

Create a Boot Disk to Reset Your Windows Password

Hopefully you've never had to experience the trauma of forgetting a password to a computer. Obviously, it's not the end of the world when it happens, and there are ways of getting around a login password without any harm to you or your computer. Today we are going to bestow this sacred power into your mortal hands.

You'll need:

- USB drive
- Windows computer or laptop
- Administrator account access

1. Download Password_Reset_Creator.zip

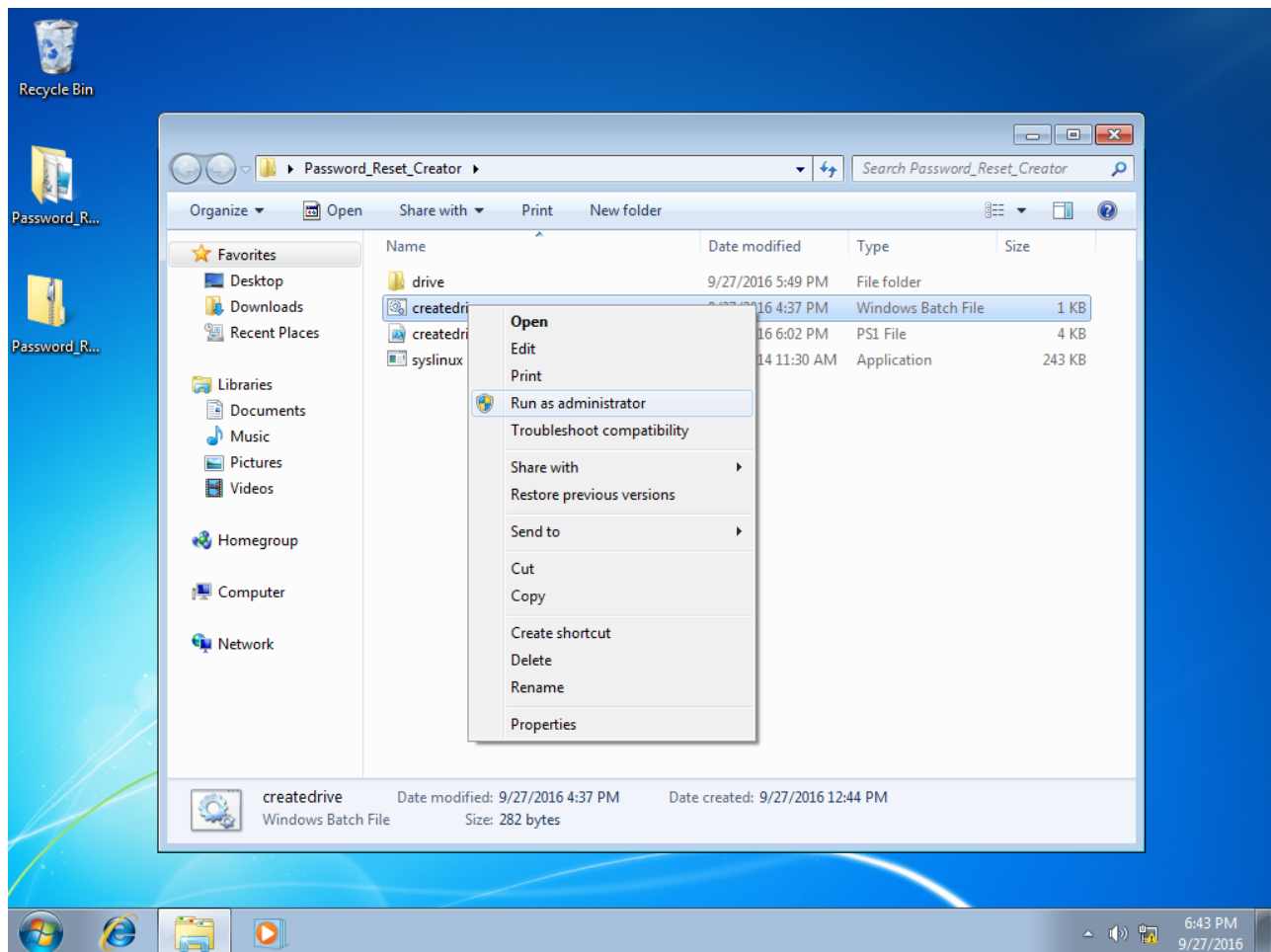
Open up a web browser and navigate to <http://tinyurl.com/ENGL316-pw>. This will download Password_Reset_Creator.zip.

