Microsoft®
Training &
Certification

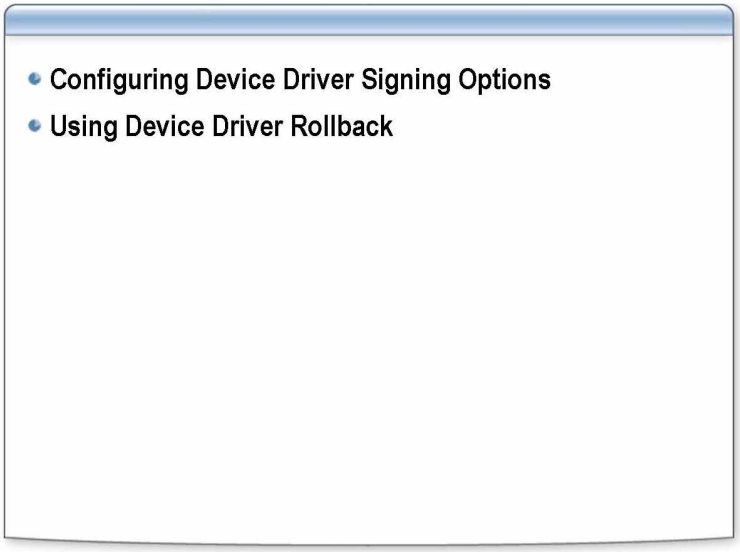
Microsoft® Official
Curriculum

Module 4: Maintaining Device Drivers

Contents

Microsoft®

Overview



Introduction

To function properly, each device that is attached to a computer requires software, known as a device driver, to be installed on the computer. Every device requires a device driver to communicate with the operating system. Device drivers that are used with the Microsoft® Windows® operating systems are typically provided by Microsoft and the device manufacturer.

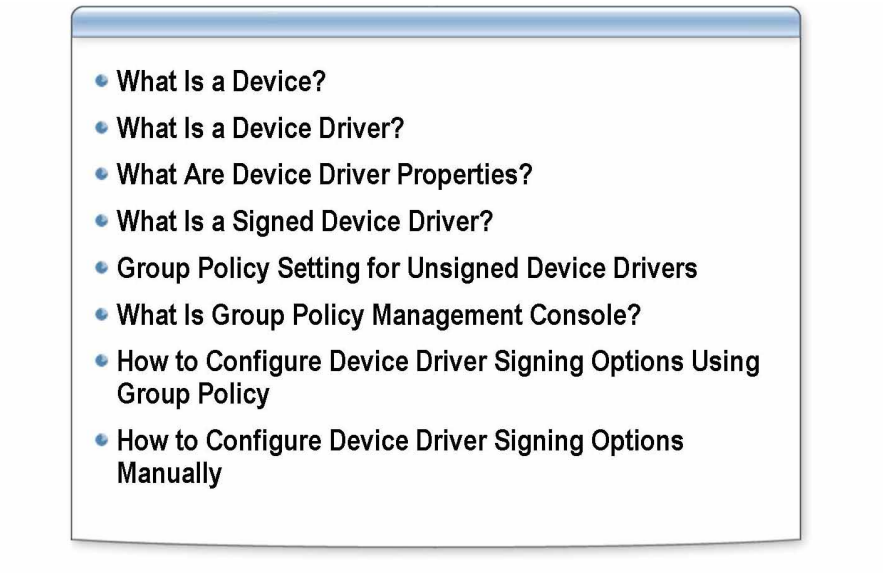
This module introduces you to concepts and procedures that will help you maintain device drivers.

Objectives

After completing this module, you will be able to:

- Configure device driver signing.
- Restore the previous version of a device driver.

Lesson: Configuring Device Driver Signing Options



Introduction

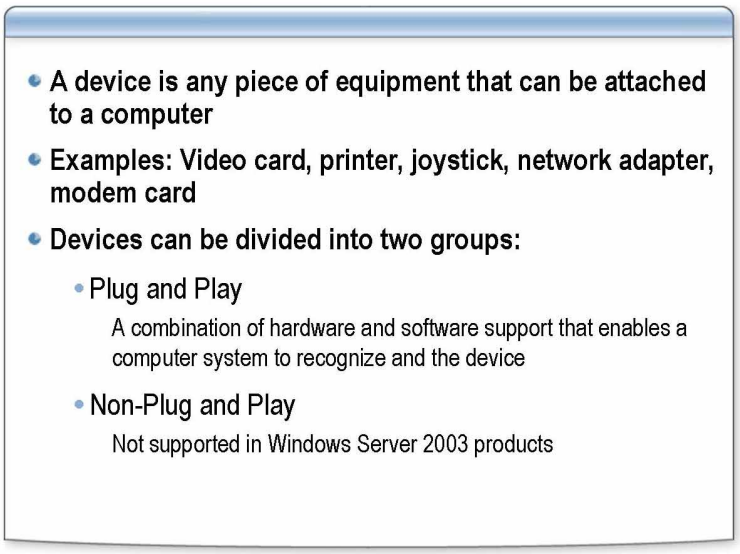
This lesson introduces devices, device drivers, device driver signing, and Group Policy driver signing settings. This lesson also describes how to configure device driver signing manually and by using Group Policy objects.

Lesson objectives

After completing this lesson, you will be able to:

- Explain devices and types of devices.
- Explain the purpose of a device driver.
- Determine device driver properties.
- Explain signed device drivers.
- Explain the Group Policy setting for unsigned device drivers.
- Explain the Group Policy Management console.
- Configure device driver signing options by using Group Policy.
- Configure device driver signing options manually.

What Is a Device?



Definition

A device is any piece of equipment that can be attached to a computer.

Examples of devices

Some examples of devices are a video card, a printer, a joystick, a network adapter, a modem card, or any other peripheral equipment.

Types of devices

Devices can be divided into two groups:

- Plug and Play

  Plug and Play is a combination of hardware and software support that enables a computer system to recognize and adapt to hardware configuration changes with little or no user intervention.

  You can add or remove Plug and Play devices dynamically, without manually changing the configuration. With Plug and Play, you can be confident that all devices will work together and that the computer will restart correctly after you add or remove the device.

  You can install some Plug and Play devices by simply plugging in the device. For other devices, such as Plug and Play Industry Standard Architecture (ISA) cards, you must turn off the computer to install the device, and then restart the computer to initialize the device. Most devices manufactured since 1995 are Plug and Play.

