**Module 10 – Troubleshooting Windows 11**

**Module Overview**

Problems with BitLocker, corruptions in the startup environment, and device driver issues can all cause Windows 11 to fail to startup correctly. It’s therefore important that you can identify the cause of these problems, and select the appropriate tool to recover Windows. In this module, you’ll learn about Windows 11 startup, the registry, device and device drivers, and how to recover files.

**Objectives**

After completing this module, you will be able to:

* Describe Windows 11 recovery tools and options
* Troubleshoot Windows 11 startup
* Configure the Windows 11 registry
* Troubleshoot devices and device drivers
* Recover files

Lesson 1

**Recovering Windows 11**

Although Windows 11 is very reliable, from time-to-time, you’ll find a computer that either won’t start, or else starts with errors. In these situations, it’s helpful to know what recovery options are available.

**Lesson Objectives**

After completing this lesson, you will be able to:

* Describe the available recovery tools.
* Use System Restore to rollback Windows.
* Use the System Configuration tool.

**Exploring recovery tools in Windows 11**

The Windows Recovery Environment (Windows RE) is provided on its own partition on the primary disk in your computer. When necessary, you can start your computer from this partition and boot into Windows RE.

It’s worth knowing that you can also launch Windows RE from System/Recovery in the **Settings** app, or by starting a computer from the Windows product DVD and choosing **Repair your computer**.

There are six tools in Windows RE, but if you launch Windows RE from Settings, two initial options display:

* **Reset this PC**. Enables you to reset your computer to its out-of-box-experience (OOBE) state, perhaps so that you can sell the computer, or pass it on to a family member.
* **Advanced startup**. Enables you to access the Windows RE recovery tools. After restarting, click **Troubleshoot** on the **Choose an option** screen.

If you’ve recently upgraded the computer from Windows 10, you might also have a third option:

* **Go back**. Allows you to roll back to an earlier version of Windows following an upgrade.

After starting into Windows RE, and selecting the Troubleshoot option, you’ll have two options:

* Reset this PC.
* Advanced options.

**Reset this PC**

When you select this option, Windows 11 reinstalls. However, before you start, you must choose from the following two options:

* **Keep my files**. Removes all settings and all apps that aren’t part of Windows by default. But your personal files are retained. The process also retains system settings, such as computer name and AD DS domain membership. Choose this option if you just want to start over, but retain the use of the device.
* **Remove everything**. Presents two options for removal:
* **Just remove my files**. Resets to factory defaults, but makes no effort to clean the drive.
* **Fully clean the drive**. Securely wipes the drive. This option is best for when you intend to sell or give away the device.

If you have multiple disks attached, you’ll need to specify whether they should also be cleaned.

Whether you choose **Keep my files** or **Fully clean the drive**, Reset this PC prompts you to choose whether to reinstall Windows from a cloud or local installation source:

* **Cloud download**. Downloads Windows 11 from the internet. Typically, the download size is around 4 GB.
* **Local reinstall**. Reinstalls Windows from local installation files in the recovery partition.

If you use disk imaging to deploy Windows, the quickest way to reset a computer is to reimage it.

**Advanced options**

When you select this option, you’re presented with a list of recovery tools. The available tools can vary depending on how you launch Windows RE. Typically, the available tools are:

* Startup Repair
* Startup Settings
* Command Prompt
* Uninstall Updates
* UEFI Firmware Settings
* System Restore
* System Image Recovery

**Startup Repair**

Windows startup is pretty reliable. However, in the past, when troubleshooting Windows startup, you’d have to thoroughly understand the startup environment. You’d also need good understanding of command-line tools for managing startup settings.

However, the Startup Repair tool in Windows RE provides a quick and easy way to verify and, where needed, resolve most common startup problems. When you click **Startup** **Repair**, Windows RE performs the following checks, fixing things as needed:

* **Verify disk metadata**. The metadata includes the boot sector and the GPT. Startup Repair verifies their integrity and, if required, repairs the metadata.
* **Verify boot configuration settings**. Windows 11 uses a configuration database to locate bootable operating systems on the local hard disk. Startup Repair verifies the integrity of the entries in this database and, where needed, creates the required entries by scanning the attached disks looking for operating system instances.
* **Resolve driver issues**. Startup Repair checks the integrity of any recently installed device drivers and, if they’re causing startup problems, it uses System Restore points to recover Windows.

Although you can perform these tasks manually, it makes sense to use the automated Startup Repair tool in the first instance.

**Startup Settings**

In earlier versions of Windows, you could press the F8 key during startup and direct the computer to startup in a special, or advanced, mode. Windows 11 provides that same capability via the Startup Settings option. The following advanced startup options are available:

* **Enable debugging**. Enables you to examine the behavior of the Windows operating system’s device drivers.
* **Enable boot logging**. Creates the Ntbtlog.txt file, which you can use for advanced troubleshooting. Ntbtlog.txt lists all drivers accessed during startup.
* **Enable low-resolution video**. Starts Windows with low resolution and refresh rate settings.
* **Enable Safe Mode**. Starts Windows with a minimal set of drivers and services. Enables get Windows running, although somewhat restricted, and allow you to perform diagnostics and fix problems preventing startup.
* **Enable Safe Mode with Networking**. Starts Windows in safe mode and provides network connectivity.
* **Enable Safe Mode with Command Prompt**. Starts Windows in safe mode with a Command Prompt only.
* **Disable driver signature enforcement**. Enables you to bypass the requirement for signed drivers.
* **Disable early launch anti-malware protection**. Prevents low-level anti-malware protection from running.
* **Disable automatic restart after failure**. Prevents the Windows operating system from restarting automatically if an error causes the operating system to fail.
* **Launch recovery environment**. Starts the computer into Windows RE.

