Manage Users

This chapter describes the different types of users in Cisco NCS 2000 SVO. This chapter also describes the tasks to manage users.

Table 1: Feature History

Feature Name	Release Information	Feature Description
View Users	Cisco NCS 2000 Release 12.2	This feature allows an admin or superuser to view the details of users who have successfully logged into SVO.

User Groups

User groups are system-defined. The users in each group have certain levels of privileges and permissions and can perform a defined set of tasks.

The system-defined user groups are:

- Superuser—A user assigned to this group has special permissions to perform any action on the system. The superuser has access to the SVO Admin Plane and the SSH interface. Superusers can create, modify, and delete users. Only one superuser can be created.
- Admin—A user assigned to this group has read and write permissions. An admin can create, modify, and delete users.
- Editor—A user assigned to this group has limited read and write permissions. An editor does not have permissions to create and manage users.

- Viewer—A user assigned to this group has only read permission. A viewer cannot perform any action on the device.

Role-Based Access Control

Table 2: Feature History

Feature Name	Release Information	Feature Description
Role-Based Access Control	Cisco NCS 2000 Release 12.3	The Role-Based Access Control (RBAC) feature allows the users belonging to the Editor, Admin, and Viewer groups to access and operate certain SVO panes.

Role-Based Access Control (RBAC) restricts or authorizes system access for users by setting permissions and privileges. Users are assigned roles depending on the resources to which they need access.

RBAC allows users belonging to the Editor, Viewer, and Admin groups to access and operate certain SVO panes as detailed below:

- **Viewer group**: You can
  - Refresh a page or pane.
  - Export reports.
  - View options in panes.

Note However, the changes cannot be applied.

- **Viewer and Editor groups**: You can perform all operations except for viewing the **Users & Access** menu when the hamburger icon at the top-left of the page is clicked.
- **Viewer and Admin groups**: Access is restricted based on the instance type. In the TXP instance:
  - For the **Node Configuration** > **Optical Configuration** menu, the **Connection Verification**, **OTDR**, **Internal Patch Cords**, **OSC**, **Optical Degree**, **Optical Degree Power Monitoring**, **Span Loss**, **Expected Input Power**, and **Fiber Attributes** tabs are not accessible.
  - The **Node Configuration** > **APC** tab is not accessible.
  - The **Provisioning** > **Raman Amplifier** tab in the card view is not accessible.

External Authentication Users for SVO

In SVO, the following users are created to manage SVO provisioning activities:

- Local users (local authentication)—Specifies users created to manage SVO instances.

- External users (external authentication)—Specifies users created on the external authentication servers.

The local and external users are mutually exclusive, for example, if there is a local user as **user1** configured on SVO, then another external user with same name **user1** is not allowed to login.

The RADIUS or TACACS user who is created on the RADIUS or TACACAS server should have the *Cisco-AVPair* reply attribute that is configured for each user on SVO to authenticate.

The following table lists the server attribute mapped to user privileges supported on SVO.

Table 3:

Cisco-AVPair Reply Attribute	Value mapped in RADIUS Server	Value mapped in TACACAS Server
shell:priv-lvl=	3	3
shell:priv-lvl=	0	0
shell:priv-lvl=	1	1

Create Users

Use this task to create users. Only an admin or superuser creates new users. Superusers cannot be created using this task.

Before you begin

Log into the SVO Web Interface

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **Users & Access**.

Step 2 In the **Users & Access** tab, click **Create**.

The Create User dialog box appears.

Step 3 Enter the following details.

a) **User Name**—Type the user name. The user name must be a minimum of six and a maximum of 40 characters. It includes alphanumeric (a-z, A-Z, 0-9) characters and the allowed special characters are @, " - " (hyphen), and " . " (dot).

b) **Password**—Enter the password which will be used by the user while logging into the system. The password must be a combination of alphanumeric (a-z, A-Z, 0-9) and special (+, #,%) characters. The minimum number of characters in the password is eight and the maximum number is 127. The password must not contain the user name.

c) **Retype Password**—Retype the password.

d) **Full Name**—Enter the full name of the user.

e) **Expiry Time (days)**—Enter the time period in days before which the user needs to change the password. For example, if the user has set the expiry time to be 20 days, the user must change the password before 20 days are over.

