OVERVIEW OF DEPLOYING WINDOWS – 10

The following list summarize various Windows 10 deployment scenarios. The scenarios are each assigned to one of three categories.

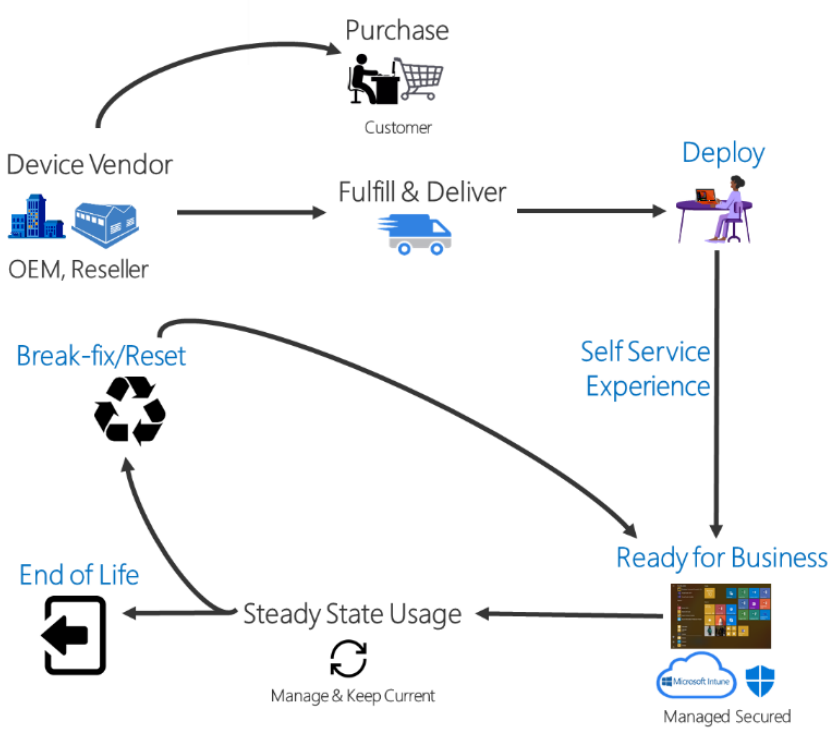
- ***Modern deployment methods*** are recommended unless you have a specific need to use a different procedure. These methods are supported with existing tools such as Microsoft Deployment Toolkit (MDT) and Microsoft Endpoint Configuration Manager.
- ***Dynamic deployment methods*** enable you to configure applications and settings for specific use cases.
- ***Traditional deployment methods*** use existing tools to deploy operating system images.

Modern deployment methods

Modern deployment methods embrace both traditional and cloud services to deliver a simple, streamlined, cost effective deployment experience.

- **Windows Autopilot**

Windows Autopilot is a new suite of capabilities designed to simplify and modernize the deployment and management of new Windows 10 PCs. Windows Autopilot enables IT professionals to customize the Out of Box Experience (OOBE) for Windows 10 PCs and provide end users with a fully configured new Windows 10 device after just a few clicks. There are no images to deploy, no drivers to inject, and no infrastructure to manage. Users can go through the deployment process independently, without the need consult their IT administrator.



- **In-place upgrade**

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.

Dynamic provisioning

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:

- **Windows 10 Subscription Activation**

Windows 10 Subscription Activation is a modern deployment method that enables you to change the SKU from Pro to Enterprise with no keys and no reboots.

- **Azure Active Directory (AAD) join with automatic mobile device management (MDM) enrolment**

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), 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. 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.

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, Windows Deployment Services, the Deploy Windows 10 with the Microsoft Deployment Toolkit, and Microsoft Endpoint Configuration Manager.

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).

1. **New computer**

Also called a "bare metal" deployment. 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 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).

2. **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 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.

3. **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.