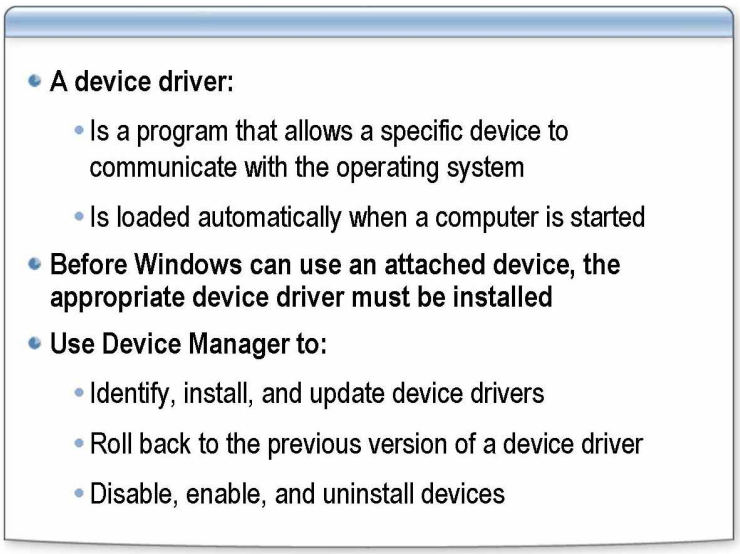
Note For more information about Plug and Play, see the white paper, *Plug and Play*, under **Additional Reading** on the Web page on the Student Materials compact disc.

- Non–Plug and Play

  Plug and Play support depends on both the hardware device and the device driver. If the device driver does not support Plug and Play, its devices behave as non–Plug and Play devices, regardless of any Plug and Play support provided by the hardware.

  Non–Plug and Play devices are not supported by products in the Windows Server 2003 family.

What Is a Device Driver?



Definition

A device driver is a software program that allows a specific device, such as a modem, network adapter, or printer, to communicate with the operating system.

Scenario

For example, you are a systems administrator for a department in a large organization. The department recently acquired three new color printers. Users are complaining that all three color printers produce prints that are blurred and grainy. You suspect that the printer device driver is at fault. To solve the problem, you visit the Web site of the printer manufacturer, download the latest device driver for the printer, and then install it on the printer server.

Key concepts

The following key concepts describe device drivers:

- A device driver is loaded automatically when a computer is started.
- Before Windows can use a device that is attached to your system, the appropriate device driver must be installed.
- If a device is listed in the Hardware Compatibility List (HCL), a device driver for that device is usually included with Windows.

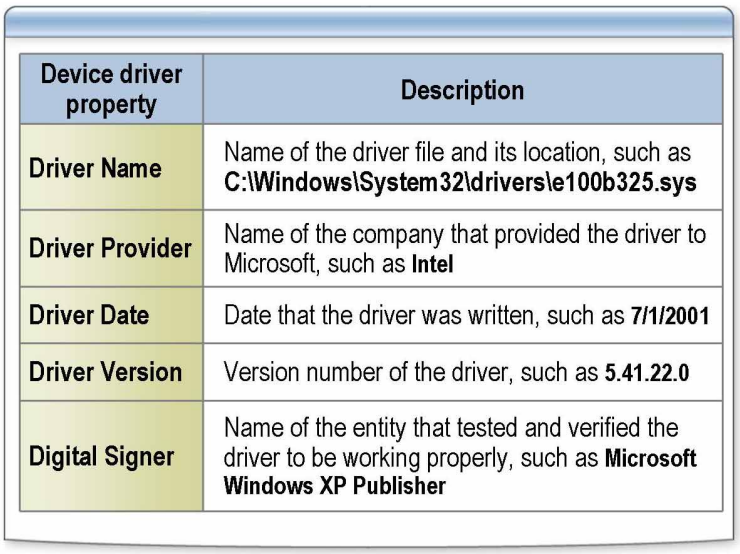
  The HCL is a list of hardware that Microsoft compiles for specific products, including Windows Server 2003 and earlier versions of Windows. The HCL for a specific product, such as Windows Server 2003, includes the hardware devices and computer systems that are compatible with that version of the product.

Note The HCL is updated as new hardware becomes available, so always check the Microsoft Web site at http://www.microsoft.com/hwdq/hcl/ for the latest HCL. When a device is on the HCL but the driver is not included with Windows or available from the Web site, you must obtain the device driver from the device manufacturer.

- You can use Device Manager, the administrative tool, to:
  - Identify the device drivers that are loaded for each device, and obtain information about each device driver.
  - Install updated device drivers.
  - Roll back to the previous version of a device driver.
  - Determine whether the hardware on your computer is working properly.
  - Disable, enable, and uninstall devices.
  - Print a summary of the devices that are installed on your computer.

Note After you load the device driver onto your system, Windows configures the properties and settings for the device. Although you can manually configure device properties and settings, you should let Windows do it. When you manually configure properties and settings, the settings become fixed, which means that Windows cannot modify them in the future if a problem arises or there is a conflict with another device.

What Are Device Driver Properties?



Device driver property	Description
Driver Name	Name of the driver file and its location, such as **C:\Windows\System32\drivers\e100b325.sys**
Driver Provider	Name of the company that provided the driver to Microsoft, such as **Intel**
Driver Date	Date that the driver was written, such as **7/1/2001**
Driver Version	Version number of the driver, such as **5.41.22.0**
Digital Signer	Name of the entity that tested and verified the driver to be working properly, such as **Microsoft Windows XP Publisher**

Introduction

One of your duties as a systems administrator may be to monitor the Web sites of hardware vendors to look for updated device drivers and then install them on your server computer. Before installing an updated device driver, you must document the properties of the device driver, such as name, date, and version.

Device driver properties

The following five properties are associated with every device driver:

- *Driver Name.* The physical name of the driver file and its location.
- *Driver Provider.* The name of the company that provided the driver to Microsoft.
- *Driver Date.* The date that the driver was written.
- *Driver Version.* The version number of the driver. The first version is typically named 1.0.
- *Digital Signer*. The name of the entity that tested and verified that the driver works properly.

