

# I want to clear my system of users who are not logged in.

---

## Keywords

openserver enterprise host desktop faststart system release 5.0.0 5.0.2 5.0.4 5.0.5 5.0.6 502 504 505 506 osr5 v5 clearutmp internet ifs 1.1.0.0 tcp/ip client dos win who logged pseudo ttys users utmp wtmp auth tcb ale ptyupd cron clear phantom ghost whodo not cwtmp

## Release

SCO OpenServer Enterprise System Release 5.0.0, 5.0.2, 5.0.4, 5.0.5, 5.0.6  
SCO OpenServer Host System Release 5.0.0, 5.0.2, 5.0.4, 5.0.5, 5.0.6  
SCO OpenServer Desktop System Release 5.0.0, 5.0.2, 5.0.4, 5.0.5, 5.0.6  
SCO Internet FastStart Release 1.0.0, 1.1.0

## Problem

DOS or Windows TCP/IP clients that have logged into an SCO UNIX system through telnet turn off their DOS or WINDOWS system or enter <Ctrl><Alt><Del> after their DOS or Windows session has hung. The UNIX "who" command on the SCO system reports them as still logged in.

- or -

DOS or Windows TCP/IP clients that have logged into an SCO UNIX system through telnet exit the SCO session normally, but the UNIX "who" command on the SCO system reports them as still logged in.

- or -

A system that is licensed for a certain number of users is unable to allow the number of licensed users to log in.

- or -

The "who" command shows users who are not logged in.

- or -

The system is no longer usable as the number of configured pseudo ttys are consumed by users who are no longer logged in.

Rebooting the system does not seem to clear any of the above problems.

## Cause

The `/etc/utmp`, `/etc/wtmp`, `/etc/utmpx` or `/etc/wtmpx` may be corrupt.

The `utmp` file and related files record user and accounting information for commands such as "who", "finger" and "login".

The `utmp` file contains information about the current state of the system, including one record for each logged-in user. The login command writes or removes a record to the `utmp` file each time a user logs in or out.

The `wtmp` file contains historical data; each time a user logs in or out, a record is written to `wtmp`.

The `utmpx` and `wtmpx` files contain additional information such as the name of the remote host for users who log in via the network. This information is not transferred to `utmp` or `wtmp`.

The `utmp` and its related files are open to login and other commands to write information about users' activities and expect that the commands that wrote to those files will clear a user properly after exiting a login session. In some instances this may not occur, especially if the user is using a DOS or Windows TCP/IP stack.

- and/or -

The `/etc/auth/system/ttys` file may be corrupt.

The `ttys` file (`/etc/auth/system/ttys`) contains entries for each terminal that can be used to log in to the system. Authentication programs use this database to determine if logging in is permitted on a particular terminal.

Users and processes related to a user's session may still be consuming ttys even after the user has exited an SCO telnet session. At some point the policy manager may not be able to function.

## Solution

`/utmp`, `wtmp`, `utmpx` and `wtmpx` may have become corrupt.

As the user root, create the following script to clear utmp, wtmp, utmpx and wtmpx prior to shutdown:

```
-----cut here-----
#!/bin/sh
# /bin/clearutmp
#
# clear utmp, wtmp, utmpx and wtmpx on shutdown or bootup
#
> /etc/utmp
> /etc/wtmp
> /etc/utmpx
> /etc/wtmpx
-----cut here-----
```

Save the clearutmp script to /bin and run:

```
# chmod 700 /bin/clearutmp
```

The above script can be run manually prior to shutting the system down, or you can add the following lines at the end of /etc/bcheckrc to clear /etc/utmp, wtmp, utmpx and wtmpx during system start-up.

As an example, add the following to the end of /etc/bcheckrc:

```
#
# Added to clear /etc/utmp, wtmp, utmpx and wtmpx on boot
#
> /etc/utmp
> /etc/wtmp
> /etc/utmpx
> /etc/wtmpx
```

NOTE: It is not recommended that /bin/clearutmp be run unless the system is about to be brought down. The utmp and related files contain valuable information about system state and start-up times; clearing those files during run-time can cause unpredictable results.

The /etc/auth/system/ttys file may be corrupt.

As the user root, create the following shell script to clear the /etc/auth/system/ttys file:

```
-----cut here-----
-----
#!/bin/sh
# /bin/clearttys
RC=0

mv /etc/auth/system/ttys /tmp/ttys.$$
touch /etc/auth/system/ttys
chown auth:auth /etc/auth/system/ttys
```

```

cd /tcb/bin
./ttyupd </dev/null >/dev/null 2>&1
RC=$?

if [ "$RC" -ne 0 ]; then
    echo "*ERROR* Running ./ttyupd (RC=$RC)" > /tmp/clear_ttys.log
else
    /tcb/bin/ale /etc/auth/system/ttys pttypd </dev/null >/dev/null 2>&1
    RC=$?

    # Both 0 and 2 exit codes are success... exit 2 is used when there
    # are no ttys to update

    if [ "$RC" -ne 0 ] && [ "$RC" -ne 2 ]; then
        echo "*ERROR* Running ./pttypd (RC=$RC)" >> /tmp/clear_ttys.log
    fi
fi

exit "$RC"
-----cut here-----
-----

```

Save the clear\_ttys script to /bin and run:

```
# chmod 700 /bin/clear_ttys
```

The script, clear\_ttys, can be run while the system is in multiuser mode when the "who" command displays users who are not logged in or use crontab to set up cron to run clear\_ttys at regular intervals.

## See Also

For information on the ttyupd command, which achieves the same result as the script above, see [Technical Article 104588](#), "Rebuild ttys file from inittab including pseudo ttys after crash."

[Technical Article 105755](#), "How to use the cwtmp utility to clear stale entries from utmp and related files."

[cron\(C\)](#), [crontab\(C\)](#), [ttys\(F\)](#), [rc\(ADM\)](#), [bcheckrc\(ADM\)](#), [who\(C\)](#), [w\(C\)](#), [last\(C\)](#)

---

TA105610 created on 16 June 1997 , last updated on 20 November 2000  
 SSL #: 483357 IT #: os3357

---

[Copyright](#) © 1996-2000 The Santa Cruz Operation, Inc.  
 All Rights Reserved.