CHAPTER 7

Configuring User Accounts and RBAC

This chapter describes how to configure user accounts and role-based access control (RBAC) on the Cisco 1000 Series Connected Grid Routers (hereafter referred to as Cisco CG-OS router).

This chapter includes the following sections:

Information About User Accounts and RBAC

You can create and manage user accounts and assign roles that limit access to operations on the Cisco CG-OS router. RBAC allows you to define the rules for and assign roles that restrict the authorization that the user has to access management operations.

This section includes the following topics:

About User Accounts

You can configure up to a maximum of 256 user accounts. Cisco CG-OS provides one default user account: *admin*.

By default, the user account does not expire unless you explicitly configure it to expire. The expire option determines the date when Cisco CG-OS disables the user account.

Caution User accounts can only be defined on the default VDC. The Cisco CG-OS router does not support multiple configuration on multiple VDCs.

Caution Cisco CG-OS does not support all numeric usernames, whether created with TACACS+ or RADIUS, or created locally on the CG-OS router. When an all numeric user name exists on an AAA server and is entered during login, the user is not logged in.

Tip The following words are reserved and cannot be used to configure users: bin, daemon, adm, lp, sync, shutdown, halt, mail, news, uucp, operator, games, gopher, ftp, nobody, nscd, mailnull, root, rpc, rpcuser, xfs, gdm, mtsuser, ftpuser, man, and sys.

Characteristics of Strong Passwords

A strong password has the following characteristics:

- At least eight characters long
- Does not contain many consecutive characters (such as “abcd”)
- Does not contain many repeating characters (such as “aaabbb”)
- Does not contain dictionary words
- Does not contain proper names
- Contains both uppercase and lowercase characters
- Contains numbers

The following are examples of strong passwords:

- If2CoM18
- 2004AsdfLkj30
- Cb1955S21

Note Please note these important notes about passwords on the Cisco CG-OS router:

- User passwords are not displayed in the configuration files.
- Clear text passwords cannot contain dollar signs ($) or spaces anywhere in the password. Also, they cannot include these special characters at the beginning of the password: quotation marks (" or '), vertical bars (|), or right angle brackets (>).
- When a password is trivial (such as a short, easy-to-decipher password), Cisco CG-OS rejects the password configuration when password-strength checking is enabled. (See Enabling Password-Strength Checking, page 7-5.) Be sure to configure a strong password as shown in the sample configuration. Passwords are case sensitive.

About User Roles

User roles contain rules that define the operations allowed for the user who is assigned the role. Each user role can contain multiple rules and each user can have multiple roles. For example, if role1 allows access only to configuration operations, and role2 allows access only to debug operations, then users who belong to both role1 and role2 can access configuration and debug operations. You can also change a user role interface policy to limit the interfaces that the user can access.

Cisco CG-OS provides four default user roles within the default VDC:

- network-admin—Complete read-and-write access to the entire Cisco CG-OS router
- network-operator—Complete read access to the entire Cisco CG-OS router
- vdc-admin—Read-and-write access limited to a VDC (in this case, the default VDC)
- vdc-operator—Read access limited to a VDC (in this case, the default VDC)

Note You cannot change the default user roles.

You can create custom roles within the default VDC. By default, the user roles that you create allow access only to the **show**, **exit**, **end**, and **configure terminal** commands.You must add rules to allow users to display or configure features.

Note When you belong to multiple roles, you can execute a combination of all the commands permitted by these roles. Access to a command takes priority over being denied access to a command. For example, suppose a user has RoleA, which denied access to the configuration commands. However, the user also has RoleB, which has access to the configuration commands. In this case, the user has access to the configuration commands.

About User Role Rules

The rule is the basic element of a role. A rule defines what operations the role allows the user to perform. You can apply rules for the following parameters:

- Command—A command or group of commands defined in a regular expression
- Feature—Commands that apply to a function provided by Cisco CG-OS
- Feature group—Default or user-defined group of features

These parameters create a hierarchical relationship. The most basic control parameter is the command. The next control parameter is the feature, which represents all commands associated with the feature. The last control parameter is the feature group. The feature group combines related features and allows you to easily manage the rules. Cisco CG-OS also supports the predefined feature group L3 that you can use.

You can configure up to 256 rules for each role.

The user-specified rule number determines the order in which the rules are applied. Rules are applied in descending order. For example, when a role has three rules, rule 3 is applied before rule 2, which is applied before rule 1.

Guidelines and Limitations

Configuring User Accounts

You can configure up to 256 user accounts on the Cisco CG-OS router.

If you have a user account configured on the local Cisco CG-OS router that has the same name as a remote user account on an AAA server, Cisco CG-OS applies the user roles for the local user account to the remote user, not the user roles configured on the AAA server.

