



# Windows Vista™

## **Step-By-Step Guide to Controlling Device Installation and Usage with Group Policy**

---

Microsoft Corporation

Published: July 2006

Author: Dave Bishop

Editor: Scott Somohano

Technical Reviewers: George Roussos, Emily Hill, Jim Cavalaris, Takashi Eto

### **Abstract**

By using the Microsoft® Windows Server® Code Name "Longhorn" and Windows Vista™ operating systems, administrators can determine which devices can be installed on computers they manage. The guide summarizes the device installation process and demonstrates several techniques for controlling the installation and usage of devices on managed computers.

**Microsoft**



This document supports a preliminary release of a software product that may be changed substantially prior to final commercial release, and is the confidential and proprietary information of Microsoft Corporation. It is disclosed pursuant to a non-disclosure agreement between the recipient and Microsoft. This document is provided for informational purposes only and Microsoft makes no warranties, either express or implied, in this document. Information in this document, including URL and other Internet Web site references, is subject to change without notice. The entire risk of the use or the results from the use of this document remains with the user. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2006 Microsoft Corporation. All rights reserved.

Microsoft, MS-DOS, Windows, Windows Server, Windows Vista, and Active Directory are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

References to any third-party products or their hardware identifiers are for illustrative purposes only. These products are not endorsed by Microsoft Corporation.

All other trademarks are property of their respective owners.



# Contents

---

|   |    |
|---|----|
| Step-By-Step Guide to Controlling Device Installation and Usage with Group Policy.....                | 7  |
| Who should use this guide? .....  | 8  |
| Benefits of controlling device installation using Group Policy .....                                  | 8  |
| Scenario overview .....   | 8  |
| Technology review.....  | 9  |
| Device installation in Windows .....  | 9  |
| Group Policy settings for device installation .....   | 12 |
| Group Policy settings for Removable Storage Access .....  | 15 |
| Requirements for completing the scenarios .....   | 18 |
| Prerequisite Procedures.....  | 19 |
| Responding to the User Account Control page .....   | 19 |
| Determining the device identification strings for your USB memory drive.....                          | 20 |
| Uninstalling your USB memory drive .....  | 25 |
| Prevent installation of all devices .....   | 26 |
| Prerequisites for preventing installation of all devices .....  | 26 |
| Steps for preventing installation of all devices .....  | 27 |
| Step 1: Configure policy to prevent installation of any device.....                                   | 27 |
| Step 2: Configure policy to allow administrators to override device installation<br>restrictions..... | 28 |
| Step 3: Test the effects of your restriction settings as a user .....                                 | 29 |
| Allow users to install only authorized devices .....  | 32 |
| Prerequisites for allowing users to install only authorized devices .....                             | 32 |
| Steps for allowing users to install only authorized devices .....                                     | 32 |
| Step 1: Create a list of authorized devices.....  | 33 |
| Step 2: Test the list of authorized devices .....   | 35 |
| Prevent installation of prohibited devices .....  | 37 |
| Prerequisites for preventing installation of prohibited devices .....                                 | 37 |
| Steps for preventing installation of prohibited devices.....  | 39 |
| Step 1: Create a list of prohibited devices.....  | 39 |
| Step 2: Test the list of prohibited devices .....   | 41 |
| Control read and write permissions on removable media .....   | 44 |
| Prerequisites for controlling read and write permissions on removable media.....                      | 45 |
| Steps for controlling read and write permissions on removable media .....                             | 45 |
| Step 1: Set computer policy to deny write access to specific removable device<br>classes .....        | 45 |

|  |    |
|--|----|
| Step 2: Test your computer policy settings ..... | 46 |
| Conclusion .....                                 | 48 |
| Logging bugs and feedback .....                  | 48 |
| Additional resources .....                       | 48 |

# Step-By-Step Guide to Controlling Device Installation and Usage with Group Policy

---

This step-by-step guide describes how you can control the installation and usage of devices on the computers that you manage. Specifically, in Microsoft® Windows Server® Code Name "Longhorn" and Windows Vista™ you can apply computer policy to:

- Prevent users from installing any device.
- Allow users to install only devices that are on an "approved" list. If a device is not on the list, then the user cannot install it.
- Prevent users from installing devices that are on a "prohibited" list. If a device is not on the list, then the user can install it.
- Deny read or write access to users for devices that are themselves removable, or that use removable media, such as CD and DVD burners, floppy disk drives, external hard drives, and portable devices such as media players, smart phones, or Pocket PC devices.

This guide describes the device installation process and introduces the identification strings that Windows uses to match a device with the device driver packages available on a computer. The guide also illustrates three methods of controlling device installation. Each scenario shows, step by step, one method you can use to allow or prevent the installation of a specific device or a class of devices. The fourth scenario shows how to deny read or write access to users for devices that are removable or that use removable media.

The example device used in the scenarios is a USB storage device. You can perform the steps in this guide using a different device. However, if you use a different device, then the instructions in the guide will not exactly match the user interface that appears on the computer.

## Important

The steps provided in this guide are intended for use in a test lab environment. This step-by-step guide is not meant to be used to deploy Windows Server features without accompanying documentation and should be used with discretion as a stand-alone document.

## Who should use this guide?

This guide is targeted at the following audiences:

- Information technology planners and analysts who are evaluating Windows Vista and Windows Server "Longhorn"
- Enterprise information technology planners and designers
- Security architects who are responsible for implementing trustworthy computing in their organization
- Administrators who want to become familiar with the technology

## Benefits of controlling device installation using Group Policy

Restricting the devices that users can install provides the following benefits:

- **Reduce the risk of data theft.** It is more difficult for users to make unauthorized copies of company data if users' computers cannot install unapproved devices that support removable media. For example, if users cannot install a CD-R device, they cannot burn copies of company data onto a recordable CD. This benefit cannot eliminate data theft, but it creates another barrier to unauthorized removal of data. You can also reduce the risk of data theft by using Group Policy to deny write access to users for devices that are removable or that use removable media. You can grant access on a per-group basis when you use Group Policy.
- **Reduce support costs.** You can ensure that users install only those devices that your help desk is trained and equipped to support. This benefit reduces support costs and user confusion.

## Scenario overview

The scenarios presented in this guide illustrate how you can control device installation and usage on the computers that you manage. The scenarios use Group Policy on a local computer to simplify using the procedures in a lab environment. In an environment where you manage multiple client computers, you should apply these settings using Group Policy deployed by Active Directory. With Group Policy deployed by Active Directory, you can apply settings to all computers that are members of a domain or an organizational unit in a domain. For more information about how to use Group Policy to manage your client computers, see "Group Policy" at the Microsoft Web site (<http://go.microsoft.com/fwlink/?linkid=55625>).

Following are descriptions of the scenarios presented in this guide:

- **Prevent installation of all devices.**

In this scenario, the administrator wants to prevent standard users from installing any device, but allow administrators to install or update devices. To complete this scenario, you configure two computer policies. The first computer policy prevents all users from installing devices, and the second policy exempts administrators from the restrictions.

- **Allow users to install only authorized devices.**

In this scenario, the administrator wants to allow users to install only the devices included on a list of authorized devices. This scenario builds on the first scenario and therefore you must complete the first scenario before attempting this scenario. To complete this scenario, you create a list of authorized devices so that users can install only those devices that you specify.

- **Prevent installation of only prohibited devices.**

In this scenario, the administrator wants to allow standard users to install most devices but prevent them from installing devices included on a list of prohibited devices. To complete this scenario, you must remove the policies that you created in the first two scenarios. After you have removed those policies, you create a list of prohibited devices so that users can install any device except those that you specify.

- **Control the use of removable media storage devices**

In this scenario, the administrator wants to prevent standard users from writing data to removable storage devices, or devices with removable media, such as a USB memory drive or a CD or DVD burner. To complete this scenario, you configure a computer policy to allow read access, but deny write access to your sample device and to any CD or DVD burner device on your computer.

## Technology review

The following sections provide a brief overview of the core technologies discussed in this guide.

### Device installation in Windows

A device is a piece of hardware with which Windows interacts to perform some function. Windows can communicate with a device only through a piece of software called a device

driver. To install a device driver, Windows detects the device, recognizes its type, and then finds the device driver that matches that type.

Windows uses two types of identifiers to control device installation and configuration. You can use the Group Policy settings in Windows Vista and Windows Server "Longhorn" to specify which of these identifiers to allow or block.

The two types of identifiers are:

- Device identification strings
- Device setup classes

### **Device identification strings**

When Windows detects a device that has never been installed on the computer, the operating system queries the device to retrieve its list of device identification strings. A device usually has multiple device identification strings, which the device manufacturer assigns. The same device identification strings are included in the .inf file that is part of the device driver package. Windows chooses which device driver package to install by matching the device identification strings retrieved from the device to those included with the driver packages.

Windows can use each string to match a device to a driver package. The strings range from the very specific, matching a single make and model of a device, to the very general, possibly applying to an entire class of devices. There are two types of device identification strings:

- **Hardware IDs.** Hardware IDs are the identifiers that provide the most exact match between a device and a driver package. The first string in the list of hardware IDs is referred to as the device ID, because it matches the exact make, model, and revision of the device. The other hardware IDs in the list match the details of the device less exactly. For example, a hardware ID might identify the make and model of the device but not the specific revision. This scheme allows Windows to use a driver for a different revision of the device, if the driver for the correct revision is not available.
- **Compatible IDs.** Windows uses these identifiers to select a device driver if the operating system cannot find a match with the device ID or any of the other hardware IDs. Compatible IDs are listed in the order of decreasing suitability. These strings are optional, and, when provided, they are very generic, such as **Disk**. When a match is made using a compatible ID, you can typically use only the most basic functions of the device.

When you install a device, such as a printer, a USB storage device, or a keyboard, Windows searches for driver packages that match the device you are attempting to install. During this search, Windows assigns a "rank" to each driver package it discovers

with at least one match to a hardware or compatible ID. The rank indicates how well the driver matches the device. Lower rank numbers indicate better matches between the driver and the device. A rank of zero represents the best possible match. A match with the device ID to one in the driver package results in a lower (better) rank than a match to one of the other hardware IDs. Similarly, a match to a hardware ID results in a better rank than a match to any of the compatible IDs. After Windows ranks all of the driver packages, it installs the one with the lowest overall rank. For more information about the process of ranking and selecting driver packages, see "How Setup Selects Drivers" at the Microsoft Web site (<http://go.microsoft.com/fwlink/?LinkId=54881>). For more information about the device driver installation process, see the "Technology review" section of the "Step-by-Step Guide to Device Driver Signing and Staging" at the Microsoft Web site (<http://go.microsoft.com/fwlink/?LinkID=69208>).

Some physical devices create one or more logical devices when they are installed. Each logical device might handle part of the functionality of the physical device. For example, a multi-function device, such as an all-in-one scanner/fax/printer, might have a different device identification string for each function.

When you use device installation restriction policies to allow or prevent the installation of a device that uses logical devices, you must allow or prevent all of the device identification strings for that device. For example, if a user attempts to install a multifunction device and you did not allow or prevent all of the identification strings for both physical and logical devices, you could get unexpected results from the installation attempt. For more detailed information about hardware IDs, see "Device Identification Strings" at the Microsoft Web (<http://go.microsoft.com/fwlink/?linkid=52665>).