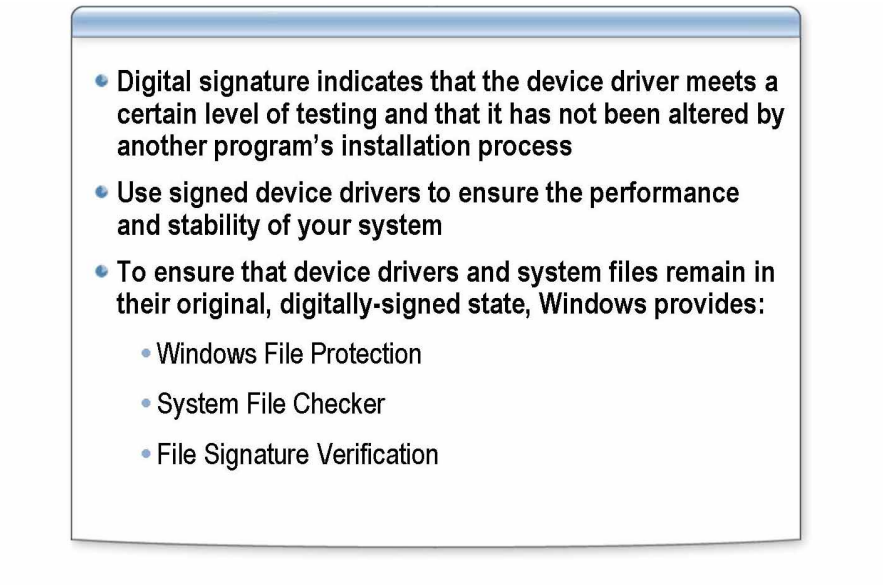
Example

The properties of a driver for a system device named Intel Pro/100+ Management Adapter with Alert On LAN are shown in the following table.

Property	Description
Driver Name	C:\Windows\System32\drivers\e100b325.sys
Driver Provider	Intel
Driver Date	7/1/2001
Driver Version	5.41.22.0
Digital Signer	Microsoft Windows XP Publisher

Note To view information about a device driver, open Device Manager, double-click the type of device that you want to view, and then on the **Driver** tab, click **Driver Details**.

What Is a Signed Device Driver?



Introduction

Each device driver and operating system file that is included with Windows has a digital signature. The digital signature indicates that the driver or file meets a certain level of testing and that it was not altered or overwritten by another program's installation process.

An administrator can configure Windows to respond to an unsigned device in one of three ways:

- Ignore device drivers that are not digitally signed
- Display a warning when it detects device drivers that are not digitally signed
- Prevent users from installing device drivers that are not digitally signed

Why use signed device drivers?

Using signed device drivers helps to ensure the performance and stability of your system. Also, it is recommended that you use only signed device drivers for new and updated device drivers.

Note Software for hardware products that display the Designed for Microsoft Windows XP logo or Designed for Microsoft Windows Server 2003 logo has a digital signature from Microsoft. This digital signature indicates that the product was tested for compatibility with Windows and has not been altered since testing.

Tools and components to maintain the digital signature of a device driver

Windows includes the following tools and components to ensure that your device drivers and system files remain in their original, digitally-signed state:

- Windows File Protection

  Windows File Protection prevents the replacement of protected system files, such as .sys, .dll, .ocx, .ttf, .fon, and .exe files. Windows File Protection is a component that runs in the background and protects all files that are installed by the Windows Setup program.

  Windows File Protection checks the file's digital signature to determine whether the new file is the correct version. If the file is not the correct version, Windows File Protection either replaces the file from the backup that is stored in the Dllcache folder or from the Windows Server 2003 compact disc. If Windows File Protection cannot locate the appropriate file, it prompts you for the location.

  By default, Windows File Protection is always enabled and allows digitally signed files to replace existing files. Currently, signed files are distributed through Windows Service Packs, Hotfix distributions, operating system upgrades and Windows Update.

- System File Checker

  System File Checker, **sfc**, is a command-line tool that scans and verifies the versions of all protected system files after you restart your computer. System File Checker replaces overwritten files with the correct system files that are provided by Microsoft. It is part of the Windows File Protection feature of Windows Server 2003. System File Checker also checks and repopulates the Dllcache folder.

  If the Dllcache folder becomes damaged or unusable, use **sfc** with the **/purgecache** switch to repair its contents. Most .sys, .dll, .exe, .ttf, .fon, and .ocx files on the Windows Server 2003 compact disc are protected.

  The following table lists the various **sfc** switches and their descriptions.

Switch	Description
/scannow	Scans all protected system files immediately
/scanonce	Scans all protected system files at the next system start
/scanboot	Scans all protected system files at every start
/cancel	Cancels all pending scans of protected system files
/enable	Enables Windows File Protection for normal operation
/purgecache	Purges the file cache and scans all protected system files immediately
/cachesize=*x*	Sets the file cache size, in megabytes
/quiet	Replaces incorrect file versions without prompting the user
/?	Displays this list

Note To start a system file check, click **Start**, click **Run**, and then type **sfc /scannow**

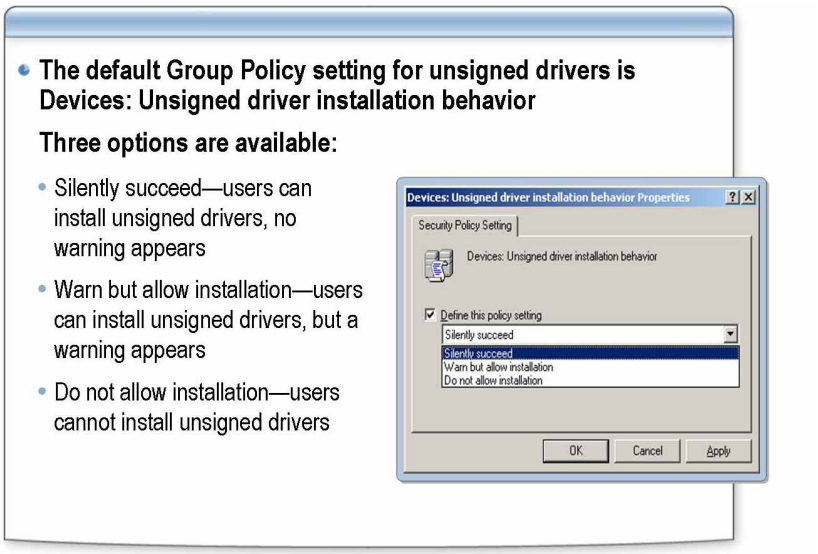
- File Signature Verification

  The system files and device driver files that are provided with Windows XP and the Windows Server 2003 family of products have a Microsoft digital signature. The digital signature indicates that the files are original, unaltered system files or that they are approved by Microsoft for use with Windows.

  By using File Signature Verification, you can identify signed and unsigned files on your computer and view the name, location, modification date, type, and version number.

  Note To start File Signature Verification, click **Start**, click **Run**, type **sigverif** and then click **OK**.

Group Policy Setting for Unsigned Device Drivers



Introduction

The Group Policy setting for unsigned device drivers is named **Devices: Unsigned driver installation behavior**. You can use it to allow users to install unsigned drivers, to warn users before they install unsigned device drivers, and to prevent users from installing unsigned device drivers.

