Microsoft

Deploying Windows 10

Automating deployment by using System Center Configuration Manager

Andre Della Monica, Russ Rimmerman, Alessandro Cesarini, and Victor Silveira

www.dbooks.org

PUBLISHED BY
Microsoft Press
A division of Microsoft Corporation
One Microsoft Way
Redmond, Washington 98052-6399

Copyright © 2016 by Microsoft Corporation

All rights reserved. No part of the contents of this book may be reproduced or transmitted in any form or by any means without the written permission of the publisher.

Library of Congress Control Number:
ISBN: 978-1-5093-0186-7

Printed and bound in the United States of America.

First Printing

Microsoft Press books are available through booksellers and distributors worldwide. If you need support related to this book, email Microsoft Press Support at mspinput@microsoft.com. Please tell us what you think of this book at http://aka.ms/tellpress.

This book is provided "as-is" and expresses the author's views and opinions. The views, opinions and information expressed in this book, including URL and other Internet website references, may change without notice.

Some examples depicted herein are provided for illustration only and are fictitious. No real association or connection is intended or should be inferred.

Microsoft and the trademarks listed at http://www.microsoft.com on the "Trademarks" webpage are trademarks of the Microsoft group of companies. All other marks are property of their respective owners.

Acquisitions Editor: Karen Szall
Developmental Editor Karen Szall
Editorial Production: Dianne Russell, Octal Publishing, Inc.
Copyeditor: Bob Russell, Octal Publishing, Inc.
Cover: Twist Creative • Seattle

Visit us today at

microsoftpressstore.com

- **Hundreds of titles available** – Books, eBooks, and online resources from industry experts
- **Free U.S. shipping**
- **eBooks in multiple formats** – Read on your computer, tablet, mobile device, or e-reader
- **Print & eBook Best Value Packs**
- **eBook Deal of the Week** – Save up to 60% on featured titles
- **Newsletter and special offers** – Be the first to hear about new releases, specials, and more
- **Register your book** – Get additional benefits



Microsoft

www.dbooks.org

Contents

Foreword ..... **v**
Introduction ..... **vi**
Errata, updates, & book support vi
Free eBooks from Microsoft Press vii
We want to hear from you vii
Stay in touch vii
Chapter 1: Why implement Windows 10? **1**
The Welcome experience 2
What's new in the user interface 4
Customizing the Start menu 5
Introducing Action Center 6
Switching between Desktop mode and Tablet mode 7
Using virtual desktops 8
Creating a new virtual desktop 8
Switching between virtual desktops 9
Using Snap 9
Cortana 10
Accessing Cortana settings 11
Cortana voice commands 11
Windows startup enhancements 12
Push Button Reset improvements 12
Microsoft Edge 13
Fixing specific sites 13
About security 15
Microsoft Passport 16
Windows Hello 16
Isolated User Mode 19
The Windows 10 upgrade process 20

Chapter 2: Windows 10 deployment options **21**
In-place upgrade 21
Predeployments steps 22
Step 1: Choosing the correct media 23
Step 2: Assessing readiness 23
Step 3: Gathering driver packages 28
A cue for testing applications 28
Manual in-place upgrade 28
Phase 1: Down Level (Old OS) 29
Phase 2: Start into WinRE (copying files) 31
Phase 3: First reboot in Windows 10 (installing features and drivers) 32
Phase 4: Second reboot in Windows 10 (configuring settings) 32
Recoverability 32
Traditional deployments 33
Bare-metal installation 33
Wipe-and-load (refresh) 34
Replace 34
Windows To Go 34
Windows Update approach 35
Get Windows 10 App 37
OS upgrade via Windows Server Update Services 39
Prerequisites 39
Configuring WSUS to support in-place upgrades 40
Configuring policies to use WSUS 41
Moving the focus to Configuration Manager 41
Chapter 3: Configuration Manager Operating System Deployment concepts **42**
The purpose of OSD 43
OSD terminology 44
Infrastructure requirements 44
WinPE 46
Task sequences 48
Task sequence variables 50
Drivers and driver packages 52
Image deployment 54
Scheduling deployments 56
Unknown computers 57
UEFI versus BIOS 58
Reporting 59

www.dbooks.org

Advanced concepts ... 60
Logging ... 60
Prestart commands ... 61
User Device Affinity ... 61
Online resources ... 62
Chapter 4: Using System Center Configuration Manager to deploy Windows 10 ... 63
Microsoft Deployment Toolkit integration with Operating System Deployment ... 64
Windows Assessment and Deployment Kit ... 66
Obtaining and importing the Windows 10 image ... 69
Customizing the Windows 10 image ... 69
In-box applications ... 70
Group Policies ... 70
Deploying and supporting Windows 10 ... 70
Managing disk configurations ... 71
Upgrade scenarios ... 74
Optimizing the Windows 10 image deployment ... 81
Monitoring the Windows 10 image deployment ... 82
After the Windows 10 image deployment ... 83
About the authors ... 84

Foreword

Windows 10 represents a major paradigm shift for Microsoft and the Windows ecosystem in general as we modernize the platform by introducing "as a service" capabilities. Hundreds of millions of devices are already running Windows 10 today. Businesses are beginning to evaluate the new capabilities of Windows 10, including Windows as a service, as part of their deployment plans. With Windows 7 recently transitioning into extended support, businesses need to begin planning for the future of their Windows operating system environment.

Although there are many aspects to consider in managing a Windows device, one of the essential early stages of the lifecycle is deployment. More than 70 percent of businesses use System Center Configuration Manager for PC management, and that market share continues to grow every quarter. Configuration Manager is an industry leader, and the Operating System Deployment (OSD) feature is one of the most popular and frequently used. The product supports many traditional operating system deployment methods as well as support for newer Windows 10 deployment scenarios such as in-place upgrade.

Andre, Alessandro, Victor, and Russ are seasoned Microsoft premier field engineers with deep technical product knowledge and real-world experience. In this book, they share this knowledge and experience with Windows 10 and Configuration Manager to help you get your deployment underway.

Aaron Czechowski
Senior program manager, Enterprise Client Management product team

www.dbooks.org

Introduction

The world, Microsoft, and the technology industry have all changed. There is no longer a half decade, or two or even three years for operating system (OS) upgrade cycles. Companies demand a continuous flow of productivity in their businesses.

Despite all of the logistics and costs involved when upgrading to a new OS by using the wipe-and-load method, companies and enterprises often developed their own methods to upgrade their operating systems because there was not much control and predictability provided by the upgrade process.

Even though deploying Windows 10 is a fairly new task—Windows 10 was released in July, 2015—most enterprises plan to deploy Microsoft's new revolutionary OS, which addresses the challenges of the traditional OS deployments, and it brings new features and security enhancements, to name but a few of the new capabilities of Windows 10.

As the authors of this book, we have called upon our real-world field experience to provide you with insights and tips on why and how to implement Windows 10 and its deployment using System Center Configuration Manager.

Here's what the book contains:

Chapter 1 provides highlights of what's new in Windows 10 and why you should implement it.

Chapter 2 familiarizes you with the Windows 10 deployment options as well as with some tips about which deployment methods to use when planning to upgrade to Windows 10.

Chapter 3 examines the Operating System Deployment (OSD) concepts to prepare you for deployment when using System Center Configuration Manager.

Chapter 4 is intended to be a walk-through—a tour of how to deploy Windows 10 using System Center Configuration Manager and its details.

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:

http://aka.ms/DeployWin10/errata

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

If you need additional support, email Microsoft Press Book Support at mspinput@microsoft.com.

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 http://support.microsoft.com.

Free eBooks from Microsoft Press

From technical overviews to in-depth information on special topics, the free eBooks from Microsoft Press cover a wide range of topics. These eBooks are available in PDF, EPUB, and Mobi for Kindle formats, ready for you to download at:

http://aka.ms/mspressfree

Check back often to see what is new!

We want to hear from you

At Microsoft Press, your satisfaction is our top priority, and your feedback our most valuable asset. Please tell us what you think of this book at:

http://aka.ms/tellpress

We know you're busy, so we've kept it short with just a few questions. Your answers go directly to the editors at Microsoft Press. (No personal information will be requested.) Thanks in advance for your input!

Stay in touch

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

www.dbooks.org

CHAPTER 1

Why implement Windows 10?

The world is being rapidly transformed with big trends such as the cloud, big data, and social media. These are all technology *transformation accelerator agents* that will change the business world forever. Mobility is also an important transformation accelerator agent in the evolution of the technology as a whole. Because of the growth of mobility, work is no longer a place, but a compilation of experiences that follows us through various devices, applications, and data.

Most professionals—and not just IT professionals—are working physically from two or three different locations. This concept extends to devices, apps, and Big Data. You probably work from two or three different devices, not including your personal devices. You might use four or five or more apps to perform your work activities on a daily basis.

The future is about more than the mobility of the device; the mobility of the *experience* will be an important factor to the technology industry. Windows 10 will help you to take advantage of these trends and be ready for the challenges ahead.

When it comes to mobility and operating systems and devices, the main concerns for most enterprises focus on security, user application accessibility, and the problems of having big complex deployments. Windows 10 attempts to address all of these valid concerns by providing a familiar and productive experience, regardless of the device type. For enterprises, one platform means using one management paradigm and security model across all devices.

Windows universal apps run on all Windows-based device types (or they can be limited to specific devices). Windows universal apps make it possible for the user interface (UI) to scale seamlessly from phone to tablet and beyond.

This chapter covers:

- The Welcome experience
- What's new in the user interface

- Switching between PC mode and Tablet mode
- Using virtual desktops
- Using Snap
- Cortana
- Windows startup changes
- Microsoft Edge
- About security
- The Windows 10 upgrade process

The Welcome experience

The Windows 10 experience is designed to be as simple as possible. The Welcome experience, or the out-of-box experience (OOBE), helps you to understand the different steps you need to perform when starting a Windows device for the first time.

The Welcome experience changes when your device is not connected to the Internet. In addition, the experience varies depending on which edition of Windows 10 is running on a device (Windows 10 is available in three different editions: Home, Professional, and Enterprise).

For example, with the Home edition, you sign in by using Microsoft account, as shown in Figure 1-1. A Microsoft account comprises a user ID (either an email address or phone number) and a password.

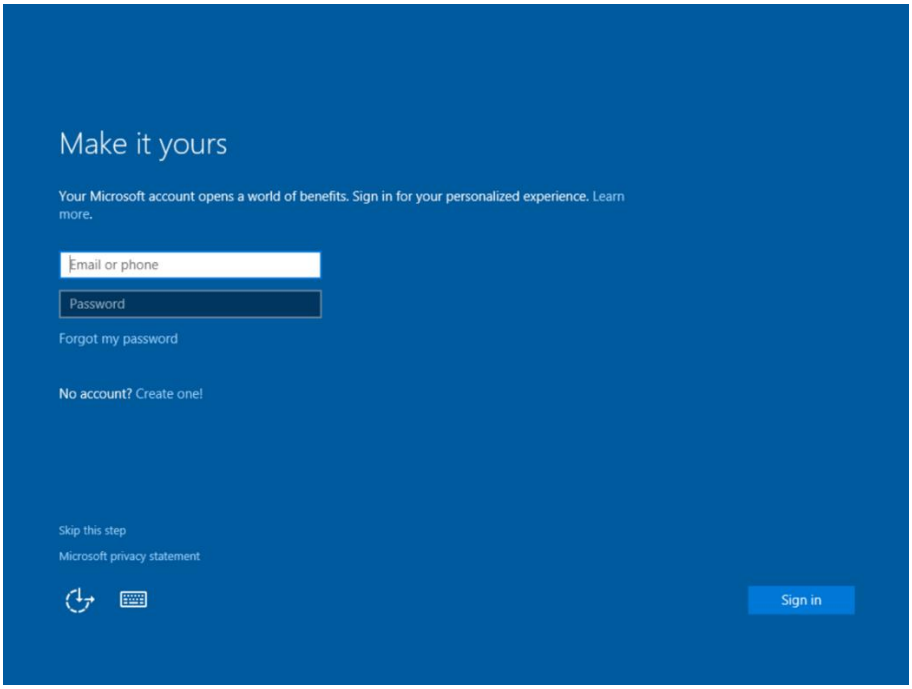


Figure 1-1: The Welcome screen for Windows 10 Home edition

With the Windows 10 Professional edition, the Welcome screen asks you to identify who owns the device. You can select My Organization or I Own It. Select one and then click Next, as shown in Figure 1-2. You are then asked to sign in.

www.dbooks.org

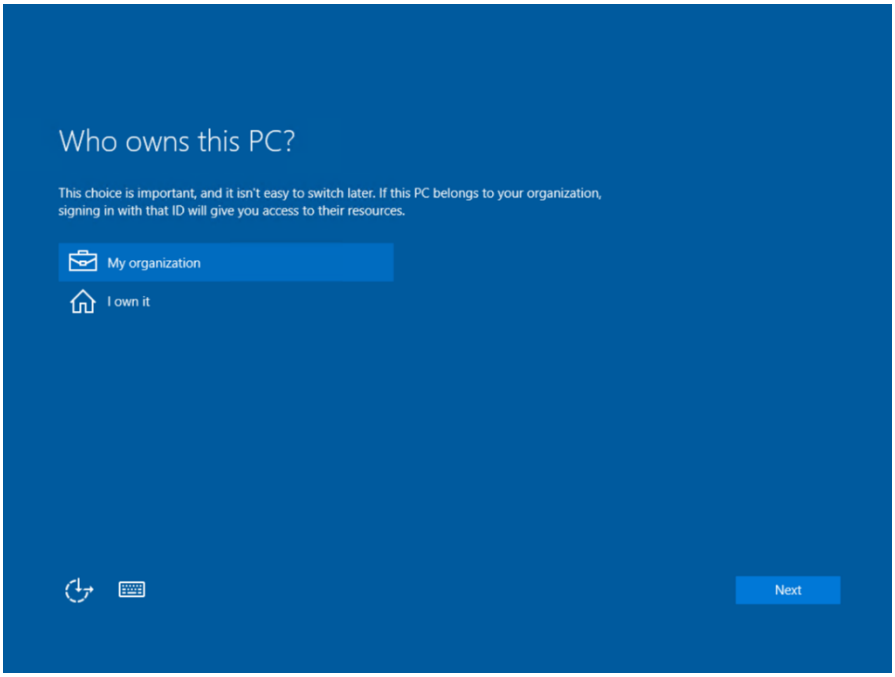


Figure 1-2: The Welcome screen for Windows 10 Professional edition

When using Windows 10 Enterprise edition connected to the Internet, you can specify an Enterprise account or you can create a local account to join a domain. Figure 1-3 demonstrates that there is a new option, Join Azure AD, with which you can join Microsoft Azure Active Directory, which is required if your enterprise implements Azure Active Directory.

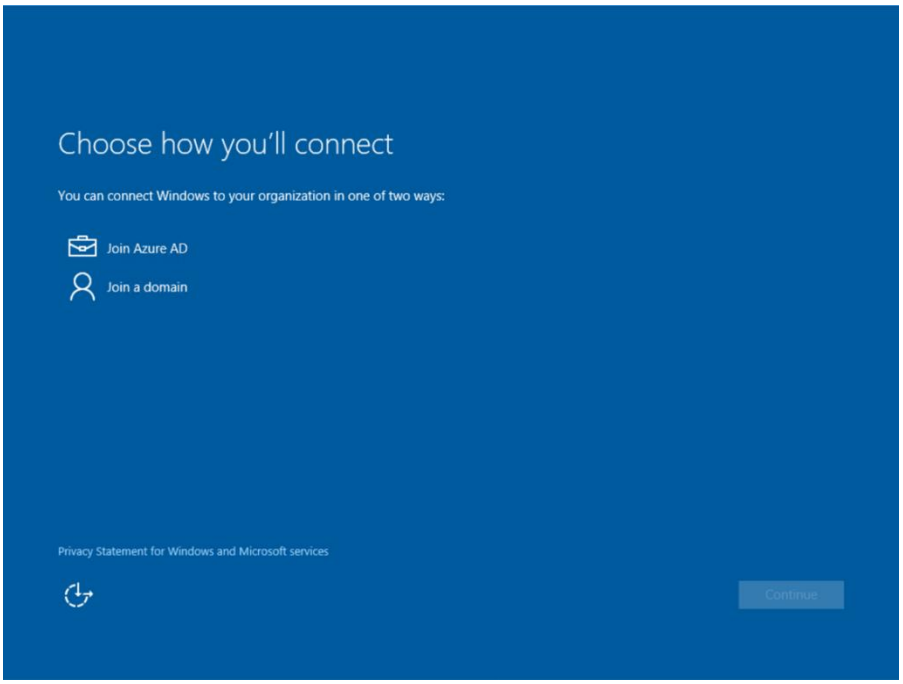


Figure 1-3: The Welcome screen for Windows 10 Enterprise edition, connected to the Internet

Unlike using the Managed Service Account (MSA), selecting Join Azure AD does not create a local account. This is the reason why there is the option for joining a domain, which does indeed create a local account, and gives you the option to join a domain later.

Important To sign in to the Azure Active Directory environment, you must turn on device registration for the account. The Windows setup is redirected to a federated server if necessary.

After the OOBE, Windows finalizes the configuration you defined and prepares for the first sign-in.

When Windows 10 is enrolled in a mobile device management environment, each user must enforce security policy and create a work PIN if required. This PIN is used for Microsoft Passport, which replaces passwords with a strong two-factor authentication process. This means that the user must present a combination of two means of identification.

By default, users are configured only with the standard text password option, but it is important to consider the password types that are available:

- Password
- PIN
- Virtual smart card
- Smart card
- Picture password

When using a picture password, the user can sign in by using a combination of gestures over a user-defined picture. For security purposes, if a projector or a beamer is detected, the actual gestures will not be shown in the projected image.

More info To learn more about using picture passwords, go to http://blogs.msdn.com/b/b8/archive/2011/12/16/signing-in-with-a-picture-password.aspx.

What's new in the user interface

After 17 years of the Windows Start menu, Microsoft introduced the Start screen in Windows 8, which was the first menu designed for both touch and nontouch devices. The user interface (UI) was easy to use for touch devices, but some users missed the small Startup menu when using a keyboard and mouse.

Windows 10 brings back the familiar Windows desktop and Start menu.

The Start menu is enhanced with resizable tiles and other new capabilities such as the ability to lock the computer, change account settings, and sign out, as shown in Figure 1-4. In addition, using the Start menu, you can access your apps, documents, pictures, and settings quickly. You can even launch advanced system tools and utilities. Note, however, that due to the various types and sizes of devices, your Start screen and Start menu will not be synchronized across your devices.

www.dbooks.org

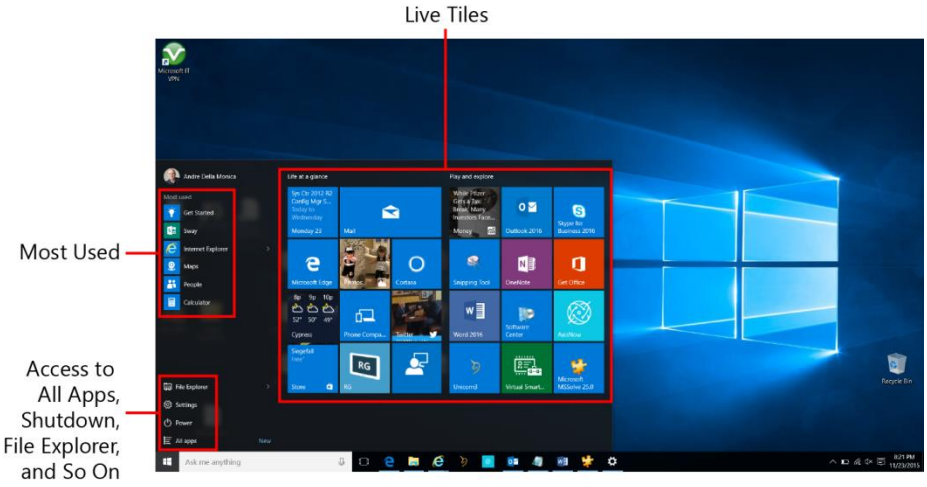


Figure 1-4: The new Start menu in Windows 10

Customizing the Start menu

Many organizations need to customize the Start menu. For example, they might want to add their business applications and utilities, add, remove, and resize tiles, change the Start screen color and accent to harmonize with those of the organization's color scheme; and apply a different desktop background.

There are multiple ways to customize the Start menu; this book focuses on one of them, which consists of a two-step process: use a Windows PowerShell command to export the new customized Layout in XML format, and then reference it into a Group Policy Object (GPO) from the Group Policy Management console.

To export the layout in XML format, use the following Windows PowerShell command:

```
Export-StartLayout –Path %temp%\StartLayout.xml –as XML
```

After running the command, copy the StartLayout.xml file to a server that has the Group Policy Management console installed, and then reference the exported XML file in the Group Policy Object (GPO) called Start Layout.

To open the Group Policy Management console, click Start > Control Panel, or simply type **Control Panel**, point to Administrative Tools, and then click Group Policy Management.

The Start Layout GPO is located at the following path from the Group Policy Management console: User Configuration > Policies > Administrative Templates > Start Menu And Taskbar.

In the Start Layout dialog box, turn on the policy setting and then, in the Start Layout File box, type the path to the exported XML file you created earlier, as shown in Figure 1-5.

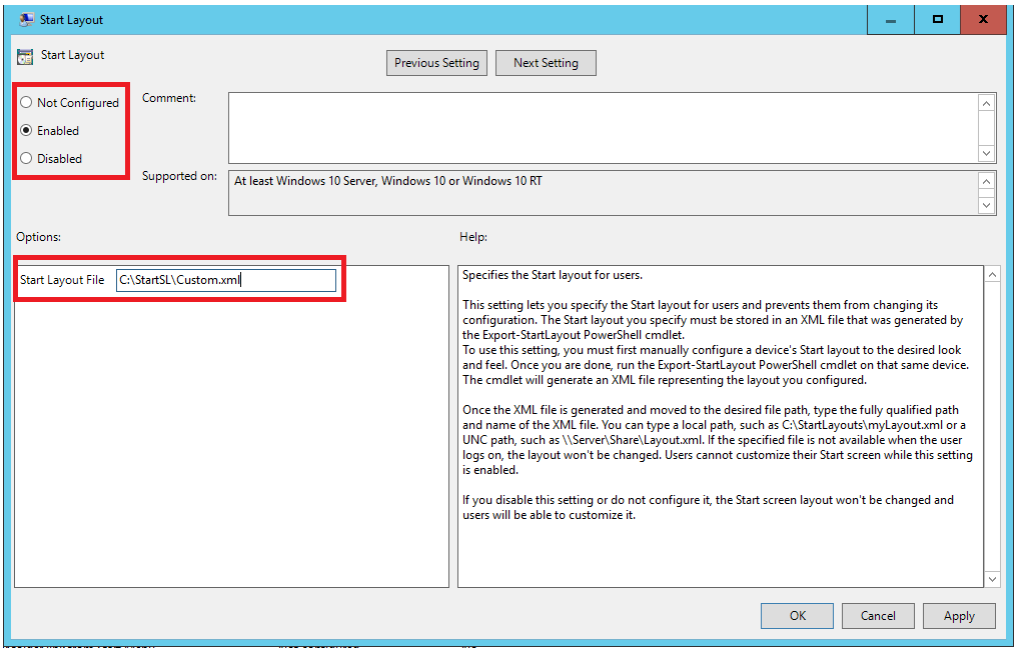


Figure 1-5: Start Layout group policy object settings from the Group Policy Management console

The Start Layout XML file gives original equipment manufacturers (OEMs) and IT professionals the option of provisioning the start layout by creating a LayoutModification.xml file. This file supports several mechanisms to modify or replace the default start layout and its tiles.

By default, new devices running Windows 10 for desktop editions have a Start menu with two columns of tiles unless the Tablet mode is turned on.

Tablet mode is turned on by default for devices with screen sizes that are less than 10 inches. For these devices, the desktop starts in full screen mode, instead of the traditional Start screen in the previous Windows versions.

You can customize the following options in Windows 10:

- Specify the number of columns in the Start menu
- Turn on or off Tablet mode
- Set Full Screen Start On Desktop to on or off

In the following example, the Start menu is set to full screen with two columns.

```
<LayoutModificationTemplate xmlns="http://schemas.microsoft.com/Start/2014/LayoutModification"
xmlns:defaultlayout="http://schemas.microsoft.com/Start/2014/FullDefaultLayout"
xmlns:start="http://schemas.microsoft.com/Start/2014/StartLayout" Version="1"> <LayoutOptions
StartTileGroupsColumnCount="2" FullScreenStart="true" /> </LayoutModificationTemplate>
```

More info You can see Start layouts for Windows 10 desktop editions at https://msdn.microsoft.com//library/windows/hardware/mt171092.

Introducing Action Center

In earlier Windows versions, a notification was lost forever after it timed-out. Windows 10 remedies this with the new Action Center, which is similar to the notification center that was first introduced in Windows Phone 8.1.

www.dbooks.org

The Action Center, maintains a persistent list of notifications. You can view it and address your notifications at a time of your choosing. Also, there are links for performing quick actions such as turning Wi-Fi on or off, and notifications are presented when your system is under security risk.

To open the Action Center, on the Windows 10 taskbar, tap or click the button, as shown in Figure 1-6.

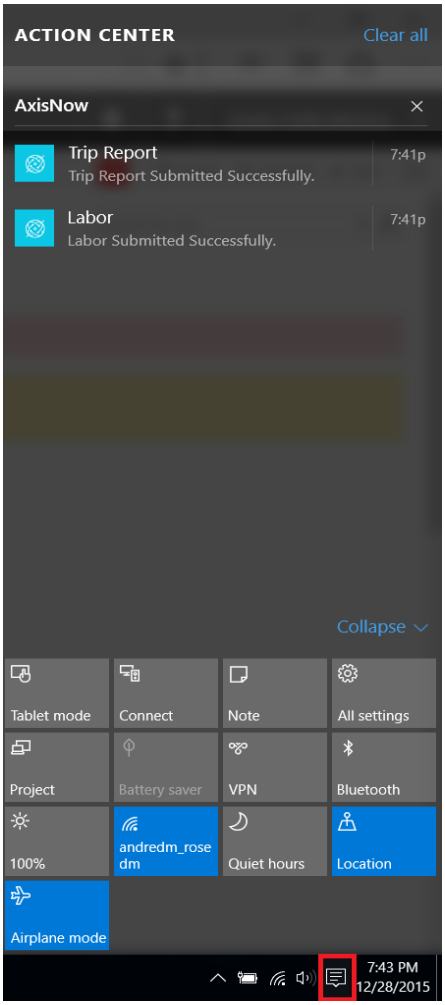


Figure 1-6: The Action Center in all Windows 10 editions

In addition, you can expand the Action Center to show 13 tiles; the main tiles are, Tablet Mode, Airplane Mode, All Settings, Bluetooth, and VPN.

Switching between Desktop mode and Tablet mode

You can switch easily between Desktop and Tablet modes in the Action Center. For example, if you are in Desktop mode and want to switch to Tablet mode, on the taskbar, click the Action Center button, and then click Tablet Mode, as shown in Figure 1-7.

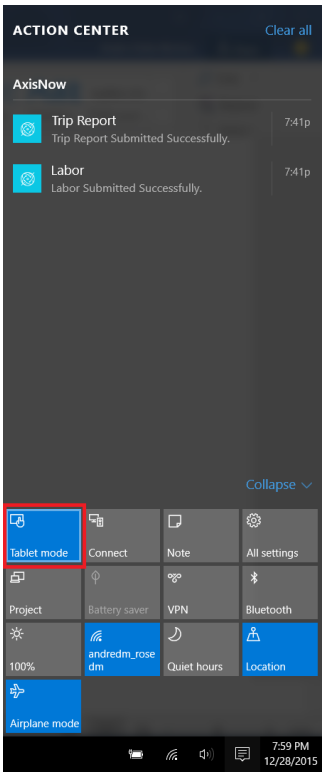


Figure 1-7: The Action Center pane with the Tablet Mode option

While in Desktop mode, the user experience is optimized for use with a keyboard and mouse. This does not mean that you cannot use touch gestures if your device supports it, but it is optimized for interacting by using a mouse and keyboard. In Tablet mode, the user experience dynamically changes to be a more touch-friendly one, including the taskbar. You can still use a mouse and keyboard, but the layout is optimized for touch-based interaction.

Important Some devices such as the Microsoft Surface can switch between modes with a hardware trigger. To switch between the desktop and the tablet mode, detach the keyboard or fold the keyboard behind the screen.

Using virtual desktops

Windows 10 adds support for using virtual desktops so that you can keep your open apps better organized. For example, you can begin using a personal app for a personal event such as birthday party plans, create a second virtual desktop that contains the required app or apps to work on the birthday plans, and use yet another virtual desktop for your work-related activities.

