Windows 10 deployment scenarios

**Applies to**

* Windows 10

To successfully deploy the Windows 10 operating system in your organization, it is important to understand the different ways that it can be deployed, especially now that there are new scenarios to consider. Choosing among these scenarios, and understanding the key capabilities and limitations of each, is a key task.

In-place upgrades

For existing computers running Windows 7, Windows 8, or Windows 8.1, the recommended path for organizations deploying Windows 10 leverages the Windows installation program (Setup.exe) to perform an in-place upgrade, which automatically preserves all data, settings, applications, and drivers from the existing operating system version. This requires the least IT effort, because there is no need for any complex deployment infrastructure.

Although consumer PCs will be upgraded using Windows Update, organizations want more control over the process. This is accomplished by leveraging tools like System Center Configuration Manager or the Microsoft Deployment Toolkit to completely automate the upgrade process through simple task sequences.

The in-place upgrade process is designed to be extremely reliable, with the ability to automatically roll back to the previous operating system if any issues are encountered during the deployment process, without any IT staff involvement. Rolling back manually can also be done by leveraging the automatically-created recovery information (stored in the Windows.old folder), in case any issues are encountered after the upgrade is finished. The upgrade process is also typically faster than traditional deployments, because applications do not need to be reinstalled as part of the process.

Because existing applications are preserved through the process, the upgrade process uses the standard Windows installation media image (Install.wim); custom images are not needed and cannot be used because the upgrade process is unable to deal with conflicts between apps in the old and new operating system. (For example, Contoso Timecard 1.0 in Windows 7 and Contoso Timecard 3.0 in the Windows 10 image.)

There are some situations where you cannot use in-place upgrade; in these situations, you can use traditional deployment (wipe-and-load) instead. Examples of these situations include:

* Changing from Windows 7, Windows 8, or Windows 8.1 x86 to Windows 10 x64. The upgrade process cannot change from a 32-bit operating system to a 64-bit operating system, because of possible complications with installed applications and drivers.
* Changing from legacy BIOS to UEFI booting. Some organizations deployed earlier versions of Windows on UEFI-enabled systems, leveraging the legacy BIOS capabilities of these systems. Because changing from legacy BIOS to UEFI requires changing the hardware configuration, disk configuration, and OS configuration, this is not possible using in-place upgrade.

**Note**  
Windows 10 does not require UEFI, so it would work fine to upgrade a system using legacy BIOS emulation. Some Windows 10 features, such as Secure Boot, would not be available after doing this.

* Windows To Go and Boot from VHD installations. The upgrade process is unable to upgrade these installations. Instead, new installations would need to be performed.
* Devices that use third-party disk encryption software. While devices encrypted with BitLocker can easily be upgraded, more work is necessary for third-party disk encryption tools. Some ISVs will provide instructions on how to integrate their software into the in-place upgrade process (check with your ISV to see if they have instructions), but if not available a traditional deployment would be needed.
* Updating existing images. While it might be tempting to try to upgrade existing Windows 7, Windows 8, or Windows 8.1 images to Windows 10 by installing the old image, upgrading it, and then recapturing the new Windows 10 image, this is not supported – preparing an upgraded OS for imaging (using Sysprep.exe) is not supported and will not work when it detects the upgraded OS.
* Dual-boot and multi-boot systems. The upgrade process is designed for devices running a single OS; if using dual-boot or multi-boot systems with multiple operating systems (not leveraging virtual machines for the second and subsequent operating systems), additional care should be taken.

Dynamic provisioning

For new PCs, organizations have historically replaced the version of Windows included on the device with their own custom Windows image, because this was often faster and easier than leveraging the preinstalled version. But this is an added expense due to the time and effort required. With the new dynamic provisioning capabilities and tools provided with Windows 10, it is now possible to avoid this.

The goal of dynamic provisioning is to take a new PC out of the box, turn it on, and transform it into a productive organization device, with minimal time and effort. The types of transformations that are available include:

* Changing the Windows edition with a single reboot. For organizations that have Software Assurance for Windows, it is easy to change a device from Windows 10 Pro to Windows 10 Enterprise, just by specifying an appropriate product or setup key. When the device restarts, all of the Windows 10 Enterprise features will be enabled.
* Configuring the device with VPN and Wi-Fi connections that may be needed to gain access to organization resources.
* Installation of additional apps needed for organization functions.
* Configuration of common Windows settings to ensure compliance with organization policies.
* Enrollment of the device in a mobile device management (MDM) solution, such as Microsoft Intune.

