

## RE: Helpdesk as local admin

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2007-02/msg00064.html>

---

- *From:* "Scott Ramsdell" <[Scott.Ramsdell@xxxxxxxxxxxx](mailto:Scott.Ramsdell@xxxxxxxxxxxx)>
  - *Date:* Mon, 5 Feb 2007 10:56:43 -0500
- 

WALI,

By default all users have the right to add 10 machines to the domain. You can modify the default domain controller policy (not default domain policy) to change this.

I routinely create a group for adding machines, and delegate the right to add machines to this group and domain admins, removing authenticating users. Sometimes office managers need to add machines such as at a remote site without local help desk staff, and I could add them to this group without giving them any other help desk level privilege.

In my experience, the help desk staff needs access to the local admin accounts. So, I cut and pasted a script together that would change the local admin passwords and would run the script after any IT personnel left.

Local admin passwords on the laptops/desktops should certainly be different than the local admin passwords on your servers.

Walking around the building, I would sometimes hear the users mention the local admin password and using it to do something they otherwise couldn't.

I would have to review with the help desk staff the importance of keeping this password known only to their group, but invariably the help desk staff would give the password out to users who had ran into an issue while out of the office. Usually, this was the screen saver lockout coming on during a Power Point presentation.

So, periodically, I would change the local admin password even if no-one had left. Also, I created a group that wouldn't apply the screen saver lockout and asked secretaries to let me know if an exec was traveling so I could drop them in that group.

Kind Regards,  
Scott Ramsdell

-----Original Message-----

RE: Helpdesk as local admin

From: listbounce@xxxxxxxxxxxxxxxxxxxxx [<mailto:listbounce@xxxxxxxxxxxxxxxxxxxxx>]  
On Behalf Of WALI  
Sent: Saturday, February 03, 2007 7:59 AM  
To: security-basics@xxxxxxxxxxxxxxxxxxxxx  
Subject: Helpdesk as local admin

Hi Guys..

So what's the defined best practise regarding HelpDesk personnel be given/told local admin account names and passwords on users PC/Workstations in order to undertake routine fault finding and applications installation?

Help Desk techies also regularly inserts new workstations into the domain hence they need certain privileges to be able to make new workstations join the domain. What could be the most secure way given the fact that Servers are running Win 2k3 and client