

Smart-**X** Software Solutions

**GPHideDrive User guide**

---

## Table of content:

<b><u>WELCOME</u></b>	<b><u>3</u></b>
FEATURES AND CAPABILITIES	4
MORE SYSTEM MANAGEMENT TOOLS	4
<b><u>CONTENTS AND REQUIREMENTS</u></b>	<b><u>7</u></b>
CONTENT	7
REQUIREMENT	ERROR! BOOKMARK NOT DEFINED.
<b><u>LICENSING AND INSTALLATION</u></b>	<b><u>7</u></b>
EVALUATION VERSION LIMITATION	7
INSTALLATION	8
<b><u>HOW DOES IT WORK?</u></b>	<b><u>8</u></b>
STEP I: DEFINING THE DRIVES	8
STEP II: CHANGING THE ADM TEMPLATE	11
STEP III: ENABLING THE NEW GROUP POLICY	13

## **Welcome**

Welcome to SmartX.

Thank you for choosing GPHideDrive, one of many tools developed by the SmartX expert team in order to improve your everyday work, and help you manage your system efficiently and productively with no effort on your part.

This chapter describes some of the features and capabilities of the tool, and lists additional helpful tools in the same field that can optimize your work environment.

For more tools, click on the link to visit our website at [www.smart-x.com](http://www.smart-x.com).

### **This Chapter Contains:**

- Features and Capabilities.
- More tools for system Management.

## **Features and Capabilities**

Here are just some of the benefits our tool has to offer:

- Extends the "Hide these specified drives in my computer", and the "Prevent access to drives from my computer" Group Policy options to include additional drive letters.
- Enables you to hide more drives than default administrative templates allow.

## **More System management tools**

### **KillPol**

This tool enables you to temporarily remove group policy restrictions for the current user.

It is a useful tool for helpdesk personnel using restricted networks.

The KillPol function helps you to answer a user's call and fix the problem without the need to log the user off and log in with your credentials. In other words, the problem can be solved without interrupting the user's work.

After effectively fixing the problem, you simply have to press a button to return to the user's regular settings.

## **DSM**

Monitors your network for duplicate SIDs computers and easily resolve it from your own workstation.

Using computer images for OS deployment? Technicians forgot to run SYSPREP / NEWSID? You probably have hundreds of duplicate SID computers in your network!

Duplicate SID computers is a major security risk and additionally might cause all kind of issues when working with third party products such as Anti Virus, Deployment systems and other system products.

Duplicate SID Monitor (DSM) is a revolutionary product which constantly monitors your network to find computers with duplicate SIDs. The information is stored locally and enables administrators to query for duplicate SID computers and resolve it remotely by a single click.

## **Working with GPHideDrive**

This chapter contains specific instructions for working with the GPHideDrive tool.

Read the content carefully, follow the steps and you will find that it is very easy to operate.

### **This Chapter Contains:**

I: Contents and Requirements.

II: Licensing and installation.

III: How does it work

# Contents and requirements

## Content

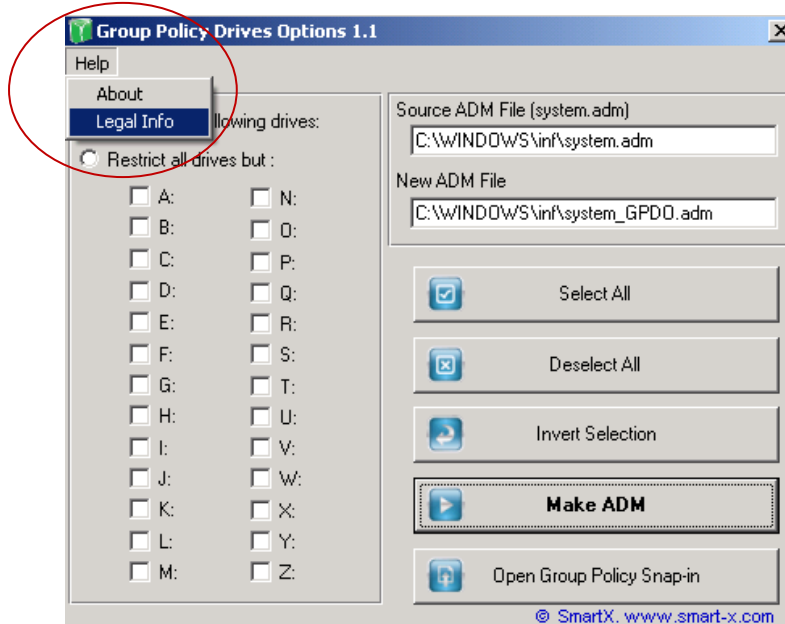
The GPHideDrive tool contains a simple exe file.

