



Router Security Audit Logs

The Router Security Audit Logs feature allows users to configure audit trails, which track changes that have been made to a router that is running Cisco IOS software.

History for Router Security Audit Logs Feature

Release	Modification
12.2(18)S	This feature was introduced.
12.0(27)S	This feature was integrated into Cisco IOS Release 12.0(27)S.
12.2(25)S	The show audit command was extended to support the filestat keyword, which displays the statistics of the audit logs and helps customers choose the filesize appropriate for their network.
12.2(27)SBC	This feature was integrated into Cisco IOS Release 12.2(27)SBC.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Restrictions for Router Security Audit Logs, page 2](#)
- [Information About Router Security Audit Logs, page 2](#)
- [How to Use Router Security Audit Logs, page 3](#)
- [Configuration Examples for Using Router Security Audit Logs, page 6](#)
- [Additional References, page 7](#)
- [Command Reference, page 8](#)



Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2003–2005 Cisco Systems, Inc. All rights reserved.

Restrictions for Router Security Audit Logs

Default Functionality

The Router Security Audit Logs feature is enabled by default and cannot be disabled. (This restriction will be lifted in a future release.)

Disk File System Requirement

The disk file system is supported only on high-end routers; audit files are created only for platforms that support the disk file system. For platforms that do not support the disk file system, audit files are not generated and persistent-data files are lost.

Cisco IOS Release 12.0(27)S Platform Restriction

Software images for Cisco 12000 series Internet routers have been deferred to Cisco IOS Release 12.0(27)S1.

Information About Router Security Audit Logs

To use router security audit logs, you should understand the following concept:

- [How Router Security Audit Logs Work, page 2](#)

How Router Security Audit Logs Work

Audit logs (also known as audit files) allow you to track changes that have been made to your router. Each change is logged as a syslog message, and all syslog messages are kept in the audit file, which is kept in the audit subsystem. Hashes are used to monitor changes in your router. A separate hash is maintained for each of the following areas:

- Running version—A hash of the information that is provided in the output of the **show version** command—running version, ROM information, BOOTLDR information, system image file, system and processor information, and configuration register contents.
- Hardware configuration—A hash of platform-specific information that is generally provided in the output of the **show diag** command.
- File system—A hash of the dir information on all of the flash file systems, which includes bootflash and any other flash file systems on the router.
- Running configuration—A hash of the running configuration.
- Startup configuration—A hash of the contents of the files on NVRAM, which includes the startup-config, private-config, underlying-config, and persistent-data files.

By default, the hashes are calculated every 5 minutes to see if any changes (events) have been made to the router. The time interval prevents a large number of hashes from being generated.

Because the audit file that is stored on the disk is circular, the number of messages that can be stored is dependent on the size of the selected file.

How to Use Router Security Audit Logs

This section contains the following procedures:

- [Specifying and Viewing Audit File Parameters, page 3](#)
- [Monitoring the Audit Subsystem, page 5](#)

Specifying and Viewing Audit File Parameters

Use this task to change the default parameters of the audit file.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **audit filesize** *size*
4. **audit interval** *seconds*
5. **exit**
6. **show audit** [*filestat*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	audit filesize <i>size</i> Example: Router(config)# audit filesize 128	(Optional) Changes the size of the audit file. • <i>size</i> —Size of the audit file in KB. Valid values range from 32 KB to 128 KB. 32 KB is the default size. Note Because the audit file is circular, this command determines the number of messages that can be stored on the disk before a wrap around occurs.
Step 4	audit interval <i>seconds</i> Example: Router(config)# audit interval 120	(Optional) Changes the time interval that is used for calculating hashes. • <i>seconds</i> —Time interval, in seconds, between hash calculations. Valid values range from 120 seconds to 3600 seconds. The default value is 300 seconds (5 minutes).

	Command or Action	Purpose
Step 5	exit Example: Router(config)# exit	(Optional) Exits global configuration mode.
Step 6	show audit [filestat] Example: Router# show audit	(Optional) Displays the contents of an audit file. <ul style="list-style-type: none"> filestat—Displays the rollover counter for the circular buffer and the number of messages that are received. The rollover counter, which indicates the number of times circular buffer has been overwritten, is reset when the audit filesize is changed (via the audit filesize command).