### **Device setup classes**

Device setup classes are another type of identification string. The manufacturer assigns the device setup class to a device in the device driver package. The device setup class groups devices that are installed and configured in the same way. For example, all CD drives belong to the CDROM device setup class, and they use the same co-installer when installed. A long number called a globally unique identifier (GUID) represents each device setup class. When Windows starts, it builds an in-memory tree structure with the GUIDs for all of the detected devices. Along with the GUID for the device setup class of the device itself, Windows may need to insert into the tree the GUID for the device setup class of the bus to which the device is attached.

When you use device setup classes to allow or prevent users from installing device drivers, you must specify the GUIDs for all of the device's device setup classes, or you might not achieve the results you want. The installation might fail (if you want it to succeed) or it might succeed (if you want it to fail).

For example, a multi-function device, such as an all-in-one scanner/fax/printer, has a GUID for a generic multi-function device, a GUID for the printer function, a GUID for the scanner function, and so on. The GUIDs for the individual functions are "child nodes" under the multi-function device GUID. To install a child node, Windows must also be able to install the parent node. You must allow installation of the device setup class of the parent GUID for the multi-function device in addition to any child GUIDs for the printer and scanner functions.

For more information, see "Device Setup Classes" at the Microsoft Web site (<http://go.microsoft.com/fwlink/?LinkId=52662>).

This guide does not depict any scenarios that use device setup classes. However, the basic principles demonstrated with device identification strings in this guide also apply to device setup classes. After you discover the device setup class for a specific device, you can then use it in a policy to either allow or prevent installation of device drivers for that class of devices.

## Group Policy settings for device installation

To enable control over device installation, Windows Vista and Windows Server "Longhorn" introduce several policy settings. You can configure these policy settings individually on a single computer, or you can apply them to a large number of computers through the use of Group Policy in an Active Directory domain. For more information about how to use Group Policy to manage your client computers, see "Group Policy" at the Microsoft Web site (<http://go.microsoft.com/fwlink/?linkid=55625>).

Whether you want to apply the settings to a stand-alone computer or to many computers in an Active Directory domain, you use the Group Policy Object Editor to configure and apply the policy settings. For more details, see "Group Policy Object Editor Technical Reference" at the Microsoft Web site (<http://go.microsoft.com/fwlink/?LinkId=56390>).

The following is a brief description of the device installation policy settings that are used in this guide.

### Note

These policy settings affect all users who log on to the computer where the policy settings are applied. You cannot apply these policies to specific users or groups except for the policy **Allow administrators to override device installation policy**. This policy exempts members of the local Administrators group from any of the device installation restrictions that you apply to the computer by configuring other policy settings as described in this section.

- **Prevent installation of devices not described by other policy settings.** This policy setting controls the installation of devices that are not specifically described by any other policy setting. If you enable this policy setting, users cannot install or update the driver for devices unless they are described by either the **Allow installation of devices that match these device IDs** policy setting or the **Allow installation of devices for these device classes** policy setting. If you disable or do not configure this policy setting, users can install and update the driver for any device that is not described by the **Prevent installation of devices that match these device IDs** policy setting, the **Prevent installation of devices for these device classes** policy setting, or the **Prevent installation of removable devices** policy setting.
- **Allow administrators to override device installation policy.** This policy setting allows members of the local Administrators group to install and update the drivers for any device, regardless of other policy settings. If you enable this policy setting, administrators can use the Add Hardware Wizard or the Update Driver Wizard to install and update the drivers for any device. If you disable or do not configure this policy setting, administrators are subject to all policy settings that restrict device installation.
- **Prevent installation of devices that match these device IDs.** This policy setting specifies a list of Plug and Play hardware IDs and compatible IDs for devices that users cannot install. If you enable this policy setting, users cannot install or update the driver for a device if any of its hardware IDs or compatible IDs match one in this list. If you disable or do not configure this policy setting, users can install devices and update their drivers, as permitted by other policy settings for device installation.

 **Note**

This policy setting takes precedence over any other policy settings that allow users to install a device. This policy setting prevents users from installing a device even if it matches another policy setting that would allow installation of that device.

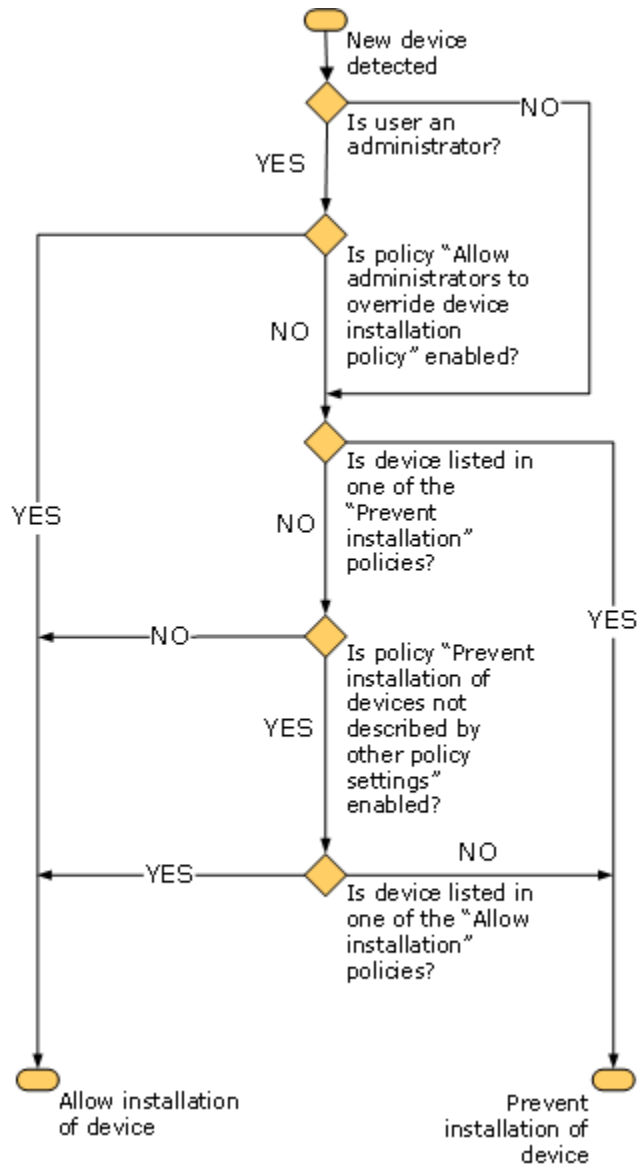
- **Prevent installation of drivers matching these device setup classes.** This policy setting specifies a list of Plug and Play device setup class GUIDs for devices that users cannot install. If you enable this policy setting, users cannot install or update drivers for a device that belongs to any of the listed device setup classes. If you disable or do not configure this policy setting, users can install and update drivers for devices as permitted by other policy settings for device installation.

 **Note**

This policy setting takes precedence over any other policy settings that allow users to install a device. This policy setting prevents users from installing a device from being installed even if it matches another policy setting that would allow installation of that device.

- **Allow installation of devices that match any of these device IDs.** This policy setting specifies a list of Plug and Play hardware IDs and compatible IDs that describe devices that users can install. This setting is intended to be used only when the **Prevent installation of devices not described by other policy settings** policy setting is enabled and does not take precedence over any policy setting that would prevent users from installing a device. If you enable this policy setting, users can install and update any device with a hardware ID or compatible ID that matches an ID in this list if that installation has not been specifically prevented by the **Prevent installation of devices that match these device IDs** policy setting, the **Prevent installation of devices for these device classes** policy setting, or the **Prevent installation of removable devices** policy setting. If another policy setting prevents users from installing a device, users cannot install it even if the device is also described by a value in this policy setting. If you disable or do not configure this policy setting and no other policy describes the device, the **Prevent installation of devices not described by other policy settings** policy setting determines whether users can install the device.
- **Allow installation of devices using drivers for these device classes.** This policy setting specifies a list of device setup class GUIDs that describe devices that users can install. This setting is intended to be used only when the **Prevent installation of devices not described by other policy settings** policy setting is enabled and does not take precedence over any policy setting that would prevent users from installing a device. If you enable this setting, users can install and update any device with a device setup class that matches one of the device setup class GUIDs in this list if that installation has not been specifically prevented by the **Prevent installation of devices that match these device IDs** policy setting, the **Prevent installation of devices for these device classes** policy setting, or the **Prevent installation of removable devices** policy setting. If another policy setting prevents users from installing a device, users cannot install it even if the device is also described by a value in this policy setting. If you disable or do not configure this policy setting and no other policy setting describes the device, the **Prevent installation of devices not described by other policy settings** policy setting determines whether users can install the device.

Some of these policies take precedence over other policies. The flowchart shown below illustrates how Windows processes them to determine whether a user can install a device or not:



### Group Policy settings for Removable Storage Access

In Windows Vista and Windows Server "Longhorn" an administrator can apply Group Policy to control whether users can read from or write to any device with removable

media. These policies can be used to help prevent sensitive or confidential material from being written to removable media or to a removable device containing storage, and then carried away from the premises.

You can apply these policy settings at the computer level so they affect every user who logs on to the computer. You can also apply them at the user level and limit enforcement to a specific user account. If you use Group Policy in an Active Directory environment, you can apply the policy settings to user groups in addition to single user accounts. Group Policy also allows you to effectively apply these policies to large numbers of computers. For more information about how to use Group Policy to manage your client computers, see "Group Policy" at the Microsoft Web site (<http://go.microsoft.com/fwlink/?linkid=55625>).

#### **Important**

These removable storage access policies do not affect software that runs in the System account context, such as the ReadyBoost technology in Windows. However, any software that runs under the security context of the current user might be affected by these restrictions. For example, if the **Removable Disks: Deny write access** policy setting is in effect for a user, even if that user is an administrator, then the BitLocker setup program cannot write its startup key to a USB drive. You might want to consider applying the restrictions to only users and groups other than the local Administrators group.

The **Removable Storage Access** policy settings also include a setting to allow an administrator to force a reboot. If a device is in use when a restricting policy is applied, the policy might not be enforced until the computer is restarted. Use the policy setting to force a restart if you do not want to wait until the next time the user restarts the computer. If the restricting policies can be enforced without restarting the computer, then the reboot option is ignored.

The policy settings can be found in two locations. The policy settings found in **Computer Configuration\Administrative Templates\System\Removable Storage Access** affect a computer and every user who logs on to it. The policy settings found in **User Configuration\Administrative Templates\System\Removable Storage Access** affect only the users to whom the policy setting is applied, including groups if Group Policy is applied using Active Directory.

The following is a brief description of the policies that enable you to control read or write access to removable storage drives. Each device category supports two policies: one to deny read access, and one to deny write access:

- **Time (in seconds) to force reboot.** Set the amount of time (in seconds) that the system will wait to restart in order to enforce a change in access rights to removable

storage devices. The restart is only forced if the restricting policies cannot be applied without it.

