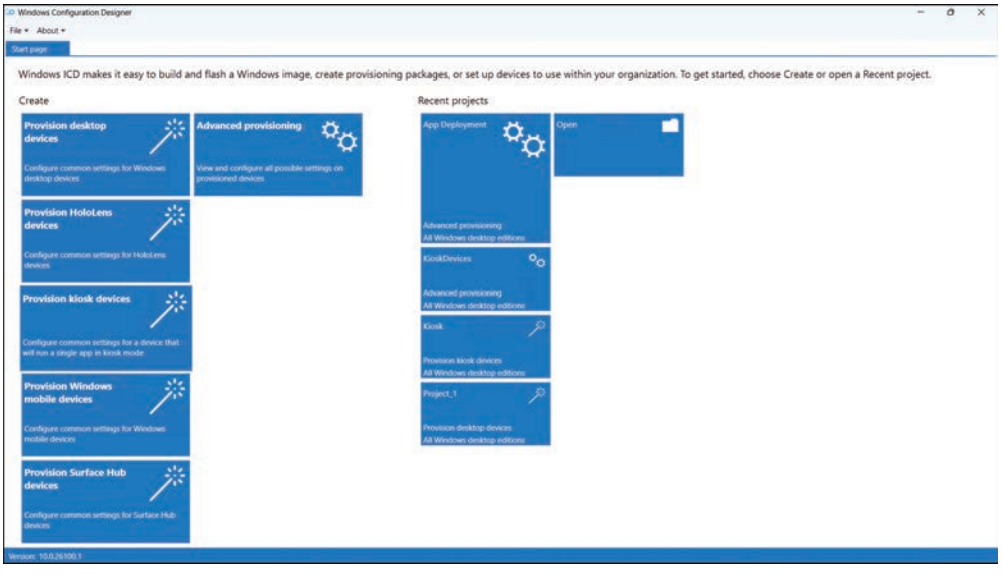

FIGURE 2-2 Creating a new provisioning package

Use the following procedure to create your provisioning package to deploy a universal line-of-business (LOB) app:

1. Select the **Advanced provisioning** tile.
2. In the **New project** wizard, on the **Enter project details** page, enter the name and a meaningful description for your provisioning package. For example, enter **Deploy LOB App1** and then select **Next**.

3. On the **Choose which settings to view and configure** page, select **All Windows desktop editions,** and select **Next**.
4. On the **Import a provisioning package (optional)** page, select **Finish**. (You can use this option to import settings from a previously configured package that mostly, but not entirely, meets your needs.)
5. On the **Available customizations** page, in **View**, select **All settings**, and then expand **Runtime settings**, as displayed in Figure 2-3.

