Manage VOS Users

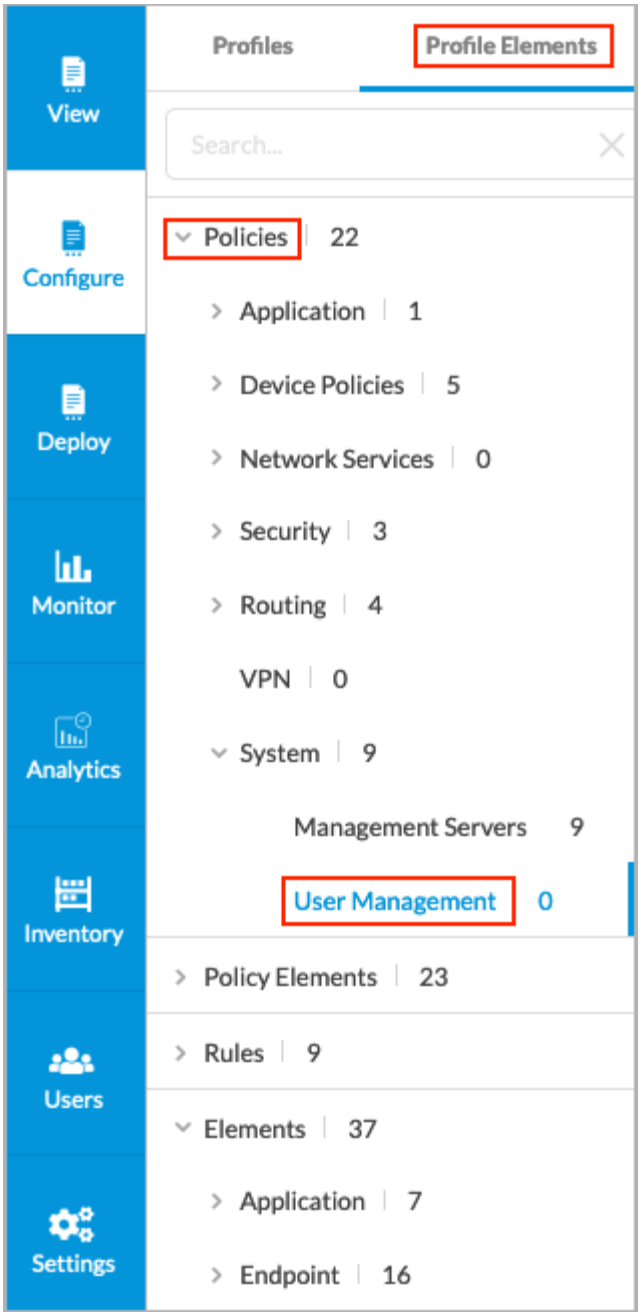
For supported software information, click here.

The User Management screen allows you to create user management policies, and add and edit Versa Operating System™ (VOS™) device users from Concerto. You can manage users from Concerto by creating system users (admin and operator) and defining access permissions for these users. A system user can do the following:

- Log in to the shell of a Versa VOS device OS and to the CLI. When logging in to the shell, the system user is placed into a Bash shell. When logging in to the CLI, the system user is placed at the CLI prompt.
- Assume the role of an administrator or operator. As an administrator, a system user can modify any part of configuration, while as an operator, the system user can only view the configuration.
- SSH to port 22 and port 2024. When using port 2024, the user is always placed in the CLI, regardless of the login that is configured. System users can launch a shell from CLI.
- Use password-less authentication on VOS devices, using the SSH public key. Password-less authentication enhances security, protecting the system against the brute force password attacks of SSH.
- Configure multiple SSH keys.