## Licensing and installation

### Evaluation version limitation

The product you have downloaded to your pc is a freeware.  
The GPHideDrive has no limitations of any kind (as explained in the EULA).

You can view the EULA content by Clicking on 'Legal info' from the 'help' menu.



## Installation

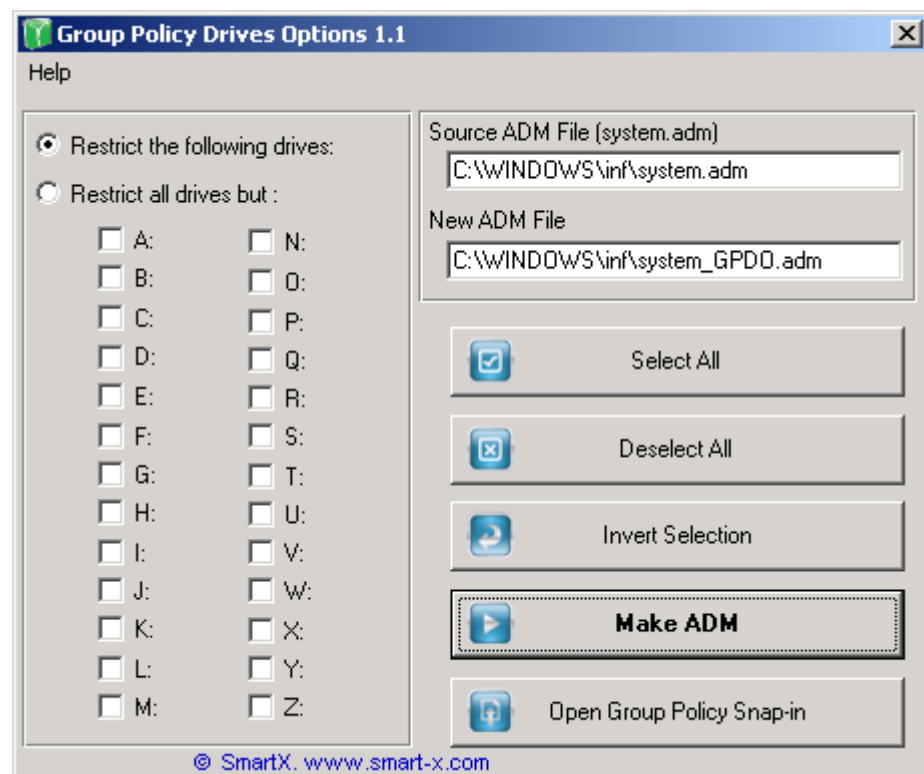
To operate the program from a downloaded file

1. Simply double click the 'SetUp.exe' file.
2. Follow the instructions in the installation wizard until you complete the installation.
3. A GPHideDrive icon will be placed on the desktop and in the programs menu.

## How does it work?

### Step I: Defining the Drives

- 1) Launch the program.