Example

The following example is sample output from the **show audit** command:

```
Router# show audit

*Sep 14 18:37:31.535:%AUDIT-1-RUN_VERSION:Hash:
24D98B13B87D106E7E6A7E5D1B3CE0AD User:

*Sep 14 18:37:31.583:%AUDIT-1-RUN_CONFIG:Hash:
4AC2D776AA6FCA8FD7653CEB8969B695 User:

*Sep 14 18:37:31.595:%AUDIT-1-STARTUP_CONFIG:Hash:
95DD497B1BB61AB33A629124CBFEC0FC User:

*Sep 14 18:37:32.107:%AUDIT-1-FILESYSTEM:Hash:
330E7111F2B526F0B850C24ED5774EDE User:

*Sep 14 18:37:32.107:%AUDIT-1-HARDWARE_CONFIG:Hash:
32F66463DDA802CC9171AF6386663D20 User:
```

[Table 1](#) describes the significant fields shown in the display.

Table 1 *show audit Field Descriptions*

Field	Description
AUDIT-1-RUN_VERSION:Hash: 24D98B13B87D106E7E6A7E5D1B3CE0AD User:	Running version, which is a hash of the information that is provided in the output of the show version command: running version, ROM information, BOOTLDR information, system image file, system and processor information, and configuration register contents.
AUDIT-1-RUN_CONFIG:Hash: 4AC2D776AA6FCA8FD7653CEB8969B695 User:	Running configuration, which is a hash of the running configuration.
AUDIT-1-STARTUP_CONFIG:Hash: 95DD497B1BB61AB33A629124CBFEC0FC User:	Startup configuration, which is a hash of the contents of the files on NVRAM, which includes the startup-config, private-config, underlying-config, and persistent-data.

Table 1 *show audit Field Descriptions (continued)*

Field	Description
AUDIT-1-FILESYSTEM:Hash: 330E7111F2B526F0B850C24ED5774EDE User:	File system, which is a hash of the dir information on all of the flash file systems, which includes bootflash and any other flash file systems on the router.
AUDIT-1-HARDWARE_CONFIG:Hash:32F6646 3DDA802CC9171AF6386663D20 User:	Hardware configuration, which is a hash of platform-specific information that is generally provided in the output of the show diag command.

Troubleshooting Tips

Although the **show audit** command displays audit file information such as the timestamp and what area is being hashed (such as the file system or hardware configuration), a description of what changes were attempted is not available. To view more detailed information regarding the hashes, use the **debug audit** command.

Monitoring the Audit Subsystem

The audit subsystem contains the audit file, which contains syslog messages that monitor changes that have been made to your system. Use this optional task to monitor audit file updates.

SUMMARY STEPS

1. **enable**
2. **debug audit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	debug audit Example: Router# debug audit	Displays debug messages for the audit subsystem.