**Command Prompt**

The Command Prompt was the of the earliest Windows recovery tools, first appearing in Windows XP. In reality, it provides little benefit in Windows 11. This is largely because Windows 11 provides numerous automatic recovery tools. However, it can still be useful to access the Command Prompt in some nuanced recovery scenarios. Using Command Prompt, you can:

* Resolve device driver problems, for example, by using sc.exe
* Manually fix the startup environment and settings (the metadata and BCD)
* Reconfigure your attached disks and their partitions and volumes by using Diskpart.exe
* Launch troubleshooting tools, such as Regedit.exe

Although the Command Prompt is designed to support command-line input and executables, you can also use it to launch some graphical tools, such as the registry editor.

**Uninstall Updates**

If you’ve recently installed updates, especially a feature update, and decide to remove it, you can use the **Uninstall Updates** option.

**UEFI Firmware Settings**

Most modern computers are installed with UEFI-based firmware. You can use this option to access the firmware settings for your computer without needing to use a vendor supplied combination of keystrokes. A number of Windows specific settings are configurable via the firmware, such as Secure Boot, in addition to more generic settings, such a WiFi and virtualization settings.

**System Restore**

Of all the available tools, this is perhaps the most useful. After you enable System Restore, Windows captures restore points periodically, and automatically prior to system configuration changes. You can use these restore points to roll your computer’s configuration back to the point-in-time that the snapshot was taken.

You can access System Restore, and apply an earlier restore point, from within Windows 11 when it’s running normally or when you’ve managed to start the computer in Safe Mode. However, having the ability to access System Restore from the recovery tools means you can roll back the configuration of a computer that you can’t start normally.

**System Image Recovery**

You can use the built-in Backup and Restore (Windows 7) tool to create a system image of your computer. Once you have a system image, perhaps stored on external storage, you can use it to overwrite the existing hard disk, replacing a failed or non-functioning Windows configuration with a known working configuration from an earlier time. In reality, for a workplace environment, there are significantly better tools and procedures available to perform this type of recovery.

**Using System Restore**

Let’s examine System Restore in more detail. Windows 11 enables System Restore features automatically. Thereafter, Windows 11 takes automatic snapshots of your computer’s configuration settings:

* Periodically
* Before any configuration changes are made
* Just prior to applying an earlier restore point during recovery

Applying a restore point doesn’t affect the data on your computer, but can have far-reaching effects.

You can use System Restore for a variety of recovery scenarios. These include:

* Driver rollback
* Removing updates
* Removing apps you just installed
* Adding back apps you just removed
* Undoing significant, or even not so significant, configuration changes

To enable or configure System Restore:

1. Click **Start**, type **recovery** and then select **Recovery**.
2. On the **Advanced recovery tools** screen, select **Configure System Restore**.
3. In the **System Properties** dialog box, select **Configure**.
4. In the **System Protection for Windows (C:)** dialog box, if necessary, select **Turn on system protection**.
5. Then use the slide bar at the bottom of the screen to allocate an amount if disk space for restore point storage. Then click **OK**.

If you want to take a snapshot (create a restore point), in the **System Properties** dialog box, click **Create** and follow the on-screen prompts to create your restore point.

Finally, if you need to use a restore point to recover Windows, you can do so in the following ways:

* If Windows is running normally, or in Safe Mode, search for and select **Recovery**. Then choose **Open System Restore**. You can now choose from the available restore points.
* If Windows won’t start, then startup into Windows RE and navigate through the screens to locate System Restore. Select it, and follow the on-screen guidance to choose and apply the appropriate restore point.

When you apply a restore point, you can click the **Scan for affected programs** link to learn what, if any, apps and drivers will be deleted by the restore point application. You can also learn what older apps and drivers will be restored by the restore point application.

**Using the System Configuration Tool**

You can use the System Configuration tool (MSConfig.exe) to manage startup options, including choosing normal startups, diagnostic startups, and selective startups. You can also use the tool to force the computer to start in Safe Mode, and then choose supplemental Safe Mode options, such as selecting networking.

However, perhaps the most useful aspect of System Configuration is the ability to use it to control startup of services. Selecting the Services tab enables you to review and configure the available services in your computer. Since services can often be a cause of startup problems, you can use the tool to locate a problematic service and disable it.

You might need to start your computer in Safe Mode and then access System Configuration to control problematic services.

**Demonstration: Accessing Windows RE**

Lesson 2

**Managing Windows 11 startup**

Windows 11 provides a number of protections against early-launch malware. These, combined with the need to unlock the BitLocker-encrypted boot volume can pose challenges when troubleshooting startup problems.

**Lesson Objectives**

After completing this lesson, you will be able to:

* Describe the Windows 11 startup architecture.
* Explain the components in Windows 11 that can help secure startup.
* Configure BCD.

**Windows 11 startup architecture**

Windows 11 startup is based on two core components. These are:

* **Windows Boot Manager**. The BOOTMGR file is located in the root directory of the primary active partition in your computer (known as the EFI System partition).

