

**NAME**

**capability.conf** – pam\_cap module configuration file

**SYNOPSIS**

**/etc/security/capability.conf**

**DESCRIPTION**

The syntax for lines in this configuration file is:

**#** <-- **'#'** precedes a comment

**<IAB><SPACE><WHO>**

Where **<IAB>** refers to the text format for an inheritable IAB capability tuple, see **cap\_text\_formats(7)** , or the words **all** or **none**.

The reserved word **all** does *not* grant *all the inheritable capabilities*, but acts as a simple *pass-through* for any prevailing IAB tuple capabilities. The reserved word **none** refers to an empty *Inheritable* capability set (and by extension an empty *Ambient* vector).

Here **<WHO>** refers to the space separated PAM username values that will be granted the specified *IAB* tuple. A name prefixed with the character **@** refers to the locally defined **/etc/group** etc users listed under that group name. An asterisk **"\*"** can be used to denote all users.

The parsing of the file chooses the first line that applies to the authenticating user, and attempts to apply that and only that.

Examples of valid syntax are:

```
# only root gets to keep what it had
all                root

# this should fire for user beta only, who will have
# cap_chown dropped from their bounding set.
!cap_chown        beta

# the next one should snag the members of the 'three' group
# granting them cap_setuid and cap_chown
cap_setuid,cap_chown    @three

# this would apply to beta and gamma, but beta is already
# granted a lack of cap_chown above. Further, if gamma is
# in the 'three' group, it would not reach this line.
cap_chown        beta gamma

# members of the 'one' group are granted the cap_setuid Inheritable
# capability, but cap_chown is dropped from their bounding set.
!cap_chown,cap_setuid    @one

# user alpha gets an ambient capability (unless it is also
# a member of the groups 'one' or 'three').
^cap_setuid        alpha

# user delta (if not a member of groups 'one' and 'three') will get
# cap_chown and cap_setgid Ambient capabilities, but have cap_setuid
# dropped from its bounding set.
^cap_chown,^cap_setgid,!cap_setuid delta

# any remaining members of group 'four' will get the cap_setuid
```

```
# Inheritable capability.  
cap_setuid          @four
```

**SEE ALSO**

**pam\_cap(8), cap\_iab(3), cap\_text\_formats(7).**