 **Note**

If no restart is forced and the policies cannot be applied due to the device being in use, then the change does not take effect until the system is restarted. If the policy change affects multiple devices, the change is enforced immediately on all devices that are not currently in use. If any of the affected devices are in use so that the change cannot be immediately enforced, then this policy to restart the computer will be enforced, if it was enabled by the administrator.

- **CD and DVD.** These policy settings allow you to deny read or write access to devices in the CD and DVD removable storage class, including USB connected devices.

 **Important**

Some third-party CD and DVD burner software interact with the hardware in a way that is not prevented by the policy. If you want to prevent all writing to CD or DVD burners, you might want to consider applying Group Policy to prevent the installation of that software.

- **Custom Classes.** These policy settings allow you to deny read or write access to any device whose Device Setup Class GUID is found in the lists you provide.
- **Floppy Drives.** These policy settings allow you to deny read or write access to devices in the Floppy Drive class, including USB connected devices.
- **Removable Disks.** These policy settings allow you to deny read or write access to removable devices that either are or emulate hard disks, such as USB memory drives or external USB hard disk drives.
- **Tape Drives.** These policy settings allow you to deny read or write access to tape drives, including USB connected devices.
- **WPD Devices.** These policy settings allow you to deny read or write access to devices in the Windows Portable Device class. These devices include "smart" devices, such as media players, mobile phones, Windows CE devices, etc.
- **All Removable Storage classes: Deny all access.** This policy setting takes precedence over any of the policy settings in this list, and if enabled, denies read and write access to any device that is identified as using removable storage. If you disable, or do not configure this policy setting, then read and write access to removable storage classes are allowed, subject to any restrictions imposed by the other policy settings in this list.

## Requirements for completing the scenarios

To complete each of the scenarios, you must have:

- A client computer running Windows Vista. This guide refers to this computer as **DMI-Client1**.
- A USB memory drive. The scenarios described in this guide use a USB memory drive as the example device. This device acts like a removable disk drive and is also known as a "thumb drive," a "flash drive," or a "keyring drive." Most USB memory drives do not require any manufacturer-provided drivers, and these devices work with the drivers provided with Windows Vista and Windows Server "Longhorn".

 **Note**

The instructions assume that your device does not require any drivers other than the drivers that are included with Windows Vista and Windows Server "Longhorn". If your device requires a driver from the manufacturer, you must provide the driver file when Windows prompts you to do so. This step is not included in the scenarios.

- (Optional) A CD or DVD burner. The last scenario demonstrates how to make devices with removable media read-only. You can set the computer policy without actually having a CD or DVD burner installed. However, if you want to verify that the computer policy is effective then you must have a CD or DVD burner device to use.
- Access to a protected administrator account on **DMI-Client1**. This guide calls this account **TestAdmin**. The procedures in this guide require administrator privileges for most steps. You must be logged into DMI-Client1 using this administrator account at the beginning of each procedure, unless you are directed otherwise.

 **Note**

Windows Vista and Windows Server "Longhorn" introduce the concept of a protected administrator account. This account is a member of the Administrators group, but by default that security privilege is not directly used. Any attempt to carry out a task that requires the elevated rights of an administrator generates a dialog box asking for permission to perform that task. This dialog box is discussed in the "[Responding to the User Account Control page](#)" section later in this guide. Microsoft recommends that you use a protected administrator account, rather than the built-in Administrator account whenever possible.

- Access to a standard user account on **DMI-Client1**. This user account has no special memberships that grant any kind of elevated permissions. This guide calls this

account **TestUser**. Only log on to your computer with this account when instructed to do so. With a standard user account, any attempt to carry out a task that requires the elevated rights of an administrator can cause a dialog box requesting the credentials of an account with administrator privileges. This dialog box is discussed in the "[Responding to the User Account Control page](#)" section later in this guide.

## Prerequisite Procedures

Before you can implement any policy for allowing or preventing users from installing a device, you must know the device identification strings for the device. You must also know how to completely uninstall your USB memory drive and its associated driver. The following procedures configure your computer to successfully execute the scenarios in this guide:

1. [Responding to the User Account Control page](#)
2. [Determining the device identification strings for your USB memory drive](#)
3. [Uninstalling your USB memory drive](#)

## Responding to the User Account Control page

Throughout this guide you are asked to perform tasks that can only be done by a member of the Administrators group. In Windows Vista and Windows Server "Longhorn", when you attempt to perform a task that requires administrator rights, the following occurs:

- If you are logged in as the built-in Administrator account (not recommended) then the operation simply proceeds. The built-in administrator account is disabled by default.
- If you are a member of the Administrators group that is not the built-in Administrator account, then a **User Account Control** dialog appears asking for permission to continue. If you click **Continue**, the task proceeds.
- If you are logged on as a standard user, then you could be prevented from doing the task. Depending on the task, you can be presented with a **User Account Control** page to provide the user name and password for an administrator account. If you provide valid credentials, then the task runs in the security context of the administrator account you provided. If you cannot provide those credentials, then you are prevented from performing the task.

### Important

Before providing credentials or permissions to run any administrative task, ensure that the **User Account Control** page is displayed in response to a task

that you initiated. If the page appears unexpectedly, then click the **Details** button and ensure that the task that is one you wish to allow.

This guide does not document every occurrence of the **User Account Control** dialog box that you will encounter in performing these procedures. When special steps are required to run specific tasks as administrator, those steps are documented in the guide.

## Determining the device identification strings for your USB memory drive

By following these steps, you can determine the device identification strings for your device. If the hardware IDs and compatible IDs for your device do not match those shown in this guide, use the IDs that are appropriate to your device.

### **Note**

In the following scenarios, you must install and then uninstall your USB memory drive. The instructions assume that your device does not require any drivers other than the drivers that are included with Windows Vista and Windows Server "Longhorn". If your device requires a driver from the manufacturer, you must provide the driver file when Windows prompts you to do so. This step is not included in the scenarios.

You can determine the hardware IDs and compatible IDs for your device in two ways. You can use Device Manager, a graphical tool included with the operating system, or DevCon, a command-line tool available for download as part of the Driver Development Kit (DDK). Use the following procedure to view the device identification strings for your USB memory drive.

### **Important**

These procedures are specific to a USB memory drive. If you are using a different type of device, you must adjust the steps accordingly. The significant difference will be the location of the device in the Device Manager hierarchy. Instead of being located in the **Disk Drives** node, you must locate your device in the appropriate node.

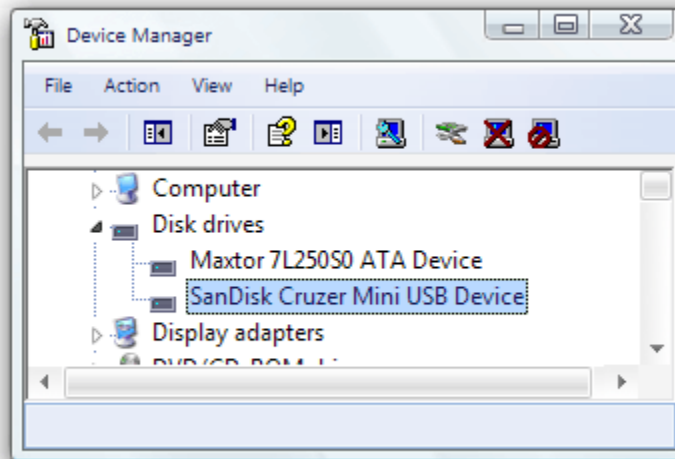
### **To find device identification strings using Device Manager**

1. Log on to your computer as **DMI-Client1\TestAdmin**.
2. Plug in your USB memory drive, and then allow installation to complete.
3. To open Device Manager, click the **Start** button, type **mmc devmgmt.msc** in the **Start Search** box, and then press **ENTER**.

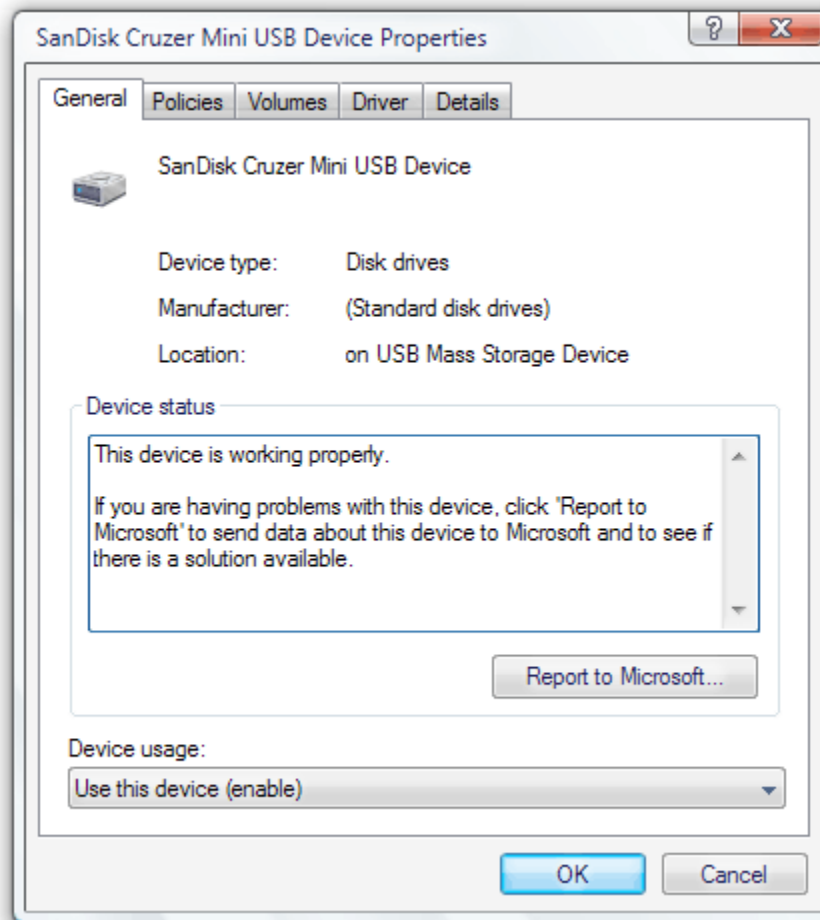
4. If the **User Account Control** dialog box appears, confirm that the action it displays is what you want, and then click **Continue**.

Device Manager starts and displays a tree representing all of the devices detected on your computer. At the top of the tree is a node with your computer's name next to it. Lower nodes represent the various categories of hardware into which your computer's devices are grouped.

