Role-Based CLI Access

First Published: February 24, 2004
Last Updated: March 30, 2011

The Role-Based CLI Access feature allows the network administrator to define "views," which are a set of operational commands and configuration capabilities that provide selective or partial access to Cisco IOS EXEC and configuration (config) mode commands. Views restrict user access to Cisco IOS command-line interface (CLI) and configuration information; that is, a view can define what commands are accepted and what configuration information is visible. Thus, network administrators can exercise better control over access to Cisco networking devices.

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 for Role-Based CLI Access" section on page 13.

Use Cisco Feature Navigator to find information about platform support and Cisco 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

Prerequisites for Role-Based CLI Access

Your image must support CLI views.

Restrictions for Role-Based CLI Access

Lawful Intercept Images Limitation

Because CLI views are a part of the Cisco IOS parser, CLI views are a part of all platforms and Cisco IOS images. However, the lawful intercept view is available only in images that contain the lawful intercept subsystem.

Maximum Number of Allowed Views

The maximum number of CLI views and superviews, including one lawful intercept view, that can be configured is 15. (This does not include the root view.)

Information About Role-Based CLI Access

Benefits of Using CLI Views

Views: Detailed Access Control

Although users can control CLI access via both privilege levels and enable mode passwords, these functions do not provide network administrators with the necessary level of detail needed when working with Cisco IOS routers and switches. CLI views provide a more detailed access control capability for network administrators, thereby, improving the overall security and accountability of Cisco IOS software.

As of Cisco IOS Release 12.3(11)T, network administrators can also specify an interface or a group of interfaces to a view; thereby, allowing access on the basis of specified interfaces.

Root View

When a system is in “root view,” it has all of the access privileges as a user who has level 15 privileges. If the administrator wishes to configure any view to the system (such as a CLI view, a superview, or a lawful intercept view), the system must be in root view.

The difference between a user who has level 15 privileges and a root view user is that a root view user can configure a new view and add or remove commands from the view. Also, when you are in a CLI view, you have access only to the commands that have been added to that view by the root view user.

About Lawful Intercept Views

Like a CLI view, a lawful intercept view restricts access to specified commands and configuration information. Specifically, a lawful intercept view allows a user to secure access to lawful intercept commands that are held within the TAP-MIB, which is a special set of simple network management protocol (SNMP) commands that store information about calls and users.

Commands available in lawful intercept view belong to one of the these categories:

- Lawful intercept commands that should not be made available to any other view or privilege level
- CLI views that are useful for lawful intercept users but do not have to be excluded from other views or privilege levels

About Superviews

A superview consists of one or more CLI views, which allow users to define what commands are accepted and what configuration information is visible. Superviews allow a network administrator to easily assign all users within configured CLI views to a superview instead of having to assign multiple CLI views to a group of users.

Superviews contain these characteristics:

- A CLI view can be shared among multiple superviews.
- Commands cannot be configured for a superview; that is, you must add commands to the CLI view and add that CLI view to the superview.
- Users who are logged into a superview can access all of the commands that are configured for any of the CLI views that are part of the superview.
- Each superview has a password that is used to switch between superviews or from a CLI view to a superview.
- If a superview is deleted, all CLI views associated with that superview will not be deleted too.

View Authentication via a New AAA Attribute

View authentication is performed by an external authentication, authorization, and accounting (AAA) server via the new attribute “cli-view-name.”

AAA authentication associates only one view name to a particular user; that is, only one view name can be configured for a user in an authentication server.

How to Use Role-Based CLI Access

- Configuring a CLI View, page 4 (required)
- Configuring a Lawful Intercept View, page 6 (optional)
- Configuring a Superview, page 7 (optional)
- Monitoring Views and View Users, page 9 (optional)

Configuring a CLI View

Perform this task to create a CLI view and add commands or interfaces to the view, as appropriate.

Prerequisites

Before you create a view, you must perform the following tasks:

- Enable AAA via the **aaa new-model** command.
- Ensure that your system is in root view—not privilege level 15.

SUMMARY STEPS

1. **enable view**
2. **configure terminal**
3. **parser view** *view-name*
4. **secret 5** *encrypted-password*
5. **commands** *parser-mode* {**include** | **include-exclusive** | **exclude**} [**all**] [**interface** *interface-name* | *command*]
6. **exit**
7. **exit**
8. **enable** [*privilege-level*] [**view** *view-name*]
9. **show parser view** [**all**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable view** **Example:** `Router> enable view`	Enables root view. • Enter your privilege level 15 password (for example, root password) if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**parser view** *view-name* **Example:** `Router(config)# parser view first`	Creates a view and enters view configuration mode.
Step 4	**secret 5** *encrypted-password* **Example:** `Router(config-view)# secret 5 secret`	Associates a command-line interface (CLI) view or superview with a password. **Note** You must issue this command before you can configure additional attributes for the view.

	Command or Action	Purpose
Step 5	**commands** *parser-mode* {**include** | **include-exclusive** | **exclude**} [**all**] [**interface** *interface-name* | *command*] **Example:** `Router(config-view)# commands exec include show version`	Adds commands or interfaces to a view. • *parser-mode*—The mode in which the specified command exists. • **include**—Adds a command or an interface to the view and allows the same command or interface to be added to an additional view. • **include-exclusive**—Adds a command or an interface to the view and excludes the same command or interface from being added to all other views. • **exclude**—Excludes a command or an interface from the view; that is, customers cannot access a command or an interface. • **all**—A "wildcard" that allows every command in a specified configuration mode that begins with the same keyword or every subinterface for a specified interface to be part of the view. • **interface** *interface-name*—Interface that is added to the view. • *command*—Command that is added to the view.
Step 6	**exit** **Example:** `Router(config-view)# exit`	Exits view configuration mode.
Step 7	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.
Step 8	**enable** [*privilege-level*] [**view** *view-name*] **Example:** `Router# enable view first`	Prompts the user for a password, which allows the user to access a configured CLI view, and is used to switch from one view to another view. After the correct password is given, the user can access the view.
Step 9	**show parser view** [**all**] **Example:** `Router# show parser view`	(Optional) Displays information about the view that the user is currently in. • **all**—Displays information for all views that are configured on the router. **Note** Although this command is available for both root and lawful intercept users, the **all** keyword is available only to root users. However, the **all** keyword can be configured by a user in root view to be available for users in lawful intercept view and CLI view.

Troubleshooting Tips

After you have successfully created a view, a system message such as the following is displayed:

```
%PARSER-6-VIEW_CREATED: view 'first' successfully created.
```

After you have successfully deleted a view, a system message such as the following is displayed:

%PARSER-6-VIEW_DELETED: view 'first' successfully deleted.

You must associate a password with a view. If you do not associate a password, and you attempt to add commands to the view via the **commands** command, a system message such as the following will be displayed:

```
%Password not set for view <viewname>.
```

Configuring a Lawful Intercept View

Perform this task to initialize and configure a view for lawful-intercept-specific commands and configuration information.

Prerequisites

Before you initialize a lawful intercept view, ensure that the privilege level is set to 15 via the **privilege** command.

Restrictions

Only an administrator or a user who has level 15 privileges can initialize a lawful intercept view.

SUMMARY STEPS

1. **enable view**
2. **configure terminal**
3. **li-view** *li-password* **user** *username* **password** *password*
4. **username** [**lawful-intercept**] *name* [**privilege** *privilege-level* | **view** *view-name*] **password** *password*
5. **parser view** *view-name*
6. **secret 5** *encrypted-password*
7. **name** *new-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable view** **Example:** `Router> enable view`	Enables root view. • Enter your privilege level 15 password (for example, root password) if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**li-view** *li-password* **user** *username* **password** *password* **Example:** `Router(config)# li-view lipass user li_admin password li_adminpass`	Initializes a lawful intercept view. After the li-view is initialized, you must specify at least one user via **user** *username* **password** *password* options.
Step 4	**username** [**lawful-intercept** [*name*] [**privilege** *privilege-level* | **view** *view-name*] **password** *password* **Example:** `Router(config)# username lawful-intercept li-user1 password li-user1pass`	Configures lawful intercept users on a Cisco device.
Step 5	**parser view** *view-name* **Example:** `Router(config)# parser view li view name`	(Optional) Enters view configuration mode, which allows you to change the lawful intercept view password or the lawful intercept view name.
Step 6	**secret 5** *encrypted-password* **Example:** `Router(config-view)# secret 5 secret`	(Optional) Changes an existing password for a lawful intercept view.
Step 7	**name** *new-name* **Example:** `Router(config-view)# name second`	(Optional) Changes the name of a lawful intercept view. If this command is not issued, the default name of the lawful intercept view is "li-view."

