searchWin2000.com Manageability

April 2, 2003 a newsletter from TechTarget

Windows 2000 in the Enterprise: Technology strategies in action

Securing public computers with loopback processing

by Douglas A. Paddock, MCSE, MCT, CIWSA, CIWCI, A+, N+

All right, I'll be the first one to admit it. I'd rather take a whipping than allow any of my computers to be put in a place where the public can freely access them. In fact, I don't like to let domain users use *their* computers. It's kind of like where I teach. I could get so much more done if I didn't have to be bothered by students. Every time you let a user near a computer, something happens, and the administrator has to fix it.

Believe it or not, there is a way to help alleviate this problem in Windows 2000 group policies, and it's called loopback processing. To view the loopback processing setting, either open an existing group policy object (GPO) or create a GPO using the Microsoft Management Con! sole (MMC) and proceed to Computer -> Administrative Templates -> System -> Group Policy -> User Group Policy loopback processing mode. The default setting for loopback processing is "Not configured."

First, let's review. As you probably know, GPOs are applied in this order: Local, Site, Domain and OU (the famous LSDOU you saw when you studied), with OU being the strongest and Local being the weakest. The closer a GPO is to the user, the "stronger" its settings effectively become. If there are multiple GPOs affecting a specific Local, Site, Domain or OU Active Directory object at a particular location (for example, if there are three GPOs in the same OU), the GPO at the top of the list is applied last and is the overruling GPO.

Last checkbox wins

The easiest way to look at this is to compare a GPO setting to a checkbox. Every GPO starting with Local gets a chance to put either Not Configured, Enabled or Disabled in the checkbox. Obviously, the last one to write to a particular checkbox wins. Since Local goes first, it is the weakest; every other policy gets a chance to overwrite its settings. The GPO at the top of the list in the location where an object resides gets applied last and is therefore the "strongest" GPO.

While a user's computer is often in the OU where the user is located, this is by no means always true, and it often depends on the administrative model used by the company in question (centralized or decentralized, and so forth). This is important, because a GPO is divided into two major parts, the **Computer Configuration** portion and the **User Configuration portion.**

Computers get their settings upon boot-up from the Computer Configuration portion of any GPOs that apply to them, and users get their configuration from the User Configuration portion of any GPOs that apply to them. In the event of a conflict between the Computer Configuration and the User Configuration portion of the same GPO, the Computer Configuration wins. There are not a lot of settings that conflict between the two, but there are a few (which are outside the scope of this article). The point to understand here is that a user gets his settings from a different place than the computer does. In a few special cases, this can cause problems that require the use of loopback processing to solve.

Loopback processing is intended for computers that are used by many users, such as computers used in public labs, classrooms and so forth. When users log on to one of these computers, you usually do not want them to have the rights they would have when they lo! g on to their home computer, because you do not want them! changing the settings on a public computer. Whether the user is a guest in your company or a regular user with a domain account, you want to give him only limited rights on a public computer.

Special privileges

Loopback processing lets you override a user's privilege settings so that instead of having his usual privileges, he has a special set of very limited privileges that you specify. It's a good idea to place all of your special purpose computers that will use loopback processing in their own GPO(s) for ease of GPO management. There are three settings we need to look at for loopback processing.

The first (and default) setting is Not configured; Not configured is the default because most computers don't need loopback processing. Enough said there.

The second setting is Enabled. In Enabled mode, there are two settings, Replace and Merge. Replace uses the settings in the computer's User Configuration secti! on of the GPO, instead of finding the settings for the user who is logging on in that user's list of GPOs. This is an excellent method for doing a complete lockdown on the computer in question, since all users will have the same rights you specify in the GPO, regardless of which computer they normally use to log on. Merge Mode lets a user's settings apply but changes the normal order of GPO application. In merge mode, the user's settings are applied first, instead of the computer's. The computer's settings are then applied last. If there is a conflict between the two, the computer's GPO settings will override the settings the user would have received from his normal GPO list.

The last setting is Disabled. If you use Disabled, or if you don't configure loopback processing at all, the effect is the same, and the user gets his normal GPO settings.

By using loopback processing, you can ensure that *no* users will change desktops, add or delete prog! rams, run unauthorized programs, use the run command, or ! generally do anything you don't want them to do on a public computer. If you have to expose a computer to public usage, loopback processing is one of your handiest tools for nailing it down tight.

For more information on this subject, see Microsoft Knowledge Base article 231287, or see "explain" under the loopback processing option in the GPO you are creating.

About the author: Douglas Paddock is an IT instructor at Louisville Technical Institute in Louisville, Ky. He holds CIW Security Analyst, MCSE, MCT, MCSA, A+ and N+ certifications.

MORE ON THIS TOPIC:

>>Visit our best Web links on Group Policy and IntelliMirror

>>Ask security expert Scott Blake a question

Rebuttal: True IT blooper
We received an overwhelming reader response to *Oops! True IT blooper 97: DOS, we hardly knew ye* and have published some excerpts from our favorite letters here. -- *The editors*

ABOUT THIS E-MAIL:

This e-mail is brought to you by **TechTarget** where you can get relevant search results from over 20 industry-specific Web sites.

If you no longer wish to receive this newsletter simply reply to this message with "REMOVE" in the subject line. Please allow 24 hours for your "REMOVE" request to be processed.