Creating a new virtual desktop

To create one or more new virtual desktops, on the taskbar, tap or click the Task View button, and then do either of the following:

- Near the lower right of the screen, tap or click New desktop, or, drag one of the apps thumbnail over to New Desktop.
- Right-click one of the apps thumbnail images, point to Move To, and then click or tap the New Desktop option, as shown in Figure 1-8.

www.dbooks.org

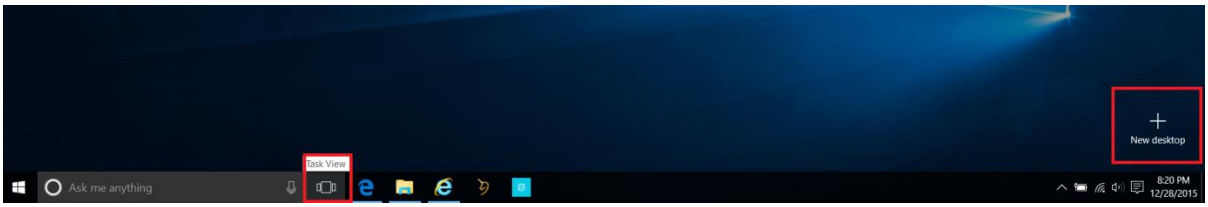


Figure 1-8: The Task View with the option to add a new virtual desktop at the lower right

Switching between virtual desktops

You can switch between the virtual desktops by following these steps:

1. On the taskbar, tap or click the Task View button.
2. Tap or click the thumbnail for the desired virtual desktop.

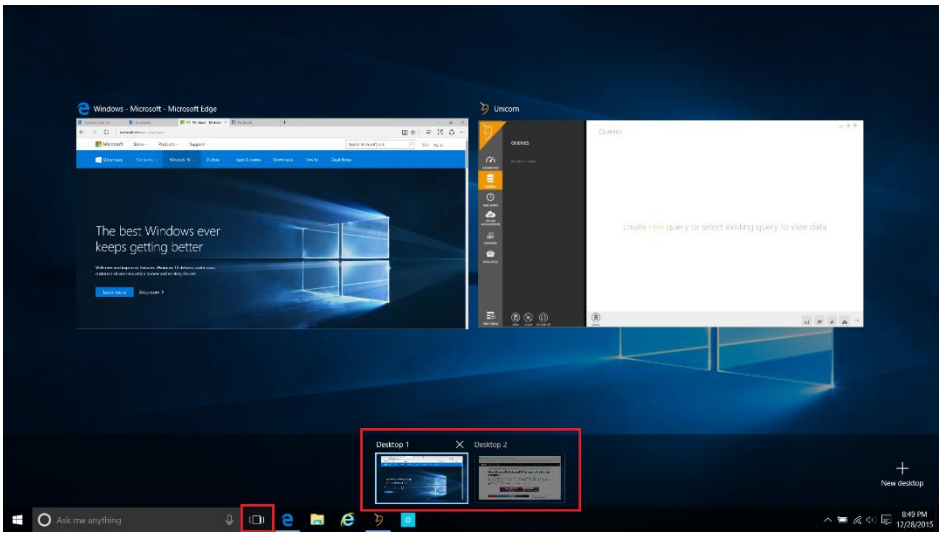


Figure 1-9: The Task View screen showing two virtual desktops

Another option is to tap or click the desired app on the taskbar, Windows 10 switches to the virtual desktop containing that app and restores the app on the desktop.

You can even move apps between desktops by opening the Task View and then clicking and dragging the application to a virtual desktop.

The Task View also makes it easy to close a virtual desktop. Each virtual desktop has a "close" button (the X in the upper-right corner) that closes its virtual desktop.

When you close a virtual desktop, the application itself remains open; it is simply moved back to the original desktop environment.

Using Snap

Windows 7 introduced a feature called Snap, which you can use to "snap" apps to the side, top, or bottom of a window. Windows 10 includes enhancements to Snap that make it even easier to manipulate the layout of opened windows on the desktop. *Snap Assist* opens when two or more apps are snapped to help you find the opened apps on your system.

Using Snap Assist, you can display apps side by side when you snap an app to the left or right. Snap Assist displays thumbnails of your other open app. Tap or click one of the thumbnails to snap it to the other half of the screen.

You can also use the Quadrant snap to arrange four windows in a two-by-two configuration if you'd like.

To snap two windows side-by-side, do the following:

1. Drag the title bar of a window to the left or right side of the screen until a half-screen outline of the window appears.
2. Release the title bar to snap the window into position.
3. Repeat steps 1 and 2 for the other window, but snapping it to the other side of the screen.

Figure 1-10 presents an example.

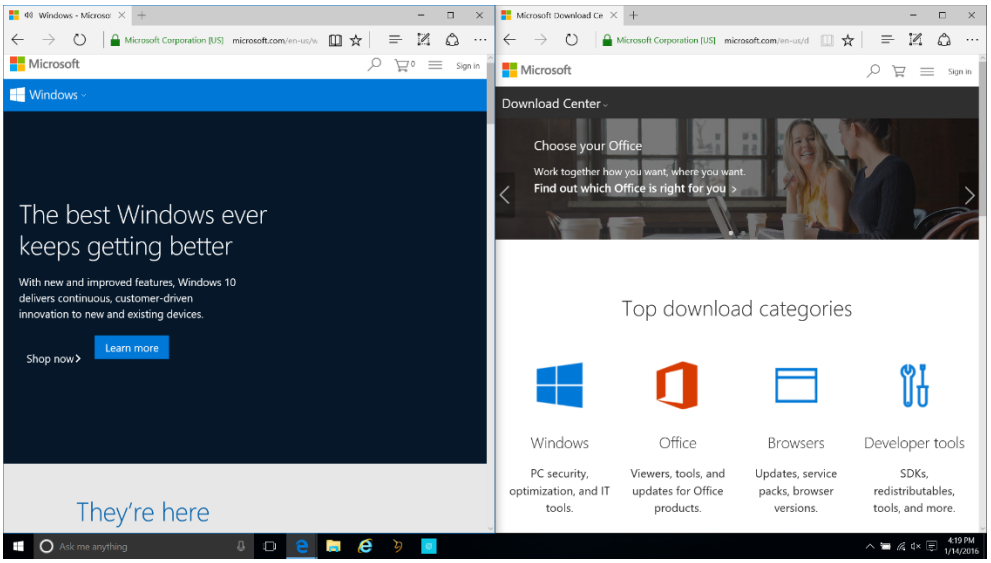


Figure 1-10: Using Snap Assist to split the screen into two windows for navigating in the Microsoft Edge

Important The Snap functionality is supported only on Windows 10 Desktop. Most of the apps support the snap functionality, but some apps have certain minimum height and width requirements, which means they do not neatly fill up the space, or they might overlap with other apps. Certain win32 messaging apps are examples of app types with specific dimensions that cannot be used with Snap Assist.

Cortana

Cortana is the Microsoft digital assistant; it uses the Bing engine in the background to help you to quickly and easily carry out searches and locate the information you want. Cortana was first introduced on Windows Phone devices and now is officially part of the new Windows operating systems.

Cortana is assuming control of many operating system (OS) search features, such as searching the local device for files, utilities, or applications, searches on OneDrive accounts, or even on your local network. You access Cortana on the taskbar, and you can manage it via either natural voice queries or by text.

www.dbooks.org

When accessing Cortana through a voice command, no touch is required. It is just a matter of saying "Hey Cortana" to get started. You can speak your command without looking at your device, making it possible to get what you need without taking your eyes off the task in front of you.

Accessing Cortana settings

You can turn the Cortana feature on or off in Cortana Settings, as shown in Figure 1-11. You also can go to Cortana Settings to train voice recognition for better accuracy and to reduce the likelihood of Cortana being activated when someone other than you says "Hey Cortana." To access the settings, do the following:

1. Toward the left end of the taskbar, click the search box labeled Ask Me Anything.
2. On the left side of the pane, click the Notebook button.
3. Click Settings.

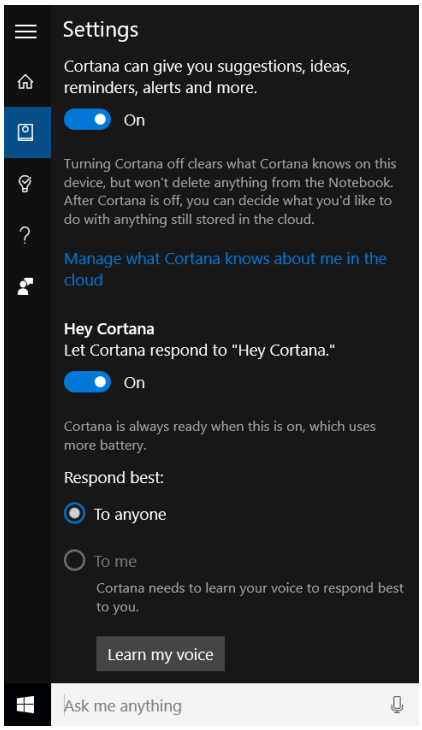


Figure 1-11: Cortana settings in Windows 10

Cortana voice commands

Here are a few examples of the Cortana voice commands available in Windows 10 desktop and mobile versions.

- **Alarm** "Wake me up at 6 A.M."; "Wake me up in 7 hours."
- **App: open** "Open Xbox."
- **Calendar event creation** "Set a meeting on my calendar for 2 P.M. to interview new candidates."
- **Email** "Send an email to my brother."
- **Settings** "Turn on Bluetooth."

- **Weather** "What is the weather forecast for tomorrow?"; "What about Saturday?"
- **Calculator** "8 plus 6"
- **Conversions** "How many ounces are in a pound?"
- **Currency** "How many dollars are in a euro?"
- **Dictionary** "Define analogy."

Windows startup enhancements

Windows Imaging Format (WIM) is a way to start the OS in a configuration for which the payload of files resides within a compressed file. It is useful for imaging devices with limited storage support, such as low-cost tablets.

Windows 10 includes tools to help you use less drive space. The *Compact OS* feature facilitates the reuse of the compression support from WIM. As a result, Compact OS offers comparable performance and resource usage to that of WIM while supporting the ability to service individual objects as needed without losing space. Compact OS is supported on both UEFI-based and BIOS-based devices.

Unlike WIM Boot, because the files are no longer combined into a single WIM file, Windows Update can replace or remove individual files as needed to help maintain the drive footprint size over time.

More info You can see how to deploy Compact OS with a USB bootable drive or by using a WIM file at https://msdn.microsoft.com/library/windows/hardware/dn940129%28v=vs.85%29.aspx.

Push Button Reset improvements

In Windows 10, it is no longer necessary to recover to a clean OS state by applying a recovery image; a clean OS state can be reconstructed by restaging the entire OS from the Windows Side by Side (WinSxS) store, instead. By reconstructing the system state, the need for a separate offline recovery image is no longer needed. In addition, the recovered or reconstructed OS is always up-to-date without having to service two separate images, the running OS, and the recovery image.

Reconstructing the OS is essentially a replacement for applying a new OS WIM. The end-to-end process will be coordinated by the Push Button Reset (PBR). After a PBR has been initiated, the following high-level steps are performed to complete the reconstruction of the OS (if using the OS while online only, there is a mechanism to fix any corruption of component store or metadata, but it requires an Internet connection):

- Enumerate list and state of all packages on the OS, and choose which to install
- Apply or generate the nucleus of the OS in a temporary directory, for example, C:\windows.new
- Populate C:\Windows.new\WinSxS with contents from old WinSxS
- Offline install chosen packages by using C:\Windows.new\WinSxS as the install source

Moving the new OS into its place, which is the process of moving the C:\windows.new to C:\windows' will be owned by the PBR process.

The location to reconstruct the new OS is defined by PBR, and it is passed to the servicing stack as input.

Beginning with Windows 8, Microsoft has been supporting a feature called Inbox Corruption Repair. This feature is able to repair corrupt system files by downloading them from Windows Update. It is commonly used to repair corruption during servicing operations, but you can also run it as a

www.dbooks.org

standalone corruption mechanism. Running this step requires an Internet connection with access to Windows Update.

Failing to repair the corruption will fail the reconstruction operation. The PBR can avoid this by disabling the verification step altogether.

Microsoft Edge

In August 1995, Microsoft launched the company's first web browser: Internet Explorer. Although at the time there were no standards for web browsers, customers were asking Microsoft to create web browsers with a lot of functionality.

Computing has changed and user expectations have changed, too. Browsers can no longer support only PCs and mobile devices. Today, we need web browsers for all kinds of devices, such as Xbox consoles, Surface Hub, HoloLens, wearables, and Internet of Things (IoT) devices.

The newest browser from Microsoft, Microsoft Edge, addresses modern standards such as HTML5, SVG, ES5, ES6, and CSS3. Microsoft Edge provides a clean interface with easy-to-configure settings. In addition, Internet Explorer 11 is still supported for backward compatibility and interoperability to maintain support for many existing applications. Using Internet Explorer might still be necessary when using legacy applications that use ActiveX controls, VBScript, and Browser Helper Objects. It is possible to set an Enterprise Site list to be opened by Internet Explorer 11 when using the Enterprise Mode Site List tool and Group Policy Objects (GPOs).

Microsoft Edge provides many productivity enhancements, including the following:

- **Cortana** Your personal assistant can help you to perform searches without leaving your current webpage
- **Web Note** Take notes (or just doodle) directly on webpages using this built-in capability.
- **Reading List** Save content to read later and easily retrieve it from your reading list.
- **Reading View** View content without all the surrounding distractions.

A native PDF viewer and Flash also provide common functionalities when navigating on the Internet.

Having these tools integrated in the web browser assists with security, helping you to avoid spyware and malware. Previously, it was necessary to download these tools separately to work with earlier versions of Internet Explorer, because most of tools changed the default search navigator and used to come with lots of viruses.

Fixing specific sites

As mentioned in the preceding section, it is possible to set an Enterprise Site list to be opened by Internet Explorer 11 when using the Enterprise Mode Site List tool and Group Policy Objects (GPOs). To do this, in the Enterprise Mode Site List Manager tool (see Figure 1-12), click Add to add all of the sites that you need. After you compile the site list, you then export it to an XML file.

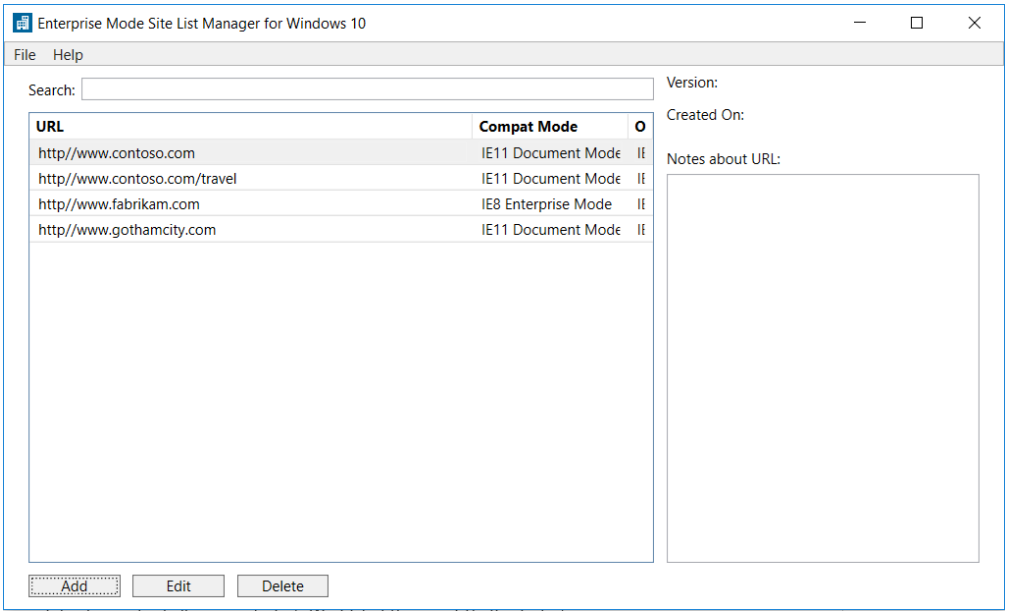


Figure 1-12: The Enterprise Mode Site List Manager tool for Windows 10

More info You can download the Enterprise Mode Site List Manager tool from the Microsoft download center at http://www.microsoft.com/download/details.aspx?id=49974.

After adding a site, it is possible to configure its compatibility mode, IE11 Document mode, IE9 Enterprise mode and others, as well as the option to open the site in Microsoft Edge or Internet Explorer 11, as shown in Figure 1-13.

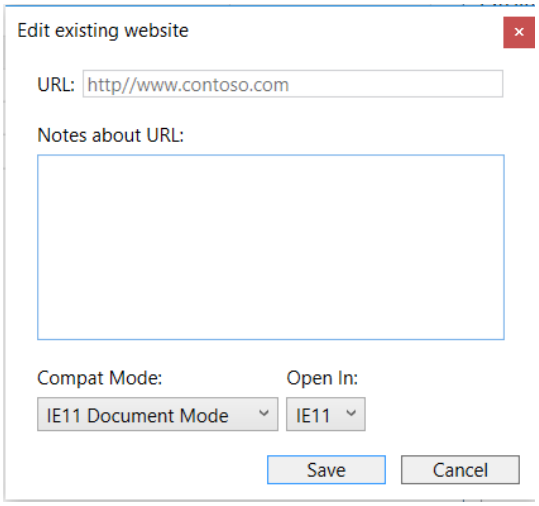


Figure 1-13: The option to edit an existing website added into the Enterprise Mode Site List Manager tool for Windows 10

The Enterprise Mode Site List Manager tool also offers the option to import an existing site list under the EMIE file format.

Next, in the Group Policy Object Management console, you need to turn on Allows You To Configure The Enterprise Site List setting, and reference the XML file that you exported from the Enterprise Mode Site List tool.

www.dbooks.org

Open your Group Policy Object Editor and go to Administrative Templates > Windows Components > Microsoft Edge > Allows You To Configure The Enterprise Mode Site List setting, as shown in Figure 1-14.

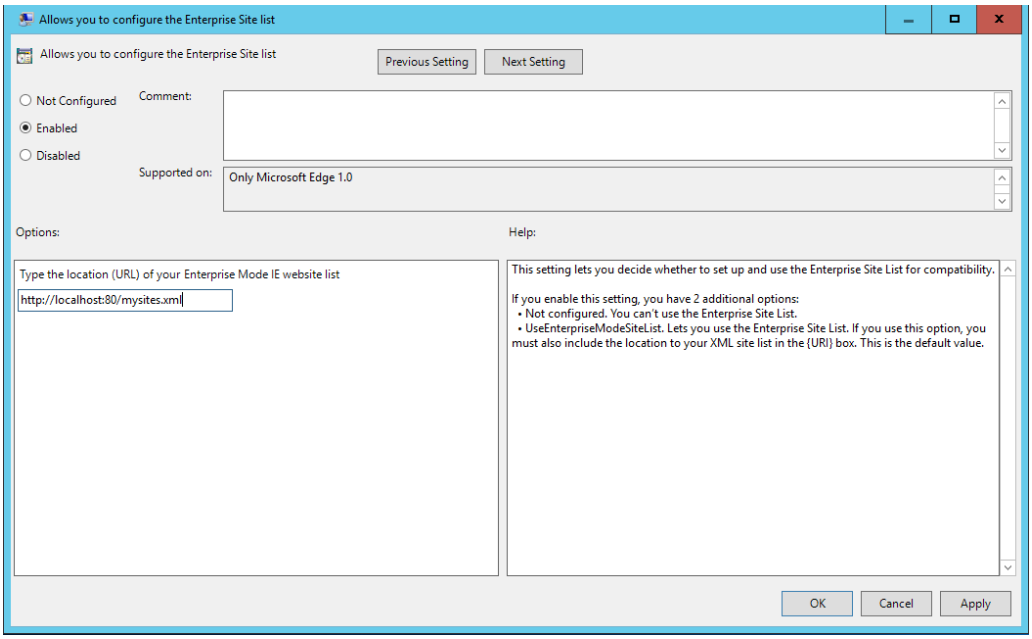


Figure 1-14: The Allows You To Configure The Enterprise Site List setting in the Group Policy Object Editor

More info For more details about using the Enterprise Mode Site List Manager settings, go to https://technet.microsoft.com/library/mt270205.aspx.

In addition, Microsoft Edge has its own standard, which is known as Microsoft Edge HTML web engine. Microsoft created this engine for the following reasons:

- Many legacy sites need to continue working.
- Developers want the latest and greatest web standard support.
- A web browser is now a service (instead of a product).

About security

Online security presents many challenges. With password theft being an ongoing problem, password security continues to be at the top of the list of those challenges. According to an article published by the BBC (http://www.bbc.com/news/technology-28654613), it is estimated that hackers have stolen more than 1.2 billion user names and passwords across the globe.

Enterprises continue to educate users on the need for password security and to establish and enforce password policies. Basic safeguards such as using unique passwords need to be encouraged. For example, if you use the same user name and password on all your websites, and one website is compromised, it is likely that all your websites will be compromised.

Pass the Hash (PtH) is a hacking technique by which an attacker can authenticate to a remote server or service by using the Windows NT LAN Manager (NTLM) authentication protocol or LanMan hash of a user password. A typical PtH attack starts with one end point being compromised by malware, which then manages to gain administrator-level access. With this access, the malware can steal the user's derived credentials and impersonate the user on other devices. As the attacker moves laterally across

the network and finds additional devices to which the user has access, the malware can steal the derived credentials from other users who previously signed in to those devices.

Over time, an attacker can typically gain access to more and more derived credentials that have increased levels of network access. Eventually, it is likely that domain administrator accounts can be compromised, and then the consequences can be even worse.

Here are the Microsoft features that address password and PtH attacks in Windows 10:

- Microsoft Passport
- Windows Hello
- Isolated User Mode

Microsoft Passport

The goal of Microsoft Passport is to remove the need to enter user names and passwords for all compliant websites, applications, and resources. Microsoft Passport approaches this goal by doing the following:

- Replacing passwords with a private key made available solely through a user gesture, which can be a PIN or biometric identifier
- Streamlining two-factor authentication
- Using credentials on familiar mobile devices for desktop sign-in
- Supporting both local and remote components such as phones, USB dongle, and so on

Windows Hello

Windows Hello is a new biometric identification system built in to Windows 10 that recognizes your face, fingerprint, and iris. Windows Hello uses Microsoft Passport as complementary technology for websites supporting the technology, which is based on asymmetric-key cryptography created by the Windows security team to identify a cellphone to a network. All devices incorporating the Intel F200 RealSense 3D Camera support the facial and iris unlock features of Windows Hello.

The world is moving toward small, touch-based sensors that have a high degree of accuracy. These sensors can mitigate the majority of known attacks by using fingerprint authentication. All current fingerprint-capable readers are supported. The following are three examples of supported devices:

- Fingerprint Sensor FPC1021
- Fingerprint Sensor FPC1150
- Next Biometrics NB-1010-S

The fingerprint process begins when your fingerprint is scanned by the reader, generating a template on your local device. If the device is compromised, the template does not allow the attacker to create your fingerprint, because the attacker needs to get local administrator rights to get the fingerprint templates.

The face-recognition process involves a RealSense camera, which is embedded above the display. It uses photographic analysis, heat detection, and depth detection to check who is trying to access the device.

Fingerprint, face, and iris recognition share the same design language for enrollment, usage, and recovery with Windows Hello, and the enrollment process is very simple.

www.dbooks.org

The Windows Hello enrollment process

In the Windows 10 device, go to Settings, click Account, and then click Sign-In Options, as shown in Figure 1-15.

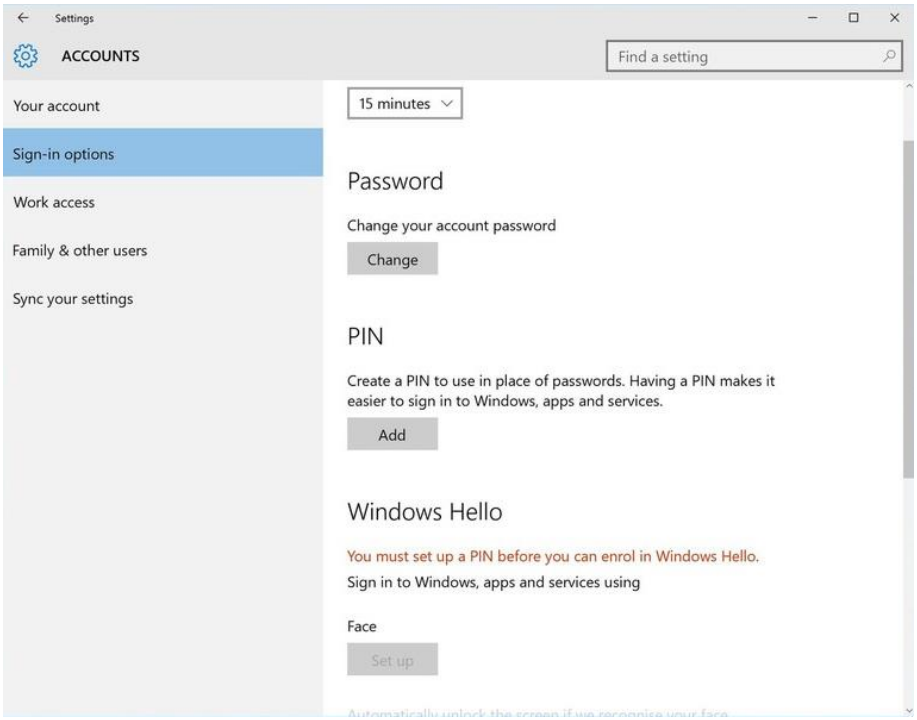


Figure 1-15: The sign-in options available in Windows 10 settings

You must have a PIN to begin using Windows Hello. You need to set up a PIN code according to your enterprise requirements, as shown in Figure 1-16. Usually a PIN has at least six digits, and cannot be made up of a pattern such as 123456 or 111111 or 222222.

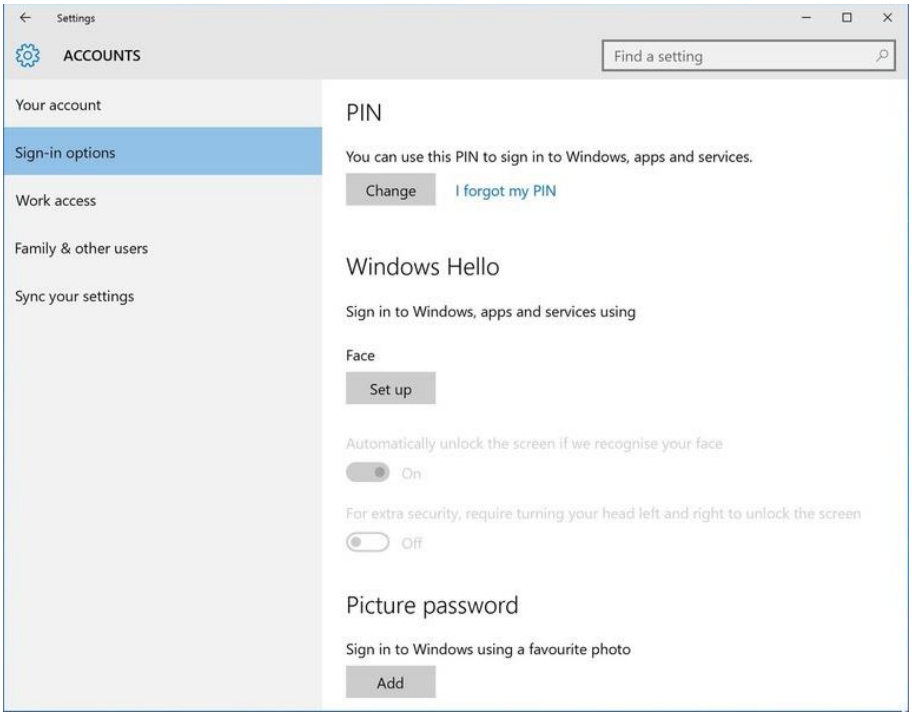


Figure 1-16: The Windows Hello Face Set Up option

After setting up the PIN, there is a Face option that you can use to unlock the screen. Click Set Up (see Figure 1-16) to unlock the screen and access the Welcome To Windows Hello page, shown in Figure 1-17.

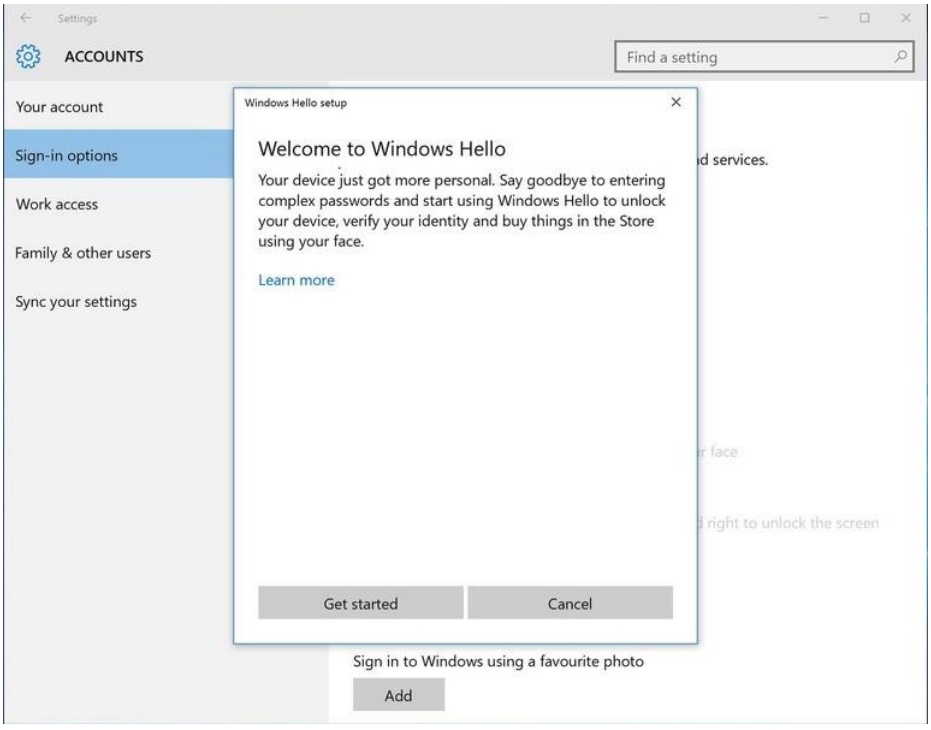


Figure 1-17: The Welcome page in the Windows Hello Setup Wizard

www.dbooks.org

For the last step in the enrollment process, you need to physically position yourself so that your face is in the center of the frame that appears on the screen, the camera captures your face for recognition. After that, you are all set, as shown in Figure 1-18. The next time you need to unlock your device, you will use face recognition for authentication.

