Exclusive Configuration Change Access and Access Session Locking

First Published: February 28, 2005
Last Updated: May 4, 2009

Exclusive Configuration Change Access (also called the "Configuration Lock" feature) allows you to have exclusive change access to the Cisco IOS XE running configuration, preventing multiple users from making concurrent configuration changes.

The Access Session Locking addition to this feature extends the Exclusive Configuration Change Access feature such that **show** and **debug** commands entered by the user holding the configuration lock always have execution priority; **show** and **debug** commands entered by other users are only allowed to run after the processes initiated by the configuration lock owner have finished.

The Exclusive Configuration Change Access feature ("exposed lock") is complementary with the locking mechanism in the Configuration Replace and Configuration Rollback feature ("rollback lock").

Finding Feature Information

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 for Exclusive Configuration Change Access and Access Session Locking" section on page 9.

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

Contents

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

Information About Exclusive Configuration Change Access and Access Session Locking

To use the Exclusive Configuration Change Access and Access Session Locking feature, you should understand the following concepts:

Exclusive Configuration Change Access Functionality

Devices running Cisco IOS XE software maintain a running configuration that determines the configuration state of the device. Changes to the running configuration alter the behavior of the device. Because Cisco IOS XE software allows multiple users to change the running configuration via the device CLI (including the device console and telnet SSH), in some operating environments it would be beneficial to prevent multiple users from making concurrent changes to the Cisco IOS XE running configuration. Temporarily limiting access to the Cisco IOS XE running configuration prevents inadvertent conflicts or cases where two users attempt to configure the same portion of the running configuration.

Exclusive configuration change access provides a mechanism to prevent concurrent configuration of Cisco IOS XE software by multiple users.

This feature provides exclusive change access to the Cisco IOS XE running configuration from the time you enter global configuration mode by using the **configure terminal** command. This gives the effect of a “configuration lock,” preventing other users from changing the Cisco IOS XE running configuration. The configuration lock is automatically released when the user exits Cisco IOS XE configuration mode.

The Exclusive Configuration Change Access feature is enabled using the **configuration mode exclusive** command in global configuration mode. Exclusive Configuration Change Access can be set to **auto**, so that the Cisco IOS XE configuration mode is locked whenever anyone uses the **configure terminal** command, or it can be set to **manual**, so that the Cisco IOS XE configuration mode is locked only when the **configure terminal lock** command is issued.

Access Session Locking

Access Session Locking, in addition to preventing concurrent configuration access, provides an option to prevent simultaneous processes, such as a **show** command entered by another user, from executing while other configuration commands are being executed. When this feature is enabled, the commands entered by the user with the configuration lock (such as configuration commands) always have priority over commands entered by other users.

How to Use Exclusive Configuration Change Access and Access Session Locking

This section contains the following procedures:

Enabling Exclusive Configuration Change Access and Access Session Locking

Perform this task to gain exclusive access to the Cisco IOS XE configuration mode.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **configuration mode exclusive** {**auto** | **manual**}
4. **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.

	Command or Action	Purpose
Step 3	**configuration mode exclusive** {**auto** | **manual**} **Example:** `Router(config)# configuration mode exclusive auto`	Enables exclusive configuration change access (configuration lock feature). When enabled, configuration sessions are performed in single-user (exclusive) mode. • The **auto** keyword automatically locks the configuration session whenever the **configure terminal** command is used. This is the default. • The **manual** keyword allows you to choose to lock the configuration session manually or leave it unlocked. **Caution** If you use the **manual** keyword, you must perform the task described in the "Obtaining Exclusive Configuration Change Access" section on page 4.
Step 4	**end** **Example:** `Router(config)# end`	Ends your configuration session and returns the CLI to privileged EXEC mode.

Obtaining Exclusive Configuration Change Access

Perform this task to obtain exclusive configuration change access for the duration of your configuration session.

Note Use of the **lock** keyword with the **configure terminal** command is only necessary if the exclusive configuration mode has been set to **manual** (see the "Enabling Exclusive Configuration Change Access and Access Session Locking" section).

SUMMARY STEPS

1. **enable**
2. **configure terminal lock**
3. Configure the system by entering your changes to the running configuration.
4. **end**
   or
   exit

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 lock** **Example:** `Router# configure terminal lock`	(Optional) Locks the Cisco IOS XE software in exclusive (single-user) mode. **Note** This command can only be used if you have previously enabled configuration locking by using the **configuration mode exclusive** command.
Step 3	Configure the system by entering your changes to the running configuration.	—

Step 4	**end**
	or
	exit
	
	Example:
	`Router(config)# end`
	`Router#`
	or
	
	Example:
	`Router(config)# exit`
	`Router#`
		Ends your configuration session, automatically releases the session lock obtained in Step 1, and exits to privileged EXEC mode.
		Note Either the **end** command, the **exit** command, or the Ctrl-Z key combination releases the configuration lock. Use of the **end** command is recommended.

Monitoring and Troubleshooting the Exclusive Configuration Change Access and Access Session Locking Feature

Perform one or both of the steps in this task to monitor or troubleshoot the Exclusive Configuration Change Access and Access Session Locking feature.

