

**NAME**

pam\_selinux - PAM module to set the default security context

**SYNOPSIS**

**pam\_selinux.so** [open] [close] [restore] [nottys] [debug] [verbose] [select\_context] [env\_params]  
[use\_current\_range]

**DESCRIPTION**

pam\_selinux is a PAM module that sets up the default SELinux security context for the next executed process.

When a new session is started, the `open_session` part of the module computes and sets up the execution security context used for the next `execve(2)` call, the file security context for the controlling terminal, and the security context used for creating a new kernel keyring.

When the session is ended, the `close_session` part of the module restores old security contexts that were in effect before the change made by the `open_session` part of the module.

Adding pam\_selinux into the PAM stack might disrupt behavior of other PAM modules which execute applications. To avoid that, *pam\_selinux.so open* should be placed after such modules in the PAM stack, and *pam\_selinux.so close* should be placed before them. When such a placement is not feasible, *pam\_selinux.so restore* could be used to temporarily restore original security contexts.

**OPTIONS****open**

Only execute the `open_session` part of the module.

**close**

Only execute the `close_session` part of the module.

**restore**

In `open_session` part of the module, temporarily restore the security contexts as they were before the previous call of the module. Another call of this module without the `restore` option will set up the new security contexts again.

**nottys**

Do not setup security context of the controlling terminal.

**debug**

Turn on debug messages via `syslog(3)`.

**verbose**

Attempt to inform the user when security context is set.

**select\_context**

Attempt to ask the user for a custom security context role. If MLS is on, ask also for sensitivity level.

**env\_params**

Attempt to obtain a custom security context role from PAM environment. If MLS is on, obtain also sensitivity level. This option and the `select_context` option are mutually exclusive. The respective PAM environment variables are `SELINUX_ROLE_REQUESTED`, `SELINUX_LEVEL_REQUESTED`, and `SELINUX_USE_CURRENT_RANGE`. The first two variables are self describing and the last one if set to 1 makes the PAM module behave as if the `use_current_range` was specified on the command line of the module.

**use\_current\_range**

Use the sensitivity level of the current process for the user context instead of the default level. Also suppresses asking of the sensitivity level from the user or obtaining it from PAM environment.

**MODULE TYPES PROVIDED**

Only the `session` module type is provided.

**RETURN VALUES****PAM\_SUCCESS**

The security context was set successfully.

**PAM\_SESSION\_ERR**

Unable to get or set a valid context.

**PAM\_USER\_UNKNOWN**

The user is not known to the system.

**PAM\_BUF\_ERR**

Memory allocation error.

**EXAMPLES**

auth required pam\_unix.so

session required pam\_permit.so

session optional pam\_selinux.so

**SEE ALSO**[execve\(2\)](#), [tty\(4\)](#), [pam.d\(5\)](#), [pam\(7\)](#), [selinux\(8\)](#)**AUTHOR**

pam\_selinux was written by Dan Walsh &lt;dwalsh@redhat.com&gt;.