

# **Secure4Audit** (auditGUARD)

*A Technical White Paper*



## **NOTICE**

As auditGUARD is a software product which is subject to change, S4Software, Inc. reserves the right to make changes in the specifications and other information contained in this document, without prior notice. While S4Software, Inc. has made every effort to ensure the accuracy and completeness of this document, S4Software, Inc. cannot be held liable for any errors or omissions. No information contained in this document shall be deemed to be a warranty for any purpose whatsoever.

Copyright (c) S4Software, Inc. 2004

auditGUARD is a trademark of S4Software, Inc.

Unix is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company Ltd.

The X Window System is a trademark of Massachusetts Institute of Technology. All other trademarks are acknowledged.

## **RESTRICTED RIGHTS LEGEND**

Use, duplication or disclosure by the Government is subject to restrictions as set forth in subprogram (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at subparagraph DFARS 252.227-7013.

S4Software, Inc.  
6633 Convoy Ct.  
San Diego, CA 92111

Phone: 858-560-8112  
Fax: 858-560-8114

E-mail: [sales@s4software.com](mailto:sales@s4software.com)

# TABLE OF CONTENTS

- The Issue ..... 1
- The Solution - Introduction to auditGUARD ..... 1
- Features ..... 2
- auditGUARD Events Configuration ..... 3
- auditGUARD Event Types ..... 6
- Report Options ..... 10
- Other Options ..... 12
- Frequently Asked Questions ..... 15
- Availability ..... 16





## The Issue

Built-in kernel auditing is a reliable way to audit system activity, but auditing methods vary considerably between Unix systems and many lack tools for configuration. Some have command line programs, with complicated switches, while others may require manual editing for various files. There are few programs for generating readable reports and even fewer tools for multi-system audit configuration. Therefore, it is cumbersome and time consuming, at best, for the system administrator to fully utilize what is available.

## The Solution - Introduction to auditGUARD

auditGUARD solves the auditing administration problem by providing a simple, easy-to-use interface from which all system auditing can be controlled.

auditGUARD provides a simple view of system auditing which hides the differences between the Unix variants. Therefore auditGUARD looks and acts the same way on different Unix platforms. A rich set of configuration options is provided so that the system administrator can easily tailor the system auditing to their specific requirements and easily modify them as requirements change.

auditGUARD also integrates easily with other account and access control products, making the system administrator's job that much easier.

---

## Summary

**auditGUARD** supplies a consistent, uniform process for tracking all system activity, including intrusion detection and all exceptional events.

**auditGUARD** provides a rich set of configuration options that allow the system administrator to tailor auditGUARD to specific requirements.

**auditGUARD** consolidates multiple files into a single standard format file and provides the ability to generate reports by selected criteria.