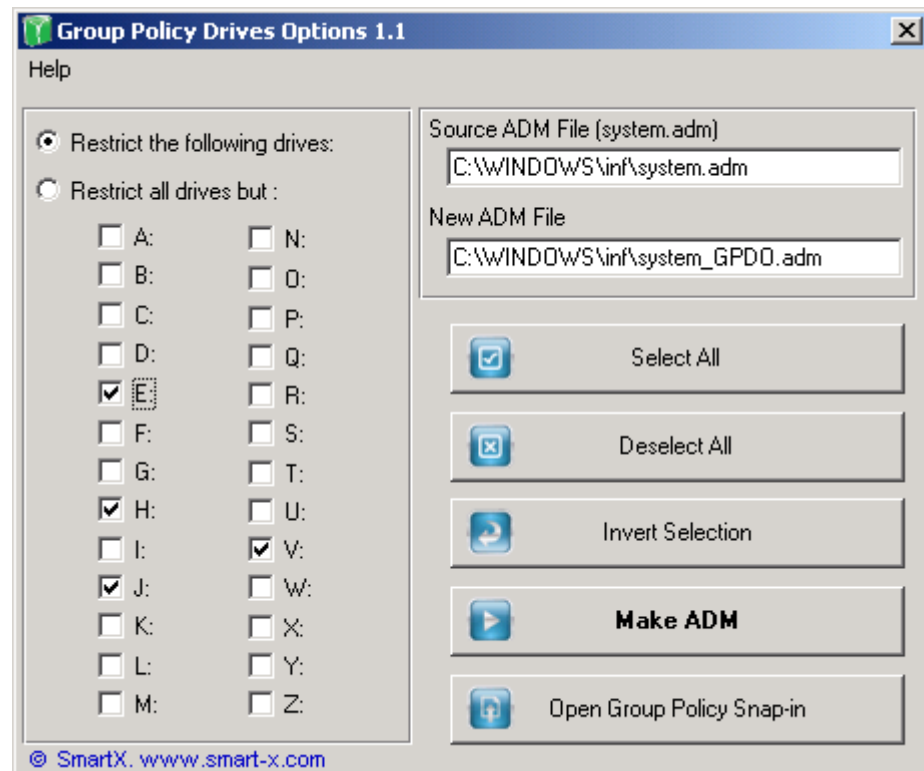




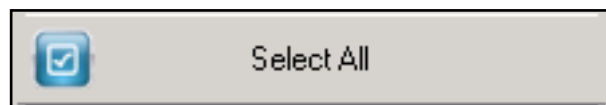
1. Specify the drives you wish to hide/ disable according to the options demonstrated:

Click on the letter of the drive you would like to hide. Repeat this step until all necessary drives are marked.

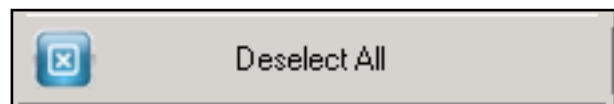
For example: **E, H, J, and V**



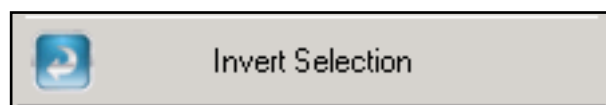
- To select all the drives press **Select All**.



- To clear selection press **Deselect All**.



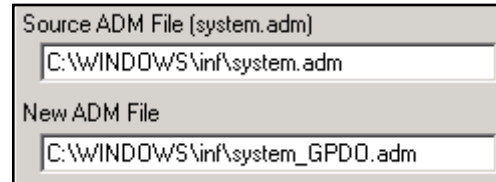
- To reverse the selection press **Invert Selection**.





If you have many drives you need to hide/ disable, Click the ***Restrict all drives but*** line and then choose the drives you **don't** want to hide/ disable. ☐ Restrict all drives but :

## 2) Define ADM.



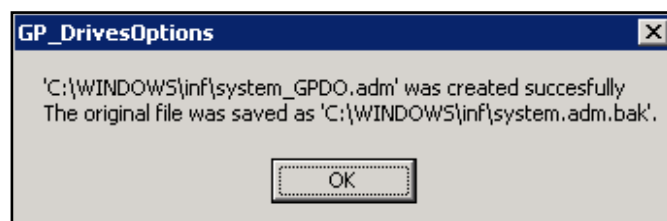
This section contains the path of the default ADM file and of the new ADM file that will contain the drives chosen.

- The upper box displays the source ADM file. The source ADM file is commonly the default system.adm file which is shipped with Windows 2000 and later OS's. This file includes the 'Hide these specified drives in my computer' and the 'Prevent access to specified drives in my computer' options.
- The lower box displays the new ADM file containing the changes. system\_GPDO.adm will include the new drive hide definitions and can be used instead of the default system.adm file.

## 3) Make ADM.



- Press the **Make ADM** button.
- Press **OK** in the displayed message.



## Step II: Changing the ADM template

1. Open Active Directory Users and Computers.
2. Change the ADM file:
  - Edit the GP in which you would like to add the drives you want to hide/disable.