2. Extract the contents of the zip file

Open up your downloads folder, right click 'Password_Reset_Creator.zip', and select "Extract All". Click the extract button when a popup comes up to confirm the location to extract it to.

3. Run 'createdrive.bat' as administrator

In the newly opened folder, right click 'createdrive.bat' and select "Run as Administrator".

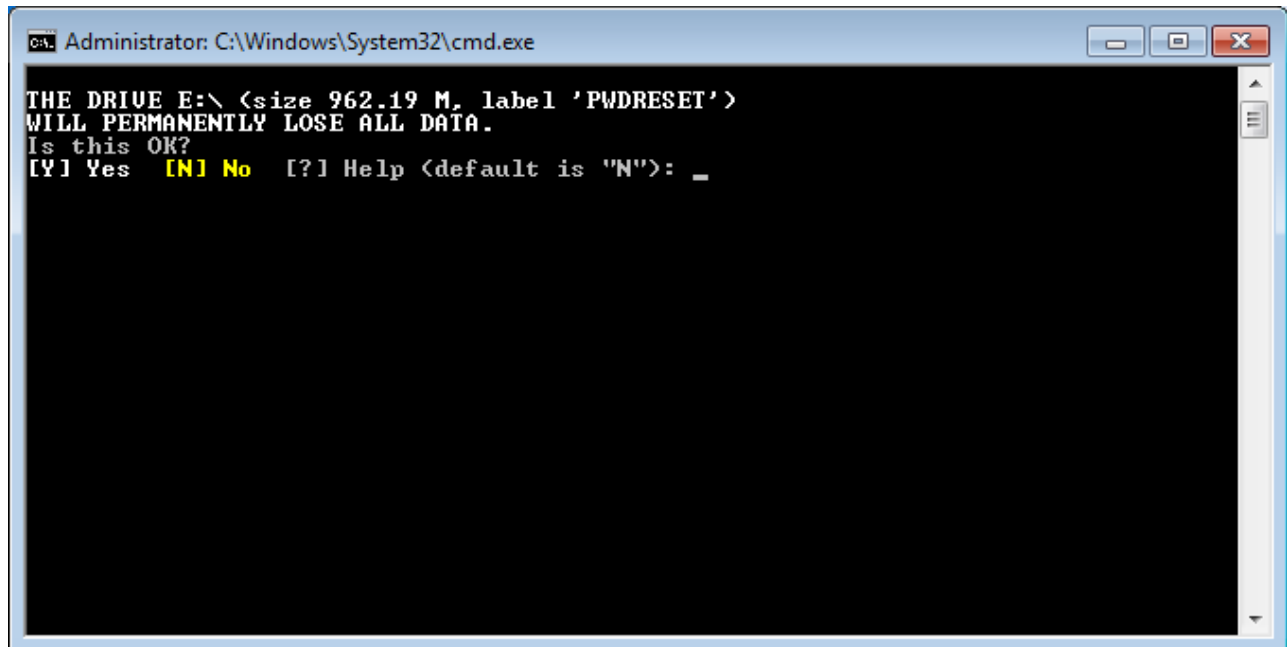


Select "Yes" at the prompt.

4. Confirm the flash drive to use

If you have more than one USB drive inserted, you will be prompted to choose which one to erase. The script will then ask you to confirm your choice.

Caution! All data will be erased from the flash drive! Please backup any data on the flash drive beforehand, and make sure you are using the correct drive.