**auditGUARD** is developed, supported and maintained by a company dedicated to software excellence!

## Features

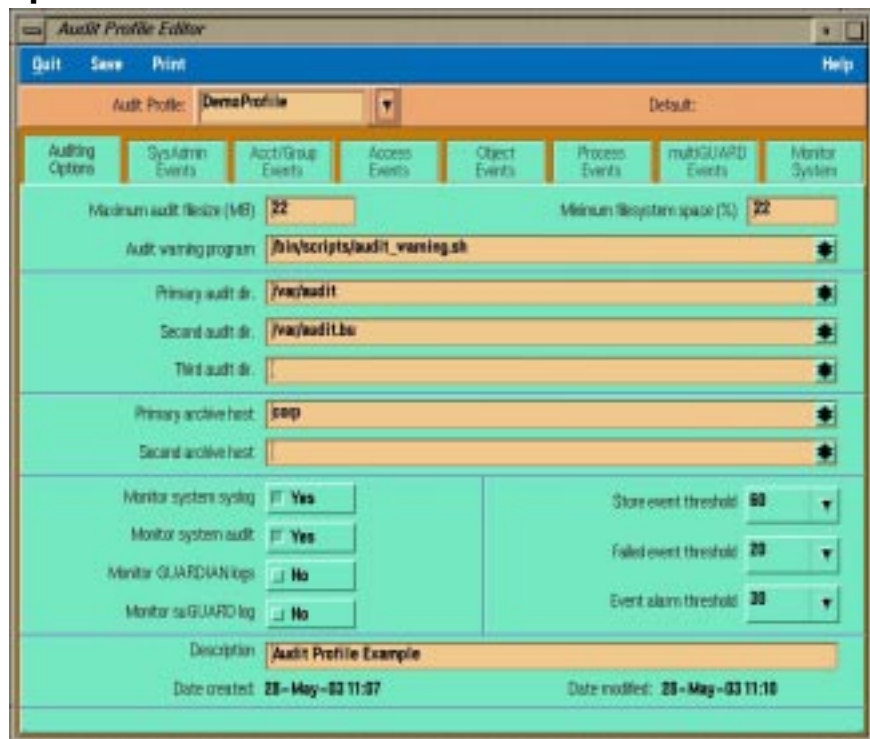
- Provides for the definition of multiple audit configuration files.
  - Provides easy-to-use menu and Motif-based GUI programs with on-line, context sensitive help messages for system auditing and reporting.
  - Hides the differences between Unix auditing variants.
  - Looks and acts the same way on all Unix platforms.
  - Enables the specific selection of audit events.
  - Allows a level to be established for each audit event.
  - Allows a script to be specified for each audit event that will be run according to user specified criteria.
  - Allows item lists for audit events to restrict auditing to items of interest.
  - Can easily be tailored to meet specific audit requirements.
  - Consolidates audit information into standard reports.
  - Reports all logins and super user access, failed login events, disk access, dataset and application access, tape drive access, terminal access and batch access.
  - Establishes pre-defined reports.
  - Supports archiving audit files to remote systems.
-

- Centralizes audit data management.
- Consolidates audit data from multiple sources.

## The auditGUARD Events Configuration

The auditGUARD menu program includes an easy-to-use interface for configuring auditing and for selecting and configuring the various system events to monitor, log and report.

### Auditing Options Screen



The screenshot displays the 'Audit Profile Editor' window. The title bar shows 'Audit Profile Editor' and standard window controls. The menu bar includes 'Quit', 'Save', 'Print', and 'Help'. Below the menu bar, there is a dropdown menu for 'Audit Profile' set to 'Demo Profile' and a 'Default:' label. A tabbed interface is visible with tabs for 'Auditing Options', 'SysAdmin Events', 'Acct/Group Events', 'Access Events', 'Object Events', 'Process Events', 'multiGUARD Events', and 'Monitor System'. The 'Auditing Options' tab is active, showing various configuration fields:

- Minimum audit file size (MB): 22
- Minimum filesystem space (%): 22
- Audit warning program: /bin/scripts/audit\_warning.sh
- Primary audit dir: /var/audit
- Second audit dir: /var/audit/bs
- Third audit dir: (empty)
- Primary archive host: ssp
- Second archive host: (empty)
- Monitor system syslog:  Yes
- Monitor system audit:  Yes
- Monitor GUARDIAN logs:  No
- Monitor multiGUARD log:  No
- Store event threshold: 60
- Failed event threshold: 20
- Event alarm threshold: 30
- Description: Audit Profile Example
- Date created: 28-May-03 11:37
- Date modified: 28-May-03 11:10

## Specifics

### Maximum audit file size

The maximum log size allowed for an audit or log file. Once a log file reaches the specified size, it is closed and a new file is started.

### Minimum filesystem space

This field contains the minimum available file system space (percentage) at which point audit files will be closed and new ones created in one of the alternative audit directories.

### Audit warning program

This field has the full pathname for a program which will be run in the event that a significant error occurs such that normal auditing cannot continue. Examples include system space, and auditing hosts not responding.

### Primary, secondary and third audit directory

The primary audit directory contains the full pathname for the primary directory in which the system audit files will be stored. Depending on the operating system being used, the filenames in this directory will be either the standard system names, or `audit1.<hostname>` (may also have a date/time suffix).

If the available space for the file system in which this directory is located drops below the *Minimum filesystem space*, the audit files will be closed, and new ones created in the *Secondary audit directory* etc.

