Manage Users

For supported software information, click here.

The Users screen displays users and their roles. Two roles are available for service providers—Service Provider Administrator and Service Provider Operator—and two roles are available for enterprises—Enterprise Administrator and Enterprise Operator.

In Releases 10.2.1 and later, the Users screen contains the Active column to show which users are currently active.

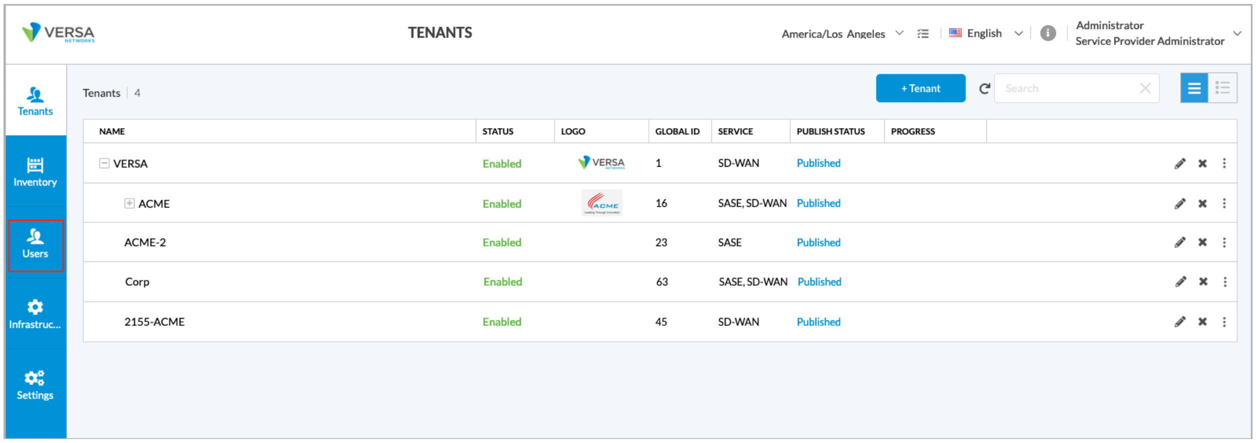
If a user has an account on an external server, such as an LDAP, a RADIUS, a TACACS+, or other server, the External User column displays Yes in the row for that user.

Create a New User

You can create users at the top-level Service Provider tenant or at the Enterprise tenant level.

To create users:

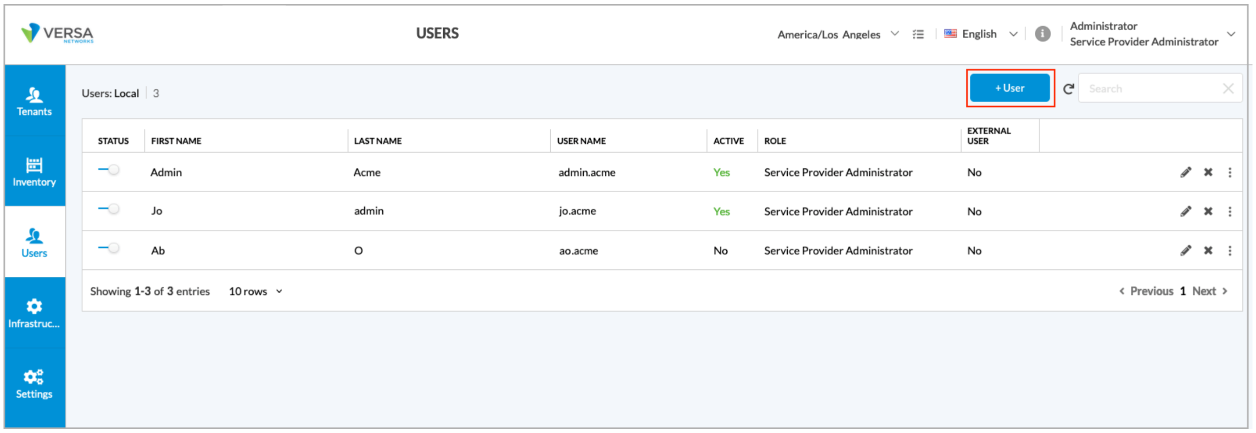
1. If you are a Service Provider administrator and want to create a new top-level Service Provider user:
   a. Log in as Service Provider administrator. The Tenants screen displays.



Tenants | 4

NAME	STATUS	LOGO	GLOBAL ID	SERVICE	PUBLISH STATUS	PROGRESS
⊟ VERSA	Enabled	VERSA	1	SD-WAN	Published	
⊞ ACME	Enabled	ACME	16	SASE, SD-WAN	Published	
ACME-2	Enabled		23	SASE	Published	
Corp	Enabled		63	SASE, SD-WAN	Published	
2155-ACME	Enabled		45	SD-WAN	Published	

   b. Click the Users lifecycle in the left navigation bar. The Users home screen displays all current users.



STATUS	FIRST NAME	LAST NAME	USER NAME	ACTIVE	ROLE	EXTERNAL USER
	Admin	Acme	admin.acme	Yes	Service Provider Administrator	No
	Jo	admin	jo.acme	Yes	Service Provider Administrator	No
	Ab	O	ao.acme	No	Service Provider Administrator	No