Create a User Management Policy

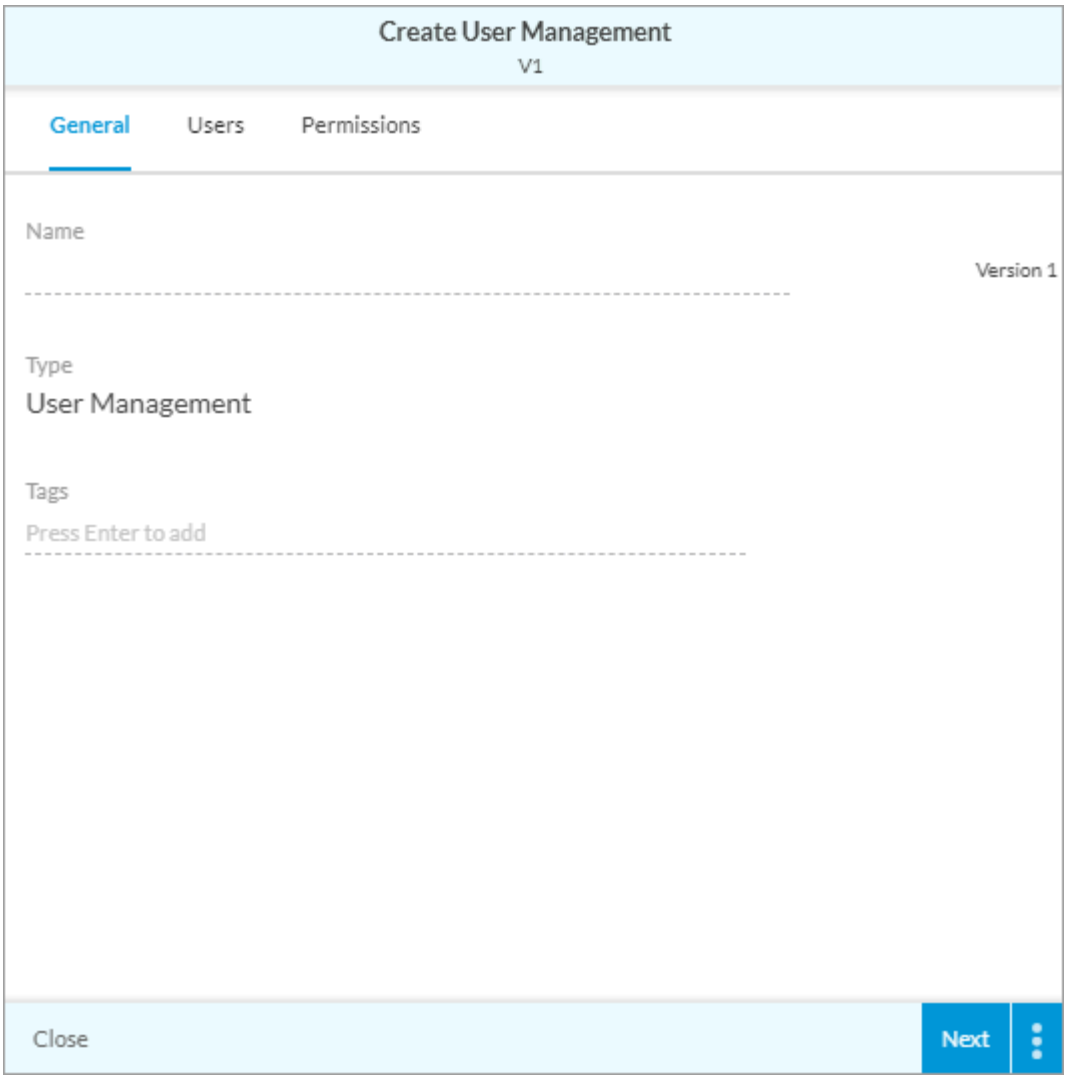
1. Go to Configure > Profile Elements > System > User Management.



The User Management screen displays.

