

## Please help!!!!I'm Desperate!!!

**Source:** <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2002-07/3952.html>

---

**From:** knsa ([knsa73@hotmail.com](mailto:knsa73@hotmail.com))

**Date:** 07/21/02

From: "knsa" <[knsa73@hotmail.com](mailto:knsa73@hotmail.com)>  
Date: Sun, 21 Jul 2002 09:15:18 -0700

There's ways of getting in, such as doing a second install of Win2K to the same system so that you can access and copy your data off. However, this approach doesn't really let you use your machine again, until you reinstall your apps. A technique that might work (provided your wife didn't update the emergency repair info) would be to boot the machine with your Win2K cd, choose the repair option on the main screen, R again to access the repair process, M to manually direct the repair and...dammit where's the option to recover the SAM?! (Sorry I was doing this procedure on a Thinkpad here, just so that I could give you accurate directions). Looks like you'd need access to the Recovery Console in order to move the repair copy of SAM from \system32\repair over to the system32\config directory. This used to be an option on NT 4.0's automated recovery options, but apparently not anymore. Nonetheless, doing a secondary install of win2k (to a different directory!) and then booting into that option will allow you to specify a new admin password for that installation, which will then allow you to copy the file over to the correct location of your older one. Confusing isn't it? But free.

Another option would be ERD commander (written by Winternals.com). The boot CD will allow you to load the security hive and reset the local administrator's password, WITHOUT requiring you to provide the current password in order to do it. Basically the app looks like a buffed-up version of Microsoft's Recovery console without the imposed limits on reading an NTFS-formatted drive's directory structure, and allows files to be written to removable media without requiring a permissions through the implementation of the Security Policy object. All you do is boot off the CD...run "loadreg"...and then type pass "administrator "password". All just as neat as you

microsoft.public.win2000.security: Please help!!!!I'm Desperate!!!

could wish...except that the program costs \$399! Kinda  
sad when a company knows it's got you by the throat, isn't  
it?

Please help!!!!I'm Desperate!!!