Showing 1-3 of 3 entries 10 rows

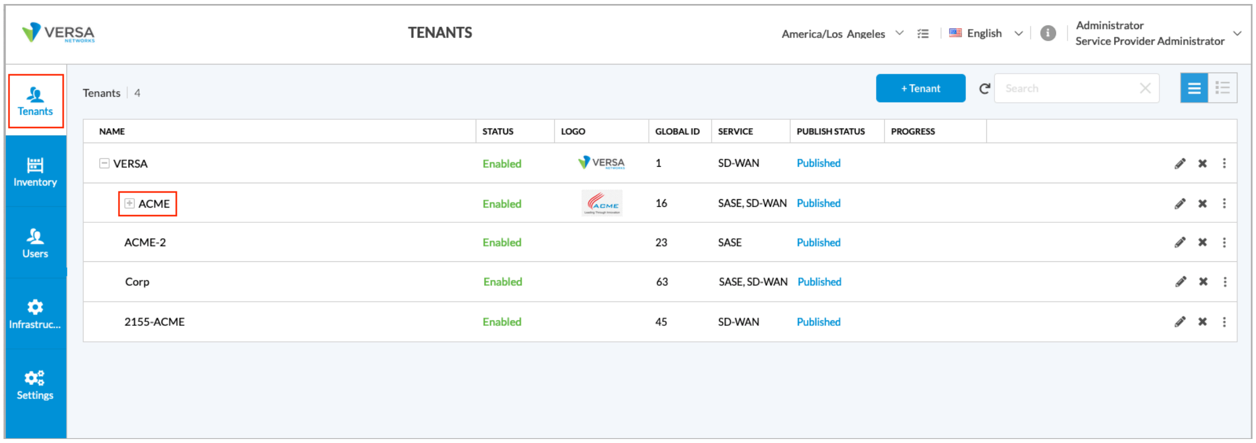
< Previous 1 Next >

c. Click the + User button. The Create User screen displays.

d. Continue with Step 5.

2. If you are a Service Provider administrator and want to create a new user for a child tenant:

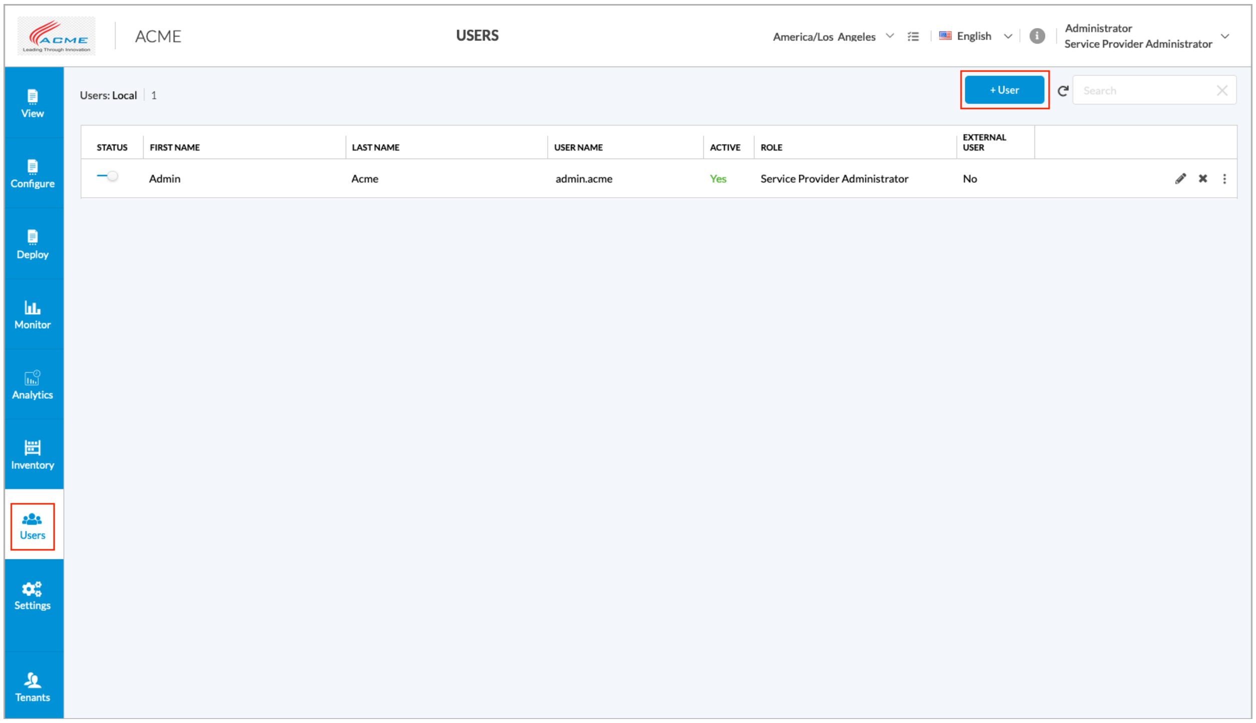
a. In the top-level Service Provider screen, click the Tenant lifecycle in the left navigation bar. The Tenants screen displays all current tenants.



NAME	STATUS	LOGO	GLOBAL ID	SERVICE	PUBLISH STATUS	PROGRESS
⊟ VERSA	Enabled	VERSA	1	SD-WAN	Published	
⊞ ACME	Enabled	ACME	16	SASE, SD-WAN	Published	
ACME-2	Enabled		23	SASE	Published	
Corp	Enabled		63	SASE, SD-WAN	Published	
2155-ACME	Enabled		45	SD-WAN	Published	

b. Click the name of the tenant to which you want to add a new user or users (ACME in the above example). The landing page for the tenant displays. Note that the landing page for each tenant is configured when the tenant is created, so it may differ from tenant to tenant.

c. Select the Users lifecycle in the left navigation bar. The Users screen for the tenant displays all currently configured users.



STATUS	FIRST NAME	LAST NAME	USER NAME	ACTIVE	ROLE	EXTERNAL USER
	Admin	Acme	admin.acme	Yes	Service Provider Administrator	No