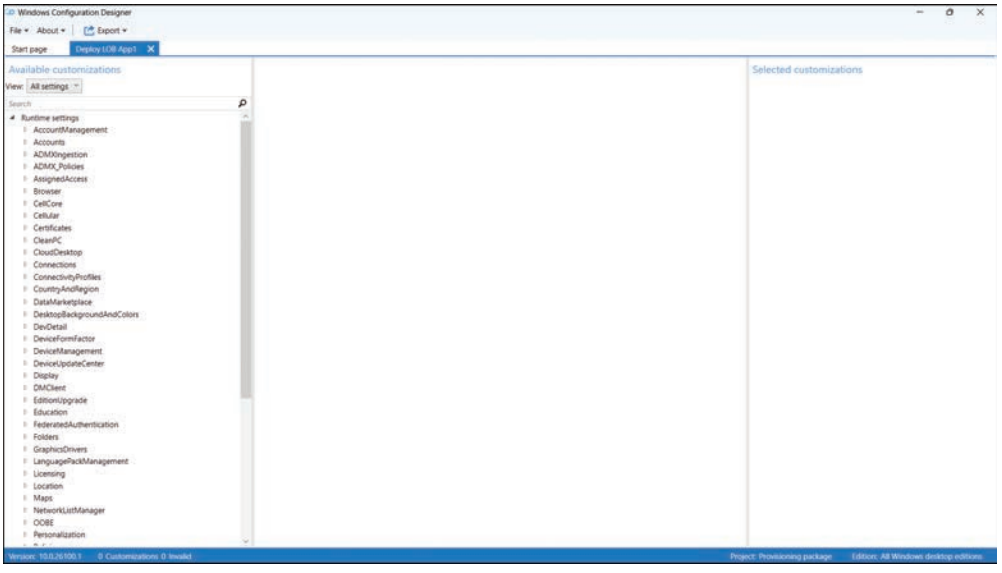

FIGURE 2-3 Available customizations for your provisioning package

6. On the **Available customizations** page, in the navigation pane, expand **Universal-AppInstall**, and then select **DeviceContextApp**.
7. In the details pane, in the **PackageFamilyName** text box, enter a name for this collection of apps. For example, enter **LOB App1**.
8. Select the **PackageFamilyName: LOB App1** node.
9. In the **ApplicationFile** text box, select **Browse**. Navigate to and select the `.appx` file representing your app, as displayed in Figure 2-4. Click **Open**.
10. In the **File** menu, select **Save** and note the location of the saved provisioning package file.
11. When prompted, click **OK**.

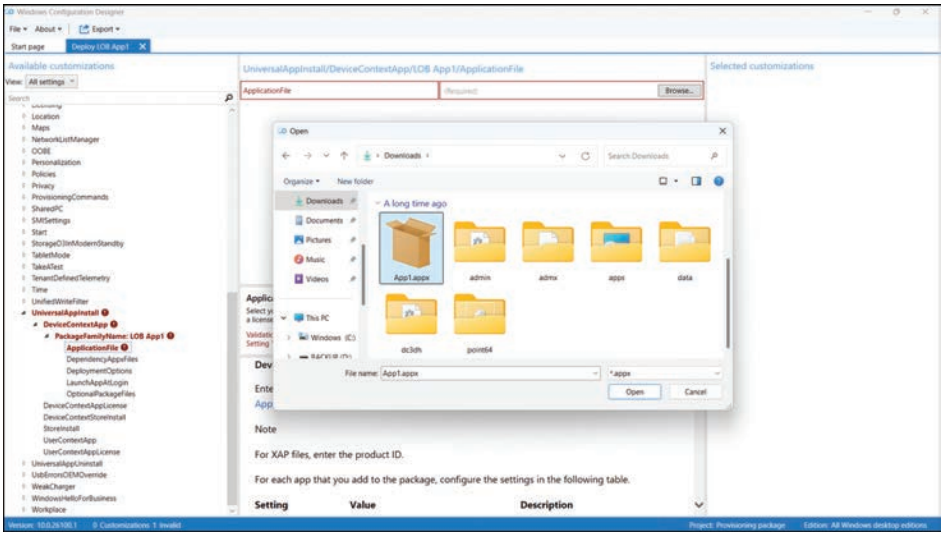

FIGURE 2-4 Adding an app to a provisioning package

You have created a customization for your app and are now ready to deploy this customization by applying the provisioning package.

> ***NOTE*** **DEPLOY POWERSHELL SCRIPTS FROM PROVISIONING PACKAGES**
>
> **If you want to use PowerShell scripts with provisioning packages, select All Windows Desktop Editions on the Choose Which Settings To View And Configure page within Advanced Provisioning. You can then add command line files in the Runtime `Settings\ProvisioningCommands\DeviceContext` area of the available customizations. To view detailed information about using scripts in provisioning packages, see *https://learn.microsoft.com/windows/configuration/provisioning-packages/provisioning-script-to-install-app*.**

Apply provisioning packages

After you have configured the settings within the Windows Configuration Designer, you export the provisioning package to a `.ppkg` file. To export your provisioning package, use the following procedure in the Windows Configuration Designer:

1. Select the project file from the **Recent Projects** area of the **Start page** or select **File** and locate the project file. (It should use the project's name and have an `.icdproj` file extension.)
2. On the menu bar, select **Export** | **Provisioning package**.
3. In the **Build** wizard, on the **Describe the provisioning package** page, the **Name** box is already complete with the project name. You can now specify the package version number and **Owner** information, such as **IT Admin**. Complete this information and select **Next**.

