

Locking Down USB Drives with Windows Server 2008 R2 and Windows Vista/7

Author: David Gullett

Published: May 25, 2010

Version: 1.00

Copyright 2010, Symmetrix Technologies

<http://www.symmetrixtech.com>

Table of Contents

A. Introduction

1. Equipment Assumptions
2. Knowledge Assumptions
3. End Result

B. Procedure

1. Operating Systems
 - a. Windows Server 2008 R2
 - b. Windows Vista and Windows 7
2. Windows 2008 Group Policies
Modifying the Server 2008 Group Policies
3. Results
After the Group Policy

C. Other Considerations

A. Introduction

It's certainly no surprise with the proliferation of portable devices such as USB flash drives, USB hard drives, mobile phones and even cameras that extra care must now be taken to prevent data theft.

The purpose of this document is to provide a method of preventing users in a Windows Server 2008 and Windows Vista/7 corporate environment from plugging in a removable USB device into a workstation and copying data to it.

1. Equipment Assumptions

A Windows 2008 R2 domain with group policies enabled
Client workstations running Windows Vista or Windows 7. This will not work with Windows XP.

2. Knowledge Assumptions

Basic Windows server management skills including group policies – this document outlines exact steps to prevent USB drives from being connected to workstations but you need to have a full understanding of group policies and your forest/domain structure as there can easily be adverse effects in complex environments. You've been warned!

3. End Result

The goal is to prevent the copying of any data to removable USB drives - including thumb, jump, flash and portable hard drives.

Even while testing this the procedures in this document the results weren't always consistent so it's really important that you test the method in your environment. At the very least it will give you a good starting place. As always, feedback is highly appreciated and we would like to update this document with your experiences.

B. Procedure

1. Operating Systems

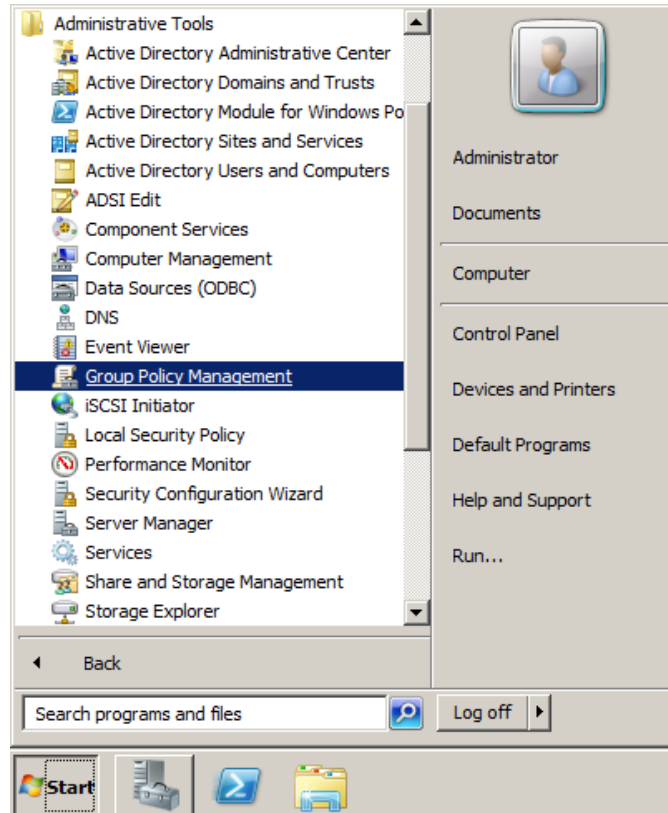
We tested with the operating systems outlined below. If you're reading this you will likely be able to install these on your own.

Windows Server 2008 R2 - This document was tested with Windows Server 2008 R2 installed as a domain controller. Earlier versions may work similarly but because of time considerations we just used the newest release.