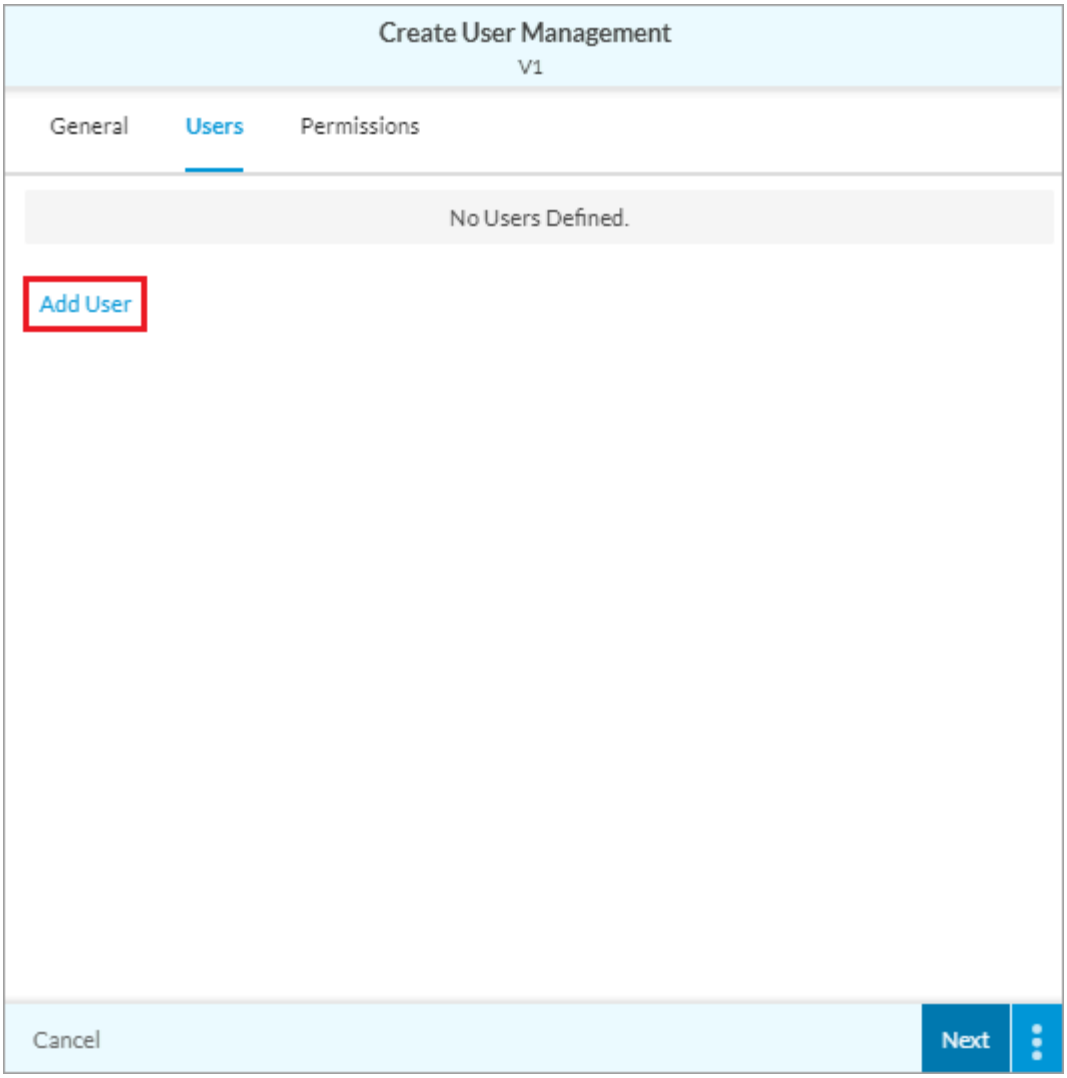
2. Click + User Management to create a user management policy. The Create User Management screen displays,

and the General tab is selected. Enter information for the following fields.