### Primary audit archive host, second archive host

This field contains the host name (or IP address in dot notation) for a host to which the monitor will direct audit records for storage. The remote host must be running the audit archive daemon (`audarcd`). Should this host become unavailable, or the archive daemon terminates, the audit monitor will redirect records to the secondary host (if defined and available).

### Monitor system syslog, system audit, GUARDIAN logs, suGUARD log

Setting these options to yes instructs `audmond` (the auditGUARD monitoring process) to monitor the various data sources for relevant events. Not all events found in this file will be used, only those which relate directly to audit items.

---

### **Store event threshold**

Each audit event is assigned a level. Whether or not the event information is stored in the suditGUARD combined log depends on the *Store event threshold*.

### **Failed event threshold**

When a failure occurs, the event level is compared to the *Failed event threshold* set here to determine whether or not the script for the event should be run.

### **Event alarm threshold**

When a successful event occurs, the event level is compared to the *Event alarm threshold* to determine whether the script for the event should be run.

### **Description**

This field is used to describe the configuration.

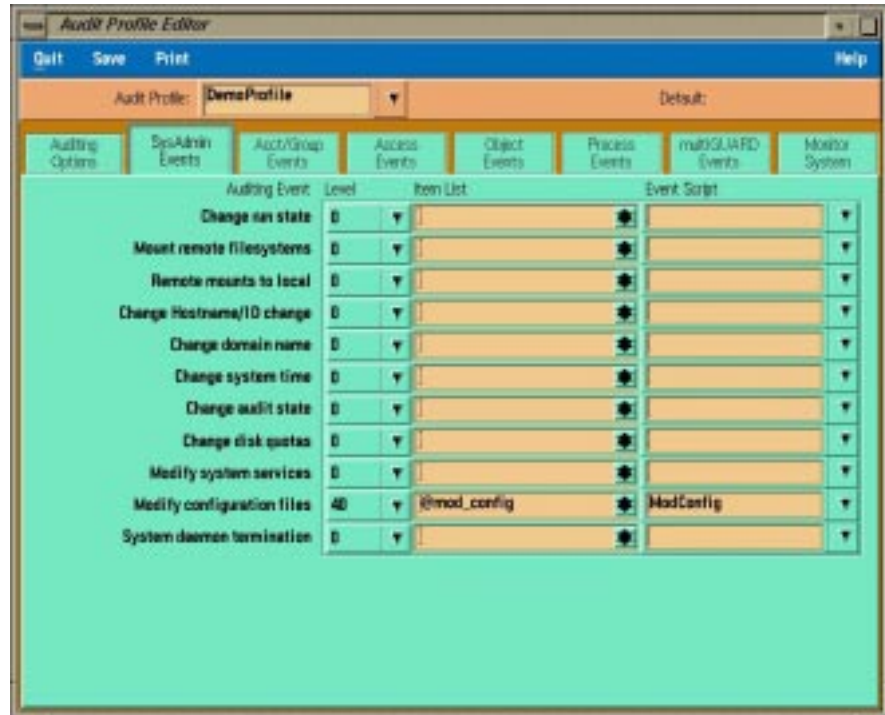
## **Event Types**

The events are grouped by type and include *SysAdmin Events*, *Acct/Group Events*, *Access Events*, *Object Events*, *Process Events*, *multiGUARD Events*. A *Monitor System* option is also included. Shown below is an example of the *SysAdmin Events* screen and a list of options available. The other event screens are similar and a list of options is provided below. Note that a level can be assigned to each event, a list of relevant items (e.g. usernames) can be supplied, and a script name can be given.

---

## SysAdmin Events

### SysAdmin Events Screen



Following is a list of auditing events which can be defined on the *SysAdmin Events* menu. Some of the options below allow the system administrator to define specific actions, or groups to be logged.

- Change run state
- Mount remote filesystems
- Remote mounts to local
- Change Hostname/ID change
- Change NIS domain
- Change system time
- Change audit state
- Change disk quotas
- Modify system services
- Modify configuration files
- System daemon termination

## Acct/Group Events

Following is a list of auditing events which can be defined on the *Acct/Group Events* menu. Some of the options below allow the system administrator to define specific users, or groups to be logged.