This drive is not assigned a driver letter.

* **Windows OS Loader**. The Winload.exe file is stored in the Windows\System32 folder on the Windows volume (known as the Boot volume).

The Windows Resume Loader, Winresume.exe, is also stored in the Windows\System32 folder. This is used to restore from hibernation.

**Windows Boot Manager**

When your computer starts, BOOTMGR is loaded first. Boot Manager then reads the Boot Configuration Data (BCD). The BCD database stores startup configuration information in a format not dissimilar to the registry. The BCD stores information about the location of bootable operating systems on the local hard disks.

These days, that’s likely to be just one operating system since not many people dual-boot or multi-boot their computers anymore; especially since you can run Android, Linux and Windows apps natively in Windows 11. You can also, of course, use a VM to host additional operating systems without the need to configure multi-boot scenarios.

Having determine the location of a bootable operating system, this information is passed to the Windows OS Loader.

**Windows OS Loader**

Winload.exe is called by the Boot Manager. The OS loader is responsible for starting the operating system kernel (ntoskrnl.exe) from the C:\Windows\System32 folder. The OS loader then scans the registry for drivers with a start value of 0. These are the lowest level drivers. Winload.exe now initializes the operating system kernel and its drivers in memory, and control passes to the kernel.

**Windows Resume Loader**

If you use Hibernate mode in your computer, and that’s relatively unlikely nowadays, instead of using the OS loader, your computer starts back from hibernation when Winresume.exe reads and applies the contents of the Hiberfil.sys file. Since power management for laptop computers is very efficient, sleep and hybrid sleep are the usual modes of operation.

**Windows 11 startup process**

Let’s examine the end-to-end startup process for a typical Windows 11 computer. This process typically consists of the following steps:

1. The UEFI performs a power-on self-test.
2. The computer locates an installed hard disk by reading information from the UEFI. This disk should contain a GPT which defines where the partitions are on the disk. The computer locates the primary active partition, and then locates the boot sector on the discovered hard disk. The boot sector calls and loads BOOTMGR.
3. BOOTMGR reads the BCD and retrieves information about the computer’s installed operating systems, and then transfers control to winload.exe.
4. Winload.exe initializes memory and loads drivers low level device drivers. These are drivers with a start value of 0.
5. These drivers initialize low-level hardware components, such as disk controllers and peripheral bus drivers. Winload.exe then transfers control to the operating system kernel, ntoskrnl.exe.
6. The kernel initializes, and then higher-level drivers are loaded by the kernel.
7. The Windows Session Manager (Smss.exe) initializes the Windows subsystem and any other required subsystems, such as Linux or Android.
8. Windows loads the Winlogon service, which displays the sign-in screen. After the user signs in to the computer, Windows Explorer loads.

**Securing Windows 11 startup**

BitLocker is used to encrypt the boot volume, or C drive, in Windows computers. This helps protect the contents of the hard disk. However, the partition that hosts the BCD cannot be encrypted.

This means that the EFI System partition is potentially vulnerable, particularly to early-launch malware. To help mitigate this risk, Microsoft provides the following security features in Windows 11 startup:

* Secure Boot
* Trusted Boot
* Measured Boot
* Microsoft Defender Credential Guard

**Secure Boot**

Secure Boot is a Windows 11 feature implemented on UEFI-based computers. It can help to secure your device by helping to eliminate the ability of early-launch malware to exploit the device. Essentially, Secure Boot verifies the integrity of each of the startup files during startup before they’re loaded. It does so by checking that each file has a valid digital signature.

A digital signature verifies the publisher of a file, and also verifies that the file contents haven’t changed since the file was signed. The UEFI won’t load any software that doesn’t pass this security check.

Since Secure Boot is mandatory in Windows 11, you don’t need to do anything to turn it on; it’s enabled by default.

**Trusted Boot**

Trusted Boot improves the Windows 11 startup protection. The winload.exe program (OS bootloader) verifies the integrity of the Windows kernel (ntoskrnl.exe) before loading it. Thereafter, the kernel verifies the integrity of the following startup components:

* The boot drivers
* Startup files
* Early launch antimalware software

**Measured Boot**

During the initial startup process, Measured Boot tracks file access. The measurements that relate to tracked files are then stored in the computer’s TPM. When startup is complete, Measured Boot submits the measurements to an antimalware app running on Windows 11; this app can forward the measurements to a health attestation system.

Measured Boot performs the following steps:

1. The UEFI firmware stores a hash of all that’s loaded before the antimalware app starts in the computer’s TPM. This includes:

* Firmware
* Bootloader
* Boot drivers

1. After startup, Windows 11 starts the remote attestation client.
2. The attestation server sends the client a unique key.
3. The TPM uses this key to digitally sign the log recorded by UEFI.
4. Windows then sends the log to the server.

As a result, you can identify computers that might have low-level malware present.

**Microsoft Defender Credential Guard**

As we learned earlier, Credential Guard helps protect sign-in information by virtualizing the Local Security Authority (LSA). As Windows sign-in is the last step in the computer startup process, you can consider Credential Guard a part of the Windows 11 startup security environment.

**Configuring the BCD**

As mentioned, the BCD is a database that stores information about bootable operating systems on the local computer. Generally, there’s no need for you to need to edit this database. Pretty much the only reason you might is because you want to make your computer dual-boot between Windows 11 and another operating system.

However, it’s important you’re familiar with the tools with which you can manage the BCD should the need arise.