You cannot delete the default admin user account.

You cannot remove the default user roles from the default admin user account.

Note A user account must have at least one user role.

Configuring Roles

You can create up to 64 user-defined roles on the Cisco CG-OS router in addition to the four default user roles (network-admin, vdc-admin, network-operator, and vdc-operator).You cannot change the default user roles.

You can add up to 256 rules to a user role.

You can assign a maximum of 64 user roles to a user account.

Creating Feature Groups

You can add up to 64 user-defined feature groups on the Cisco CG-OS router in addition to the default feature group, L3.

Default Settings

Table 7-1 lists the default settings for user accounts and RBAC parameters.

Table 7-1 Default User Accounts and RBAC Parameters

Parameters	Default
User account password	Undefined
Password strength checking	Enabled
User account expiry date	None
User account role in the default VDC	Network-operator if the creating user has the network-admin role, or vdc-operator if the creating user has the vdc-admin role
Default user roles in the default VDC	Network-admin, network-operator, vdc-admin, and vdc-operator
Interface policy	All interfaces are accessible
Feature group	L3: Enables Layer 3 on the Cisco CG-OS router

Enabling Password-Strength Checking

You can enable password-strength checking, which prevents you from creating weak passwords for user accounts. For information about strong passwords, see Characteristics of Strong Passwords, page 7-2.

By default, this option is enabled on the Cisco CG-OS router.

BEFORE YOU BEGIN

No prerequisites.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**password strength-check**	Enables password-strength checking. By default, this option is enabled. You can disable password-strength checking by using the **no** form of this command.
Step 3	**show password strength-check**	(Optional) Displays the password-strength check configuration.
Step 4	**copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

EXAMPLE

This example shows how to enable password-strength checking.

```
router_cgr01# configure terminal
router_cgr01(config)# password strength-check
router_cgr01(config)# copy running-config startup-config
```

Configuring User Accounts

You can create a maximum of 256 user accounts on a Cisco CG-OS router. User accounts have the following attributes:

- Username
- Password
- Expiry date
- User roles

You can enter the password in clear text format or encrypted format for the Cisco CG-OS router. The password encrypts clear text passwords before saving them to the running configuration. Encrypted format passwords are saved to the running configuration without further encryption.

User accounts can have a maximum of 64 user roles. For more information on user roles, see Configuring Roles, page 7-7.

Note The Cisco CG-OS router only supports the default VDC. The Cisco CG-OS router does not support multiple VDCs.

Note Changes to user account attributes do not take effect until the user logs in and creates a new session.

Note You cannot delete the default admin user account. You can create another account with the network-admin or vdc-admin role.

BEFORE YOU BEGIN

Determine which roles to assign to which user accounts.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**show role**	(Optional) Displays the user roles available. You can configure other user roles, if necessary. (See Creating User Roles and Rules, page 7-7.)
Step 3	**username** *user-id* [**password** [**0** | **5**] *password*] [**expire** *date*] [**role** *role-name*]	Configures a user account. User accounts can have a maximum of 64 user roles. *user-id*–Case-sensitive, alphanumeric character string with a maximum length of 28 characters. *password*–Default password is undefined. The **0** option indicates that the password is clear text and the **5** option indicates that the password is encrypted. The default is **0** (clear text). **Note** If you do not specify a password, the user might not be able to log in to the Cisco CG-OS router. For information about using SSH public keys instead of passwords, see Specifying the SSHv2 Public Keys for User Accounts, page 5-4. *date*–Format is YYYY-MM-DD. The default is no expiry date.
Step 4	**show user-account**	(Optional) Displays the role configuration.
Step 5	**copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

EXAMPLE

This example shows how to configure a user account.

```
router_cgr01# configure terminal
router_cgr01(config)# show role
router_cgr01(config)# username NewUser password 5 4Ty18Rnt expire 2013-01-15 jsmith
router_cgr01(config)# copy running-config startup-config
```

Configuring Roles

This section includes the following topics:

- Creating User Roles and Rules, page 7-7
- Creating Feature Groups, page 7-8
- Changing User Role Interface Policies, page 7-9
- Verifying Configuration, page 7-10

Creating User Roles and Rules

You can configure up to 64 user roles. Each user role can have up to 256 rules. You can assign a user role to more that one user account.

The rule number that you specify determines the order in which the rules are applied. Cisco CG-OS applies the rules in descending order. For example, when a role has three rules, rule 3 is applied before rule 2, which is applied before rule 1.

BEFORE YOU BEGIN

Identify which roles and rules must be assigned to each user account.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**role name** *role-name*	Specifies a user role and enters role configuration mode. The *role-name* argument is a case-sensitive, alphanumeric character string with a maximum length of 16 characters.