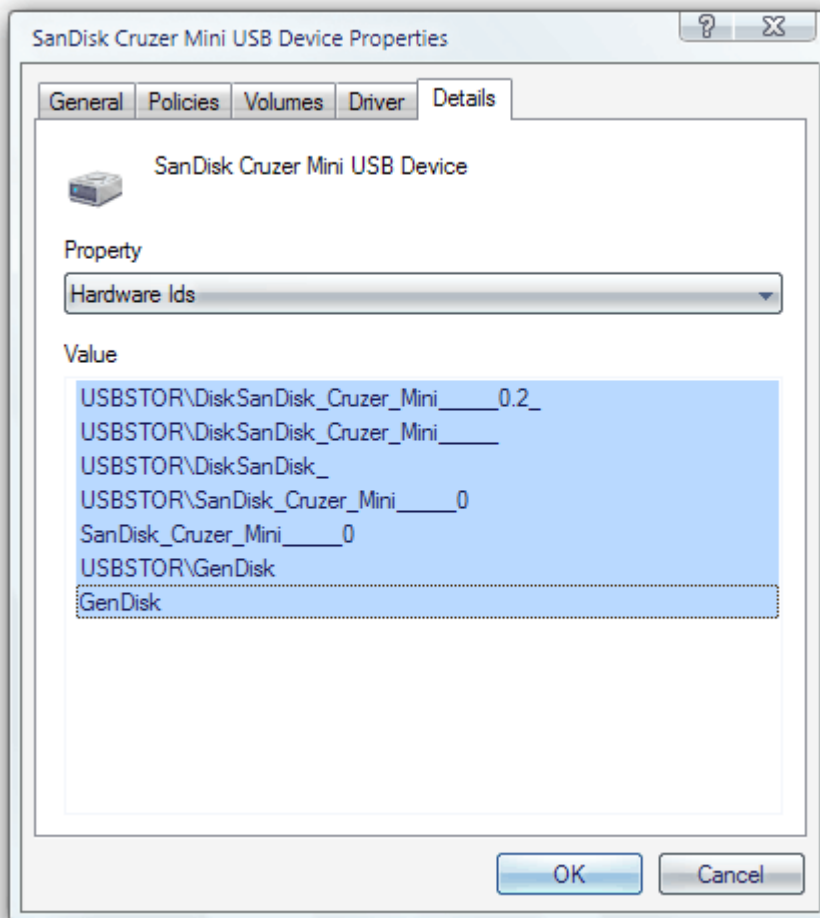
5. Double-click **Disk drives** to open the list.



6. Right-click the entry for your USB memory drive, and then click **Properties**.  
The **Device Properties** dialog box appears.



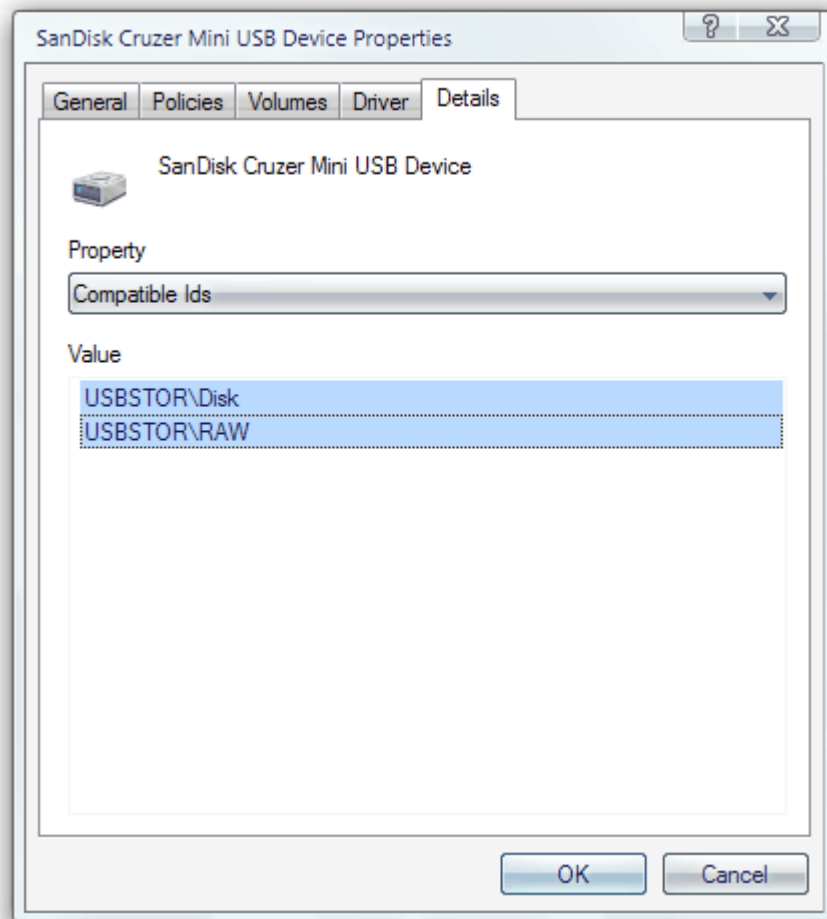
7. Click the **Details** tab.
8. In the **Property** list, click **Hardware Ids**.  
Under **Value**, make note of the strings displayed.



 **Note**

You can copy the strings to the Clipboard by highlighting the text and pressing CTRL-C. Because many hardware IDs have multiple underscore characters, it is helpful to copy them to a text file from which you can paste when you must specify an identifier. This approach greatly reduces the chance of an error when you must add a specific identifier to a list of approved or prohibited devices.

9. In the **Property** list, click **Compatible Ids**.  
Under **Value**, make note of the strings displayed.



10. Click **OK** to close the dialog box.

 **Note**

You can also determine your device identification strings using the DevCon command-line utility. You can download DevCon from the Microsoft Help and Support site. For more information, see "The DevCon command-line utility functions as an alternative to Device Manager" at the Microsoft Web site (<http://go.microsoft.com/fwlink/?LinkId=56391>).

You can find additional details about the DevCon utility and its operation on the Microsoft Developer Network (MSDN) site. For more information, see "DevCon" at the Microsoft Web site ().

The specific syntax needed to use DevCon to determine your hardware IDs is also on MSDN. For more information, see "DevCon HwIDs" at the Microsoft Web site ([http://msdn.microsoft.com/en-us/library/aa393071.aspx](#)).

## Uninstalling your USB memory drive

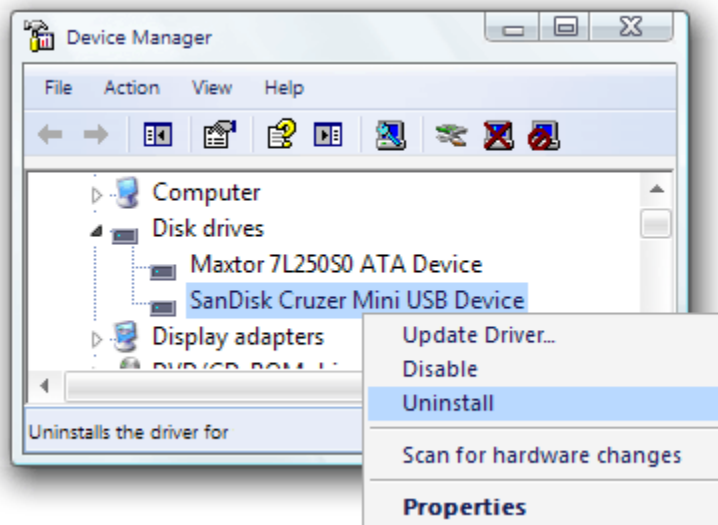
In normal day-to-day use of a USB memory drive, you might typically just pull the drive out of the USB port. However, for this guide, you must also uninstall the device driver to ensure that each scenario is started with the computer in a suitable state. If you fail to uninstall and remove the device when directed, the policies tested in the scenarios below will not have any effect and you will not see the expected results. Use these same steps throughout this guide when you are directed to uninstall and remove your device.

### Important

Do not physically disconnect your device from the USB port until you get to the last step.

### To uninstall your USB memory drive

1. Log on to your computer **DMI-Client1\TestAdmin**.
2. To open Device Manager, click the **Start** button, type **mmc devmgmt.msc** in the **Start Search** box, and then press **ENTER**.
3. If the **User Account Control** dialog box appears, confirm that the action it displays is what you want, and then click **Continue**.
4. Right-click the entry for your USB memory drive, and then click **Uninstall**.



5. In the **Confirm Device Removal** dialog box, click **OK** to allow the uninstall process to complete.
6. When Windows completes the uninstall process, it removes the device entry from the Device Manager tree.
7. Unplug your USB memory drive from the USB port.

## Prevent installation of all devices

This scenario documents the typical steps required to implement the most restrictive configuration, where all device installations are prevented and existing devices cannot be updated with new device drivers. Users will not be able to install a device and use it without intervention from an administrator. Administrators can still install or update any device as needed.

### Prerequisites for preventing installation of all devices

To complete the procedures in this scenario, you must uninstall your USB memory drive as described in the "[Uninstalling your USB memory drive](#)" section earlier in this document.

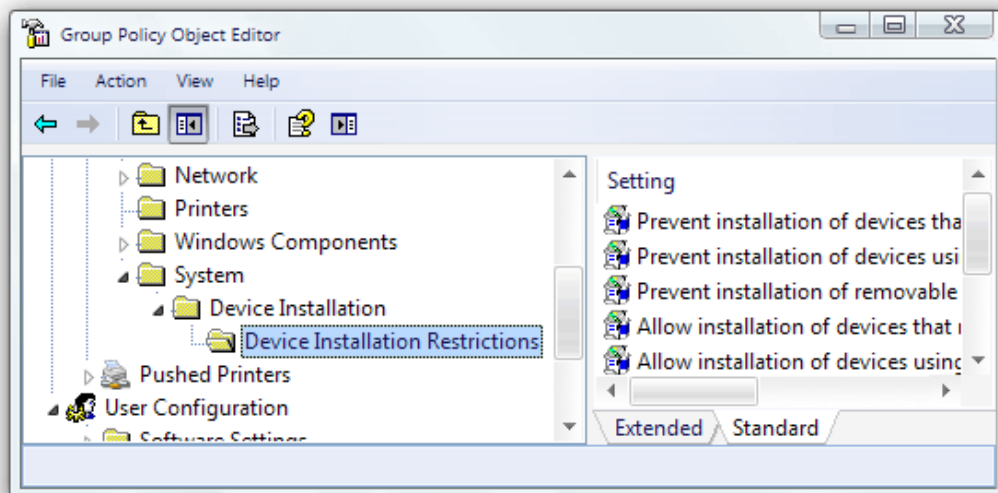
## Steps for preventing installation of all devices

1. [Configure policy to prevent installation of any device](#)
2. [Configure policy to allow administrators to override device installation restrictions](#)
3. [Test the effects of your restriction settings as a user](#)

### Step 1: Configure policy to prevent installation of any device

#### ► To configure policy that prevents installation or update of any device

1. Log on to your computer as **DMI-Client1\TestAdmin**.
2. To open Group Policy Object Editor, click the **Start** button, type **mmc gpedit.msc** in the **Start Search** box, and then press **ENTER**.
3. If the **User Account Control** dialog box appears, confirm that the action it displays is what you want, and then click **Continue**.
4. In the Group Policy Object Editor navigation pane, double-click **Computer Configuration** to open it. Then open **Administrative Templates**, open **System**, open **Device Installation**, and then open **Device Installation Restrictions**.



5. In the details pane, right-click **Prevent installation of devices not described by other policy settings**, and click **Properties**.

The policy dialog box appears with the current settings.

6. On the **Setting** tab, click **Enabled** to turn the policy on.
7. Click **OK** to save your settings and return to Group Policy Object Editor.