**BCDEdit.exe**

You can use this command-line tool from an elevated Command Prompt. It enables you to:

* Add, modify, or remove entries from the BCD store.
* Import or export entries to and from the BCD store.
* Query entries.
* List active settings.
* Apply global changes to all entries.
* Change the default time-out value for multiboot configurations.

Possible reasons to use BCDEdit include:

* **Adding a new hard disk**. If you add a disk, and disk numbering changes, you’ll have to update the BCD to use the new disk number. This is unlikely as the primary disk is numbered 0, and any additional disks are numbered sequentially after 0.
* **Enable multiboot**. If you want to start another operating system, you’ll need to edit the BCD to identify the operating systems and their paths. Since Windows support Linux and Android as subsystems, and you can virtualize other operating systems using Client Hyper-V, this, too, is unlikely.
* **New deployment**. If you deploy Windows 11 to a new computer that has a blank hard disk, you’ll need to add a boot store entry to the BCD.
* **Backup and restore**. If you need to backup or restore the BCD.

The following table describes the more common command-line options for BCDEdit.exe.

|  |  |
| --- | --- |
| Command | Description |
| /createstore | Creates a new BCD store with no entries. |
| /export | Exports the BCD store to a specified file. |
| /import | Restores the BCD store from a specified file. |
| /copy | Copies boot entries. |
| /create | Creates boot entries. |
| /delete | Deletes boot entries. |
| /set | Creates or modifies a boot entry’s elements. |
| /enum | Lists the boot entries. |
| /default | Specifies the default boot entry. |

**BootRec.exe**

You can use the BootRec.exe command-line tool in the Windows RE Command Prompt. You can use the following command-line switches with BootRec.exe:

* **/FixMbr**. Verifies and repairs the MBR.
* **/FixBoot**. Verifies and repairs the boot sector.
* **/ScanOS**. Scans for Windows installations.
* **/ReBuildBCD**. Scans for Windows installations and rebuilds the BCD based on findings.

It’s important to remember that if you want to troubleshoot or fix the BCD, the easiest way is to use Startup Repair in Windows RE.

**Demonstration: Reviewing startup settings**

Lesson 3

**Configuring the registry**

Windows 11 stores user and computer configuration data in the registry. When a configuration change is made, that change is recorded in the registry. When Windows starts, and when apps are loaded, settings are retrieved from the registry.

You won’t need to make direct changes to the registry very often, and when you do, it’s important you exercise caution as mistakes can render your computer unusable. In this lesson, you’ll learn about the registry’s structure, and how to safely make edits when needed.

**Lesson Objectives**

After completing this lesson, you will be able to:

* Describe the registry.
* Identify tools that you can use to edit the registry.

**What is the registry?**

The registry has a hierarchical structure which logically groups objects in a series of hives, keys, subkeys, and values.

**Hives**

The top level folder in the registry is known as a Hive. There are five hives.

|  |  |
| --- | --- |
| Hive | Description |
| HKEY\_CURRENT\_USER | Contains configuration information for the currently signed-in user. This hive is a shortcut to a key stored in HKEY\_USERS. Externally, this hive is stored as NTUSER.DAT in the user’s profile folder. Sometimes known as HKCU. |
| HKEY\_LOCAL\_MACHINE | Contains all computer settings. This is the hive you might spend time editing. Sometimes known as HKLM. |
| HKEY\_USERS | Contains a collection of all the configuration information for all users that have signed in locally to the computer, including the currently signed-in user. You’ll never need to edit the contents of this hive. |
| HKEY\_CLASSES\_ROOT | Contains file association information and determines which app opens when a user accesses a specific file type on the file system. Represents merged data from Software\Classes in HKLM and HKCU. |
| HKEY\_CURRENT\_CONFIG | Contains information about the current hardware profile that the local computer used during system startup. Data shown here is populated from HKLM. |

Although the registry is represented as a single hierarchical structure of hives, keys, and values, it is a collection of files stored C:\Windows\System32\Config.

**Keys and subkeys**

Beneath the hives, there are keys and subkeys. These are much like folders in a file system, containing subfolders and files. The point of this hierarchy is to group related settings together so that it’s easier to locate specific settings.

**Values**

Values are used to configure specific properties of the operating system. There are several different value types, depending on what you’re trying to configure.

|  |  |  |
| --- | --- | --- |
| Value type | Data type | Description |
| REG\_SZ | String | Fixed-length text string. |
| REG\_EXPAND\_SZ | Expandable string | Variable length text string. Used to store variables. |
| REG\_MULTI\_SZ | Multiple strings | Multiple string values. |
| REG\_BINARY | Binary | Raw binary data, often displayed in hex. |
| REG\_DWORD | DWORD | 32 bit (4-byte) numbers. |

When you make changes to the registry, you must ensure that you not only store the value in the right hive, key, and subkey, but that you also create the correct value and assign the right value type.

**Working with the registry**

It’s not common to have to edit the registry directly. This is largely because you can reconfigure your computer using other methods, and rely on the changes being reflected in the registry. If you have to edit the registry, you can use one of several methods.

**The Registry Editor tool**

You can use the Regedit.exe tool to navigate and edit the registry. You can use this tool to review registry values, make changes, and both import and export keys, subkeys, and values.