Examples

The following example is sample output from the **debug audit** command:

```
Router# debug audit

*Sep 14 18:37:31.535:disk0:/forensics.log -> File not found

*Sep 14 18:37:31.535:%AUDIT-1-RUN_VERSION:Hash:
```

```

24D98B13B87D106E7E6A7E5D1B3CE0AD User:
*Sep 14 18:37:31.583:%AUDIT-1-RUN_CONFIG:Hash:
4AC2D776AA6FCA8FD7653CEB8969B695 User:
*Sep 14 18:37:31.587:Audit:Trying to hash nvram:startup-config
*Sep 14 18:37:31.587:Audit:nvram:startup-config Done.
*Sep 14 18:37:31.587:Audit:Trying to hash nvram:private-config
*Sep 14 18:37:31.591:Audit:nvram:private-config Done.
*Sep 14 18:37:31.591:Audit:Trying to hash nvram:underlying-config
*Sep 14 18:37:31.591:Audit:nvram:underlying-config Done.
*Sep 14 18:37:31.591:Audit:Trying to hash nvram:persistent-data
*Sep 14 18:37:31.591:Audit:nvram:persistent-data Done.
*Sep 14 18:37:31.595:Audit:Trying to hash nvram:ifIndex-table
*Sep 14 18:37:31.595:Audit:Skipping nvram:ifIndex-table
*Sep 14 18:37:31.595:%AUDIT-1-STARTUP_CONFIG:Hash:
95DD497B1BB61AB33A629124CBFEC0FC User:
*Sep 14 18:37:31.595:Audit:Trying to hash filesystem disk0:
*Sep 14 18:37:31.775:Audit:Trying to hash attributes of
disk0:c7200-p-mz.120-23.S
*Sep 14 18:37:32.103:Audit:disk0:c7200-p-mz.120-23.S DONE
*Sep 14 18:37:32.103:Audit:disk0:DONE
*Sep 14 18:37:32.103:Audit:Trying to hash filesystem bootflash:
*Sep 14 18:37:32.103:Audit:Trying to hash attributes of
bootflash:c7200-kboot-mz.121-8a.E
*Sep 14 18:37:32.107:Audit:bootflash:c7200-kboot-mz.121-8a.E DONE
*Sep 14 18:37:32.107:Audit:Trying to hash attributes of
bootflash:crashinfo_20030115-182547
*Sep 14 18:37:32.107:Audit:bootflash:crashinfo_20030115-182547 DONE
*Sep 14 18:37:32.107:Audit:Trying to hash attributes of
bootflash:crashinfo_20030115-212157
*Sep 14 18:37:32.107:Audit:bootflash:crashinfo_20030115-212157 DONE
*Sep 14 18:37:32.107:Audit:Trying to hash attributes of
bootflash:crashinfo_20030603-155534
*Sep 14 18:37:32.107:Audit:bootflash:crashinfo_20030603-155534 DONE
*Sep 14 18:37:32.107:Audit:bootflash:DONE
*Sep 14 18:37:32.107:%AUDIT-1-FILESYSTEM:Hash:
330E7111F2B526F0B850C24ED5774EDE User:
*Sep 14 18:37:32.107:Audit:Hashing entitymib entry for 7206VXR chassis,
Hw Serial#:28710795, Hw Revision:A
*Sep 14 18:37:32.107:Audit:Hashing entitymib entry for NPE 400 Card, Hw
Serial#:28710795, Hw Revision:A
*Sep 14 18:37:32.107:Audit:Hashing entitymib entry for Chassis Slot
*Sep 14 18:37:32.107:Audit:Hashing entitymib entry for I/O Dual
FastEthernet Controller
*Sep 14 18:37:32.107:Audit:Hashing entitymib entry for i82543
(Livengood)
*Sep 14 18:37:32.107:Audit:Hashing entitymib entry for i82543
(Livengood)
*Sep 14 18:37:32.107:Audit:Hashing entitymib entry for Chassis Slot
*Sep 14 18:37:32.107:Audit:Hashing entitymib entry for Chassis Slot
*Sep 14 18:37:32.107:Audit:Hashing entitymib entry for Chassis Slot
*Sep 14 18:37:32.107:Audit:Hashing entitymib entry for Chassis Slot
*Sep 14 18:37:32.107:Audit:Hashing entitymib entry for Chassis Slot
*Sep 14 18:37:32.107:Audit:Hashing entitymib entry for Chassis Slot
*Sep 14 18:37:32.107:%AUDIT-1-HARDWARE_CONFIG:Hash:
32F66463DDA802CC9171AF6386663D20 User:

```

Configuration Examples for Using Router Security Audit Logs

This section contains the following configuration example:

- [Specifying Audit Log Parameters: Example, page 7](#)

Specifying Audit Log Parameters: Example

The following example shows how to specify an audit file size of 128kb and that hashes should be calculated every 2 minutes:

```
Router(config)# audit filesize 128
Router(config) audit interval 120
```

Additional References

The following sections provide references related to Router Security Audit Logs.