Example of an unsigned driver

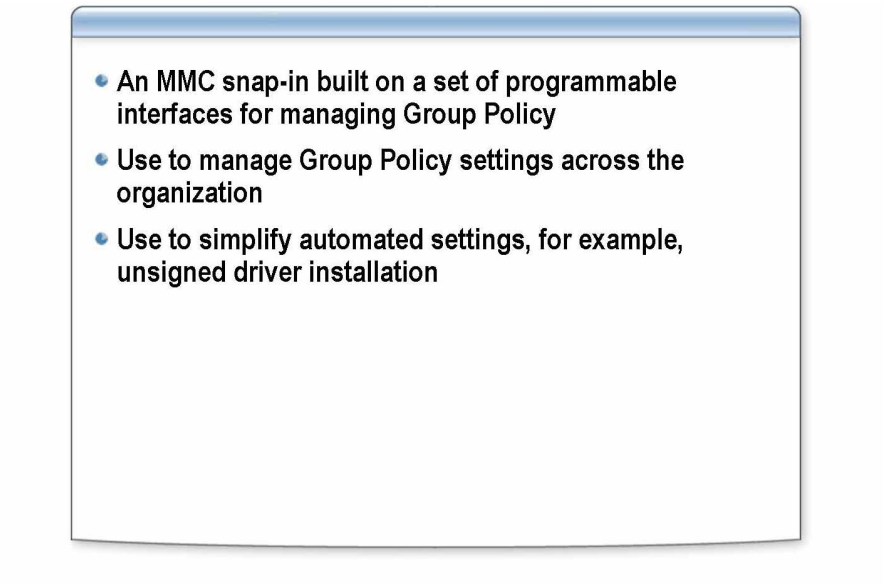
You are a systems administrator for an organization that does not allow users to install unsigned device drivers on their computers. The organization has over 1,000 computers, so enforcing this rule by manually configuring each computer is an impractical solution. The most efficient way to enforce this rule is to automate the setting by configuring Group Policy.

Group Policy options

The **Unsigned driver installation behavior** Group Policy setting has three options:

- *Silently succeed.* Allows the user to install an unsigned device driver without receiving a warning.
- *Warn but allow installation.* Allows the user to install an unsigned device driver, but a warning about installing unsigned device drivers is displayed.
- *Do not allow installation.* Prevents the installation of unsigned device drivers.

What Is Group Policy Management Console?



Definition

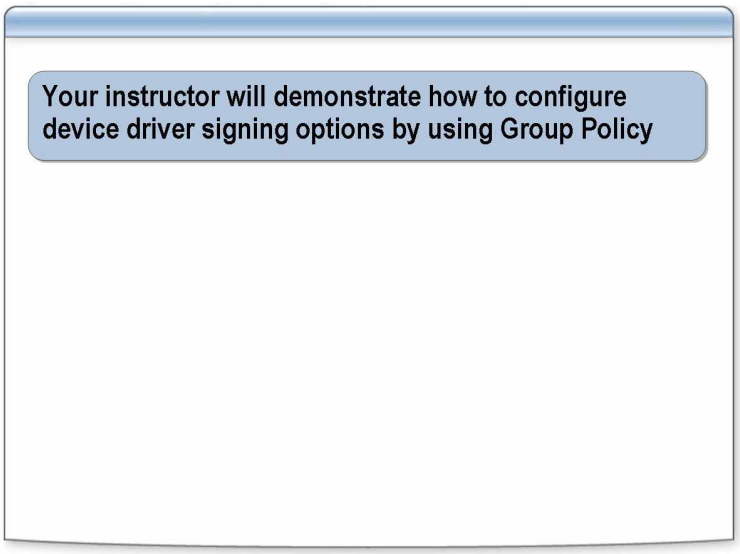
The Group Policy Management console is a set of programmable interfaces for managing Group Policy, as well as an MMC snap-in that is built on those programmable interfaces. Together, the components of the Group Policy Management console consolidate the management of Group Policy.

The Group Policy Management console lets you manage Group Policy for multiple domains and sites within one or more forests, all in a simplified user interface (UI) with drag-and-drop support.

Manage Group Policy settings for unsigned drivers

You can manage your Group Policy setting for unsigned device drivers for all the users in your organization by using the Group Policy Management console.

How to Configure Device Driver Signing Options by Using Group Policy



Introduction

This topic introduces how to configure device driver signing options by using the Group Policy Management Console.

Procedure

To configure device driver signing options using the Group Policy Management Console:

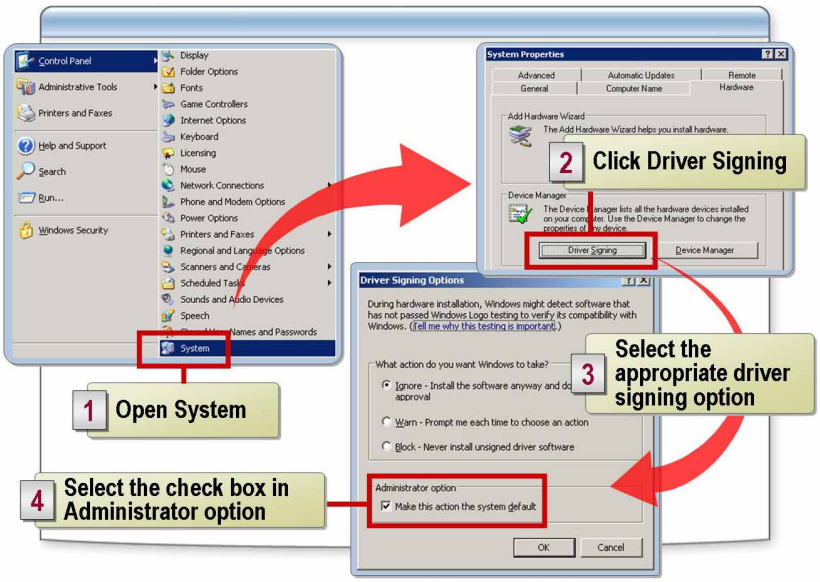
1. Create a snap-in for Active Directory® Users and Computers.
   a. Log on with your user account.
   b. On the **Start** menu, click **Run**.
   c. In the **Run** dialog box, in the **Open** box, type **runas /user:nwtraders\administrator mmc** and then click **OK**.
   d. When prompted for a password, type **P@ssw0rd** and then press ENTER.
   e. In the **Console1** window, click **File**, and then click **Add/Remove Snap-in**.
   f. In the **Add/Remove Snap-in** dialog box, click **Add**.
   g. In the **Add Standalone Snap-in** dialog box, click **Group Policy Management**, and then click **Add**.
   h. Click **Close**, and then click **OK**.