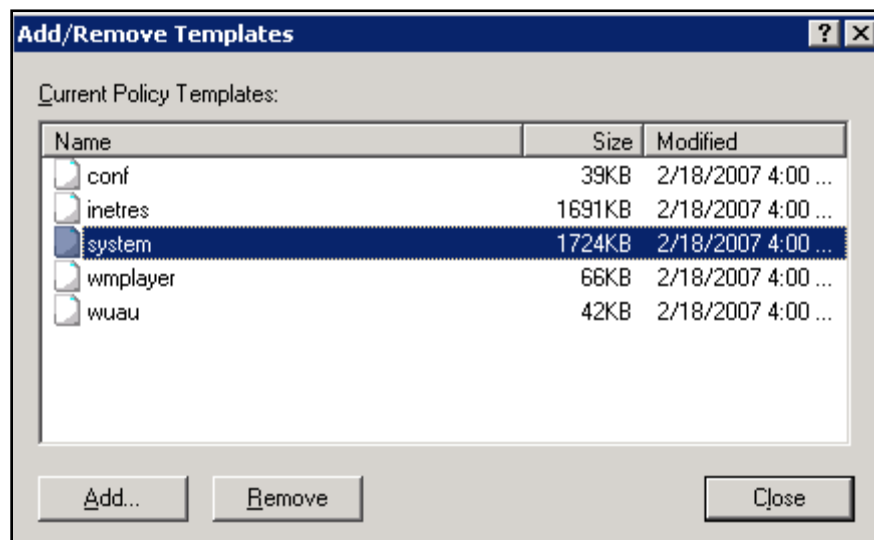
- Expand **User Configuration**.



- Right click on **Administrative Templates** and choose **Add/Remove Templates**



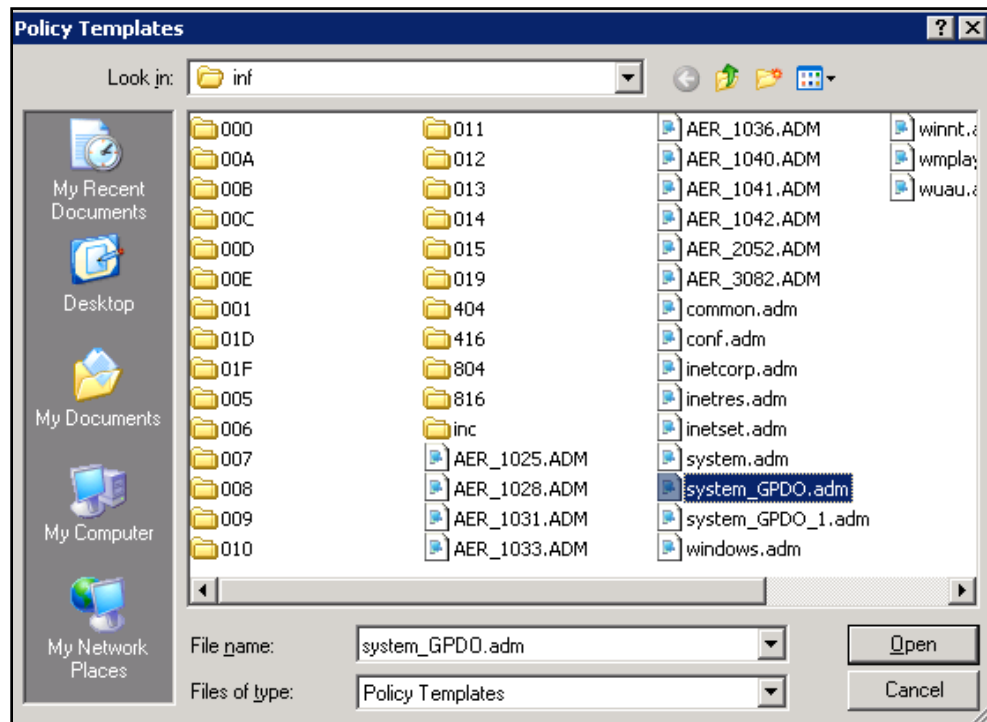
- In the **Add/ Remove Templates** window, click on the **System** line, and then click on **Remove**.



