



# Role-Based CLI Access

---

**Last Updated: January 26, 2012**

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 EXEC and configuration (Config) mode commands. Views restrict user access to 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 networking devices.

- [Finding Feature Information, page 1](#)
- [Prerequisites for Role-Based CLI Access, page 1](#)
- [Restrictions for Role-Based CLI Access, page 2](#)
- [Information About Role-Based CLI Access, page 2](#)
- [How to Use Role-Based CLI Access, page 3](#)
- [Configuration Examples for Role-Based CLI Access, page 9](#)
- [Additional References, page 12](#)
- [Feature Information for Role-Based CLI Access, page 13](#)

## 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](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

## Prerequisites for Role-Based CLI Access

Your image must support CLI views.



---

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

# Restrictions for Role-Based CLI Access

## Lawful Intercept Images Limitation

CLI views are a part of all platforms and Cisco IOS images because they are a part of the Cisco IOS parser. 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, page 2](#)
- [Root View, page 2](#)
- [About Superviews, page 2](#)
- [View Authentication via a New AAA Attribute, page 3](#)

# Benefits of Using CLI Views

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 XE routers. CLI views provide a more detailed access control capability for network administrators, thereby, improving the overall security and accountability of Cisco IOS XE software.

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 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 the following 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 3](#)
- [Configuring a Lawful Intercept View, page 6](#)
- [Configuring a Superview, page 7](#)
- [Monitoring Views and View Users, page 9](#)

## Configuring a CLI View

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

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
<p><b>Step 1</b> <code>enable view</code></p> <p><b>Example:</b></p> <pre>Router&gt; enable view</pre>	<p>Enables root view.</p> <ul style="list-style-type: none"> <li>Enter your privilege level 15 password (for example, root password) if prompted.</li> </ul>
<p><b>Step 2</b> <code>configure terminal</code></p> <p><b>Example:</b></p> <pre>Router# configure terminal</pre>	<p>Enters global configuration mode.</p>
<p><b>Step 3</b> <code>parser view view-name</code></p> <p><b>Example:</b></p> <pre>Router(config)# parser view first</pre>	<p>Creates a view and enters view configuration mode.</p>
<p><b>Step 4</b> <code>secret 5 encrypted-password</code></p> <p><b>Example:</b></p> <pre>Router(config-view)# secret 5 secret</pre>	<p>Associates a command-line interface (CLI) view or superview with a password.</p> <p><b>Note</b> You must issue this command before you can configure additional attributes for the view.</p>
<p><b>Step 5</b> <code>commands parser-mode {include   include-exclusive   exclude} [all] [interface interface-name   command]</code></p> <p><b>Example:</b></p> <pre>Router(config-view)# commands exec include show version</pre>	<p>Adds commands or interfaces to a view.</p> <ul style="list-style-type: none"> <li><i>parser-mode</i> --The mode in which the specified command exists.</li> <li><b>include</b> --Adds a command or an interface to the view and allows the same command or interface to be added to an additional view.</li> <li><b>include-exclusive</b> --Adds a command or an interface to the view and excludes the same command or interface from being added to all other views.</li> <li><b>exclude</b> --Excludes a command or an interface from the view; that is, customers cannot access a command or an interface.</li> <li><b>all</b> --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.</li> <li><b>interface interface-name</b> -- Interface that is added to the view.</li> <li><i>command</i> --Command that is added to the view.</li> </ul>

Command or Action	Purpose
<b>Step 6</b> <code>exit</code>  <b>Example:</b> <code>Router(config-view)# exit</code>	Exits view configuration mode.
<b>Step 7</b> <code>exit</code>  <b>Example:</b> <code>Router(config)# exit</code>	Exits global configuration mode.
<b>Step 8</b> <code>enable [privilege-level] [view view-name]</code>  <b>Example:</b> <code>Router# enable view first</code>	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.
<b>Step 9</b> <code>show parser view all</code>  <b>Example:</b> <code>Router# show parser view</code>	(Optional) Displays information about the view that the user is currently in. <ul style="list-style-type: none"> <li><b>all</b> --Displays information for all views that are configured on the router.</li> </ul> <b>Note</b> Although this command is available for both root and lawful intercept users, the <b>all</b> keyword is available only to root users. However, the <b>all</b> keyword can be configured by a user in root view to be available for users in lawful intercept view and CLI view.

- [Troubleshooting Tips, page 5](#)

## Troubleshooting Tips

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

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

After you have successfully deleted a view, a system message such as the following will be 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

Use this task to initialize and configure a view for lawful-intercept-specific commands and configuration information. (Only an administrator or a user who has level 15 privileges can initialize a lawful intercept view.)

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 following 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

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

### 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	<b>enable view</b>  <b>Example:</b>  Router> enable view	Enables root view. <ul style="list-style-type: none"> <li>• Enter your privilege level 15 password (for example, root password) if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b>  Router# configure terminal	Enters global configuration mode.

Command or Action	Purpose
<p><b>Step 3</b> <b>li-view</b> <i>li-password</i> <b>user</b> <i>username</i> <b>password</b> <i>password</i></p> <p><b>Example:</b></p> <pre>Router(config)# li-view lipass user li_admin password li_adminpass</pre>	<p>Initializes a lawful intercept view.</p> <p>After the li-view is initialized, you must specify at least one user via <b>user</b> <i>username</i> <b>password</b> <i>password</i> options.</p>
<p><b>Step 4</b> <b>username</b> <b>lawful-intercept</b> [<i>name</i>] [<b>privilege</b> <i>privilege-level</i>] <b>view</b> <i>view-name</i>] <b>password</b> <i>password</i></p> <p><b>Example:</b></p> <pre>Router(config)# username lawful-intercept li-user1 password li-user1pass</pre>	<p>Configures lawful intercept users on a Cisco device.</p>
<p><b>Step 5</b> <b>parser view</b> <i>view-name</i></p> <p><b>Example:</b></p> <pre>Router(config)# parser view li view name</pre>	<p>(Optional) Enters view configuration mode, which allows you to change the lawful intercept view password or the lawful intercept view name.</p>
<p><b>Step 6</b> <b>secret 5</b> <i>encrypted-password</i></p> <p><b>Example:</b></p> <pre>Router(config-view)# secret 5 secret</pre>	<p>(Optional) Changes an existing password for a lawful intercept view.</p>
<p><b>Step 7</b> <b>name</b> <i>new-name</i></p> <p><b>Example:</b></p> <pre>Router(config-view)# name second</pre>	<p>(Optional) Changes the name of a lawful intercept view.</p> <p>If this command is not issued, the default name of the lawful intercept view is “li-view.”</p>

- [Troubleshooting Tips, page 7](#)

## 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

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

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.

**Note**

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.

**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
<p><b>Step 1</b> <b>enable view</b></p> <p><b>Example:</b></p> <pre>Router&gt; enable view</pre>	<p>Enables root view.</p> <ul style="list-style-type: none"> <li>• Enter your privilege level 15 password (for example, root password) if prompted.</li> </ul>
<p><b>Step 2</b> <b>configure terminal</b></p> <p><b>Example:</b></p> <pre>Router# configure terminal</pre>	<p>Enters global configuration mode.</p>
<p><b>Step 3</b> <code>parser view superview-name superview</code></p> <p><b>Example:</b></p> <pre>Router(config)# parser view su_view1 superview</pre>	<p>Creates a superview and enters view configuration mode.</p>
<p><b>Step 4</b> <b>secret 5 <i>encrypted-password</i></b></p> <p><b>Example:</b></p> <pre>Router(config-view)# secret 5 secret</pre>	<p>Associates a CLI view or superview with a password.</p> <p><b>Note</b> You must issue this command before you can configure additional attributes for the view.</p>



Command or Action	Purpose
<p><b>Step 5</b> view view-name</p> <p><b>Example:</b></p> <pre>Router(config-view)# view view_three</pre>	<p>Adds a normal CLI view to a superview.</p> <p>Issue this command for each CLI view that is to be added to a given superview.</p>
<p><b>Step 6</b> exit</p> <p><b>Example:</b></p> <pre>Router(config-view)# exit</pre>	<p>Exits view configuration mode.</p>
<p><b>Step 7</b> exit</p> <p><b>Example:</b></p> <pre>Router(config)# exit</pre>	<p>Exits global configuration mode.</p>
<p><b>Step 8</b> show parser view all</p> <p><b>Example:</b></p> <pre>Router# show parser view</pre>	<p>(Optional) Displays information about the view that the user is currently in.</p> <ul style="list-style-type: none"> <li>• <b>all</b> --Displays information for all views that are configured on the router.</li> </ul> <p><b>Note</b> Although this command is available for both root and lawful intercept users, the <b>all</b> keyword is available only to root users. However, the <b>all</b> keyword can be configured by a user in root view to be available for users in lawful intercept view and CLI view.</p>

## 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

- [Configuring a CLI View Example, page 10](#)
- [Verifying a CLI View Example, page 10](#)
- [Configuring a Lawful Intercept View Example, page 11](#)
- [Configuring a Superview Example, page 11](#)

## Configuring a CLI View Example

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$Rl6BXXKecMEiQesxLyqygW.
commands exec include-exclusive show ip interface
commands exec include show ip
commands exec include show
commands exec include logout
!
```

## Verifying a CLI View Example

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 interface** 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
dvmp                 DVMP 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
.
.
.

```

## Configuring a Lawful Intercept View Example

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

```

## Configuring a Superview Example

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

The following sections provide references related to Role-Based CLI Access.

### Related Documents

Related Topic	Document Title
Security commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	<i>Cisco IOS Security Command Reference</i>
SNMP, MIBs, CLI configuration	“Configuring SNMP Support”

### 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 XE releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

### 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
<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>	<p><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></p>

## Feature Information for Role-Based CLI Access

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](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

**Table 1** Feature Information for Role-Based CLI Access

Feature Name	Releases	Feature Information
Role-Based CLI Access	Cisco IOS XE Release 2.1	<p>This feature enables network administrators to restrict user access to CLI and configuration information.</p> <p>In Cisco IOS XE Release 2.1, this feature was introduced on Cisco ASR 1000 Series Service Aggregation Routers.</p> <p>The following commands were new or modified by this feature: <b>commands (view)</b>, <b>enable</b>, <b>li-view</b>, <b>name (view)</b>, <b>parser view</b>, <b>parser view superview</b>, <b>secret</b>, <b>show parser view</b>, <b>show users</b>, <b>username</b>, <b>view</b>.</p>

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned 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. (1110R)

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

© 2012 Cisco Systems, Inc. All rights reserved.