

Windows Password Recovery using RescueBRU

1. Boot a RescueBRU client CD on the machine that needs the password reset.
2. At the RescueBRU main menu, exit to shell. Open a new terminal window by clicking the icon on the taskbar.
3. At the prompt, type:
`ntfs-3g /dev/sda1 /mnt/windows`
and press enter.

- Note that /dev/sda1 is the first partition on the boot drive. This usually corresponds to the C: drive in Windows, but may not in all cases. We will determine shortly if this is the correct partition. If the computer uses an HP CISS RAID controller, the first partition may be /dev/cciss/c0d0p1. If the computer uses NVMe drives, the first partition may be /dev/nvme0n1p1.
4. At the prompt, type:
`cd /mnt/windows/WINDOWS/system32/config`
and press enter.
5. If you get an error saying "No such file or directory", you have mounted the wrong partition. Type:
`cd; umount /mnt/windows`
and press enter. Repeat steps 3 and 4 and try a different partition in the ntfs-3g command (/dev/sda2, for example). If step 4 did not produce an error, continue with step 6.
6. At the prompt, type:
`chntpw SAM`
and press enter.
7. The chntpw menu will appear. Look in the Account bits section and see if "Disabled" is checked. If so, proceed to the next step. If not, proceed to step 11.
8. Type 4 at the Select: [q] > prompt and press enter. You should see "Unlocked!"
9. Type y at the Write hive files? (y/n) [n] : prompt and press enter. You should see "0 <SAM> - OK"
10. Perform step 6. The chntpw menu will appear.
11. Type 1 at the Select: [q] > prompt and press enter. You should see "Password cleared!"
12. Type y at the Write hive files? (y/n) [n] : prompt and press enter. You should see "0 <SAM> - OK"
13. At the prompt, type:
`cd; umount /mnt/windows; sync`
and press enter.
14. Ensure that you have removed the RescueBRU client CD from the drive and at the prompt, type:
`reboot`
and press enter.
15. The PC will reboot into Windows. It may want to run a chkdsk. Allow the chkdsk to run. The Administrator account has a blank password. This may cause the PC to automatically log in to Windows after reboot. It is strongly recommended that a new Administrator password is set before returning the PC to service.

Revision Information:

Revision 1 – 1/28/2015 – Initial release.

Revision 2 – 3/19/2021 – Updated to reference NVMe drives.