4. To secure the .ppkg file, you can optionally encrypt the package and digitally sign it. Once signed, only packages that are trusted can be applied on a client computer. On the **Select security details for the provisioning package** page, choose whether you want to encrypt or sign your package (or both) and then select **Next**. (To digitally sign your package, you must have an appropriate digital certificate that users of your package trust.)
5. On the **Select where to save the provisioning package** page, specify where you want to store the package and then select **Next**.
6. On the **Build the provisioning package** page, select **Build**. Your provisioning package is exported to your specified location.
7. The **All done** page appears. Make a note of the package details and then select **Finish**.
8. You can now apply the package to client devices and run the `.ppkg` file.

You can deploy the provisioning package to users by sending the package via email, physical media, or by sharing the file using OneDrive for Business. The settings are applied to the target device by one of the following methods:

- Running the `.ppkg` file
- Adding the provisioning package using the Settings app
- Use the `Add-ProvisioningPackage` Windows PowerShell cmdlet

Provisioning packages can be applied to a device during the first-run experience when a device is first turned on using a USB drive containing the provisioning package or after the out-of-box experience (OOBE) has been completed.

NEED MORE REVIEW? **APPLY A PROVISIONING PACKAGE DURING INITIAL SETUP**

To review further details about applying provisioning packages during OOBE, refer to the Microsoft website at *https://learn.microsoft.com/windows/configuration/provisioning-packages/provisioning-apply-package#during-initial-setup*.

Manage and troubleshoot provisioning packages

You have already learned how using provisioning packages as part of your dynamic provisioning of Windows 11 can simplify your deployment processes.

The Windows Configuration Designer (WCD) tool can be installed from the Microsoft Store as an app, which allows it to be regularly updated. Alternatively, you can install the Windows Configuration Designer tool as part of Windows ADK.

The WCD interface is simple, and common tasks are offered using the available wizards, which can be used to create a provisioning package that can be used in the following environments:

- **Provision desktop devices** Provides the typical settings for Windows 11 desktop devices.

- **Provision HoloLens devices** Provides the typical settings for Windows 11 Holographic devices, such as HoloLens headsets.
- **Provision kiosk devices** Provides the typical settings for a device running a single app.
- **Provision Windows mobile devices** Provides the typical settings for Windows 11 mobile devices.
- **Provision Surface Hub devices** Provides the typical settings for Surface Hub devices.
- **Advanced provisioning** Enables you to view and configure all available settings. Choose this option if you are unsure which specific package type to use.

Most provisioning packages will be aimed at provisioning Windows 11 desktop devices and will use the advanced configuration option because this allows the greatest customization.

Provisioning packages offer administrators a quick and simplified mechanism to configure devices securely. Once created, the settings within a `.ppkg` file can be viewed using the WCD and edited using the built-in wizards or the advanced editor. When provisioning packages that need to be deployed to remote devices, they can be protected using encryption and signed.

Several usage scenarios for provisioning packages are shown in Table 2-3.

TABLE 2-3 Usage Scenarios for Provisioning Packages

Scenario	Phase	Description
New devices with Windows 11 need to have apps deployed to the devices.	New device	Provisioning packages can be used to deploy apps to devices.
Existing Windows 11 Pro devices need to be upgraded to Windows 11 Enterprise.	Upgrade	Provisioning packages can be used to change the Windows edition by deploying product keys or licenses using the Edition Upgrade settings.
You must update device drivers on Windows 11 devices.	Maintain	Provisioning packages can be used to deploy device drivers to devices.