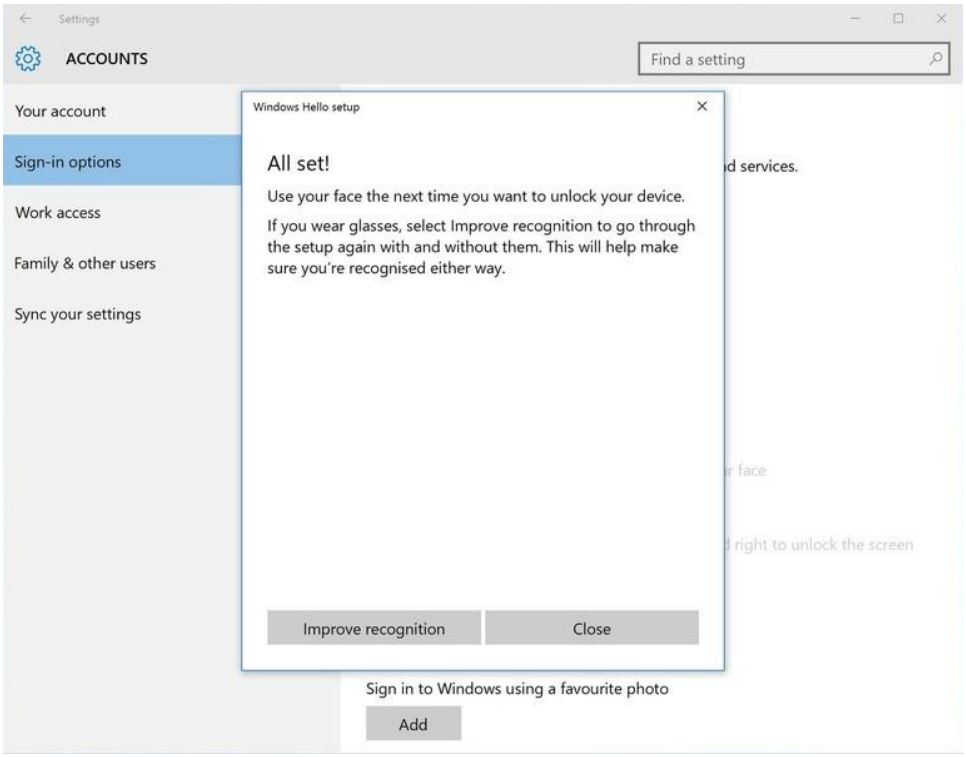


Figure 1-18: The Windows Hello configuration is done

Isolated User Mode

There are two pieces to the Windows OS architecture: the Kernel and the User mode. Because the Kernel can be vulnerable to attacks, it is also necessary to protect the User mode code from the Kernel.

Isolated User Mode (IUM) brings a secure Kernel, separated from the normal New Technology Operating System Kernel, or NTOS Kernel, that does not know or have access to the address space of the User mode code, which means literally no normal kernel-mode access to user-mode data.

The IUM provides a runtime environment for *Trustlets*, which are the processes running in IUM that are Trustlets isolated from one another. Secure Kernel runs in Secure Ring 0 and provides a hardened interface to proxy NTOS system calls.

The Local Authentication Authority (LSA) process in the OS, which serves to authenticate and log users on to the local systems, communicates with the isolated LSA by using remote procedure calls (RPC).

Data stored by using virtualization-based security is not accessible to the rest of the OS.

Credential Guard does not host any device drivers; instead, it hosts only a small subset of OS binaries that are needed for security. All of these binaries are signed with a certificate that is trusted by virtualization-based security.

Virtual TPM is a feature that allows the emulation of a TPM and provides that to guest virtual machines running on a host.

More info To learn more, go to https://technet.microsoft.com/library/mt483740(v=vs.85).aspx.

The Windows 10 upgrade process

The first question that always comes after a new OS release is "Why upgrade?" This section addresses this question and also describes the upgrade process and its improvements in Windows 10.

Despite all the logistics and costs involved when upgrading to a new OS, using the wipe-and-load method, enterprises previously had to develop their own methods to upgrade their operating systems because there was no control or predictability provided by the upgrade process. Now that releases are continuously rolling out instead of arriving in somewhat predictable cycles every two or three years, enterprises demand a continuous flow of productivity in their businesses. But, rolling upgrades cannot hamper productivity.

Microsoft developed a meaningful in-place upgrade process internally with Microsoft IT that has become the deployment method offered to all customers, including enterprises and consumers.

In Windows 10, the recommended deployment is the in-place upgrade for the existing devices, such as Windows 7, Windows 8, and Windows 8.1. Windows 10 does all of the work for you by preserving all data, settings, applications, drivers, and so on. The other methods, such as wipe-and-load provisioning, are still there.

There are four primary phases within the OS upgrade process from the architecture perspective: Down Level, Windows Recovery Environment, First Boot, and Second Boot. Chapter 2 contains detailed descriptions for each of these phases.

www.dbooks.org

CHAPTER 2

Windows 10 deployment options

This chapter describes the preparation steps for a successful deployment of Windows 10 in an enterprise environment by using Configuration Manager. It also explains all of the other methods available today for migrating to the new operating system.

This chapter covers:

- In-place upgrade
- Predeployment steps
- Manual in-place upgrade
- Traditional deployments
- Windows To Go
- Windows Update approach
- OS upgrade via Windows Server Update Services
- Moving the focus to Configuration Manager

In-place upgrade

Moving away from an earlier version of the Windows operating system (OS)has always been one of the biggest challenges faced by IT professionals—especially when they need to make important decisions regarding managing users' data and applications. In fact, the need to wipe and load all users' files and applications and upgrade to a new OS is a cause for two major concerns:

- What if a document is lost during the process?
- What if a key application is forgotten or not configured properly?

Windows 10 overcomes these issues by making the migration preparation and testing simpler.

You can now upgrade computers running Windows 7, Windows 8, and Windows 8.1 directly to the latest version of Windows 10 through the in-place upgrade process, without the need to reimage the device.

> **More info** To learn more, go to https://technet.microsoft.com/windows/dn798755#administration.

Although there are still valid scenarios to continue using the traditional wipe-and-load method, the in-place upgrade is the new recommended option.

> **Note** Unfortunately, the in-place upgrade is not available for migrating Windows XP to Window 7, Windows XP to Windows 8.1, and Windows 7 to Windows 8.1.

The following table can help you to decide which option is best for your environment:

With in-place upgrade you can…	With wipe-and-load you can…
• Reduce upfront testing and deployment preparation • Deploy Windows faster: 30 to 60 minutes, on average, to upgrade • Use a smaller OS package: the Windows Imaging Format (WIM) file is from the default OS media, the size is smaller because it does not contain any application • Preserve all data, settings, applications, and drivers • Have robust rollback capabilities to a functional down-level OS should a failure occur	• Change from Windows x86 to x64 • Change OS language • Change disk partitioning • Change from BIOS to UEFI • Change to a lower SKU (e.g., Enterprise to Professional) • Manage configuration changes such as change of domain membership, local administrators, and bulk applications swap • Upgrade systems by using Windows-To-Go, or those that start from a virtual hard drive (VHD) • Upgrade systems with dual-boot or multi-boot • Upgrade systems that use certain third-party disk encryption products

> **Note** Chapter 4 provides further information about how to implement wipe-and-load and in-place upgrades by using Configuration Manager.

Predeployments steps

This section contains guidelines on how to plan for a trouble-free in-place migration.

www.dbooks.org

Step 1: Choosing the correct media

Windows 10 media is available for download at the Volume Licensing Center (VLC) at https://www.microsoft.com/licensing/servicecenter/default.aspx. With VLC media, the installation process uses a generic product key. The computers installed with such media are by default Key Management Service (KMS) clients; no additional configuration is needed.

The other option is to use the Media Creation Tool (MCT) that can generate an installation USB flash drive or an ISO file. The MCT is available at http://go.microsoft.com/fwlink/?LinkId=691209.

VLC media is recommended in an enterprise environment because MCT media has some limitations:

- You cannot use MCT media for upgrading a Windows Enterprise edition.
- Setupcomplete.cmd will not run if there is an original equipment manufacturer (OEM) key on the system that you want to upgrade or if Windows is running a non-Volume License build.

Note You can determine if you are using the wrong media by looking at the log file at C:\windows\panther\UnattendGC\SetupAct.log. There, you will see the following:

Info [windeploy.exe] *OEM license detected, will not run SetupComplete.cmd*

What is Setupcomplete.cmd?

Setupcomplete.cmd is a file that is created under %WINDIR%\Setup\Scripts to run a post-installation script in Full OS. It is required by Configuration Manager and Microsoft Deployment Toolkit (MDT). Here's what Setupcomplete.cmd does:

- After applying the OS and the system restart, MDT uses Setupcomplete.cmd to resume the task sequence.
- After the Windows Mini-Setup and the restart, Configuration Manager uses this script to install the Configuration Manager Client and to continue with the Task Sequence engine in Full OS.
- In Configuration Manager, setupcomplete.cmd contains this command:

```
%windir%\system32\osdsetuphook.exe /execute
```

More info To see additional examples of Setupcomplete.cmd, go to https://technet.microsoft.com/library/hh825167.aspx and https://msdn.microsoft.com/library/windows/hardware/dn898472(v=vs.85).aspx.

Step 2: Assessing readiness

It is very important to assess which devices will support a Windows 10 upgrade. The minimum requirements are as follows:

- **OS** Windows 7, Windows 8, or Windows 8.1
- **Processor** 1 GHz or faster processor (CPU) or system-on-a-chip (SoC)

Note To install a 64-bit OS on a 64-bit PC, the processor needs to support CMPXCHG16b, PrefetchW, and LAHF/SAHF.

- **RAM** 1 GB for a 32-bit OS and 2 GB for a 64-bit OS
- **Hard drive space** 16 GB for a 32-bit OS and 20 GB for a 64-bit OS

- **Graphics card** DirectX 9 or later with WDDM 1.0 driver
- **Display** 800x600

> **More info** To learn more, go to http://www.microsoft.com/en-US/windows/windows-10-specifications#sysreqs).

With Configuration Manager, you can create a basic custom report to assess some of the hardware readiness. Here is an example:

```
select *,
CASE WHEN
(([CPU (GHz)] >=1 and version like '6.%') and
  (([RAM (GB)] >=2 and Architecture = 'x64-based PC' and [System Disk Size (GB)] >=20)
   or ([RAM (GB)] >=1 and Architecture = 'X86-based PC' and [System Disk Size (GB)] >=16))
 )
THEN 'Yes' ELSE 'No' END AS [HW Ok for Windows 10]
from (SELECT distinct SYS.Netbios_Name0 as Name, Ops.Caption0 as OS, Ops.CSDVersion0 as SP,
LEFT(Ops.Version0,3)  as Version,
ROUND(CONVERT(FLOAT,CPU.MaxClockSpeed0), -2)/1000 AS [CPU (GHz)],
ROUND(ROUND(CONVERT(FLOAT,MEM.TotalPhysicalMemory0) / 1048576, 2) , 1) AS [RAM (GB)],
CS.SystemType0 as Architecture,
LDISK.Size0/1024 AS [System Disk Size (GB)],
MAX(VID.VideoModeDescription0) as [Screen resolution]
FROM v_R_System SYS LEFT JOIN v_GS_LOGICAL_DISK LDISK on SYS.ResourceID = LDISK.ResourceID
LEFT JOIN v_GS_COMPUTER_SYSTEM CS on SYS.ResourceID = CS.ResourceID
LEFT JOIN v_GS_X86_PC_MEMORY MEM on SYS.ResourceID = MEM.ResourceID
LEFT JOIN v_GS_Processor CPU on SYS.ResourceID = CPU.ResourceID
LEFT JOIN v_GS_VIDEO_CONTROLLER VID on SYS.ResourceID = VID.ResourceID
LEFT JOIN v_GS_OPERATING_SYSTEM Ops on SYS.ResourceID = Ops.ResourceID
WHERE  (LDISK.DeviceID0 = 'C:' and SYS.Operating_System_Name_and0 not like 'Microsoft Windows NT%Server%')
Group by SYS.Netbios_Name0,Ops.Caption0,Ops.CSDVersion0,
Ops.Version0,CPU.MaxClockSpeed0,MEM.TotalPhysicalMemory0,CS.SystemType0,LDISK.Size0) as Assessment  order by
10,1
```

The results will resemble those presented in Figure 2-1.

	Name	OS	SP	Version	CPU (GHz)	RAM (GB)	Architecture	System Disk Size (GB)	Screen resolution	HW Ok for Windows 10
1	FC-CL01	Microsoft Windows 8.1 Enterprise	NULL	6.3	2.7	1	x64-based PC	126	1024 x 768 x 4294967296 colors	No
2	FC-CL02	Microsoft Windows 7 Enterprise	Service Pack 1	6.1	2.7	1	X86-based PC	126	NULL	Yes
3	FC-CM01	Microsoft Windows Server 2012 R2 Standard	NULL	6.3	2.7	8	x64-based PC	126	1920 x 1080 x 4294967296 colors	Yes
4	FC-DC01	Microsoft Windows Server 2012 R2 Standard	NULL	6.3	2.7	2	x64-based PC	126	1920 x 1080 x 4294967296 colors	Yes

Figure 2-1: Results of a Windows 10 compatibility custom report

> **Note** For a more comprehensive report, you could consider installing the Upgrade Assessment Tool, as described at https://technet.microsoft.com/library/jj677180.aspx. Unfortunately, as of this writing, the Windows 10 version of the tool is not yet available.

Alternatively, you might want to use Microsoft Assessment and Planning Toolkit (MAP), which is available at https://technet.microsoft.com/library/dd627342.aspx, and take the necessary remediation steps before you begin the roll-out. This version has already been updated with Windows 10 information and is quite simple to install. You can configure MAP to connect to the Configuration Manager database to reuse information already collected offline, as shown in Figure 2-2.

www.dbooks.org

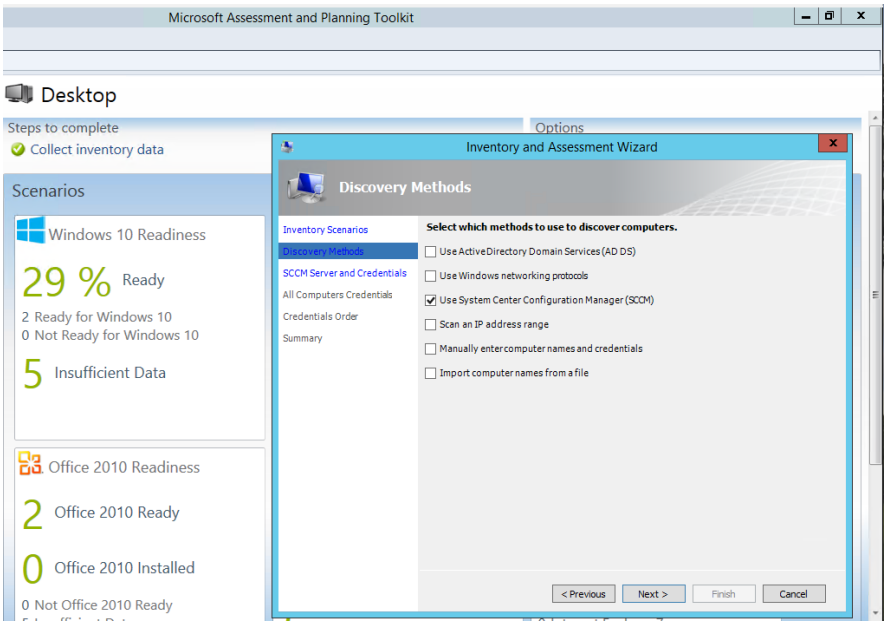


Figure 2-2: Using MAP to check Windows 10 readiness

One last method to evaluate Windows 10 readiness is to use the embedded option */Compat ScanOnly* in the setup.exe file. You can test it by running the following command:

```
SETUP.EXE /Auto Upgrade /Quiet /NoReboot /DynamicUpdate Disable /Compat ScanOnly
```

> **More info** For all Windows setup command-line options, go to https://msdn.microsoft.com/library/windows/hardware/dn938368(v=vs.85).aspx.

If you want to check whether your system is compatible, do the following:

1. Open C:\$Windows.~BT\Sources\Panther\setupact.log to check the progress.
2. Open C:\$Windows.~BT\Sources\Panther\setuperr.log and check the last line that contains

```
CsetupHost::Execute result = code
```

Here are the most common results codes:

- No issues found: 0xC1900210
- Compatibility issues found (hard block): 0xC1900208
- Migration choice (auto upgrade) not available (probably the wrong SKU or architecture): 0xC1900204 and 0xC190010E
- Does not meet system requirements for Windows 10: 0xC1900200
- Insufficient free hard drive space: 0xC190020E
- Problem unmounting the WIM file: 0xC1420127

> **More info** To learn more, go to http://blogs.technet.com/b/mniehaus/archive/2015/08/23/windows-10-pre-upgrade-validation-using-setup-exe.aspx.

Alternatively, you can run the following command:

```
Setup.exe /Auto Upgrade /Quiet /NoReboot /DynamicUpdate Disable /Compat ScanOnly /CopyLogs
%SystemRoot%\Logs\Win10ReadyCheck
```

With the /CopyLogs option, Setup.exe creates two folders:

- MoSetup, which contains the BlueBox.log. This is helpful to troubleshoot the command used to launch the setup and possible errors.
- Panther, where you can find many prerequisite checks information files.

How to create a Compliance Settings readiness report

To automate this assessment process by using Configuration Manager with baselines, perform the following procedure:

1. Mount your Windows 10 media and copy its content to a source repository (e.g., \\Servername\Source$\OS\Win10Ent_en_VLC_x64).
2. Download the Win10ReadyCheck.vbs script from http://aka.ms/DeployWin10/files.

> **Note** This script runs Setup.exe in "test upgrade mode" and then copies the setup logs and checks for compatibility issues. If no issues are found, it creates the file C:\Windows\Logs\Win10ReadyCheck\Win10Ready-Success.txt. To help you with troubleshooting, the script creates C:\Windows\Logs\Win10PreCheck.log, as well.

3. Save the script under the same folder of the Windows media; that is, \\Servername\Source$\OS\Win10Ent_en_VLC_x64.
4. Create a package that uses \\Servername\Source$\OS\Win10Ent_en_VLC_x64 as content source and Win10ReadyCheck.vbs as the program.
5. Configure the program to run only on the correct architecture (e.g., All Windows 8.1 x64 + Windows 7 SP1 [x64]).
6. Ensure that the option Copy The Content Of This Package To A Package Share On Distribution Point is selected.
7. Deploy the package/program to a test collection and then select to Run Program From Distribution Point.

Repeat the preceding steps for the x86 architecture and create another package/program, this time using the x86 media source. The script Win10ReadyCheck.vbs is the same one.

Now, create a few Configuration Items (CIs) and a Baseline that will be needed to generate a report:

1. Create a CI that checks for the existence of the file C:\Windows\Logs\Win10ReadyCheck\Win10Ready-Success.txt.
2. In the Client Settings section, ensure that the PowerShell Execution Policy is set to Bypass so that the scripts that follow run correctly.
3. Create a CI that checks for free hard drive space by using this Windows PowerShell script:

```
## Check Free-Disk-Space
[Int]$DesiredSpace = "7"
Try
{
$Freespace = gwmi -Query "Select FreeSpace from Win32_LogicalDisk where DeviceID='$env:SystemDrive'"
}
Catch
{
```


www.dbooks.org

```
write-host "Exception Type: $($_.Exception.GetType().FullName)" -ForegroundColor Red
write-host "Exception Message: $($_.Exception.Message)" -ForegroundColor Red
}
[Int]$FreespaceGB = ($Freespace.FreeSpace / 1024 / 1024 / 1024)
If ($FreespaceGB -ge $DesiredSpace)
{
return "Compliant"
}
Else
{
return "NonCompliant"
}
```

4. Optional: Create a CI to check available memory by using this script:

```
## Check Memory
[Int]$DesiredMemory = "2"
Try
{
$Memory = gwmi -Query "Select TotalVisibleMemorySize from Win32_OperatingSystem"
}
Catch
{
write-host "Exception Type: $($_.Exception.GetType().FullName)" -ForegroundColor Red
write-host "Exception Message: $($_.Exception.Message)" -ForegroundColor Red
}
[Int]$MemoryGB = ($Memory.TotalVisibleMemorySize / 1024 / 1024)
If ($MemoryGB -ge $DesiredMemory)
{
return "Compliant"
}
Else
{
return "NonCompliant"
}
```

5. Optional: Create a CI to check the Client Version by using this script:

```
## Get SCCM-Client-Version
## 5.00.8239.1301
[String]$DesiredVersion = "5.00.8239.1301"
Try
{
$SCVersion = gwmi -Namespace root\ccm -Query "Select ClientVersion from SMS_Client"
}
Catch
{
write-host "Exception Type: $($_.Exception.GetType().FullName)" -ForegroundColor Red
write-host "Exception Message: $($_.Exception.Message)" -ForegroundColor Red
}
If ($SCVersion.ClientVersion -eq $DesiredVersion)
{
return "Compliant"
}
Else
{
return "NonCompliant"
}
```

6. Create a Baseline containing all of the preceding CIs and deploy it to a Test collection.

7. Review the report "Summary of the compliance by configuration items for a configuration baseline" (see Figure 2-3) for potential issues.

Summary compliance by configuration items for a configuration baseline

Configuration Baseline Name	Configuration Baseline Purpose	Configuration Item Name	Configuration Item Revision	Configuration Item Type	Compliance %	Compliant	Non-Compliant	Failed	Remediated	Not-Applicable
PFE Win10 Readiness	Required	Win10-Ready-PreCheck-Success-File	1	OS	50	1	1	0	0	0
PFE Win10 Readiness	Required	Win10-Ready-Memory-Amount	2	OS	50	1	1	0	0	0
PFE Win10 Readiness	Required	Win10-Ready-ConfigMgr-Client-Version	2	OS	100	2	0	0	0	0
PFE Win10 Readiness	Required	Win10-Ready-ConfigMgr-Disk-Freespace	1	OS	100	2	0	0	0	0

Figure 2-3: Configuration Baseline to assess Windows 10 readiness

Step 3: Gathering driver packages

With a better understanding of which computers you can upgrade, another important step is to check the compatibility for device drivers. You can do this by connecting to the Hardware Manufacturer's website. Some computer manufacturers provide packs of drivers for MDT or SCCM. These driver packs contain all of the drivers needed for each device. The following are driver packs for some common manufacturers:

- http://www8.hp.com/us/en/ads/clientmanagement/drivers-pack.html (HP Driver Pack)
- http://en.community.dell.com/techcenter/enterprise-client/w/wiki/2065.dell-command-deploy-driver-packs-for-enterprise-client-os-deployment (Dell Command | Deploy – Driver Packs for Enterprise Client OS Deployment)
- https://support.lenovo.com/us/en/documents/ht074984 (Lenovo Microsoft System Center Configuration Manager [SCCM] and Microsoft Deployment Toolkit [MDT] Package Index)

Note that most of the drivers that work with Windows 7 or Windows 8.1 should work with Windows 10. If during the in-place upgrade the computer has access to the Internet, the setup process will install new drivers through Windows Update or the manufacturer's website.

> **Note** You can search to determine whether Windows 10 drivers are available in the Windows Update catalog by going to http://catalog.update.microsoft.com/v7/site/Search.aspx?q=driver.

As a last step, ensure that all of the existing packages (Chipset, Network, Video, Audio, and Touchpad in particular) are available to you, in case you need to reinstall a driver after the in-place upgrade.

> **Important** If you plan to import new driver packages in your Configuration Manager 2012 R2 with SP1 environment, ensure that you have installed at least the Cumulative Update 2 (KB3100144). The update contains the fix 3084586, which corrects a problem whereby the content for the driver package might be duplicated multiple times. This causes the package file to be significantly larger than the package in the original source location. Additionally, the process to import the new drivers by using the Import New Driver Wizard can take much more time than you expect.
>
> For more information, go to https://support.microsoft.com/kb/3084586.

A cue for testing applications

Although it is always a good idea to create an isolated lab before beginning deployments with real devices, instead of working directly on a physical machine, you should first take a copy of an existing computer; for example, by using Disk2vhd. After the machine is captured and converted to vhdx, you can attach it to a Hyper-V environment, and you can test the process as many times as needed.

The Disk2vhd approach is good to isolate potential applications compatibility issues.

> **More info** Disk2vhd is available from https://technet.microsoft.com/sysinternals/ee656415.aspx.

Manual in-place upgrade

The Manual upgrade is probably the easiest way to have a real feeling of how the upgrade process works, taking you step by step through screens with prefilled default options. These are the identical steps that take place in an unattended setup. Looking under the hood of this process can be very helpful for troubleshooting any installation.

www.dbooks.org

All you need is Windows 10 media and a computer with Windows 7, 8, or 8.1 (there are no specific requirements for service packs or updates installed). Just remember to use the same Language and Architecture (x86/x64) as the version that you are upgrading. Also remember that upgrading from Windows Enterprise to Windows Professional is not possible.

The following sections describe the four phases of the upgrade:

1. Down Level
2. Windows Recovery Environment (WinRE) (or SafeOS)
3. First Boot
4. Second Boot

These are names the setup uses in the logs.

Phase 1: Down Level (Old OS)

This the phase during which the upgrade process is initiated by the setup.exe file, the main OS installer, when run from what it is called a Down Level OS, or the previous OS installed on the user device. For example, when running setup.exe to upgrade to Windows 10 from Windows 7, the Windows 7 OS is the Down Level OS.

The installer begins by asking if you want to download the latest updates and drivers.

> **Note** You can run Setup.exe directly by using /InstallDrivers<location> to specify where the new Windows 10 drivers are located.

A new folder called C:\$WINDOWS.~BT is created.

The main steps of the setup in the old OS can be summarized as follows:

- Perform system checks
- Create an inventory of drivers and applications and compatibility assessment
- Prepare WinRE

System checks

The setup checks to verify that the system has the correct CPU, memory, and enough hard drive space to run the upgrade and a possible restore.

In case there is not enough free space, the process now supports external storage: you will see instructions during the upgrade for what to do. You might need to either remove unneeded files from your device or insert a USB flash drive to complete the upgrade.

The setup also ensures that no Portable Workspace (i.e., Windows To Go USB) is used, that the host is not started from VHD, and that if UEFI is used, it is a compliant version (secure start requires firmware that supports UEFI v2.3.1 Errata B and has the Microsoft Windows Certification Authority in the UEFI signature database).

The file C:\$WINDOWS.~BT\Sources\Panther\setupact.log is a good resource for viewing the result of all these checks.

Inventory and compatibility

The next step is creating a full inventory of all the drivers and then checking their compatibility—in particular, critical drivers such as Network and Storage that could be a blocker for the installation.

You can find further information about Blocking Configurations in the file C:\$WINDOWS.~BT\Sources\Panther\ScanResult.xml:

```
<?xml version="1.0" encoding="UTF-8"?>
<CompatReport MigXmlFile="DrZ9C4CLgEiIrHz2.3.8.0.0_APPRAISER_Migration.xml">
 <System X64Running="True" X64Capable="True"/>
  <Hardware>
   <HardwareItem HardwareType="Setup_BitlockerNoTargetSupport">
    <CompatibilityInfo BlockingType="None"/>
   </HardwareItem>
   <HardwareItem HardwareType="Setup_TargetIsNonStagedBuild">
    <CompatibilityInfo BlockingType="None"/>
   </HardwareItem>
   <HardwareItem HardwareType="Setup_LanguagePackDetected">
    <CompatibilityInfo BlockingType="None"/>
   </HardwareItem>
   <HardwareItem HardwareType="Setup_LicenseActivation">
    <CompatibilityInfo BlockingType="None"/>
   </HardwareItem>
   <HardwareItem HardwareType="Setup_PendingFirmwareUpdateWithPower">
    <CompatibilityInfo BlockingType="None"/>
   </HardwareItem>
   <HardwareItem HardwareType="Setup_SecureBoot">
    <CompatibilityInfo BlockingType="None"/>
   </HardwareItem>
  </Hardware>
<SystemInfo OSMinorVersion="3" OSMajorVersion="6" UplevelEdition="Windows 10"/>
 <Devices/>
  <DriverPackages>
   <DriverPackage HasSignedBinaries="False" BlockMigration="True" Inf="oem0.inf"/>
   <DriverPackage HasSignedBinaries="True" BlockMigration="False" Inf="acpi.inf"/>
  </DriverPackages>
 <Programs/>
</CompatReport>
```

At the same time, using advanced heuristics, the setup detects and creates an inventory of all applications. All inventoried content is then checked against a compatibility database that is available offline as part of the Windows 10 media (\Sources\appraiser.sdb). This database not only contains a list of compatibility and incompatibility, but also the necessary steps of remediation that can be performed during the setup phase.

> **Note** With Internet connectivity, the computer downloads the latest version of the compatibility database only when the Download And Install Updates (Recommended) option is selected during the initial setup.

The files * _APPRAISER_* Inventory.xml contain helpful information for the Compatibility Check assessment results; they are created under C:\$WINDOWS.~BT\Sources\Panther.

At the end of the compatibility check, the setup offers you the possibility to keep personal files and apps, just personal files, or nothing (the default is to keep everything). Only incompatible drivers and apps that cannot be remediated with the compatibility database information are blocked; for applications that are not known in the database, you will be asked what to do.

