Understanding Group Policy “Tattooing”

By Darren Mar-Elia

CTO & Founder

SDM Software, Inc.

2008

Policies & Preferences

You've probably vaguely heard of registry tattooing as it relates to the old NT 4 system policy. Tattooing was the effect that you saw whenever you applied a registry policy to a computer or user and then removed that policy file. Even though the policy file was gone, those registry values that were set by the policy remained–tattooed into the registry until you explicitly removed them, either by setting the policy to the opposite value or manually going in and deleting the registry values. This wasn't very helpful when managing systems or users that changed roles. As a result, when Microsoft introduced Group Policy in Win2K, they sought to change this tattooing behavior, at least for registry values. NT 4 System Policy became Administrative Templates in Win2000 (and later) Group Policy and with it came a new capability to prevent registry tattooing.

Basically, how Group Policy prevents registry tattooing is fairly simple. Microsoft has allocated 4 registry keys–2 under HKEY_LOCAL_MACHINE and 2 under HKEY_CURRENT_USER which are considered "no-tattooing zones". Any registry values placed under one of these 4 keys will be removed when the policy no longer applies. These 4 keys are:

```
HKEY_LOCAL_MACHINE\Software\Policies
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies
HKEY_CURRENT_USER\Software\Policies
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies
```

Most of the Admin. Template policies that you get out-of-the-box in Windows fall under one of these 4 keys. Microsoft has ensured that any applications that are part of Windows or built by Microsoft (e.g. Office) will look into one of these 4 keys to determine their behavior. So if you want to hide the Run command from a user's start menu, Explorer will look for a value called "NoRun" under HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer, and if it

finds it, and it's set to 1, the Run command will be hidden from the Start Menu. Registry values that fall under one of these above 4 keys are called, what else, Policies. Registry values that are controlled by Group Policy but do not fall under one of these 4 keys are called Preferences (this is not the same as "Group Policy Preferences", which came later and don't necessarily relate to this). Preferences don't benefit from the "no-tattooing zone" and thus if you set a preference within a GPO, and then remove that GPO, the preferences are not removed, just as in NT 4. Preferences are common when you create your own, custom ADM files, since in those cases you often have to set registry values that don't fall within these 4 "special" keys.

How It Works Under the Covers

You might wonder how this all works–how Windows manages to "un-tattoo" these policies when the GPO no longer applies. Well, the mechanism is quite simple really. Each time a foreground or background policy processing cycle kicks off, if Admin. Template policy is meant to be applied (that is, if the GPO has changed since the last time it was processed), the first thing that Windows does is remove all registry values under our 4 magic keys. This is known as a ResetPolicies operation.

Once all registry values under these 4 keys are removed, policy processing occurs normally. If any GPOs containing policies were removed since the last processing cycle, they won't exist anymore, since they were all removed by the ResetPolicies operation. In this way, Windows guarantees that policies don't tattoo the registry. A brute force but effective mechanism for cleaning things up that aren't used anymore.

Other Kinds of Tattooing

Registry policy is not the only area in Group Policy that is subject to tattooing. Basically any policy area that does not have an option to explicitly remove itself if the GPO falls out of scope of the computer or user will leave a trail

behind. Some obvious ones that come to mind include registry and file system security policy. These policy areas aren't undone if the GPO no longer applies. In the case of registry and file system security, permissions are changed only when the GPO is applied, but since there is no easy "rollback" of file system or registry security, these permissions changes linger after the policy is removed.

Similarly, Software Installation and Folder Redirection policy can be tricky in terms of its tattooing effect. Both have options to "un-do" things that were done, like uninstalling software when the machine or user falls out of scope or redirecting My Documents back to the local user profile in the case of Folder Redirection policy. However, in both cases this mechanism has proven problematic for administrators and users alike. So, its important to never un-do one of these kinds of policies lightly without a good plan in place for dealing with the fallout.