Configuration Change Notification and Logging

Last Updated: November 29, 2011

Prior to the introduction of this feature, the only way to determine if the Cisco IOS software configuration had changed was to save a copy of the running and startup configurations to a local computer and do a line-by-line comparison. This comparison method can identify changes that occurred, but does not specify the sequence in which the changes occurred, or the person responsible for the changes.

The Configuration Change Notification and Logging (Config Log Archive) feature allows the tracking of configuration changes entered on a per-session and per-user basis by implementing an archive function. This archive saves 'configuration logs' that track each configuration command that is applied, who applied the command, the parser return code (PRC) for the command, and the time the command was applied. This feature also adds a notification mechanism that sends asynchronous notifications to registered applications whenever the configuration log changes.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

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

Restrictions for Configuration Change Notification and Logging

- Only complete commands input in a configuration mode are logged.
- Commands that are part of a configuration file applied with the **copy** command are not logged.

Information About Configuration Change Notification and Logging

Configuration Log

The Configuration Change Notification and Logging feature tracks changes made to the Cisco IOS software running configuration by maintaining a configuration log. This configuration log tracks changes initiated only through the command-line interface (CLI) or HTTP. Only complete commands that result in the invocation of action routines are logged. The following types of entries are not logged:

- Commands that result in a syntax error message
- Partial commands that invoke the router help system

For each configuration command that is executed, the following information is logged:

- The command that was executed
- The name of the user that executed the command
- A configuration change sequence number
- Parser return codes for the command

Note In some environments the configuration mode and the time of the executed command may also be logged.

You can display information from the configuration log through the use of the **showarchivelogconfig** command, with the exception of the parser return codes, which are for use by internal Cisco IOS applications only.

Configuration Change Notifications and Config Change Logging

You can configure the Configuration Change and Notification Logging feature to send notification of configuration changes to the Cisco IOS software system logging (syslog) process. Syslog notifications allow monitoring of the configuration log information without performing polling and information gathering tasks.

The Configuration Change Notification and Logging feature allows the tracking of configuration changes entered by users on a per-session and per-user basis. This tool allows administrators to track any

configuration change made to the Cisco IOS software running configuration, and identify the user that made that change.

- Config Logger Enhancements for EAL4+ Certification, page 3

Config Logger Enhancements for EAL4+ Certification

Further enhancements to the Configuration Change Logging process were implemented in Cisco IOS Release 12.3(14)T. These enhancements support an effort to ensure the logging process meets the requirements set forth in the Conformance to Common Criteria, Evaluation Assurance Level 4+ (EAL4+) Firewall Protection Profiles. These enhancements include changes to meet the following requirements:

- If you change any logging parameters, those changes are logged. This is effected by the sending of a syslog message for each change to the running-config from a copy operation (for example, on **copy***source***running-config**).
- Modifications to the Group of Administrative Users are logged; failure attempts for access to privileged EXEC mode (“enable” mode) are logged.

Note EAL Certification is not claimed by Cisco for Cisco IOS Release 12.3(14)T. These enhancements provide the groundwork for future Certification.

The above logging actions are disabled by default. To enable these logging characteristics, perform the task described in the “Configuring the Configuration Change Notification and Logging Feature” section.

How to Configure the Configuration Change Notification and Logging Feature

- Configuring the Configuration Change Notification and Logging Feature, page 3
- Displaying Configuration Log Entries and Statistics, page 5
- Clearing Configuration Log Entries, page 7

Configuring the Configuration Change Notification and Logging Feature

Perform this task to enable the Configuration Change Notification and Logging feature.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **archive**
4. **log config**
5. **logging enable**
6. **logging size** *entries*
7. **hidekeys**
8. **notify syslog**
9. **end**

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	**archive** **Example:** `Router(config)# archive`	Enters archive configuration mode.
Step 4	**log config** **Example:** `Router(config-archive)# log config`	Enters configuration change logger configuration mode.
Step 5	**logging enable** **Example:** `Router(config-archive-log-config)# logging enable`	Enables the logging of configuration changes. • Logging of configuration changes is disabled by default.