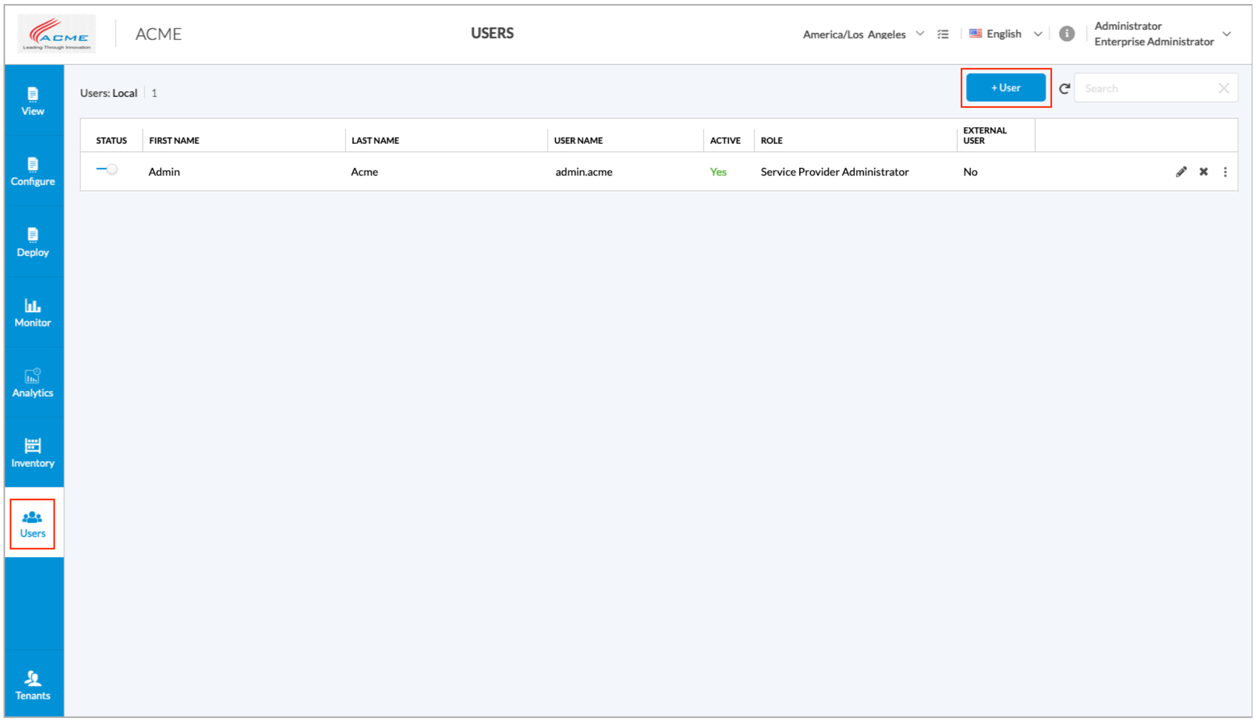
   d. Click the +User button. The Create User screen displays.

   e. Continue with Step 5.

3. If you are an Enterprise administrator and want to create a new Enterprise user:

   a. Log in as Enterprise Administrator. The landing page for the tenant displays. Note that the landing page for each tenant is configured when the tenant is created, so it may differ from tenant to tenant.

   b. Select the Users lifecycle in the left navigation bar. The Users screen for the tenant displays all currently configured users.



STATUS	FIRST NAME	LAST NAME	USER NAME	ACTIVE	ROLE	EXTERNAL USER
	Admin	Acme	admin.acme	Yes	Service Provider Administrator	No

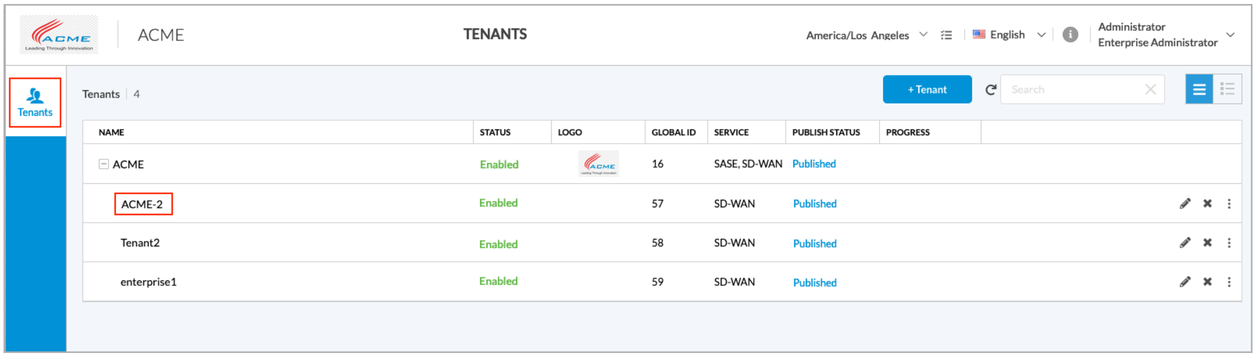
c. Click the +User button. The Create User screen displays.

d. Continue with Step 5.

4. If you are an Enterprise administrator and want to create a new Enterprise user for a child tenant:

    a. Log in as Enterprise Administrator. The landing page for the tenant displays. Note that the landing page for each tenant is configured when the tenant is created, so it may differ from tenant to tenant.

    b. Select Tenant lifecycle in the left navigation panel. The Enterprise Tenants screen displays the tenant and its child tenants.



NAME	STATUS	LOGO	GLOBAL ID	SERVICE	PUBLISH STATUS	PROGRESS
ACME	Enabled		16	SASE, SD-WAN	Published	
ACME-2	Enabled		57	SD-WAN	Published	
Tenant2	Enabled		58	SD-WAN	Published	
enterprise1	Enabled		59	SD-WAN	Published	

