



Exclusive Configuration Change Access and Access Session Locking

First Published: February 28, 2005

Last Updated: May 2, 2008

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”).

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the [“Feature Information for Exclusive Configuration Change Access and Access Session Locking”](#) section on page 10.

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS 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

- [Information About Exclusive Configuration Change Access and Access Session Locking, page 2](#)
- [How to Use Exclusive Configuration Change Access and Access Session Locking, page 3](#)



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

© 2005–2008 Cisco Systems, Inc. All rights reserved.

- [Configuration Examples for Exclusive Configuration Change Access and Access Session Locking, page 6](#)
- [Additional References, page 7](#)
- [Command Reference, page 9](#)
- [Feature Information for Exclusive Configuration Change Access and Access Session Locking, page 10](#)

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, page 2](#)
- [Access Session Locking, page 3](#)

Exclusive Configuration Change Access Functionality

Devices running Cisco IOS 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 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 running configuration. Temporarily limiting access to the Cisco IOS 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 software by multiple users.

This feature provides exclusive change access to the Cisco IOS 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 running configuration. The configuration lock is automatically released when the user exits Cisco IOS 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 configuration mode is locked whenever anyone uses the **configure terminal** command, or it can be set to **manual**, so that the Cisco IOS configuration mode is locked only when the **configure terminal lock** command is issued.

The Exclusive Configuration Change Access feature is complementary with the locking mechanism for the [Configuration Replace and Configuration Rollback](#) feature introduced in Cisco IOS Release 12.2(25)S and 12.3(7)T.

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, page 3](#) (required)
- [Obtaining Exclusive Configuration Change Access, page 4](#) (optional)
- [Monitoring and Troubleshooting the Exclusive Configuration Change Access and Access Session Locking Feature, page 5](#) (optional)

Enabling Exclusive Configuration Change Access and Access Session Locking

Perform this task to gain exclusive access to the Cisco IOS 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. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 3	<pre>configuration mode exclusive {auto manual}</pre> <p>Example: Router(config)# configuration mode exclusive auto</p>	<p>Enables exclusive configuration change access (configuration lock feature). When enabled, configuration sessions are performed in single-user (exclusive) mode.</p> <ul style="list-style-type: none"> 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. 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	<pre>end</pre> <p>Example: Router(config)# end</p>	<p>Ends your configuration session and returns the CLI to privileged EXEC mode.</p>

Obtaining Exclusive Configuration Change Access

Perform this task to obtain exclusive configuration change access for the duration of your configuration session. 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**
3. **configure terminal lock**
4. Configure the system by entering your changes to the running configuration.
5. **end**
or
exit

DETAILED STEPS

	Command or Action	Purpose
Step 1	<pre>enable</pre> <p>Example: Router> enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	<pre>configure terminal</pre> <p>Example: Router# configure terminal</p>	<p>Enters global configuration mode.</p>

	Command or Action	Purpose
Step 3	<p>configure terminal lock</p> <p>Example: Router(config)# configure terminal lock</p>	<p>(Optional) Locks the Cisco IOS software in exclusive (single-user) mode.</p> <ul style="list-style-type: none"> This command can only be used if you have previously enabled configuration locking by using the configuration mode exclusive command. Available only in Cisco IOS Release 12.3(14)T or later.
Step 4	Configure the system by entering your changes to the running configuration.	—
Step 5	<p>end or exit</p> <p>Example: Router(config)# end Router# or</p> <p>Example: Router(config)# exit Router#</p>	<p>Ends your configuration session, automatically releases the session lock obtained in Step 1, and exits to privileged EXEC mode.</p> <p>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.</p>

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                : 3
User                    : unknown
TTY                     : 0
```

```

Type                : EXCLUSIVE
State               : LOCKED
Class               : EXPOSED
Count               : 1
Pending Requests   : 0
User debug info     : configure terminal
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) : 6
Lock Expiration timer (in Sec) : 593
Router(config)#

```

Step 2 debug configuration lock

Use this command to enable debugging of Cisco IOS configuration locks (exposed class locks or rollback 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 6](#)
- [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 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 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
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/techsupport

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Configuration Fundamentals Command Reference* at

http://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf_book.html. For information about all Cisco IOS commands, use the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or a Cisco IOS master commands list.

- **configuration mode exclusive**
- **configure terminal**
- **debug configuration lock**
- **show configuration lock**

Feature Information for Exclusive Configuration Change Access and Access Session Locking

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS 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 software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS 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	12.3(14)T 12.0(31)S 12.2(33)SRA 12.4(11)T 12.2(33)SXH 12.2(33)SB	<p>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.</p> <p>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.</p> <p>The Exclusive Configuration Change Access feature (“exposed lock”) is complementary with the locking mechanism in the Configuration Replace and Configuration Rollback feature (“rollback lock”).</p> <p>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.</p> <p>The extended feature was integrated into Releases 12.2(33)SRA, 12.4(11)T, 12.2(33)SXH, and 12.2(33)SB.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> Information About Exclusive Configuration Change Access and Access Session Locking How to Use Exclusive Configuration Change Access and Access Session Locking

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA,

CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo 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. (0903R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2005-2008 Cisco Systems, Inc. All rights reserved.