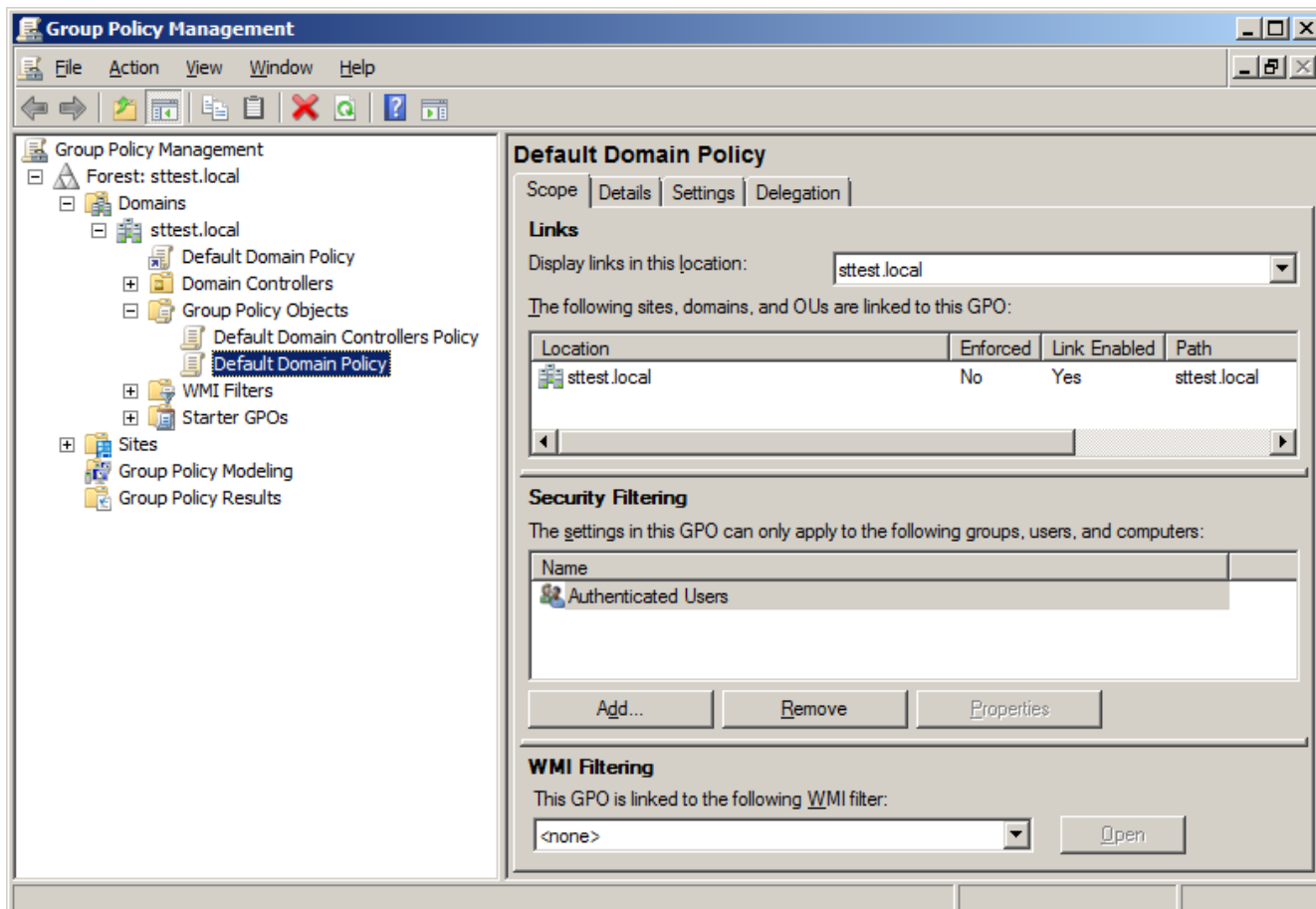
Windows Vista and Windows 7 - We also used only Windows Vista and Windows 7 on the client machines for testing for reasons that you'll see in the screenshots below. There are third party utilities that will enable this functionality in Windows XP but that is beyond the scope of this document.

2. Windows 2008 Group Policies

The first step is to modify the domain's group policies. Log on to a domain controller as a domain administrator equivalent account. Click on Start, then Administrative Tools, then finally open Group Policy Management as pictured below. Note: this can also be done from a workstation if you have the proper tools installed on it.