Finally, the settings of the components of the current OS are gathered so that they can be migrated.

> **More info** To learn more about how the application compatibility database works, go to https://msdn.microsoft.com/library/bb432182(v=vs.85).aspx.

Prepare WinRE

At this point, the setup has created a map of what to migrate and cached all the necessary drivers needed. In this step, the setup does the following:

1. Copy Install.wim to C:\$WINDOWS.~BT\Sources
2. Extract WinRE.wim to C:\$WINDOWS.~BT\Sources\SafeOS

www.dbooks.org

3. Mount WinRE.wim to C:\$WINDOWS.~BT\Sources\SafeOS\SafeOS.Mount and inject all startup-critical drivers, if needed
4. Prepare the system to restart in WinRE

More info WinRE is a tool for troubleshooting an OS offline; it is now used in Windows 10 also to deploy the main OS instead of a plain Windows Preinstallation Environment (WinPE).

For more details, go to https://msdn.microsoft.com/library/windows/hardware/dn938364(v=vs.85).aspx.

Phase 2: Start into WinRE (copying files)

After the system restarts from WinRE, the upgrade process lays down the new OS (Install.wim) to $WINDOWS.~BT\NewOS.

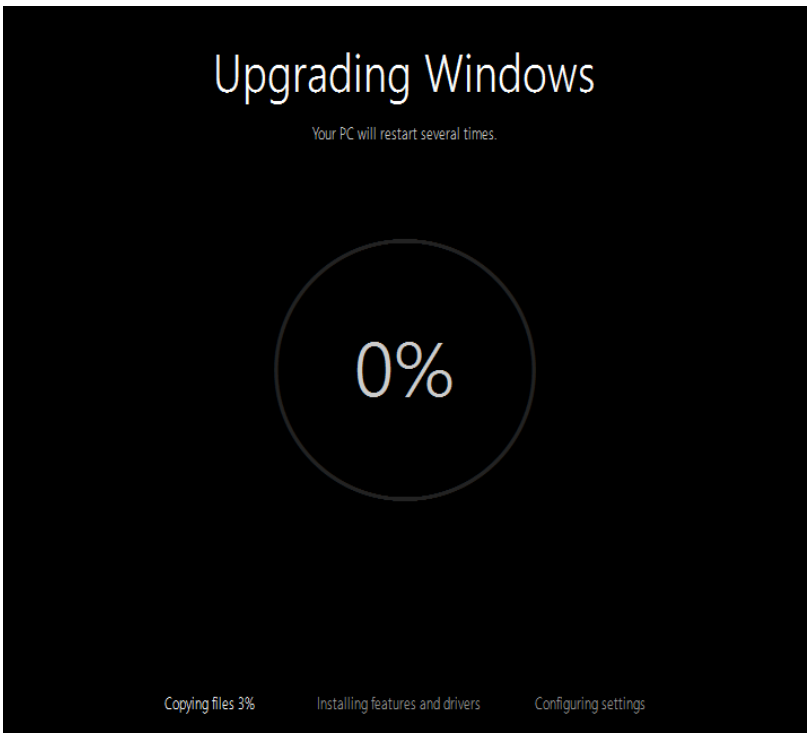


Figure 2-4: WinRE phase of a Windows Update

The existing folders Windows, Program Files, Users, ProgramData, inetpub, SkyDriveTemp, Recovery, and Perflogs are moved to Windows.old so that you can recover the system in case something goes wrong, or go back to the old OS if you want to.

Then, the upgrade performs all of the offline migration tasks and puts the drivers in the drivers store.

Finally, the New OS pieces are moved from $WINDOWS.~BT\NewOS to the root of the system drive. The system then restarts in Full OS.

Note You can follow what is happening in this phase by pressing Shift+F10 and opening the $WINDOWS.~BT\Sources\Panther\setupact.log.

Phase 3: First reboot in Windows 10 (installing features and drivers)

This phase includes the sysprep specialize pass. The most important steps are summarized here:

1. Installation of drivers
2. Configuration of Appx (WindowsApps)
3. Configuration of WinRE
4. Processing of a provisioning package
5. Installation of Windows features
6. Partial restoration of data and settings

Note The system is now in Full OS and the setupact.log has been moved to C:\Windows\Panther. The log file for troubleshooting driver installation issues is located at C:\Windows\INF\setupapi.*.log

For all of the details about Setup states, go to https://technet.microsoft.com/library/cc721913(v=ws.10).aspx. To learn how to use a provisioning package, go to https://technet.microsoft.com/library/mt203963(v=vs.85).aspx and https://msdn.microsoft.com/en-us/library/windows/hardware/mt147439(v=vs.85).aspx.

Phase 4: Second reboot in Windows 10 (configuring settings)

The system is almost ready: the setup completes the final migration of data and settings, and then enters the Out-of-Box-Experience (OOBE) pass.

Next, setup asks whether you want to use "Express Settings" or create your own customized settings.

Then, you are asked about enabling Cortana and keeping default apps for Photos, Music, Video, and Internet Browsing. When this is done, the process is finalized and you are now ready to use Windows 10. You are greeted with the following message:

"All your files are exactly where you left them."

More info For a full list of preferences, go to http://windows.microsoft.com/en-us/windows-10/services-setting-preferences.

Recoverability

The remarkable feature of Windows 10 Upgrade is the ability to do a full recovery of the old OS at any phase during the process. Here is what happens in each of the four phases should you need to do this:

- Down Level phase: If the process is interrupted or cancelled during this phase, it will run a cleanup of the C:\$Windows.~BT folder.
- WinRE phase: If the process is interrupted here, the system will restart into the original OS with no further action (WinRE is configured to run only once).
- First or Second Boot phase: if something goes wrong (such as a particular driver causing issues), the system will do the following:
  - Start by using the recovery OS.
  - Undo all the changes.

www.dbooks.org

- Run a cleanup task.
- Start by using the original OS.

Even upon the successful installation of Windows 10, you still have the option to uninstall it and go back to the original OS, but only within one month of installation. To do this, go to the Action Center, click All Settings, and then select Update & Security. Next, click Recovery, and then finally select the Go Back option.

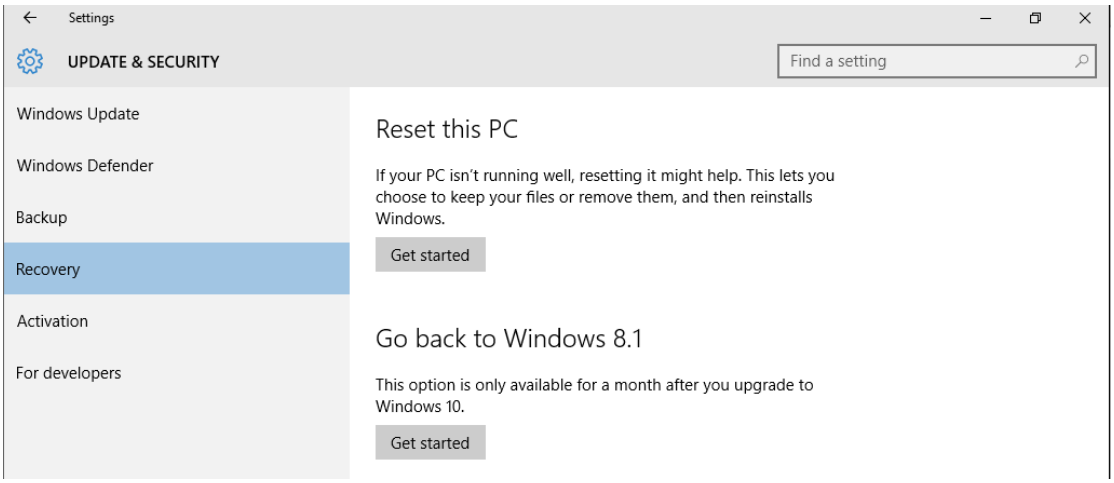


Figure 2-5: Going back to the previous Windows OS

Note This option is no longer available if you have deleted Windows.old or a month has passed since the upgrade. The scheduled task that automatically removes Windows.old is \Microsoft\Windows\Setup\SetupCleanupTask.

Traditional deployments

Like its predecessor, Windows 10 supports all traditional deployment methods, which can be summarized as follows:

- Bare metal (new computer)
- Wipe-and-load (refresh)
- Replace

Bare-metal installation

This is the cleanest of installation methods because the hard drive is always repartitioned and formatted. It is meant for brand new hardware or a device that needs to be repurposed. You can also use it to install Windows on a computer that starts from a VHD, unlike the in-place migration.

The manual bare-metal installation is straightforward and similar to previous Windows versions. It begins by starting in WinPE from the Windows media or Preboot Execution Environment (PXE). Then, you must configure regional settings, select the installation type (which, in this case, is Custom: Install Windows Only (advanced)), and then choose how to partition and format the drive(s). At this point, the setup will continue installing the OS image.

After the system has restarted for the second time, the most important improvement, as outlined in Chapter 1, is the option Who Owns The PC, with which you can designate the device's owner.

Note This option is only available when the computer is connected to the Internet. It is not available when using Windows Enterprise, because the setup program assumes that you are already working on a company-owned device.

There are two options: I Own It, and My Organization. If you select My Organization, you will be asked how you want to connect; here, your options are Join Azure AD (i.e., you have an Office365 account) or Join A Domain.

The new Azure Active Directory join is particularly interesting because it offers new opportunities to IT professionals, who now have the option to ship new devices to people working remotely, with no need to prepare them in advance: these devices will be automatically enrolled in the organization's device management solution, such as Intune or Configuration Manager, as part of joining them to Azure Active Directory.

More info To learn more, go to http://blogs.technet.com/b/ad/archive/2015/05/13/azure-active-directory-and-windows-10-making-the-enterprise-cloud-a-reality.aspx.

Wipe-and-load (refresh)

This process is used to reinstall a computer and keep user data and settings. When the PC is reinstalled, the OS can be the same or a different one.

Note Wipe-and-load is also the recommended method to move from Windows 7/8/8.1 Enterprise to Windows 10 Professional, because it is not possible to do this via an in-place upgrade.

You can initiate wipe-and-load from a running OS or from WinPE. The first step is to make a backup of the data and then wipe the drive, the OS is installed, and optionally some applications are installed, as well. At the end of the process, the data and settings are "loaded" (restored) and the computer is ready for use.

The "wipe" consists of deleting all files and directories from the drive, except for a few folders, one of which is where the data and settings are stored.

More info For more details on the wipe process, go to http://blogs.technet.com/b/configurationmgr/archive/2010/06/30/how-to-use-usmt-4-hardlinking-in-a-configuration-manager-2007-task-sequence.aspx (middle of the page).

Replace

This scenario is often used to replace an old machine with a new one; it is also commonly used to change the drive layout to migrate from BIOS to UEFI.

Data is captured from the source computer to a network share or an external drive (backup). The new computer is installed similar to that of a bare-metal deployment, and then the data and settings are restored from the backup.

Windows To Go

Windows Enterprise has a unique feature called Windows To Go, with which IT professionals can provide users with a fully working version of Windows running on a USB external device. Windows To Go drives can use the same image that enterprises use for their desktops and laptops, and they can be managed like any other normal PC.

www.dbooks.org

Here are the minimum requirements for implementation:

- One computer running Windows 10 Enterprise
- The install.wim or a captured image from the Windows Enterprise media itself
- A USB drive that is Windows To Go certified

For the manual installation, first insert your certified USB device. Next, right-click Start, select Control Panel, and then click Windows To Go (or simply run pwcreator.exe).

The setup will first ask for the location of the WIM file: if you're unsure of this, simply use the install.wim from the Enterprise media. Then, you can optionally provide a BitLocker password. Continue by clicking Create, in a few more minutes, your USB drive should be ready to go.

Finally, click No when you see the question "Do you want to automatically boot your PC from a Windows To Go workspace?"

After you have a Windows To Go device with Windows 10, you can also use it to test hardware compatibility for any device that is a candidate to migrate to Windows 10. Although this is not the quickest method, it is definitively the cleanest and the most reliable. All you need to do is configure the computer to start from USB and check whether Windows To Go works correctly and what drivers are missing or require attention. Windows To Go will not touch your hard drive, because by default internal drives are offline; thus, you can enjoy the Windows 10 experience with a minimum of effort.

More info To learn more about how to implement Windows To Go with Configuration Manager, go to https://technet.microsoft.com/library/jj651035.aspx.

Note If you are running Configuration Manager 2012 SP1, ensure that you have at least the Cumulative Update 2 installed (https://support.microsoft.com/sv-se/kb/3100144), because it fixes an issue by which Administrators cannot select a Windows 10–based image by using the Windows To Go Creator Wizard.

Windows Update approach

Windows Update is broadly used by consumers and small businesses because there is no need to install a server and the update installation behavior can be controlled via policies. Windows Update can now upgrade older versions to the latest Windows 10 version (with some limitations described in just a few moments), and there is a new Defer Upgrades And Updates policy by which you can delay upgrades for an additional one to eight months for machines pointing directly to Windows Update, as shown in Figure 2-6.

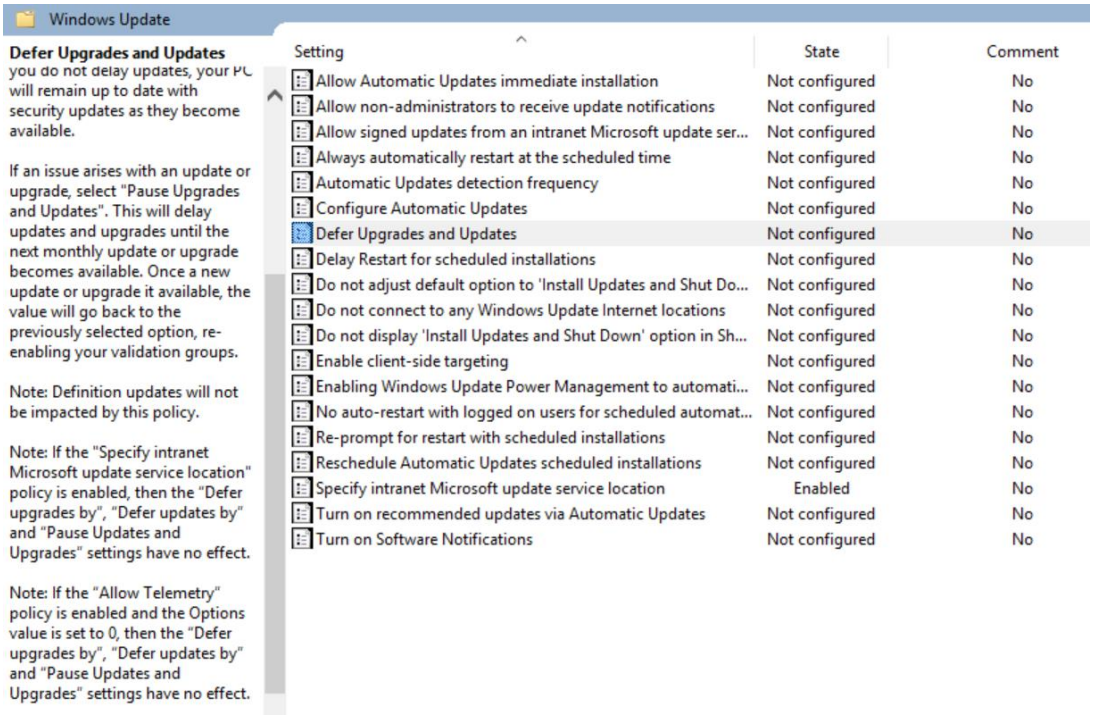


Figure 2-6: Defer Upgrades and Updates policy

Note The Defer Upgrades and Updates policy is only available starting from Windows 10 version 1511. If you would like to configure this setting via Group Policies, you will need the new Administrative Templates (.admx) for Windows 10 1511, available at https://www.microsoft.com/download/details.aspx?id=48257.

Following is an explanation of how in-place upgrade works with Windows Update.

The first thing to consider is that Windows Update upgrade does not work with any Enterprise editions. (See https://support.microsoft.com/kb/3081048.)

The following table can help you decide whether the Windows Update approach is a viable option for your environment.

OS to be upgraded	ConfigMgr/MDT/Media	Windows Update
Windows 7 Pro	YES	NO
Windows 7 Enterprise	YES	NO
Windows 7 Pro with SP1	YES	YES (with update 2952664 installed)
Windows 7 Enterprise with SP1	YES	NO
Windows 8 Pro	YES	NO
Windows 8 Enterprise	YES	NO
Windows 8.1 Pro	YES	YES (with updates 2919355 and 2976978 installed)
Windows 8.1 Enterprise	YES	NO
Windows 10 Pro (1507)	YES	YES (only for non KMS activated clients)
Windows 10 Enterprise (1507)	YES	YES (only for non KMS activated clients)

www.dbooks.org

Note Windows Update in-place upgrade requirements and limitations may be subject to change in future versions of Windows 10 and after July 29, 2016. This is the date when the free upgrade for compatible devices that are running Windows 7 Service Pack 1 or Windows 8.1, expires, as described at http://windows.microsoft.com/windows-10/upgrade-to-windows-10-faq.

Here are some additional considerations:

- The upgrade package is approximately 2.5 GB, so you should connect from a nonmetered connection to avoid extra charges.
- It is recommended to install update 3112343 (for Windows 7) and update 3112336 (for Windows 8.1) because they activate support for additional upgrade scenarios to Windows 10, providing a smoother experience should you need to retry an OS upgrade due to certain failure conditions.

More info See https://support.microsoft.com/kb/3112343 and https://support.microsoft.com/kb/3112336 (December's 2015 Windows Client updates). As of this writing, these Knowledge Base articles contain the latest Windows Update client packages available for download. *These are not the ones listed under* https://support.microsoft.com/kb/949104 *which contains links to older versions from 2014*. Newer versions will become available in the following months, superseding December's 2015 Windows Client updates.

Get Windows 10 App

To upgrade Windows 7 SP1 or Windows 8.1 to Windows 10 with Windows Update, you must first install the update 3035583 (called "Get Windows 10 App"), as shown in Figure 2-7.

More info To learn more, go to https://support.microsoft.com/kb/3035583#bookmark-prerequisite.

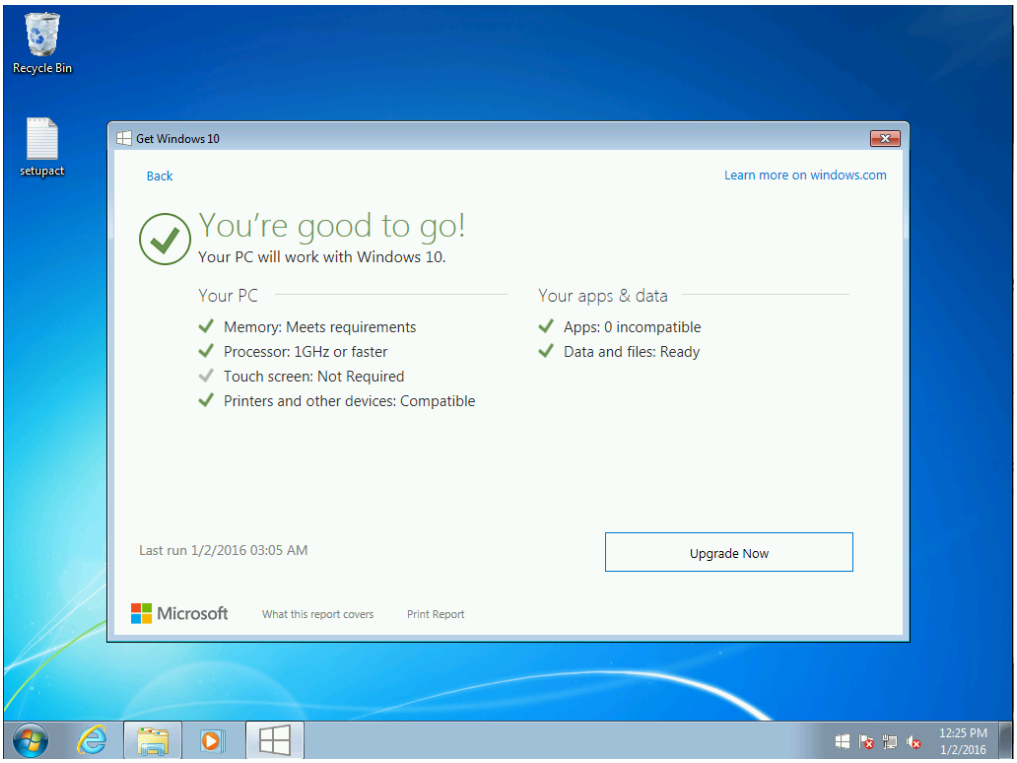


Figure 2-7: The Get Windows 10 App and the Compatibility report

The app is installed under C:\Windows\System32\GWX, and it runs with the process called GWX.exe.

A Windows logo appears on the taskbar. Click this icon to start a guided in-place upgrade process. The app also generates a compatibility report, as shown in Figure 2-7.

When you select the Upgrade Now option, the Windows Update client is instructed to start the process.

> **Note** Ensure that there are no other updates with a pending restart because they will cause the Get Windows 10 App to become unresponsive at the Starting Download stage.

The Windows Update client will download all of the installation files. Here are the most important among them:

- The latest version of the Compatibility database (appraiser.sdb)
- The Windows 10 Electronic Software Download file (Image.esd), which is just a few megabytes smaller than the Install.wim
- The setup file WindowsUpdateBox.exe

> **Note** The setup command looks like this (from C:\Windows\WindowsUpdate.log):
>
> ```
> "C:\Windows\SoftwareDistribution\Download\a92f8878ea38cac4505fcefd787bd88e\WindowsUpdateBox.exe" /ClassId
> c8b741f1-76a9-4daf-8e44-3ef0bdae6d81  /PreDownload /Update /ClientId 2541fd59-5545-45e0-b481-0e37aae0847a
> /ReportId {5915BCC6-7D09-4076-BB29-BF11F09F6FD7}.202
> ```

After it is started, WindowsUpdateBox.exe copies install.esd into C:\$Windows.~BT\Sources and runs System checks, Drivers and Applications Inventory, and the Compatibility Assessment (again).

www.dbooks.org

In the window that opens, select Start The Upgrade Now. You are then logged-off and the installation begins.

The experience is similar to the manual in-place upgrade, from the WinRE phase.

> **More info** To learn how to manage Windows 10 notification and upgrade via the "Get Windows 10 App," go to https://support.microsoft.com/kb/3080351.

OS upgrade via Windows Server Update Services

Windows Server Update Services (WSUS) is a better approach for managing the upgrades in an enterprise because you can perform additional testing and evaluation by selecting what you want to install and to which group of devices, all via a management console.

This section describes how to configure WSUS to perform an in-place upgrade. This method is very similar to Windows Update, the main difference being that you need to have at least one local server to deploy updates. The limitations for supported operating systems are similar to the Windows Update method, with the only addition of Windows Enterprise, which is listed in the WSUS catalog as a possible target for the upgrade.

> **Note** As of this writing, only Windows Professional upgrades were tested with this method.

Prerequisites

Here are the prerequisites to support Windows 10 upgrades via WSUS:

- Windows Server 2012 or Windows Server 2012 R2 with Update 2919355

> **Note** Be sure to use the latest media to install Windows Server 2012 R2. If you're unsure, check the date of the file install.wim, which should be November 21, 2014 or later.

- WSUS with hotfix 3095113 installed

> **Note** The hotfix is needed to use the new Upgrades Classification in WSUS. With Windows Server 2012 R2, the version of WSUS should be 6.3.9600.18057 or newer, to fully support Windows 10. For more details, go to https://support.microsoft.com/kb/3095113.

Installing KB 3112343 (Windows 7) and KB 3112336 (Windows 8.1) on Windows Client is also recommended here.

Internet Information Services and the missing mime type

In December 2015, an issue was reported whereby computers are unable to download .esd files from the WSUS server. This happens when in Internet Information Services (IIS), because the file type .esd is not defined under mime types.

To overcome this problem, click Start, run **iinetmgr**, navigate to Wsus Administration, and then click Content. Next, click Mime Types, Add, and then type the following into the text box:

```
File Name Extension:
.esd
MIME type:
application/octet-stream
```

By doing so, you will avoid Error 0x80244019 (= URI/file not found). An example of the error is shown in this WindowsUpdate.log excerpt:

```
File URL = http://server:8530/Content/7C/6F5CAF07827FAE0E37739F3222603EAF38808B7C.esd, local path =
C:\Windows\SoftwareDistribution\Download\64509357e45e1af1317c778b14109a6a\10586.0.151029-
1700.th2_release_CLIENTENTERPRISE_VOL_x64fre_en-us.esd
DownloadManager   Progress failure bytes total = 2659650046, bytes transferred = 0
DownloadManager CUpdateDownloadJob::GetNetworkCostSwitch() Neither unrestricted or restricted network cost
used, so using current cost
DownloadManager Error 0x80244019 occurred while downloading update; notifying dependent calls.
```

More info To learn more, go to https://social.technet.microsoft.com/Forums/en-US/d7dbb851-4e3a-41d9-9072-1f16d7b1bc1e/fix-domain-windows-10-wsus-upgrade-issues-file-not-found?forum=winserverwsus.

Configuring WSUS to support in-place upgrades

Next, you need to make the Update files available in the WSUS Content library so that they are available to clients for download.

To approve a Windows 10 Upgrade, perform the following steps (if you are familiar with the WSUS update approval process, you can skip this section):

1. Open Server Manager, click Tool, and then select Windows Server Update Services.
2. When the WSUS console opens, click the server name to expand the item; select Options.
3. Select Products And Classifications, and then add Windows 10 to the Products and add Upgrades to the Classification.
4. Click OK to confirm.
5. In the left pane of the console, click the server name.
6. In the right pane, select Synchronize Now and wait for the process to complete.
7. Back in the left pane, click the server name, expand Updates, and then select All Updates.
8. In the right pane, right-click the row(s) of the upgrade(s) that you want to install.
9. In the Approve Updates window, select Approve, right-click All Computers, and then select Approve For Install (or press Ctrl+i).

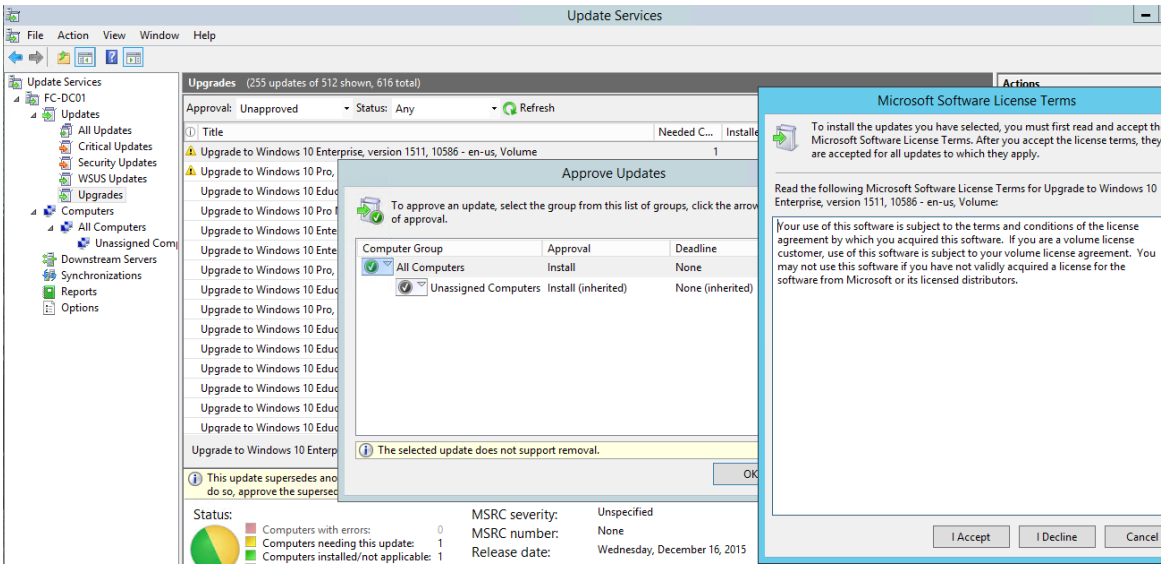


Figure 2-8: The WSUS console showing the Windows 10 upgrades

www.dbooks.org

Go back to the main WSUS dashboard to verify that the Upgrades have finished downloading. When the Download Status shows Updates Needing Files: 0, you are ready to move to the next step.

Configuring policies to use WSUS

To point your clients to the WSUS, you need to create a policy.

1. On the client for which you want to *test* the WSUS Upgrade, click Start, and then type **gpedit.msc** to run the test.
2. Navigate to Computer Configuration, select Administrative Templates > Windows Components > Windows Update.
3. In the right pane (settings), select Specify Intranet Microsoft Update Service Location, and then select Enabled.
4. In the sections Set The Intranet Update Service For Detecting Update and Set The Intranet Statistics Server, copy the URL of your WSUS server (such as, http://server.withfqdn.local:8530).

> **Note** You could also create a group policy object, although for testing on just a few machines a local policy might be more practical. Group Policies are definitively the way to go for putting this configuration in production.

5. While still on the client computer, run these commands:

```
gpupdate /force
wuauclt /detectnow
wuauclt /reportnow
```

6. Verify under WindowsUpdate.log that the client detects the upgrade, as demonstrated here:

```
Agent     * Updates to install = 1
Agent     *   Title = Upgrade to Windows 10 Pro, version 1511, 10586
```

7. Finally, open Control Panel and select Windows Update. The upgrade to Windows 10 will show up.
8. Click Get Started and the process continues, such as in the Windows Updates method.