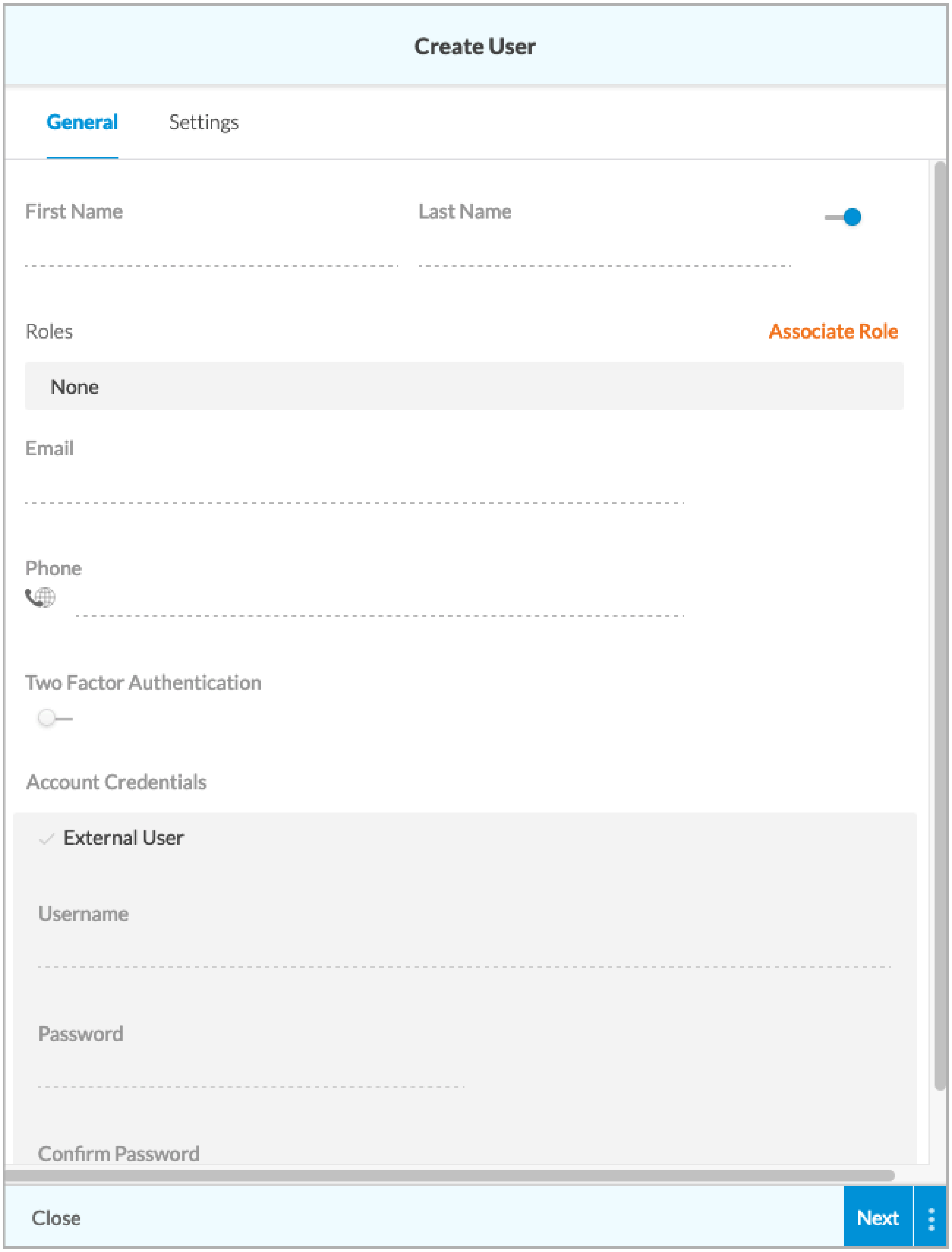
    c. Click the name of the tenant to which you want to add a new user or users.

    d. Select the Users lifecycle in the left navigation bar. The Users screen for the tenant displays all currently configured users.

    e. Click the +User button. The Create User screen displays.

    f. Continue with Step 5.