**Working with REG files**

You can create text files with a .reg extension. If formatted correctly, you can import settings from a .reg file. Your file must start with a line that reads as follows:

Windows Registry Editor Version 5.00

Thereafter, you can define the values you want to create or edit by defining the hive, key, subkey and value as displayed in the following example:

[HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\services\cdfs]

"Start"=dword:00000004

This example targets the **Start** value located in HKLM\SYSTEM\ControlSet001\services\cdfs and assigns it the DWORD value of 4.

After you create your .reg file, double-click the file to merge the contents with the registry.

**Using Group Policy preferences**

You can use Group Policy preferences to configure the registry. This is perhaps the safest and easiest approach to take. Use the following procedure to make changes by using Group Policy:

1. Open **Group Policy Management** and locate the appropriate GPO.
2. Open the GPO for editing.
3. In the **Group Policy Management Editor**, expand either **User Configuration** or **Computer Configuration** and then expand **Preferences**.
4. Expand **Windows Settings**, and then select **Registry**.
5. Right-click **Registry** and then select **New**. Click **Registry Item**.
6. In the **New Registry Properties** dialog box, select the **Hive**, **Key Path**, and **Value name**. Choose a valid **Value type** and enter the **Value data**.
7. Choose the **Action** (Create, Replace, Update, or Delete) and then click **OK**.

Like all Group Policy preferences, these values can be overwritten by local configuration changes.

**Windows PowerShell**

You can also use Windows PowerShell to make changes to the registry. Interestingly, PowerShell displays the registry structure much like a file system. You can navigate the structure of the registry by using commands which you might normally use to navigate the file system. For example, use the following commands to navigate to HKLM\System\CurrentControlSet\Services\atapi and list the values:

cd hklm:

cd \system\currentcontrolset\services\atapi

dir

If you want to make changes, you can use the **Set-ItemProperty** cmdlet.

Lesson 4

**Managing devices and drivers**

Drivers occupy the lowest level in the Windows system architecture: the kernel. Consequently, unreliable or unsafe drivers can compromise the integrity of Windows causing Windows to be unstable, or worse, to stop. It’s important that you know how to identify problematic drivers, and be able to remove them.

Users want to be able to add hardware to their computers; it’s pretty easy to do these days, since so many peripherals are attached via USB. However, you might want to manage the addition of hardware peripherals. One way to do that is to manage device driver installation.

In this lesson, you’ll learn how to manage device drivers, including how to roll a driver back and, when needed, remove a driver. You’ll also learn how to restrict device installation.

**Lesson Objectives**

After completing this lesson, you will be able to:

* Describe the Windows driver architecture.
* Describe tools for managing devices drivers.
* Restrict device installation.

**Overview of the driver architecture**

As you learned earlier, the Windows architecture consists of two main layers: user mode and kernel mode. Device drivers occupy kernel mode, which enables fast device access. However, it also means that unreliable or unsafe drivers can create significant problems for Windows.

**What is a device driver?**

A device driver is a small package that sits between a piece of hardware and the operating system. Drivers are not only operating system specific (i.e. Windows, Linux, Android), but often version specific. So, there’s no guarantee that a driver designed for Windows 7 works on Windows 11; although it might.

Microsoft provides a library of drivers that are certified and tested, and digitally signed, in the driver store on Windows 11. However, if you have a peripheral that requires a driver that Microsoft doesn’t provide, you might be able to obtain it from Windows Update, or from the hardware vendor’s website.

**What are driver packages?**

A driver is not usually a single file. A driver package provides the files that make up a device driver. Typically, a driver package consists of the following:

* **A device setup information file**. This text file has a .inf extension and provides information about the type of the device, and the associated files that make up the driver package.
* **The driver files**. The driver actually consists of one or several .sys files and dynamic-link libraries (DLLs). These are the components that interface with the hardware device.
* **A security catalog file**. To help ensure that the driver is from a reputable source, drivers must be signed in Windows 11. The security catalog file, which has a .cat extension, contains this digital signature.

All drives must be signed in Windows 11.

**What is the driver store?**

You usually want to make things convenient for your users. When a user inserts a new webcam into a USB port on their computer, they want it to initialize so that they can use it in Microsoft Teams.

Microsoft ship Windows with a large number of preinstalled drivers that can help make things easy for your users. When a user adds a new device, the driver store is checked for the required driver and, if available, it’s loaded, and the device is initialized.

The driver store is located at C:\Windows\System32\DriverStore.

**Staging drivers**

If a user tries to add a specific hardware device, and the drivers are not present in the driver store, your user will need elevated privilege to add the driver. Since that’s not something you’d typically want to allow, you could anticipate your user’s needs, and stage the required drivers.

Staging means the preinstallation into the driver store of device drivers that are not included by default. When a user adds a hardware component, the driver store is checked. Because the driver has been added, the device can initialize without the user needing the elevated permissions required to install a driver.

You can stage drivers in a number of ways, depending on your situation. For example, if you use disk imaging as a means to deploy Windows to new computers, it makes sense to include any anticipated drivers in the store before you capture the image. Thereafter, any computer deployed using the image also has the staged drivers in their driver store.

If you deploy Windows using Microsoft Deployment Toolkit, or Configuration Manager, you can add a task in a task sequence to include the deployment of additional drivers. These are then deployed when the image is deployed, but are not included in the image itself. This is a useful way of incorporating more recent drivers.