Moving the focus to Configuration Manager

This chapter provided an overview of the basic options IT professionals could consider to migrate. It aimed to give some insights on how the process works and the most important logs for troubleshooting. The core process stays the same whether you do it manually or via Windows Update or WSUS; however, if you have Configuration Manager in your environment, you will most likely want to use this to deploy Windows 10.

The chapters that follow discuss how OS deployment works in Configuration Manager and how to fully automate the process by using task sequences.



Get the latest news from Microsoft Press sent to your inbox.

- New and upcoming books
- Special offers
- Free eBooks
- How-to articles

Sign up today at MicrosoftPressStore.com/Newsletters

Microsoft

www.dbooks.org

CHAPTER 3

Configuration Manager Operating System Deployment concepts

With the development and much anticipated arrival of Windows 10, enterprises will need a comprehensive toolset to deploy the operating system to their end users. Using the Operating System Deployment feature—otherwise known as OSD—Microsoft System Center Configuration Manager provides the IT administrator with various methods to deploy Windows 10. OSD also provides organization-wide, end-to-end monitoring and troubleshooting insights throughout the process.

This chapter is an overview of OSD and its capabilities for deploying an operating system (OS) within an enterprise environment. Understanding the foundational concepts and the components used for a Windows OS deployment is imperative for a successful installation.

It's highly recommended that you test the OSD feature in a lab environment, disconnected from the production environment, and also during the development cycle of a task sequence to avoid mistaken deployments to critical systems.

This chapter covers:

- The purpose of OSD
- OSD terminology
- Infrastructure requirements
- WinPE
- Task sequences
- Drivers and driver packages
- Image deployment
- UEFI versus BIOS
- Reporting
- Advanced concepts
- Online resources

The purpose of OSD

Using the OSD feature, you can configure an unattended or attended automated deployment process that is repeatable to many machines by using the existing Configuration Manager infrastructure. You can target an OS deployment to existing clients already managed or to unmanaged new computers that are unknown to the Configuration Manager environment. The following core areas historically have proven to be difficult barriers to overcome within environments of any size; OSD helps you to better cope with and mitigate these barriers:

- **Content distribution**

  Windows OS images are typically large in size. The content management features and functionality provides a scalable solution for you to replicate the image contents to all hosting servers, and finally, to end-user computers, all while averting any disruptions to the WAN links.

- **Scheduling or self-service**

  The administrator has the ability to control when the deployment of the OS will begin for end-user machines or provide users with the flexibility to carry out installation according to their scheduling needs. This can be set globally for all upgrade candidates or scheduled accordingly for individual requirements on machine resources in specific business units by way of grouping into collections and targeting via a deployment.

- **Reporting, monitoring, and troubleshooting**

  Upgrading many devices is comparable to upgrading one device. With centralized reporting mechanisms, you can monitor and further drill an overall deployment status into specific system statuses to troubleshoot individual machine issues or issues affecting many machines. The time-to-resolution is greatly reduced when the resolution has been identified.

www.dbooks.org

OSD terminology

The core concepts of OSD contain many terms that you should be familiar with when planning an OSD strategy. The following table provides definitions for these terms:

Term	Definition
Image	File-based replica of a hard drive. Supports Windows Imaging Format (WIM) file format.
Target computer	The computer on which you install a Microsoft Windows OS image.
Reference computer	Fully configured computer from which you generate the WIM file.
Source computer	Existing computer that is managed by Configuration Manager. It contains the user state data and settings that will be migrated to a new destination computer.
Destination computer	Computer that will receive the user state data and settings that are migrated from a source computer.
Sysprep	Windows system preparation tool that facilitates image creation on reference computers running Windows operating systems.
User State Migration Tool (USMT)	Utility used to collect and restore system, application, and user data.
Windows Preinstallation Environment (WinPE)	Preinstallation environment used in OS deployment.
PXE	Preboot Execution Environment (WinPE).
Windows Imaging Format (WIM file)	A file containing an operating system/data image.

Infrastructure requirements

Configuration Manager consists of various site system roles as a prerequisite for OSD; others are optional although highly recommended. Figure 3-1 provides an overview of these roles.

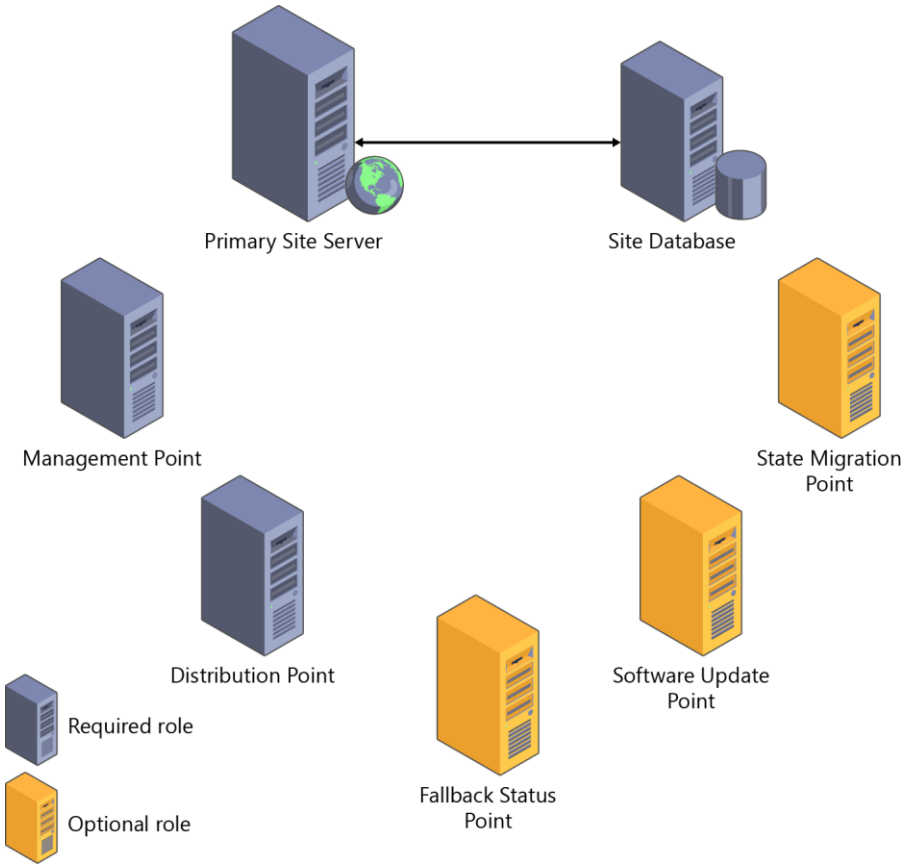


Figure 3-1: Site system roles for OSD

Following is a description of each of the roles

- The Distribution Point (DP) required role provides content during deployments. Types of content consist of applications, software packages, software updates, OS images, and device driver packages. This site system role could be placed in remote office branches to provide clients with a local content source to avoid downloading large content files such as WIMs over the WAN links. Bandwidth throttling and scheduling options are available to control content distribution and, alternatively, a Pull function to enhance bandwidth usage over WAN links. It accommodates network startup if PXE is turned on. If you do want to turn on PXE startup functionality, you will need Windows Deployment Services and a DHCP server with IP helper configurations on network routers.
- The Management Point (MP) required role provides clients with configuration and deployment policies and assists in identifying content location for software retrieval based on the client's network location. It also receives configuration data from clients and state messages for reporting during a deployment. The MP role typically is located alongside the Primary Site Server, and there can be more than one, depending on the number of clients being managed to distribute the load.
- The State Migration Point (SMP) optional role maintains user state data from systems being refreshed or replaced. You can also set the retention period for the user's data on this site system.
- The Software Update Point (SUP) optional role is used to determine which software updates would be applicable to a machine during the build process and throughout the life of the computer while it is managed by Configuration Manager. This site system requires that Windows Server Update Services (WSUS) is installed prior to configuration.

www.dbooks.org

- The Fallback Status Point (FSP) optional role provides an alternative method for clients to report any client agent installation or client communication–related issues with the MP.

Aside from the site system roles, the Network Access Account is a requirement of OSD for authentication and access to the Configuration Manager environment by clients.

WinPE

WinPE startup images are lightweight versions of the Microsoft Windows OS with limited components and services that requires 512 MB of memory for the base version. If adding additional drivers, packages, or applications, you will need more memory. When a computer is started with WinPE, it is initialized in a RAM drive under the drive letter X:\, which allows for better performance and to temporarily write data such as log files that you can review while in the environment. Also, while WinPE is running, it supports hot-swapping devices such as USB drives. Figure 3-2 displays a computer that was started into WinPE 10, viewing the disk configuration by using the diskpart.exe command.

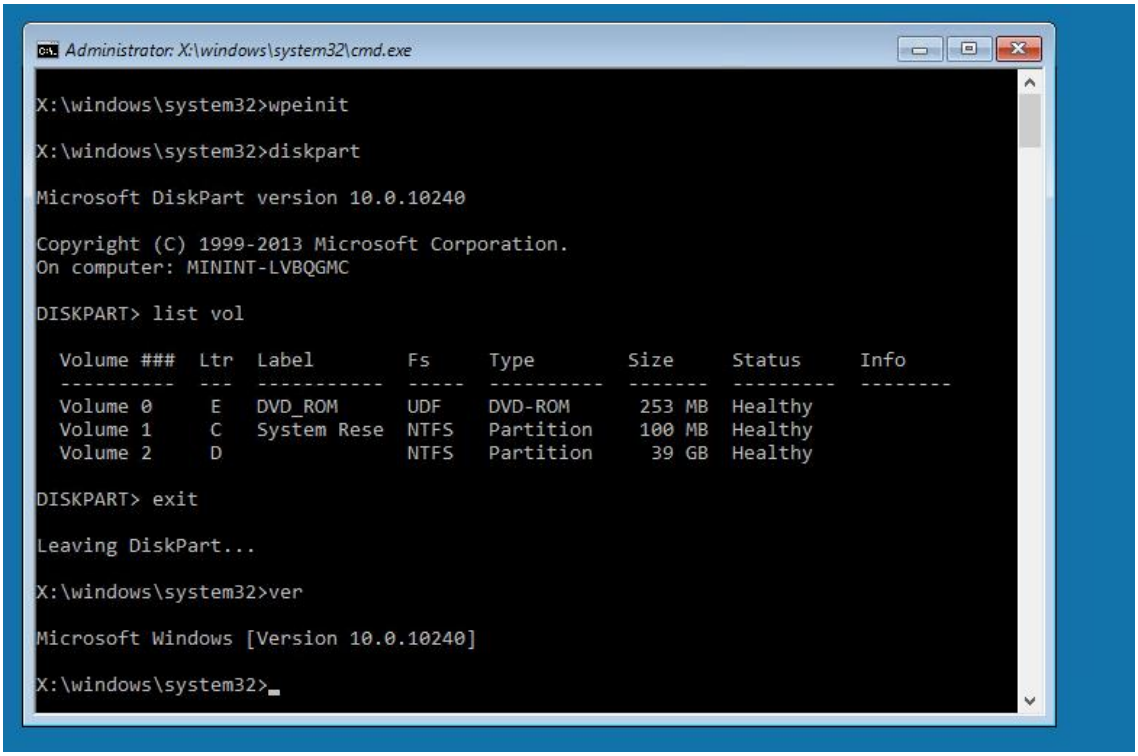


Figure 3-2: Computer started into WinPE 10

When you start into a WinPE OS, you can perform several different tasks on the host machine, such as the following:

- Use tools to set up the hard drive before installing Windows
- Initiate an image capture or deploy an image to an attached drive
- Run plug-ins, apps, or scripts
- Modify an existing Windows installation while it is not running

- Retrieve or back up data from a drive for which there is no functional OS
- Add a custom shell or GUI for automation of tasks

The lightweight OS will run from the Windows command-line environment (CLE), and the following features are supported:

- Batch files and scripts, including support for Windows Script Host (WSH), and ActiveX Data Objects (ADO), and optional support for Windows PowerShell.
- Applications, including Win32 application programming interfaces (APIs) and optional support for HTML Applications (HTA).
- Drivers, including a generic set of drivers that can run networking, graphics, and mass storage devices.
- Image capturing and servicing, including Deployment Image Servicing and Management (DISM).
- Networking, including connecting to file servers by using TCP/IP and NetBIOS over TCP/IP via LAN.
- Storage, including NTFS, DiskPart, and BCDBoot.
- Security tools, including optional support for BitLocker and the Trusted Platform Module (TPM), Secure Boot, and other tools.
- Hyper-V, including virtual hard drive (VHD) files, mouse integration, mass storage, and network drivers that make it possible for WinPE to run in a hypervisor.

> **More info** For a list of optional components as well as instructions on how to add them manually to a WinPE image, refer to https://msdn.microsoft.com/library/windows/hardware/dn938382(v=vs.85).aspx.

For the purposes of Configuration Manager OSD, two WinPE startup images (one x86 and one x64) are included during the installation of Configuration Manager via the preinstalled supported version of the Windows Assessment and Deployment Kit (ADK). You can also create, customize, and import startup images into Configuration Manager for use with image deployment. You can use the properties of the startup images to change the behavior at run time. For example, you can add startup-critical drivers to the image, turn on prestart commands to run custom scripts, add an image background, add optional components, and for troubleshooting turn on command-line support when the F8 key is pressed. The startup images are essentially managed as packages that are used to install the OS on target computers via a task sequence. As a prerequisite, the package must be made available on the DP before deploying an OS to a target computer, and if you make any changes, you must update the DP, as well.

To deploy Windows 10, you must use the WinPE startup images from the ADK for Windows 10. The WinPE 10 startup image version supports the deployments of Windows 7 through to Windows 10.

For specific information on the use of the ADK with Configuration Manager to deploy Windows 10, refer to http://blogs.technet.com/b/configmgrteam/archive/2015/08/05/windows-10-adk-and-configuration-manager.aspx?pi168308=2.

To customize WinPE for use in Configuration Manager, refer to https://technet.microsoft.com/library/dn387582.aspx.

For a complete WinPE 10 reference, visit https://msdn.microsoft.com/library/windows/hardware/dn938389%28v=vs.85%29.aspx.

www.dbooks.org

Task sequences

Installing an OS on a target computer via Configuration Manager is accomplished by means of *task sequences*. It is the driving mechanism of OSD that prepares a computer for the Windows OS WIM and performs post installation and configuration tasks. The following table describes the components of a task sequence:

Term	Definition
Action	The command of a single step within a task sequence. These are made up of built-in actions and custom actions.
Custom action	A command line typed by the administrator that will run on the client computer. For example, this could be the processing of a script.
Built-in action	A predefined action that might require further configuration.
Condition	A parameter that determines whether a group or step should process the action if evaluated to be true or false.
Step	The basic component of a task sequence or group. Each step contains an action and an optional conditional check to determine if it can be run.
Group	A logical arrangement of steps that can also have a conditional check. Using groups provides simplicity and readability of the task sequence and allows for better error handling.

As depicted in Figure 3-3, task sequences are a sequential set of tasks that you can deploy to a computer to initiate the processing of individual instructions at the command-line level, with or without user input.

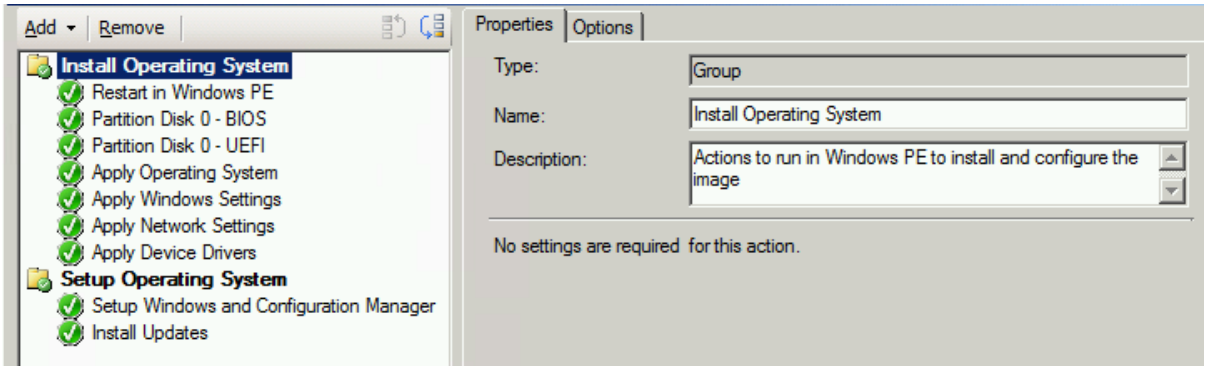


Figure 3-3: Default task sequence (created via the New Task Sequence Wizard) containing action steps

More info For a complete list and description of task sequence steps, refer to https://technet.microsoft.com/library/hh846237.aspx.

As each step runs, a test determines if a condition is properly satisfied before carrying out that step's commands. Based on the result, the step will either run or be skipped. Figure 3-4 shows an example of a condition that queries Windows Management Instrumentation (WMI) for the model of computer to determine if the device drivers in the step should be applied. You can also set conditions on a group, which will result in multiple underlying steps within the group being skipped if the desired result is not met. The next step will not run unless the previous action has completed successfully, unless the Continue On Error option is selected, which you would typically use for unique situations and troubleshooting. A task sequence is deemed to have run successfully when all steps have completed without error.

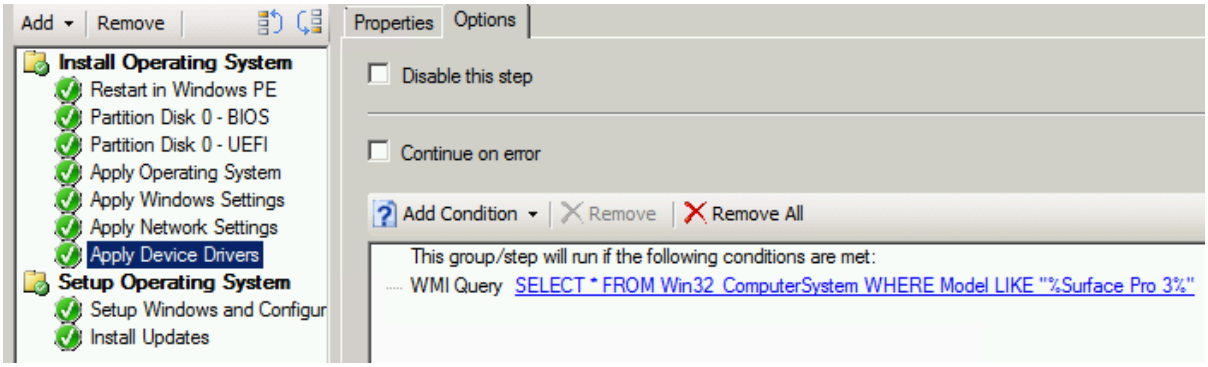


Figure 3-4: Condition set on a step via the options tab

You can define the following built-in conditions within a step and combine them by using the If statement to evaluate whether Any, All, or None of the conditions are true before proceeding with the step:

- Task Sequence Variable
- Operating System Version
- File Properties
- Folder Properties
- Registry Setting
- Query WMI
- Installed Software

For bare-metal, refresh, and wipe-and-load scenarios, when a task sequence is first carried out for OSD, it uses the built-in action of restarting a computer to begin the imaging process if it is not already in WinPE. To accomplish this, a WinPE startup image must be associated with the task sequence. To associate a startup image with a task, in the Properties dialog box, click the Advanced tab, and then, in the Use A Boot Image section, select the boot image, as shown in Figure 3-5.

www.dbooks.org

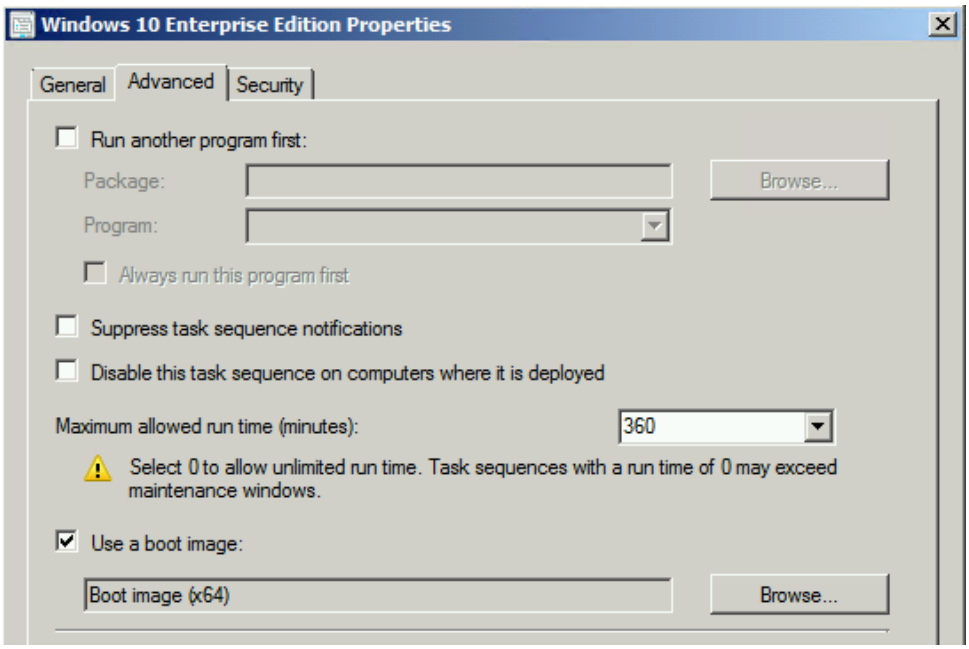


Figure 3-5: Boot image associated with a Task sequence

Task sequence variables

Task sequence variables are a set of name and corresponding value pairs that you use to configure and customize step actions and conditions throughout the running of a task sequence. You can use task sequence variables in the task sequence environment to perform the following actions:

- Configure settings for a task sequence action
- Supply command-line arguments for a task sequence step
- Evaluate a condition that determines whether a task sequence step or group is run
- Provide values for custom scripts used in a task sequence

The types of variables are as follows:

- Action variables provide a method to configure, override, and customize task sequence action steps.
- Built-in variables are initiated before the task sequence steps run and are available throughout the process. An underscore prefixed to a variable indicates that the variable is read-only. Built-in variables without the underscore can be used to define a value prior to running the task sequence.
- Custom variables are defined within the task sequence at run time via a script, on a computer record, collection, or the Set Task Sequence Variable step.

Administrators have the flexibility to create their own variables and values, which can be useful for cases in which custom actions are needed. For example, you could use a custom script in a step to query a database to determine values for variables that are defined for a later step that applies specific settings during a software installation. The possibilities of using variables to perform custom actions are endless, which provides the administrator with great control over the imaging process. Custom variables that are established by the administrator persist after restarts that are initiated by

the task sequence; otherwise, they are lost if the system is restarted by outside intervention, such as a user pressing the power button.

There are multiple ways to set variables. You can define them within the task sequence editor by using the built-in action named Set Task Sequence Variable; on a collection; a computer record within a collection; and via a script processed by the task sequence at run time.

Variables defined on a computer record take precedence over collection-based variables, and variables defined within a collection take precedence over built-in variables. Furthermore, if a computer record exists in multiple collections that have conflicting variables defined, the administrator can set a priority on the collection to enforce which will take precedence. Figure 3-6 shows a setting of 9, which dictates highest priority over another collection shown in Figure 3-7, which has a lower setting of 1 (the lowest setting). The variable settings defined on a computer record or collection are provided to the computer at the time the task sequence runs via policy. If the same variable is defined within a script as it is running, the script variable value will take precedence.

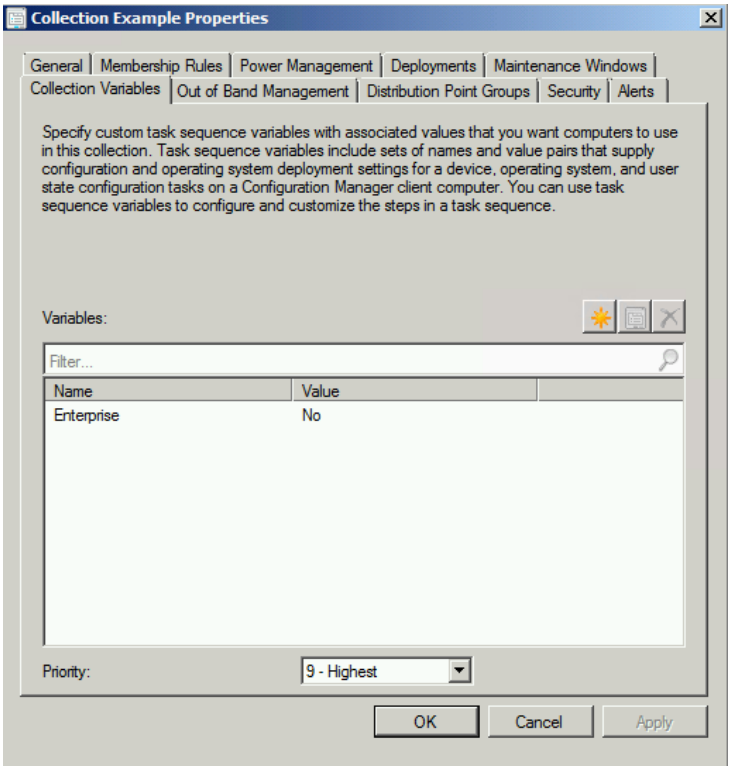


Figure 3-6: A collection containing a variable with highest priority

www.dbooks.org

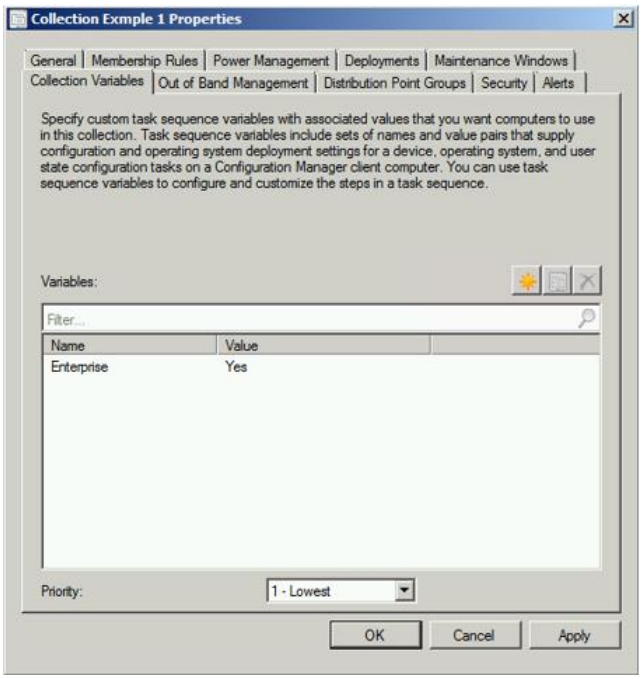


Figure 3-7: A collection containing a variable with lowest priority

Variables defined on collections without a value pair will result in a prompt to the end user of the computer on which the task sequence is running. This makes it possible for the user to input his own value. A simple example of this might be the entry of the computer name or asset information which will then be consumed by the task sequence and applied during a particular step.

More info For a complete list of the built-in variables refer to https://technet.microsoft.com/library/hh273375.aspx.

For a complete list of action variables, refer to https://technet.microsoft.com/library/hh273365.aspx.

Drivers and driver packages

To deploy an OS to a computer by using OSD, you must include dependent drivers for the model of machines to which you intend to deploy the OS. Configuration Manager provides a driver catalog to import and manage Windows device drivers for the environment. After you import the drivers, you can group them into packages that are typically based on computer model and distribute the packages to DPs for access by the task sequence at run time.

In most organizations, there are various hardware types that you must take into account prior to deployment of an OS at a mass scale. One of the primary reasons for this is to determine which machines are eligible for a particular OS installation and identifying the device driver requirements. This process would consist of testing WinPE functionality to ensure that the network and storage components are accessible using the generic built-in drivers; if not, the compatible drivers need to be injected into the startup image that will be used to run a task sequence. It is important to only inject startup-critical drivers into WinPE, which consist of network and storage drivers, other drivers such as audio are not needed and would only bloat the image size.

An effective way to test startup-critical drivers for WinPE is by using the drvload command while in the WinPE environment. Remember, WinPE supports hot swapping USB devices. You can simply copy the needed drivers to a USB stick and insert into the USB port of the machine. At this point, the device

will be assigned a drive letter. From the command prompt, change to the drive letter assigned and run **drvload.exe <driver filename>.inf**. If the driver does not load successfully, errors will be generated.

Next, hardware devices such as laptops and desktops would need to go through this testing cycle to identify the drivers to be installed while a task sequence is running. The drivers required are dependent on the version of the OS, architecture (x86 or x64), and the hardware components of the device.

When embarking on a driver management strategy, a key aspect to maintaining the driver catalog is to construct a folder structure that will be used as the source to import the drivers. The folder structure created on disk should also be created in the Configuration Manager console for consistency and ease of administration over time. While importing the drivers via the Import Driver Wizard, it is highly recommended that you add custom categories that consist of the OS, architecture, and computer model to which it applies. The purpose for doing this is to simplify searching and maintaining the catalog as hardware models reach the end of their life cycles. Another aspect of this is to easily identify and define the driver package that will be used during the creation of a task sequence.

