(HowTo) Windows login bypass

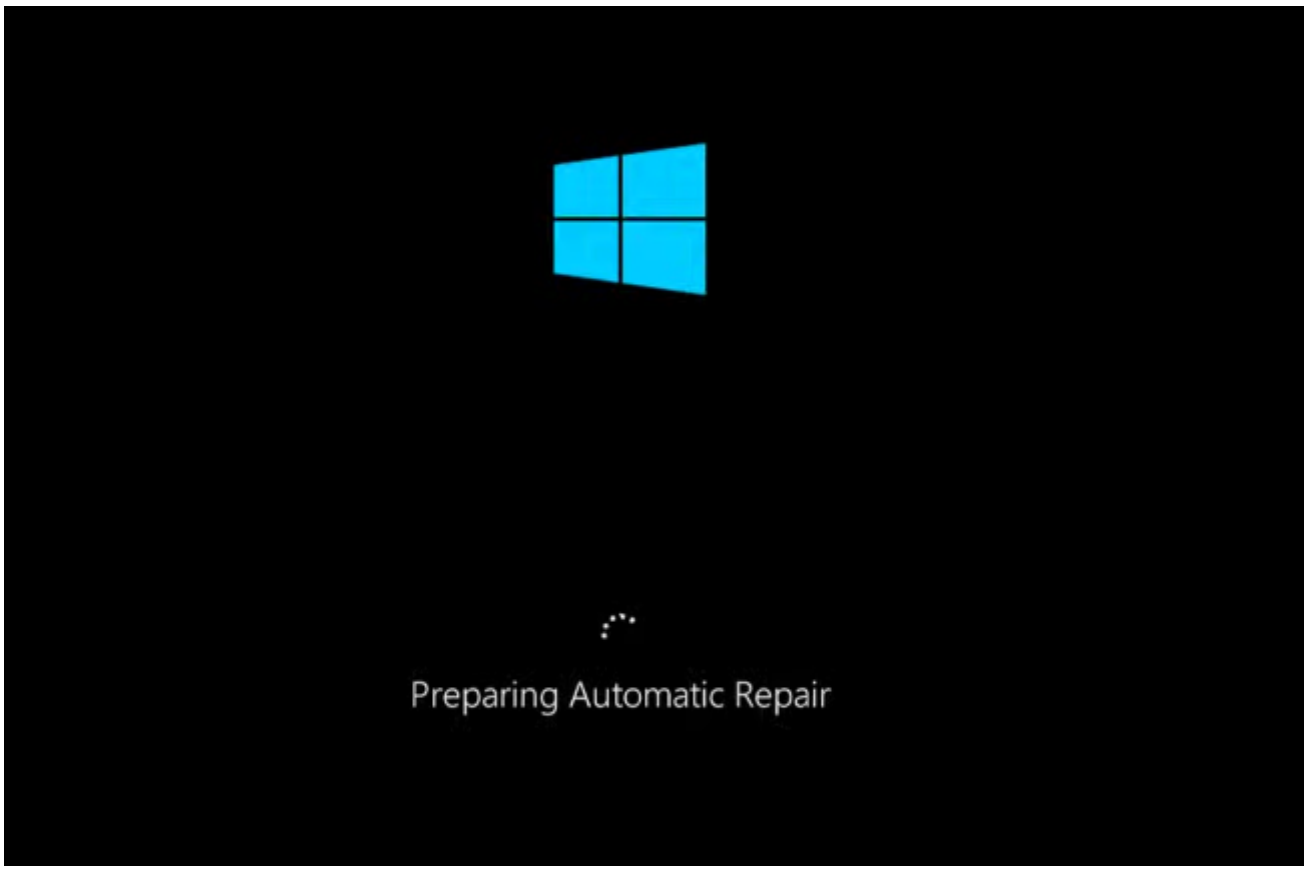
Description

This document will show you how to bypass the Windows user login password in a few different ways (Not tested with cloud account only local).

Steps

Method 1 (Ease of Access "GUI")

1. First turn off the computer.
2. Second turn it on then right away hold the power button to force it to shutdown.
3. Do step 1 and 2 twice and you should see automatic repair.



4. Once you see the blue screen click the following in the order below.
    1. Advanced Options
    2. Troubleshoot
    3. Advanced Options
    4. System Image Recovery
5. Once on the System Image Recovery screen click the following in the order below.
    1. Cancel
    2. Next