5. In the User lifecycle screen, click + User. In the Create User screen, enter information for the following fields.



Create User

General Settings

First Name

Last Name

Roles

Associate Role

None

Email

Phone

Two Factor Authentication

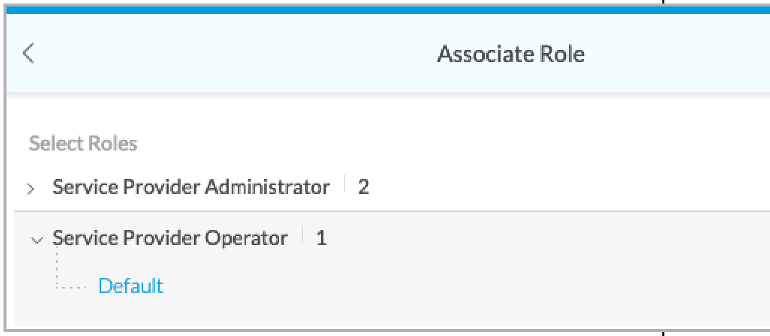
Account Credentials

✓ External User

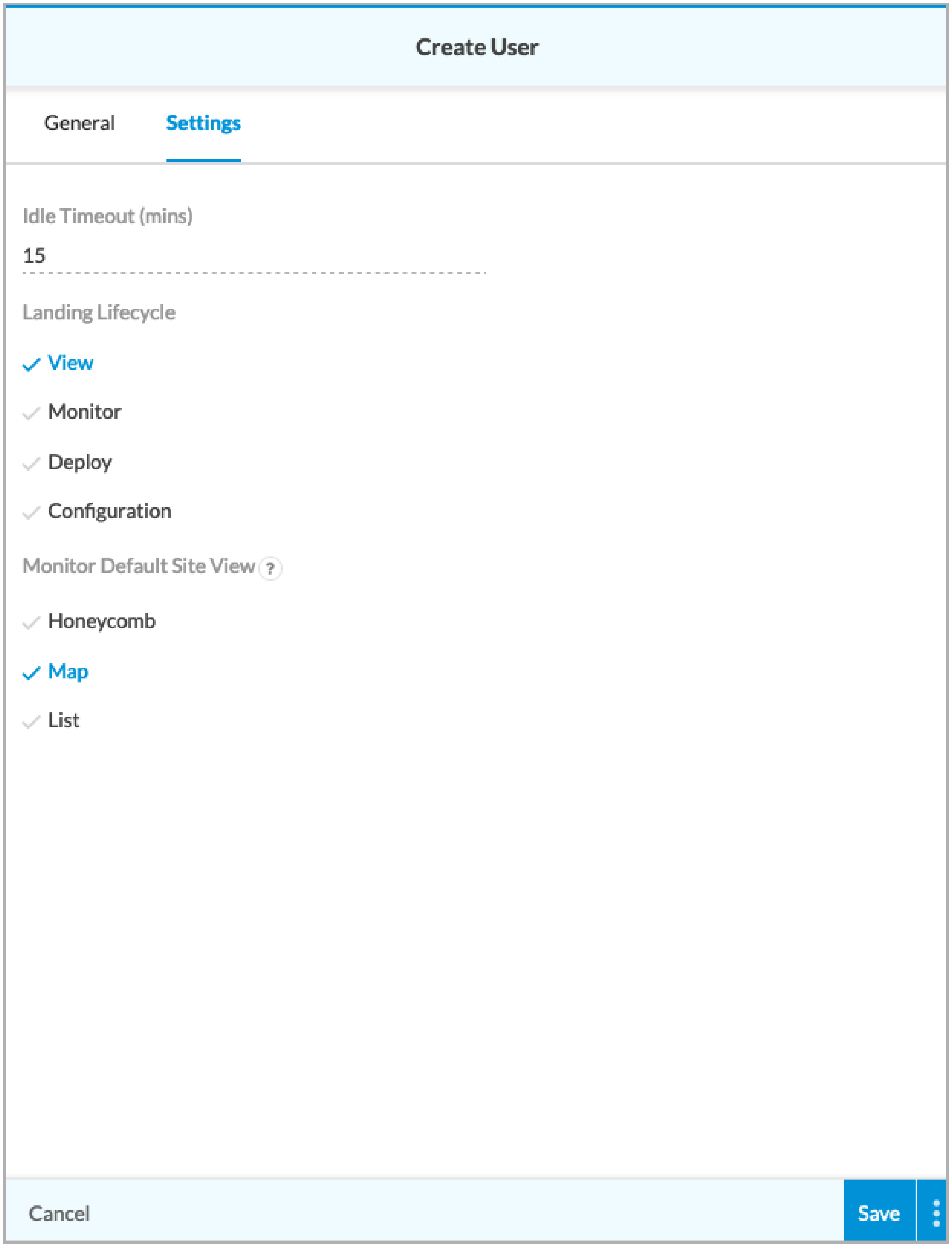
Username

Password

Confirm Password

Field	Description
First name (Required)	Enter the user's first name.
Last name (Required)	Enter the user's last name. The slide bar to the right indicates that the user's status is enabled. Click the slide bar to disable the user's status.
Role (Required)	Click Associate Role. The Associate Role screen displays. Choose a role for the new user, and then click Save. The example below shows that a default service provider operator role has been selected.  Associate Role Select Roles Service Provider Administrator 2 Service Provider Operator 1 Default
Email (Required)	Enter the user's email address.
Phone	Enter the user's phone number. This is required when you enable two-factor authorization.
Two-Factor Authentication	(For Releases 10.2.1 and later.) Click the slide bar so that it is blue to enable two-factor authentication.
Account Credentials (Group of Fields)	
◦ External User	Click if the user is an external user.
◦ Username (Required)	Enter the user's username.
◦ Password	Enter the user's password for an internal user. You cannot change the password for an external user.
◦ Confirm password	For internal users only, enter the user's password again.

6. Select the Settings tab, or click Next, and enter information for the following fields.



Idle Timeout (mins)

15

Landing Lifecycle

✓ View

Monitor

Deploy

Configuration

Monitor Default Site View ?

Honeycomb

✓ Map

List

Field	Description
Idle Timeout	Enter how long, in minutes, the user can be idle before being logged out.
Landing Lifecycle	Choose the lifecycle screen to display when the user first accesses Concerto orchestrator.
Monitor Default Site View	Choose which view to display when the user first accesses Concerto orchestrator.

7. Click Save.

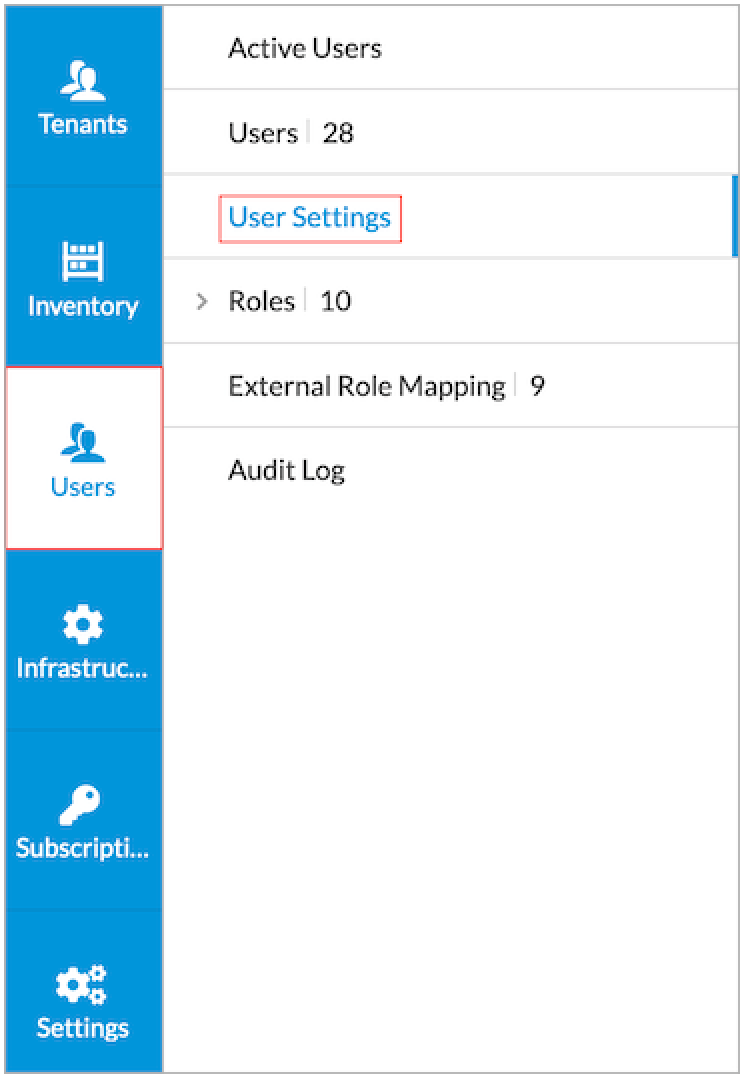
Configure User Settings

For Releases 11.4.1 and later.