Ref: https://docs.microsoft.com/en-us/windows/deployment/windows-10-deployment-scenarios

==========

CONFIGURING DEVICES AND DRIVERS

- **Add a device to a Windows 10 PC**

Windows 10 usually finds devices automatically when you plug them in or turn them on. If it doesn't, follow these steps:

1. Select **Start** > **Settings** > **Devices** > **Bluetooth & other devices**.
2. Select **Add Bluetooth or other device** and follow the instructions.

- **Install a printer in Windows 10**

When you connect a printer to your PC or add a new printer to your home network, you can usually start printing right away. Windows 10 supports most printers, so you probably won't have to install special printer software.

➢ ***To install or add a network, wireless, or Bluetooth printer***

If your printer is on and connected to the network, Windows should find it easily. Available printers can include all printers on a network, such as Bluetooth and wireless printers or printers that are plugged into another computer and shared on the network. You might need permission to install some printers.

1. Select the **Start** button, then select **Settings** > **Devices** > **Printers & scanners**.

2. Select **Add a printer or scanner**. Wait for it to find nearby printers, then choose the one you want to use, and select **Add device**.

   If your printer isn't in the list, select **The printer that I want isn't listed**, and then follow the instructions to add it manually using one of the options.

➢ **How to install the latest driver for your printer**

Here are several ways to update your printer driver.

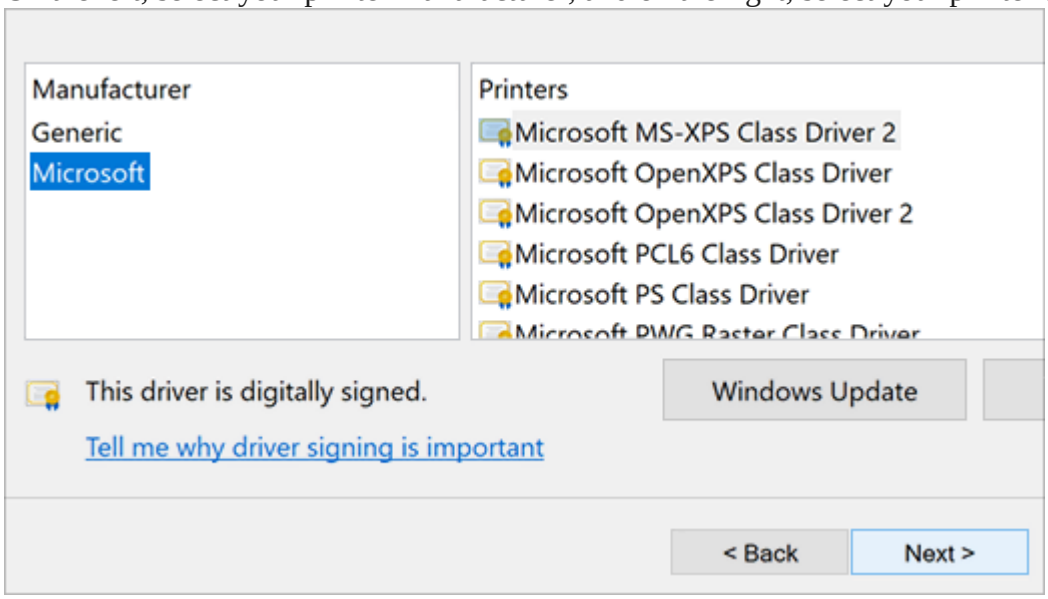
1. Use Windows Update
2. Install software that came with your printer
3. Download and install the driver from the printer manufacturer's website

➢ **What to do if the driver doesn't install**

If you double-click the installation file and nothing happens, follow these steps:

1. Select **Start** , then select **Settings** > **Devices** > **Printers & scanners** .
2. On the right, scroll down to **Related Settings** and select **Print server properties**.
3. Select the **Drivers** tab, and see if your printer listed. If it is, you're all set.
4. If you don't see your printer listed, select **Add**, and in the **Welcome to the Add Printer Driver Wizard**, select **Next**.
5. Select your device's architecture, and then select **Next**.