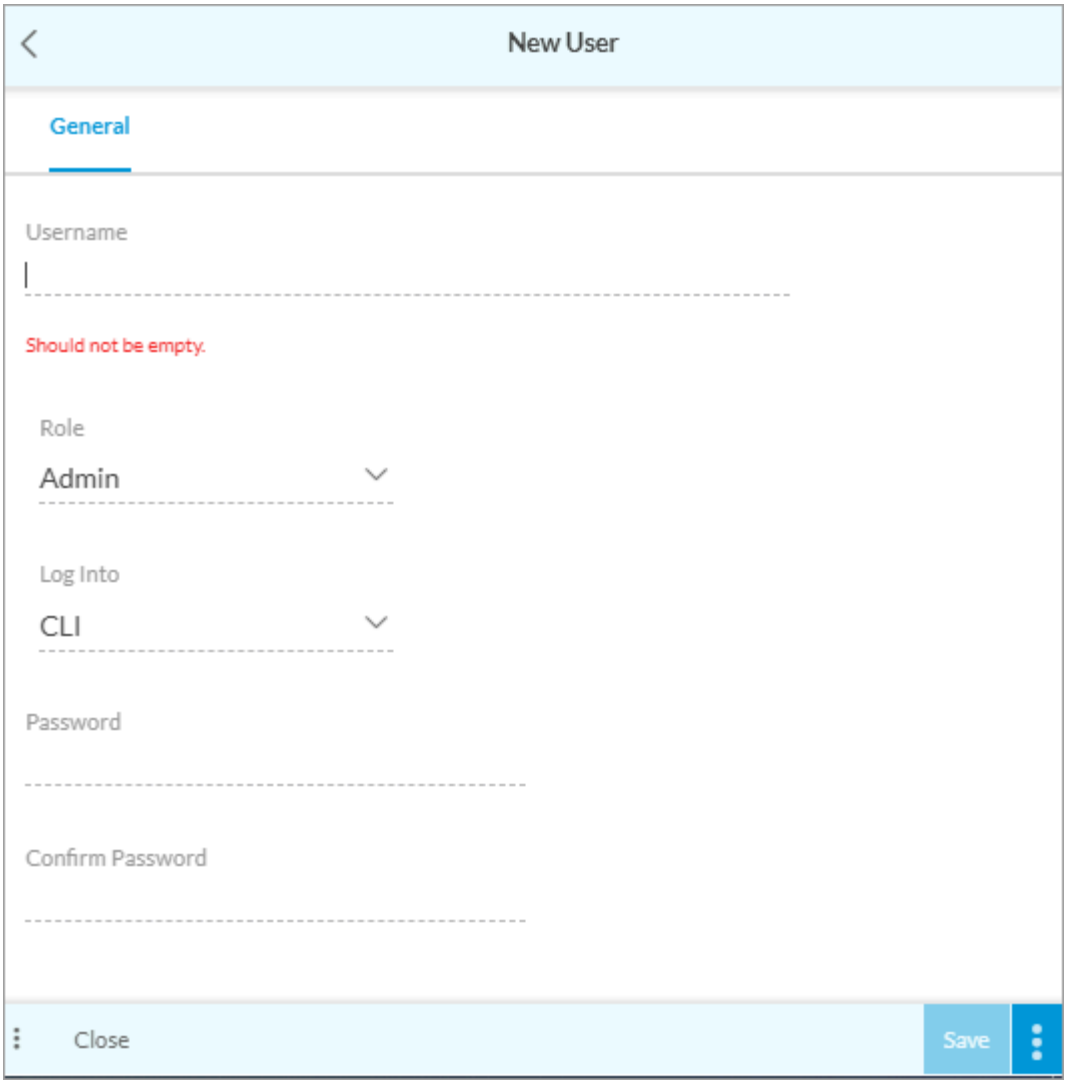


Field	Description
Name	Enter a name for the user management policy.
Tags	(Optional) Enter one or more tags. A tag is free-text alphanumeric descriptor without white space or special characters. You can create multiple tags for the same object. Tags allow you to locate a policy when you perform a filtered search of all policies.