   Note If you are on a domain controller, click **Start**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.

2. In the Group Policy Management window, expand **Group Policy Management**, expand **Forest: nwtraders.msft**, expand **Domains**, expand **nwtraders.msft**, expand **Locations**, and then expand your *ComputerName* organizational unit.

3. Right-click your *ComputerName* organizational unit, and then click **Create and Link a GPO Here**.
4. In the **New GPO** dialog box, type *ComputerName* **Unsigned Device Driver Policy** and then click **OK**.
5. Expand *ComputerName*, right-click *ComputerName* **Unsigned Device Driver Policy**, and then click **Edit**.
6. In the console tree of the Group Policy Object Editor window, under **Computer Configuration**, expand **Windows Settings**, expand **Security Settings**, expand **Local Policies**, and then click **Security Options**.
7. In the details pane, double-click **Devices: Unsigned driver installation behavior**.
8. In the **Properties** dialog box for **Devices: Unsigned driver installation behavior**, select the **Define this policy setting** check box.
9. In the drop-down list, click **Do not allow installation**, and then click **OK**.
10. Close all windows.

How to Configure Device Driver Signing Options Manually



Introduction

Use the following procedure when you must manually configure a computer. For example, you are the systems administrator for the engineering department in a large organization. All the computers in the organization are configured by a policy that blocks the installation of unsigned device drivers. Software developers in your department need to test a new unsigned device driver that they developed. They cannot test the unsigned device driver because of the policy. You must manually configure their computers to allow the installation of unsigned device drivers.

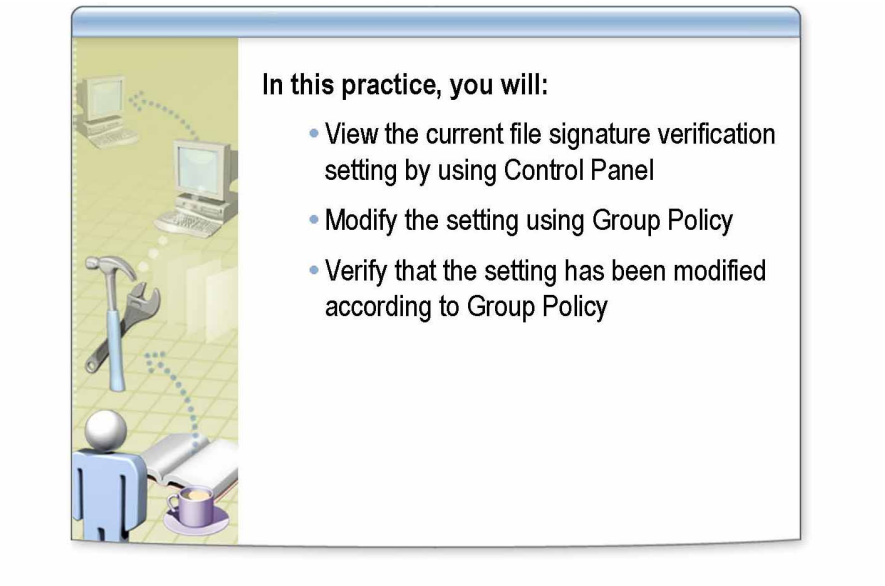
Procedure

To configure device driver signing options manually:

1. Click **Start**, click **Control Panel**, and then double-click **System**.
2. On the **Hardware** tab, click **Driver Signing**.
3. In the **Driver Signing Options** dialog box, in the **What action do you want Windows to take** box, select the appropriate option:
   a. Ignore–Install the software anyway and don't ask for my approval
   b. Warn–Prompt me each time to choose an action
   c. Block–Never install unsigned driver software
4. Under **Administration option**, select the **Make this action the system default** check box, and then click **OK**.

Note As an administrator, you can select the **Make this action the system default** check box to apply the selected setting as the default for all users who log on to this computer.

Practice: Configuring Device Driver Signing Options



Objective

In this practice, you will view the current file signature verification setting by using Control Panel. You will then use Group Policy to modify the setting and verify that the setting was modified.

Scenario

All device drivers must be signed, tested, and approved before users are allowed to install the device drivers on their computers. You will configure Group Policy to enforce the driver signing standards for all computers in the domain.

This practice is a simulation, which you will use as an interactive exercise. To complete this practice, you need the following:

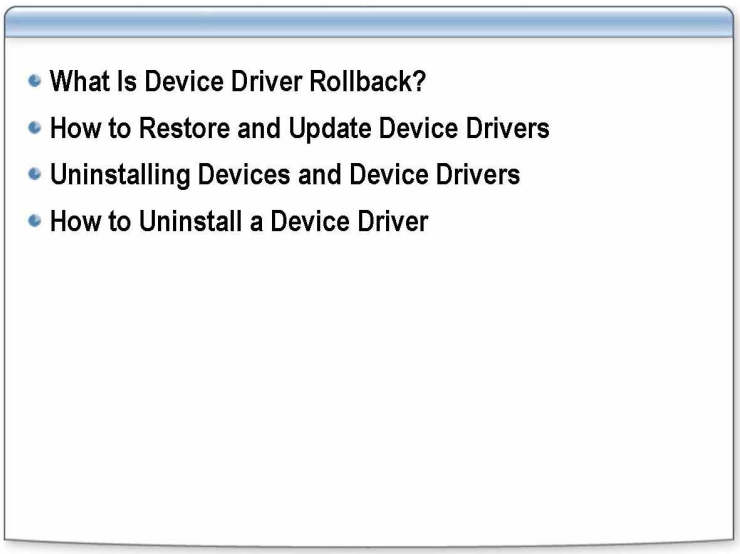
- A computer running Microsoft Windows Server 2003, Windows XP Professional, Windows 2000, Microsoft Windows NT® 4.0, Windows 98, or Windows 95.
- A minimum display resolution of 800 x 600 with 256 colors.

Practice

► **To start the simulation**

1. Insert the Student Materials compact disc into your CD-ROM drive.
2. At the root of the compact disc, double-click **Default.htm**.
3. On the Student Materials Web page, click **Multimedia**.
4. Click **Configuring Device Driver Signing Options**.
5. Read the introduction information, and then click the link to start the practice.

Lesson: Using Device Driver Rollback



Introduction

If a device stops functioning after you install an updated device driver for the device, you can use the Roll Back Driver feature to restore the previous version of the driver. By using this feature, you can avoid spending hours searching for a copy of the original driver that was installed. However, you cannot roll back a driver more than once.