- Create new account
- Modify account
- Delete account
- Account inactivation
- Change shell (*chsh*)
- Change system time
- Create new group
- Modify group
- Delete group

## Access Events

Following is a list of auditing events which can be defined on the *Access Events* menu. Some of the options below allow the system administrator to define specific users to be logged.

- Local login
  - Remote login
  - Modem login
  - ftp login
  - Change UID (*su*)
  - Invalid login mode
  - Invalid login location
  - Login outside window
  - Excessive login tries
-

## Object Events

Following is a list of auditing events which can be defined on the *Object Events* menu. The options below allow the system administrator to define specific files to be logged.

- File creation
- File deletion
- File open
- File read
- File write
- Change file attributes
- Create directory
- Delete directory
- Modify directory
- Remote connections
- Modify system devices
- Other objects

## Process Events

Following is a list of auditing events which can be defined on the *Process Events* menu. The options below allow the system administrator to define specific executable program pathnames to be logged.

- Execute process
  - Run remote process
  - Kill process
  - Change attributes
  - Change working directory
-

## multiGUARD Events

Following is a list of auditing events which can be defined on the *multiGUARD Events* menu. The options below allow the system administrator to define specific commands or files to be logged.

- Server/daemon termination
- Create audit profile
- Modify audit profile
- Delete audit profile
- Create command profile
- Modify command profile
- Delete command profile
- Inactivate command profile

## Monitor System

Following is a list of monitoring options which can be defined on the *Monitor system* menu. Some of the options below allow the system administrator to define specific filenames.

- Monitor swap space
  - Monitor root filesystems
  - Monitor other filesystems
-

## Report Options

The reports can be used to generate information based on specific criteria. Shown below is a copy of the Audit items report.

The screenshot shows a window titled "Default" with a menu bar containing "Exit". The main content area displays the following text:

```
(c) S4Software, Inc. 2003      auditGUARD - Selected Audit Item Report.      Host: sun
28-May-03 13:10                Page: 1
```

Time (PDT)	Host Name	Account Name	PID	System Event Code	Event Value	Rtn. Stat	auditGUARD Itm.Flg	Item
28-May-03 12:50	sun	aguser	2759	ACS/login-rig			32/34+	aguser
28-May-03 12:52	sun	aguser	2776	ACS/login-rig			32/34+	aguser
28-May-03 12:53	sun	testuser	2786	ACS/login-rig			32/34+	testuser
28-May-03 12:55	sun	root	2752	ABM/sys-mod			1a/40+	/etc/inittab
28-May-03 12:55	sun	testuser	2809	OBJ/fin-opn	0x000		43/40+	///etc/rc2.d/S99test
28-May-03 12:58	sun	aguser	2822	ACS/login-rig		299	32/34+	aguser
28-May-03 12:59	sun	aguser	2830	ACS/login-rig			32/34+	aguser
28-May-03 13:00	sun	aguser	2840	OBJ/fin-opn	0x000		43/40+	/etc/rc2.d/S99audit
28-May-03 13:01	sun	aguser	2849	OBJ/fin-opn	0x000		43/40+	/etc/rc2.d/S99audit
28-May-03 13:01	sun	aguser	2857	OBJ/fin-opn	0x000		43/40+	/etc/rc2.d/S99audit
28-May-03 13:05	sun	root	2752	ABM/sys-mod			1a/40+	/etc/dfs/dftab
28-May-03 13:07	sun	root	2752	ABM/sys-attr			1a/40+	/etc/dfs/dftab
28-May-03 13:07	sun	root	2752	ABM/sys-mod			1a/40+	/etc/dfs/dftab
28-May-03 13:08	sun	root	2752	ABM/sys-attr			1a/40+	/etc/dfs/dftab
28-May-03 13:09	sun	testuser	2939	OBJ/fin-opn	0x000		43/40+	///etc/inittab

Number of events found 15  
Number of events selected 15

### Account events report

This option is used to generate a report of all events relating to one or more accounts as selected from the pop-up account list. Events for this report are anything which modifies the selected account(s).

