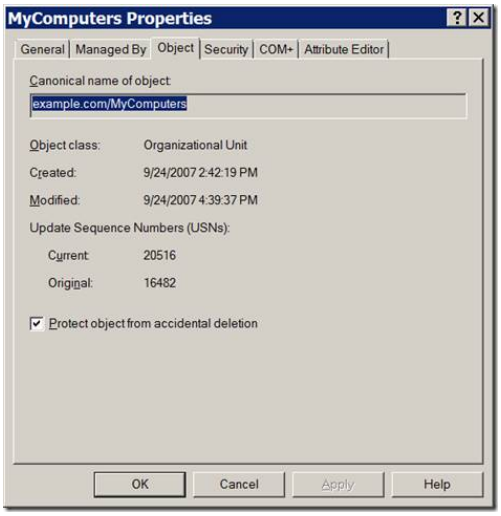
KAK - Protect AD Objects from accidential deletion

http://msmvps.com/blogs/ulfbsimonweidner/archive/2007/09/25/protect-objects-from-accidential-deletion-in-windows-server-2008.aspx

Avalialbe in the GUI of Windows Server 2008, but also possible in any version of Active Directory, you are able to protect any object from accidental deletion. I had to recover a couple productive ADs over the past couple years, and everytime it was because of a accidental deletion. Also I've seen that OUs have been accidentally moved - this happened propably to everyone with files/folders in Windows Explorer - you accidentally got stuck on the mouse-key while hovering over a folder and drop it accidentally on another folder.

So how do you protect objects from accidental deletion in Windows Server 2008? That's easy - first switch on the Advanced View, then go into the properties of the object in question. Here - on the "Object"-Tab - you'll find the new checkbox "Protect Object from accidental deletion".



By default, OUs created in Active Directory-Users and -Computers are protected. However, when you don't create the OU in Active Directory-Users and -Computers or you created them before you got Windows Server 2008 in your domain (how likely - I know) the OU will not being protected from accidental deletion.

However, what's quite interesting is what's being done in the Background: The Security-Descriptor of this object is being modified with a Deny-Entry for Everyone to delete and delete subtree. So it's downward compatible with Windows Server 2003 and Windows 2000, and you are even able to do this either manually or using DSACLS today.

If you want to use DSACLS to protect an OU you can use the following command:

```
dsacls ou=MyUsers,dc=example,dc=com /d Everyone:SDDT
```

So if you are creating your OU-Structure with "dsadd ou" you might want to use this command to protect the OU from deletion. The checkbox in the GUI will also reflect this change, however I've seen that it sometimes takes a while or is inconsistently displaying wheter the OU is protected or not, however this might be a bug in the current beta and you should make sure it's protected using the security tab to make sure it's protected.

As I said, you'd be able to do this today as well. And if you want to protect your whole OU-Structure, you can use the following command to protect every OU in the domain:

```
for /f %i in ('dsquery ou -limit 0') do dsacls %i /d everyone:SDDT
```

Update: Marcus has pointed out that I the above command is only working if your OUs don't include any spaces. That's right, the for-command takes spaces as a delimiter and therefore will put everything behind the first space in the variable %j, after the second space in %k a.s.o. So here's the corrected command which allows spaces in your DN ("tokens=*" state that everything should be included in the first variable, you could also do a 1,3,* which would put the first part into %i, the third into %j and the rest in %k,.. Marcus suggested another way which would also work by not specifying any delimiters "delimns="):

```
for /f "tokens=*" %i in ('dsquery ou -limit 0') do dsacls %i /d everyone:SDDT
```

If you just want to protect certain levels, you only need to change the dsquery command.