Related Documents

Related Topic	Document Title
System startup and file maintenance	The section “File Management” in the <i>Cisco IOS Configuration Fundamentals Configuration Guide</i>
File maintenance commands	<i>Cisco IOS Configuration Fundamentals Command Reference</i> , Release 12.2

Standards

Standards	Title
None	—

MIBs

MIBs	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
None	—

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Command Reference

This section documents modified commands only.

- [audit filesize](#)
- [audit interval](#)
- [debug audit](#)
- [show audit](#)

audit filesize

To change the size of the audit file, use the **audit filesize** command in global configuration mode. To return the audit file to its default size, use the **no** form of this command.

audit filesize *size*

no audit filesize *size*

Syntax Description

<i>size</i>	Size of the audit file in KB. Valid values range from 32 KB to 128 KB. 32 KB is the default size.
-------------	---

Defaults

The audit file is 32 KB.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)S	This command was introduced.
12.0(27)S	This feature was integrated into Cisco IOS Release 12.0(27)S.
12.2(27)SBC	This commnad was integrated into Cisco IOS Release 12.2(27)SBC.

Usage Guidelines

The audit file is a fixed file size in the disk file system. The audit file contains syslog messages (also referred to as hashes), which monitor changes that have been made to your router. Because the audit file that is stored on the disk is circular, the number of messages that can be stored is dependent on the size of the selected file. Also, the size determines the number of messages that can be stored on the disk before a wrap around occurs.

You should always ensure that the audit file is secure. The audit file should be access protected so that only the audit subsystem can access it.



Note

Audit logs are enabled by default and cannot be disabled.

Examples

The following example shows how to change the audit file size to 128 KB:

```
Router(config)# audit filesize 128
```

Related Commands

Command	Description
audit interval	Changes the time interval that is used for calculating hashes.
show audit	Displays contents of the audit file.

audit interval

To change the time interval that is used for calculating hashes, use the **audit interval** command in global configuration mode. To return to the default value, which is 5 minutes, use the **no** form of this command.

audit interval *seconds*

no audit interval *seconds*

Syntax Description

<i>seconds</i>	Time interval, in seconds, between hash calculations. Valid values range from 120 seconds to 3600 seconds. The default value is 300 seconds (5 minutes).
----------------	--

Defaults

300 seconds (5 minutes)

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)S	This command was introduced.
12.0(27)S	This feature was integrated into Cisco IOS Release 12.0(27)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27) SBC.

Usage Guidelines

Hashes are used to monitor changes in your router. A separate hash is maintained for each of the following areas:

- Running version—A hash of the information that is provided in the output of the **show version** command—running version, ROM information, BOOTLDR information, system image file, system and processor information, and configuration register contents.
- Hardware configuration—A hash of platform-specific information that is generally provided in the output of the **show diag** command.
- File system—A hash of the dir information on all of the flash file systems, which includes bootflash and any other flash file systems on the router.
- Running configuration—A hash of the running configuration.
- Startup configuration—A hash of the contents of the files on NVRAM, which includes the startup-config, private-config, underlying-config, and persistent-data files.

By default, the hashes are calculated every 5 minutes to see if any changes (events) have been made to the network. The time interval prevents a large number of hashes from being generated.



Note

Audit logs are enabled by default and cannot be disabled.

Examples

The following example shows how to specify hashes to be calculated every 120 seconds (2 minutes):

```
Router(config)# audit interval 120
```

Related Commands

Command	Description
audit filesize	Changes the size of the audit file.
show audit	Displays contents of the audit file.

debug audit

To display debug messages for the audit subsystem, use the **debug audit** command in privileged EXEC mode. To disable debugging for the audit subsystem, use the **no** form of this command.

debug audit

no debug audit

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(18)S	This command was introduced.
	12.0(27)S	This feature was integrated into Cisco IOS Release 12.0(27)S.
	12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.

Usage Guidelines Audit files allow you to track changes that have been made to your router. Each change is logged as a syslog message, and all syslog messages are kept in the audit file, which is kept in the audit subsystem.