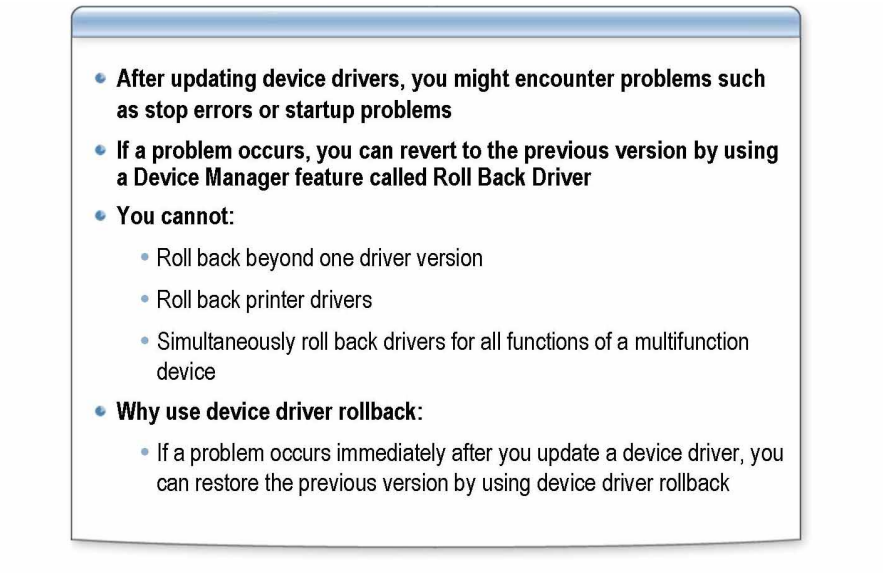
This lesson describes how to restore, update, and uninstall device drivers.

Lesson objectives

After completing this lesson, you will be able to:

- Explain device driver rollback.
- Restore a previous version of a device driver and update device driver.
- Describe the effects of uninstalling device drivers and devices.
- Uninstall a device driver.

What Is Device Driver Rollback?



Introduction

Updating one or more device drivers can cause problems. For example, a device can stop functioning, a stop error may be displayed, and startup problems can occur. To prevent problems from occurring after you upgrade a device driver, avoid using beta or unsigned device drivers. These device drivers might not be fully tested for compatibility with Windows Server 2003.

Why use device driver rollback?

If a problem occurs immediately after you update a device driver, you can restore the previous version by using the Roll Back Driver feature in Device Manager. If the problem prevents you from starting Windows Server 2003 in normal mode, you can roll back device drivers in safe mode.

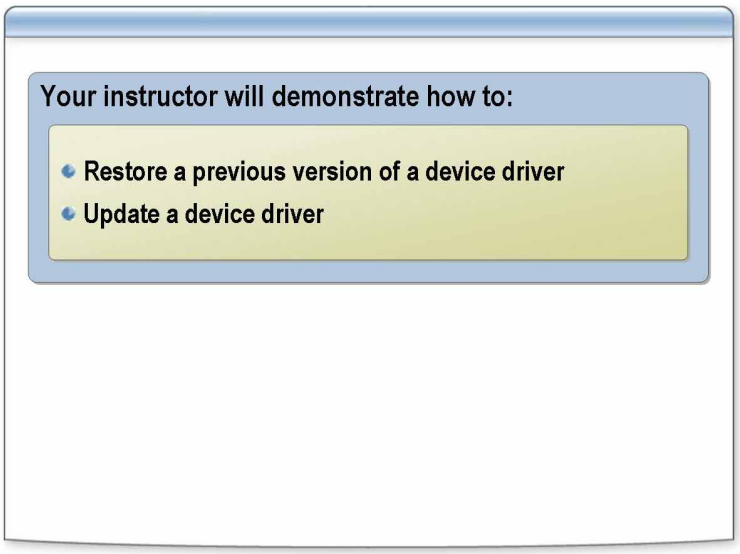
Note You must be logged on as an administrator or a member of the Administrators group to roll back a driver, or you must have been delegated this authority.

Driver rollback limitations

When using device driver rollback, be aware of the following limitations:

- You can roll back only one driver version. For example, you cannot restore the second to the last version of a driver.
- You cannot roll back printer drivers because Device Manager does not support or display printer properties.
- You cannot simultaneously roll back device drivers for all functions of a multifunction device. You must roll back each driver separately. For example, for a multifunction device that provides audio and modem functionality, you must roll back the modem driver and the audio driver separately.

How to Restore and Update Device Drivers



Introduction

This topic covers the procedures that you use to restore and update device drivers.

Procedure for restoring a device driver

As a systems administrator, you may need to restore a previous version of a driver. For example, a user complains that after he installed a new modem driver on his computer, his connection speed dropped from 56 kilobits per second (Kbps) to 14.4 Kbps. He wants you to restore the previous version of the driver.

To restore the previous version of a device driver:

1. Click **Start**, click **Control Panel**, double-click **System**, click **Hardware**, and then click **Device Manager**.

   Note Another way to open Device Manager is to click **Start**, right-click **My Computer**, click **Manage**, and then click **Device Manager**.

2. In Device Manager, double-click the type of device that you want to restore the device drivers for, right-click the device driver that you want to roll back to, and then click **Properties**.
3. On the **Driver** tab, click **Roll Back Driver**.
4. At the prompt, click **Yes** to confirm that you want to roll back to the previous driver.
   a. If the driver rollback process does not find a previous driver, the following message appears:

      "No driver files have been backed up for this device. If you are having problems with this device you should view the Troubleshooter information. Would you like to launch the Troubleshooter?"

   b. If you answer Yes, the Troubleshooter wizard guides you through a series of steps to help you troubleshoot your device.

Note If rolling back the device driver does not resolve the problem, you can use the Last Known Good Configuration or System Restore. For more information about Last Known Good Configuration and System Restore, see Module 7, "Managing Disaster Recovery," in Course 2275, *Maintaining a Microsoft Windows Server 2003 Environment.*

Procedure for updating device drivers

When hardware vendors develop new devices for computers, the device drivers that are initially included with the product are often rudimentary. A few months later, the hardware vendors often provide newer device drivers that are more stable and offer more features. As a systems administrator, you must visit the Web sites of hardware vendors to download the new device drivers and update your servers.