3. Select the User tab, and then click Add User.

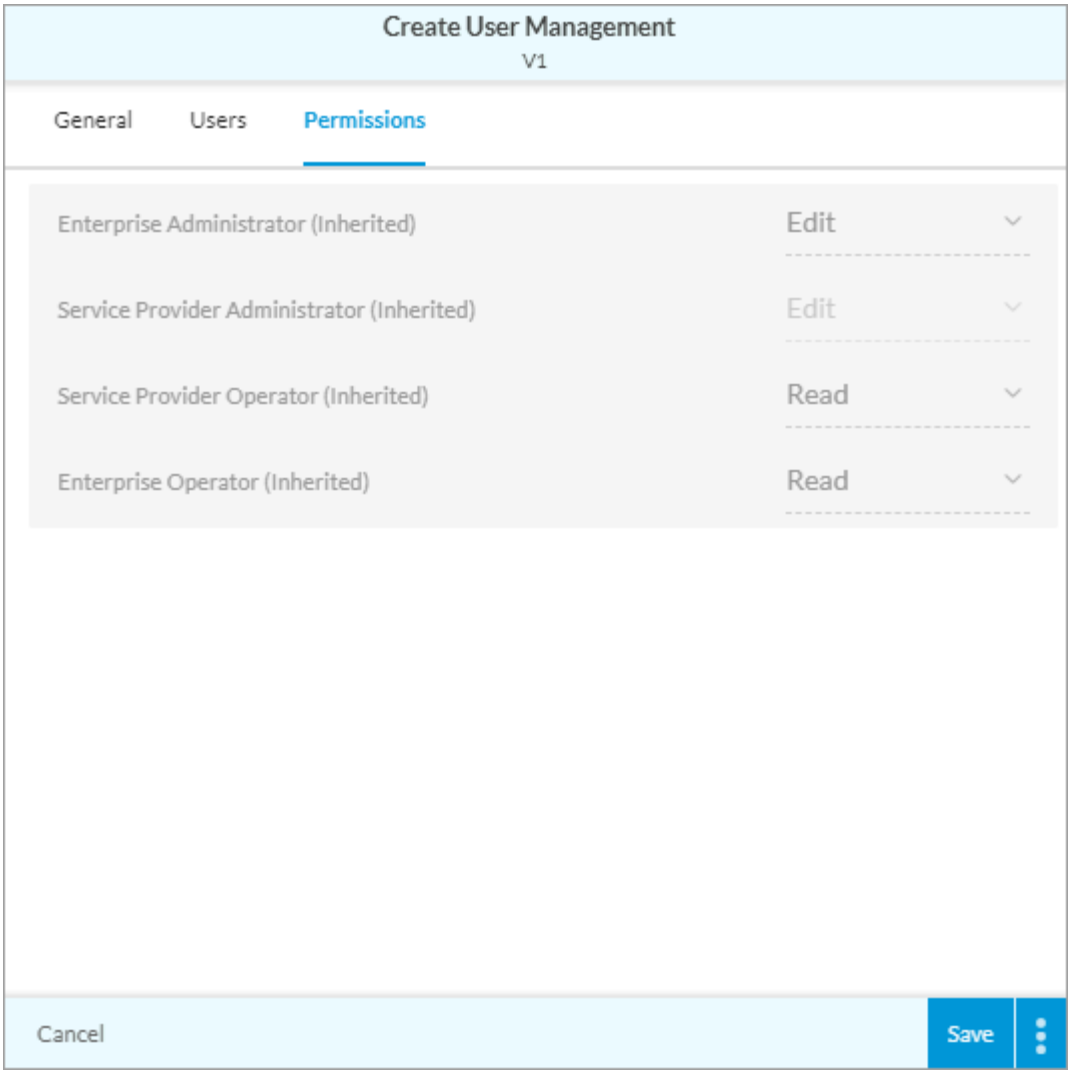


The New User screen displays. Enter information for the following fields.



Field	Description
Username	Enter a name for the VOS user. *Range*: 2 through 31 characters
Role	Select the user role: ◦ Admin—Super user with sudo privileges who can connect via SSH or to the CLI to the device on port 22 and port 2024. An admin user can modify any part of configuration. This is the default. ◦ Operator—Console user who can log in to only to the CLI and only using the physical or virtual console. *Default*: Admin
Log Into	Select the login method: ◦ CLI ◦ Shell Note that if Role is Admin, The CLI and Shell options are displayed. For Operator, only the CLI option is displayed.
Password	Enter a password for the user. You can also use a parameterized variable as password.
Confirm Password	Confirm the password.

4. Click Save.
5. Select the Permissions tab and revise the permissions, if desired. The options are Edit, Read, and Hide.



6. Click Save.

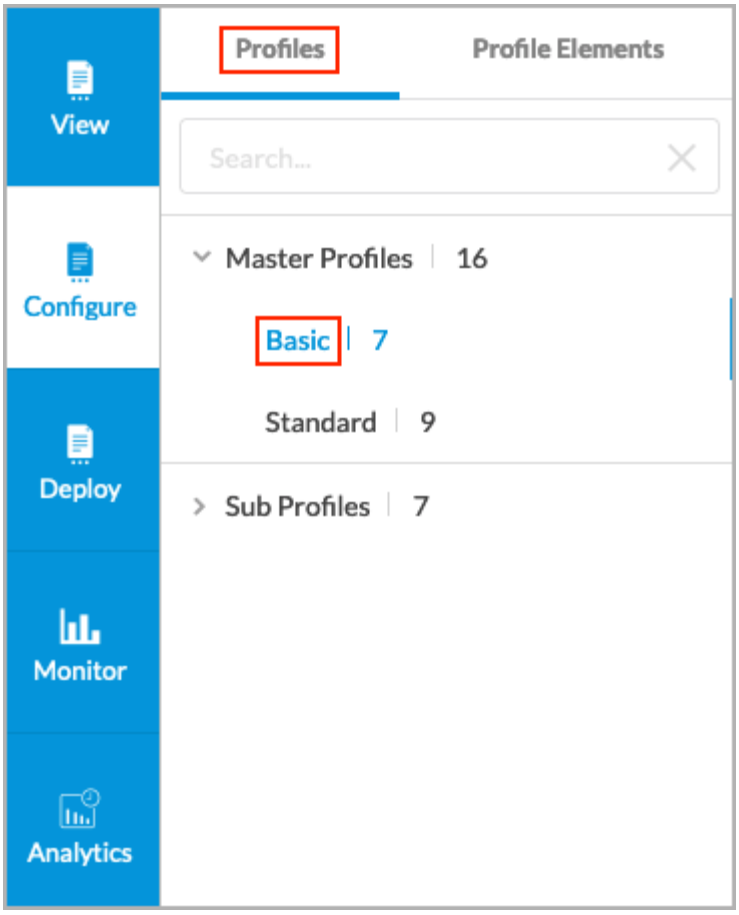
You can also add user management policies from a basic master profile, standard master profile, or a system type subprofile. For more information, see Associate a User Management Policy with a Master Profile.

