

# Cisco IOS Role–Based Access Control with SDM: Separating Configuration Permission Between Operational Groups

Document ID: 106263

---

## Introduction

### Prerequisites

- Requirements

- Components Used

- Conventions

### Background Information

#### Configure

- Associate Users with a View

- Parser View Configuration

- SDM CLI Views Support

#### Verify

#### Troubleshoot

#### NetPro Discussion Forums – Featured Conversations

#### Related Information

---

## Introduction

Routing and security functionality is traditionally supported in separate devices, which offers a clear division of management responsibility between the networking infrastructure and security services. The convergence of security and routing functionality in the Cisco Integrated Services Routers does not offer this clear, multi–device separation. Some organizations need a segregation of configuration capability to restrict customers or service management groups along functional boundaries. CLI Views, a Cisco IOS Software feature, seeks to address this need with Role–Based CLI Access. This document describes the configuration defined by SDM support of Cisco IOS Role–Based Access Control, and offers background into the capabilities of CLI Views from the Cisco IOS Command–Line Interface.

## Prerequisites

### Requirements

There are no specific requirements for this document.

### Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

## Background Information

Many organizations delegate responsibility for the maintenance of routing and infrastructural connectivity to a network operations group, and responsibility for the maintenance of firewall, VPN, and intrusion prevention functionality to a security operations group. CLI Views can restrict security functionality configuration and monitoring capability to the secops group, and conversely restrict the network connectivity, routing, and other infrastructural tasks to the netops group.

Some service providers want to offer limited configuration or monitoring ability to customers, but not allow customers to configure or view other device settings. Once again, CLI Views offer granular control over CLI capability to restrict users or user groups to execute only authorized commands.



Cisco IOS software has offered a capability to restrict CLI commands with a TACACS+ server for authorization to permit or deny capability to execute CLI commands based on username or user group membership. CLI Views offer similar capability, but the policy control is applied by the local device after the specified view of the user is received from the AAA server. When AAA Command Authorization is used, every command must be individually authorized by the AAA server, which causes frequent dialogue between the device and the AAA server. CLI Views allow per-device CLI policy control, whereas AAA Command Authorization applies the same command authorization policy to all devices a user accesses.

## Configure

In this section, you are presented with the information to configure the features described in this document.

**Note:** Use the Command Lookup Tool (registered customers only) to obtain more information on the commands used in this section.

### Associate Users with a View

Users can be associated with a local CLI View by a return attribute from AAA or in local Authentication configuration. For local configuration, the username is configured with an additional **view** option, which matches the configured **parser view** name. These example users are configured for the default SDM Views:

```
username fw-user privilege [privilege-level] view SDM_Firewall
username monitor-user privilege [privilege-level] view SDM_Monitor
username vpn-user privilege [privilege-level] view SDM_EasyVPN_Remote
username sdm-root privilege [privilege-level] view root
```

Users who are assigned to a given view can temporarily switch to another view if they have the password for the view that they want to enter. Issue this exec command in order to change views:

```
enable view view-name
```

## Parser View Configuration

CLI Views can be configured from the router CLI, or through SDM. SDM provides static support for four views, as discussed in the SDM CLI Views Support section. In order to configure CLI View from the Command-Line Interface, a user must be defined as a **root** view user, or they must belong to view with access to the **parser view** configuration. Users who are not associated with a view and who try to configure views receive this message:

```
router(config#parser view test-view
No view Active! Switch to View Context
```

CLI Views allow inclusion or exclusion of complete command hierarchies for both executive and configuration modes, or only portions thereof. Three options are available to allow or disallow a command or command hierarchy in a given view:

```
router(config-view)#commands configure ?
exclude          Exclude the command from the view
include          Add command to the view
include-exclusive Include in this view but exclude from others
```

CLI Views truncate the running-config so the Parser View configuration is not displayed. However, the Parser View configuration is visible in the startup-config.

Refer to Role-Based CLI Access for more information about view definition.

## Verifying Parser View Association

Users who are assigned to a Parser View can determine which view they are assigned to when they are logged in to a router. If the **show parser view** command is allowed for the users views, they can issue the **show parser view** command in order to determine their view:

```
router#sh parser view
Current view is 'SDM_Firewall'
```

## SDM CLI Views Support

SDM offers three default views, two for configuration and monitoring of Firewall and VPN components, and one restricted monitoring-only view. An additional default **root** view is available in SDM as well.

SDM does not provide the ability to modify the commands included in or excluded from each default view, and offers no capability to define additional views. If additional views are defined from the CLI, SDM does not offer the additional views in its **User Accounts/Views** configuration panel.

