The .Default user is not the default user

devblogs.microsoft.com/oldnewthing/20070302-00

March 2, 2007

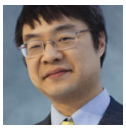
Raymond Chen

If you ever gone spelunking in the `HKEY_USERS` registry key, you've no doubt found the user named `HKEY_USERS\.Default`. Who is this guy? Despite its name, the profile for the .Default user is not the default user profile. It's actually the profile for the Local System account and is an alias for `HKEY_USERS\S-1-5-18`. (`S-1-5-18` is the security identifier for the Local System account.) Consequently, settings in `HKEY_USERS\.Default` are used by programs and services that run as Local System. The most visible examples of programs that run as Local System are `winlogon` and `logonui`, the programs that display the interface for logging onto the system. Whatever color scheme and screen saver you choose for the Local System profile get used at the logon screen. Unfortunately, the name `.Default` has led people to believe that this user's settings are the basis for new user profiles. In retrospect, calling it `.Default` was probably a bad decision. It just gave people the wrong idea. Here's one customer that was faked out:

> I'm setting the values in `HKEY_USERS\.Default\International` but when I create a new user, that user doesn't pick up those settings. I'm stumped.

The registry settings for new users do not come from the `.Default` user. Rather, they come from what I've started calling the "template user", which is kept† in the file `C:\Documents and Settings\Default User\ntuser.dat`. This hive is not loaded most of the time (since there's no reason to waste memory on something that is needed only rarely), so if you want to make a change to the template user, you'll have to load the hive manually. Mind you, messing with the template user hive directly is most likely not supported. The supported way of modifying the template user hive on Windows XP is to use the system preparation tool "SysPrep". Boot into factory mode, make your customizations to the current user, then reseal. The resealing process propagates the current user's settings to the template user (or, more specifically, the ones that can safely be propagated to the template user—you don't want to propagate things like encryption keys) before "resealing" the system for deployment. (No, I don't know what the mechanism is for Windows Vista.) **Nitpicker's corner**

†s/which is kept/which is typically kept on US-English systems/

Raymond Chen

Follow