Create User Profiles and Assign Privileges

To provide controlled access to the System Admin configurations on NCS 1004, you must create user profiles and assign privileges. While assigning privileges, you can specify command rules and data rules, and apply these rules to user groups. To create users, groups, command rules, and data rules, use the authentication, authorization, and accounting (`aaa`) commands in the System Admin Config mode. You can also use the `aaa` commands to change the disaster-recovery password.

You can use a username and a password for authentication. On successful authentication, you can execute commands and access data elements that are based on the command rules and data rules. Users, who are part of a user group, have access privileges to the system as defined in the command rules and data rules for that user group.

Use the **show run aaa** command in the System Admin Config mode to view existing aaa configurations.

The topics that are covered in this chapter are:

Create a User Profile

Users are included in a user group and assigned certain privileges. The users have restricted access to the commands and configurations in the System Admin console, based on assigned privileges.

NCS 1004 supports up to 1024 user profiles.

Note Users who are created in the System Admin are different from users who are created in XR. As a result, the username and password of a System Admin user cannot be used to access the XR, and the other way round.

As a XR user, you can access the System Admin by entering the **admin** command in the XR EXEC mode. NCS 1004 does not prompt you to enter any username and password. As a XR user, you are provided full access to the System Admin console.

Procedure

Step 1 **admin**

Example:

```
RP/0/RP0/CPU0:ios# admin
```

Enters System Admin EXEC mode.

Step 2 **config**

Example:

```
sysadmin-vm:0_RP0# config
```

Enters System Admin config mode.

Step 3 **aaa authentication users user** *user_name*

Example:

```
sysadmin-vm:0_RP0#(config)#aaa authentication users user us1
```

Creates a new user and enters user configuration mode. In the example, the user "us1" is created.

Step 4 **password** *password*

Example:

```
sysadmin-vm:0_RP0#(config-user-us1)#password pwd1
```

Specifies the password that is used for the user authentication when you log in as System Admin.

Step 5 **uid** *user_id_value*

Example:

```
sysadmin-vm:0_RP0#(config-user-us1)#uid 100
```

Specifies numeric value. You can enter any 32-bit integer.

Step 6 **gid** *group_id_value*

Example:

```
sysadmin-vm:0_RP0#(config-user-us1)#gid 50
```

Specifies numeric value. You can enter any 32-bit integer.

Step 7 **ssh_keydir** *ssh_keydir*

Example:

```
sysadmin-vm:0_RP0#(config-user-us1)#ssh_keydir dir1
```

Specifies any alphanumeric value.

Step 8 **homedir** *homedir*

Example:

```
sysadmin-vm:0_RP0#(config-user-us1)#homedir dir2
```

Specifies any alphanumeric value.

Step 9 Use the **commit** or **end** command.

commit—Saves the configuration changes and remains within the configuration session.

end—Prompts user to take one of these actions:

- **Yes**—Saves configuration changes and exits the configuration session.
- **No**—Exits the configuration session without committing the configuration changes.
- **Cancel**—Remains in the configuration session, without committing the configuration changes.

What to do next

- Create a user group that includes the user profile that is created in this task. See Create a User Group, on page 3.
- Create command rules that apply to the user group. See Create Command Rules, on page 4.
- Create data rules that apply to the user group. See Create Data Rules, on page 7.

Create a User Group

Create a new user group to associate command rules and data rules with it. The command rules and data rules are enforced on all users that are part of the user group.

NCS 1004 supports up to 32 user groups.

Before you begin

Create a user profile. See Create a User Profile, on page 1.

Procedure

Step 1 **admin**

Example:

```
RP/0/RP0/CPU0:ios# admin
```

Enters System Admin EXEC mode.

Step 2 **config**

Example:

```
sysadmin-vm:0_RP0# config
```

Enters System Admin config mode.

Step 3 **aaa authentication groups group** *group_name*

Example:

```
sysadmin-vm:0_RP0#(config)#aaa authentication groups group gr1
```

Creates a new user group (if it is not already present) and enters the group configuration mode. In this example, the user group "gr1" is created.

Note By default, the system creates the user group "root-system" during the root user creation. The root user is part of this user group. Users added to this group get root user permissions.

Step 4 **users** *user_name*

Example:

```
sysadmin-vm:0_RP0#(config-group-gr1)#users us1
```

Specifies the name of the user that must be part of the user group.

You can specify multiple usernames that are enclosed within double quotes. For example, **users** "*user1 user2* ...".

Step 5 **gid** *group_id_value*

Example:

```
sysadmin-vm:0_RP0#(config-group-gr1)#gid 50
```

Specifies numeric value. You can enter any 32-bit integer.