6. On the left, select your printer manufacturer, and on the right, select your printer driver.



7. Select **Next**, select **Finish**, and follow the instructions to add your driver.
8. Follow the instructions in the section above to remove and reinstall the printer.

- **Update the device driver**

1. In the search box on the taskbar, enter **device manager**, then select **Device Manager**.
2. Select a category to see names of devices, then right-click (or press and hold) the one you'd like to update.
3. Select **Search automatically for updated driver software**.
4. Select **Update Driver**.
5. If Windows doesn't find a new driver, you can try looking for one on the device manufacturer's website and follow their instructions.

- **Reinstall the device driver**

1. In the search box on the taskbar, enter **device manager**, then select **Device Manager**.
2. Right-click (or press and hold) the name of the device, and select **Uninstall**.
3. Restart your PC.
4. Windows will attempt to reinstall the driver.

- **Install or add a network, wireless, or Bluetooth scanner**

If your scanner is turned on and connected to the network, Windows should find it automatically. Available scanners can include all scanners on a network, such as Bluetooth and wireless scanners or scanners that are plugged into another device and shared on the network. Here's a way to do it manually.

1. Select **Start** > **Settings** > **Devices** > **Printers & scanners** or use the following button.

2. Select **Add a printer or scanner**. Wait for it to find nearby scanners, then choose the one you want to use, and select **Add device**.

If your scanner isn't in the list, select **The printer that I want isn't listed**, and then follow the instructions to add it manually

Ref:

1. Add a device to a Windows 10 PC: https://support.microsoft.com/en-gb/windows/add-a-device-to-a-windows-10-pc-ae095699-4d4f-40da-8702-e9662a855364
2. Install a printer in Windows 10: https://support.microsoft.com/en-gb/windows/install-a-printer-in-windows-10-cc0724cf-793e-3542-d1ff-727e4978638b
3. How to install the latest driver for your printer: https://support.microsoft.com/en-gb/windows/how-to-install-the-latest-driver-for-your-printer-4ff66446-a2ab-b77f-46f4-a6d3fe4bf661#ID0EBD=Windows_10
4. Update drivers in Windows 10: https://support.microsoft.com/en-gb/windows/update-drivers-in-windows-10-ec62f46c-ff14-c91d-eead-d7126dc1f7b6
5. Install and use a scanner in Windows 10: https://support.microsoft.com/en-gb/windows/install-and-use-a-scanner-in-windows-10-4fd9f33a-25b6-159a-3cde-3f009b02a81a

==========

MANAGING APPS IN WINDOWS

➢ App types

There are two classes of apps:

- **Provisioned**: Installed in user account the first time you sign in with a new user account.
- **Installed**: Installed as part of the OS.

There are different types of apps that can run on your Windows client devices. Following are some of the common apps used on Windows devices.

- **Microsoft 365 apps**: These apps are used for business and productivity, and include Outlook, Word, Teams, OneNote, and more. Depending on the licenses your organization has, you may already have these apps. Using an MDM provider, these apps can also be deployed to mobile devices, including smartphones.
- **Power Apps**: These apps connect to business data available online and on-premises, and can run in a web browser, and on mobile devices. They can be created by business analysts and professional developers.
- **.NET apps**: These apps can be desktop apps that run on the device, or web apps. Some common .NET apps include:
  - **Windows Presentation Foundation (WPF)**: Using .NET, you can create a WPF desktop app that runs on the device, or create a WPF web app. This app is commonly used by organizations that create line of business (LOB) desktop apps.
  - **Windows Forms (WinForm)**: Using .NET, you can create a Windows Forms desktop app that runs on the device, and doesn't require a web browser or internet access. Just like Win32 apps, WinForm apps can access the local hardware and file system of the computer where the app is running.

- **Universal Windows Platform (UWP) apps**: These apps run and can be installed on many Windows platforms, including tablets, Microsoft HoloLens, Xbox, and more. All UWP apps are Windows apps. Not all Windows apps are UWP apps.