If you choose to import drivers during the process of identifying the requirements for makes and models of machines in the environment, you might encounter a duplicate driver that was previously imported. The Import Driver Wizard provides four options for this circumstance:

- Import the driver and append a new category to the existing categories
- Import the driver and keep the existing categories
- Import the driver and overwrite the existing categories
- Do not import the driver

You can create driver packages during the import process, or afterward, via the driver packages node in the console. You can group drivers into a single package that would help streamline OS deployments to specific models of machines. In the event that duplicate drivers are added to multiple packages, only one instance of the driver-related file will exist on the DP by using the single-instance storage capability of the site system role. To understand how single-instance storage functions, go to http://blogs.technet.com/b/configmgrteam/archive/2013/10/29/understanding-the-configuration-manager-content-library.aspx.

In many scenarios, the most efficient method to install device drivers with accuracy is to use the Apply Driver Package task sequence step. To correctly identify the computer for which the driver package is intended, you can set a condition on the options tab of the step to query WMI and determine the model of machine. Following is what the query would look like:

```
Select * from Win32_ComputerSystem where Model LIKE "%<computer model>%"
```

In some cases, there might be instances of drivers provided by hardware manufacturers that are installed via applications. These hardware-based applications should maintain the intended installation logic. To accomplish applying these types of drivers, you can create an application through the Configuration Manager console and add it to the task sequence. To avoid installing the driver on the wrong computer, in these instances you can also similarly set a condition on the Install Application task sequence step to query WMI to determine the model of machine, as previously stated.

More info For further guidance on driver management, go to https://technet.microsoft.com/library/gg712674.aspx.

www.dbooks.org

Image deployment

There are three deployment scenarios that Configuration Manager can address:

- **New computer** This typically involves a blank machine or preexisting OS installation that needs to be replaced with an enterprise-standard deployment, and the data is not needed. The deployment methods used can be via startup media, PXE initiated, or offline media.
- **Computer refresh** This consists of a wipe-and-load that is generally initiated while in the existing OS. A task sequence is deployed to the existing client computer that is managed by Configuration Manager. Data and settings preservation is important for this scenario and must be carried out before the existing OS is replaced. Following OS replacement, the data and settings must then be restored.
- **Computer replace** This consists of swapping out the existing machine for a new machine but preserving the original user data and settings. This scenario also applies to changing the firmware mode from BIOS to UEFI. After the user data and settings are preserved off of the machine, the new computer scenario begins on the new hardware and restores the user data.

While planning an OSD strategy, you need to consider what the deployment type will be; Lite Touch Installation or Zero Touch Installation.

Lite Touch Installation consists of user interaction to initiate the deployment of the OS and/or provide information during the installation. This could consist of preparing the computer to start and run the task sequence, to entering values such as a computer name, defining computer purpose, and so on.

Zero Touch Installation is a deployment that does not require any user interaction and is fully automated. You would typically use this scenario as a required deployment that is initiated per the schedule that the administrator defines.

Regardless of the deployment type, you can design one task sequence to handle both of these scenarios.

After the requirements have been met along with any custom actions you might have provided for the task sequence, the following methods are available for deployment:

- **PXE deployments** Computers that support PXE startup can be used to initiate a network startup to request a deployment over the network. This type of deployment method suits new computers that are being provisioned in the environment for the first time. This method also works well when there is no physical presence at the destination computer. PXE-initiated deployments let client computers request a deployment over the network. In this deployment method, the OS image and a WinPE startup image are sent to a DP that is configured to accept PXE startup requests. To configure PXE startup, Windows Deployment Services must be installed on the DP server and the role must be configured for PXE. Figure 3-8 shows the configuration options for a PXE-enabled DP.

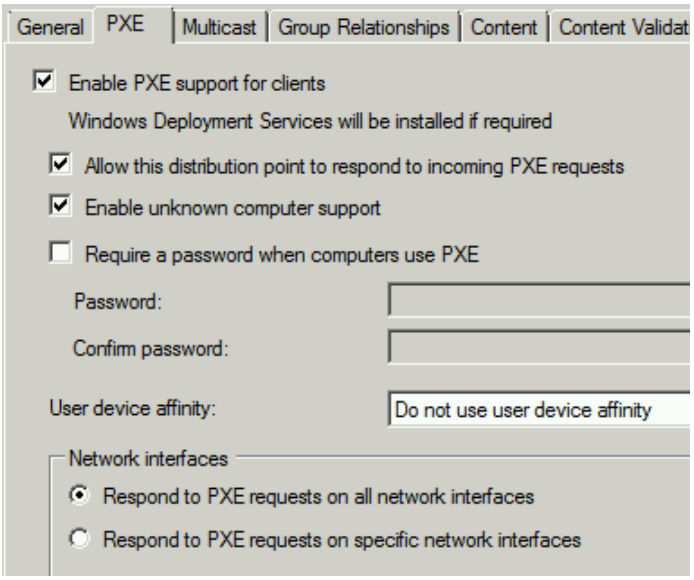


Figure 3-8: PXE options available on DP role

More info To learn more about PXE-initiated deployments, see Planning for PXE-Initiated Operating System Deployments in Configuration Manager.

For common issues related to PXE startup, go to http://blogs.technet.com/b/configurationmgr/archive/2011/01/05/troubleshooting-the-pxe-service-point-and-wds-in-configuration-manager-2007.aspx.

- **Multicast deployments** Multicast deployments provide network optimization when multiple clients are scheduled to download the same OS image concurrently. Rather than having each client download the same image over separate connections, the DP provides a single multicast session over the network that clients can hook into and download. Clients can join a multicast session already in progress. In this deployment method, the OS image is sent to a DP. The image is deployed when client computers request the location of the DP containing the image. You can configure the Multicast options via the DP role.

More info To learn more about deploying operating systems to multiple clients, read "Planning a Multicast Strategy in Configuration Manager," which you can find at https://technet.microsoft.com/library/hh397406.aspx.

- **Bootable media deployments** Bootable media deployments allow starting from USB, CD, or ISO by way of WinPE. When the destination computer starts, it retrieves the task sequence from the MP, and the OS image and other content dependencies from the DP. Because the content is not on the media, you can easily update the content without a dependency on the startup media.

More info For more information about bootable media, see the section "Bootable Media Operating System Deployments" of the Planning for Media Operating System Deployments in Configuration Manager topic.

- **Stand-alone media deployments** With stand-alone media deployments, you can deploy operating systems for situations in which it is not practical to download an OS image or other large content over the network. This type of deployment also suits environments without network connectivity or low bandwidth network connectivity. This consists of using media such as a USB stick to place the startup image, task sequence, and all content dependencies on the media. You can take steps to password-protect the media. There are also ways to expire the media to ensure

www.dbooks.org

that it is not used after a certain period of time, ensuring that outdated enterprise standards are not being used. For an example of this, go to http://blogs.technet.com/b/deploymentguys/archive/2012/02/15/expiring-outdated-stand-alone-media.aspx.

More info To learn more about stand-alone media, see the section "Stand-Alone Media Operating System Deployments" of the Planning for Media Operating System Deployments in Configuration Manager topic.

- **Prestaged Media deployments** Prestaged media deployments let you deploy an OS to a computer that is not fully provisioned. The prestaged media is a WIM file that the manufacturer or an enterprise staging center can install on a bare-metal computer that is not connected to the Configuration Manager environment.

  Later, when the computer starts in the System Center Configuration Manager environment, it does so by using the startup image provided by the media, and then connects to the site management point for available task sequences that complete the download process. This method of deployment can reduce network traffic because the startup image and OS image are already on the destination computer. Starting at Configuration Manager SP1, you can specify applications, packages, and driver packages to include in the prestaged media.

More info To learn more about prestaged media, see the section "Prestaged Media Operating System Deployments" of the Planning for Media Operating System Deployments in Configuration Manager topic.

Scheduling deployments

For a computer on the network to receive a task sequence, you have the option to create a deployment which would point to a collection containing the computer resource for which it is intended. This could be for existing clients managed by Configuration Manager or unknown computers, which is discussed further in the next section.

When creating a deployment, the purpose is defined as Available or Required. Available would be an optional deployment, either available in the Software Center for refresh scenarios or available to choose from when PXE or startup media is used. Required is typically for forceful installations that run from start to finish with no user interaction. There are also options to make it available for certain resource types (see Figure 3-9):

- **Only Configuration Manager Clients** Only valid for existing computers that are managed, refresh scenarios fit the purpose
- **Configuration Manager Clients, Media And PXE** Available to existing clients and unknown bare-metal scenarios
- **Only Media And PXE** Available to startup media and PXE startup–eligible computers, bare-metal scenarios
- **Only Media And PXE (Hidden)** Hidden from the Software Center, typically for testing purposes

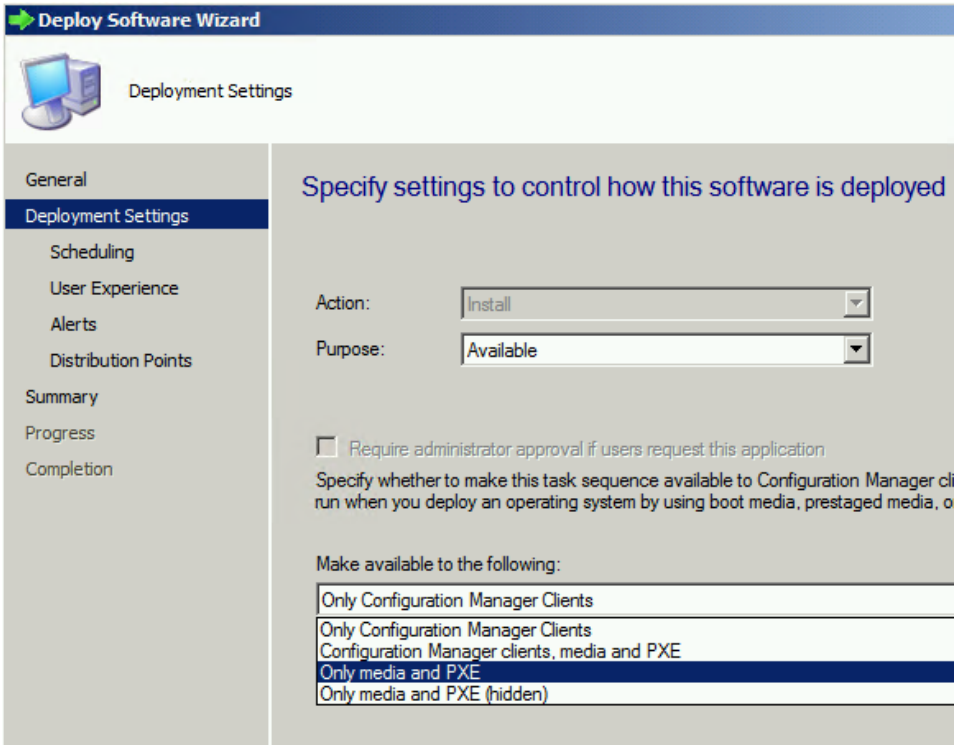


Figure 3-9: Deployment settings

If you select Required, the next page in the wizard (see Figure 3-10) enforces that you define an assignment schedule. If the deployment deadline has passed or you select As Soon As Possible, the task sequence will run immediately when the computer attains the policy.

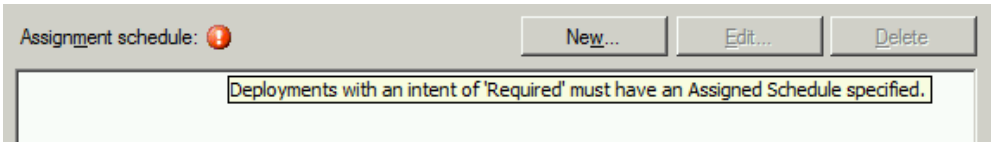


Figure 3-10: The Scheduling tab of the deployment wizard shows mandatory schedule required

Unknown computers

Configuration Manager has the ability to deploy task sequences to computers that are unknown to the environment by using PXE, startup media, or prestaged media. Unknown means that there is no existence of a computer record in the database. Unknown computers are classified as the following:

- A computer that has not been discovered
- A computer not imported into Configuration Manager
- A computer on which the Configuration Manager client has not been installed

A collection named All Unknown Computers with two architecture-based records for x86 and x64 exist. When an unknown computer is started, it is considered an *unprovisioned* computer, meaning it is eligible to receive any task sequences deployed to the collection containing the unknown computer records. If there is a deployment with a purpose of Required directed toward the collection, it will run immediately. For deployments that are configured with a purpose of Available, the user will be prompted to select the task sequence to run. This means that you can have multiple "Available"

www.dbooks.org

deployments from which to choose. More than one Required deployment might produce undesirable results because the sequence in which the task runs is nondeterministic in this scenario.

With this capability, importing computer information that consists of either the MAC address or SMBIOS is not required.

In the event of a failure during the run time of a task sequence, you might find that attempting to PXE-start the computer again to run the task sequence will result in failure, as well. The reason for this is because the MAC address of the computer is now known to Configuration Manager. To remediate this, you can create a query-based collection to search for the MAC address and then delete the computer record manually. The computer record name can be displayed as "unknown", MININT%, or the valid computer name if it progressed far enough in the task sequence.

It is very important to be aware of what deployments are targeting the unknown computer records with a purpose of Required. This can result in systems being reimaged mistakenly if they are PXE-started unintentionally. For example, an unprovisioned computer startup order might be PXE first, and upon restart will be wiped and reloaded with a different configuration. You can incorporate methods to perform condition-based evaluations within the task sequence prior to formatting or applying the OS WIM file; if the condition is not met, exit the task sequence. There is also password protection for PXE startup to avoid destructive outcomes and unauthorized access.

UEFI versus BIOS

UEFI (Unified Extensible Firmware Interface) is a standard firmware interface for personal computers. It was designed to replace BIOS (basic input/output system). BIOS has been the PC firmware standard for decades, but with the recent advancements in computer hardware, the stage is being set to remediate its shortcomings with the UEFI standard. More than 140 technology companies participate in the Unified EFI Forum, including Microsoft. New devices being shipped with Windows 10 must have UEFI firmware by default and Secure Boot technology turned on. Regardless of this requirement, legacy BIOS systems will still function with Windows 10 installed.

Some of the limitations of BIOS are as follows:

- 16-bit
- 1 MB address space
- Slow performance on ROM startup
- Master Boot Record (MBR) maximum bootable disk size of 2.2 TB

The advantages of UEFI over BIOS are the following:

- Security features such as Secure Boot and encrypted drives that prevent malware from running before the OS is loaded
- Faster startup and resume times
- Support for drives larger than 2.2 TB as well as drives with more than four partitions
- Support for modern, 64-bit firmware device drivers that the system can use to address more than 17.2 billion GB of memory during startup
- Backward compatibility to use BIOS with UEFI hardware, although Secure Boot must be turned off
- Support for multicast image deployments

Many current computers have the capability to use a BIOS or UEFI firmware mode—switching between one and the other is a fairly simple task. However, there are items to take into consideration with regard to OS deployment and changing existing systems that are on BIOS mode to UEFI mode:

- Changing from BIOS to UEFI requires changing the MBR/NTFS to GPT/FAT32 and NTFS. This translates to reinstalling the OS. This would be the equivalent to a wipe-and-load deployment.
- Ensure that the startup option you select matches the setting you want to have. It is common for old machines to have several startup options for BIOS but only a few for UEFI, or vice versa.
- When deploying from media, the media must be FAT32 for UEFI, and FAT32 has a file-size limitation of 4 GB.
- UEFI does not support cross-platform startup, you will need to have the correct startup media (32 or 64-bit).
- For UEFI-based PCs that support both UEFI and legacy BIOS modes, WinPE needs to be started in the correct mode in order to correctly install Windows. For more information, see WinPE: Boot in UEFI or legacy BIOS mode.

The 32-bit version of WinPE can start 32-bit UEFI and BIOS PCs, and 64-bit BIOS PCs.

The 64-bit version of WinPE can start 64-bit UEFI and BIOS PCs.

Reporting

When running a task sequence for OSD, the resulting success or failure for each step is returned to the Primary Site via state messages that you can view from the various reports included with the Reporting feature. Configuration Manager utilizes SQL Reporting Services and provides administrators with a close-to-real-time view of the progress of a running task sequence. The reports can provide a summary progress of running task sequences and link to detailed reporting views of the current step that is running. If a failure occurs, the resulting error code is returned. This facilitates immediate investigation into the issue. The built-in reports focused around task sequences consist of the following categories:

- Deployments
- Deployment status
- Progress
- References (consists of task sequence dependencies that should be available on a DP)

There are also reports available for driver management that can assist the administrator in identifying and maintaining the driver catalog throughout a device driver's life cycle. Figure 3-11 shows an example of some of the available reports.

www.dbooks.org



Icon	Name	Category
	Content referenced by a specific task sequence	Task Sequence - References
	Progress of a task sequence	Task Sequence - Progress
	Chart - Weekly progress of a task sequence	Task Sequence - Progress
	Progress of all task sequences	Task Sequence - Progress
	Status of all unknown computers	Task Sequence - Progress
	Progress of task sequences for operating system deployments	Task Sequence - Progress
	All task sequence deployments available to unknown computers	Task Sequence - Deployments
	Count of failures in each phase or group of a specific task sequence	Task Sequence - Deployments
	All task sequence deployments	Task Sequence - Deployments
	All system resources currently in a specific group or phase of a specific task s...	Task Sequence - Deployments
	All system resources where a task sequence deployment failed within a specif...	Task Sequence - Deployments
	Count of failures in each phase or group of a specific task sequence deploym...	Task Sequence - Deployments
	Progress of all deployments for a specific task sequence	Task Sequence - Deployments
	Summary report for a task sequence deployment	Task Sequence - Deployments
	Progress of a running task sequence deployment	Task Sequence - Deployments
	Deployment status of all task sequence deployments	Task Sequence - Deployments
	Progress of a running task sequence	Task Sequence - Deployments
	History of a task sequence deployment on a computer	Task Sequence - Deployment Status

Figure 3-11: Some of the various reports available for task sequences

There is also the flexibility to create custom reports if any of the built-in reports are not meeting specific criteria. For more information on the reporting component, refer to https://technet.microsoft.com/library/gg699377.aspx.

Advanced concepts

Configuration Manager provides a complete set of tools for the administrator to deploy an OS and troubleshoot issues along the way. It can be further enhanced to add deployment customizations based on the requirements of the environment and also add user-specific needs.

Logging

Configuration Manager is equipped with logging features that by default record process information for every component running on both the client and server. In most cases, an administrator will refer to the log files that are pertinent to a component experiencing an issue. With respect to OSD, it is useful to first review the available built-in reports to determine the status of a task sequence that was running on a computer. For cases in which there has been an error reported on a particular step, there might not be a need to examine the log files. The reports provide initial details that might result in identifying the resolution as per the error code provided before investigating the log files.

Two of the most accessed log files during an OSD deployment are the SMSTS.LOG (Client) and SMSPXE.LOG (Server).

The SMSTS.LOG consists of all activities of a running task sequence. To gain access to the log file while in WinPE, you can press F8 (if turned on in the startup image) to open a command-prompt window in which you can access the X:\ drive, navigate to the folder, and open the file by using notepad or cmtrace.exe. The following table shows the possible locations of the log file, depending on the phase of the task sequence:

Deployment Phase	Location
While running in WinPE	X:\Windows\Temp\SMSTSLog\
Full OS with ConfigMgr client	%temp%\SMSTSLog\
Within OS while task sequence running	<CCMInstallDir>\Logs\SMSTSLog
Within OS and task sequence complete	<CCMInstallDir>\Logs

The SMSPXE.LOG consists of the activities when attempting to PXE-start a computer. Entries in this log file will indicate if a computer has contacted the DP\PXE server for a policy request and the responses to the client. In most cases, if a computer is unable to PXE-start, a review of this log file for the MAC address or the computer SMBIOS of the requesting computer can reveal why a computer has not been able to do so. If the PXE component is turned on for a site server, the log will be located in \SMS_CCM\Logs. If PXE is turned on for a remote DP, the log file will be located within \Program Files\Microsoft Configuration Manager\Logs by default.

For a complete list of the various log files relating to OSD, go to https://technet.microsoft.com/library/hh427342.aspx#BKMK_OSDLog.

For custom error codes as they relate to OSD, go to https://technet.microsoft.com/library/bb735886.aspx.

Prestart commands

Prior to running a task sequence on a computer, you can initiate a script or executable to interact with the user from within WinPE. This is beneficial to prompt the user for specific information and then consume the resulting input into a variable for later use in the task sequence. A popular method is to use an HTML Application to present a UI in which the user can provide information such as computer name, department, and asset tag. There are many examples online that demonstrate this capability.

More info To learn more, go to https://technet.microsoft.com/library/jj651034.aspx.

User Device Affinity

User Device Affinity (UDA) is a method to associate a user with one or more devices. The purpose of UDA is to facilitate deployment of applications to the user instead of determining the user's computer and deploying to it. This essentially means that the applications the user should have will be installed based on the primary device she uses, and this could be defined as multiple devices. Configuration Manager supports a single primary user for a device, multiple users per device, and multiple primary devices per user. With respect to OSD, you can integrate UDA as part of the imaging process in order to have the users applications installed before they log on. This can accelerate the deployment process and make it less complex.

More info To learn more, refer to the following links:

How to Manage User Device Affinity: https://technet.microsoft.com/library/gg699365.aspx

How to Associate Users with a Destination Computer: https://technet.microsoft.com/library/hh846243.aspx

UDA and OS Deployment: http://blogs.technet.com/b/inside_osd/archive/2011/06/20/configuration-manager-2012-user-device-affinity-and-os-deployment.aspx

www.dbooks.org

Online resources

- Documentation Library for System Center 2012 Configuration Manager
- System Center 2012 Configuration Manager Forums
- System Center 2012 Configuration Manager Survival Guide
- System Center Configuration Manager Team Blog
- System Center Configuration Manager Support Team Blog
- System Center Configuration Manager Support
- Submit Configuration Manager Product Ideas
- Report Configuration Manager Product Issues

CHAPTER 4

Using System Center Configuration Manager to deploy Windows 10

This chapter covers the requirements, processes, and intricacies of using System Center Configuration Manager to deploy Windows 10. Topics covered include the Microsoft Deployment Toolkit and Automated Deployment Kit integration with System Center Configuration Manager. Also discussed are the actual deployment processes, including obtaining, importing, and customizing the Windows 10 image; managing disk configurations; and, finally, optimizing, deploying, and monitoring the Window 10 deployment.

www.dbooks.org

This chapter covers:

- Microsoft Deployment Toolkit integration with Operating System Deployment
- Windows Assessment and Deployment Kit
- Obtaining and importing the Windows 10 image
- Customizing the Windows 10 image
- Deploying and supporting Windows 10

Microsoft Deployment Toolkit integration with Operating System Deployment

Microsoft Deployment Toolkit (MDT) is a free, fully supported download from Microsoft that adds via System Center Configuration Manager approximately 280 enhancements to Windows operating system (OS) deployments. Although it is not a technical requirement, it is commonly preferred by Configuration Manager administrators to utilize MDT when customizing, capturing, and deploying Windows operating systems by using Configuration Manager. In addition to integrating MDT with Configuration Manager, it is also often a preference by administrators to use an MDT Lite Touch (LTI) task sequence to create Windows reference images used in Configuration Manager.

When MDT is integrated with Configuration Manager, the MDT task sequence takes additional instructions from the MDT rules. In its most simple form, these settings are stored in a text file, CustomSettings.ini, but you also can choose to store the settings in a Microsoft SQL Server database, and run Microsoft Visual Basic Scripting Edition (VBScripts), Windows PowerShell scripts, or call web services to dynamically determine the settings to use during an OS deployment. The MDT task sequences created within the Configuration Manager Administrator Console can utilize additional dynamically populated variables above and beyond those that are provided out of the box with Configuration Manager. These dynamic variables can help to further reduce the total number of task sequences required in Configuration Manager by optionally storing the dynamic settings outside of the task sequences themselves.

Integrating MDT into your Configuration Manager environment also makes possible the use of a capability called User Driven Installation (UDI). With UDI, you can provide end users or desktop support personnel with the means to interact with a number of OS deployment steps. Some examples are naming the machine, choosing an organizational unit (OU), and choosing the applications to install. The UDI component comes included with a UDI Wizard Designer, as shown in Figure 4-1, which gives the administrator the ability to customize the interface presented during the installation of the OS.

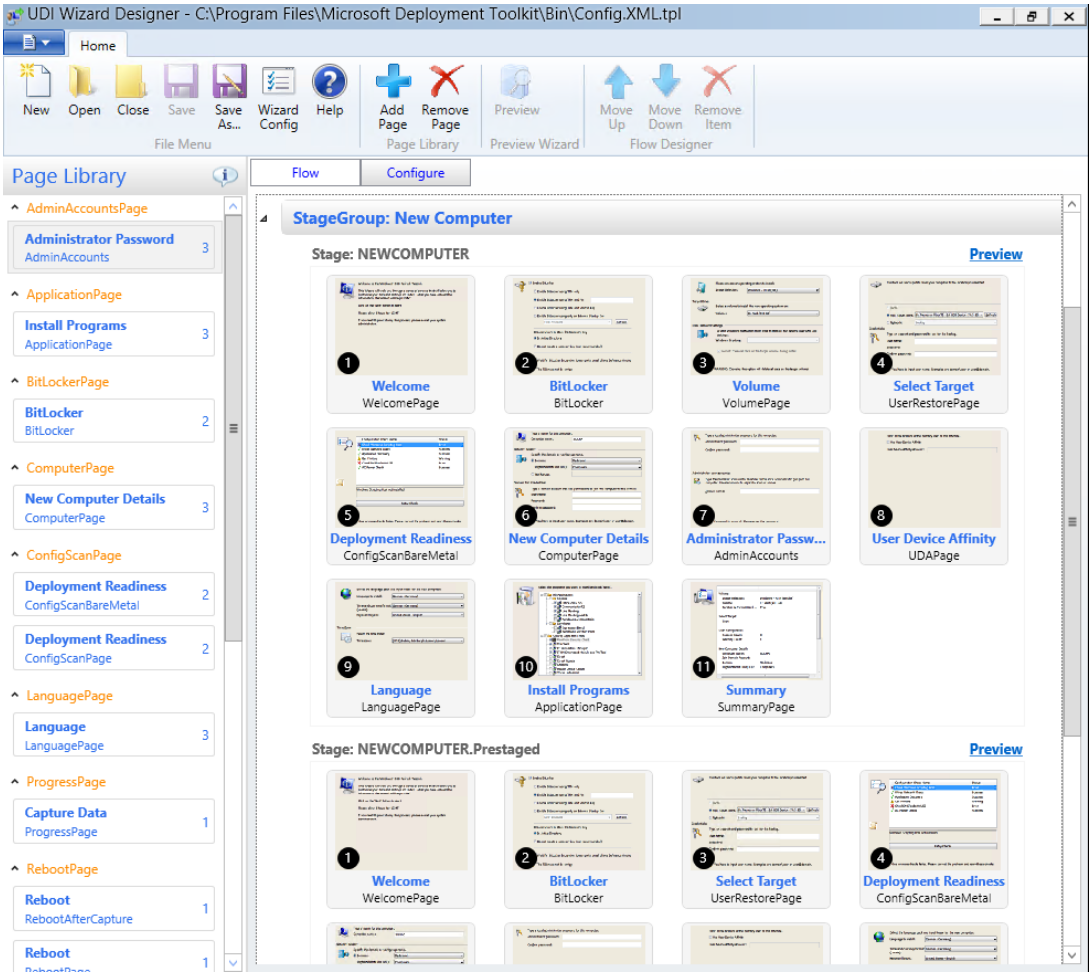


Figure 4-1: The optional UDI wizard in the UDI Wizard Designer

More info For a quick-start guide to using UDI, go to https://technet.microsoft.com/library/dn781087.aspx.

Another benefit of MDT commonly preferred by Configuration Manager administrators is the ability to more easily create reference images through a build-and-capture task sequence created in the MDT Workbench. There are many customization tasks such as installing language packs which many administrators find easier to install in their core image through a task sequence created in the MDT Workbench, as opposed to a task sequence in Configuration Manager's OSD capability. You can also use the same image for every type of OS deployment—Microsoft Virtual Desktop Infrastructure (VDI), System Center 2012 R2 Virtual Machine Manager (SCVMM), MDT, System Center Configuration Manager, Windows Deployment Services (WDS), and more. MDT also supports a Suspend action through the use of an MDT script named LTISuspend.wsf that allows for reboots. LTISupend.wsf also provides a shortcut on the desktop that will resume the task sequence. This can be useful when you need to perform a manual installation or check the reference image before it's automatically captured. The flexibility of using whichever methods you are most comfortable with is the primary reason administrators choose Configuration Manager as their OS deployment tool of choice.

If you do choose to integrate MDT into your Configuration Manager site, the minimum version of MDT that includes support for deploying a fresh installation of Windows 10 is MDT 2013 with Update 1. This version of MDT includes support for deploying operating systems running Windows 7 through Windows 10. As of this writing, MDT 2013 Update 2 is the latest released version available.

www.dbooks.org

MDT 2013 Update 2 is primarily a quality release; no new major features have been added since the Update 1 release.

> **More info** To learn more about the improvements in MDT 2013 Update 2, go to http://blogs.technet.com/b/msdeployment/archive/2015/12/22/mdt-2013-update-2-now-available.aspx.

If you are currently running MDT 2012 Update 1 or higher, you can perform an in-place upgrade of your current MDT installation to MDT 2013 Update 1 or higher. If you are running a version released prior to MDT 2012 Update 1, you first must uninstall MDT and then install MDT 2013 Update 1 or Update 2. It is always recommended to back up your current MDT environment before attempting to upgrade.

Existing MDT task sequences that you've created in Configuration Manager 2012 are not modified during the MDT upgrade and should continue to function without any issue. After installing MDT 2013 Update 1 or higher, on the start menu of each machine that has the Configuration Manager Administrator console installed, run the Configure ConfigMgr Integration Wizard. This properly registers the new MDT components and extensions, and installs the updated MDT templates into the Configuration Manager Administrator Console.