Another way to stage drivers is to use the **pnputil.exe** Command Prompt tool. In order to perform this manual staging, you must use the following procedure:

1. Sign in as administrator.
2. Open an elevated **Command Prompt**.
3. Run the following command:

* Pnputil /add-driver *path\driver.inf*
* Substitute *path/driver.inf* for the path and name of the appropriate .inf file for your staged driver.

If you want to add multiple drivers, place them in the same folder, and then use a wildcard to define the name of the .inf file:

Pnputil /add-driver *path\\*.inf*

You can use pnputil.exe to list, add, or remove drivers from the store. The following table describes the some of the pnputil.exe parameters you can use.

|  |  |
| --- | --- |
| Command parameter | Description |
| pnputil.exe /add-driver | Adds a driver package. |
| pnputil.exe /add-driver /install | Adds and then immediately installs a driver package. |
| pnputil.exe /enum-drivers | Lists all non-Microsoft packages. |
| pnputil.exe /delete-driver | Deletes specified packages. |

**Tools for managing device drivers**

If you want to review, update, or remove any device drivers, you can use a number of tools to complete the task. You can use Device Manager, Bluetooth & devices in the Settings app, Device and printers in Control Panel, and Windows PowerShell to manage your devices.

**Device Manager**

Device Manager is a management console snap-in. Under the name of the local computer, it lists all the available devices in the computer, and their current status.

You can access Device Manager by right-clicking **Start** and then selecting **Device Manager**.

If a device has stopped responding, or it performing with errors, you can use Device Manager to:

* **Update the driver**. If you suspect the driver is creating problems, consider updating it. Right-click the device and then click **Update driver**. Follow the onscreen instructions to complete the process.
* **Disable the device**. If a device stops responding correctly, or at all, you can disable it. The device displays a down arrow to indicate its state.
* **Enable a device**. To enable a disabled device, right-click it an choose **Enable device**.

Disabling and then enabling a device can sometimes resolve device problems.

* **Uninstall the device**. If disabling and enabling a device doesn’t resolve an issue, uninstall the device. If necessary, choose the option to remove the driver. Then scan for hardware changes, and Windows detects the device and installs the default driver.
* **Roll back the driver**. If a recent driver update is suspected of causing a problem, you can roll back the driver to an earlier version. Use this option before using the less targeted System Restore.
* **Review device details**. Check details about the device and its settings. Details are numerous, but include: Status, Problem code, Class, Class GUID, Driver description.
* **Review device events**. Review events related to the device and its use.
* **Review resources**. Displays details like the IRQ, I/O, DMA, and any conflicts.
* **Scan for hardware changes**. Forces Windows to detect all installed hardware.

**System Information**

Enables you to review the following:

* **Hardware Resources**. Displays information about the resources devices are using, such as DMA, I/O,IRQs, and Memory. Also provides a node to review any conflicts.
* **Components**. Lists system components, including: Multimedia, Sound Device, Display, Network, Storage, and USB. Devices with problems are displayed in the Problem Devices node.
* **Software Environment**. Displays System Drivers, Environment Variables, Services, Running Tasks, and much more.

From a device driver management perspective, the most useful node is Hardware Resources. The **msinfo32.exe** command loads System Information.

**Bluetooth & devices**

Use the **Settings** app to access **Bluetooth & devices**. You can then review the available devices in your computer, including:

* Bluetooth devices
* Devices
* Printers & scanners
* Cameras
* Mouse
* Touchpad
* USB

Select Devices to gain access to a list of peripherals connected to, or at least configured for use with, your computer. Bluetooth & devices is useful for adding new devices, and reviewing the connection status of peripherals, such as Bluetooth audio and pens.

**Devices and printers**

Devices and Printer provides fairly high-level information about installed peripherals such as storage devices, printers, scanners, and multimedia devices, like smart TVs. You can select a peripheral, and then right-click it to access device actions. Some actions are device specific, but there are two generic options:

* **Remove the device**. Enables you to remove the device.
* **Troubleshoot the device**. Enables you to launch a troubleshooting wizard that can detect problems, and offer guidance on possible mitigations.

You can access Devices and Printers from Control Panel.

**Windows PowerShell**

Windows PowerShell provides a quick solution to retrieving information about device drivers. You can also use Windows PowerShell Remoting to retrieve device information from one or several remote computers in a single step. The following table displays the cmdlets that you can use for device management.

|  |  |
| --- | --- |
| Cmdlet | Description |
| Get-PnpDevice | Displays PnP devices information. |
| Get-PnpDeviceProperty | Displays detailed properties about a specified PnP device. |
| Enable-PnpDevice | Enables a PnP device. |
| Disable-PnpDevice | Disables a PnP device. |

**Restricting device installation**

As you learned earlier, to enable standard users to install devices without elevating their system privilege, you can stage the drivers by adding them to the driver store. While its helpful for users to be able to enable certain devices, it can become difficult to manage if you allow users to install any device (and its driver) that they want.

Fortunately, you can use Group Policy settings to restrict device installation. You can use these settings to enforce a corporate device installation policy. For example, the policy might prohibit the introduction of certain device types, while it might allow for the introduction of other device types.