- **Win32 apps**: These apps are traditional Windows apps that run on the device, and are often called desktop apps. They require direct access to Windows and the device hardware, and typically don't require a web browser. These apps run in 32-bit mode on 64-bit devices, and don't depend on a managed runtime environment, like .NET.

- **System apps**: Apps installed in the C:\Windows\ directory. These apps are part of the Windows OS.

- **Web apps** and **Progressive web apps (PWA)**: These apps run on a server, and don't run on the end user device. To use these apps, users must use a web browser and have internet access. **Progressive web apps** are designed to work for all users, work with any browser, and work on any platform.

  Web apps are typically created in Visual Studio, and can be created with different languages.

➢ **Android™ apps**

Starting with Windows 11, users in the Windows Insider program can use the Microsoft Store to search, download, and install Android™ apps. This feature uses the Windows Subsystem for Android, and allows users to interact with Android apps, just like others apps installed from the Microsoft Store.

➢ **Add or deploy apps to devices**

When your apps are ready, you can add or deploy these apps to your Windows devices. This section lists some common options.

- **Manually install**: On your devices, users can install apps from the Microsoft Store, from the internet, and from an organization shared drive. These apps, and more, are listed in **Settings** > **Apps** > **Apps and Features**.

- **Mobile device management (MDM)**: Use an MDM provider, like Microsoft Intune (cloud) or Configuration Manager (on-premises), to deploy apps. For example, you can create app policies that deploy Microsoft 365 apps, deploy Win32 apps, create shortcuts to web apps, add Store apps, and more.

- **Microsoft Store**: Using the Microsoft Store app, Windows users can download apps from the public store. And, they can download apps provided by your organization, which is called the "private store". If your organization creates its own apps, you can use **Windows Package Manager** to add apps to the private store.

  To help manage the Microsoft Store on your devices, you can use policies:

- On premises, you can use Administrative Templates in Group Policy to control access to the Microsoft Store app:
  - User Configuration\Administrative Templates\Windows Components\Store
  - Computer Configuration\Administrative Templates\Windows Components\Store
- Using Microsoft Intune, you can use Administrative Templates (opens another Microsoft web site) or the Settings Catalog (opens another Microsoft web site) to control access to the Microsoft Store app.

Ref: https://docs.microsoft.com/en-us/windows/application-management/apps-in-windows-10

==========

MONITORING WINDOWS SYSTEMS

Process Explorer is an advanced monitoring tool for Windows that shows real-time file system, Registry and process/thread activity. It combines the features of two legacy Sysinternals utilities, *Filemon* and *Regmon*, and adds an extensive list of enhancements including rich and non-destructive filtering, comprehensive event properties such as session IDs and user names, reliable process information, full thread stacks with integrated symbol support for each operation, simultaneous logging to a file, and much more. Its uniquely powerful features will make Process Monitor a core utility in your system troubleshooting and malware hunting toolkit.

Process Monitor includes powerful monitoring and filtering capabilities, including:

- More data captured for operation input and output parameters
- Non-destructive filters allow you to set filters without losing data
- Capture of thread stacks for each operation make it possible in many cases to identify the root cause of an operation
- Reliable capture of process details, including image path, command line, user and session ID
- Configurable and moveable columns for any event property
- Filters can be set for any data field, including fields not configured as columns
- Advanced logging architecture scales to tens of millions of captured events and gigabytes of log data
- Process tree tool shows relationship of all processes referenced in a trace
- Native log format preserves all data for loading in a different Process Monitor instance
- Process tooltip for easy viewing of process image information
- Detail tooltip allows convenient access to formatted data that doesn't fit in the column
- Cancellable search
- Boot time logging of all operations

NOTE: Write process explorer steps from lab record.

==========

(1)

POST-INSTALLATION CONFIGURATION TASKS

Post-installation configuration refers to the **set of activities performed after installing an operating system, software, or hardware** to ensure that it is secure, functional, optimized, and ready for use. These tasks are essential for **system stability, performance, security, and usability.**

---

1. Applying System Updates and Patches

After installation, the system may be outdated.
Why it's important:

- Fixes security vulnerabilities.
- Improves performance and stability.
- Ensures compatibility with new hardware/software.