Troubleshooting Tips

To display information for all users who have access to a lawful intercept view, issue the **show users lawful-intercept** command. (This command is available only to authorized lawful intercept view users.)

Configuring a Superview

Perform this task to create a superview and add at least one CLI view to the superview.

Prerequisites

Before adding a CLI view to a superview, ensure that the CLI views that are added to the superview are valid views in the system; that is, the views have been successfully created via the **parser view** command.

Restrictions

You can add a view to a superview only after a password has been configured for the superview (via the **secret 5** command). Thereafter, issue the **view** command in view configuration mode to add at least one CLI view to the superview.

SUMMARY STEPS

1. **enable view**
2. **configure terminal**
3. **parser view** *superview-name* **superview**
4. **secret 5** *encrypted-password*
5. **view** *view-name*
6. **exit**
7. **exit**
8. **show parser view** [**all**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable view** **Example:** `Router> enable view`	Enables root view. • Enter your privilege level 15 password (for example, root password) if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**parser view** *superview-name* **superview** **Example:** `Router(config)# parser view su_view1 superview`	Creates a superview and enters view configuration mode.
Step 4	**secret 5** *encrypted-password* **Example:** `Router(config-view)# secret 5 secret`	Associates a CLI view or superview with a password. **Note** You must issue this command before you can configure additional attributes for the view.
Step 5	**view** *view-name* **Example:** `Router(config-view)# view view_three`	Adds a normal CLI view to a superview. Issue this command for each CLI view that is to be added to a given superview.

	Command or Action	Purpose
Step 6	**exit** **Example:** `Router(config-view)# exit`	Exits view configuration mode.
Step 7	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.
Step 8	**show parser view** [**all**] **Example:** `Router# show parser view`	(Optional) Displays information about the view that the user is currently in. • **all**—Displays information for all views that are configured on the router. **Note** Although this command is available for both root and lawful intercept users, the **all** keyword is available only to root users. However, the **all** keyword can be configured by a user in root view to be available for users in lawful intercept view and CLI view.

Monitoring Views and View Users

To display debug messages for all views—root, CLI, lawful intercept, and super—use the **debug parser view** command in privileged EXEC mode.

Configuration Examples for Role-Based CLI Access

Example: Configuring a CLI View

The following example shows how to configure two CLI views, “first” and “second.” Thereafter, you can verify the CLI view in the running configuration.

```
Router(config)# parser view first
00:11:40:%PARSER-6-VIEW_CREATED:view 'first' successfully created.
Router(config-view)# secret 5 firstpass
Router(config-view)# command exec include show version
Router(config-view)# command exec include configure terminal
Router(config-view)# command exec include all show ip
Router(config-view)# exit
Router(config)# parser view second
00:13:42:%PARSER-6-VIEW_CREATED:view 'second' successfully created.
Router(config-view)# secret 5 secondpass
```

```
Router(config-view)# command exec include-exclusive show ip interface
Router(config-view)# command exec include logout
Router(config-view)# exit
!
!
Router(config-view)# do show run | beg view
parser view first
 secret 5 $1$MCmh$QuZaU8PIMPlff9sFCZvgW/
 commands exec include configure terminal
 commands exec include configure
 commands exec include all show ip
 commands exec include show version
 commands exec include show
!
parser view second
 secret 5 $1$iP2M$R16BXKecMEiQesxLyqygW.
 commands exec include-exclusive show ip interface
 commands exec include show ip
 commands exec include show
 commands exec include logout
!
```