Associate a User Management Policy with a Master Profile

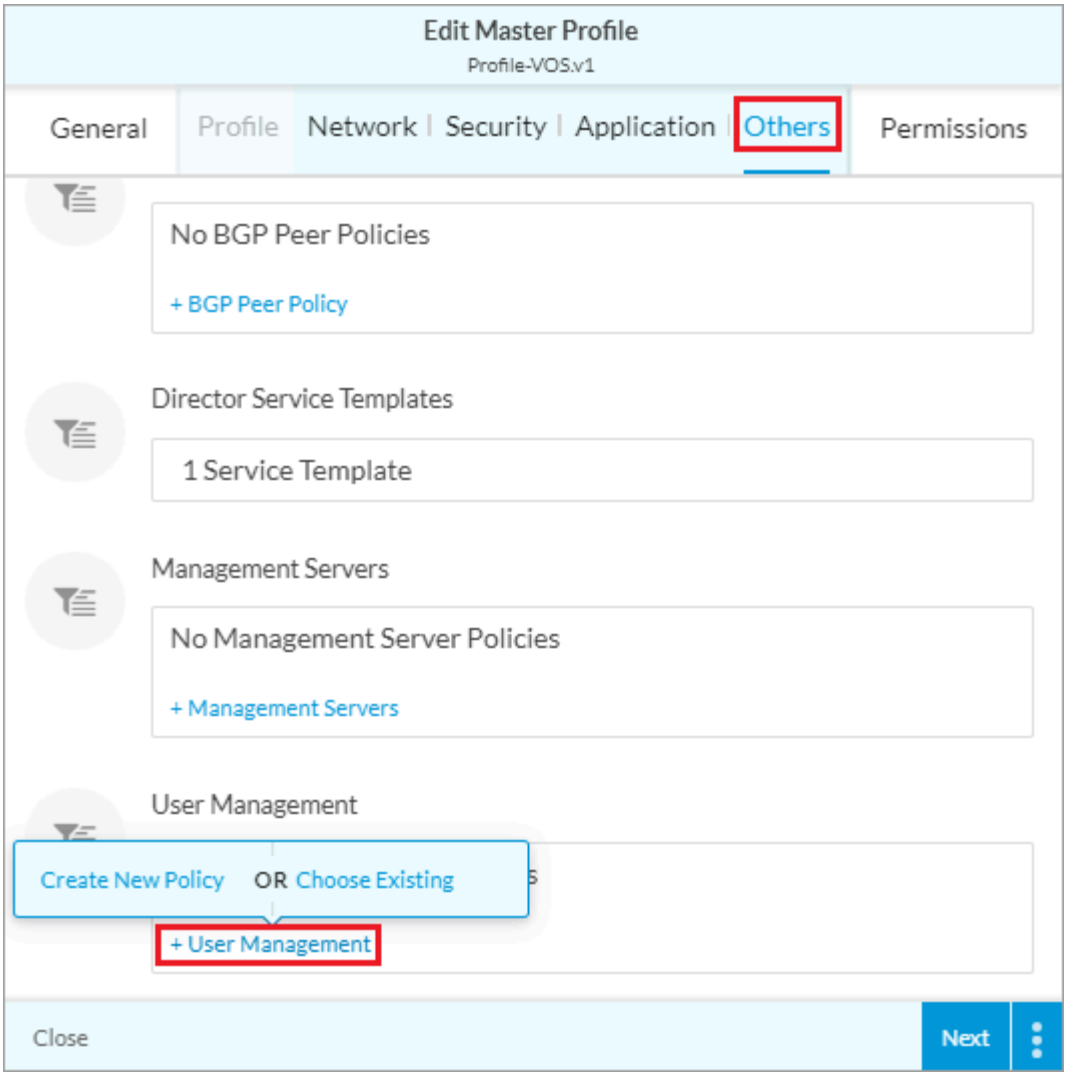
You can associate a user management policies with a basic master profile or standard master profile.

Associate a User Management Policy with a Basic Master Profile

1. Select Configure in the left menu bar on the Concerto tenant's home screen. Then select Secure SD-WAN > Profiles.



2. Select Master Profiles > Basic, and then click the basic master profile to associate with the user management policy. The Edit Master Profile screen displays. For more information, see Configure Profiles.
3. Select the Others tab and then click + User Management.