You will also need to create a new MDT Toolkit Files package for use in any new Zero Touch Installation (ZTI) task sequences you will create following the MDT 2013 Update 1 or higher installation. You can utilize any previously created MDT Toolkit Files packages with your previously created task sequences, but any new task sequences must reference the updated MDT Toolkit Files package in order to support the new capabilities added to the newly installed version of MDT.

Windows Assessment and Deployment Kit

The Windows Assessment and Deployment Kit (ADK) is a collection of tools and documentation that original equipment manufacturers, original design manufacturers, and IT Professionals use to customize, assess, and deploy Windows operating systems. The Windows ADK enables two key scenarios, Windows deployment and Windows assessment, and supports deployment of operating systems running Windows 7 through Windows 10. Keep in mind that these are just tools and not a complete solution on their own. When you combine these tools with MDT and Configuration Manager, you get the complete deployment solution.

Included in the Windows 10 ADK installation are the Application Compatibility Toolkit (ACT), Deployment Tools, Windows Preinstallation Environment (WinPE), User State Migration Tool (USMT), Volume Activation Management Tool (VAMT), Windows Performance Toolkit (WPT), Windows Assessment Toolkit, and Windows Assessment Services. Another new component, which was not in previous ADK versions, is the Windows Imaging and Configuration Designer (ICD), which gives you the ability to streamline image customizations, deployment, and provisioning across all Windows devices. You can use Windows ICD to create provisioning packages containing drivers, apps, language packs, settings, and more, which you can then install from a file share, USB media, or deploy to existing clients via Configuration Manager.

> **More info** To learn more about Windows ICD, go to https://msdn.microsoft.com/library/windows/hardware/dn916112(v=vs.85).aspx and https://channel9.msdn.com/Events/Windows-Deployment/Windows-Deployment-Fest-2015/Windows-Imaging-and-Configuration-Designer-WICD.

To successfully install a new Configuration Manager Site Server, you must satisfy the following three Windows 10 ADK prerequisites:

- **Deployment Tools** The Deployment Tools component of ADK provides some of the key tools required for servicing and manipulating Windows images. Some examples are Deployment Image Servicing and Management (DISM), which is used to install updates and optional components to images; OSCDIMG, which is used to create ISOs of customized images; and BCDBoot which facilitates the management of system partitions.
- **WinPE** WinPE is the minimal OS designed to prepare a computer for installation and servicing of Windows. Both the x86 and x64 architecture flavors of WinPE are included in the installation of the Windows ADK. The WinPE version included with the ADK for Windows 10 begins with 10.0.
- **USMT** USMT provides the Scanstate and Loadstate tools, which are required to migrate user's profile data from a previous Windows installation to a new Windows installation. MDT and Configuration Manager use USMT as part of the OS deployment process.

A new capability in USMT introduced in the Windows 10 ADK facilitates migration of applications and third-party drivers. The Windows PowerShell cmdlet Export-WindowsDriver provides the ability to migrate third-party device drivers from a Windows image to a destination folder. This feature existed in the Windows 8.1 ADK, but with the Windows 10 ADK, the drivers are now stored in a provisioning package (PPKG) file. Invoking ScanState.exe by using the /apps switch will capture all Windows Store applications that are installed under the following folders:

```
C:\Windows

C:\Program Files

C:\Program Files (x86)

C:\ProgramData

C:\Users
```

USMT preserves user-generated content, the user's customized experience of Windows, and application settings within the constraints of OS and application compatibility.

You can download the Windows 10 ADK from http://go.microsoft.com/fwlink/p/?LinkId=526740. You must install the Windows ADK on each computer that currently hosts, or will host, a Central Administration Site or Primary Site server before you install the Configuration Manager site. If an older version of the Windows ADK is currently installed on your Configuration Manager site servers, you must uninstall the previous version prior to installing the Windows 10 ADK. The Windows 10 ADK is required to support bare-metal, refresh, and dynamic provisioning methods of deploying Windows 10. For in-place upgrades, you can use either the Windows 8.1 or Windows 10 ADK.

> **Note** Removing the Windows ADK will automatically remove the included version of USMT. A default USMT package creation utilizes this installation as the source path location when initially creating the USMT package. If you have the need to continue using the older version of USMT in your task sequences after uninstalling the ADK, it is recommended that you copy the USMT files to a new location and modify the USMT package to use the new path prior to uninstalling the ADK.

Each version of System Center Configuration Manager supports a specific version of the Windows Automated Installation Kit (AIK) or ADK. You can service or customize boot images from the Configuration Manager console when they are based on a WinPE version from the supported version of Windows AIK or Windows ADK. If you want to customize a WinPE startup image that is based on any other version of the Windows AIK or ADK other than the version which is installed on the Configuration Manager site server, you must use customization methods such as DISM.EXE outside of the Configuration Manager console. For more information, visit https://technet.microsoft.com/library/dn387582.aspx.

When customizing boot images, it is always a best practice to import drivers only when the out-of-box WinPE drivers do not provide the basic network or disk functionality required to successfully

www.dbooks.org

apply your Windows image. Not only will this practice keep the boot image sizes small, it will also reduce the chance of issues caused by incorrect drivers being utilized during the WinPE processes.

More info To learn more about customizing WinPE startup images for use in Configuration Manager, go to https://technet.microsoft.com/library/dn387582.aspx.

Installing the Windows ADK manually on a small number of site servers might be acceptable. However, if you need to install on a large number of servers, you can opt to download the Windows ADK components and silently install them by using Configuration Manager or any other desired method. To do so, select the Download The Windows Assessment And Deployment Kit – Windows 10 For Installation On A Separate Computer option and type the desired download path, as shown in Figure 4-2.

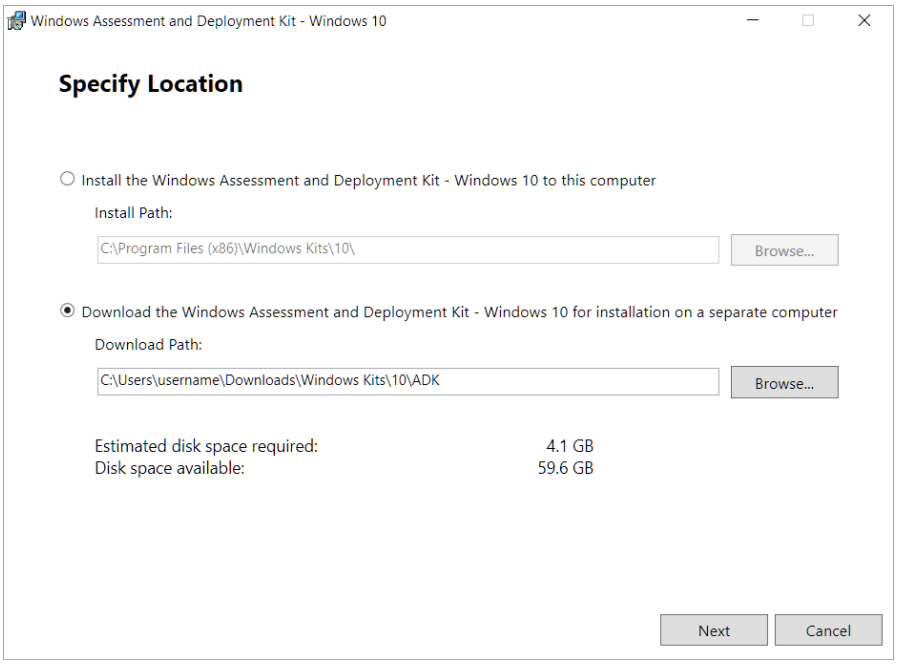


Figure 4-2: The Specify Location dialog box

Alternatively, you can use the command line ADKSETUP.EXE /LAYOUT to download the ADK installer files locally for installation on other machines. After the ADK components have finished downloading, you can review the list of Windows ADK feature names available to install by running ADKSETUP.EXE /LIST at a command prompt. The dialog box shown in Figure 4-3 appears, listing all of the available features that you can install.

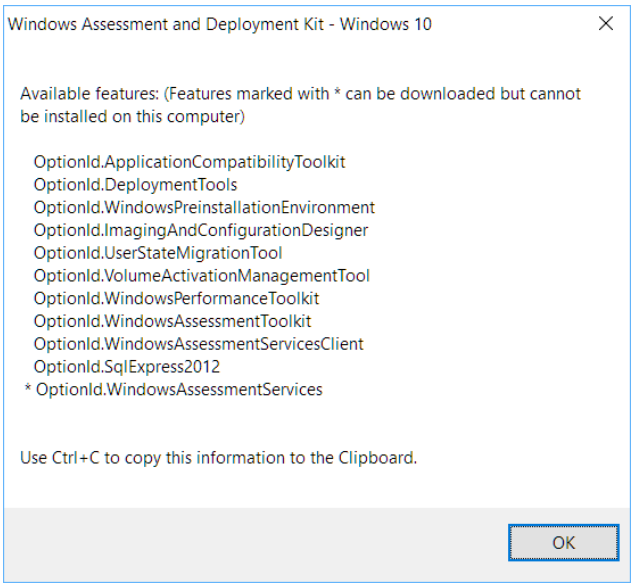


Figure 4-3: The Windows 10 ADK available features dialog box

To silently install the Windows 10 ADK components that are prerequisites for Configuration Manager, you can create an application or package in Configuration Manager by using the command line ADKSETUP.EXE /Quiet /Features OptionId.DeploymentTools OptionID.WindowsPreinstallationEnvironment OptionId.UserStateMigrationTool. Running this command line within the directory in which you've saved the Windows 10 ADK download installs the Deployment Tools, WinPE, and USMT components that are required to install a new Configuration Manager Primary or Central Administration site server, or after removal of the Windows 8.1 ADK on an existing site server.

Obtaining and importing the Windows 10 image

To deploy Windows 10, you need to acquire the appropriate installation media for your environment, as outlined in Chapter 2. If you will be testing in a lab environment, downloading and importing the Windows 10 ISO from MSDN might be sufficient. For a production deployment, you will need to download and import the appropriate Windows edition from the Microsoft Volume Licensing Service Center (VLSC). Importing the correct Windows edition is important, because even though it is possible to upgrade from Windows 7 SP1 through Windows 8.1 Professional to Windows 10 Enterprise, you cannot perform an in-place upgrade from Windows Enterprise to Windows 10 Professional. For all supported scenarios of switching from one Windows edition to another, go to https://technet.microsoft.com/en-us/library/mt605190(v=vs.85).aspx.

To support an in-place upgrade scenario, you must import the extracted Windows 10 installation media into the Operating System Upgrade Packages node within the Operating Systems node of the Configuration Manager Administrator Console.

Customizing the Windows 10 image

You can customize the Windows 10 Start menu layout by using a variety of methods. Here are some examples:

- Using the Windows PowerShell cmdlet Export-StartLayout to export the customizations after customizing the menu on a test computer, and Import-StartLayout to reimport them
- Using the Windows ICD to create provisioning packages

www.dbooks.org

- Modifying the Layoutmodification.xml file, which is located in C:\Users\Default\AppData\Local\Microsoft\Windows\Shell, and importing it into the Start Layout group policy located in User Configuration\Administrative Templates\Start Menu and Taskbar group policy setting within the Group Policy Management Console (GPMC)
- Using Mobile Device Management (MDM) policies

More info To learn more about customizing the Windows 10 Start menu, go to https://msdn.microsoft.com/library/windows/hardware/mt171092(v=vs.85).aspx and https://technet.microsoft.com/library/mt484194(v=vs.85).aspx.

In-box applications

It is commonly desired to customize the applications that are automatically installed during a default installation of Windows. Additionally, customizing the default Start menu layout and removing any undesirable desktop clutter to ensure as positive an end-user experience as possible is desired.

You can remove many of the in-box applications that are installed during the Windows 10 installation either offline from within WinPE or online from within the Windows 10 installation. You can automate and run the script to remove these applications by using Windows PowerShell cmdlets, all in a single step within the Windows 10 deployment task sequence.

More info For a sample script to assist with removing in-box applications, go to http://blogs.technet.com/b/mniehaus/archive/2015/11/11/removing-windows-10-in-box-apps-during-a-task-sequence.aspx.

Group Policies

You can download a customizable reference spreadsheet outlining the Windows 10 Group Policies settings from http://www.microsoft.com/download/details.aspx?id=25250. The Group Policy administrative templates for each build of Windows 10 are available at http://www.microsoft.com/download/details.aspx?id=48257.

Windows 10 version 1511 includes a new Group Policy setting, Turn Off Microsoft Consumer Experiences, which prevents the automatic installation of consumer applications and games such as Twitter, Minecraft, and others. To customize this, you will need to download the Windows 10 1511 Group Policy template and import it into your Group Policy definitions folder.

Deploying and supporting Windows 10

Windows 10 provides new deployment capabilities, scenarios, and tools by building on technologies introduced in Windows 7, and Windows 8.1, while at the same time introducing a new "Windows as a Service" concept to keep the OS up to date. Together, these changes require that you rethink the traditional deployment process.

The ability to deploy Windows 10 is a new capability which is possible beginning with Configuration Manager 2012 SP2 CU1 and Configuration Manager R2 SP1 CU1. Although the Windows 8.1 ADK is a prerequisite for installing these versions of Configuration Manager 2012, they also support installing the Windows 10 ADK version. The Windows 10 ADK is required in order to support all Windows 10 image deployment scenarios other than in-place upgrades. If you are currently running one of these versions of Configuration Manager with the Windows 8.1 ADK, you can successfully deploy an in-place upgrade task sequence to perform an in-place upgrade of an existing Windows 7 or Windows 8.1 client to Windows 10, just as you can if you have the Windows 10 ADK installed. Additionally, if you

are integrating MDT into your Configuration Manager hierarchy, you must also install MDT 2013 Update 1 or higher to support Windows 10 deployments other than in-place upgrades.

Microsoft has extended Configuration Manager 2012 support for Windows 10 to include the first two builds of the Windows 10 Current Branch releases (Windows 10 RTM and 1511). To support releases beyond this, you must upgrade your Configuration Manager hierarchy to Configuration Manager version 1511 or higher.

Windows 10 clients and devices can be managed solely using Microsoft Intune or through a Hybrid scenario in which some clients are managed via Intune, whereas others are managed on-premises by using the Intune integration capabilities of Configuration Manager.

More info To view a video discussing the management of Windows 10 with Microsoft Intune and Hybrid management scenarios, go to https://channel9.msdn.com/Events/Ignite/2015/BRK3310.

Managing disk configurations

In this section, you will gain a better understanding of what methods are available to deploy Windows to different drive types, including platter-type hard drives, solid-state drives (SSDs), or virtual hard drives (VHDs).

Following are some of the improvements related to hard drives in Windows 10:

- **Compact OS, single-sourcing, and image optimization** This feature provides the ability to compress the files for the entire OS, including your preloaded desktop applications. Compact OS makes it possible for you to run the OS from compressed files (similar to WIMBoot in Windows 8.1 update 1), and single-instancing gives you the ability to run Windows desktop applications in compressed files. The new processes help maintain a small footprint over time by using individual files, rather than combining them into a Windows Imaging Format (WIM) file. Compact OS is supported on both UEFI and BIOS-based devices. Unlike WIMBoot—for which the files are included into a single WIM file—Windows Update can replace or remove individual files as needed to help maintain the drive footprint size over time.
- **Deploy Windows by using Full Flash Update (FFU)** With FFU images, you can apply a Windows image directly to a drive or SD card, laying down the entire drive at once, including the partition information. To create and apply FFU images, you can use the Windows ICD or the Windows 10 version of DISM, which is included in the Windows 10 version of Windows Preinstallation Environment (WinPE). After you've created an FFU image, you cannot modify or edit it offline. FFU images are typically too large to fit on a standard FAT32-formatted USB flash drive. To get around this, you can either use a separate storage drive or network location, or you can split the image into smaller .sfu files.

There are some considerations which you must take into account depending on whether you will be deploying UEFI/GPT-based hard drive partitions, or BIOS/MBR-based partitions.

For a UEFI/GPT-based hard drive partition, you must format the hard drive which includes the Windows partition by using a GUID partition table (GPT) file system. Additional drives can use either the GPT or the master boot record (MBR) file format. A GPT drive can have up to 128 partitions, and each partition can have a maximum of 18 exabytes (roughly 18.8 million terabytes) of drive space.

UEFI/GPT Windows partition requirements

The requirements for UEFI/GPT Windows partition are as follows:

- **System (EFI) partition** The device must contain a system partition. On GPT drives, this is referred to as the EFI System Partition, or ESP. This partition is most commonly stored on the primary hard drive. This is the device's startup partition.

www.dbooks.org

The minimum size for the ESP partition is 100 MB, and it must be formatted by using the FAT32 file format. When creating a new task sequence, a 512 MB EFI partition will be created to support UEFI-based clients. The partition is managed by the OS and should not contain any other files, including Windows Recovering Environment (WinRE) tools.

Note For Advanced Format 4K Native (4-KB-per-sector) drives, the minimum size is 260 MB, due to a limitation of the FAT32 file format. The minimum partition size of a FAT32 drive is calculated as sector size (4KB) x 65527 = 256 MB.

Advanced Format 512e drives are not affected by this limitation, because their emulated sector size is 512 bytes. 512 bytes x 65527 = 32 MB, which is less than the 100 MB minimum size for this partition.

- **Microsoft Reserved Partition (MSR)** Beginning in Windows 10, the size of the MSR partition is 16 MB; however, when creating a new task sequence, a 128 MB MSR partition will be created by default. The MSR is a reserved partition that does not receive a partition ID, and it cannot store user data.
- **Other utility partitions** Any other utility partitions not managed by Windows must be located before the Windows, data, and recovery image partitions. This makes it possible for end users to perform actions such as resizing the Windows partition without affecting system utilities.

  You should protect against end users accidently modifying utility partitions by making them hidden partition types in the Format And Partition Disk task sequence steps. This prevents these partitions from appearing in File Explorer.
- **Windows partition** The Windows partition (commonly referred to as OSDisk) must have at least 20 GB of drive space for 64-bit Windows 10 versions, or 16 GB for 32-bit Windows 10 versions. The partition must be formatted by using the NTFS format. The Windows partition must have at least 10 GB of free space after completion of the out-of-box experience (OOBE).
- **Recovery tools partition** The recovery tools partition (commonly referred to as the WinRE Tools partition) must be at least 300 MB. The WinRE partition will store the Windows Recovery Environment image (WINRE.WIM) which is typically between 250-300 MB, depending on the base language and customizations added, plus enough free space so that backup utilities can capture the partition. If the partition is less than 500 MB, it must have at least 50 MB of free space. If the partition is 500 MB or larger, it must have at least 320 MB of free space. If the partition is larger than 1 GB, it is recommended to have at least 1 GB of free space.

The default drive partitioning, as shown in Figure 4-4, for UEFI-based PCs in an unmodified Create New MDT Task Sequence menu option is as follows:

- 300 MB WinRE Tools (Recovery) partition
- 512 MB EFI (system) partition
- 128 MB MSR partition
- 100 percent of remaining space for the Windows partition

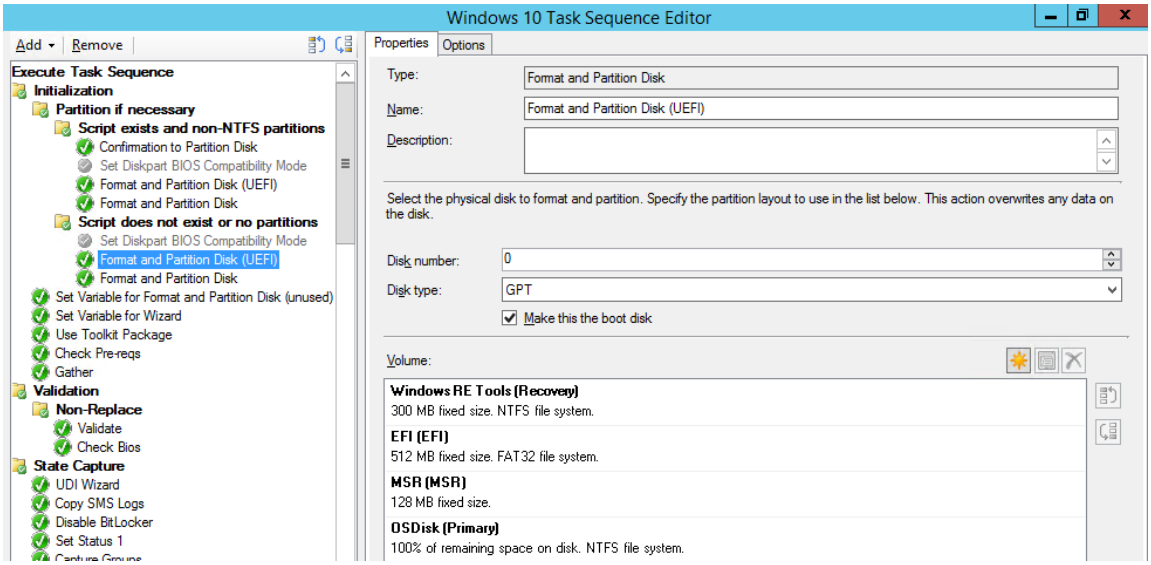


Figure 4-4: Format And Partition Disk task sequence step in a Create New MDT task sequence

The default layout (see Figure 4-5) for UEFI-based PCs in an unmodified non-MDT task sequence is as follows:

- 500 MB EFI (system) partition
- 128 MB MSR partition
- Windows Primary partition using 99 percent of the remaining space on the drive
- WinRE Tools (Recovery) partition using 1 percent of the remaining space on the drive

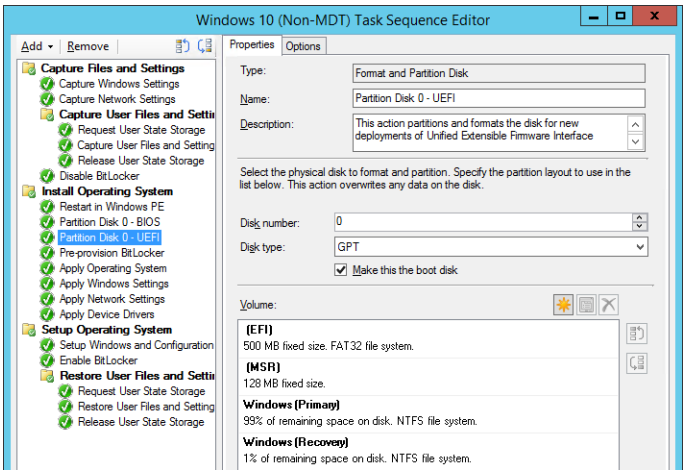


Figure 4-5: Format And Partition Disk task sequence step in a non-MDT task sequence

For a BIOS-based device, you must format the hard drive by using an MBR file system. Windows does not support the GPT file system on BIOS-based computers.

An MBR drive can have up to four standard partitions. Typically, these standard partitions are referred to as *primary partitions*.

More info For more information about how to create additional partitions beyond this limit, see https://msdn.microsoft.com/library/windows/hardware/dn898506(v=vs.85).aspx.

www.dbooks.org

BIOS/MBR Windows partition requirements

Following are the requirements for BIOS/MBR Windows partition:

- **System partition** Each startup drive must contain a system partition. The system partition must be configured as the active partition. The minimum size of this partition is 100 MB.
- **Windows partition** This partition must have at least 20 GB of space for a 64-bit Windows 10 version, or 16 GB for 32-bit versions. The partition must be formatted by using the NTFS file format. The partition must have at least 10 GB of free space after the user has completed the OOBE. The partition can have a maximum of 2 TB of space.
- **Recovery tools partition** The WinRE tools image (WINRE.WIM) should be on a separate partition than the Windows partition to support automatic failover and to support starting Windows BitLocker Drive Encryption–encrypted partitions. The same free drive space requirements as just outlined for a UEFI-based device apply to a BIOS-based device for the recovery tools partition. For BIOS/MBR-based systems, it is still possible to combine the WinRE tools partition with the system partition. It is also no longer necessary to create and maintain a separate full-system recovery image when deploying Windows 10 for desktop editions (Home, Professional, and Enterprise). Windows 10 can perform a refresh or reset by using the built-in Reset This PC feature.

Upgrade scenarios

Increasingly rapid release cycles have made it necessary to build a scalable approach to deploying Windows 10 and future releases. Through various acquisitions, Microsoft's own IT department gained additional insight into the challenges that Microsoft customers face when deploying a new OS into environments that use different applications and platforms. Through this knowledge, there have been significant improvements made to ensure that the upgrade experience to Windows 10 is simpler and less costly overall to all IT organizations as compared to previous OS versions. The following table depicts the traditional refresh process commonly used to deploy earlier OS versions, the much improved in-place upgrade method, and a new modern method of using provisioning packages and profiles.

Traditional For existing devices; using Configuration Manager and MDT	***Refresh*** Use if significant changes are needed, such as OS architecture change x86 versus x64. The traditional process is: • Capture data and settings • Deploy (custom) OS image • Inject drivers • Install apps • Restore data and settings
Improved For existing devices, using Configuration Manager and MDT	***Upgrade*** Recommended for existing devices (Windows 7, Windows 8, Windows 8.1) • Let Windows and Configuration Manager do the work • Preserve all data, settings, apps, and drivers

	• Install (standard) OS image • Restore everything

Modern
For new devices, using Configuration Manager, WICD, Intune, and Azure AD
	IT pro provisioning
	• Provisioning package
	  • Windows Image and Configuration Designer (WICD)
	  • Transform into an enterprise device
	• Provisioning profile with Configuration Manager
	User provisioning
	Azure AD Join with Intune auto-enrollment

In-place upgrade

Windows 10 formally offers in-place upgrade as a deployment scenario. Much can be learned by reviewing the case study available at https://www.microsoft.com/itshowcase/Article/Content/668 outlining how Microsoft IT deployed Windows 10 to 96,000 distributed users within a three-month period using primarily in-place upgrade methods. This document covers everything from early adoption processes; Internet Explorer, Microsoft Edge, and third-party application compatibility testing and issue mitigation; lessons learned; and many other aspects which should be considered prior to, during, and after each of the deployment phases. A list of additional helpful links is provided within the Resources section at the end of the case study document.

An in-place upgrade to Windows 10 upgrades an existing Windows 7 and higher OS while retaining the applications, settings, drivers, and user data that exist on the computer. The in-place upgrade is faster (30 to 60 minutes on average) and more resilient than traditional OS deployment methods. In the event of a failure during the in-place upgrade task sequence, the client is automatically rolled back to its original state so that the device is returned to an operational state for the end user. The in-place upgrade content that is downloaded to the client is much smaller because the currently installed applications do not need to be reinstalled as they would following a clean Windows 10 installation. The only exception is if an incompatible application needed to be uninstalled prior to the in-place upgrade. In this case, a Windows 10 compatible version of the application would need to be reinstalled after completion of the in-place upgrade, if it is still needed.

As outlined in Chapter 2, there are some situations in which an in-place upgrade is not possible or might not be practical. In these situations, you can use the wipe-and-load (refresh) deployment method, instead. Clients running Windows 7 through 8.1 that meet the minimum hardware requirements and have applications installed that do not have known compatibility issues with Windows 10 can be in-place upgraded to Windows 10. You can accomplish this by using Configuration Manager 2012 SP2 CU1 or R2 SP1 CU1 with the Windows 8.1 or Windows 10 ADK, or Configuration Manager (current branch) with the Windows 10 ADK.

For an in-place upgrade from a previous OS to Windows 10, the Windows 10 installation media that you import for deployment must be of the same architecture and language as the operating systems you will be upgrading. If your current Configuration Manager hierarchy version is Configuration Manager 2012 R2 SP1 or higher and you wish to begin testing in-place upgrades to existing clients, you can use the sample scripts available at http://blogs.technet.com/b/configmgrteam/archive/2014/10/29/how-to-upgrade-to-win-10-using-the-task-sequence-in-sc-2012-r2-configmgr.aspx. By importing the sample task sequence provided and populating the appropriate Windows 10 installation media, you will be able to quickly begin testing in-place upgrades to Windows 10 regardless of whether you are running the Windows 8.1 or Windows 10 ADK.

www.dbooks.org

Configuration Manager (current branch), which requires the Windows 10 ADK as a prerequisite, offers a new task sequence option, Upgrade An Existing Operating System From Upgrade Package, as shown in Figure 4-6. With this new task sequence type, you can deploy an Operating System Upgrade Package that has been imported into the Configuration Manager Administrator Console natively without using the aforementioned sample scripts, which were useful to deploy in-place upgrades using Configuration Manager 2012.

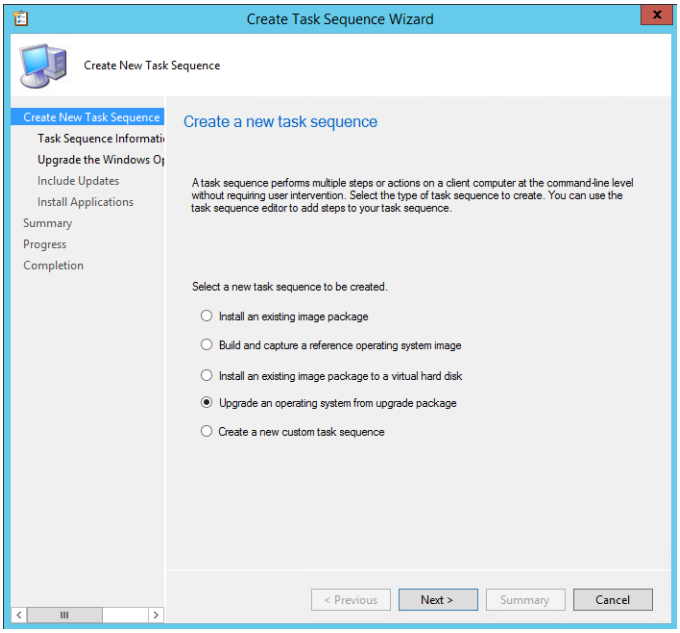


Figure 4-6: Create Task Sequence Wizard page

The Upgrade An Operating System From Upgrade Package task sequence option automatically creates the required steps to check the existing client for upgrade readiness. Here is what it does:

- Ensure that the client OS can be upgraded and meets minimum hardware and free drive space criteria
- Upgrade the OS
- Optionally install software updates

If any of the steps in the task sequence fail, the task sequence will automatically roll the client back to the previous OS. Figure 4-7 shows the steps that are automatically created during the Upgrade An Operating System From Upgrade Package task sequence.