	Command	Purpose
Step 3	**rule** *number* {**deny** | **permit**} **command** *command-string*	Configures a command rule. The *command-string* argument can contain spaces and regular expressions. For example, "interface ethernet *" includes all Ethernet interfaces. Repeat this command for as many rules as needed.
	rule *number* {**deny** | **permit**} {**read** | **read-write**}	Configures a read-only or read-and-write rule for all operations.
	rule *number* {**deny** | **permit**} {**read** | **read-write**} **feature** *feature-name*	Configures a read-only or read-and-write rule for a feature. Use the **show role feature** command to display a list of features. Repeat this command for as many rules as needed.
	rule *number* {**deny** | **permit**} {**read** | **read-write**} **feature-group** *group-name*	Configures a read-only or read-and-write rule for a feature group. Use the **show role feature-group** command to display a list of feature groups. Repeat this command for as many rules as needed.
Step 4	**description** *text*	(Optional) Configures the role description. You can include spaces in the description.
Step 5	**show role**	(Optional) Displays the user role configuration.
Step 6	**copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

EXAMPLE

This example shows how to create the user role UserA and define rules for that user.

```
router_cgr01# configure terminal
router_cgr01(config)# role name operator_noc
router_cgr01(config-role)# rule 1 deny command clear users
router_cgr01(config-role)# rule 2 deny read-write
router_cgr01(config-role)# rule 3 permit read feature ospf
router_cgr01(config-role)# rule 4 deny read-write L3
router_cgr01(config-role)# copy running-config startup-config
```

Creating Feature Groups

You can create custom feature groups to add to the default list of features provided by Cisco CG-OS. These groups contain one or more of the features. You can create up to 64 feature groups on the Cisco CG-OS router.

Note You cannot change the default feature group L3.

BEFORE YOU BEGIN

Identify any specific features that must be specified in the Cisco CG-OS router.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**role feature-group** *group-name*	Specifies a user role feature group and enters role feature group configuration mode. The *group-name* argument is a case-sensitive, alphanumeric character string with a maximum length of 32 characters.
Step 3	**feature** *feature-name*	Specifies a feature for the feature group. Repeat this command for as many features as needed. **Note** Use the **show role component** command to display a list of features.
Step 4	**show role feature-group**	(Optional) Displays the role feature group configuration.
Step 5	**copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

EXAMPLE

This example shows how to create the custom feature group GroupA to expand the default list of features provided by Cisco CG-OS.

```
router_cgr01# configure terminal
router_cgr01(config)# role feature GroupA
router_cgr01(config-role-featuregrp)# feature abc
router_cgr01(config-role-featuregrp)# copy running-config startup-config
```

Changing User Role Interface Policies

You can change a user role interface policy to limit the interfaces that the user can access. By default, a user role (unless specifically configured otherwise) allows a user to have access to all interfaces on the Cisco CG-OS router.

Note You cannot change the default roles network-admin, network-operator, vdc-admin, and vdc-operator.

BEFORE YOU BEGIN

Create one or more user roles. (See Creating User Roles and Rules, page 7-7.)

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**role name** *role-name*	Specifies a user role and enters role configuration mode.
Step 3	**interface policy deny**	Enters role interface policy configuration mode.
Step 4	**permit interface {ethernet | cellular | wimax}** *slot/port*	Specifies a list of interfaces that the role can access. Repeat this command for each interface to which you want the user to have access.
Step 5	**show role**	(Optional) Displays the role configuration.
Step 6	**copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

EXAMPLE

This example shows how to change a user role interface policy to limit the user to be able to access and configure only specific Ethernet interfaces on the Cisco CG-OS router.

```
router_cgr01# configure terminal
router_cgr01(config)# role name EthOnly1to4
router_cgr01(config-role)# interface policy deny
router_cgr01(config-role-interface)# permit interface ethernet 2/1-4
router_cgr01(config-role-interface)# copy running-config startup-config
```

Verifying Configuration

To display user account and RBAC configuration information, enter any or all of the following commands:

Command	Purpose
show role	Displays the user role configuration.
show role feature	Displays the feature list.
show role feature-group	Displays the feature group configuration.
show startup-config security	Displays the user account configuration in the startup configuration.
show running-config security [**all**]	Displays the user account configuration in the running configuration. The **all** keyword displays the default values for the user accounts.
show user-account	Displays user account information.

Configuration Example

The following example shows how to configure a user role:

```
role name UserA
    rule 3 permit interface ethernet 2/1-4
    rule 2 permit read feature ospf
    rule 1 deny command clear *
```

The following example shows how to configure a user role feature group:

```
role feature-group name Security-features
    feature radius
    feature aaa
    feature access-list
```