When using provisioning packages, you might need to troubleshoot them if devices are not configured as expected.

There are several areas on which you can focus your attention when troubleshooting provisioning packages, as follows:

- Configuration errors and missing customizations
- Expired Entra ID Token
- Export errors, including encryption and signing issues
- User issues
- Advanced troubleshooting

If you have deployed the `.ppkg` file to multiple devices, and they have all failed to process the required changes, then you should first inspect the provisioning package. Locate the

project file (with the `.icdproj` file extension) and open it using the WCD. You should then inspect the settings and confirm that they match your expectations and the design specification or change the documentation for the provisioning package.

If you use the configuration wizard to configure automatic enrollment into Entra ID, you should ensure that the bulk token embedded inside the provisioning package has not expired. By default, this token is set to expire one month after creation, though you can manually set the token expiry date to 180 days after the creation date. If the package is used after the Bulk Token has expired, the package will fail to install. You must edit the package, apply for a new Bulk Token, and re-export the package.

After verifying the customization settings are correct, you should export the package again. Increment the version number to avoid confusion with the package's previous version. Packages with the same versioning number will not be applied to the same target device twice.

If issues are suspected with either the encryption or signing of the package, you can export without these enhancements and redeploy to your test machine to determine whether the issue remains.

For users, devices can be configured by placing the provisioning package on a USB drive and inserting it during the initial OOBE setup phase. Windows Setup should automatically recognize the drive and ask the user if they want to install the provisioning package. If the package is not recognized, check that the file is in the root directory of the USB drive.

You can use the Windows Performance Recorder to perform advanced troubleshooting for provisioning packages on user devices. The Windows Performance Recorder in the Windows ADK offers advanced Event Tracing for Windows. The system events recorded by this tool can be analyzed using Windows Performance Analyzer, available from the Windows ADK or Microsoft Store.

NEED MORE REVIEW? **PROVISIONING PACKAGES FOR WINDOWS 11**

To review further details about provisioning packages, refer to the Microsoft website at *https://learn.microsoft.com/windows/configuration/provisioning-packages/provisioning-packages*.

Plan and implement device upgrades for Windows 11

If an organization's environment is running fully working and supported Windows 10 operating systems, Microsoft recommends using an in-place upgrade strategy to deploy Windows 11 to these devices.

The upgrade process updates the operating system while retaining the apps, user data, and user settings. Utilizing in-place upgrades can offer a low-risk, quick, and reliable method of transforming devices and enabling users to be productive once the upgrade has been completed.

If administrators fear that an existing installation is "old" or not a reliable candidate to upgrade to Windows 11, they could redeploy the legacy operating system—complete with

apps, policies, and settings—and then perform the in-place upgrade shortly afterward. Another benefit of using an in-place upgrade approach is that driver and app compatibility issues are minimized.

When planning to deploy Windows 11, you should consider whether your existing version of Windows can be directly upgraded to Windows 11 and whether you can migrate from one version of Windows 11 to a different version of the same release.

When upgrading from one version of Windows to a later version, the upgrade process can preserve personal data, settings, and applications. If you recently upgraded from a previous version of Windows and want to downgrade, you can only downgrade to Windows 10 within 10 days of upgrading when using the built-in rollback process within the Settings app.

In a few situations, you can perform an edition downgrade. In these situations, you should note that all personal data is maintained, though any incompatible applications and settings will be removed.

> ***NOTE*** **WINDOWS 11 LTSC**
>
> **An in-place upgrade from Windows 7, Windows 8.1, or Windows 10 Semi-Annual Channel to Windows 11 Long Term Servicing Channel (LTSC) version is not supported. For more information on Windows 11 LTSC and how it should be used, visit *https://learn.microsoft.com/windows/deployment/update/waas-overview#long-term-servicing-channel*.**

Windows upgrade and downgrade paths

You should review the information in Tables 2-4 and Table 2-5, which display the various upgrade and downgrade paths available in Windows 10 and 11.