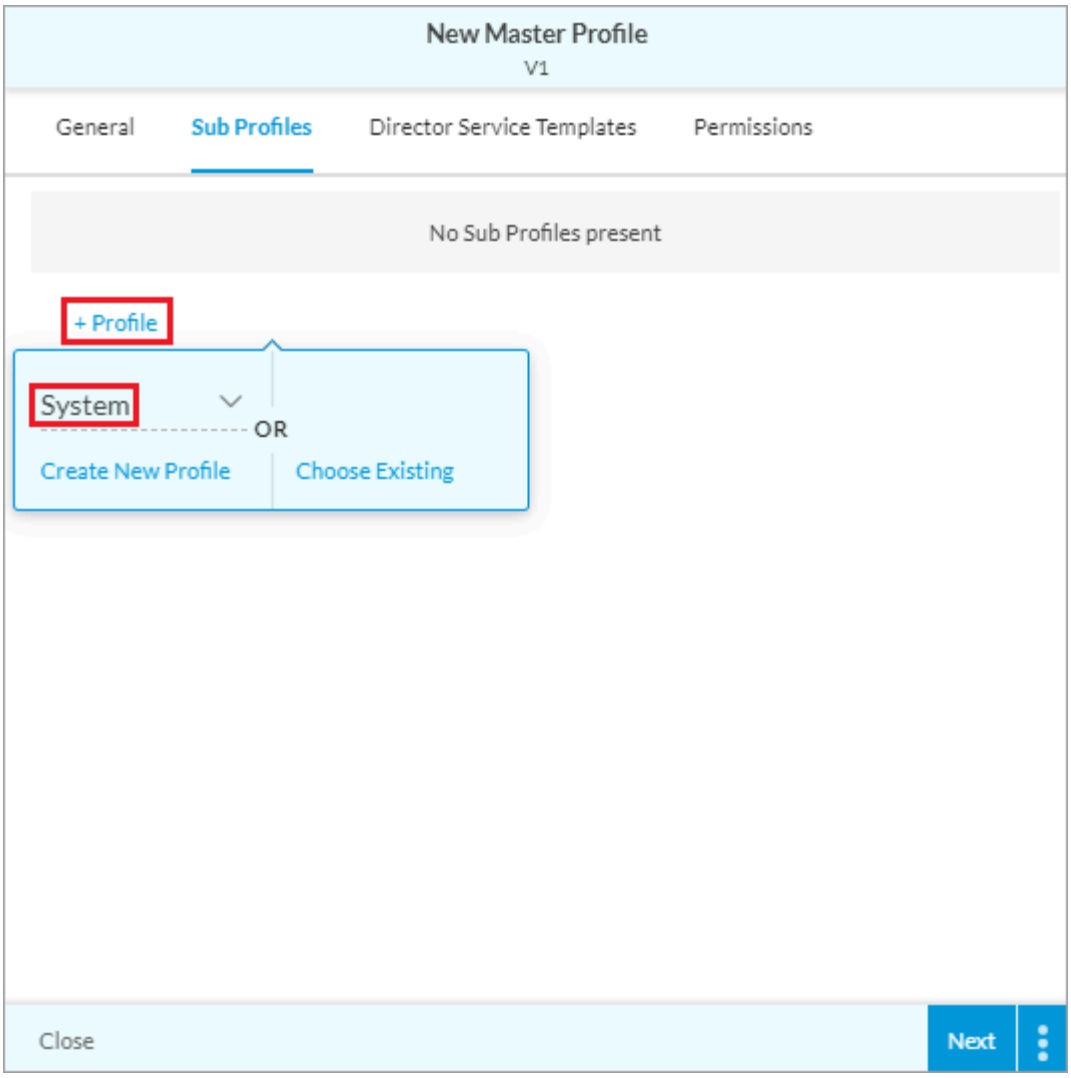
4. To associate an existing user management policy with the basic master profile, click Choose Existing and then select the user management policy.
5. To add a user manager policy, click Create New Policy. The Create User Management screen displays. For more information, see Create a User Management Policy, above.
6. Click Next and then save the basic master profile.