The user is automatically moved to the Change Password group after the time period in the Expiry Time field elapses. The user must change the password before performing any other action.

f) **Warning Before Expiry (days)**—Enter the number of days the user is warned of the expiry of the password.
g) **Max Retry Number**—Enter the number of maximum retries for the user. The user is logged out of the system if the password is incorrectly entered after this number of attempts is reached.
h) **Group**—Select the group from the drop-down list. The available options are admin, editor, and viewer.

Step 4 Click **Create**.

The new user is added to the list.

Change Password

Use this task to change password for the user. Only an admin or superuser can change the password.

Before you begin

Log into the SVO Web Interface

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **Users & Access**.

Step 2 In the **Users & Access** tab, check the check box corresponding to the user you want to change the password, and click **Reset Password**.

The **reset** *Username* **password** dialog box appears.

Step 3 Enter the new password in the **New Password** field.

The password must be a combination of alphanumeric (a-z, A-Z, 0-9) and special (+, #,%) characters. The minimum number of characters in the password is eight and the maximum is 127. The password must not contain the user name.

Step 4 Retype the same password in the **Retype Password** field.

Step 5 Click **Reset Password**.

A confirmation message appears.

Step 6 Click **OK**.

View Users

Use this task to view users. Only an admin or superuser can view the activities of users.

Before you begin

Log into the SVO Web Interface

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **Users & Access**.

Step 2 In the **Users & Access** tab, click **Login**.

The **Last Successful Logins** dialog box appears.

Step 3 View the displayed details in the **Last Successful Logins** tab.

- **Login ID**—Displays the session ID.
- **User**—Displays the user name.
- **Last Login Date**—Displays the date and time on which the user had last logged in.
- **Last Logout Date**—Displays the date and time on which the user had last logged out.
- **Interface**—Displays the interface type that the user used to last log in. The interface types are web UI, CLI, NETCONF, and Unknown.

Delete Users

Use this task to delete users. Only an admin or superuser can delete users.

Note Superusers cannot be deleted.

Before you begin

Log into the SVO Web Interface

Procedure

Step 1 Click the hamburger icon at the top-left of the page, and select **Users & Access**.

Step 2 In the **Users & Access** tab, check the check box corresponding to the user you want to delete and click **Delete User**.

A confirmation message appears.

Step 3 Click **Yes**.

Modify User Settings

Use this task to change the user settings.

Before you begin

Log into the SVO Web Interface

Procedure

Step 1 Click the User icon at the top-right of the page, and select **Users & Access**.

The **User Login Details** and **User Configurations** tabs appear.

Step 2 View the displayed details in the User Login Details tab.

- **Last Login Date**—The date on which the user had last logged in.
- **Last Logout Date**—The date on which the user had last logged out.
- **Last Login Interface**—The interface used for last login.
- **Number of Failed Login Attempts**—The number of times the user has had failed login attempts before the current login.
- **Last Failed Login Message**—The reason for the last login failure.
- **Warning Message**—The message displays the number of days remaining for the expiry of the current password.

Step 3 To change the user attributes, go to the **User Configurations** tab. The following attributes can be changed by a superuser or an admin user except the user name.

- **User Name**—Displays the user name.
- **Group**—The original group a user was created in. An admin or a superuser can change the group to which a user belongs. Also, when a user has reached the set **Expire Time**, the user is moved automatically to the Change Password user group. The user must change the password before performing any other action on the system.
- **Full Name**—Displays the full name of the user.
- **Max Retry Number**—The number of times the user can attempt to login. The default value is 3.
- **Expire Time (days)**—The number of days the current password is valid. The default value is 180.
- **Warning Before Expire (days)**—The user is warned about the number of days remaining before the expiry of the current password. The value entered for this field must be lesser than the value entered for the **Expire Time** field. The default value is 14.

Step 4 Click **Apply**.

A confirmation message appears.

Step 5 Click **Yes**.