

**NAME**

pam\_tty\_audit – Enable or disable TTY auditing for specified users

**SYNOPSIS**

**pam\_tty\_audit.so** [disable=*patterns*] [enable=*patterns*]

**DESCRIPTION**

The pam\_tty\_audit PAM module is used to enable or disable TTY auditing. By default, the kernel does not audit input on any TTY.

**OPTIONS****disable=*patterns***

For each user matching *patterns*, disable TTY auditing. This overrides any previous **enable** option matching the same user name on the command line. See NOTES for further description of *patterns*.

**enable=*patterns***

For each user matching *patterns*, enable TTY auditing. This overrides any previous **disable** option matching the same user name on the command line. See NOTES for further description of *patterns*.

**open\_only**

Set the TTY audit flag when opening the session, but do not restore it when closing the session. Using this option is necessary for some services that don't **fork()** to run the authenticated session, such as **sudo**.

**log\_passwd**

Log keystrokes when ECHO mode is off but ICANON mode is active. This is the mode in which the tty is placed during password entry. By default, passwords are not logged. This option may not be available on older kernels (3.9?).

**MODULE TYPES PROVIDED**

Only the **session** type is supported.

**RETURN VALUES**

PAM\_SESSION\_ERR

Error reading or modifying the TTY audit flag. See the system log for more details.

PAM\_SUCCESS

Success.

**NOTES**

When TTY auditing is enabled, it is inherited by all processes started by that user. In particular, daemons restarted by an user will still have TTY auditing enabled, and audit TTY input even by other users unless auditing for these users is explicitly disabled. Therefore, it is recommended to use **disable=\*** as the first option for most daemons using PAM.

To view the data that was logged by the kernel to audit use the command **aureport --tty**.

The *patterns* are comma separated lists of glob patterns or ranges of uids. A range is specified as *min\_uid:max\_uid* where one of these values can be empty. If *min\_uid* is empty only user with the uid *max\_uid* will be matched. If *max\_uid* is empty users with the uid greater than or equal to *min\_uid* will be matched.

**EXAMPLES**

Audit all administrative actions.

```
session required pam_tty_audit.so disable=* enable=root
```

**SEE ALSO**

**aureport**(8), **pam.conf**(5), **pam.d**(5), **pam**(7)

**AUTHOR**

pam\_tty\_audit was written by Miloslav Trma <mitr@redhat.com>. The log\_passwd option was added by Richard Guy Briggs <rgb@redhat.com>.