Associate a User Management Policy with a Standard Master Profile

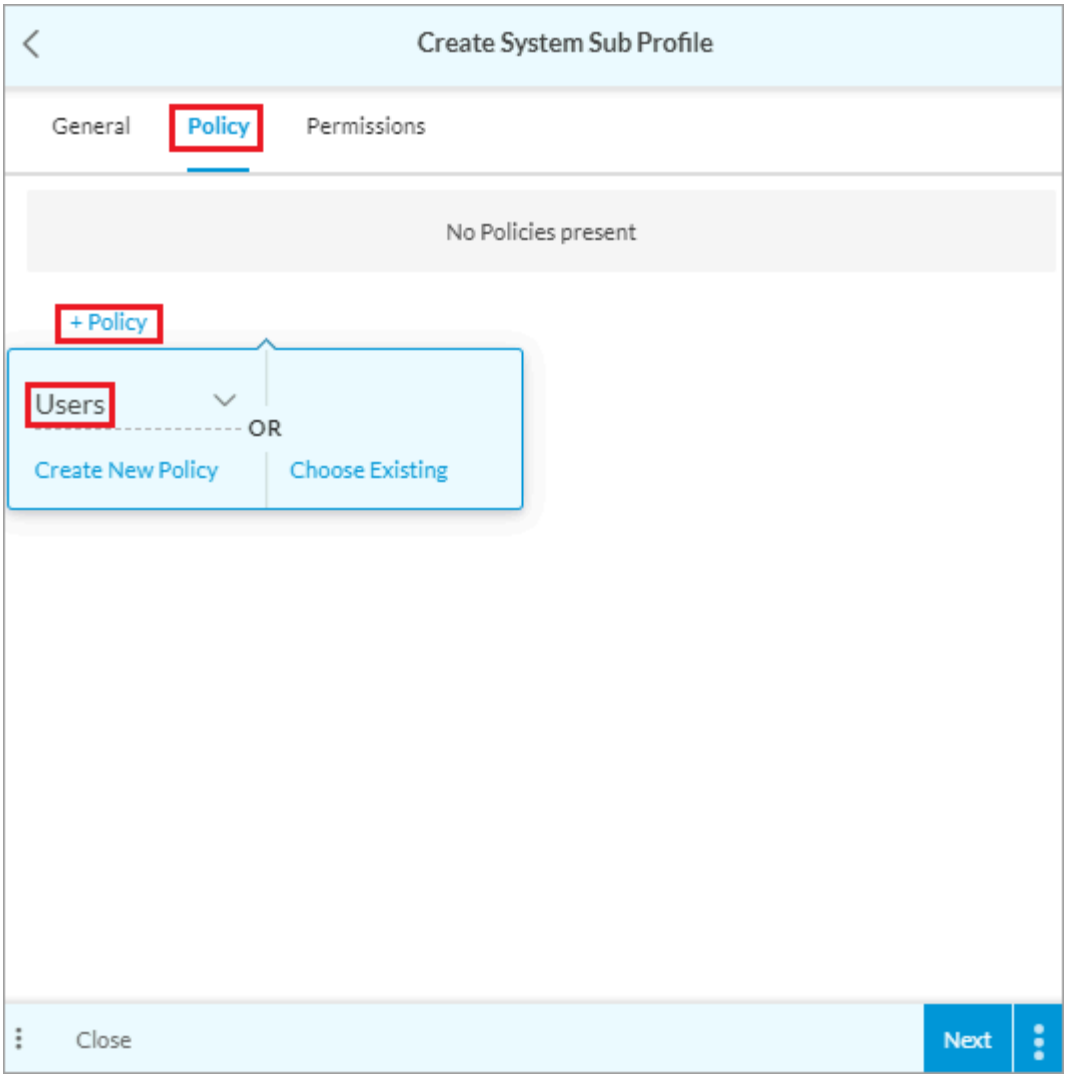
You associate a user management policy with a standard master profile by selecting or adding a system type subprofile that uses your user management policy.

1. Select Configure in the left menu bar on the Concerto tenant's home screen. Then select Secure SD-WAN > Profiles.
2. Select Master Profiles > Standard, and then click + Standard to create a standard master profile or select an existing standard master profile to associate with the user management policy. For more information, see Configure Profiles.

3. The New/Edit Master Profile screen displays. Select the Subprofiles tab.



4. Click + Profile, select System, and then click Create New Profile. The Create System Subprofile screen displays.
5. Select the Policy tab and then click + Policy.



6. Select Users in the drop-down list.
7. To associate an existing user management policy with the standard master profile, click Choose Existing and then select the user management policy.
8. To add a new user management policy, click Create New Policy. The Create User Management screen displays. For more information, see Create a User Management Policy, above.
9. Click Next and then save the subprofile.
10. Save the standard master profile.

Supported Software Information

Releases 11.3.1 and later support all content described in this article.

Additional Information

Configure Profiles