

用组策略打造系统安全功能

1.隐藏“我的电脑”中指定的驱动器(Windows XP/2003)

此组策略可以从“我的电脑”和“Windows 资源管理器”上删除代表所选硬件驱动器的图标。并且驱动器号代表的所有驱动器不出现在标准的打开对话框上。

打开“组策略控制台→用户配置→管理模板→Windows 组件→Windows 资源管理器”中的“隐藏‘我的电脑’中的这些指定的驱动器”并启用此策略，并在下面列表框中选择一个驱动器或几个驱动器。

提示:这项策略只删除驱动器图标。用户仍可通过使用其它方式继续访问驱动器的内容。同时这项策略不会防止用户使用程序访问这些驱动器或其内容。并且也不会防止用户使用磁盘管理即插即用来看并更改驱动器特性。

2.防止从“我的电脑”访问驱动器(Windows 2000/XP/2003)

此策略让用户无法查看在“我的电脑”或“Windows 资源管理器”中所选驱动器的内容。同时它也禁止使用运行对话框、镜像网络驱动器对话框或 Dir 命令查看在这些驱动器上的目录。

打开“组策略控制台→用户配置→管理模板→Windows 组件→Windows 资源管理器”中的“防止从‘我的电脑’访问驱动器”并启用此策略，并在下面列表框中选择一个驱动器或几个驱动器。

提示:这些代表指定驱动器的图标仍旧会出现在“我的电脑”中，但是如果用户双击图标，会出现一条消息解释设置防止这一操作。同时这些设置不会防止用户使用其它程序访问本地和网络驱动器。并且不防止他们使用磁盘管理即插即用查看和更改驱动器特性。

3.禁止使用命令提示符(Windows 2000/XP/2003)

在 Windows 2000/XP/2003 下，我们可以运行 cmd.exe 进入命令提示符状态，并可以继续运行一些 DOS 命令和其他命令程序。出于对安全的考虑，有些系统应该屏蔽此功能。

打开“组策略控制台→用户配置→管理模板→系统”中的“阻止访问命令提示符”并启用此策略，并在下面列表框中选择是否“也停用命令提示符脚本处理”，这个设置还决定批处理文件 趁.cmd 和.bat 是否可以在计算机上运行。

如果启用这个设置，在用户试图打开命令窗口时，系统会显示一条消息，解释设置阻止这一操作。

4.禁止更改显示属性(Windows 2000/XP/2003)

选择“控制面板”中的“显示”或在 Windows 桌面的空白处单击右键选择“属性”，

可进入“显示设置”对话框，可以对桌面主题、桌面背景、屏保程序、显示设置等各项进行设置，如果你不想让别人随意更改各项设置，可以通过组策略将它隐藏起来。

打开“组策略控制台→用户配置→管理模板→控制面板→显示”，然后可以看到隐藏桌面选项卡、隐藏主题选项卡、隐藏保护程序选项卡、隐藏设置选项卡等策略配置，可根据需要对这些项目进行配置。比如启用了“隐藏‘桌面’选项卡”策略后，再打开“显示属性”对话框，就看不到“桌面”标签了，这样自然就无法再对桌面属性进行更改了。

5.禁用注册表编辑器(Windows 2000/XP/2003)

为了防止他人进入电脑后对注册表文件进行修改，可以在组策略中对注册表编辑器做禁止访问设置。具体操作方法:打开“组策略控制台→用户配置→系统”中的“阻止访问注册表编辑工具”并启用此策略。

此策略被启用后，用户试图启动注册表编辑器(Regedit.exe 及 Regedt32.exe)的时候，系统会禁止这类操作并弹出警告消息。

6.彻底禁止访问“控制面板”(Windows 2000/XP/2003)

如果不希望其他用户访问计算机的“控制面板”，同样可以使用组策略来实现。打开“组策略控制台→用户配置→管理模板→扩展面板”中的“禁止访问控制面板”并启用此策略。

此策略启用后可以防止“控制面板”程序文件(Control.exe)的启动。他人将无法启动“控制面板”(或运行任何“控制面板”项目)。另外，这个设置将从“开始”菜单中删除“控制面板”。同时这个设置还从“Windows 资源管理器”中删除“控制面板”文件夹。

7.禁止建立新的拨号连接(Windows 2000/XP/2003)

如果不想让别人在计算机中建立新连接来拨号上网的话，组策略也可以做到。打开“组策略控制台→用户配置→管理模板→网络→网络连接”中的“禁止访问新建连接向导”并启用此策略。

启用此策略后，在“网络连接”文件夹和“开始菜单”中就不会出现“建立新连接”。

提示:此设置无法阻止用户使用诸如 Internet Explorer 这样的其它程序来绕过此设置。另外此设置必须重新启动计算机后才能生效。

8.禁用“添加/删除程序”(Windows 2000/XP/2003)

“控制面板”中“添加或删除程序”项目允许你安装、卸载、修复并添加和删除 Windows 的功能和组件以及种类很多的 Windows 程序。如果你想阻止其他用户安装或卸载程序，可利用组策略来实现。

打开“组策略控制台→用户配置→管理模板→控制面板→添加→删除程序”中的“删除‘添加/删除程序’程序”并启用此策略，当我们再打开“控制面板”中“添加/删除程序”模块的时候，会自动弹出警告窗口，而“添加/删除程序”则无法运行。

此外，在“添加/删除程序”分支中还可以对 Windows“添加/删除程序”项中的“添加新程序”、“从 CD-ROM 或软盘添加程序”、“从 Microsoft 添加程序”、“从网络添加程序”等项进行隐藏，通过这些策略项目的设置，起到了保护计算机中系统文件及应用程序的作用。

9.限制使用应用程序(Windows 2000/XP/2003)

如果你的电脑设置了多个用户，有些程序我们可能不希望其他用户随意运行，也能在组策略中设置。

打开“组策略控制台→用户配置→管理模板→系统”中的“只运行许可的 Windows 应用程序”并启用此策略，然后点击下面的“允许的应用程序列表”边的“显示”按钮，弹出一个“显示内容”对话框，在此单击“添加”按钮来添加允许运行的应用程序即可。以后一般用户只能运行“允许的应用程序列表”中的程序。