Tasks include:

- Checking for OS updates via Windows Update, apt/yum in Linux.
- Installing security patches.
- Updating drivers and firmware.
- Restarting the system if required.

---

2. Configuring Network Settings

Network configuration ensures communication between systems.

Key tasks:

- Assigning a **static IP address** (servers) or enabling DHCP (clients).
- Configuring **subnet mask, default gateway, DNS servers.**
- Setting a **hostname** to identify the device.
- Testing connectivity using ping or traceroute.
- Verifying internet access.

Why it matters:

- Proper network setup allows devices to communicate securely and reliably.

---

3. Creating and Managing User Accounts

Systems should not operate with default admin accounts.

Tasks include:

- Creating local or domain user accounts.
- Assigning appropriate permissions and group memberships.
- Setting password complexity and expiration policies.

- Disabling/renaming default admin or root accounts (for security).

Importance:

- Protects system from unauthorized access.
- Enforces least privilege principle.

---

4. Configuring Security Settings

Security hardening ensures the system is protected against threats.

Tasks include:

- Enabling and configuring the firewall (e.g., Windows Firewall, ufw in Linux).
- Installing antivirus/endpoint protection.
- Disabling unused services, ports, and startup programs.
- Setting up encryption for drives (e.g., BitLocker, LUKS).
- Configuring SSH keys and disabling remote root login (Linux).
- Setting auditing and logging policies.

Importance:

- Reduces attack surface and prevents unauthorized access.

---

5. Setting Up Storage and File System

After installation, storage may need to be configured.

Tasks include:

- Creating and formatting partitions.
- Mounting file systems.
- Configuring RAID or Logical Volume Manager (LVM).
- Setting permissions for folders and files.
- Creating shared folders (Windows or Samba).
- Organizing directory structure.

Importance:

- Ensures efficient data management and system performance.

---

6. Installing Essential Drivers and Software

Some devices require additional drivers after OS installation.

Tasks include:

- Installing chipset, network, graphics, and audio drivers.
- Adding management tools such as monitoring or backup software.
- Installing productivity or required application software.

Importance:

- Ensures full hardware functionality and system usability.

---

7. Configuring System Services

Many systems require certain services to be enabled or disabled.

Tasks include:

- Enabling automatic service startup (e.g., web server, database).
- Disabling unwanted/unnecessary services.
- Checking service dependencies.
- Adjusting service permissions.

Importance:

- Ensures critical services run correctly while reducing resource waste.

---

8. Performance Optimization

Optimization improves speed and efficiency.

Tasks include:

- Configuring virtual memory/page file.
- Tuning CPU scheduling/priority.
- Adjusting system power settings.
- Enabling caching mechanisms.

Importance:

- Provides better system responsiveness and stability.

---

9. Configuring Backup and Recovery

Backups protect data in case of system failure.

Tasks include:

- Setting up automated backups (daily, weekly).
- Selecting backup destinations (external drive, cloud, NAS).
- Verifying backup integrity.

- Enabling system restore points (Windows) or snapshots (Linux, VM).

Importance:

- Ensures data recovery during disasters or accidental deletions.

---

10. Logging and Monitoring Configuration

Monitoring helps administrators detect issues early.

Tasks include:

- Configuring Event Viewer (Windows) or syslog/journald (Linux).
- Setting up alerts for CPU, disk, memory usage.
- Enabling audit logs.
- Integrating logs with central logging systems (SIEM).

Importance:

- Helps in troubleshooting and detecting security incidents.

---

11. Testing and Validation

After completing configuration, the system must be tested.

Tasks include:

- Testing network connectivity.
- Verifying user access and permissions.
- Checking service functionality (web server, database, file sharing).
- Ensuring updates were applied successfully.

Importance:

- Confirms that the system is ready for operational use.