## Step 2: Configure policy to allow administrators to override device installation restrictions

The next policy enables administrators to override restrictions imposed by the other device installation policy settings, including the policy you just enabled.

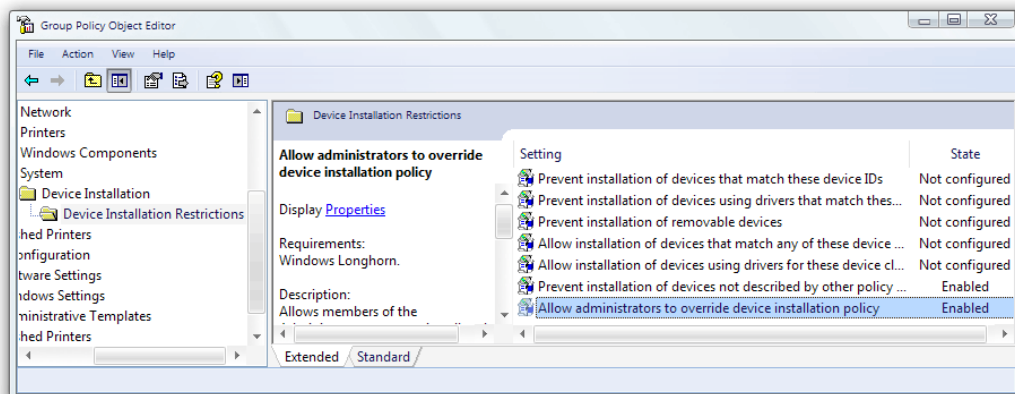
### ► To configure policy to allow administrators to override device installation restrictions

1. In the details pane, right-click **Allow administrators to override device installation policy**, and then click **Properties**.

The policy dialog box appears with the current settings.

2. On the **Setting** tab, click **Enabled** to turn the policy setting on.
3. Click **OK** to save your setting and return to Group Policy Object Editor.

Both policies now show their state as enabled.



4. Close Group Policy Object Editor.

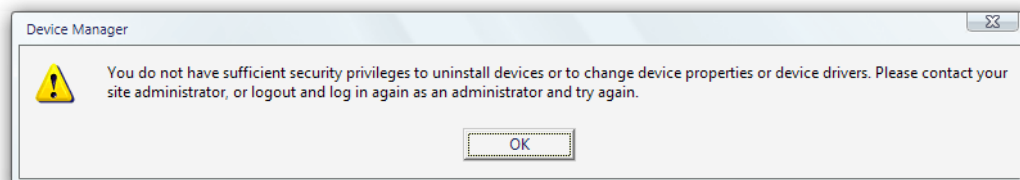
### Step 3: Test the effects of your restriction settings as a user

With both policies enabled, you can apply them to the computer and attempt to install the device to see the restrictions work.

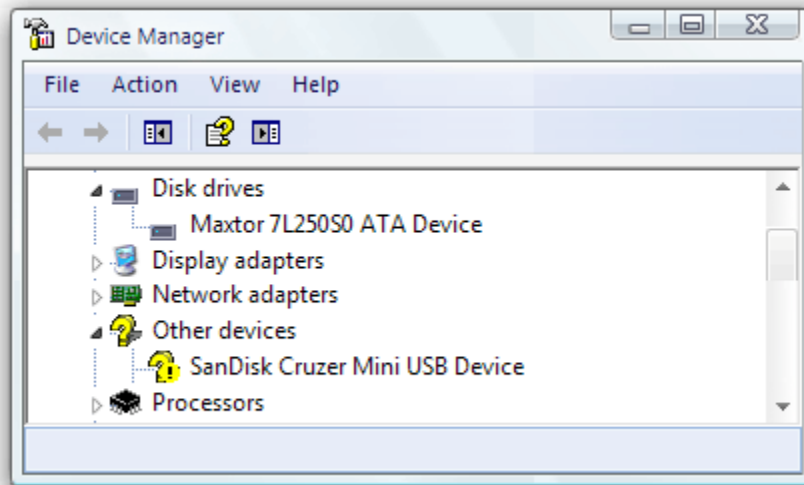
#### ▶ To test the effects of your restriction settings as a user

1. If your device is installed, uninstall and remove it by following the steps in the "[Uninstalling your USB memory drive](#)" section earlier in this document.
2. Click the **Start** button, type **gpupdate /force** in the **Start Search** box, and then press **ENTER**.
3. When the GPUdate command has finished, log off of your computer, and then log on as **DMI-Client1\TestUser**.
4. To open Device Manager, click the **Start** button, type **mmc devmgmt.msc** in the **Start Search** box, and then press **ENTER**.

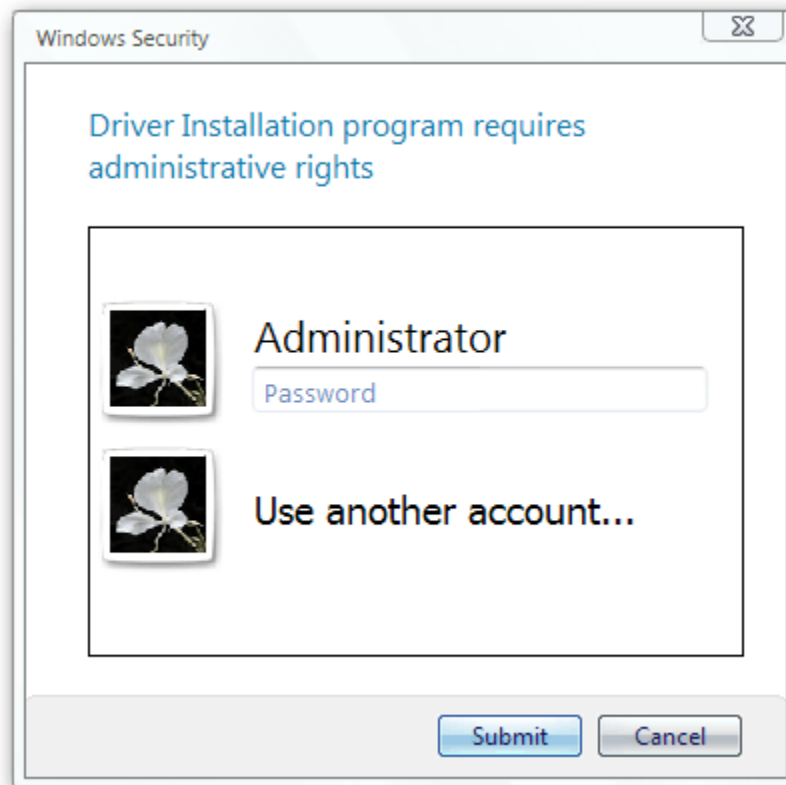
The following message appears, indicating that you do not have permissions to make any changes in Device Manager.



5. Click **OK** to acknowledge the message.  
Device Manager starts, and you can view the devices in the computer.
6. Plug in your USB memory drive.  
Until the installation is completed successfully, the device appears in Device Manager under the **Other devices** node.



7. Because you are logged on as a standard user without administrative rights, and device installation is now restricted, the following dialog box appears:

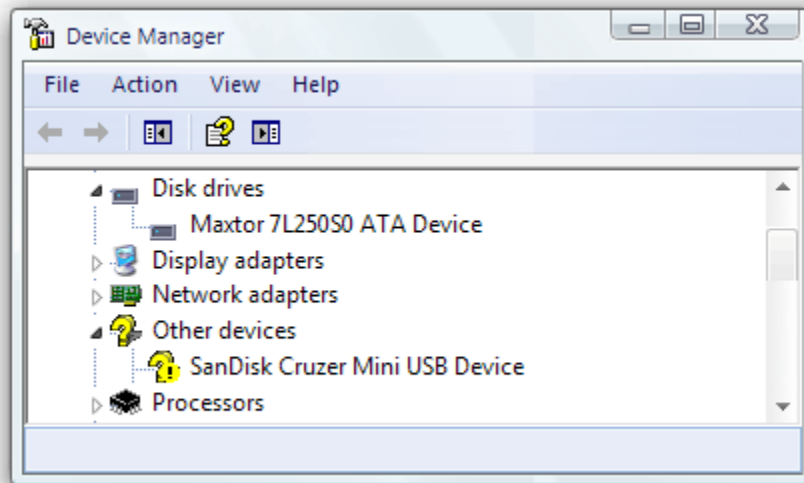


8. To simulate a typical user response, click **Locate and install driver software (recommended)**.

A variant of the **User Account Control** dialog box appears, asking you for a user name and password for an account that has administrator rights.

9. Because a user would not have administrator credentials to supply, click **Cancel** to abort the attempt as a user would do.

The device driver installation fails, and the device remains under the **Other devices** node and is not functional.



## Allow users to install only authorized devices

This scenario builds upon the first scenario, [Prevent installation of all devices](#), where you prevented the installation of any device. In this scenario, you add a list of allowed devices to the policy and include the hardware ID for your USB memory drive.

### Prerequisites for allowing users to install only authorized devices

To complete this task, you must first complete all of the steps in the first scenario, [Prevent installation of all devices](#).

### Steps for allowing users to install only authorized devices

In this section, you add allowed devices to the restrictions imposed in [Prevent installation of all devices](#), by creating a list of authorized devices.

1. [Create a list of authorized devices](#)
2. [Test the effects of the list as a user](#)

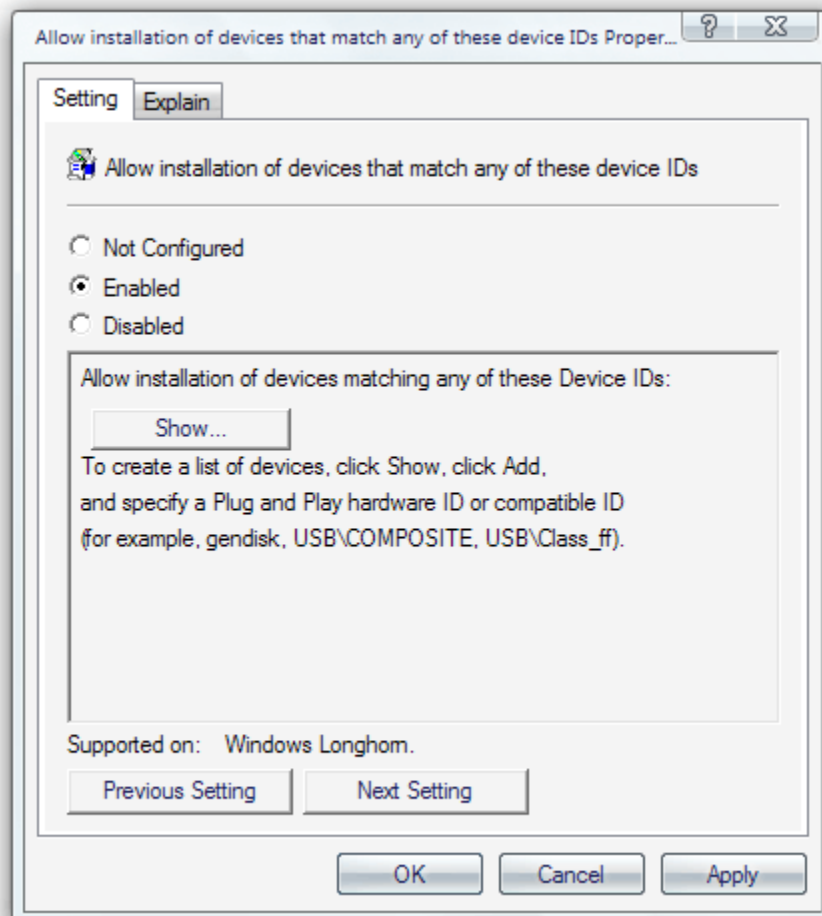
## Step 1: Create a list of authorized devices