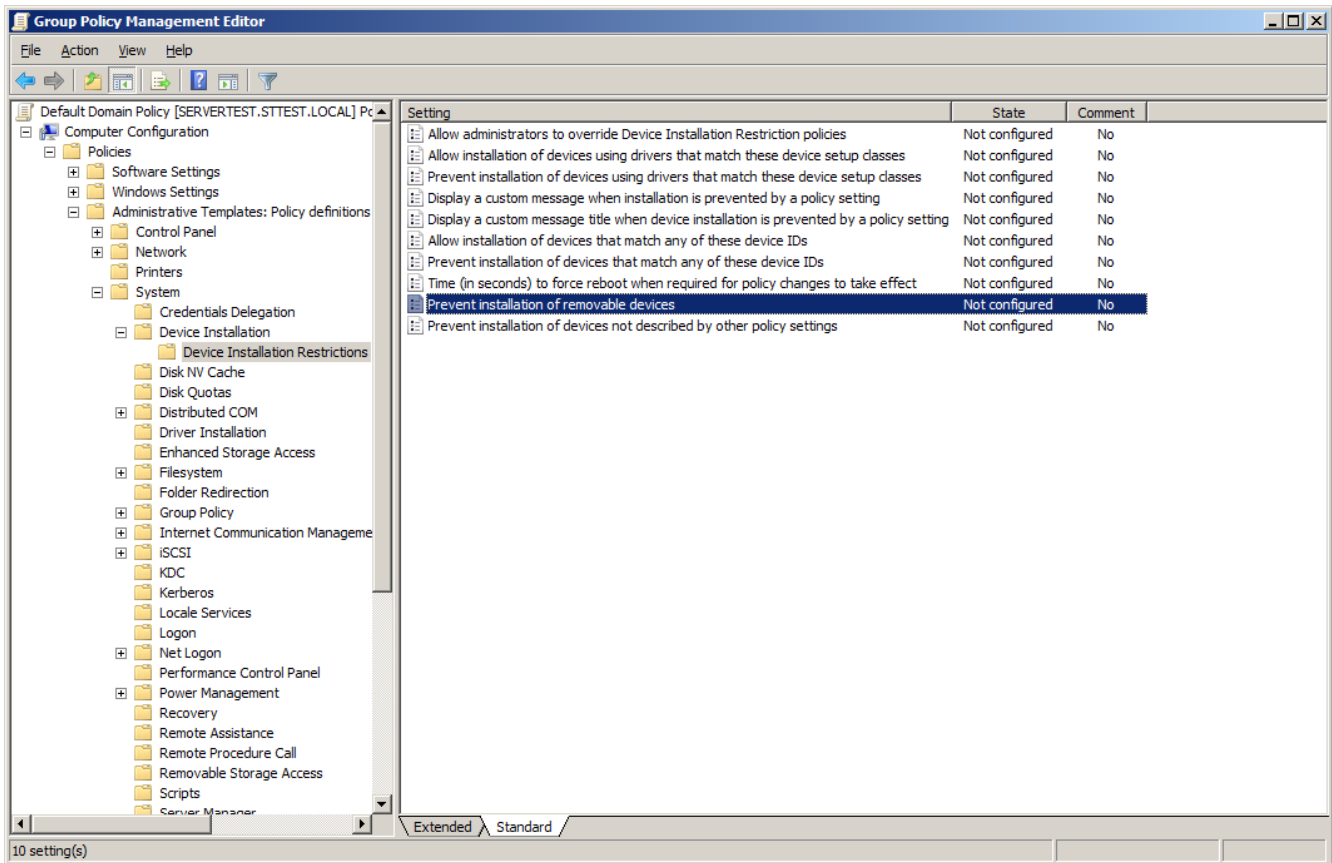


Drill down through the group policy management pane until you reach the Default Domain Policy. Right-click on it and select Edit.



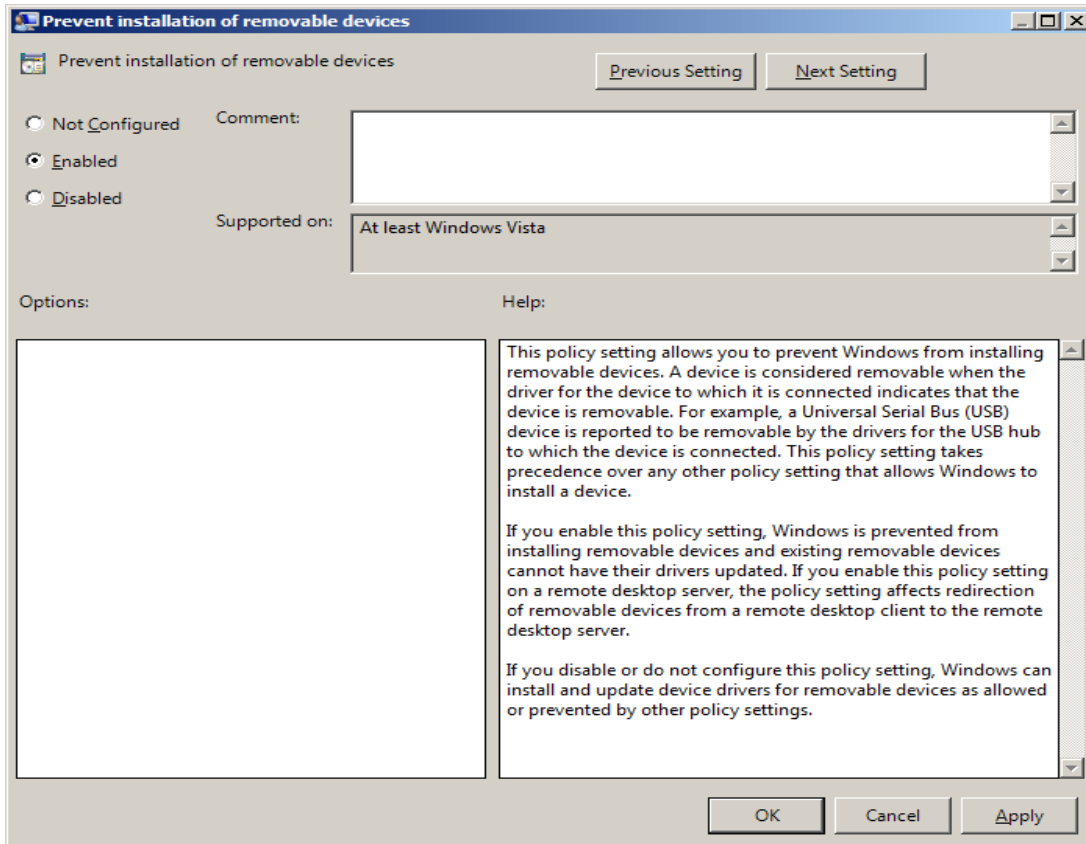
PLEASE NOTE: When you make this change it will affect every machine on your network including all workstations, servers and domain controllers. In order to apply this only to your workstations or groups of workstations you will need to create custom group policies and organizational units which is far beyond the scope of this document. It has been exhaustively documented elsewhere.