Example: Verifying a CLI View

After you have configured the CLI views "first" and "second," you can issue the **enable view** command to verify which commands are available in each view. The following example shows which commands are available inside the CLI view "first" after the user has logged into this view. (Because the **show ip** command is configured with the all option, a complete set of suboptions is shown, except the **show ip interface** command, which is using the include-exclusive keyword in the second view.)

```
Router# enable view first
Password:

00:28:23:%PARSER-6-VIEW_SWITCH:successfully set to view 'first'.
Router# ?
Exec commands:
  configure  Enter configuration mode
  enable     Turn on privileged commands
  exit       Exit from the EXEC
  show       Show running system information

Router# show ?

  ip       IP information
  parser   Display parser information
  version  System hardware and software status

Router# show ip ?

  access-lists            List IP access lists
  accounting              The active IP accounting database
  aliases                 IP alias table
  arp                     IP ARP table
  as-path-access-list     List AS path access lists
  bgp                     BGP information
  cache                   IP fast-switching route cache
  casa                    display casa information
  cef                     Cisco Express Forwarding
  community-list          List community-list
  dfp                     DFP information
  dhcp                    Show items in the DHCP database
```

```
  drp                     Director response protocol
  dvmrp                   DVMRP information
  eigrp                   IP-EIGRP show commands
  extcommunity-list       List extended-community list
  flow                    NetFlow switching
  helper-address          helper-address table
  http                    HTTP information
  igmp                    IGMP information
  irdp                    ICMP Router Discovery Protocol
.
.
.
```

Example: Configuring a Lawful Intercept View

The following example shows how to configure a lawful intercept view, add users to the view, and verify the users that were added:

```
!Initialize the LI-View.
Router(config)# li-view lipass user li_admin password li_adminpass
00:19:25:%PARSER-6-LI_VIEW_INIT:LI-View initialized.
Router(config)# end

! Enter the LI-View; that is, check to see what commands are available within the view.
Router# enable view li-view
Password:

Router#
00:22:57:%PARSER-6-VIEW_SWITCH:successfully set to view 'li-view'.
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# parser view li-view
Router(config-view)# ?
View commands:
  commands  Configure commands for a view
  default   Set a command to its defaults
  exit      Exit from view configuration mode
  name      New LI-View name      ===This option only resides in LI View.
  no        Negate a command or set its defaults
  password  Set a password associated with CLI views

Router(config-view)#

! NOTE:LI View configurations are never shown as part of 'running-configuration'.

! Configure LI Users.
Router(config)# username lawful-intercept li-user1 password li-user1pass
Router(config)# username lawful-intercept li-user2 password li-user2pass

! Displaying LI User information.
Router# show users lawful-intercept

li_admin
li-user1
li-user2
Router#
```

Example: Configuring a Superview

The following sample output from the **show running-config** command shows that "view_one" and "view_two" have been added to superview "su_view1," and "view_three" and "view_four" have been added to superview "su_view2":

```
!
parser view su_view1 superview
 secret 5 <encoded password>
 view view_one
 view view_two
!
parser view su_view2 superview
 secret 5 <encoded password>
 view view_three
 view view_four
!
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	*Cisco IOS Master Commands List, All Releases*
Security commands	*Cisco IOS Security Command Reference*
SNMP, MIBs, CLI configuration	*Cisco IOS Network Management Configuration Guide*, Release 15.0.
Privilege levels	"Configuring Security with Passwords, Privilege Levels and, Login Usernames for CLI Sessions on Networking Devices" module.

MIBs

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

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 Role-Based CLI Access

Table 1 lists the release history for this feature.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which 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 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.

Table 1 Feature Information for Role-Based CLI Access

Feature Name	Releases	Feature Information
Role-Based CLI Access	12.3(7)T 12.3(11)T 12.2(33)SRB 12.2(33)SB 12.2(33)SXI Cisco IOS XE 3.1.0SG	This feature enables network administrators to restrict user access to CLI and configuration information. In 12.3(11)T, the CLI view capability was extended to restrict user access on a per-interface level, and additional CLI views were introduced to support the extended view capability. Also, support to group configured CLI views into a superview was introduced. The following commands were introduced or modified: **commands (view)**, **enable**, **li-view**, **name (view)**, **parser view**, **parser view superview, secret**, **show parser view**, **show users**, **username**, **view**.

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.