### ▶ To create an approved device list

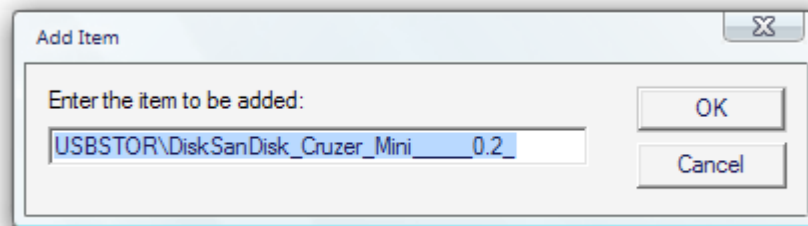
1. Log on to your computer as **DMI-Client1\TestAdmin**.
2. If your device is currently installed, uninstall and remove it by following the steps in the "[Uninstalling your USB memory drive](#)" section earlier in this document.
3. To open Group Policy Object Editor, click the **Start** button, type **mmc gpedit.msc** in the **Start Search** box, and then press ENTER.
4. In the Group Policy Object Editor navigation pane, double-click **Computer Configuration** to open it. Then open **Administrative Templates**, open **System**, open **Device Installation**, and then open **Device Installation Restrictions**.
5. In the details pane, right-click **Allow installation of devices that match any of these device IDs**, and then click **Properties**.

The policy dialog box appears with the current settings.

6. On the **Setting** tab, click **Enabled** to turn on this policy.

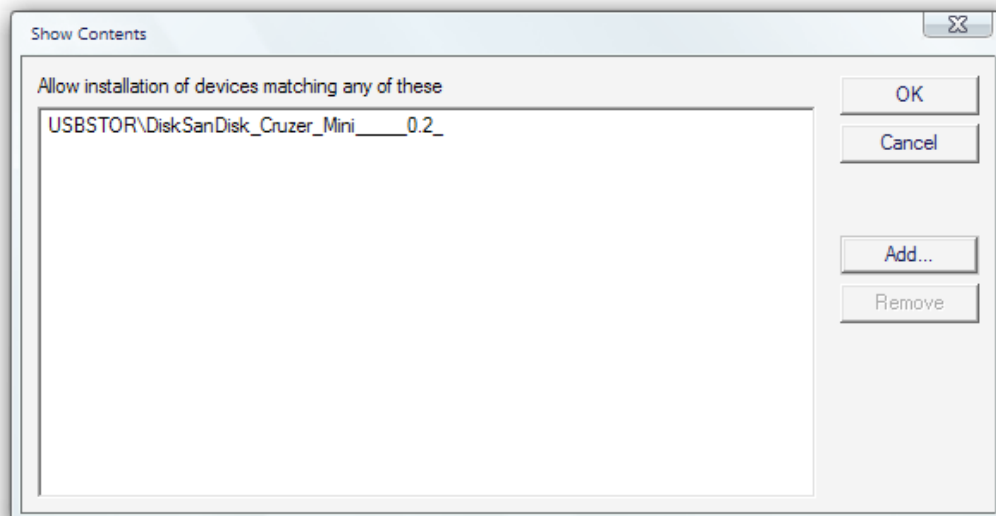


7. Click **Show** to view the list of allowed devices in the **Show Contents** dialog box. By default, the list is empty.
8. Click **Add** to open the **Add Item** dialog box.
9. Enter the device ID (the first hardware ID) for your device.



10. Click **OK** to return to the **Show Contents** dialog box.

Your device now appears in the list.



11. Click **OK** to return to the policy dialog box.

12. Click **OK** to save your new policy setting.

## Step 2: Test the list of authorized devices

With the policy setting enabled, you can apply it to the computer and attempt to install the device.

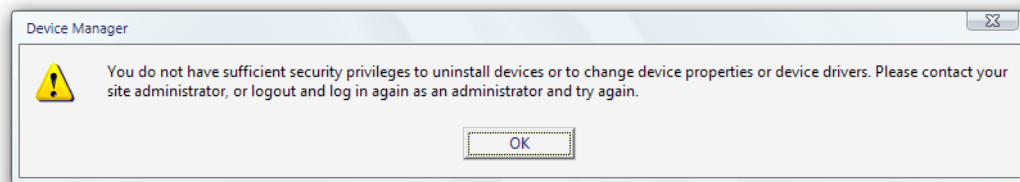
### ▶ To test the list of authorized devices

1. Click the **Start** button, type **gpupdate /force** in the **Start Search** box, and then press

**ENTER.**

2. When the `gupdate` command has finished, log off of your computer, and then log on as **DMI-Client1\TestUser**.
3. To open Device Manager, click the **Start** button, type **mmc devmgmt.msc** in the **Start Search** box, and then press ENTER.

The following message appears, indicating that you do not have permissions to make any changes in Device Manager.

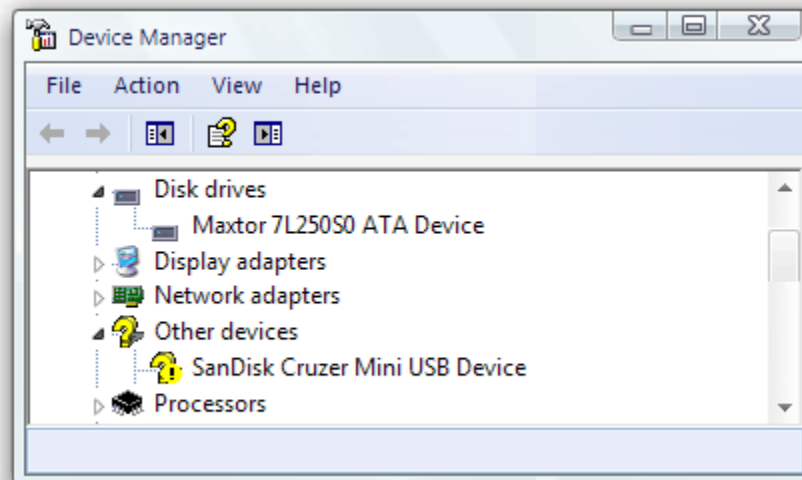


4. Click **OK** to close the message.

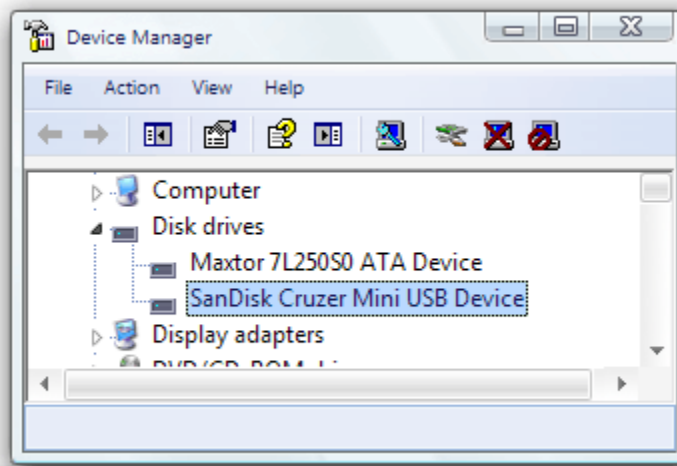
Device Manager starts, and you can view the devices in the computer.

5. Plug in your USB memory drive.

The device appears in Device Manager under the **Other devices** node until Windows completes the installation.



6. After Windows completes the installation, the device moves to the **Disk Drives** node in Device Manager and is fully functional.



## Prevent installation of prohibited devices

This scenario presents an alternative way to control device installation. In the first two scenarios, you prevented installation of all devices except those allowed by a list of authorized devices. In this scenario, you allow installation of all devices except those on a list of prohibited devices. You also remove the exception for administrators that you created in the first scenario so that even an administrator is affected by the policy.

### Prerequisites for preventing installation of prohibited devices

If you completed the steps in [Prevent installation of all devices](#) and [Allow users to install only authorized devices](#), you must disable those policies using the following steps:

- Enable installation of all devices.
- Remove the exception for members of the Administrators group to allow device installation.
- Remove the hardware ID from the approved device list.

#### ▶ To enable installation of all devices

1. Log on to your computer as **DMI-Client1\TestAdmin**.
2. To open Group Policy Object Editor, click the **Start** button, type

**mmc gpedit.msc** in the **Start Search** box, and then press ENTER.

3. In the Group Policy Object Editor navigation pane, double-click **Computer Configuration** to open it. Then open **Administrative Templates**, open **System**, open **Device Installation**, and then open **Device Installation Restrictions**.
4. In the details pane, right-click the node **Prevent installation of devices not described by other policy settings**, and then click **Properties**.

The policy dialog box appears with the current settings.

5. Click **Disabled** to turn the policy setting off.
6. Click **OK** to save your setting and return to Group Policy Object Editor.

The next step is to remove the policy that granted an exception to members of the Administrators group.

▶ **To remove the exception for administrators to Group Policy restrictions**

1. In Group Policy Object Editor, right-click **Allow administrators to override device installation policy**, and then click **Properties**.

The policy dialog box appears with the current settings.

2. On the **Setting** tab, click **Disabled** to turn the policy setting off.
3. Click **OK** to save your setting and return to Group Policy Object Editor.

The next step is to remove the hardware ID from the list of authorized devices that you created in the second scenario.

▶ **To remove the hardware ID from the list of authorized devices**

1. In Group Policy Object Editor, right-click **Allow installation of devices that match any of these device IDs**, and then click **Properties**.

The policy dialog box appears with the current settings.

2. On the **Setting** tab, click **Show** to view the list of authorized devices.
3. In the **Show Contents** dialog box, select the name of your USB memory drive, and then click **Remove**.

Windows removes your device from the list.

4. Click **OK** to close the **Show Contents** dialog box and return to the policy dialog box.
5. Click **Disabled** to turn off the policy setting.