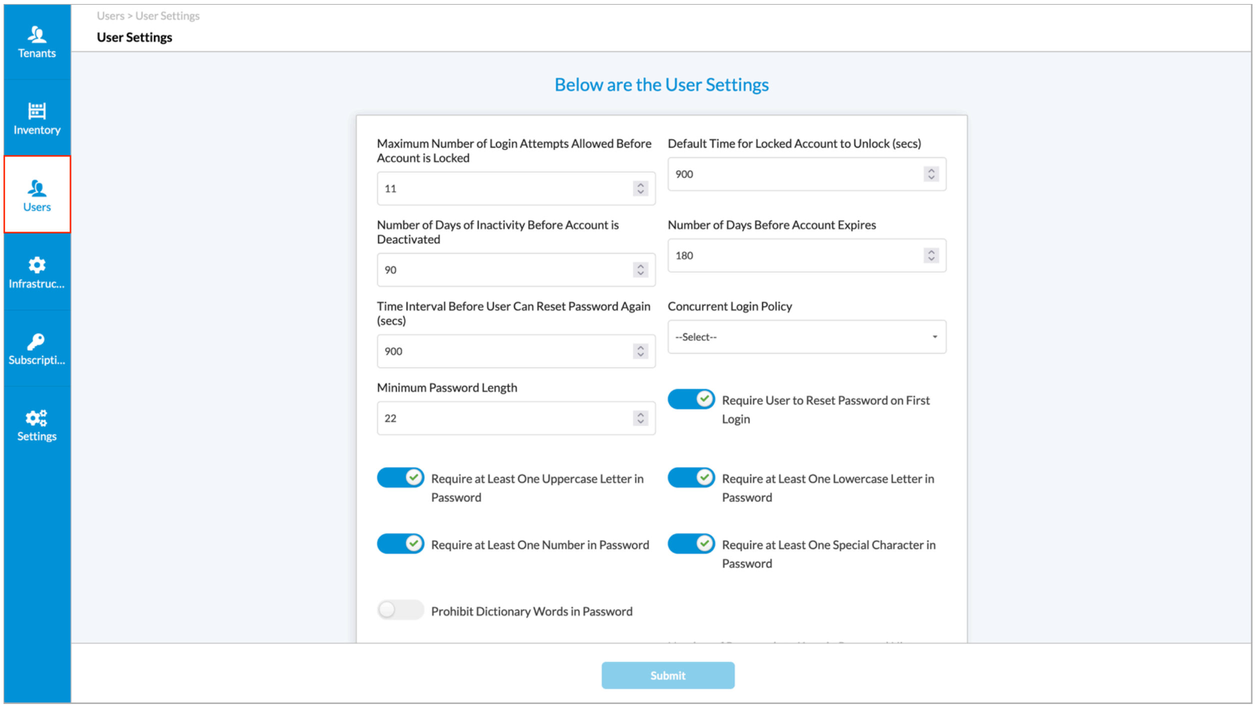
You can configure settings for users in the User Settings screen, including settings for the password policy. The User Settings screen is available at the Service ;Provider level and is applicable to all users at the Service Provider and Enterprise levels.

To configure user settings:

1. In Service Provider view, click the Users lifecycle in the left navigation panel, and then select User Settings.



2. In the User Settings screen, enter information for the following fields.



Below are the User Settings

Maximum Number of Login Attempts Allowed Before Account is Locked: 11

Default Time for Locked Account to Unlock (secs): 900

Number of Days of Inactivity Before Account is Deactivated: 90

Number of Days Before Account Expires: 180

Time Interval Before User Can Reset Password Again (secs): 900

Concurrent Login Policy: --Select--

Minimum Password Length: 22

☑ Require User to Reset Password on First Login

☑ Require at Least One Uppercase Letter in Password

☑ Require at Least One Lowercase Letter in Password

☑ Require at Least One Number in Password

☑ Require at Least One Special Character in Password

□ Prohibit Dictionary Words in Password

Setting	Description
Maximum Number of Login Attempts Allowed Before Account is Locked	Enter the number of user login attempts that are allowed before the user's account access is locked. Configuring a maximum number of login attempts protects against brute force login attacks.
Default Time for Locked Account to Unlock	Enter the default time before a locked account is unlocked, in seconds. If a user enters the wrong password too many times and is locked out, the user's account is unlocked after this amount of time has passed.
Number of Days of Inactivity Before Account is Deactivated	Enter the number of days that an account can be inactive before the account is deactivated.
Number of Days Before Account Expires	Enter the number of days before an account expires.
Time Interval Before User Can Reset Password Again (secs)	If a user resets their password, enter the amount of time, in seconds, that must pass before the user can reset their password again.
Concurrent Login Policy	Select a concurrent login policy. A concurrent login allows a user to log in to a system using the same

Setting	Description
	credentials but using different devices. Note that this field is supported in Versa Director Releases 22.1 and later. ◦ Allow—Allow concurrent logins. ◦ Deny—Do not allow concurrent logins. ◦ Force Logout—The active user is logged out before another user can log in with the same credentials.
Minimum Password Length	Enter the minimum length of the password. Note that this field is supported in Versa Director Releases 22.1 and later.
Require at Least One Uppercase Letter in Password	Click the slider bar to require at least one uppercase letter in a password.
Require at Least One Lowercase Letter in Password	Click the slider bar to require at least one lowercase letter in a password.
Require at Least One Number in Password	Click the slider bar to require at least one number in a password.
Require at Least One Special Character in Password	Click the slider bar to require at least one special character in a password.
Require User to Reset Password on First Login	Click the slider bar to require a user to reset their password when logging in for the first time.
Prohibit Dictionary Words in Password	Click the slider bar to prohibit users from using dictionary words in their password. A password dictionary contains a list of words or characters that users may not use in their passwords. Note that this field is supported in Versa Director Releases 22.1 and later.
Enable Password History	Click the slider bar to enable password history. ◦ Number of Passwords to Keep in Password History—Enter a number of passwords to keep in the password history (or use the up and down arrows) that the user is not allowed to reuse.
Expire Password	Click the slider bar to expire passwords.