Drill down through the policy settings on the left to Computer Configuration/Policies/Administrative Templates/System/Device Installation/Device Installation Restrictions. In the right pane double click on the "Prevent Installation of Removable Devices" line.



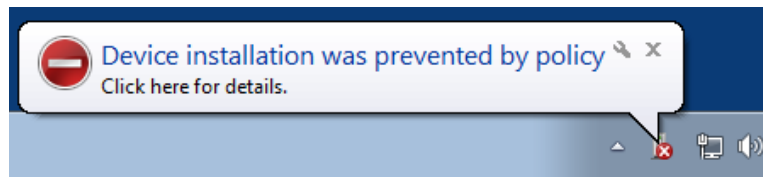
In the next box, click the Enabled radio button and click OK.

As you can see in the image below, this modification will only work with Windows Vista or newer. There are third party utilities that can help you lock down Windows XP workstations.

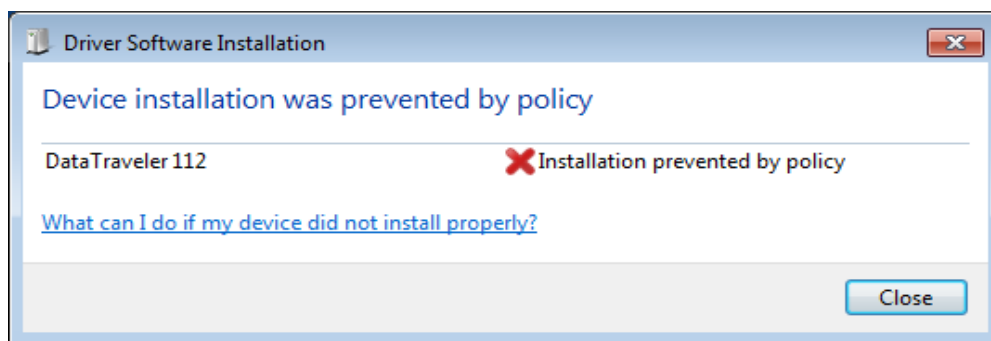


3. Results

Once the policy takes effect you will get an “Device installation was prevented by policy” error in Windows 7 when a USB drive is inserted into the target machine (shown below).



When you click on the balloon error you get a standard dialog box also reading “Device installation was prevented by policy” in the center of the screen.



C. Other Considerations

As with any document relating to security, don't take this guide as absolute gospel. You need to perform thorough testing in your environment.

We also highly recommend reviewing Microsoft's documentation regarding group policies. Pay particular attention to controlling the policy scope through linking to organizational units.

Another excellent tool provided by Microsoft is the Group Policy Results Wizard (this used to be called the Resultant Set of Policy, or “RSoP” tool in earlier versions of Windows). It generates reports that show you exactly how policies are applied to specific users or computers.

Comments, feedback and contributions are welcome and encouraged at articles@symmetrixtech.com.

Visit us on the web at <http://www.symmetrixtech.com> for the latest news on Snort Report and to download the newest version.

Revision History:

2010-05-25 – 1.0 - Initial release