There are two primary dynamic provisioning scenarios:

* **Azure Active Directory (Azure AD) Join with automatic mobile device management (MDM) enrollment.** In this scenario, the organization member just needs to provide their work or school user ID and password; the device can then be automatically joined to Azure Active Directory and enrolled in a mobile device management (MDM) solution with no additional user interaction. Once done, the MDM solution can finish configuring the device as needed.
* **Provisioning package configuration.** Using the [Windows Imaging and Configuration Designer (ICD)](https://go.microsoft.com/fwlink/p/?LinkId=619358), IT administrators can create a self-contained package that contains all of the configuration, settings, and apps that need to be applied to a machine. These packages can then be deployed to new PCs through a variety of means, typically by IT professionals. For more information, see [Configure devices without MDM](https://docs.microsoft.com/en-us/windows/configuration/configure-devices-without-mdm).

Either way, these scenarios can be used to enable “choose your own device” (CYOD) programs where the organization’s users can pick their own PC and not be restricted to a small list of approved or certified models (programs that are difficult to implement using traditional deployment scenarios).

While the initial Windows 10 release includes a variety of provisioning settings and deployment mechanisms, these will continue to be enhanced and extended based on feedback from organizations. As with all Windows features, organizations can submit suggestions for additional features through the Windows Feedback app or through their Microsoft Support contacts.

Traditional deployment

New versions of Windows have typically been deployed by organizations using an image-based process built on top of tools provided in the [Windows Assessment and Deployment Kit](https://docs.microsoft.com/en-us/windows/deployment/windows-adk-scenarios-for-it-pros), Windows Deployment Services, the [Deploy Windows 10 with the Microsoft Deployment Toolkit](https://docs.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/deploy-windows-10-with-the-microsoft-deployment-toolkit), and [System Center Configuration Manager](https://docs.microsoft.com/en-us/windows/deployment/deploy-windows-sccm/deploy-windows-10-with-system-center-2012-r2-configuration-manager).

With the release of Windows 10, all of these tools are being updated to fully support Windows 10. Although newer scenarios such as in-place upgrade and dynamic provisioning may reduce the need for traditional deployment capabilities in some organizations, these traditional methods remain important and will continue to be available to organizations that need them.

The traditional deployment scenario can be divided into different sub-scenarios. These are explained in detail in the following sections, but the following provides a brief summary:

* **New computer.** A bare-metal deployment of a new machine.
* **Computer refresh.** A reinstall of the same machine (with user-state migration and an optional full Windows Imaging (WIM) image backup).
* **Computer replace.** A replacement of the old machine with a new machine (with user-state migration and an optional full WIM image backup).

New computer

This scenario occurs when you have a blank machine you need to deploy, or an existing machine you want to wipe and redeploy without needing to preserve any existing data. The setup starts from a boot media, using CD, USB, ISO, or Pre-Boot Execution Environment (PXE). You can also generate a full offline media that includes all the files needed for a client deployment, allowing you to deploy without having to connect to a central deployment share. The target can be a physical computer, a virtual machine, or a Virtual Hard Disk (VHD) running on a physical computer (boot from VHD).

The deployment process for the new machine scenario is as follows:

1. Start the setup from boot media (CD, USB, ISO, or PXE).
2. Wipe the hard disk clean and create new volume(s).
3. Install the operating system image.
4. Install other applications (as part of the task sequence).

After taking these steps, the computer is ready for use.

Computer refresh

A refresh is sometimes called wipe-and-load. The process is normally initiated in the running operating system. User data and settings are backed up and restored later as part of the deployment process. The target can be the same as for the new computer scenario.

The deployment process for the wipe-and-load scenario is as follows:

1. Start the setup on a running operating system.
2. Save the user state locally.
3. Wipe the hard disk clean (except for the folder containing the backup).
4. Install the operating system image.
5. Install other applications.
6. Restore the user state.

After taking these steps, the machine is ready for use.

Computer replace

A computer replace is similar to the refresh scenario. However, since we are replacing the machine, we divide this scenario into two main tasks: backup of the old client and bare-metal deployment of the new client. As with the refresh scenario, user data and settings are backed up and restored.

The deployment process for the replace scenario is as follows:

1. Save the user state (data and settings) on the server through a backup job on the running operating system.
2. Deploy the new computer as a bare-metal deployment.

**Note**  
In some situations, you can use the replace scenario even if the target is the same machine. For example, you can use replace if you want to modify the disk layout from the master boot record (MBR) to the GUID partition table (GPT), which will allow you to take advantage of the Unified Extensible Firmware Interface (UEFI) functionality. You can also use replace if the disk needs to be repartitioned since user data needs to be transferred off the disk.