	Command or Action	Purpose
Step 6	**logging size** *entries* **Example:** `Router(config-archive-log-config)# logging size 200`	(Optional) Specifies the maximum number of entries retained in the configuration log. • Valid values for the *entries* argument range from 1 to 1000. The default value is 100 entries. • When the configuration log is full, the oldest entry is deleted every time a new entry is added. **Note** If a new log size is specified that is smaller than the current log size, the oldest log entries is immediately purged until the new log size is satisfied, regardless of the age of the log entries.
Step 7	**hidekeys** **Example:** `Router(config-archive-log-config)# hidekeys`	(Optional) Suppresses the display of password information in configuration log files. **Note** Enabling the **hidekeys** command increases security by preventing password information from being displayed in configuration log files.
Step 8	**notify syslog** **Example:** `Router(config-archive-log-config)# notify syslog`	(Optional) Enables the sending of notifications of configuration changes to a remote syslog.
Step 9	**end** **Example:** `Router(config-archive-log-config)# end`	Exits to privileged EXEC mode.

Displaying Configuration Log Entries and Statistics

Perform this task to display entries from the configuration log or statistics about the memory usage of the configuration log.

To display configuration log entries and to monitor the memory usage of the configuration log, the Configuration Change Notification and Logging feature provides the **showarchivelogconfig** command.

SUMMARY STEPS

1. **enable**
2. **show archive log config** *number* [*end-number*]
3. **show archive log config provisioning**
4. **show archive log config statistics**
5. **exit**

DETAILED STEPS

Step 1 **enable**

Use this command to enable privileged EXEC mode. Enter your password if prompted. For example”

Example:

```
Router> enable
```

Step 2 **show archive log config** *number* [*end-number*]

Use this command to display configuration log entries by record numbers. If you specify a record number for the optional *end-number* argument, all log entries with record numbers between the values entered for the *number* and *end-number* arguments are displayed. For example:

```
Router# show archive log config 1 2
```

Example:

```
idx   sess   user@line        Logged command
 1     1     user1@console    logging enable
 2     1     user1@console    logging size 200
```

This example displays configuration log entry numbers 1 and 2. Valid values for the *number* and *end-number* argument range from 1 to 2147483647.

Step 3 **show archive log config provisioning**

Use this command to display all configuration log files as they would appear in a configuration file rather than in tabular format. For example:

Example:

```
Router# show archive log config all provisioning
archive
 log config
  logging enable
  logging size 200
```

This display also shows the commands used to change configuration modes, which are required to correctly apply the logged commands.

Step 4 **show archive log config statistics**

Use this command to display memory usage information for the configuration. For example:

Example:

```
Router# show archive log config statistics
Config Log Session Info:
   Number of sessions being tracked: 1
   Memory being held: 3910 bytes
   Total memory allocated for session tracking: 3910 bytes
   Total memory freed from session tracking: 0 bytes
Config Log log-queue Info:
   Number of entries in the log-queue: 3
   Memory being held in the log-queue: 671 bytes
```

```
   Total memory allocated for log entries: 671 bytes
   Total memory freed from log entries:: 0 bytes
```

Step 5 **exit**

Use this command to exit to user EXEC mode. For example:

Example:

```
Router# exit
Router>
```

Clearing Configuration Log Entries

Entries from the configuration log can be cleared in one of two ways. The size of the configuration log can be reduced using the **loggingsize** command, or the configuration log can be disabled and then re-enabled with the **loggingenable**command.

- Clearing the Configuration Log by Reducing the Log Size, page 7
- Clearing the Configuration Log by Disabling the Configuration Log, page 9

Clearing the Configuration Log by Reducing the Log Size

Perform this task to clear entries from the configuration log using the **loggingsize**command.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **archive**
4. **log config**
5. **logging size** *entries*
6. **logging size** *entries*
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**archive** **Example:** `Router(config)# archive`	Enters archive configuration mode.
Step 4	**log config** **Example:** `Router(config-archive)# log config`	Enters configuration change logger configuration mode.
Step 5	**logging size** *entries* **Example:** `Router(config-archive-log-config)# logging size 1`	Specifies the maximum number of entries retained in the configuration log. **Note** Setting the size of the configuration log to 1 results in all but the most recent entry being purged.
Step 6	**logging size** *entries* **Example:** `Router(config-archive-log-config)# logging size 200`	Specifies the maximum number of entries retained in the configuration log. **Note** The size of the configuration log should be reset to the desired value after clearing the configuration log.
Step 7	**end** **Example:** `Router(config-archive-log-config)# end`	Exits to privileged EXEC mode.