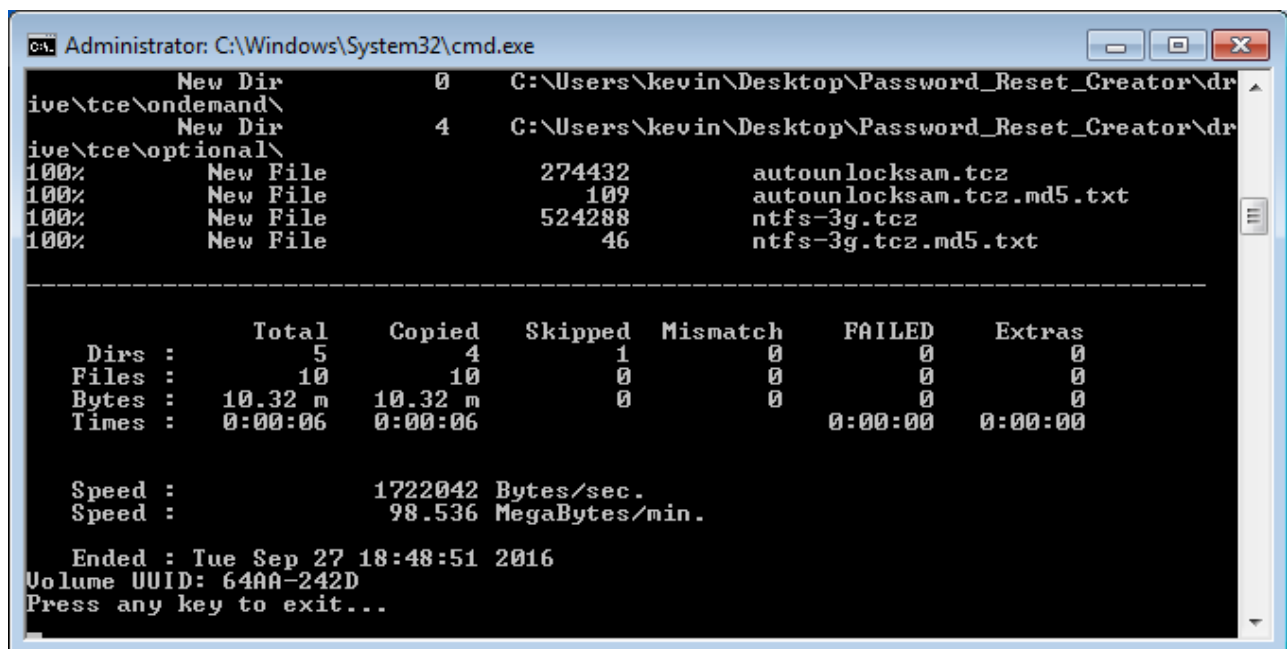
```
Administrator: C:\Windows\System32\cmd.exe

THE DRIVE E:\ <size 962.19 M, label 'PWDRESET'>
WILL PERMANENTLY LOSE ALL DATA.
Is this OK?
[Y] Yes  [N] No  [?] Help <default is "N">: _
```

Once you type "Y" for yes, press the enter key and watch the script run.

5. Exit the program and restart Windows

The script is finished when it says "Press any key to exit..."



```
Administrator: C:\Windows\System32\cmd.exe

New Dir          0      C:\Users\kevin\Desktop>Password_Reset_Creator\dr
ive\tce\ondemand\
New Dir          4      C:\Users\kevin\Desktop>Password_Reset_Creator\dr
ive\tce\optional\
100%      New File          274432      autounlocksam.tcz
100%      New File          109      autounlocksam.tcz.md5.txt
100%      New File      524288      ntfs-3g.tcz
100%      New File          46      ntfs-3g.tcz.md5.txt

-----

      Dirs :      Total      Copied      Skipped      Mismatch      FAILED      Extras
      Files :      10      10      0      0      0      0
      Bytes :      10.32 m      10.32 m      0      0      0      0
      Times :      0:00:06      0:00:06      0:00:00      0:00:00

      Speed :      1722042 Bytes/sec.
      Speed :      98.536 MegaBytes/min.

      Ended : Tue Sep 27 18:48:51 2016
      Volume UUID: 64AA-242D
      Press any key to exit...
```

Exit the window and shut down the computer. You've now built the boot disk and put it on a flash drive. The next steps will show you how to use it.

6. Boot from the USB drive

When you turn your computer back on, look at your screen for an option that says "Boot Options", "Boot Menu", or "Startup Device". The specific hotkey may differ depending on what computer you use, but the hotkey should be listed next to the options listed on screen. Press that button as the computer starts up.

vmware®

Starting

Press F2 to enter SETUP, F12 for Network Boot, ESC for Boot Menu

Next, choose to boot to the USB drive.