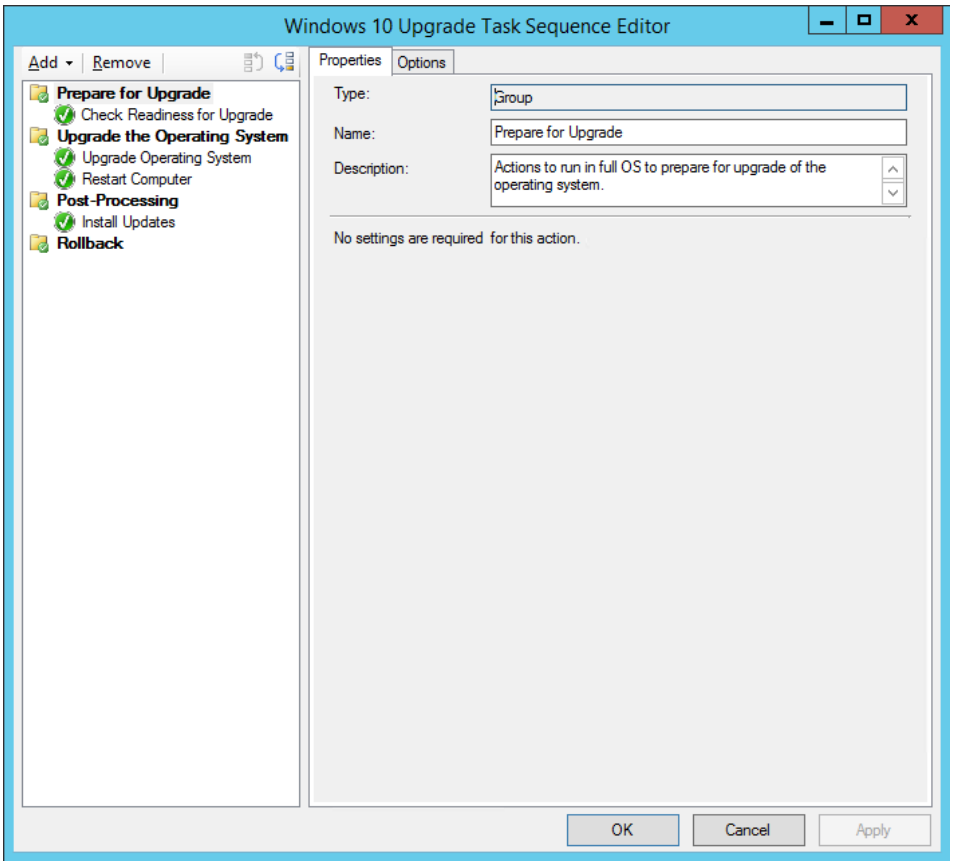


Figure 4-7: The Windows 10 Upgrade Task Sequence Editor

The Check Readiness For Upgrade step (see Figure 4-8) checks to ensure that the client meets the minimum processor and memory requirements and that it is currently running a Windows client OS as opposed to a Windows Server OS. Optionally, you can configure the readiness check to validate that there is a specific minimum amount of drive space available. Adjusting these settings in the task sequence step to lower than default values will prevent you from installing Windows 10 on unsupported hardware. For example, if you lower the Ensure Minimum Memory value to 1024 and try to install the 64-bit version of Windows 10 on a machine with only 1 GB of RAM, the setup process will fail due to the prerequisite checks, which are accomplished during the preparation phase of the Windows 10 installation.

www.dbooks.org

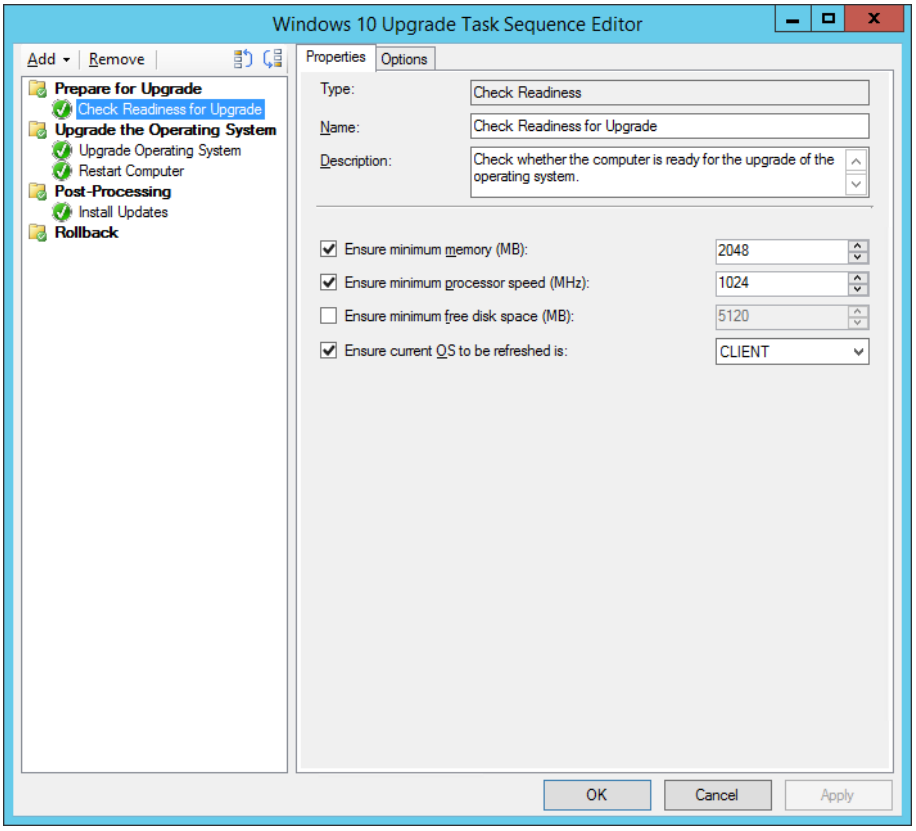


Figure 4-8: Check Readiness For Upgrade step in the Windows 10 Upgrade Task Sequence Editor

The Upgrade Operating System step (see Figure 4-9) shows the Upgrade package that was selected when creating the task sequence. Optionally, you can type a product key, if desired, as well as a time-out for the upgrade process. An option to perform a Windows Setup compatibility scan without actually starting the upgrade is also provided. This option will only validate whether the upgrade process would continue or stop due to any incompatible applications which are currently installed on the clients.

During an in-place upgrade, the existing operating system's \Windows directory is renamed to \Windows.OLD. This directory contains the files needed to roll back to the existing OS version in the event of a failure during the upgrade. The Windows.OLD directory is automatically removed after one month via the built-in Windows maintenance tasks. Alternatively, you can use the built-in Disk Cleanup tool to clean the directory, or use other custom scripts, as desired.

There are many command-line switches that you can use with the SETUP.EXE in the root of the Windows 10 installation media. These switches are automatically called depending on which check boxes are selected in the Upgrade Operating System task sequence step in Figure 4-9.

More info To learn more about the command-line switches that are available, go to https://msdn.microsoft.com/library/windows/hardware/dn938368(v=vs.85).aspx.

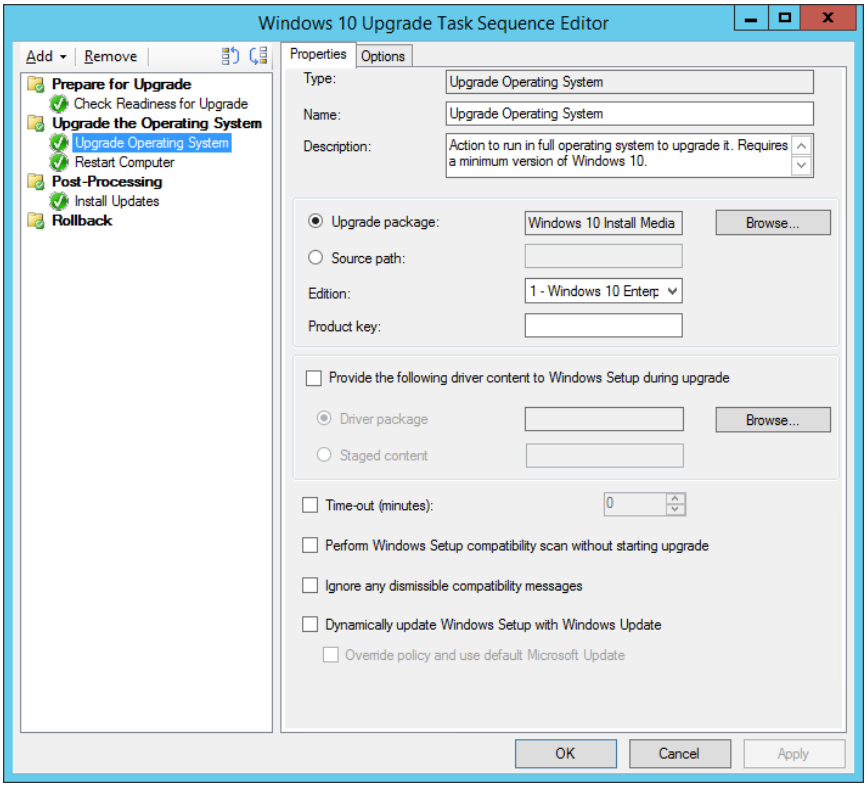


Figure 4-9: Upgrade Operating System step in the Upgrade an operating system from upgrade package task sequence

The most basic command line used to silently upgrade an existing OS to Windows 10 without automatically restarting at the end is SETUP.EXE /Auto Upgrade /Quiet /NoReboot. However, there are additional command-line switches that you can use during the planning and testing phase of the deployment to the rest of your enterprise. One example is /Compat ScanOnly, which is controlled by the Perform Windows Setup Compatibility Scan Without Starting Upgrade option. As its name implies, this option performs the Windows 10 installation compatibility checks without actually performing the upgrade.

The Dynamically Update Windows Setup With Windows Update option utilizes the /DynamicUpdate Disable command-line switch. This option is also recommended when utilizing the compatibility scan option in order to prevent the clients from also attempting to download the latest updates from Windows Update. The full command line to accomplish a compatibility scan when using a Configuration Manager package or task sequence that is called is SETUP.EXE /Auto Upgrade /Quiet /NoReboot /DynamicUpdate Disable /Compat ScanOnly.

You can add more task sequence steps as needed to facilitate removing any incompatible applications prior to the Windows 10 installation initiating, to reinstall compatible versions following the completion, or for any additional customizations that are desired.

Wipe-and-load (refresh)

The wipe-and-load scenario, commonly referred to as a *refresh*, might be desirable for scenarios in which the currently deployed operating systems are not well standardized. Lack of standardized devices can obviously cause an unpredictable, frustrating experience for end users, and is therefore also costly for an IT organization to support.

If there are currently 32-bit operating systems existing in the environment, you might want to consider taking advantage of the numerous improvements offered by running a 64-bit OS. This is

www.dbooks.org

another scenario that requires a refresh type deployment because it is not possible to change from one OS architecture to another during an in-place upgrade.

During the refresh deployment scenario, you must back up any user data and OS customizations that you need retain by using a tool such as USMT prior to wiping the PC. You can take advantage of the migration to Windows 10 as an opportunity to standardize and optimize the environment. Figure 4-10 depicts the refresh process at a high level.

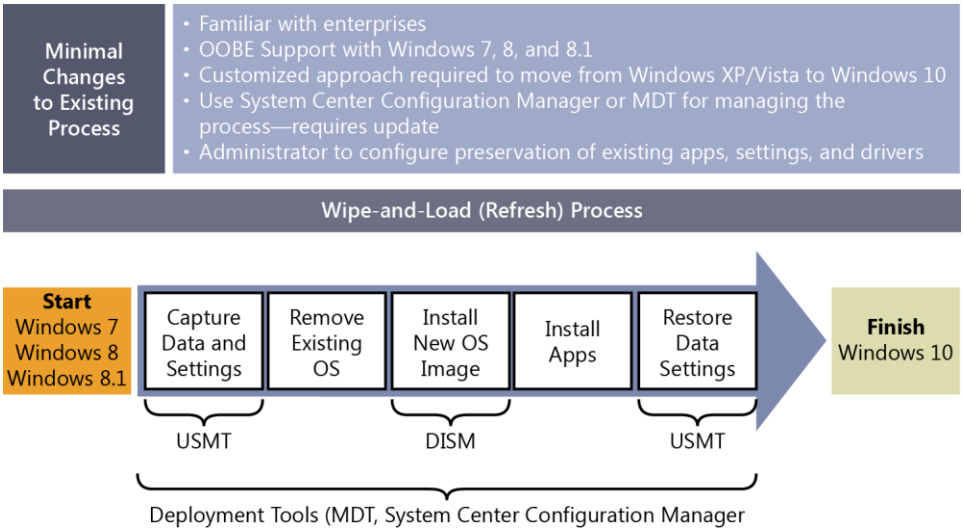


Figure 4-10: An overview of the wipe-and-load process

As mentioned previously, you must use Windows ADK 10, which includes the WinPE 10 version startup image, to deploy a fresh installation of Windows 10. The Windows 10 ADK and its included version of Windows 10 PE also support deploying Windows 7, 8, and 8.1 operating systems, as well. If you prefer to use the MDT Workbench to create your reference image, you can find a step-by-step walkthrough of this process at https://technet.microsoft.com/library/mt297533(v=vs.85).aspx. You can then import the reference image into the Operating System Images node in the Configuration Manager Administrator Console for deployment.

Dynamic provisioning

You can use *dynamic provisioning* to configure new devices that are already running a Windows 10 OS. With dynamic provisioning, you can accomplish tasks such as transforming a retail device into an enterprise device, removing unnecessary items, adding organizational applications, and applying enterprise-standard configurations. This is accomplished by using provisioning packages, or PPKG files, which you create by using the Windows ICD component of the Windows 10 ADK. You can utilize provisioning packages to turn on support for a Choose Your Own Device (CYOD) scenario, whereby the organization's users can use their own hardware. In a scenario such as this, it is typically desirable to standardize the device so that it conforms to enterprise specifications. Here are some examples of these customizations:

- Changing the Windows edition from Professional to Enterprise
- Configuring VPN and Wi-Fi profiles
- Enrolling devices into Microsoft Intune
- Installation of modern (APPX) applications
- Configuration of Windows settings to ensure compliance with organizational policies

The Windows ICD provides wizards for creating the provisioning packages in a PPKG file format. You create PPKG files by using the WIM format, so it is possible to apply or mount them using DISM or ImageX. PPKG files created by the Windows ICD ultimately contain the desired customizations for the OS. They can be applied to an existing OS during the OOBE phase, deployed at runtime via deployment of the PPKG file itself, or embedded into the image by using Configuration Manager OSD and MDT.

Optimizing the Windows 10 image deployment

With the release of System Center Configuration Manager (current branch), a new peer-to-peer caching feature has been introduced to improve the overall bandwidth consumption when deploying an OS to remote endpoints. Additionally, precaching content to clients can ensure an improved success rate during the Windows 10 deployment.

WinPE Peer Cache

A new capability in Configuration Manager (current branch) makes it possible to use WinPE Peer Cache during OS deployments. This feature is designed to greatly reduce WAN traffic when imaging client machines at remote locations which do not have a local DP. Figure 4-11 shows the process flow of a WinPE Peer Cache in a branch office. The first client to be imaged will download its content from a remote DP, whereas the second client being imaged will download its content from the first client.

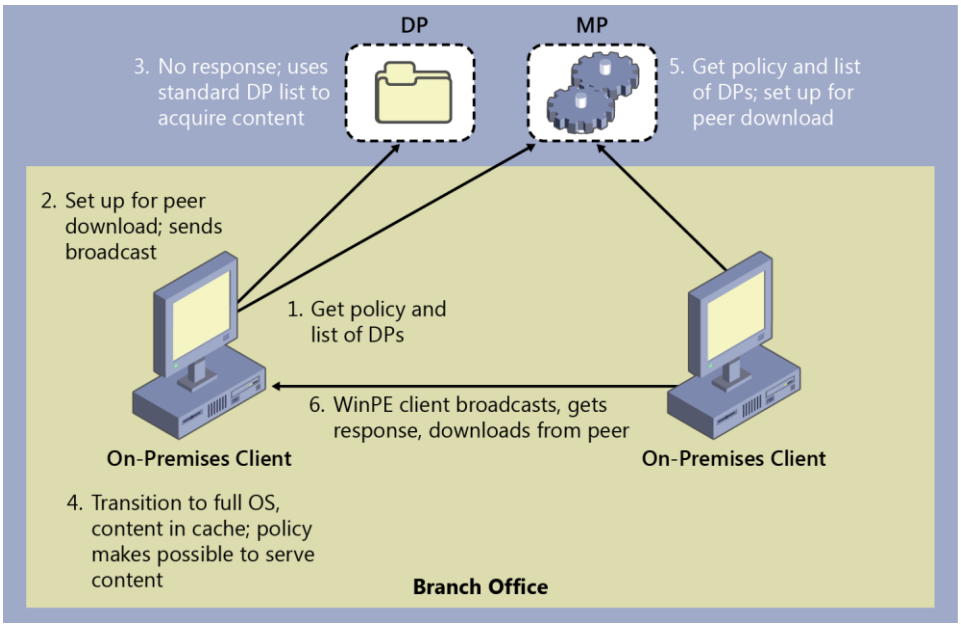


Figure 4-11: WinPE Peer Cache process flow while imaging two clients in a branch office

Here are the main characteristics of the feature:

- Designed to minimize the WAN traffic in branch office scenarios
- Similar to Windows BranchCache, but does not use this technology
- Uses Management Points (MP) to apply a policy to turn on WinPE peer cache
- A WinPE Peer Cache source client stores the task sequence content in its cache
- During WinPE task sequences, clients download the needed content from their peers instead of downloading it directly from DPs.

www.dbooks.org

When you turn on WinPE Peer Cache in Client Settings, the message shown in Figure 4-12 appears. By default, TCP port 8004 is used for the initial network broadcast during a peer cache handshake. TCP port 8003 is used during the content download process. This traffic is either HTTP or HTTPS, depending on whether PKI certificates are used to encrypt the peer communications between clients.

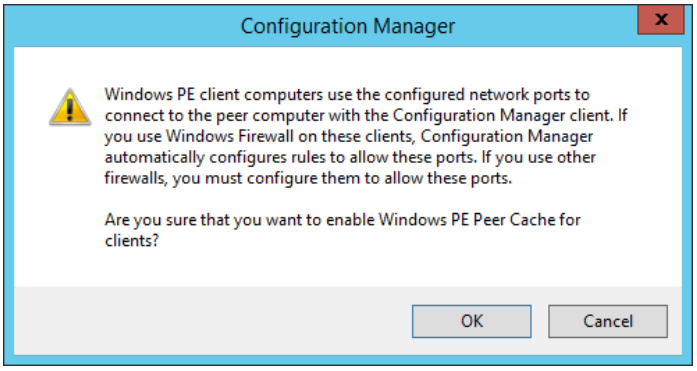


Figure 4-12: The message displays when you turn on WinPE Peer Cache

More info To learn more about how WinPE Peer Cache works, go to https://technet.microsoft.com/library/mt613173.aspx#BKMK_PeerCacheWork.

Monitoring the Windows 10 image deployment

As with any OS installation or upgrade, there are a variety of reasons that the upgrade or clean installation process might fail along the way. You can find a useful knowledge base article to assist with troubleshooting titled Troubleshooting Common Windows 10 Upgrade Errors and Issues at https://support.microsoft.com/kb/3107983.

During an in-place upgrade, the Windows 10 installation media is cached to the client's C:_SMSTaskSequence directory. As soon as the Windows 10 Setup.exe process begins on a client, a hidden directory is created on the client in $Windows.~BT\Sources\Panther. This directory is used to store various files created and referenced during the OS installation. A log file named SETUPACT.LOG is created in this directory and is helpful for troubleshooting and monitoring the end-to-end OS installation progress. Additionally, a SETUPERR.LOG is also created, which is used to store any errors that are generated, regardless of whether they are of significant enough impact to cause the installation to fail. If you are performing compatibility checks on a large number of machines, it can also be helpful to use the /CopyLogs <path> switch with Setup.exe, which copies the resulting compatibility check results log and XML files to a central file share for review.

You can use the error code reference provided in TechNet article KB3107983 to help determine a root cause in the event of an OS installation failure. For example, if you do not provide the minimum hardware required to install Windows 10, you will see an error 0xC1900200, as shown in Figure 4-13.

```
MOUPG  SetupManager: Found sysreq compat issues
MOUPG  CSetupManager::ExecuteInstallMode(662): Result = 0xC1900200
MOUPG  CSetupManager::ExecuteDownlevelMode(376): Result = 0xC190020
MOUPG  Setup phase change: [SetupPhasePrepare] -> [SetupPhaseError]
```

Figure 4-13: A sample error viewed in the SETUPACT.LOG caused by the computer not meeting the minimum requirements to install Windows 10

The hexadecimal value 0xC1900210 is generated in the SETUPACT.LOG if no issues were found that would prevent the installation of Windows 10 from proceeding. If the setup process continues past the preparation phase and experiences a fatal error, the client runs SETUPROLLBACK.CMD and stores the rollback related logs in $Windows.~BT\Sources\Rollback. After the drive configuration is

complete, the SETUPACT.LOG is moved to %Windir%\Panther and continues logging the progress during the rest of the in-place upgrade. At the end of the upgrade, SETUPCOMPLETE.CMD runs, and the previous operating system installation is placed in the Windows.OLD directory.

More info For additional Windows setup technical reference information, go to https://msdn.microsoft.com/library/windows/hardware/dn938377(v=vs.85).aspx.

After the Windows 10 image deployment

New Windows 10 upgrade releases will be made available approximately two to three times per year. Configuration Manager (current branch) provides the capabilities needed to keep clients up-to-date with this new faster release cycle. To deploy these servicing updates to Windows 10 clients, you must have Configuration Manager version 1511 or higher and a Software Update Point that is installed on Windows Server 2012 or higher that also has the Windows Server Update Services (WSUS) hotfix (available at https://support.microsoft.com/kb/3095113) installed. When these requirements are met, a new "Upgrades" software update classification is visible in the Software Update Point component properties of the topmost site in the hierarchy. With Configuration Manager version 1511 and higher, there is also a new Windows 10 servicing node in the Administrator Console which displays a dashboard depicting the current state of the Windows 10 deployment rings in the Configuration Manager managed environment. You can also preview the updates that are required and can be deployed based on the selected criteria by clicking the Preview button, as shown in Figure 4-14.

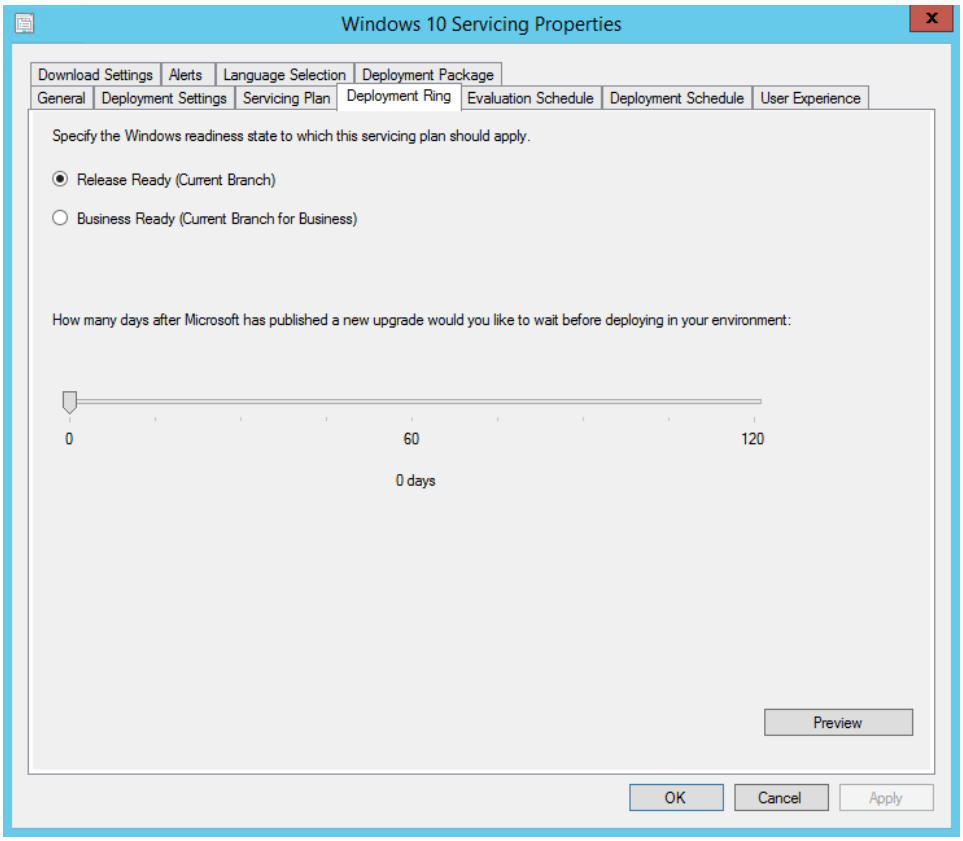


Figure 4-14: Deployment Ring configuration for servicing Windows 10 clients

More info For additional information on Windows 10 servicing for updates and upgrades, go to https://technet.microsoft.com/library/mt598226(v=vs.85).aspx.

www.dbooks.org

About the authors

This book merges contributions from several technology experts.

Lead



Andre Della Monica is a senior premier field engineer for Microsoft and has been working with System Center Configuration Manager since it was known as SMS. Before moving to his current position, he was recognized as a top support engineer on Consumer Technical Support for Microsoft Platform products. Andre attended college in São Paulo, Brazil, and earned his technology degree in computer network management. He resides in Houston, Texas, with his wife, Rose, his daughter, Sarah, and his son, Samuel. In his free time, he enjoys producing and recording music as well as being an Xbox gamer.

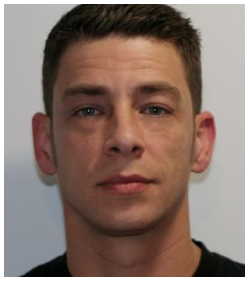
Authors



Alessandro Cesarini serves as premier field engineer at Microsoft and is based in Madrid. With more than 20 years' of IT experience in multinational environments (Spain, the United Kingdom, France, Austria, Hungary, Poland, and Italy) he is helping customers with migration and deployment of Windows using Windows Assessment and Deployment Kit (ADK), Microsoft Deployment Toolkit (MDT), and System Center Configuration Manager. When he is not working or traveling, Alessandro is riding his bicycle, cooking at home, playing Squash or Pádel, and spending time with his wife, Eva.



Russ Rimmerman is a senior premier field engineer for Microsoft supporting System Center Configuration Manager. He has been with Microsoft for more than five years. During his 13-year tenure working with Configuration Manager, he has engaged with customers owning moderately simple to ultra-complex Configuration Manager hierarchies across nearly every industry. Before joining Microsoft, Russ spent five years in the United States Air Force and also spent time as both a consultant and as a senior IT administrator. He coauthored the e-book *Microsoft System Center Software Update Management Field Experience* from Microsoft Press. Russ currently resides in Cypress, Texas, and enjoys anything involving water, anything related to or resembling technology, and, most important, spending time with his wife, Susan, and their one-year-old twin boys, Owyn and Jaxen.



Victor Silveira is a Microsoft System Center premier field engineer with a primary focus on Configuration Manager. Prior to his current role, he was a network analyst, managing various technologies and concentrating his skillset in the management space beginning with SMS 1.2/2.0. Later, he moved to a premier support engineer position with Microsoft and transitioned to team technical lead supporting SMS 2003/2007. Victor attended RCC Institute of Technology and earned his technology degree in computer network management. He is based in Toronto, Ontario, Canada, with his family and has an interest in photography, snowboarding, and DIY projects.

Contributing author

Herbert Fuchs is a premier field engineer based in Austria. He has more than 16 years' of experience in the IT-business in both the private and public sectors. He is best known as a troubleshooter and firefighter for the System Center Configuration Manager technology. For work/life balance, Herbert enjoys sports and playing PC games.

www.dbooks.org

Now that you've read the book...

Tell us what you think!

Was it useful?
Did it teach you what you wanted to learn?
Was there room for improvement?

Let us know at http://aka.ms/tellpress

Your feedback goes directly to the staff at Microsoft Press, and we read every one of your responses. Thanks in advance!





From technical overviews to drilldowns on special topics, get *free* ebooks from Microsoft Press at:

www.microsoftvirtualacademy.com/ebooks

Download your free ebooks in PDF, EPUB, and/or Mobi for Kindle formats.

Look for other great resources at Microsoft Virtual Academy, where you can learn new skills and help advance your career with free Microsoft training delivered by experts.

Microsoft Press

www.dbooks.org