### Activity by level report

This option generates a report of all events where the associated audit item level was equal to or greater than a given value at the time the event occurred.

### auditGUARD activity report

This option is used to generate a report showing all auditGUARD activity. Unlike other report options, the input for this file does not come from the composite log files (auditguard.clg), but from the local auditGUARD log file /usr/datalynx/auditguard.clg/auditguard.log.

**Audit items report**

This option will generate a report of all events which are associated with one or more audit items.

**Events by host report**

This option is used to generate a report of all events which occurred on a given hostname or IP address.

**Object events report**

This option is used to generate a report of all events associated with a given object name or pathname. Objects can be files, directories, devices or other system objects. The pathname may include wild-cards which will be interpreted according to standard Unix template rules.

**PID tracing report**

This report tracks a given PID through all its child processes. Therefore, given a login PID it is possible to track a user's movements.

**User activity report**

This option is used to generate a report of all events which were caused by one or more users.

**Warning/alarm events report**

This option is used to generate a report of all events which triggered an event script. These occur when the audit item level for the event is equal to or greater than the current processing level, the event object is in the list (if there is one), and a script is defined.

---

## System Auditing

auditGUARD controls the system auditing through the System Auditing Menu. The following options are provided.

- Enable system auditing
- Disable system auditing
- Modify auditing profile
- Switch system audit files
- Print current audit profile

## Audit Monitor

The Audit Monitor is the auditGUARD daemon which controls the collection of audit data from the various sources. This menu contains the following options.

- Audit monitor status
  - Start audit monitor
  - Stop audit monitor
  - Set threshold levels
  - Start new log file
  - Change log directories
  - Switch current log directory
  - Switch current archiving host
-

## Archive Daemon

The Archive Daemon is the auditGUARD daemon which controls the archiving of audit data. This menu contains the following options.

- Archive daemon status
- Start audit archive daemon
- Stop audit archive daemon
- Change archive directories
- Switch current archive directory

## Profiles

Following is a list of options provided under the Profiles menu.

- Create audit profile
- Edit an audit profile
- Delete an audit profile
- Print an audit profile
- Load a default audit profile

## Accounts

Following is a list of options provided under the Account Profile menu.

- List all accounts
  - Create an account profile
  - Edit an account profile
  - Delete an account profile
  - Activate an account profile
  - Inactivate an account profile
  - Print account information
-

## Frequently Asked Questions

### **Do I have to be an audit expert to use auditGUARD?**

No! auditGUARD simplifies the selection of auditing events by organizing them into intelligible classes which remain the same across multiple version of Unix.

### **I've heard auditing generates so much data that there are constant storage problems. Is this true?**

First of all, with auditGUARD it is easy to be selective about what audit data you want to collect. Secondly, auditGUARD can be configured to automatically rename and start new log files when they grow too large. So you control what data you want, which reduces the amount of data you're dealing with, and you tell auditGUARD how large to allow a file to get before starting a new one.

### **What am I supposed to do with all of this information?**

Let auditGUARD worry about it! You can specify scripts to be run when successful or failed events are detected if the event has a level greater than a threshold value. You define what events warrant immediate attention, then let auditGUARD watch for them. In addition, auditGUARD offers a number of useful reports which can be generated at any time.

### **How can I protect my audit data against hackers who know how to change the log information?**

auditGUARD can be configured to store audit records on a remote host to which login access is strictly limited. It can also audit log file changes so that tampering can be detected.

---

# Availability

auditGUARD is currently available for most popular versions of Unix including the following:

Hewlett-Packard	HP/UX 10.x +
IBM	AIX 4.x +
Sun	Solaris 2.x +

To obtain a copy of auditGUARD to evaluate on your system visit us on our web page:

**<http://www.s4software.com>**

Or send email to our sales department:

**[sales@s4software.com](mailto:sales@s4software.com)**

Or call us:

**(858) 560-8112**

Be sure to include your operating system type and full name and address for delivery.

---