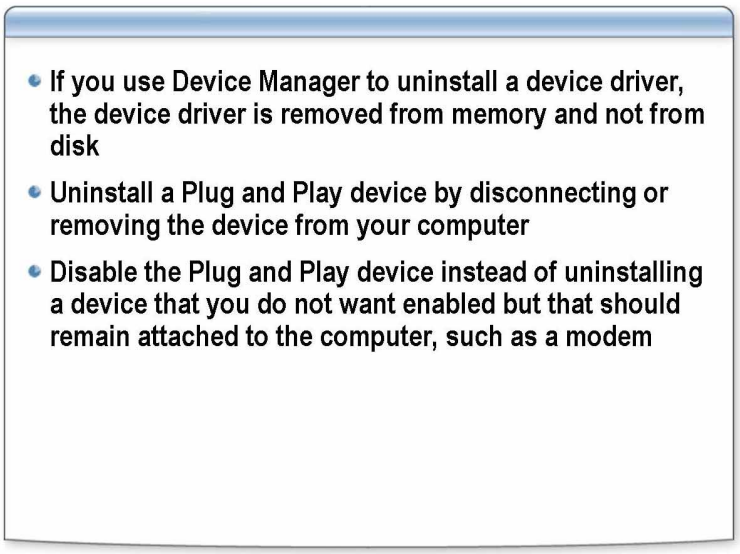
To update device drivers:

1. Click **Start**, click **Control Panel**, double-click **System**, click **Hardware**, and then click **Device Manager**.
2. In Device Manager, double-click the type of device that you want to update or change.
3. Right-click the specific device driver that you want to update or change, and then click **Update Driver**.
4. The Hardware Update Wizard appears. Follow the instructions.

Note Another way to gain access to the **Update Driver** button is to double-click the type of device driver that you want to update, and then on the **Driver** tab, click **Update Driver**.

Important To perform the preceding two procedures, you must have been delegated the appropriate authority. As a security best practice, consider using **Run as** to perform this procedure.

Uninstalling Devices and Device Drivers



Introduction

When you use Device Manager to uninstall a device driver, the device driver is removed from memory but not from the hard disk. Until you remove the device, Windows automatically reloads the driver the next time the computer is restarted.

Uninstalling a Plug and Play device

You uninstall a Plug and Play device by disconnecting or removing the device from your computer. Some devices, such as cards that plug into the motherboard, require that you turn off the computer first. To ensure that you uninstall a Plug and Play device properly, consult the device manufacturer's installation and removal instructions.

Uninstalling devices vs. disabling devices

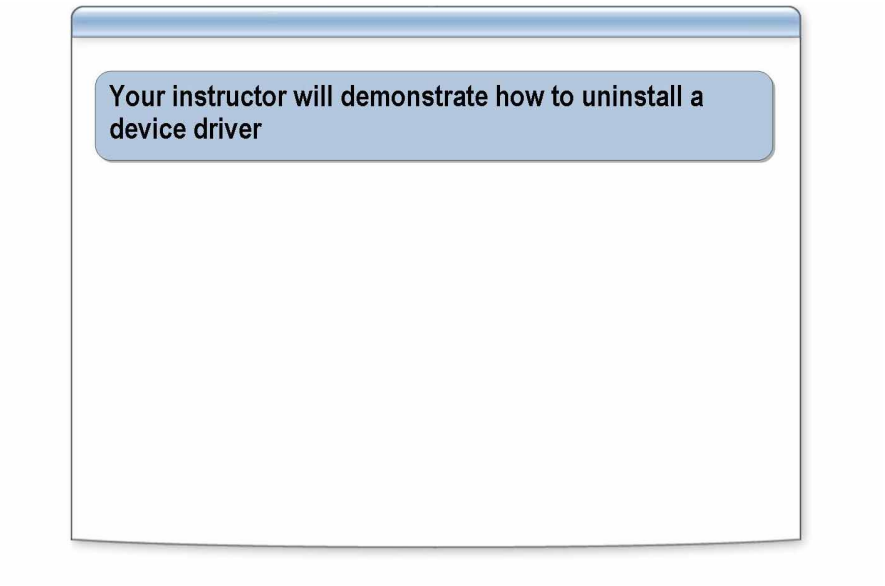
If you want a Plug and Play device to remain attached to a computer without being enabled, you can disable the device instead of uninstalling it.

When you disable a device, the device stays physically connected to your computer, but Windows updates the system registry so that the device drivers for the disabled device are no longer loaded when you start your computer. The device drivers are available again when you enable the device.

Disabling devices is useful if you must switch between two hardware devices, such as a networking card and a modem, or if you need to troubleshoot a hardware issue.

Note To enable or disable devices, open Device Manager, double-click the type of device that you want to enable or disable, right-click the specific device you want, and then click **Enable** or **Disable**.

How to Uninstall a Device Driver



Introduction

As a systems administrator, you may be required to uninstall device drivers. For example, one of the resource servers on the network is scheduled to be upgraded with new hardware devices. You must remove all of the old hardware devices on the server and uninstall the unnecessary device drivers. After removing the devices, you must use Device Manager to verify that all of the unnecessary device drivers are removed. If any unnecessary device drivers remain, you can use the **Uninstall** feature to remove them.

Procedure

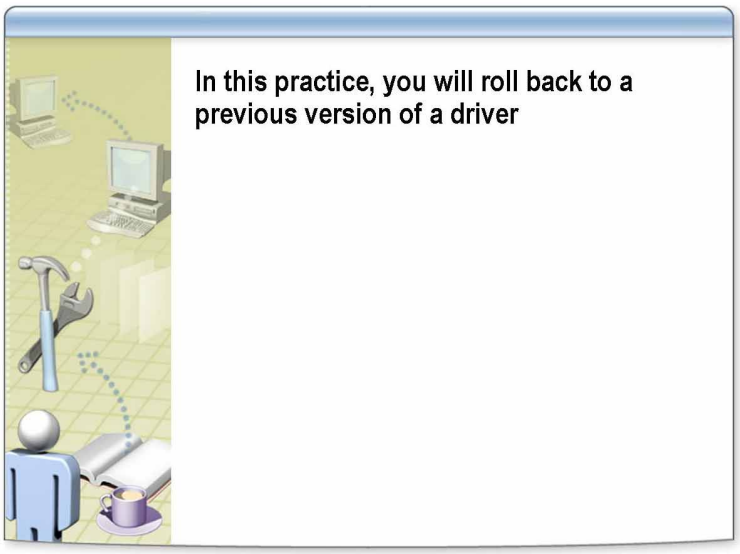
To uninstall a device driver:

1. To open Device Manager, click **Start**, click **Control Panel**, double-click **System**, click **Hardware**, and then click **Device Manager**.
2. Double-click the type of device you want to uninstall.
3. Right-click the specific device driver that you want to uninstall, and then click **Uninstall**.

