Circumventing Group Policy Settings

https://blogs.technet.microsoft.com/markrussinovich/2005/04/30/circumventing-group-policy-settings/

Group policy settings are an integral part of any Windows-based IT environment. If you're a network administrator you use them to enforce corporate security and desktop management policy, and if you're a user you've almost certainly been frustrated by the limitations imposed by those policies. Regardless of which you are, you should be aware that if the users in your network belong to the local administrator's group they can get around policies any time they want.

There are two steps to circumventing a group policy setting: identifying the setting's location and preventing the setting from being applied. There are many group policy references available, but since machine group policy settings store in the HKEY_LOCAL_MACHINE branch of the Registry and per-user group policy settings store in HKEY_CURRENT_USER, if you don't know the location of the setting that's preventing you from doing something you want you can use Regmon to find it.

The number of desktop lockdown settings available to group policy administrators is enormous. They can prevent you from doing anything from changing your desktop appearance and start menu to running certain applications. Two commonly applied settings include a pre-configured screen saver program so that users don't waste resources on frivolous screen savers, and a screen saver timeout so that systems aren't left indefinitely accessible when a user steps away. When these settings are in effect Windows omits the screen saver tab of display properties control panel applet or doesn't let you modify the screen saver or its timeout. I'm going to show you how to use the power of being a local administrator and Regmon to track down these settings and override them on your own system.

The first step is to launch Regmon and capture a trace of policy setting being read by whatever process enforces it. Explorer implements most policies, reading some at the time you login and others when you perform specific actions. If the policy setting is read during the logon process you must run Regmon in the local system account so that it captures a trace of your logon. You can do that by using psexec:

psexec –s –i –d c:\sysint\regmon.exe

The instance of Regmon that launches will survive subsequent logoffs and logons and capture all activity during those activities.

Explorer doesn't show the display properties dialog, but to easily determine which process hosts a configuration dialog such as the display properties dialog, simply run Process Explorer and highlight the dialog with Process Explorer's window-finder toolbar button. Process Explorer selects the owning process in response, which for the display properties dialog is a Rundll32.exe process (look at its command line in its Process Explorer properties dialog to see how it launches).

Next, search or visually scan the resulting Regmon trace for strings that you think might be in the name of the Registry key or value related to the policy setting you are targeting. For example, if you scan a trace of the display properties execution you'll find a query of HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System\NoDispScrSavPage. In the trace displayed below the value is set to 1, which means that a per-user policy is in effect and that the screen saver page won't show on the display properties.

rundll32.exe:1848	OpenKey	HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System	SUCCESS	Access: 0x1
rundll32.exe:1848	QueryValue	HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System\NoDispScrSavPage	NOT FOUND	
rundll32.exe:1848	CloseKey	HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System	SUCCESS	
rundll32.exe:1848	OpenKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System	SUCCESS	Access: 0x1
rundll32.exe:1848	QueryValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System\NoDispScrSavPage	SUCCESS	0x1
rundll32.exe:1848	CloseKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System	SUCCESS	
rundll32.exe:1848	OpenKey	HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System	SUCCESS	Access: 0x1
rundll32.exe:1848	QueryValue	HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System\NoDispSettingsPage	NOT FOUND	
rundll32.exe:1848	CloseKey	HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System	SUCCESS	
rundll32.exe:1848	OpenKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System	SUCCESS	Access: 0x1
rundll32.exe:1848	QueryValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System\NoDispSettingsPage	NOT FOUND	
rundll32.exe:1848	CloseKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System	SUCCESS	

Once you've identified a policy's Registry value you can prevent the policy from being applied by removing all access to the Registry key in which it's stored. Double-click on the value in Regmon's trace to open Regedit to the value, move to the parent key and open the security editor. In most cases the security of the key is inherited so you won't be able to just remove the existing access entries. Instead, you'll have to open the permissions editor's advanced security dialog and remove inherited security. If you try to edit the permissions of the key and you are denied access use the advanced security dialog to make yourself owner of the key (since the local administrator's group has the Take Ownership privilege assigned to it) and then you'll be able to modify its security.

The next time you open the display properties dialog it won't be able to read the policy settings and will behave as if the policy is undefined. Unfortunately, the HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System key doesn't store the screen saver selection or timeout policies, so if those are defined you'll see a dialog like this:

If you capture another Regmon trace and look through it for relevant values you'll find these queries:

rundll32.exe:5612	OpenKey	HKCU\Software\Policies\Microsoft\Windows\Control Panel\Desktop	SUCCESS	Access: 0x20019
rundll32.exe:5612	QueryValue	HKCU\Software\Policies\Microsoft\Windows\Control Panel\Desktop\SCRNSAVE.EXE	SUCCESS	"scrnsave.scr"
rundll32.exe:5612	QueryValue	HKCU\Software\Policies\Microsoft\Windows\Control Panel\Desktop\ScreenSaverIsSecure	SUCCESS	"1"
rundll32.exe:5612	QueryValue	HKCU\Software\Policies\Microsoft\Windows\Control Panel\Desktop\ScreenSaverSetting...	NOT FOUND	
rundll32.exe:5612	QueryValue	HKCU\Software\Policies\Microsoft\Windows\Control Panel\Desktop\ScreenSaveTimeOut	SUCCESS	"600"
rundll32.exe:5612	QueryValue	HKCU\Software\Policies\Microsoft\Windows\Control Panel\Desktop\ScreenSaveActive	SUCCESS	"1"
rundll32.exe:5612	CloseKey	HKCU\Software\Policies\Microsoft\Windows\Control Panel\Desktop	SUCCESS	

Once you remove all access to HKCU\Software\Policies\Microsoft\Windows\Control Panel\Desktop you'll be able to reopen the display properties dialog and select the screen saver of your choice. I recommend that you leave the timeout to whatever your network administrator has defined (or lower it) so that you don't get into real trouble by violating the security policy (as opposed to the usage policy you violate by changing the screen saver).

This demonstration highlights the fact that networks that run with users as local administrators have no way to police the usage of their computers. The reason that most networks leave their users with so much power is that many line-of-business applications violate basic security programming guidelines and won't run otherwise. However, by using Regmon and Filemon to find the Registry keys, files and directories that an application is unable to access as a limited user, and then defining security group policy settings so that limited users have access to those resources, network administrators can run users in limited accounts and gain real control of corporate computer usage and security policies.

Originally by Mark Russinovich on 4/30/2005 10:01:00 PM
Migrated from original Sysinternals.com/Blog