Sticky Keys Trick

https://www.thewindowsclub.com/reset-administrator-password-windows-sticky-keys

For a general Windows user, resetting a **lost or forgotten administrative password** can be a bit troublesome if you don't have the proper tools and techniques to reset it, depending on the underlying OS that you're using. However, there are several third-party free password recovery tools available in the market that can help you reset your password, but that's not our topic here. In this guide, we show you how to reset & recover a lost or forgotten Windows password using a simple **Sticky Keys** trick.

Sticky Keys enables users to enter key combinations by pressing keys in sequence rather than simultaneously. This is desirable, especially for users who cannot press the keys in combination due to some physical challenges. Although the method of enabling Sticky keys helps simplify various tasks, its system files can be replaced.

You can replace an Ease of Access system file like **sethc.exe**, with a Command Prompt, and then use **cmd.exe** to make system changes.

Before proceeding with this method, please make a note of the following:

1. When you reset a Windows password, all the files that have been compressed/encrypted using tools such as *Encrypting File Systems (EFS)* will be lost.
2. Stored Internet Explorer passwords and settings will be lost as well.

So if you have a **backup** it will be good for you.

TIP: Our Ease Of Access Replacer lets you replace Ease of Access button in Windows with useful tools, including CMD.

Reset Administrator password in Windows 11/10

For resetting the password, you will need a Windows PE bootable drive which can be used to access the command prompt where you will have to set the new password.

Follow the below steps once you have the Windows PE DVD booted and ready.

1. Boot from the Windows PE DVD and open Command Prompt from the Advanced troubleshooting menu.

2. Enter the drive letter where your Operating System is installed, which is usually the C: Drive. Initially, you should be on X: drive which is the default residence for Windows PE.

3. Type in the below command after replacing C with the drive where Windows is installed on your PC.

```
copy C:\Windows\system32\sethc.exe C:\
```

Reset Administrator password

4. After taking the backup of the original file, run the below command to replace it in the original location.

```
copy /y C:\Windows\system32\cmd.exe C:\windows\system32\sethc.exe
```

The above command should replace the sethc.exe file with the cmd.exe file.

5. Now, restart your PC and navigate to the screen where it requires a password. Press the SHIFT key 5 times.

6. A command prompt window should open where you can enter the below command and reset your account password. You can get the list of current users on your PC by using the command **net user**.

```
net user your_account  new_password
```

How to reset forgotten Administrator password using sticky keys trick in Windows

Well, that’s it! You should be able to reset the password now.

Once you are in, you should replace the cmd.exe file with the original sethc.exe system file.

---

1. On Windows computers, you press a special key to access the boot menu or BIOS. If your startup screen doesn't show you which key to press just before the Windows startup logo appears, reboot your computer and quickly press ESC, DELETE, F8, F9, F10, F11, or F12 right as it begins to start up. Search online for "boot menu" and the specific make and model of your computer to find the right key.

2. If the boot menu appears, select the **Boot from DVD** or **Boot from USB** option to boot from the Windows installation disc you inserted, then move on to step 5.
3. If the boot menu doesn't appear after a few restarts, try entering the BIOS menu instead: turn the computer off and on again, and press DELETE, F2, F9, F10, F12, or ESC. Search online for "BIOS" and your computer model to find the right key.
4. Once you're inside the BIOS, find the boot options and change the order or priority of your boot devices (often by using your arrow keys) to make the USB or DVD the top option. Then save the changes and exit the BIOS.
5. Reboot the computer again. You should briefly see the message `Press any key to boot from CD or DVD` or `Press any key to boot from USB device`. Press any key (such as the spacebar) *immediately* to boot from your DVD or USB.
6. When the Windows installation disc starts up, click **Next>Repair your computer>Troubleshoot>Command Prompt**, as shown in Figure 2-2. The menu order or the option names might look different, but look for the Windows command prompt.

Warning: *Make sure you* don't install *Windows 10 -- that would wipe out all the files from the PC you're trying to recover!*

An image with four Windows setup screens.
No Starch Press

Figure 2-2: Use the Windows installation disc to access the command prompt.