6. Click **OK** to save your changes and return to Group Policy Object Editor.

## Steps for preventing installation of prohibited devices

To prevent users from installing specific devices, you create a list of prohibited devices. In this section, you will:

1. [Create a list of prohibited devices](#)
2. [Test the list of prohibited devices](#)

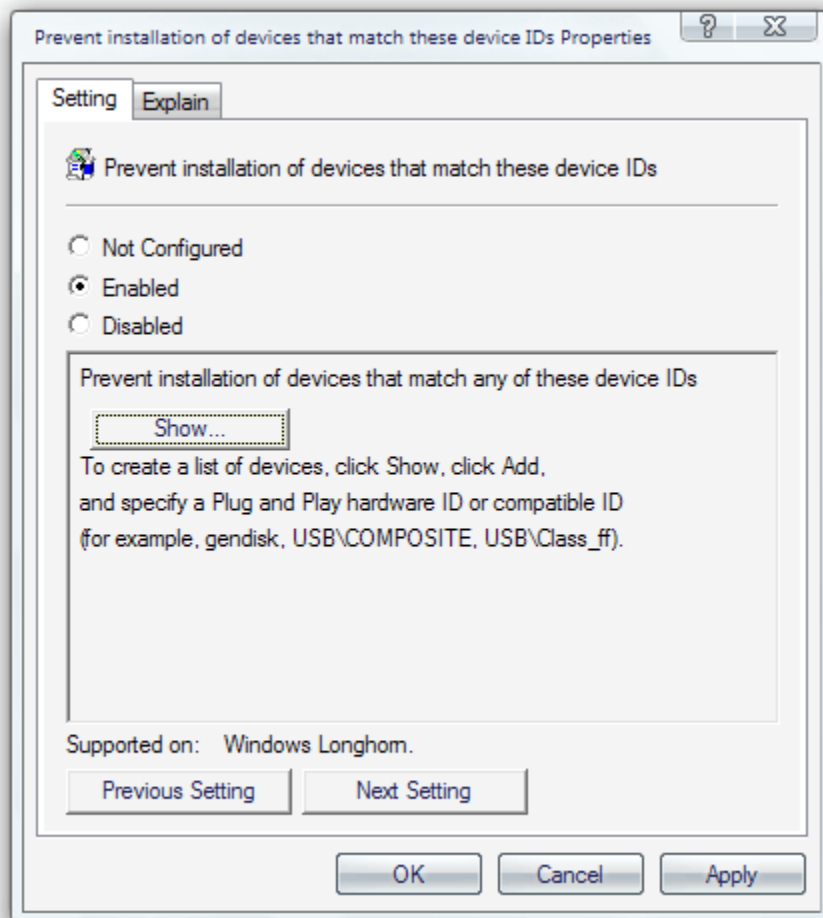
### Step 1: Create a list of prohibited devices

#### To create a list of prohibited devices

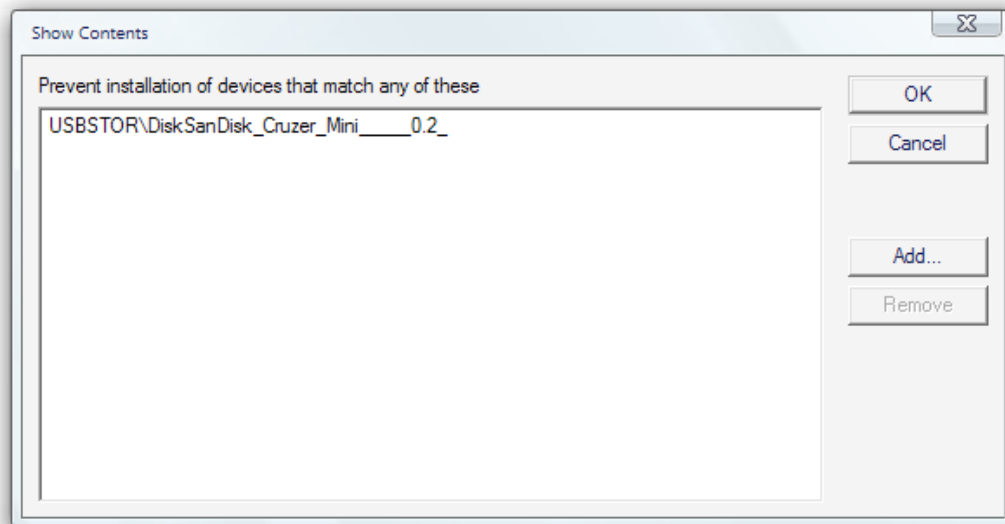
1. If your device is currently installed, uninstall and remove it by following the steps in the "[Uninstalling your USB memory drive](#)" section earlier in this document.
2. Log on to your computer as **DMI-Client1\TestAdmin**.
3. If it is not already running, start Group Policy Object Editor. To do so, click the **Start** button, type **mmc gpedit.msc** in the **Start Search** box, and then press ENTER.
4. In the tree, double-click **Computer Configuration** to open it. Then open **Administrative Templates**, open **System**, open **Device Installation**, and then open **Device Installation Restrictions**.
5. In the details pane, right-click **Prevent installation of devices that match these device IDs**, and then click **Properties**.

The policy dialog box appears with the current settings.

6. On the **Setting** tab, click **Enabled** to turn on this policy.



7. Click **Show** to view the list of prohibited devices.
  8. In the **Show Contents** dialog box, click **Add**.
  9. In the **Add Item** dialog box, type the device ID (the first hardware ID) that you found for your device.
  10. Click **OK** to return to the **Show Contents** dialog box.
- Your device now appears in the list.



11. Click **OK** to return to the policy dialog box.
12. Click **OK** to save your new policy setting.

## Step 2: Test the list of prohibited devices

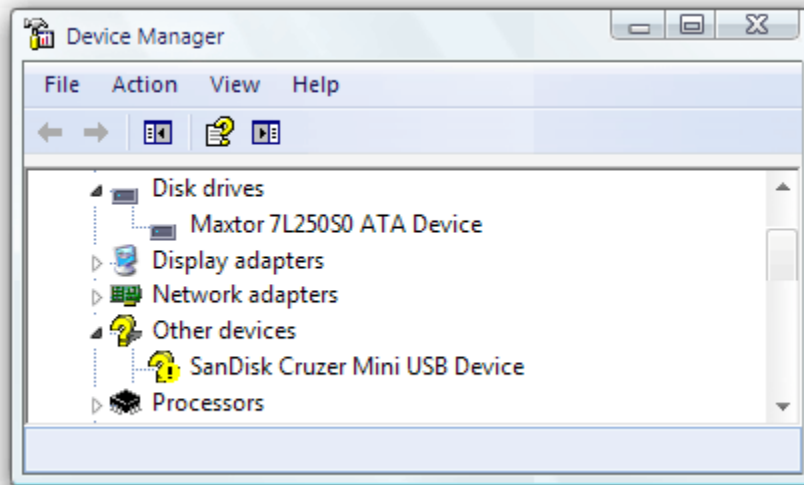
Now you can attempt to install the device. You can install other devices because policy no longer prevents their installation, but you cannot install this specific device, even when you are logged on as a member of the Administrators group.

### ▶ To test the list of prohibited devices

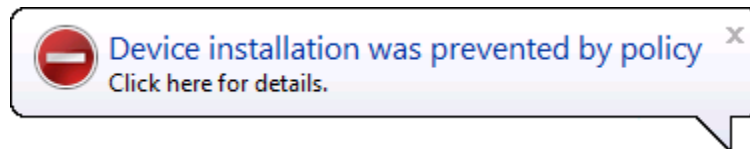
1. Click the **Start** button, type **gpupdate /force** in the **Start Search** box, and then press **ENTER**.
2. When the gpupdate command has finished, close the command prompt.
3. To open Device Manager, click the **Start** button, type **mmc devmgmt.msc** in the **Start Search** box, and then press **ENTER**.
4. Plug in your USB memory drive.

The device appears in Device Manager under the **Other devices** node.

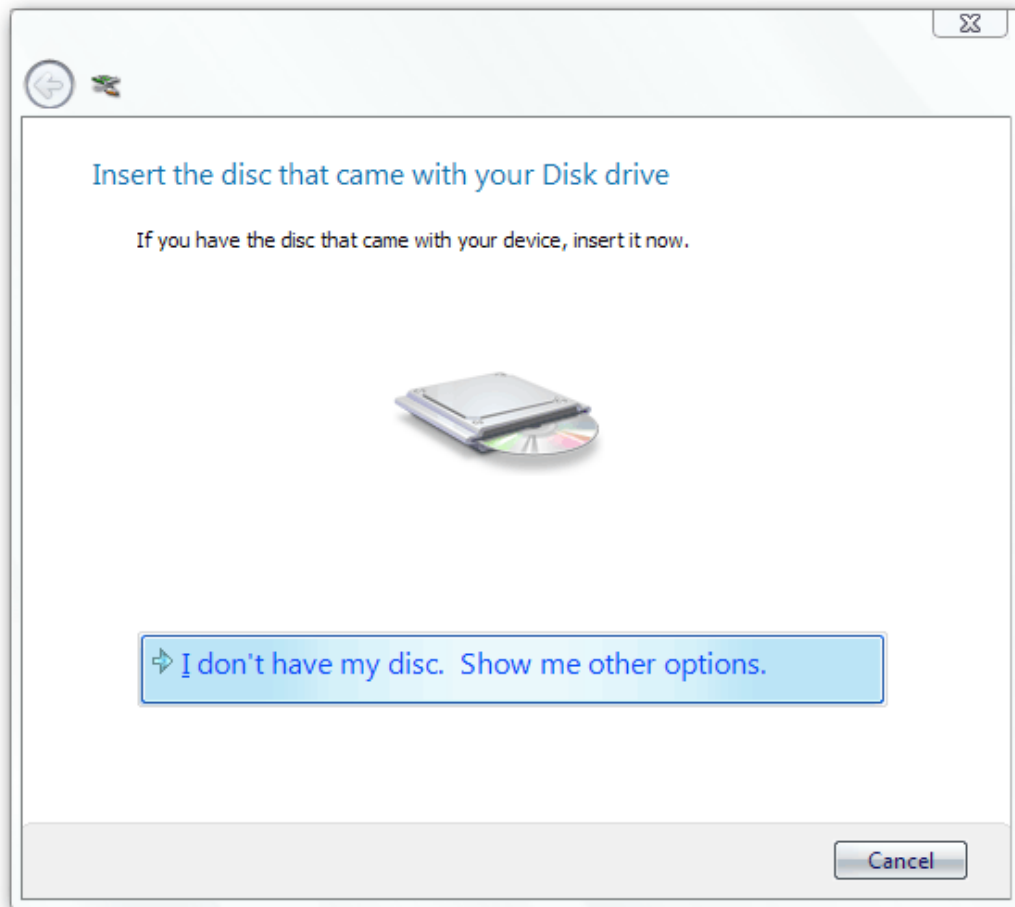
The installation does not complete, and the device does not function.