If all goes well, you'll see this loading screen.

```
Booting Core 6.4.1
Running Linux Kernel 3.16.6-tinycore.
Checking boot options... Done.
Starting udev daemon for hotplug support... Done.
Waiting as requested... 4 sd 32:0:0:0: [sdb] Asking for cache data failed

Scanning hard disk partitions to create /etc/fstab
Setting Language to C Done.
Possible swap partition(s) enabled.
Loading extensions... Done.
Setting keymap to us Done.
Restoring backup files from /mnt/sdb1/tce/mydata.tgz /
Done.
```

This menu will come up next.

```
(/_--_-\)          www.tinycorelinux.net

login[1619]: root login on 'tty1'
Found Windows Partition at /dev/sda2
chntpw version 1.00 140201, (c) Petter N Hagen
Hive </mnt/sda2/windows/system32/config/sam> name (from header): <\SystemRoot\Sy
stem32\Config\SAM>
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 666c <lf>
File size 262144 [40000] bytes, containing 7 pages (+ 1 headerpage)
Used for data: 295/55672 blocks/bytes, unused: 6/5544 blocks/bytes.

<>=====<> chntpw Main Interactive Menu <>=====<>

Loaded hives: </mnt/sda2/windows/system32/config/sam>

  1 - Edit user data and passwords
  2 - List groups
    - - -
  9 - Registry editor, now with full write support!
  q - Quit (you will be asked if there is something to save)

What to do? [1] -> _
```

7. Select an RID

On this screen, you'll see a list of usernames and RIDs. Type in the RID to the left of the username you want to reset the password for. In this case, we want to reset the password for alyssa's account, so we type in "03eb".

```
<>=====<> chntpw Main Interactive Menu <>=====<>

Loaded hives: </mnt/sda2/windows/system32/config/sam>

  1 - Edit user data and passwords
  2 - List groups
    - - -
  9 - Registry editor, now with full write support!
  q - Quit (you will be asked if there is something to save)

What to do? [1] ->

==== chntpw Edit User Info & Passwords ====

: RID -|----- Username -----| Admin? |- Lock? --|
: 01f4 | Administrator           | ADMIN  | *BLANK*  |
: 03eb | alyssa                      |        |          |
: 01f5 | Guest                        |        | dis/lock |
: 03e9 | HomeGroupUser$              |        |          |
: 03ea | kevin                       | ADMIN  | *BLANK*  |

Please enter user number (RID) or 0 to exit: [3ea] 03eb_
```

8. Clear the password

Next, enter 1 to clear the user's password.

```

Username: alyssa
fullname: alyssa
comment :
homedir :

00000221 = Users (which has 3 members)

Account bits: 0x0210 =
[ ] Disabled           : [ ] Homedir req.       : [ ] Passwd not req. :
[ ] Temp. duplicate   : [X] Normal account    : [ ] NMS account    :
[ ] Domain trust ac  : [ ] Wks trust act.     : [ ] Srv trust act  :
[X] Pwd don't expir  : [ ] Auto lockout      : [ ] (unknown 0x08) :
[ ] (unknown 0x10)   : [ ] (unknown 0x20)    : [ ] (unknown 0x40) :

Failed login count: 0, while max tries is: 0
Total login count: 1

- - - User Edit Menu:
1 - Clear (blank) user password
(2 - Unlock and enable user account) [seems unlocked already]
3 - Promote user (make user an administrator)
4 - Add user to a group
5 - Remove user from a group
q - Quit editing user, back to user select
Select: [q] > 1_

```

9. Quit and write hive files

Now that the user's password is cleared, we can exit and reboot the computer. Press 'q' in the User Edit Menu and Main Menu to quit the program.

```

comment :
homedir :

00000221 = Users (which has 3 members)

Account bits: 0x0210 =
[ ] Disabled           : [ ] Homedir req.       : [ ] Passwd not req. :
[ ] Temp. duplicate   : [X] Normal account    : [ ] NMS account    :
[ ] Domain trust ac  : [ ] Wks trust act.     : [ ] Srv trust act  :
[X] Pwd don't expir  : [ ] Auto lockout      : [ ] (unknown 0x08) :
[ ] (unknown 0x10)   : [ ] (unknown 0x20)    : [ ] (unknown 0x40) :

Failed login count: 0, while max tries is: 0
Total login count: 1
** No NT MD4 hash found. This user probably has a BLANK password!
** No LANMAN hash found either. Try login with no password!

- - - User Edit Menu:
1 - Clear (blank) user password
(2 - Unlock and enable user account) [seems unlocked already]
3 - Promote user (make user an administrator)
4 - Add user to a group
5 - Remove user from a group
q - Quit editing user, back to user select
Select: [q] > q_

```

When it asks to "Write hive files?", make sure to enter 'y'! Otherwise, your changes will not be saved.

10. Reboot Windows and login

Finally, reboot Windows. Now you can login without a password to the account you edited! Congratulations!

And just like that, you're a personal computer system administrator. If you have a random PC that's account is locked, you can now get back in and use it like normal.