TABLE 2-4 Windows 10 Upgrade and Downgrade Paths

Starting edition	Destination Windows 10 edition				
	Windows 10 Home	**Windows 10 Pro**	**Windows 10 Pro Education**	**Windows 10 Education**	**Windows 10 Enterprise**
Windows 10 Home	X	X	X	X	
Windows 10 Pro	D	X	X	X	X
Windows 10 Education		D	D	X	
Windows 10 Enterprise		D	D	X	X

X = The upgrade path is supported. D = The downgrade path is supported.

The upgrade paths for Windows 11, excluding the N editions, are shown in Table 2-5.

TABLE 2-5 Windows 11 Upgrade and Downgrade Paths

Starting edition	Destination Windows 11 edition				
	Windows 11 Home	Windows 11 Pro	Windows 11 Pro Education	Windows 11 Education	Windows 11 Enterprise
Windows 10 Home		X	X	X	
Windows 10 Pro			X	X	X
Windows 10 Education				X	
Windows 10 Enterprise				X	X
Windows 10 Pro Education				X	
Windows 10 Cloud		X	X	X	X
Windows 10 Core			X	X	X
Windows 11 Home		X	X	X	
Windows 11 Pro			X	X	X
Windows 11 Education				X	
Windows 11 Enterprise				X	X
Windows 11 Pro Education				X	
Windows 11 Cloud		X	X	X	X
Windows 11 Core			X	X	X

X = The upgrade path is supported. D = The downgrade path is supported.

NOTE **WINDOWS 11 EDITION UPGRADE**

The process is quick and easy for organizations performing a supported upgrade from one edition of Windows 11 to another. The new product key can be added to the device and will be upgraded. There are multiple possible variants of the edition upgrade; some require a reboot, and others allow the upgrade without a reboot.

Downgrade paths due to license expiration

Organizations with an expired or expiring volume license agreement can opt to downgrade their edition of Windows 11 to an edition with an active license. Like the options for performing an edition upgrade, if a downgrade path is supported, the user's apps and settings will be available in the downgraded version of Windows 11. In this way, you can continue to use Windows.

Plan and configure user state migration

Users are at the heart of every organization, and data is seldom held on a device. Users often invest a lot of time and effort in configuring their Windows environment. This can include customizing their apps, such as developing templates and toolbars.

Losing app data and personalized settings can significantly affect the productivity and even the morale of users. By migrating their Windows and app settings, you will likely reduce the number of help desk calls and avoid user downtime required to customize their desktops and find missing files.

Most user data is contained in a profile, and the user folders are synchronized to a cloud-based location by using a solution such as Enterprise State Roaming in Entra ID.

When devices contain data, you might want to transfer or migrate that data to a new device. Microsoft supports this migration process using the Windows ADK tools. These tools and processes require specialist knowledge and often add significant time and cost to the rollout project.

PRESERVING USER STATE DATA

When you upgrade to Windows 11, unless you perform an in-place upgrade, you might overlook the migration of the user's app data and Windows settings.

You should aim to migrate user settings, which are often contained in their user profiles, during your Windows 11 deployment project.

Following are the two traditional methods of upgrading to Windows 11 that don't involve an in-place upgrade:

- **Side-by-side migration** This type of migration is used when the source and destination computers for the upgrade are different machines. You install a new computer with Windows 11 and then migrate the data and user settings from the computer running the older operating system to the new computer.
- **Wipe-and-load migration** In this scenario, the source and destination computers are the same. You back up the user data and settings to an external location and then install Windows 11 on the user's existing computer. Afterward, you restore user data and settings.

USER STATE MIGRATION TOOL

You can automate much of the user profile migration process for large-scale deployments by using deployment automation tools, such as Configuration Manager or MDT. Both solutions use the User State Migration Tool (USMT), part of the Windows ADK.

For smaller migrations, you can use USMT directly from the command line to capture user accounts, user files, operating system settings, and application settings; you can then migrate the captured settings to a new Windows installation.