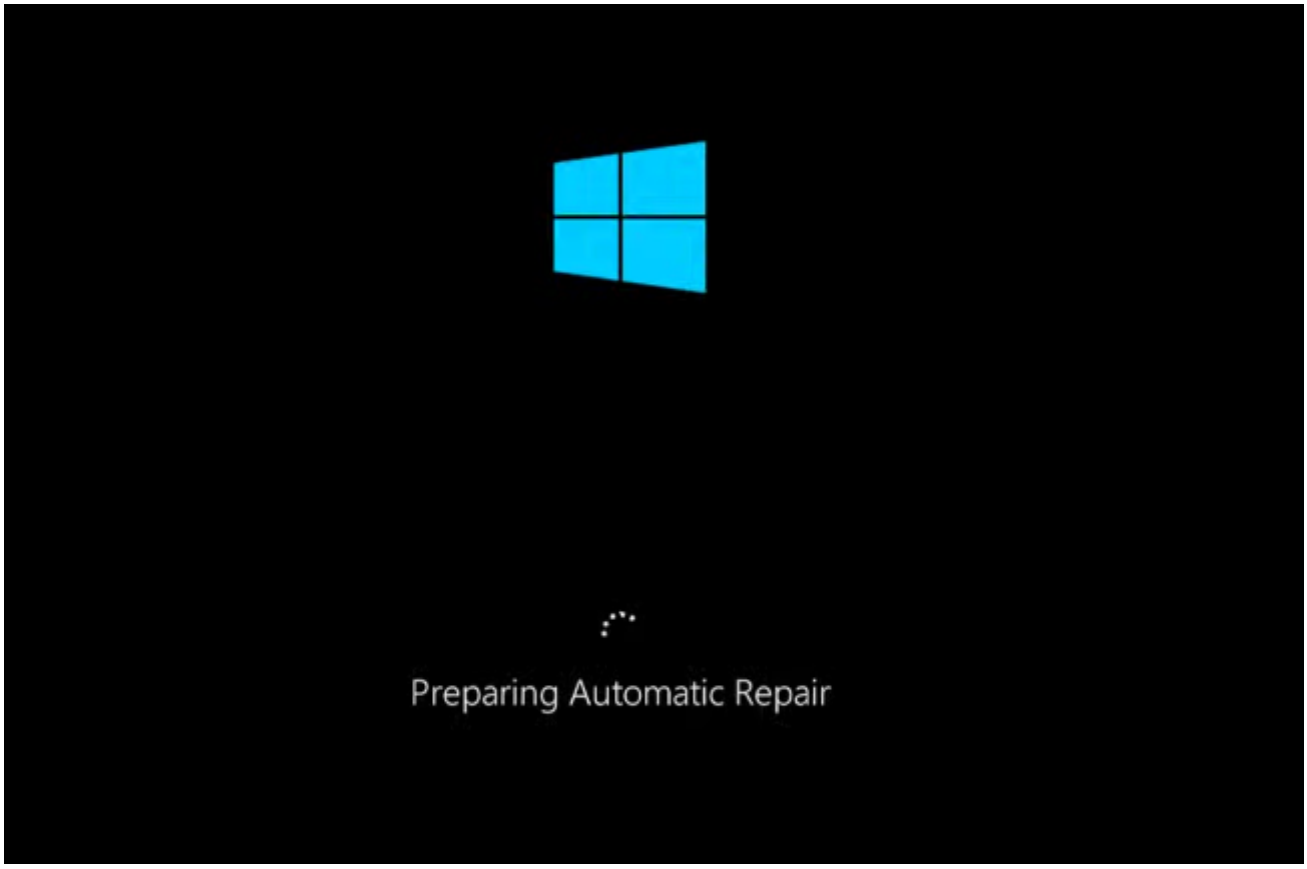
3. Advanced
4. Install a driver
5. OK

6. Once the explorer window is open do the following.
    1. Navigate to *E:\Windows\System32* (Choose your windows drive letter)
    2. Rename *Utilman* to *Utilman1*
    3. Rename *cmd* to *utilman*
7. Close the explorer window and click continue to restart the computer.
8. Once booted click on Ease of Access button to open CMD.
9. List all available users.
   `net user`
10. Reset the users password.
    `net user [USER] *`
    - Use double quotes if the username has spaces (e.g.: "user name").
    - For no password leave the new password blank, just press enter.
11. Clean up once logged on.
    1. Navigate to *C:\Windows\System32* (Choose your windows drive letter)
    2. Rename *utilman* to *cmd*
    3. Rename *Utilman1* to *Utilman*

Method 2 (Ease of Access "CLI")

1. First turn off the computer.
2. Second turn it on then right away hold the power button to force it to shutdown.

3. Do step 1 and 2 twice and you should see automatic repair.



4. Once you see the blue screen click the following in the order below.
    1. Advanced Options
    2. Troubleshoot
    3. Advanced Options
    4. Command Prompt
5. Once the command prompt window is open do the following.
    1. Navigate to *C:\Windows\System32* (Choose your windows drive letter)

       `c:`

       `cd Windows\System32`
    2. Rename *Utilman* to *Utilman1*

       `ren utilman.exe utilman.old`
    3. Copy *cmd* to *utilman*

       `copy cmd.exe utilman.exe`
6. Close the command prompt and click continue to restart the computer.
7. Once booted click on Ease of Access button to open CMD.
8. List all available users.

   `net user`
9. Reset the users password.

   `net user [USER] *`

    - Use double quotes if the username has spaces (e.g.: "user name")

    - For no password leave the new password blank, just press enter.

10. Clean up once logged on.
    1. Navigate to *C:\Windows\System32* (Choose your windows drive letter)
    2. Delete *utilman.exe*
    3. Rename *utilman.old* to *utilman.exe*

Resources

- YouTube video (Method 1): https://www.youtube.com/watch?v=4ZhA0C2YVw0
- YouTube video (Method 2): https://www.youtube.com/watch?v=sduC0y-bLrk