7. Once you've reached the Windows command prompt (usually a black, text-based window), type **c:** and press **ENTER** to change to the C: drive, as shown here:

```
X:\> c:
```

8. Enter the command **`dir`** to see a list of files and folders on the C: drive. Look for a folder called Windows (it will be marked <DIR>, short for *directory*).

```
C:\> dir
 Volume in drive C is Windows 10
 Volume Serial Number is B4EF-FAC7
 Directory of C:\
--snip--
03/15/2018 02:51 AM   <DIR>     Users
05/19/2019 10:09 AM   <DIR>     Windows *1
--snip--
```

This folder (*1) contains the operating system files, including the command prompt application and the Sticky Keys program file that we need to swap out to perform this hack.

9. If there's no *Windows* directory on the C: drive, try the same process in the D: drive by entering **`d:`** and then **`dir`**. If the D: drive doesn't have the *Windows* directory either, keep

going through the alphabet (E:, F:, G:, and so on) until you find a drive containing *Windows* in its listing.

Gaining Administrator-Level Access

Now to replace the *sethc.exe* Sticky Keys program with the *cmd.exe* command prompt program. Then we'll be able to create a new administrator account on the computer.

1. Enter the following three commands:

```
C:\> cd \Windows\System32\
C:\Windows\System32\> copy sethc.exe sethc.bak
C:\Windows\System32\> copy cmd.exe sethc.exe
```

   These commands enter the directory where we can find both *sethc.exe* and *cmd.exe*, create a backup copy of the Sticky Keys program, and replace the original Sticky Keys program file with a copy of the command prompt program file. This way, whenever the computer runs *sethc.exe*, it will open a command prompt window in place of the Sticky Keys program.

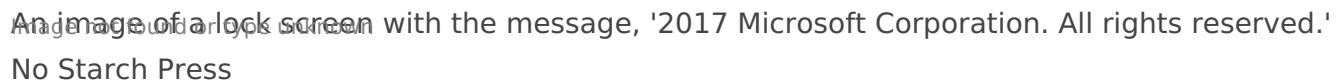

   Figure 2-3: Opening a command prompt window

2. After the third command, Windows will ask you if you want to overwrite *exe*. Enter **Y** to proceed.
3. Remove the Windows 10 installation DVD or USB and reboot the computer.
4. When the PC boots to the login screen, press **SHIFT** five times. Instead of the usual Sticky Keys program, you should see a command prompt window pop up *in front* of the login screen, as shown in Figure 2-3.
5. Enter the following two commands into the command prompt window:

```
C:\Windows\System32\> net user ironman Jarvis /add
C:\Windows\System32\> net localgroup administrators ironman /add
```

   The first command adds a user account named *ironman* with the password *Jarvis* to the Windows computer. The second command adds the *ironman* user to the list of local administrators. This means that when we log in as *ironman*, we'll have administrator-level access to all the files on the computer.

   Figure 2-4: We've successfully added a user named ironman as an administrator on this computer.

6. When you see a success message like the one in Figure 2-4, close the command prompt.

In addition to creating a new user account, you can also reset the password of an existing user from the command prompt window by entering **`net user`** followed by the existing username and the new password you want to set -- for example, net user bryson Thisisyournewpassword!. However, you should never reset another person's password without their permission and the permission of the computer's owner.

An image of a locked screen with login.
No Starch Press

Figure 2-5: You can now use the ironman user to log in to this Windows PC

Now You're an Administrator. Log In!

Congratulations! You now have access to the machine as an administrator. Go ahead and log in. Enter **`.\ironman`** as the username (or select **ironman** from the list of accounts, as shown in Figure 2-5). The dot and backslash before ironman tell Windows the account is local to the computer and not stored on a network server. After entering the username, enter the password, **`Jarvis`**.

An image of a Windows File Explorer page.
No Starch Press

Figure 2-6: As an administrator-level user, you can see all users' files, not just your own.

Since we made the *ironman* user a member of the local administrators group, you should have administrator-level access to *all* files and folders, including all users and documents *in C:\Users*, as shown in Figure 2-6.

When you click into another user's folder for the first time, you'll see a pop-up message saying you need permission to open another user's files, as shown in Figure 2-7. Since you're an administrator, click **Continue** to grant yourself permanent access!

The Sticky Keys hack works only on Windows machines. However, computers running macOS are vulnerable to physical access hacks as well.

An image with the message, 'You don't currently have permission to access this folder.'
No Starch Press

Figure 2-7: Administrators can give themselves permission to access anyone's files on the same computer.

Revision #3
Created 6 July 2024 21:11:39 by ColtM
Updated 7 August 2024 23:24:39 by ColtM