SUMMARY STEPS

1. **show configuration lock**
2. **debug configuration lock**

DETAILED STEPS

Step 1 **show configuration lock**

Use this command to display the status and details of any current configuration locks, including the owner, user, terminal, lock state, and lock class.

If you cannot enter global configuration mode, you can use this command to determine if the configuration session is currently locked by another user, and who that user is.

```
Router# show configuration lock
```

```
Parser Configure Lock
-----------------------------------------------------
Owner PID : -1
User : unknown
TTY : -1
Type : NO LOCK
State : FREE
Class : unknown
Count : 0
Pending Requests : 0

User debug info :
Session idle state : TRUE
No of exec cmds getting executed : 0
No of exec cmds blocked : 0
Config wait for show completion : FALSE
Remote ip address : Unknown
Lock active time (in Sec) : 0
Lock Expiration timer (in Sec) : 0
Router(config)#
```

Step 2 **debug configuration lock**

Use this command to enable debugging of Cisco IOS XE configuration locks (exposed class locks).

```
Router# debug configuration lock

Session1 from console
==========================

Router# configure terminal lock
Configuration mode locked exclusively. The lock will be cleared once you exit out of
configuration mode using end/exit
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
Parser : LOCK REQUEST in EXCLUSIVE mode
Parser: <configure terminal lock> - Config. Lock requested by process <3> client <PARSER
Client>
Parser: <configure terminal lock> - Config. Lock acquired successfully !
Router(config)#
```

Configuration Examples for Exclusive Configuration Change Access and Access Session Locking

This section provides the following configuration examples:

- Configuring an Exclusive Lock in Auto Mode: Example, page 7
- Configuring an Exclusive Lock in Manual Mode: Example, page 7

Configuring an Exclusive Lock in Auto Mode: Example

The following example shows how to enable the exclusive lock in auto mode for single-user auto configuration mode using the **configuration mode exclusive auto** command. Once the Cisco IOS XE configuration file is locked exclusively, you can verify this configuration by using the **show configuration lock** command.

```
Router#
Router# configure terminal
Router(config)# configuration mode exclusive auto
Router(config)# exit

Router#
Router# configure terminal
! Locks configuration mode exclusively.

Router(config)# show configuration lock

Parser Configure Lock

Owner PID        :  10
User             :  User1
TTY              :  3
Type             :  EXCLUSIVE
State            :  LOCKED
Class            :  Exposed
Count            :  0
Pending Requests :  0
User debug info  :  0
```

Configuring an Exclusive Lock in Manual Mode: Example

The following example shows how to enable the exclusive locking feature in manual mode by using the **configuration mode exclusive manual** command. Once you have configured manual exclusive mode, you can lock the configuration mode by using the **configure terminal lock** command. In this mode, the **configure terminal** command will not automatically lock the parser configuration mode.

```
Router#
Router# configure terminal
Router(config)# configuration mode exclusive manual
Router(config)# exit

Router# configure terminal lock
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#

*Mar 25 17:02:45.928:  Configuration mode locked exclusively. The lock will be cleared
once you exit out of configuration mode using end/exit
```

Additional References

The following sections provide references related to the Exclusive Configuration Change Access and Access Session Locking feature.

Related Documents

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

Standards

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

MIBs

MIB	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 XE releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	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 Exclusive Configuration Change Access and Access Session Locking

Table 1 lists the features in this module and provides links to specific configuration information.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS XE software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 1 lists only the Cisco IOS XE software release that introduced support for a given feature in a given Cisco IOS XE software release train. Unless noted otherwise, subsequent releases of that Cisco IOS XE software release train also support that feature.

Table 1 Feature Information for Exclusive Configuration Change Access and Access Session Locking

Feature Name	Releases	Feature Information
Exclusive Configuration Change Access and Access Session Locking	Cisco IOS XE Release 2.1	Exclusive Configuration Change Access (also called the "Configuration Lock" feature) allows you to have exclusive change access to the Cisco IOS running configuration, preventing multiple users from making concurrent configuration changes. The Access Session Locking addition to this feature extends the Exclusive Configuration Change Access feature such that **show** and **debug** commands entered by the user holding the configuration lock always have execution priority; **show** and **debug** commands entered by other users are only allowed to run after the processes initiated by the configuration lock owner have finished. The Exclusive Configuration Change Access feature ("exposed lock") is complementary with the locking mechanism in the Configuration Replace and Configuration Rollback feature ("rollback lock"). The Configuration Lock feature was integrated into Release 12.0S, and the Access Session Locking feature extension was implemented. The **configuration mode exclusive command** was extended to include the following keyword options: **expire**, **lock-show**, **interleave**, **terminate**, **config_wait**, and **retry_wait**. The output of the **show configuration lock** command was improved. In Cisco IOS XE Release 2.1, this feature was introduced on Cisco ASR 1000 Series Routers. The following sections provide information about this feature: • Information About Exclusive Configuration Change Access and Access Session Locking • How to Use Exclusive Configuration Change Access and Access Session Locking