



Configuration Change Notification and Logging

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.

Before the introduction of the Configuration Change Notification and Logging feature, the only way to determine if the Cisco 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.

- [Finding Feature Information, on page 1](#)
- [Restrictions for Configuration Change Notification and Logging, on page 1](#)
- [Information About Configuration Change Notification and Logging, on page 2](#)
- [How to Configure Configuration Change Notification and Logging, on page 3](#)
- [Configuration Examples for Configuration Change Notification and Logging, on page 9](#)
- [Additional References, on page 9](#)
- [Feature Information for Configuration Change Notification and Logging, on page 10](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and 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.

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.

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 software running configuration by maintaining a configuration log. This configuration log tracks changes initiated only through the 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 device help system

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

- The command that was executed
- The configuration mode in which the command was executed
- The name of the user that executed the command
- The time at which the command was executed
- A configuration change sequence number
- Parser return codes for the command

You can display information from the configuration log by using the **show archive log config** command, with the exception of the parser return codes, which are for use by internal Cisco 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 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 software running configuration, and identify the user that made that change.

Config Logger Enhancements for EAL4+ Certification

The Config Logger Enhancements for EAL4+ Certification feature ensures that 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 configuration from a copy operation (for example, **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. These enhancements provide the groundwork for future certification.

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

How to Configure Configuration Change Notification and Logging

Configuring Configuration Change Notification and Logging

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: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	archive Example:	Enters archive configuration mode.

	Command or Action	Purpose
	Device(config)# archive	
Step 4	log config Example: Device(config-archive)# log config	Enters configuration change logger configuration mode.
Step 5	logging enable Example: Device(config-archive-log-config)# logging enable	Enables the logging of configuration changes. <ul style="list-style-type: none"> Logging of configuration changes is disabled by default.
Step 6	logging size <i>entries</i> Example: Device(config-archive-log-config)# logging size 200	(Optional) Specifies the maximum number of entries retained in the configuration log. <ul style="list-style-type: none"> Valid values for the <i>entries</i> 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. <p>Note If a new log size is specified that is smaller than the current log size, the oldest log entries are immediately purged until the new log size is satisfied, regardless of the age of the log entries.</p>
Step 7	hidekeys Example: Device(config-archive-log-config)# hidekeys	(Optional) Suppresses the display of password information in configuration log files. <p>Note Enabling the hidekeys command increases security by preventing password information from being displayed in configuration log files.</p>
Step 8	notify syslog Example: Device(config-archive-log-config)# notify syslog	(Optional) Enables the sending of notifications of configuration changes to a remote syslog.
Step 9	end Example: Device(config-archive-log-config)# end	Returns 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. You can enter the commands in any order.

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

SUMMARY STEPS

1. **enable**
2. **show archive log config** *number* [*end-number*]
3. **show archive log config all 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:

```
Device> 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 in the range from the value entered for the *number* argument through the *end-number* argument are displayed. For example:

```
Device# show archive log config 1 2

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

Example:

This example displays configuration log entry numbers 1 and 2. The range for the *number* and *end-number* arguments is 1 to 2147483647.

Step 3 **show archive log config all 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:

```
Device# 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:

```
Device# 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:

```
Device# exit
Device>
```

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 by using the **logging size** command, or the configuration log can be disabled and then reenabled with the **logging enable** command.

Clearing the Configuration Log by Resetting the Log Size

This task shows how to clear the configuration log by reducing the log size to 1, then resetting the log size to the desired value, by entering the **logging size** command twice.

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	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: Device> enable	<ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	archive Example: Device(config)# archive	Enters archive configuration mode.
Step 4	log config Example: Device(config-archive)# log config	Enters configuration change logger configuration mode.
Step 5	logging size <i>entries</i> Example: Device(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 <i>entries</i> Example: Device(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: Device(config-archive-log-config)# end	Exits to privileged EXEC mode.

Clearing the Configuration Log by Disabling the Configuration Log

SUMMARY STEPS

- enable
- configure terminal
- archive
- log config
- no logging enable
- logging enable

7. end

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	archive Example: Device(config)# archive	Enters archive configuration mode.
Step 4	log config Example: Device(config-archive)# log config	Enters configuration change logger configuration mode.
Step 5	no logging enable Example: Device(config-archive-log-config)# no logging enable	Disables the logging of configuration changes. Note Disabling the configuration log results in all records being purged.
Step 6	logging enable Example: Device(config-archive-log-config)# logging enable	Enables the logging of configuration changes.
Step 7	end Example: Device(config-archive-log-config)# end	Exits to privileged EXEC mode.

Configuration Examples for Configuration Change Notification and Logging

Example: Configuring Configuration Change Notification and Logging

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 with the **hidekeys** command, and syslog notifications are turned on with the **notify syslog** command.

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

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Information about managing configuration files	“Managing Configuration Files” module in the <i>Managing Configuration Files Configuration Guide</i>
Commands for managing configuration files	Cisco IOS Configuration Fundamentals Command Reference

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

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		<p>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.</p> <p>The following commands were introduced or modified: archive, hidekeys, log config, logging enable, logging size, notify syslog, show archive log config.</p>