

Zaboravljena administratorska zaporka na Windowsima 10

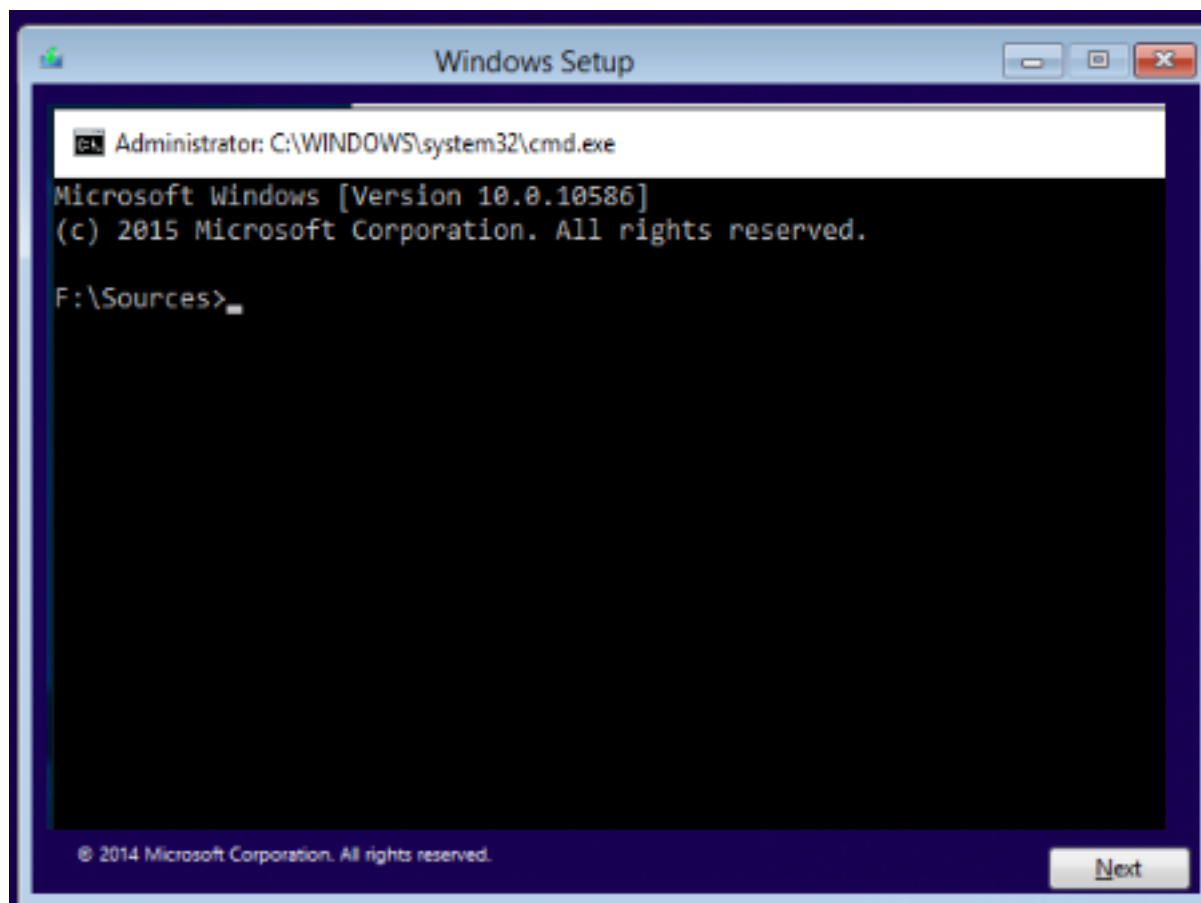


U članku <https://sysportal.carnet.hr/node/1570> [1] prikazali smo kako postupiti u slučaju zaboravljene zaporka na operativnom sustavu Linux, a u ovom članku pozabavit ćemo se zaboravljenom zaporkom na Windowsima 10. Da bi stvar bila zanimljivija, na računalu je bio samo jedan jedini korisnik s administratorskim ovlastima i mnoštvom važnih datoteka.

Od alata trebat će nam samo instalacijski medij Windowsa 10 (USB ili DVD, što nam je već pri ruci).

Prvo napravimo reboot računala s instalacijskog medija. Kad se prikaže sučelje Windows Setupa, pritisnemo tipke **Shift+F10**, što nam omogućava naredbenolinijski način rada. Nije potrebno podešavanje jezika i ostalih mogućnosti





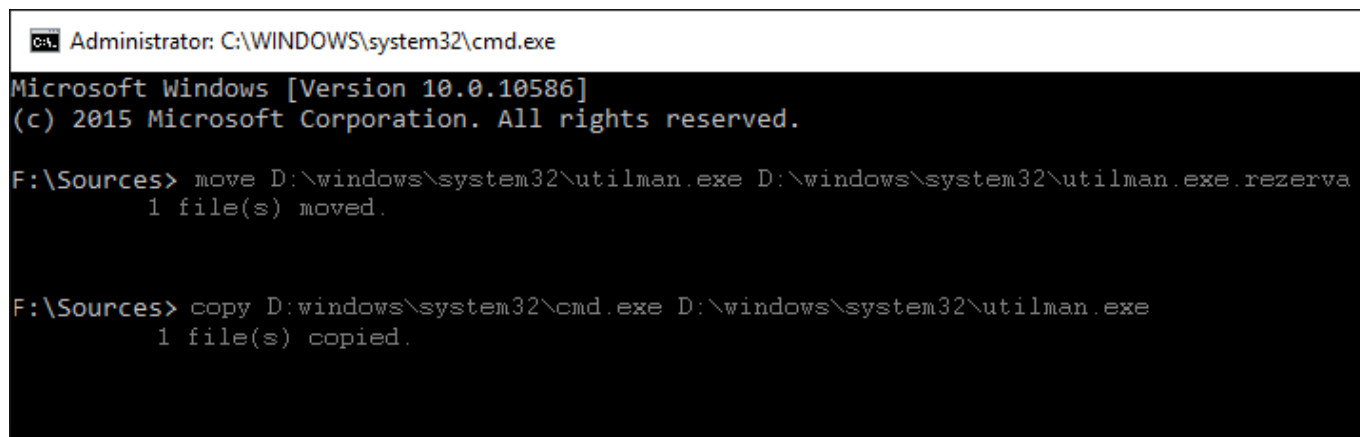
Sljedeći korak je preimenovanje datoteke "**utilman.exe**" u "**utilman.exe.rezerva**". Utilman.exe je Windows aplikacija koja omogućuje korisniku da konfigurira Accessibility alate Magnifier, High Contrast Theme, Narrator i On Screen Keyboard, ali ćemo ovaj alat uz određene "trikove" iskoristiti za zaobilazak windows logon procesa.

Datoteka utilman.exe standardno je smještena u direktoriju C:\windows\system32\, no prilikom boot-a s instalacijskog medija moramo obratiti pažnju na ime uređaja, konkretno u našem primjeru je to bio disk D:\

```
move D:\windows\system32\utilman.exe D:\windows\system32\utilman.exe.rezerva
```

Nakon što smo preimenovali utilman.exe, na mjesto te aplikacije kopirat ćemo cmd.exe:

```
copy D:\windows\system32\cmd.exe D:\windows\system32\utilman.exe
```



Ukratko, **wpeutil** je Windows Preinstallation Environment, alat koji omogućava pokretanje određenih naredbi kao što su naredbe za ponovno pokretanje računala, shutdown, stopiranje windows vatrozida, podešavanje jezika i inicijalizaciju mreže.

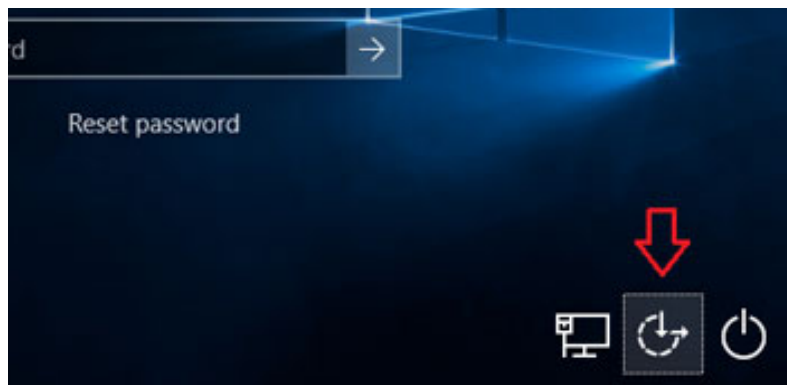
```
Administrator: C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

F:\Sources> move D:\windows\system32\utilman.exe D:\windows\system32\utilman.exe.rezerva
1 file(s) moved.

F:\Sources> copy D:\windows\system32\cmd.exe D:\windows\system32\utilman.exe
1 file(s) copied.

F:\Sources> wpeutil reboot
```

Kad se Windows 10 ponovo pokrene, u donjem desnom kutu kliknite na **Ease of Access** koji će sad otvoriti dobri stari cmd.exe:



U naredbenom retku kreirat ćemo novog korisnika s administrativnim ovlastima.

Upišite sljedeće naredbe (za dodavanje korisnika i za dodavanje u grupu administratora):

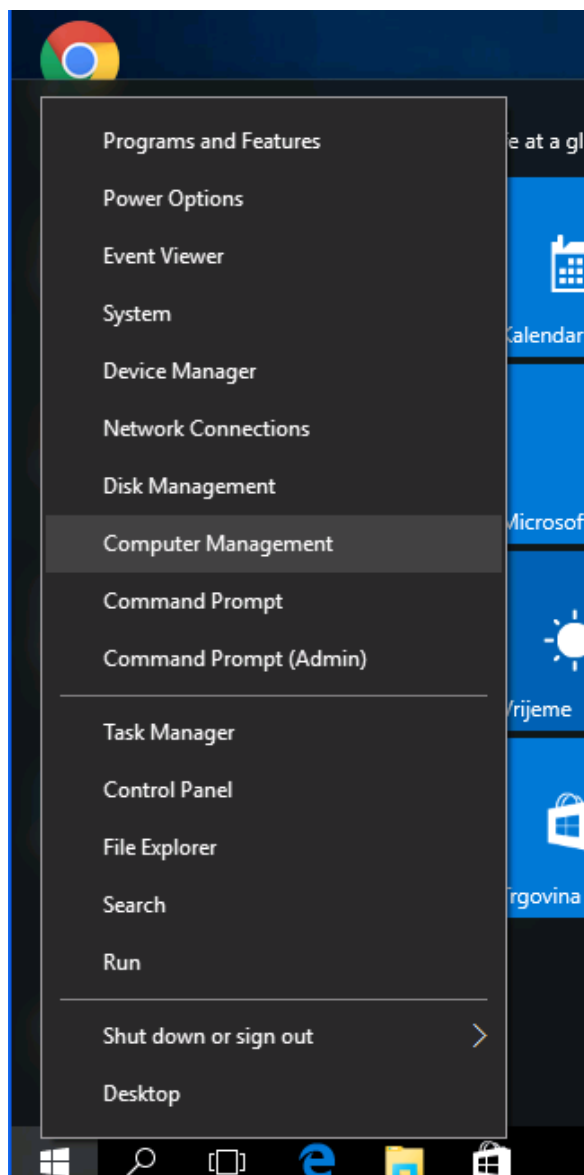
```
net user pero /add
net localgroup administrators pero /add
```