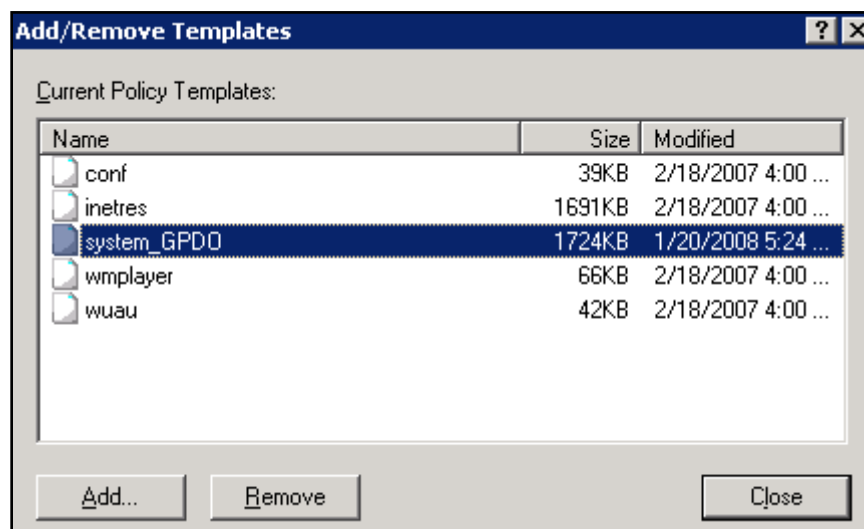
- Click on **Add** 

- Double click on the ADM file you have created.

for example: ***system\_gpdo.adm***



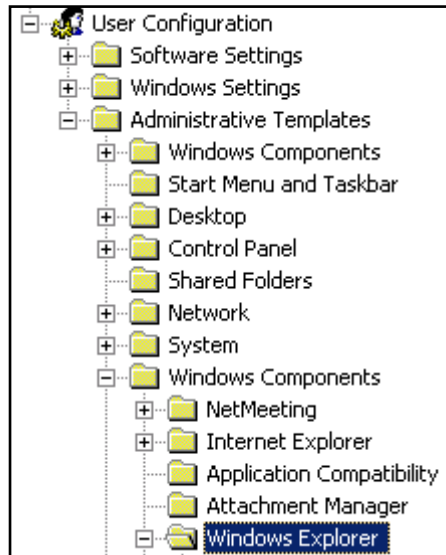
- The chosen ADM will appear in the ***Add/ Remove Template*** window.



- Click on ***Close***

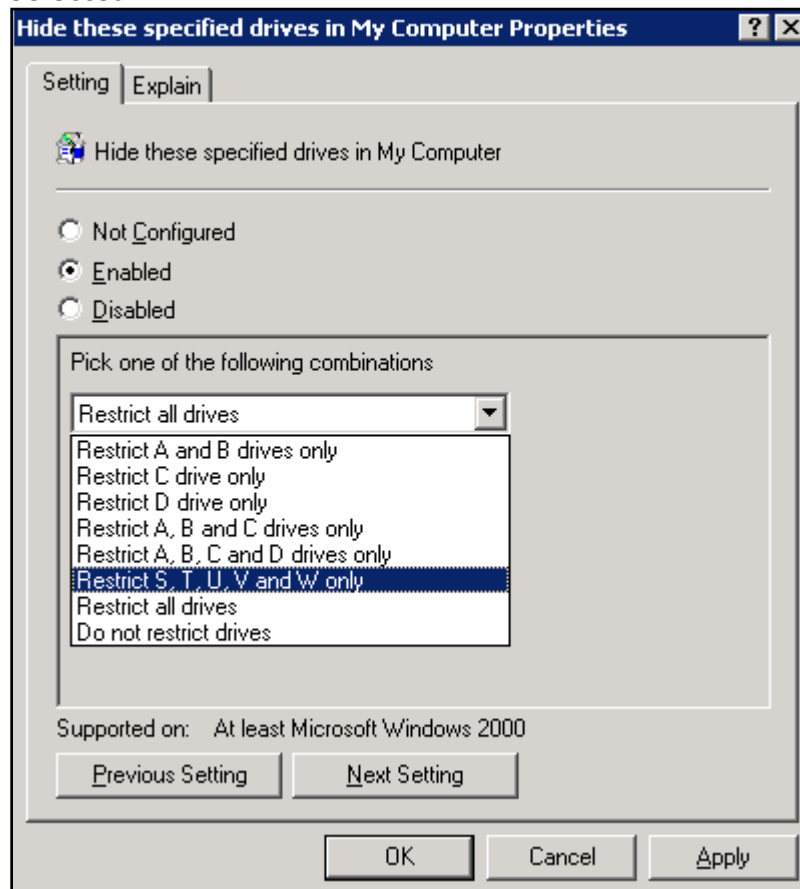
## Step III: Enabling the New Group Policy

1. Under the expended **user configuration**, expand **Administrative templates**.
2. Expand **Windows Components**.
3. Double click on **Windows Explorer**.



4. On the right, double click on **Hide these specified drives in my computer** or **Prevent access to drives from my computer**.
  - Click on **Enabled**.

- Open the drop-down list and you will see the drives you have selected.



- Select the relevant option, and click on **OK**.