These views and respective command permissions are pre-defined for SDM:

### SDM\_Firewall View

```
parser view SDM_Firewall
secret 5 $l$w/cD$TlryjKM8aGCnIaKSm.Cx9/
commands interface include all ip inspect
commands interface include all ip verify
commands interface include all ip access-group
commands interface include ip
commands interface include description
commands interface include all no ip inspect
```

```

commands interface include all no ip verify
commands interface include all no ip access-group
commands interface include no ip
commands interface include no description
commands interface include no
commands configure include end
commands configure include all access-list
commands configure include all ip access-list
commands configure include all interface
commands configure include all zone-pair
commands configure include all zone
commands configure include all policy-map
commands configure include all class-map
commands configure include all parameter-map
commands configure include all appfw
commands configure include all ip urlfilter
commands configure include all ip inspect
commands configure include all ip port-map
commands configure include ip cef
commands configure include ip
commands configure include all crypto
commands configure include no end
commands configure include all no access-list
commands configure include all no ip access-list
commands configure include all no interface
commands configure include all no zone-pair
commands configure include all no zone
commands configure include all no policy-map
commands configure include all no class-map
commands configure include all no parameter-map
commands configure include all no appfw
commands configure include all no ip urlfilter
commands configure include all no ip inspect
commands configure include all no ip port-map
commands configure include no ip cef
commands configure include no ip
commands configure include all no crypto
commands configure include no
commands exec include all vlan
commands exec include dir all-filefilesystems
commands exec include dir
commands exec include crypto ipsec client ezvpn connect
commands exec include crypto ipsec client ezvpn xauth
commands exec include crypto ipsec client ezvpn
commands exec include crypto ipsec client
commands exec include crypto ipsec
commands exec include crypto
commands exec include write memory
commands exec include write
commands exec include all ping ip
commands exec include ping
commands exec include configure terminal
commands exec include configure
commands exec include all show
commands exec include all debug appfw
commands exec include all debug ip inspect
commands exec include debug ip
commands exec include debug
commands exec include all clear

```

## **SDM\_EasyVPN\_Remote View**

```

parser view SDM_EasyVPN_Remote
secret 5 $1$UnC3$ienYd0L7Q/9xfCNkBQ4Uu.
commands interface include all crypto
commands interface include all no crypto

```

```
commands interface include no
commands configure include end
commands configure include all access-list
commands configure include ip radius source-interface
commands configure include ip radius
commands configure include all ip nat
commands configure include ip dns server
commands configure include ip dns
commands configure include all interface
commands configure include all dot1x
commands configure include all identity policy
commands configure include identity profile
commands configure include identity
commands configure include all ip domain lookup
commands configure include ip domain
commands configure include ip
commands configure include all crypto
commands configure include all aaa
commands configure include default end
commands configure include all default access-list
commands configure include default ip radius source-interface
commands configure include default ip radius
commands configure include all default ip nat
commands configure include default ip dns server
commands configure include default ip dns
commands configure include all default interface
commands configure include all default dot1x
commands configure include all default identity policy
commands configure include default identity profile
commands configure include default identity
commands configure include all default ip domain lookup
commands configure include default ip domain
commands configure include default ip
commands configure include all default crypto
commands configure include all default aaa
commands configure include default
commands configure include no end
commands configure include all no access-list
commands configure include no ip radius source-interface
commands configure include no ip radius
commands configure include all no ip nat
commands configure include no ip dns server
commands configure include no ip dns
commands configure include all no interface
commands configure include all no dot1x
commands configure include all no identity policy
commands configure include no identity profile
commands configure include no identity
commands configure include all no ip domain lookup
commands configure include no ip domain
commands configure include no ip
commands configure include all no crypto
commands configure include all no aaa
commands configure include no
commands exec include dir all-file systems
commands exec include dir
commands exec include crypto ipsec client ezvpn connect
commands exec include crypto ipsec client ezvpn xauth
commands exec include crypto ipsec client ezvpn
commands exec include crypto ipsec client
commands exec include crypto ipsec
commands exec include crypto
commands exec include write memory
commands exec include write
commands exec include all ping ip
commands exec include ping
```

```
commands exec include configure terminal
commands exec include configure
commands exec include all show
commands exec include no
commands exec include all debug appfw
commands exec include all debug ip inspect
commands exec include debug ip
commands exec include debug
commands exec include all clear
```

## SDM\_Monitor View

```
parser view SDM_Monitor
secret 5 $1$RDYW$OABbxSgtx1kOozLlkBeJ9/
commands configure include end
commands configure include all interface
commands configure include no end
commands configure include all no interface
commands exec include dir all-filestystems
commands exec include dir
commands exec include all crypto ipsec client ezvpn
commands exec include crypto ipsec client
commands exec include crypto ipsec
commands exec include crypto
commands exec include all ping ip
commands exec include ping
commands exec include configure terminal
commands exec include configure
commands exec include all show
commands exec include all debug appfw
commands exec include all debug ip inspect
commands exec include debug ip
commands exec include debug
commands exec include all clear
```

## Verify

There is currently no verification procedure available for this configuration.

## Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

## NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

|  |
|--|
| NetPro Discussion Forums – Featured Conversations for Security |
| Security: Intrusion Detection [Systems]                        |
| Security: AAA  |
| Security: General  |
| Security: Firewalling  |

## Related Information

- [Role-Based CLI Access](#)
  - [Technical Support & Documentation – Cisco Systems](#)
- 

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2007 – 2008 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

---

Updated: May 12, 2008

Document ID: 106263

---