## NAME

**au_get_state**, **au_notify_initialize**, **au_notify_terminate** - audit event notification

## LIBRARY

Basic Security Module Library (libbsm, -lbsm)

## SYNOPSIS

**#include <bsm/libbsm.h>**

*int*
**au_get_state**(*void*);

*uint32_t*
**au_notify_initialize**(*void*);

*int*
**au_notify_terminate**(*void*);

## DESCRIPTION

The **au_notify** audit notification API tracks audit state in a form permitting efficient update, avoiding frequent system calls to check the kernel audit state. It is implemented only for Darwin/Mac OS X.

The **au_get_state**() function provides a lightweight way to check whether or not auditing is enabled. If a client wants to use this function to determine whether an entire series of audit calls should be made -- as in the common case of a caller building a set of tokens, then writing them -- it should cache the audit status in a local variable. This function always returns the current state of auditing. If audit notification has not already been initialized by calling **au_notify_initialize**() it will be automatically initialized on the first call of this function.

The **au_notify_initialize**() function initializes audit notification.

The **au_notify_terminate**() function cancels audit notification and frees the resources associated with it. Responsible code that no longer needs to use **au_get_state**() should call this function.

## RETURN VALUES

If no error occurred the **au_get_state**() function returns AUC_NOAUDIT if auditing is disabled or suspended, and AUC_AUDITING if auditing is enabled and active. Otherwise, the function can return any of the errno values defined for setaudit(2), or AU_UNIMPL if audit does not appear to be supported by the system.

The **au_notify_initialize**() function returns 0 on success, AU_UNIMPL if audit does not appear to be supported by the system, or one of the status codes defined in <*notify.h*> on Mac OS X to indicate the error.

The **au_notify_terminate**() function returns 0 on success, or -1 on failure.

## SEE ALSO

libbsm(3), notify(3) (Mac OS X)

## HISTORY

The OpenBSM implementation was created by McAfee Research, the security division of McAfee Inc., under contract to Apple Computer, Inc., in 2004. It was subsequently adopted by the TrustedBSD Project as the foundation for the OpenBSM distribution.

## AUTHORS

This software was created by Apple Computer, Inc.

The Basic Security Module (BSM) interface to audit records and audit event stream format were defined by Sun Microsystems.