Role-Based CLI Access

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, 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 for Role-Based CLI Access, page 11
- Feature Information for Role-Based CLI Access, page 12

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.

Prerequisites for Role-Based CLI Access

Your image must support CLI views.
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

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 devices. 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.

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 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
Superview

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, its associated CLI views are not deleted.

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

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

Before You Begin

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

- Enable AAA using 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 [inclusive]
4. secret [0 | 5] encrypted-password
5. commands parser-mode {exclude | include-exclusive | include} [all] [interface interface-name | command]
6. end
7. enable [privilege-level | view view-name]
8. show parser view all

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable view</td>
</tr>
<tr>
<td>Example:</td>
<td>Device&gt; enable view</td>
</tr>
<tr>
<td></td>
<td>Enables root view.</td>
</tr>
<tr>
<td></td>
<td>• Enter your privilege level 15 password (for example, root password) if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>parser view view-name [inclusive]</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# parser view first inclusive</td>
</tr>
<tr>
<td></td>
<td>Creates a view including all commands by default. If the inclusive keyword option is not selected, it creates a view excluding all commands by default. You are in the view configuration mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>secret [0</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-view)# secret 5 secret</td>
</tr>
<tr>
<td></td>
<td>Associates a CLI view or superview with a password.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>You must issue this command before you can configure additional attributes for the view.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>With CSCts50236, the password can be removed or overwritten. Use the no secret command to remove the configured password.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>commands parser-mode {exclude</td>
</tr>
<tr>
<td></td>
<td>Adds commands or interfaces to a view and specifies the mode in which the specified command exists.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config-view)# commands exec include show version</td>
<td><strong>Note</strong> While configuring parser view profiles, the following no or default commands are not saved to the startup configuration. These commands are in use until the device is reloaded. Once the device is reloaded, reapply these commands to get the required results.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• commands configure include all no</td>
</tr>
<tr>
<td></td>
<td>• commands interface include all no</td>
</tr>
<tr>
<td></td>
<td>• commands configure include all default</td>
</tr>
</tbody>
</table>

**Step 6**

<table>
<thead>
<tr>
<th>end</th>
<th>Exits view configuration mode and returns to privileged EXEC mode.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-view)# end</td>
</tr>
</tbody>
</table>

**Step 7**

<table>
<thead>
<tr>
<th>enable [privilege-level</th>
<th>view view-name]</th>
<th>Prompts you for a password to access a configured CLI view, and you can switch from one view to another view. Enter the password to access the CLI view.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Device# enable view first</td>
<td></td>
</tr>
</tbody>
</table>

**Step 8**

<table>
<thead>
<tr>
<th>show parser view all</th>
<th>(Optional) Displays information for all views that are configured on the device.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Device# show parser view all</td>
</tr>
</tbody>
</table>

**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**

You must associate a password with a view. If you do not associate a password, and you attempt to add commands to the view using the commands command, a system message such as the following is 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.
Before You Begin

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

**Note**

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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**        | **enable view** | Enables root view.  

  - Enter your privilege level 15 password (for example, root password) if prompted.  

<table>
<thead>
<tr>
<th>Example:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Device&gt; enable view</td>
<td></td>
</tr>
</tbody>
</table>
| **Step 2**        | **configure terminal** | Enters global configuration mode.  

<table>
<thead>
<tr>
<th>Example:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>
| **Step 3**        | **li-view li-password user username password password** | Initializes a lawful intercept view.  

  - After the li-view is initialized, you must specify at least one user via `user username password password` options.  

<table>
<thead>
<tr>
<th>Example:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Device(config)# li-view li-password user li_admin password li_adminpass</td>
<td></td>
</tr>
</tbody>
</table>
| **Step 4**        | **username lawful-intercept [name] [privilege privilege-level | view view-name] password password** | Configures lawful intercept users on a Cisco device.  