Examples The following example is sample output from the **debug audit** command:

```
Router# debug audit

*Sep 14 18:37:31.535:disk0:/forensics.log -> File not found

*Sep 14 18:37:31.535:%AUDIT-1-RUN_VERSION:Hash:
24D98B13B87D106E7E6A7E5D1B3CE0AD User:
*Sep 14 18:37:31.583:%AUDIT-1-RUN_CONFIG:Hash:
4AC2D776AA6FCA8FD7653CEB8969B695 User:
*Sep 14 18:37:31.587:Audit:Trying to hash nvram:startup-config
*Sep 14 18:37:31.587:Audit:nvram:startup-config Done.
*Sep 14 18:37:31.587:Audit:Trying to hash nvram:private-config
*Sep 14 18:37:31.591:Audit:nvram:private-config Done.
*Sep 14 18:37:31.591:Audit:Trying to hash nvram:underlying-config
*Sep 14 18:37:31.591:Audit:nvram:underlying-config Done.
*Sep 14 18:37:31.591:Audit:Trying to hash nvram:persistent-data
*Sep 14 18:37:31.591:Audit:nvram:persistent-data Done.
*Sep 14 18:37:31.595:Audit:Trying to hash nvram:ifIndex-table
*Sep 14 18:37:31.595:Audit:Skipping nvram:ifIndex-table
*Sep 14 18:37:31.595:%AUDIT-1-STARTUP_CONFIG:Hash:
95DD497B1BB61AB33A629124CBFEC0FC User:
*Sep 14 18:37:31.595:Audit:Trying to hash filesystem disk0:
*Sep 14 18:37:31.775:Audit:Trying to hash attributes of
disk0:c7200-p-mz.120-23.S
*Sep 14 18:37:32.103:Audit:disk0:c7200-p-mz.120-23.S DONE
*Sep 14 18:37:32.103:Audit:disk0:DONE
*Sep 14 18:37:32.103:Audit:Trying to hash filesystem bootflash:
```

```

*Sep 14 18:37:32.103:Audit:Trying to hash attributes of
bootflash:c7200-kboot-mz.121-8a.E
*Sep 14 18:37:32.107:Audit:bootflash:c7200-kboot-mz.121-8a.E DONE
*Sep 14 18:37:32.107:Audit:Trying to hash attributes of
bootflash:crashinfo_20030115-182547
*Sep 14 18:37:32.107:Audit:bootflash:crashinfo_20030115-182547 DONE
*Sep 14 18:37:32.107:Audit:Trying to hash attributes of
bootflash:crashinfo_20030115-212157
*Sep 14 18:37:32.107:Audit:bootflash:crashinfo_20030115-212157 DONE
*Sep 14 18:37:32.107:Audit:Trying to hash attributes of
bootflash:crashinfo_20030603-155534
*Sep 14 18:37:32.107:Audit:bootflash:crashinfo_20030603-155534 DONE
*Sep 14 18:37:32.107:Audit:bootflash:DONE
*Sep 14 18:37:32.107:%AUDIT-1-FILESYSTEM:Hash:
330E7111F2B526F0B850C24ED5774EDE User:
*Sep 14 18:37:32.107:Audit:Hashing entitymib entry for 7206VXR chassis,
Hw Serial#:28710795, Hw Revision:A
*Sep 14 18:37:32.107:Audit:Hashing entitymib entry for NPE 400 Card, Hw
Serial#:28710795, Hw Revision:A
*Sep 14 18:37:32.107:Audit:Hashing entitymib entry for Chassis Slot
*Sep 14 18:37:32.107:Audit:Hashing entitymib entry for I/O Dual
FastEthernet Controller
*Sep 14 18:37:32.107:Audit:Hashing entitymib entry for i82543
(Livengood)
*Sep 14 18:37:32.107:Audit:Hashing entitymib entry for i82543
(Livengood)
*Sep 14 18:37:32.107:Audit:Hashing entitymib entry for Chassis Slot
*Sep 14 18:37:32.107:Audit:Hashing entitymib entry for Chassis Slot
*Sep 14 18:37:32.107:Audit:Hashing entitymib entry for Chassis Slot
*Sep 14 18:37:32.107:Audit:Hashing entitymib entry for Chassis Slot
*Sep 14 18:37:32.107:Audit:Hashing entitymib entry for Chassis Slot
*Sep 14 18:37:32.107:Audit:Hashing entitymib entry for Chassis Slot
*Sep 14 18:37:32.107:%AUDIT-1-HARDWARE_CONFIG:Hash:
32F66463DDA802CC9171AF6386663D20 User:

```

Related Commands

Command	Description
audit filesize	Changes the size of the audit file.
audit interval	Changes the time interval that is used for calculating hashes.

show audit

To display the contents of an audit file, use the **show audit** command in privileged EXEC mode.

show audit [filestat]

Syntax Description	filestat	(Optional) Displays the rollover counter for the circular buffer and the number of messages that are received.
		The rollover counter, which indicates the number of times circular buffer has been overwritten, is reset when the audit filesize is changed (via the audit filesize command).

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(18)S	This command was introduced.
	12.0(27)S	This feature was integrated into Cisco IOS Release 12.0(27)S.
	12.2(25)S	The filestat keyword was added.
	12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.

Usage Guidelines

The audit file is a fixed file size in the disk file system. The audit file contains syslog messages (also known as hashes), which monitor changes that are made to your router. A separate hash is maintained for each of the following areas: running version, running configuration, startup configuration, file system, and hardware configuration. The **show audit** command will display any changes that are made to any of these areas.



Note

Audit logs are enabled by default and cannot be disabled.

Examples

The following example is sample output from the **show audit** command:

```
Router# show audit

*Sep 14 18:37:31.535:%AUDIT-1-RUN_VERSION:Hash:
24D98B13B87D106E7E6A7E5D1B3CE0AD User:

*Sep 14 18:37:31.583:%AUDIT-1-RUN_CONFIG:Hash:
4AC2D776AA6FCA8FD7653CEB8969B695 User:

*Sep 14 18:37:31.595:%AUDIT-1-STARTUP_CONFIG:Hash:
95DD497B1BB61AB33A629124CBFEC0FC User:

*Sep 14 18:37:32.107:%AUDIT-1-FILESYSTEM:Hash:
330E7111F2B526F0B850C24ED5774EDE User:

*Sep 14 18:37:32.107:%AUDIT-1-HARDWARE_CONFIG:Hash:
```

```
32F66463DDA802CC9171AF6386663D20 User:
```

Table 2 describes the significant fields shown in the display.

Table 2 *show audit Field Descriptions*

Field	Description
AUDIT-1-RUN_VERSION:Hash: 24D98B13B87D106E7E6A7E5D1B3CE0AD User:	Running version, which is a hash of the information that is provided in the output of the show version command: running version, ROM information, BOOTLDR information, system image file, system and processor information, and configuration register contents.
AUDIT-1-RUN_CONFIG:Hash: 4AC2D776AA6FCA8FD7653CEB8969B695 User:	Running configuration, which is a hash of the running configuration.
AUDIT-1-STARTUP_CONFIG:Hash: 95DD497B1BB61AB33A629124CBFEC0FC User:	Startup configuration, which is a hash of the contents of the files on NVRAM, which includes the startup-config, private-config, underlying-config, and persistent-data.
AUDIT-1-FILESYSTEM:Hash: 330E7111F2B526F0B850C24ED5774EDE User:	File system, which is a hash of the dir information on all of the flash file systems, which includes bootflash and any other flash file systems on the router.
AUDIT-1-HARDWARE_CONFIG:Hash:32F6646 3DDA802CC9171AF6386663D20 User:	Hardware configuration, which is a hash of platform-specific information that is generally provided in the output of the show diag command.

Related Commands

Command	Description
audit filesize	Changes the size of the audit file.
audit interval	Changes the time interval that is used for calculating hashes.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

© 2003–2005 Cisco Systems, Inc. All rights reserved.

■ show audit