You can access the required Group Policy settings in the following locations:

* Computer Configuration / Policies / Administrative Templates / System / Driver Installation
* Computer Configuration / Policies / Administrative Templates / System / Device Installation / Device Installation Restrictions

The following table contains a description of both of the available settings in the Driver Installation node.

|  |  |
| --- | --- |
| Group Policy Setting | Group Policy description |
| Allow non-administrators to install drivers for these device setup classes | Specifies a list of device setup class GUIDs defining driver packages that standard users can install. |
| Turn off Windows Update device driver search prompt | Specifies whether the administrator is prompted to use Windows Update to search for device drivers. |

The following table contains a description of some of the available settings in the Device Installation Restrictions node.

|  |  |
| --- | --- |
| Group Policy setting | Group Policy description |
| Allow administrators to override Device Installation Restrictions policies | Determines if members of the Administrators group can install and update the drivers for any device, regardless of other policy settings. |
| Allow installation of devices using drivers that match these device setup classes | Allows you to specify a list of device setup class GUIDs for driver packages that Windows can install. |
| Prevent installation of devices using drivers that match these device setup classes | Allows you to specify a list of device setup class GUIDs for driver packages that Windows cannot install. |
| Allow installation of devices that match any of these device IDs | Allows you to specify a list of hardware IDs and compatible IDs for devices that Windows can install. |
| Prevent installation of devices that match any of these device IDs | Allows you to specify a list of hardware IDs and compatible IDs for devices that Windows cannot install. |
| Prevent installation of removable devices | Prevents Windows from installing removable devices. |
| Prevent installation of devices not described by other policy settings | Prevents the installation of devices that aren’t specifically defined in any other policy setting. |

**Demonstration: Performing driver rollback**

Lesson 5

**Recovering files**

You could argue that the whole point of a file-server infrastructure is to serve files. Many, perhaps most, user files reside on file servers or network attached storage. For these server stored files, there will exist a means to back up user content.

But things are a little more difficult on users’ devices. When users save their content to a local library, such as Documents or Pictures, you need to consider how best to provide recovery for those files, if needed.

Windows 11 provides two main file recovery tools, and in this lesson, you’ll learn how to use these tools to recover locally stored files.

**Lesson Objectives**

After completing this lesson, you will be able to:

* Describe reasons for file recovery and explain available methods.
* Describe File History and Previous Versions.
* Describe Backup and Restore (Windows 7).
* Describe OneDrive recovery options.

**Why back up?**

When user data is stored locally, it’s at risk of loss for a number of reasons. It’s therefore important you consider those reasons, and plan for mitigations to address them.

**Common reasons for file loss**

There are a number of possible reasons why users files may become unavailable. These include:

* **Deletion**. Accidental deletion of a file or folder.
* **Virus**. Malicious code encrypting or damaging files.
* **Version control**. A user saving their work over an earlier version that, in hindsight, they wanted to retain.
* **Theft**. A user’s computer is lost or stolen.

**Possible mitigations**

Knowing how files can become unavailable enables to you consider how to avoid those scenarios. Let’s examine each of the key reasons for file loss, and consider some possible mitigations:

* **Deletion**. Consider implementing backup procedures to protect against deletion. Use a local backup tool for files stored on the users’ local hard disks. Alternatively, consider using a Windows Server feature, like Folder Redirection, to point users’ libraries to a file server UNC. Then use server backup to provide for recovery. You can also implement Microsoft OneDrive.
* **Virus**. Implement robust antivirus and anti-malware procedures. Enable all necessary Windows 11 security features to help protect against this problem. Back up users content so that if recovery is needed, it’s possible.
* **Version control**. Implement a versioning system to manage versions. If users store files in SharePoint Server or SharePoint Online, you can manage versions. But Windows 11 also provides File History as a means for managing previous versions of locally stored files.
* **Theft**. Protect your organization against data leakage by implementing BitLocker on all user devices running Windows 11. But this doesn’t help users get their files back. So, again, consider directing user content to file server shared folders, and backing those folders up.

For those situations where you have data on users’ local hard drives, Windows provides a number or recovery options. These are:

* **File History**. Enables users to review previous versions of their files and select a version for recovery.
* **Backup and Restore (Windows 7)**. Enables users to create and manage scheduled back up jobs. Provides an intuitive file recovery interface.
* **System image backup**. Enables an administrator to take a complete snapshot of the hard drive of a specific computer. If the entire drive becomes unavailable, by using Windows RE, the drive can be recovered from a system image backup.
* **Manual file copying**. Educating your users to create multiple copies of files can be beneficial, but is difficult to automate and manage.
* **OneDrive sync**. If you implement OneDrive, when users save content to their local libraries, this content is synced to their OneDrive storage in the Microsoft cloud. OneDrive provides basic file recovery tools, including Version history and the Recycle bin.

**Using File History and Previous Versions**

File History and Previous Versions work together to enable users to easily recover files that they’ve either deleted, or overwritten. To provide this protection, start by enabling and configuring File History.

**Enabling File History**

To enable File History, use the following procedure:

1. Open **Control Panel** and then search for **File History**.
2. Click **File History** in the returned list.
3. In **Control Panel**, on the **File History** page, in the navigation pane, click **Select Drive**.
4. Choose a drive to use to store File History backups. This can’t be the same drive you’re protecting, and therefore the C: drive doesn’t display. Click **OK**.

* You can use any external drive, like a memory stick or SD card, or a network location. Using the latter option provides additional benefits because you could choose to target a location that’s also backed up by server backup procedures.