Step 6 Use the **commit** or **end** command.

commit-Saves the configuration changes and remains within the configuration session.

end—Prompts user to take one of these actions:

- **Yes**—Saves configuration changes and exits the configuration session.
- **No**—Exits the configuration session without committing the configuration changes.
- **Cancel**—Remains in the configuration session, without committing the configuration changes.

What to do next

- Create command rules. See Create Command Rules, on page 4.
- Create data rules. See Create Data Rules, on page 7.

Create Command Rules

Command rules are a set of rules that you can define for users of a user group to permit or deny the use of certain commands. You can associate command rules to a user group and apply the rule to a complete list of users in the user group.

You can create a command rule by specifying whether to permit or deny an operation, on command. The following table lists the possible operation and permission combinations:

Operation	**Accept Permission**	**Reject Permission**
Read (R)	Displays command on the CLI, when you enter "?" from the CLI.	Does not display command on the CLI, when you enter "?" from the CLI.

Execute (X)	Executes command from the CLI.	Could not execute command from the CLI.
Read and execute (RX)	Displays command on the CLI and can execute command.	Command is not visible or executable from the CLI.

By default, all the permissions are set to **Reject**.

Each command rule is identified by a number that is associated with it. When you apply multiple command rules to a user group, the command rule with a lower number takes precedence. For example, cmdrule5 permits read access, while cmdrule10 rejects read access. When both these command rules are applied to the same user group, user in this group gets read access because cmdrule 5 takes precedence.

As an example, you can create the command rule to deny read and execute permissions for the "show platform" command.

Before you begin

Create a user group. See Create a User Group, on page 3.

Procedure

Step 1 **admin**

Example:

```
RP/0/RP0/CPU0:ios# admin
```

Enters System Admin EXEC mode.

Step 2 **config**

Example:

```
sysadmin-vm:0_RP0# config
```

Enters System Admin config mode.

Step 3 **aaa authorization cmdrules cmdrule** *command_rule_number*

Example:

```
sysadmin-vm:0_RP0#(config)# aaa authorization cmdrules cmdrule 1100
```

Specifies numeric value as the command rule number. You can enter a 32-bit integer.

Important Do no use numbers 1–1000 because they are reserved by Cisco.

This command creates a new command rule (if it is not already present) and enters the command rule configuration mode.

In the example, command rule "1100" is created.

Note By default, the system creates "cmdrule 1" when the root-system user is created. This command rule provides "accept" permission to "read" and "execute" operations for all commands. Therefore, the root user has no restrictions that are imposed on it, unless "cmdrule 1" is modified.

Step 4 **command** *command_name*

Example:

```
sysadmin-vm:0_RP0#(config-cmdrule-1100)#command "show platform"
```

Specifies the command for which permission is to be controlled.

If you enter an asterisk '*' for **command**, it indicates that the command rule is applicable to all commands.

Step 5 **ops {r | x | rx}**

Example:

```
sysadmin-vm:0_RP0#(config-cmdrule-1100)#ops rx
```

Specifies the operation for which permission has to be set:

- **r** — Read
- **x** — Execute
- **rx** — Read and execute

Step 6 **action** {**accept** | **accept_log** | **reject**}

Example:

```
sysadmin-vm:0_RP0#(config-cmdrule-1100)#action reject
```

Specifies whether users are permitted or denied the use of the operation.

- **accept** — Users are permitted to perform the operation
- **accept_log**— Users are permitted to perform the operation and every access attempt is logged.
- **reject**— Users are restricted from performing the operation.

Step 7 **group** *user_group_name*

Example:

```
sysadmin-vm:0_RP0#(config-cmdrule-1100)#group gr1
```

Specifies the user group on which the command rule applies.

Step 8 **context** *connection_type*

Example:

```
sysadmin-vm:0_RP0#(config-cmdrule-1100)#context *
```

Specifies the type of connection to which this rule applies. The connection type can be *netconf* (Network Configuration Protocol), *cli* (Command Line Interface), or *xml* (Extensible Markup Language). It is recommended that you enter an asterisk '*'; this indicates that the command rule applies to all connection types.

Step 9 Use the **commit** or **end** command.

commit–Saves the configuration changes and remains within the configuration session.

end–Prompts user to take one of these actions:

- **Yes**–Saves configuration changes and exits the configuration session.
- **No**–Exits the configuration session without committing the configuration changes.
- **Cancel**–Remains in the configuration session, without committing the configuration changes.

What to do next

Create data rules. See Create Data Rules, on page 7.

Create Data Rules

Data rules are rules based on which users of the user group are either permitted, or denied, accessing and modifying configuration data elements. The data rules are associated to a user group. The data rules are applied to all the users who are part of the user group.

Each data rule is identified by a number that is associated to it. When multiple data rules are applied to a user group, the data rule with a lower number takes precedence.

Before you begin

Create a user group. See Create a User Group, on page 3.