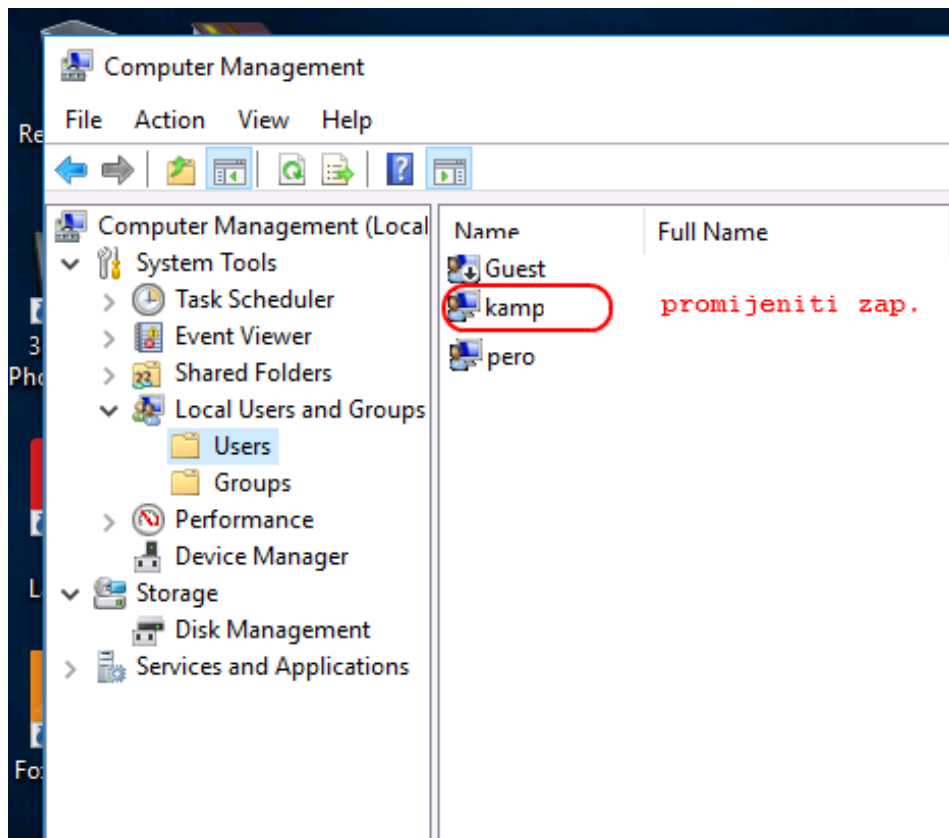
```
Administrator: C:\Windows\system32\utilman.exe
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Windows\system32> net user pero /add
The command completed successfully.

C:\Windows\system32> net localgroup administrators pero /add
The command completed successfully.
```

Nakon što se računalno pokrene, trebali bi vidjeti novog korisnika pero, odaberite ga i prijavite se. Nakon prijave pomoću Computer Management-a dodijelite zaboravnom korisniku novu zaporku.





Kad izmjenite zaporku, ponovo pokrenite računalo s USB ili DVD medija i vratite sve na početno stanje (datoteku utilman.exe.rezerva ponovno preimenujte u utilman.exe):

```
move D:\windows\system32\utilman.exe.rezerva D:\windows\system32\utilman.exe
```

i naravno **wpeutil reboot**

Zaboravni korisnik s novom zaporkom sad može pristupiti svojim podacima i to u neizmjenjenom obliku.

sri, 2016-08-03 09:43 - Zdravko RašićKuharice: [Windows](#) [2]

Kategorije: [Sigurnost](#) [3]

Vote: 5

Vaša ocjena: Nema Average: 5 (2 votes)

Source URL: <https://sysportal.carnet.hr/node/1669>

Links

[1] <https://sysportal.carnet.hr/node/1570>

[2] <https://sysportal.carnet.hr/taxonomy/term/18>

[3] <https://sysportal.carnet.hr/taxonomy/term/30>