<table>
<thead>
<tr>
<th>Example:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Device(config)# username lawful-intercept li-user1 password li-user1pass</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>parser view view-name</strong></td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# parser view li view name</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><strong>secret 5 encrypted-password</strong></td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-view)# secret 5 secret</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><strong>name new-name</strong></td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-view)# name second</td>
</tr>
</tbody>
</table>

**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.

**Before You Begin**

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 using the `parser view` command.

**Note**

You can add a view to a superview only after you configure a password for the superview (using 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. end
7. show parser view all

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables root view.</td>
</tr>
<tr>
<td>enable view</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device&gt; enable view</td>
<td>Enter your privilege level 15 password (for example, root password) if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Creates a superview and enters view configuration mode.</td>
</tr>
<tr>
<td>parser view superview-name superview</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config)# parser view su_view1 superview</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Associates a CLI view or superview with a password.</td>
</tr>
<tr>
<td>secret 5 encrypted-password</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config-view)# secret 5 secret</td>
<td>You must issue this command before you can configure additional attributes for the view.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Adds a normal CLI view to a superview.</td>
</tr>
<tr>
<td>view view-name</td>
<td>Issue this command for each CLI view that is to be added to a given superview.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config-view)# view view_three</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Exits view configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>end</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config-view)# end</td>
<td></td>
</tr>
<tr>
<td>Device#</td>
<td></td>
</tr>
</tbody>
</table>
### Purpose

**Command or Action** | **Purpose**
---|---
**Step 7** | show parser view all

(Optional) Displays information for all views that are configured on the device.

**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 superview-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.

```
Device(config)# parser view first inclusive
Device(config-view)# secret 5 firstpass
Device(config-view)# command exec exclude show version
Device(config-view)# command exec exclude configure terminal
Device(config-view)# command exec exclude all show ip
Device(config-view)# exit
Device(config)# parser view second
Device(config-view)# secret 5 secondpass
Device(config-view)# command exec include-exclusive show ip interface
Device(config-view)# command exec include logout
Device(config-view)# exit

Device(config-view)# do show running-config | beg view

parser view first inclusive
secret 5 $1$MCmh$QuZaHsP1MPlff9sFCZvgW/
commands exec exclude configure terminal
commands exec exclude configure
commands exec exclude all show ip
commands exec exclude show version
commands exec exclude show
!
parser view second
secret 5 $1$P2MSR16BXXkceMEiQesxLYqy9W.
commands exec include-exclusive show ip interface
commands exec include show ip
commands exec include show
commands exec include logout
!```

---

User Security Configuration Guide
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.)

Device# enable view first
Password:
Device# ?
Exec commands:
    configure Enter configuration mode
    enable Turn on privileged commands
    exit Exit from the EXEC
    show Show running system information
Device# show ?
    ip IP information
    parser Display parser information
    version System hardware and software status
Device# show ip ?
    access-lists List IP access lists
    accounting The active IP accounting database
    alias 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 Device 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.
Device(config)# li-view lipass user li_admin password li_adminpass
Device(config)# end
! Enter the LI-View; that is, check to see what commands are available within the view.
Device# enable view li-view
Password:
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# parser view li-view
Device(config-view)# ?
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", "view_three", and "view_four" have been added to superview "su_view2":

```
Device# show running-config
!
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 for Role-Based CLI Access

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS commands</td>
<td>Cisco IOS Master Command List, All Releases</td>
</tr>
</tbody>
</table>
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 . An account on Cisco.com is not required.
# Table 1: Feature Information for Role-Based CLI Access

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role-Based CLI Access</td>
<td></td>
<td>The Role-Based CLI Access feature enables network administrators to restrict user access to CLI and configuration information. 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, and view.</td>
</tr>
<tr>
<td>Role-Based CLI Inclusive Views</td>
<td></td>
<td>The Role-Based CLI Inclusive Views feature enables a standard CLI view including all commands by default. The following command was modified: parser view inclusive.</td>
</tr>
</tbody>
</table>