Although quite dated, USMT has received several updates, which make it more secure and usable. It is available as a command-line tool. The features include

- **Size estimation of the migration stores** Allows you to gauge the amount of storage you will need to perform a data capture for a targeted Windows device.

- **Encryption of the migration stores** This protects the information stored in the user's profile, reducing the risk of data being compromised while being stored.
- **Hard links to the migration store** This is useful for PC refresh scenarios that do not involve the reformatting of the primary Windows partition. Using a hard-link migration store with USMT allows the restore process to come from the same local partition, significantly increasing transfer performance.
- **Perform offline migrations** You can run migrations from within a Windows Preinstallation Environment (WinPE). You can also perform migrations from the data stored in `Windows.old` directories.

You perform a user state migration in two phases as follows:

1. Settings and data are captured (collected) from the source and stored in a secure migration store using the ScanState tool.
2. Captured settings and data are restored to the destination computer using the LoadState tool.

Also, USMT can be scripted to enhance efficiency, and it can be customized with settings and rules using the following migration XML files:

- `MigApp.xml`
- `MigDocs.xml`
- `MigUser.xml`
- Custom XML files that you can create

The types of data that USMT can capture and migrate are shown in Table 2-6.

TABLE 2-6 Data Types Accessible by USMT

Data type	Example	Description
User accounts, user settings, and user data	My Documents, My Video, My Music, My Pictures, Desktop files, Start menu, Quick Launch settings, and Favorites	Local and domain-based user accounts. Folders from each user profile.
Shared user data	Shared Documents, Shared Video, Shared Music, Shared Desktop files, Shared Pictures, Shared Start menu, and Shared Favorites	Folders from the Public profiles.
Files, folders, and settings	Files, folders, and Registry keys	USMT searches fixed drives, collecting files with any file name extensions, folders, and Registry keys defined in the configuration XML file.
NTFS permissions	Access control lists (ACLs)	USMT can migrate the ACL information for specified files and folders.
Operating system components	Mapped network drives, network printers, folder options, EFS files, users' personal certificates, and Internet Explorer settings	USMT migrates most standard operating system settings.

Data type	Example	Description
Supported applications settings	Microsoft Office, Skype, Google Chrome, Adobe Acrobat Reader, Apple iTunes, and more	USMT will migrate settings for many applications, which can be specified in the MigApp.xml file. The version of each application must match the source and destination computers. With Microsoft Office, USMT allows migration of the settings from an earlier version of an Office application.

As displayed in Table 2-6, the list of settings that can be migrated is quite extensive. However, the following settings cannot be migrated with USMT:

- Local printers and hardware-related settings
- Device drivers
- Passwords
- Customized icons for shortcuts
- Shared folder permissions
- Files and settings if the operating systems have different languages installed

USMT comprises several command-line tools and configuration files, which use XML files to store customizations. The USMT components are described in Table 2-7.

TABLE 2-7 USMT Components

Component	Description
ScanState.exe	Scans a source computer, collects files and settings, and writes them to a migration store. (The store file can be password protected and can be compressed and encrypted if required. You cannot use the `/nocompress` option with the `/encrypt` option.) You can turn off the default compression with the `/nocompress` option.
LoadState.exe	Migrates the files and settings from the migration store to the destination computer.
USMTUtils.exe	Used to compress, encrypt, and validate the migration store files.
Migration XML files	`MigApp.xml`, `MigUser.xml`, or `MigDocs.xml` files, and custom XML files that USMT uses to configure the process.
Config.xml	Used with the `/genconfig` option to exclude data from a migration.
Component manifests	Controls which operating system settings are to be migrated. These manifests are specific to the operating system and are not modifiable.

Use the following steps to initiate the collection of the files and settings from the source computer and back up the settings and files to a network share:

1. Ensure you have a backup of the source computer.
2. Close all applications.

Index

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V

W-X-Y-Z