Examples

The following example shows how to clear the configuration log by reducing the log size to 1, then resetting the log size to the desired value:

```
Router# configure terminal
Router(config)# archive
Router(config-archive)# log config
Router(config-archive-log-config)# logging size 1
Router(config-archive-log-config)# logging size 200
Router(config-archive-log-config)# end
```

Clearing the Configuration Log by Disabling the Configuration Log

Perform this task to clear entries from the configuration log using the **loggingenable**command.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **archive**
4. **log config**
5. **no logging enable**
6. **logging enable**
7. **end**

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	**archive** **Example:** `Router(config)# archive`	Enters archive configuration mode.
Step 4	**log config** **Example:** `Router(config-archive)# log config`	Enters configuration change logger configuration mode.
Step 5	**no logging enable** **Example:** `Router(config-archive-log-config)# no logging enable`	Disables the logging of configuration changes. **Note** Disabling the configuration log results in all records being purged.

	Command or Action	Purpose
Step 6	**logging enable** **Example:** `Router(config-archive-log-config)# logging enable`	Enables the logging of configuration changes.
Step 7	**end** **Example:** `Router(config-archive-log-config)# end`	Exits to privileged EXEC mode.

Examples

The following example clears the configuration log by disabling and then re-enabling the configuration log:

```
Router(config)# archive
Router(config-archive)# log config
Router(config-archive-log-config)# no logging enable
Router(config-archive-log-config)# logging enable
Router(config-archive-log-config)# end
```

Configuration Examples for the Configuration Change Notification and Logging Feature

Configuring the Configuration Change Notification and Logging Feature Example

The following example shows how to enable configuration logging with a maximum of 200 entries in the configuration log. In the example, security is increased by suppressing the display of password information in configuration log records, and syslog notifications are turned on.

```
configure terminal
archive
 log config
 logging enable
 logging size 200
 hidekeys
 notify syslog
```

Additional References

The following sections provide references related to the Configuration Change Notification and Logging. feature:

Related Documents

Related Topic	Document Title
Information about managing configuration files	Managing Configuration Files
Commands for managing configuration files	*Cisco IOS Configuration Fundamentals Command Reference*

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	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
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	--

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for Configuration Change Notification and Logging

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1 Feature Information for Configuration Change Notification and Logging

Feature Name	Releases	Feature Information
Configuration Change Notification and Logging	12.3(4)T 12.2(25)S 12.2(27)SBC 12.2(33)SRA 12.2(33)SXH 12.2(33)SB	The Configuration Change Notification and Logging (Configuration Logging) feature allows the tracking of configuration changes entered on a per-session and per-user basis by implementing a configuration log. The configuration log tracks each configuration command that is applied, who applied the command, the parser return code for the command, and the time the command was applied. This feature also adds a notification mechanism that sends asynchronous notifications to registered applications whenever the configuration log changes. In 12.2(33)SB, this feature was implemented on the Cisco 10000 series. The following sections provide information about this feature: The following commands were modified by this feature: **archive**, **hidekeys**, **log config**, **logging enable**, **logging size**, **notify syslog**, **show archive log config**.
Config Logger Enhancements for EAL4+ Certification	12.3(14)T 12.2(27)SBC	Further enhancements to the Configuration Change Logging process were implemented in Cisco IOS Release 12.3(14)T and 12.2(27)SBC. These enhancements support an effort to ensure the logging process meets the requirements set forth in the Conformance to Common Criteria, Evaluation Assurance Level 4+ (EAL4+) Firewall Protection Profiles. The following section provides information about this feature: