

Re: Remote Desktop Users and Least User Rights

Do you use AD? I'd surely hope so, if you have hundreds of machines.

If so, you have several options – you could use Restricted Groups (via group policy) to add an AD group to each local workstation's RemoteDesktop group, or you could create a simple startup script assigned via GPO to add them. Restricted groups can be handy, but they can also be a bit of a PITA as they will always replace the entire local group membership with whatever you defined (rather than merely adding). So, I tend to use the startup script method.

Also, I personally don't set up a one-to-one relationship between a domain user & his/her workstation; if that PC isn't working, I want them to be able to connect to another that is. Hence, I don't add only Joe to Joe's computer "Remote Desktop Users" group.

E.g., you could set up AD security groups called LocalAdmins, LocalPowerUsers, LocalRDUsers.

The batch file would have this:

```
.....  
net localgroup administrators DOMAIN\localadmins /add  
net localgroup power users DOMAIN\localpowerusers /add  
net localgroup remote desktop users DOMAIN\LocalRDUsers /add  
.....
```

You can create/link a new GPO at the appropriate OU where your computers live (if you haven't created custom ones, you'll need to – unless you're using SBS, which creates its own hierarchy).

Edit the GPO – go to Computer Configuration \ Windows Settings \ Scripts (startup/shutdown)

Double-click Startup, click Add

Copy the batch file you created to the clipboard, then paste it in the window here

Exit/apply/ok/finish whatever

All the computers in this OU should have the startup script applied when they restart, and you can now control all this centrally, while sitting comfortably at your desk eating bon-bons. Add whomever you like (whether individual users, or other AD security groups) to the LocalRDUsers group and they'll have access.

Kudos on the plan to secure your workstations – users shouldn't run w/admin rights.

Thanks for the information.

We do run AD, but I currently don't have the rights for doing group

Re: Remote Desktop Users and Least User Rights

policies. Before I'm given those rights I need to jump through a few hoops by taking a group policy class and basically proving that I'm not a total chowder head. I think they call it quality control! :-)

That being said, I am planning on using the Restricted Groups policy to accomplish some of our goals. I'm told that the Restricted Groups policy alone does not get us all the way there in terms of restricting user rights, and that it does, as you point out, come with it's own bag of issues. Guess I'll have to take the class to get more information on that. In the mean time, I'll run your ideas by someone who does have the permissions to work with our group policies and we'll test them out.

Sure thing – it's good to do research first. You might consider setting up a lab environment (even using virtual servers/PCs) to play with this. The Group Policy Management Console is a must (you need W2003 servers to run this on, although you could install/run it on a WinXP box too – just not W2k) . You can use modeling/etc to test stuff before you implement it. Very handy. Try subscribing to microsoft.public.windows.group_policy & lurk there for a while.

I'm not sure why the users with remote access were setup the way they were. That was all done before I was hired.

This is a common occurrence....and it's a good one to address.

We do have a Citrix farm with a couple of Citrix admins. It seems to me that we could just setup access through our Citrix portal to whatever applications people need to use from remote locations and avoid the issue on the desktop entirely.

Yes, that's also true – and you'd have an easier time with central administration of your apps/data that way, plus easier centralized security/access.

--Tom