Note Another way to gain access to the **Uninstall** button is to double-click the type of device driver that you want to uninstall, and then, on the **Driver** tab, click **Uninstall**.

4. In the **Confirm Device Removal** dialog box, click **OK**.
5. To verify that the devices are removed, open Device Manager, right-click the computer name, and then click **Scan for hardware changes**.

Practice: Using Device Driver Rollback



Objective

In this practice, you will roll back to a previous version of a device driver.

Scenario

You are the systems administrator for an organizational unit on a large network. A user in the organization downloaded an unsigned driver from the Internet and installed it, which has caused the mouse on the computer to stop working. You must roll back to the previous version of the driver.

Practice

► **Install the unsigned mouse driver**

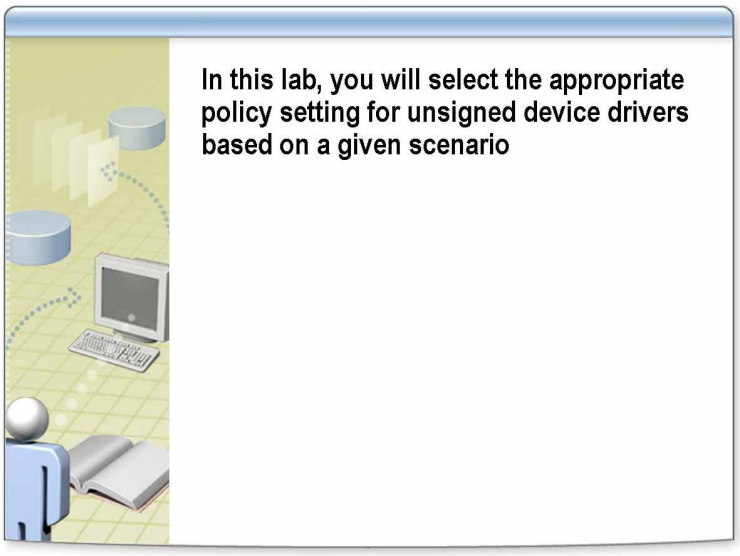
1. Log on to the **nwtraders** domain as *Computer***User** with a password of **P@ssw0rd**.
2. Open Control Panel and use **Run As** to open **System** with administrator privileges by holding down the SHIFT key, right-clicking **System**, and then clicking **Run as**.
3. Select **The following user**, type **nwtraders\administrator** and the administrator password in the respective boxes, and then click **OK**.
4. On the **Hardware** tab, click **Driver Signing**, and then set the driver-signing options to **Warn – Prompt me each time to choose an action**.
5. On the **Hardware** tab, click **Device Manager**, expand **Mice and other pointing devices**, right-click the mouse icon, and select **Update Driver**.

6. In the **Hardware Update Wizard**, install the mouse driver using the following parameters.

When prompted	Select
What do you want the wizard to do?	Install from a list or specific location
Please choose your search and installation options	Don't search. I will choose the driver to install.
Select the device driver you want to install for this hardware	Have Disk
Copy manufacturer's files from	Type: **C:\MOC\2275\Practices\Mod04**
Confirm Device Install	Yes
The software has not passed Windows Logo testing	Continue Anyway

7. Restart the computer if prompted.
8. Log on to the **nwtraders** domain as *Computer***User** with a password of **P@ssw0rd**.
9. Open Control Panel, and using Run As, open **System** with administrator privileges.
10. On the **Hardware** tab, click **Device Manager**, open the **Properties** dialog box for the mouse, and then review the driver date and version for the unsigned driver.
11. Roll back to the previous driver, and note the driver date and version.
12. Restart the computer if prompted.

Lab A: Maintaining Device Drivers



Objective

In this lab, you will select the appropriate policy setting for unsigned device drivers based on a given scenario.

Scenario

You are the systems administrator for an organizational unit on a network. All 500 users in the organization were issued laptop computers. You are concerned that some users may try to install unsigned device drivers that they find on the Internet. You must change the policy settings so that users are restricted when they try to install unsigned device drivers on their computers.

Estimated time to complete this lab: 15 minutes

Exercise 1
Viewing the Current File Signature Verification Setting

In this exercise, you will view the current file signature verification setting.

Tasks	Specific instructions
▪ Log on to the **nwtraders** domain.	**a.** Log on to the **nwtraders** domain as *Computer***User** with a password of **P@ssw0rd**. **b.** In Control Panel, open **System**, click the **Hardware** tab, and then view the default file signature verification setting.

Exercise 2
Modifying the Default Setting

In this exercise, you will modify default settings for all computers by using Group Policy Management Console.

Tasks	Specific instructions
▪ Start the Group Policy Management Console.	**a.** Use **runas** to start the Group Policy Manager snap-in with administrative privileges: **runas /user:nwtraders\administrator "mmc %windir%\system32\gpmc.msc"** **b.** Expand **Group Policy Management**, expand **Forest:nwtraders.msft**, expand **Domains**, expand **nwtraders.msft**, expand **Locations**, and then click your *ComputerName* organizational unit. **c.** Right-click *ComputerName,* create a new Group Policy object and name it *ComputerName* **Unsigned Device Driver Policy**. **d.** Right-click *ComputerName* **Unsigned Device Driver Policy** to edit the policy. **e.** In the Group Policy Object Editor window, under **Computer Configuration**, expand **Windows Settings**, expand **Security Settings**, expand **Local Policies**, and then click **Security Options**. **f.** Open the **Properties** dialog box for **Devices: Unsigned driver installation behavior**. **g.** Enable the **Define this policy setting**, click **Do not allow installation**, and then click **OK**. **h.** Close all windows.

Exercise 3
Adding a Computer to the Organizational Unit

In this exercise, you will add your computer to the appropriate Nwtraders organizational unit.

Tasks	Specific instructions
▪ Log on to the **nwtraders** domain.	**a.** Use **runas** to open a command prompt with administrative privileges. **b.** On the command line, type each of the following commands, and then press ENTER: **cd \MOC\2275\Practices\Mod04** **oumove** **c.** The computer restarts.

Exercise 4
Verifying the New File Signature Verification Setting

In this exercise, you will verify the new file signature verification setting.

Tasks	Specific instructions
1. Log on to the **nwtraders** domain.	**a.** Log on to the **nwtraders** domain as *Computer***User** with a password of **P@ssw0rd**. **b.** In Control Panel, open **System**, and then verify that the default file signature verification setting is set to **Block – Never install unsigned driver software**.
2. Close all windows.	▪ Close all windows and log off.