Procedure

Step 1 **admin**

Example:

```
RP/0/RP0/CPU0:ios# admin
```

Enters System Admin EXEC mode.

Step 2 **config**

Example:

```
sysadmin-vm:0_RP0# config
```

Enters System Admin config mode.

Step 3 **aaa authorization datarules datarule** *data_rule_number*

Example:

```
sysadmin-vm:0_RP0#(config)#aaa authorization datarules datarule 1100
```

Specifies a numeric value as the data rule number. You can enter a 32-bit integer.

Important Do no use numbers between 1–1000 because they are reserved by Cisco.

This command creates a new data rule (if it is not already present) and enters the data rule configuration mode. In the example, data rule "1100" is created.

Note By default, the system creates "datarule 1", when the root-system user is created. This data rule provides "accept" permission to "read", "write", and "execute" operations for all the configuration data. Therefore, the root user has no restrictions that are imposed on it, unless "datarule 1" is modified.

Step 4 **keypath** *keypath*

Example:

```
sysadmin-vm:0_RP0#(config-datarule-1100)#keypath  /aaa/disaster-recovery
```

Specifies the key path of the data element. The key path is an expression defining the location of the data element. If you enter an asterisk '*' for **keypath** , it indicates that the command rule is applicable to all configuration data.

Step 5 **ops** *operation*

Example:

```
sysadmin-vm:0_RP0#(config-datarule-1100)#ops rw
```

Specifies the operation for which permission has to be set. Use the following letters to identify various operations:

- c—Create
- d—Delete
- u—Update
- w—Write (a combination of create, update, and delete)
- r—Read
- x—Execute

Step 6 **action** {**accept** | **accept_log** | **reject**}

Example:

```
sysadmin-vm:0_RP0#(config-datarule-1100)#action reject
```

Specifies whether to permit or deny users to perform the operation.

- **accept**—Permit users to perform the operation
- **accept_log**—Permit users to perform the operation and log every access attempt
- **reject**—Restrict users from performing the operation

Step 7 **group** *user_group_name*

Example:

```
sysadmin-vm:0_RP0#(config-datarule-1100)#group gr1
```

Specifies the user group to which you can apply the data rule. You can also specify multiple group names.

Step 8 **context** *connection type*

Example:

```
sysadmin-vm:0_RP0#(config-datarule-1100)#context *
```

Specifies the type of connection to which this rule applies. The connection type can be *netconf* (Network Configuration Protocol), *cli* (Command Line Interface), or *xml* (Extensible Markup Language). We recommend that you enter an asterisk '*', which indicates that the command applies to all connection types.

Step 9 **namespace** *namespace*

Example:

```
sysadmin-vm:0_RP0#(config-datarule-1100)#namespace *
```

Enters asterisk '*' to indicate that the data rule is applicable to all namespace values.

Step 10 Use the **commit** or **end** command.

commit—Saves the configuration changes and remains within the configuration session.

end—Prompts user to take one of these actions:

- **Yes**—Saves configuration changes and exits the configuration session.
- **No**—Exits the configuration session without committing the configuration changes.
- **Cancel**—Remains in the configuration session, without committing the configuration changes.

Change Disaster-Recovery Username and Password

When you define the root-system username and password initially after starting NCS 1004, you can use the same username and password for disaster recovery in the System Admin mode. However, you can also change the username and password.

The disaster-recovery username and password are useful in these scenarios:

- Access the system when the AAA database, which is the default source for authentication in System Admin, is corrupted.
- Access the system through the management port, when the System Admin console is not working.
- Create new users by accessing the System Admin using the disaster-recovery username and password, when the regular username and password are forgotten.

Note At a time, you can configure only one disaster-recovery username and password.

Before you begin

Create a user profile. For details, see Create a User Profile, on page 1.

Procedure

Step 1 **admin**

Example:

```
RP/0/RP0/CPU0:ios# admin
```

Enters System Admin EXEC mode.

Step 2 **config**

Example:

```
sysadmin-vm:0_RP0# config
```

Enters System Admin config mode.

Step 3 **aaa disaster-recovery username** *username* **password** *password*

Example:

```
sysadmin-vm:0_RP0#(config)#aaa disaster-recovery username us1 password pwd1
```

Specifies the disaster-recovery username and the password. You must select an existing user as the disaster-recovery user.

In the example, 'us1' is selected as the disaster-recovery user and assigned the password as 'pwd1'. You can enter the password as a plaintext or md5 digest string.

When you must make use of the disaster recovery username, you need to enter it as *username***@localhost**.

Step 4 Use the **commit** or **end** command.

commit-Saves the configuration changes and remains within the configuration session.

end-Prompts user to take one of these actions:

- **Yes**-Saves configuration changes and exits the configuration session.
- **No**-Exits the configuration session without committing the configuration changes.
- **Cancel**-Remains in the configuration session, without committing the configuration changes.