5. Windows displays a message in the notification area stating the reason why the installation failed:

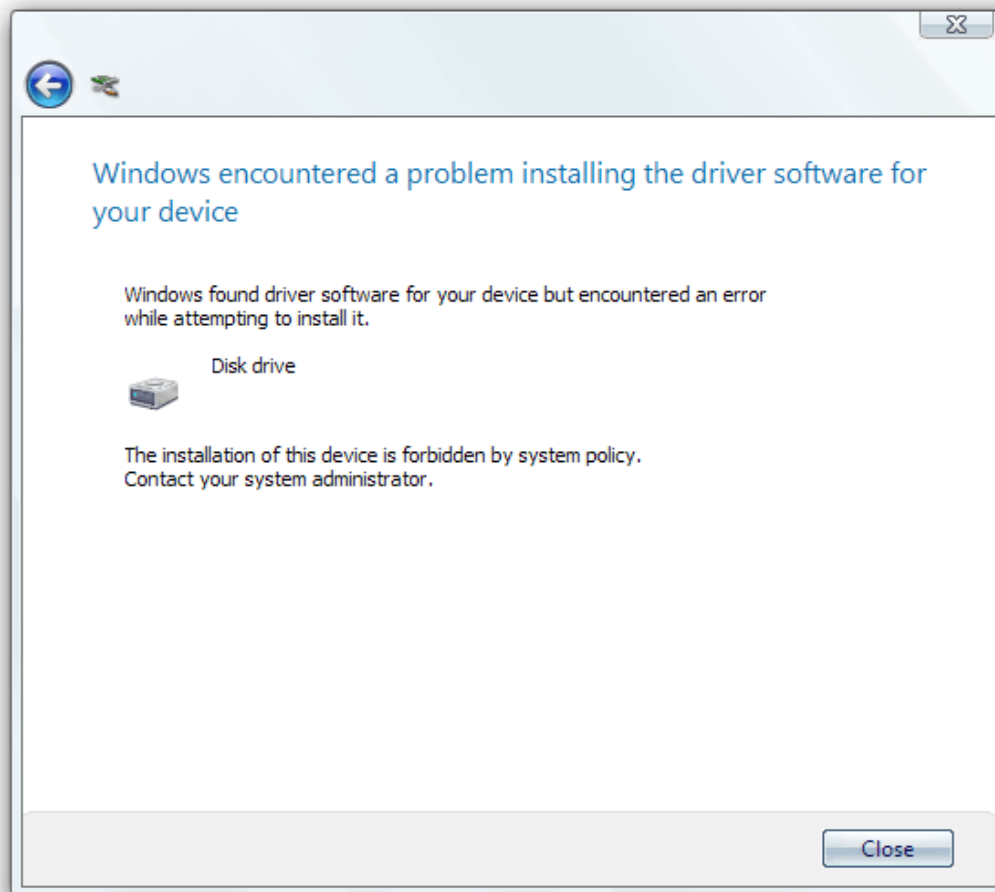


6. You can attempt to bypass the restrictions by manually installing the driver for the device. Right-click the device, and then click **Update Driver Software**.
7. The operating system prompts you to provide the device driver for the device.



8. To simulate what a user might attempt, click **Search automatically for updated driver software.**

A message appears stating that Windows found but could not install the driver. The last paragraph explains that the installation attempt failed because it is forbidden by the policy you created.



9. Click **Close**.

## Control read and write permissions on removable media

This scenario demonstrates how you can control read or write access to removable devices or devices that use removable media, on computers running Windows Vista and Windows Server "Longhorn". In this scenario, you set Group Policy to make your USB memory drive read-only. You also set Group Policy to make any CD or DVD burner attached to your computer read-only, in effect disabling the burning feature.

## Prerequisites for controlling read and write permissions on removable media

Before you can try the procedures in this section, you must disable the policy that prevents the installation of USB memory drives.

### ▶ To disable the policy that prevents the installation of USB memory drives

1. If your device is currently installed, uninstall and remove it by following the steps in the "[Uninstalling your USB memory drive](#)" section earlier in this document.
2. In the details pane of the Group Policy Object Editor, right-click **Prevent installation of devices that match these device IDs**, and then click **Properties**.

The policy dialog box appears with the current setting.

3. On the **Settings** tab, click **Show** to view the list of prohibited devices.
4. In the **Show Contents** dialog box, click your USB memory drive, click **Remove**, and then click **OK**.
5. On the **Setting** tab, click **Disabled** to turn off this policy setting.
6. Click **OK** to save your change.

## Steps for controlling read and write permissions on removable media

1. [Set computer policy to deny write access to specific removable device classes](#)
2. [Test your computer policy settings](#)

### Step 1: Set computer policy to deny write access to specific removable device classes

The policies you set in this procedure will block write access to many removable storage devices. However, the exact computer policy that blocks write access to your device can vary based on the specific make and model device. You can also use the **Custom Classes** policy, but it requires you to identify the device setup class GUID for the specific device.

### ▶ To deny write access to specific removable device classes

1. In the Group Policy Object Editor navigation pane, open **Computer**

**Configuration**, then open **Administrative Templates**, open **System**, and then open **Removable Storage Access**.

2. Right-click **CD and DVD: Deny write access**, and then click **Properties**.
3. On the **Properties** dialog box, click **Enabled** to turn on the restriction, and then click **OK**.
4. Repeat steps 2 and 3 for the following computer policies:
  - **Removable Disks: Deny write access**
  - **Floppy Drives: Deny write access**
  - **WPD Devices: Deny write access**
5. Close Group Policy Object Editor.

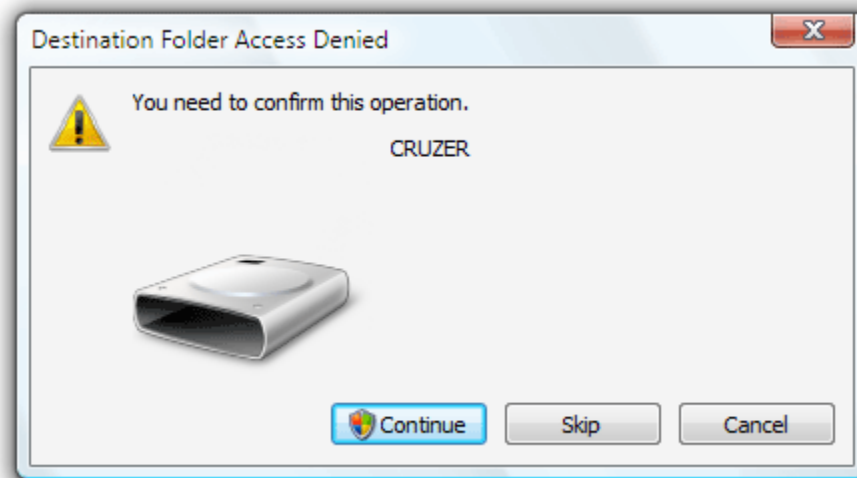
## Step 2: Test your computer policy settings

If a device is in use, the write access restriction policy cannot be immediately enforced. To apply the computer policy, restart the computer.

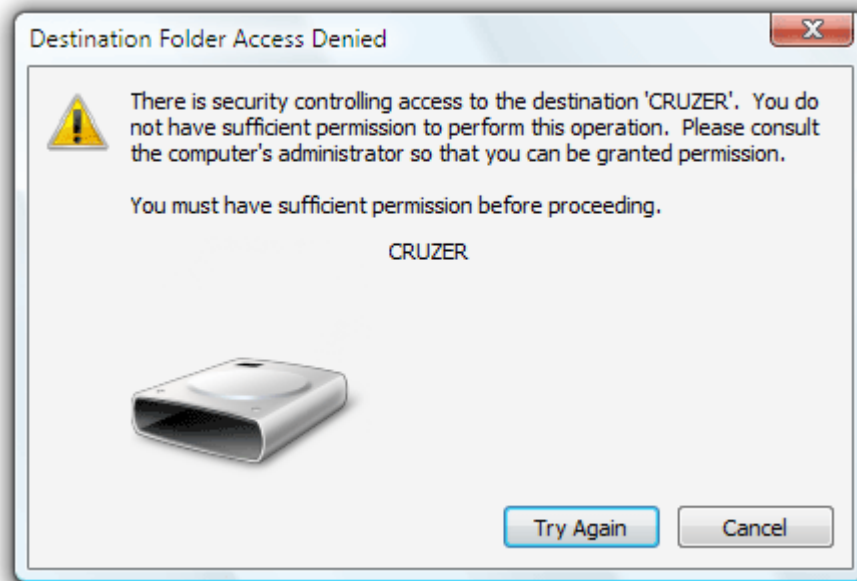
### ▶ To test your computer policy settings

1. Click the **Start** button, type **gpupdate /force** in the **Start Search** box, and then press **ENTER**.
2. When the gpupdate command has finished, restart your computer.
3. Log on to your computer as **DMI-Client1\TestAdmin**.
4. Plug in your USB memory drive, and then wait until Windows notifies you that it is operational.
5. Click **Start**, click **Computer**, and then double-click your USB memory drive.
6. In Windows Explorer, right-click an open area of the details pane, click **New**, and then click **Folder**.

Windows displays an error message explaining why the attempt to create a folder failed.



7. Click **Continue** to try to work around the restriction.
8. If the **User Account Control** dialog box appears, confirm that the action it displays is what you want, and then click **Continue**.
9. Windows displays a second message indicating the reason it cannot write to the folder.



10. Click **Cancel** to close the dialog box.

## Conclusion

In this guide you used a sample device in a lab environment to learn how to control whether or not your users can install a device. You also learned how to restrict access to removable storage devices or devices that use removable media. Controlling installation and device usage this way improves your security, and enhances the effectiveness of your help desk by limiting the devices that users can install to those your organization approves and supports. The scenarios used to demonstrate these configurations included:

- **Prevent installation of all devices.**

In this scenario, you prevented standard users from installing any device, but allowed administrators to install or update devices.

- **Allow users to install only authorized devices.**

In this scenario, you allowed standard users to install only those devices included on a list of authorized devices.

- **Prevent installation of only prohibited devices.**

In this scenario, you allowed standard users to install most devices but prevented them from installing devices included on a list of prohibited devices.

- **Control the use of removable media storage devices**

In this scenario, you prevented standard users from writing data to removable storage devices, or devices with removable media, such as a USB memory drive or a CD or DVD burner.

## Logging bugs and feedback

Your feedback is welcome. If the scenarios included do not work as described or if they fail to capture the way you want to use the technology, please tell us. We will use the feedback that you provide to improve the quality of this documentation. Send your comments on this documentation to [Vista Feedback](mailto:vistafb@microsoft.com) (vistafb@microsoft.com).

For feedback about Windows Vista, please use the [Contact Us](#) link at the bottom of the Windows Vista Web page at <http://www.microsoft.com/windowsvista>.

## Additional resources

For more information about device installation:

- Device Management and Installation  
<http://go.microsoft.com/fwlink/?LinkId=59274>
- How Setup Selects Device Drivers  
<http://go.microsoft.com/fwlink/?LinkId=54881>
- Device Identification Strings  
<http://go.microsoft.com/fwlink/?LinkId=52665>

For more information about the DevCon tool:

- "DevCon" at the Microsoft Web site  
<http://go.microsoft.com/fwlink/?linkid=54880>
- The DevCon command-line tool functions as an alternative to Device Manager  
<http://go.microsoft.com/fwlink/?LinkId=56391>
- DevCon HwIDs  
<http://go.microsoft.com/fwlink/?linkid=56389>

For more information about User Account Control in Windows Vista:

- User Account Control  
<http://go.microsoft.com/fwlink/?linkid=68249>

For more information about Group Policy:

- Group Policy  
<http://go.microsoft.com/fwlink/?LinkId=55625>