1. Click **Exclude folders**. Add any folders you want to exclude, and click **Save**. By default, File History protects the default libraries (Documents, Pictures, and so on).
2. Click **Advanced settings**, and specify:

* How often copies should be saved
* How long to keep copies

1. Click **Save changes**.
2. On the File History page, click **Turn on** to enable File History.

**Using Previous Versions**

After you’ve enabled File History, your users’ files are backed up periodically, as specified by your settings. If you want to review the available versions of a file, you can use the following procedure:

1. Navigate to the file, right-click the file, and select **Properties**.
2. In the ***filename* Properties** dialog box, click the **Previous Versions** tab. All versions of the file are displayed in date order.
3. To review versions, select one of the listed file versions, and click the down arrow adjacent to Open. Select Open in File History.
4. The file is displayed in File History. Use the navigation buttons to review each version of the file.
5. When you locate the appropriate version, select the Restore button. The file restores to the original location.
6. You are prompted to Replace or Skip Files since a version of the file still exists. Choose the appropriate option.
7. Close the File History window.

**Backup and Restore (Windows 7)**

For users that prefer to perform manual or scheduled backups of specified folders, Windows 11 provides the Backup and Restore (Windows 7) tool. So-called, because it is broadly the same as the Backup and Restore tool provided in Windows 7.

Although Windows Backup is easy to configure and use, it does require that an administrator configures the appropriate settings on all user devices. In workplace networks, most administrators will seek other methods to protect user content. For this reason, it’s considered more of a home user recovery system.

Before you can schedule backup operations, you must enable and configure Backup and Restore settings.

**Configuring Backup and Restore**

To enable File History, use the following procedure:

1. Open **Control Panel** and then search for **Backup**.
2. Click **Backup and Restore (Windows 7)** in the returned list.
3. In **Control Panel**, on the **Backup and Restore (Windows 7)**page, in the navigation pane, click **Set up Backup**. The Set up backup wizard starts.
4. On the **Select where you want to save your backup** page, select an external drive, or choose a network location. Click **Next**.
5. On the **What do you want to back up?** page, select **Let Windows choose** and click **Next**. You can also select Let me choose, and add additional folders. By default, Windows backs up the libraries and includes a System image backup.
6. On the **Review your backup settings** page, click **Save settings and run backup**.

Backup also creates a default schedule backup job for **Every Sunday at 19:00**. You can change the schedule to suit your needs.

If you want to change the settings, on the **Backup and Restore (Windows 7)** page in **Control Panel**, you can:

* Turn off the backup schedule
* Create a system image
* Create a system repair disc
* Change scheduled backup settings
* Manage space allocated to backup
* Initiate a manual backup
* Restore files

**Restoring files**

Restoring files is straightforward. From the **Backup and Restore (Windows 7)** page in **Control Panel**, use the following procedure:

1. Click **Restore my files**. The Restore Files wizard starts.
2. Click **Browse for files**, as applicable.
3. A **Browse the backup for files** window opens. A single folder is displayed that represents the root of the backed up drive.
4. Navigate through the folder structure until you locate the file that you want to restore. Click **Add** **files**.
5. In the **Restore Files** window, click **Next**.
6. On the **Where do you want to restore your files?** page, click either In the original location, or choose another location and click **Restore**.
7. Close all open windows.

**Recovering files in OneDrive**

If your organization has a Microsoft 365 subscription, then users with a Microsoft 365 Office license can use OneDrive for Business. OneDrive provides 1 TB of storage space for each user, which can be extended by the administrator. The OneDrive app is integrated in Windows 11 and Windows Explorer, making it easy for users to work with. When users store files in their local OneDrive folder, these files sync to the cloud.

One of the advantages of using OneDrive is that it provides built-in recovery. Versioning for files is enabled by default, as is a Recycle bin.

**Recovering deleted files**

If a user deletes a file from their local OneDrive folder, that delete action is synced to the cloud instance of the file, deleting it. However, the cloud instance of the file is moved to the Recycle bin. The user can select the **OneDrive** icon on the taskbar and then click the **Recycle bin** tile.

Recently deleted files display in a web browser tab. Users can then select one or more files, and then click **Restore** on the toolbar. Files are restored to their original location, and synced back down to the user’s local computer.

**Viewing version history**

If a user wants to review or recover an earlier version of a file from their OneDrive folder, they can easily do so. The user selects the file, right-clicks it, and selects **OneDrive**. From the OneDrive menu, they select **Version history**. Previous versions are displayed, and the user can review specific versions, or restore a selected version.

**Demonstration: Enabling File History**

**Lab: Troubleshooting Windows 11**

**Question:**In the lab, you performed driver rollback. How else could you have recovered the earlier driver?

**Module Review and Takeaways**

Review Questions

**Question:**You’ve enabled File History and used the default values. You create and work on a file immediately after enabling File History. After ten minutes, you realize you’ve overwritten the file’s contents with incorrect information. Can you recover earlier versions of the file?

**Question:**Your computer has stopped responding. You restart the computer, but it won’t start. You know you created a system restore point yesterday, but since your computer won’t start, what can you do to access that restore point?

Tools

The following table lists the tools that this module references.

| **Tool** | **How used** | **Where found** |
| --- | --- | --- |
| BCDEdit.exe | * Verify the BCD | Command Prompt |
| Bootrec.exe | * Verify startup metadata | Windows RE Command Prompt |
| Regedit.exe | * Review and edit the registry | Built-in to Windows |
| WBAdmin.exe | * Perform backup and restore operations | Command Prompt |