Iowa State University
IT Services Technical Notes

IT

Windows Enterprise
OU Administrator Policy and Procedures
Group Policy Object Procedures

Steven L. Kunz
Last update: January 21, 2011

When a “Group Policy Object” (hereafter referred to as a “GPO”) is created by an OU administrator there are four main areas of GPO management to keep in mind:

Naming of GPOs

You will probably find it most useful to establish a naming convention (probably based on your department abbreviation) to name your GPO. Since all actual GPO objects live together in one container, a naming scheme will help you identify all GPOs created by the OU admins in your department.

Ownership and Access Control of the GPOs – Important Defaults to Leave Alone

IMPORTANT – Every GPO is created with full access (edit/delete/modify) for the groups “Enterprise Admins” and “Domain Admins”. In addition, the group “ENTERPRISE DOMAIN CONTROLLERS” has “read” access. DO NOT REMOVE OR MODIFY these default permissions. There are processes that run (such as a domain AD schema update) that must edit every GPO in the domain. Removing the default access for these groups causes considerable delay. The Enterprise Admins need to restore the default access controls for each such GPO one-by-one. It does not make them happy.

Ownership and Access Control of the GPOs – Defaults to Change

Windows by default will give full control to only the OU admin creating the GPO. It will also set the “ownership” of the GPO to that OU admin. Unless the creator remembers to add other groups (such as "!<ou> Admins") at the time they create it, the real possibility remains that the GPO will be "orphaned" when the original OU admin leaves (the replacement OU admin will not be able to alter the GPO object). This means the ITS Enterprise Administrators are the only recourse for the new OU admin to recover control of the GPOs used by the department.

After creating each GPO you should use the Group Policy Management console to alter the delegated control of the GPO. Select the GPO link, then select the "Delegation" tab. Use the “Add” button to add "!<ou> Admins” with the power to “Edit settings, delete, modify security”. Next use the "Remove" button to remove privs granted only to you.

The “ownership” of the GPO should also be altered so it is owned by the same "!<ou> Admins”. Do this with the “Advanced” button to get the “Security Settings”, then click

“Advanced” again and find the “Owner” tab. Click the “Owner” tab and add the “"!<ou> Admins” as an “Other Users and Groups” item. Highlight "!<ou> Admins” in the list and click “Apply” to change the ownership to the "!<ou> Admins” group.

Multiple Links to a Single GPO

Remember that a single GPO can be “linked to” from multiple OUs. If you have a common GPO that you apply to ten separate OUs within your departmental OU, you do NOT need ten GPO objects. You need ONE GPO object, linked to from ten locations. This has the added benefit in that you only have to change ONE GPO to cause the change to be reflected in all ten locations (the ten locations linked to the one object).

A “link” to a GPO is seen by the “scroll with a little arrow on it” with the OU structure as viewed with the Group Policy Management console. The “Scope” tab shows the GPO “linked to” (the GPO itself actually resides in the “Group Policy Objects” container).

The actual GPO itself is viewed in the “Group Policy Objects” container (near the bottom of the domain container in the Group Policy Management console). You can see each place it is linked to with the “Scope” tab.

Cleanup of Unused GPOs

Multiple GPOs may be created when experimenting with various settings. However, each GPO is an object that must be stored and replicated throughout the domain controller structure. Please remember to delete any of your GPOs that are not linked to any OU locations if you are fairly sure you won’t need them in the future. Try not waste Enterprise GPO storage or replication bandwidth with lots of unused GPO objects.