Setting	Description
	◦ Number of Days Before Password Expires—Enter the number days before a password expires (or use the up and down arrows).

3. Click Submit.

Map External User Roles in Concerto

For Releases 11.3.1 and later.

The external role-mapping feature allows you to map an external user's custom role to a local default Concerto role so that the external user can log in to Concerto successfully. You can map external users both at the service provider and tenent levels.

Role mapping is required in the following scenarios:;

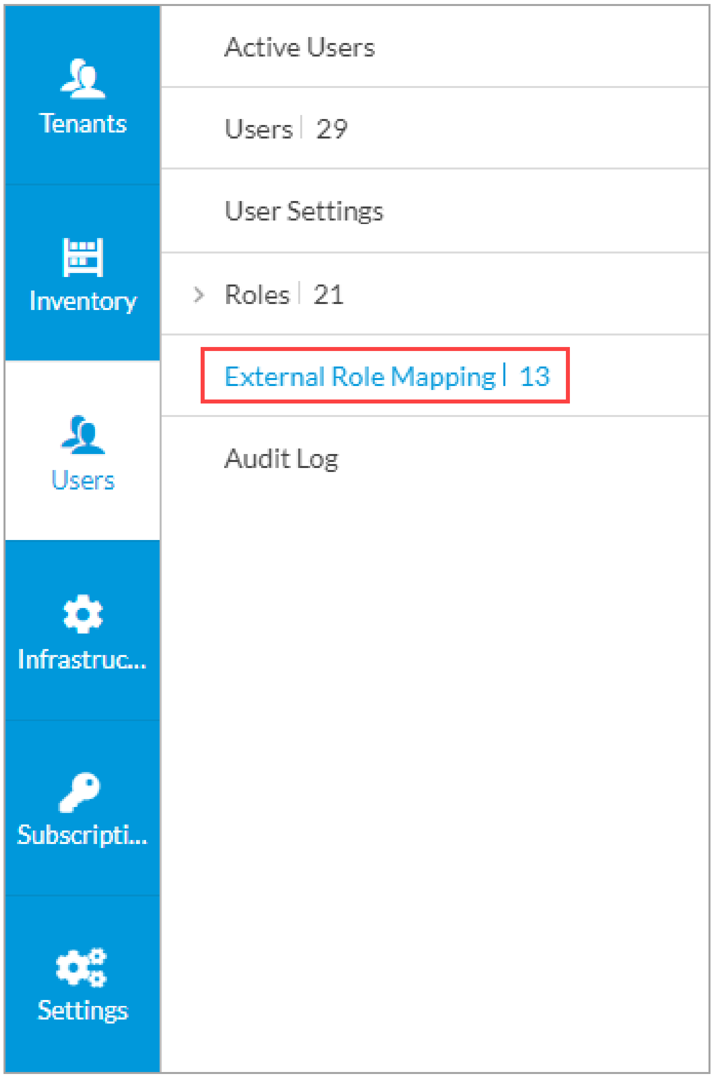
- If a single sign-on (SSO) user role configured in an identity provider (IDP), such as Okta or Ping Identity, is a custom role (that is, a role that is not present in Concerto)
- If a user is created in Versa Director with a custom role
- If a user role configured in an external server (such as Active Directory, RADIUS, and TACACS+ servers) is a custom role (that is, a role that is not present in Concerto)

As an example, let's say that a custom user role, AcmeOperator, has been configured in an IDP. For the AcmeOperator user to login to Concerto successfully, you must map this role to a local default Concerto role, such as Enterprise Administrator or Enterprise Operator. Then, when AcmeOperator attempts to log in to Concerto, Concerto maps the AcmeOperator role to its Enterprise Administrator or Enterprise Operator role and allows AcmeOperator to log in to Concerto.

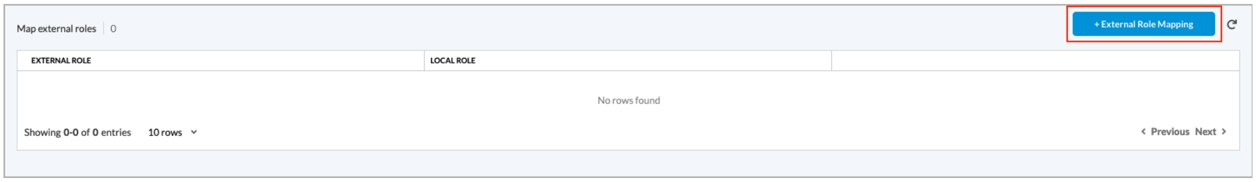
In Releases 11.4.1 and later, you can map the external custom role created in Versa Director, an IDP, or an external server to a local custom Concerto role and to a local default Concerto role.

To map an external user with a custom role to a local Concerto role:

1. Go to Users lifecycle and click External Role Mapping.



2. Click + External Role Mapping in the main screen.



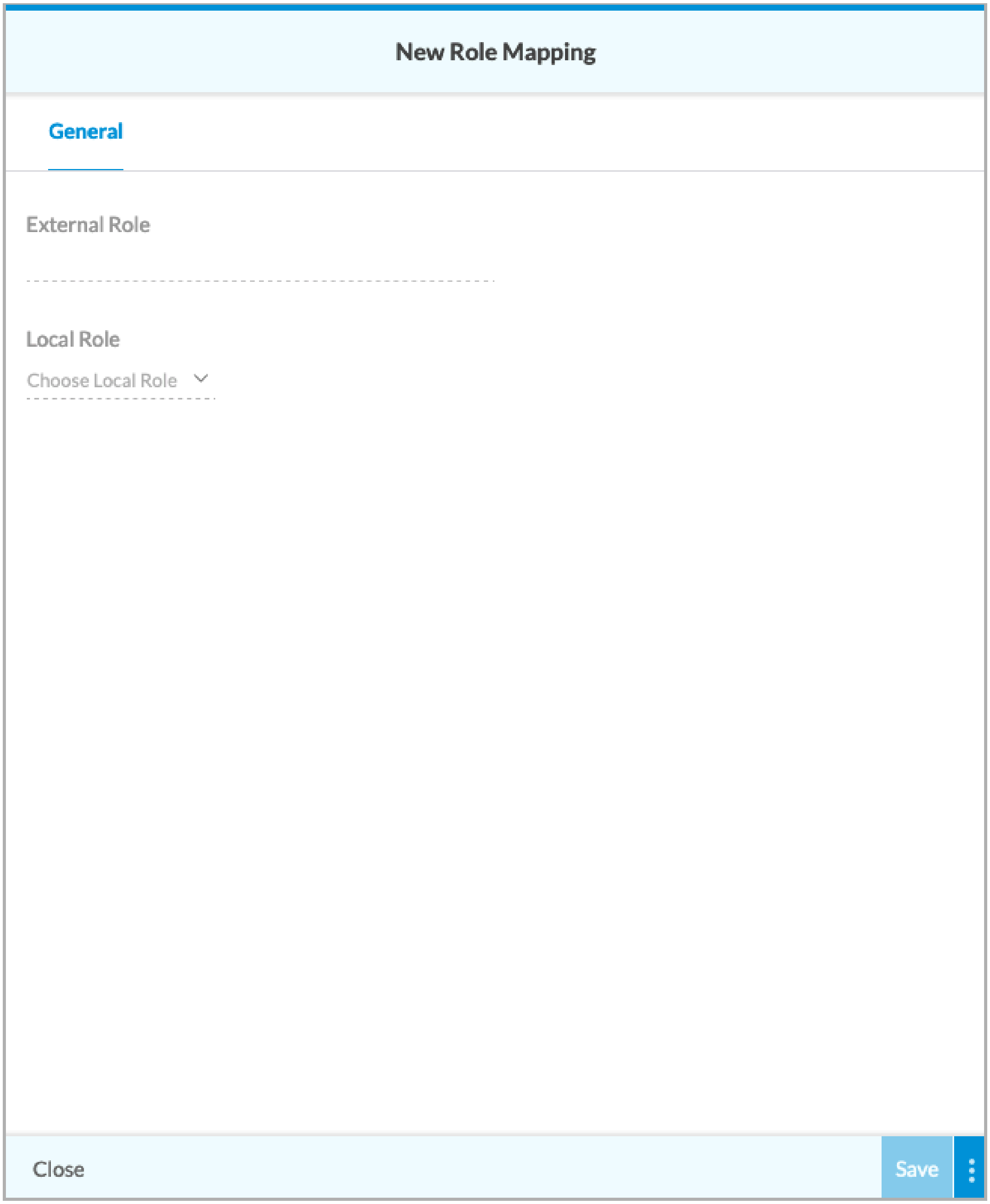
Map external roles | 0

EXTERNAL ROLE	LOCAL ROLE	
	No rows found	

Showing 0-0 of 0 entries 10 rows

‹ Previous Next ›

3. In the New Role Mapping screen, enter information for the following fields.



New Role Mapping

General

External Role

Local Role

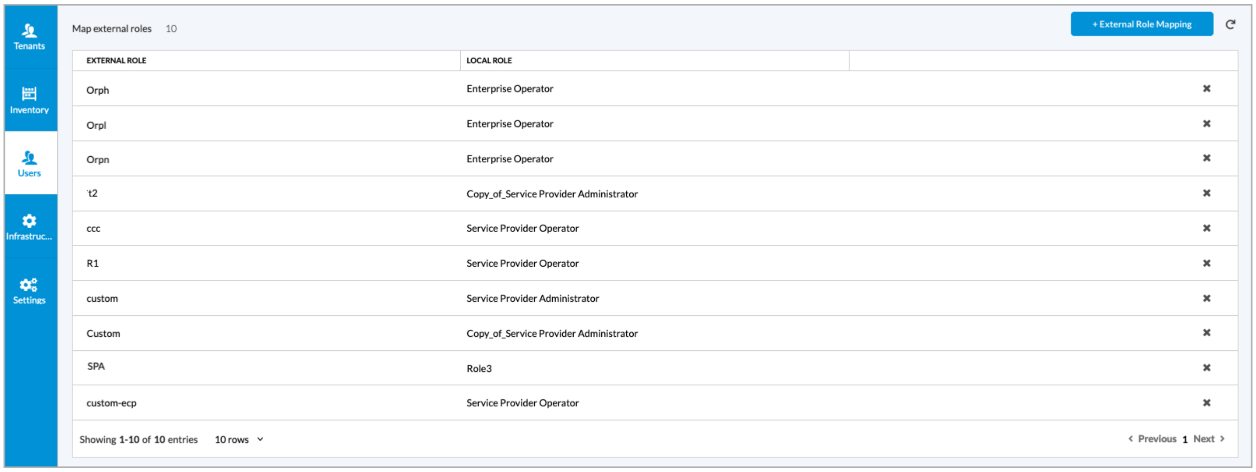
Choose Local Role

Field	Description
External Role	Enter the name of the external role.

Field	Description
Local Role	Select the local Concerto role that to map to the external role.

4. Click Save.

The following example shows a list of external user roles and the local Concerto roles to which they are mapped.



Map external roles 10

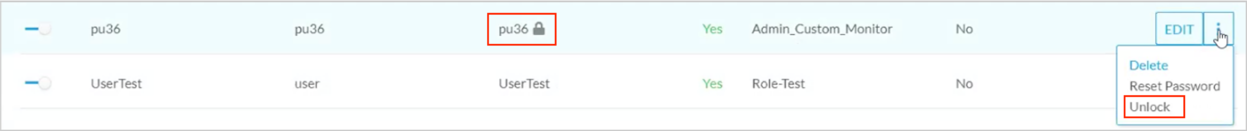
EXTERNAL ROLE	LOCAL ROLE	
Orph	Enterprise Operator	✖
Orpl	Enterprise Operator	✖
Orpn	Enterprise Operator	✖
't2	Copy_of_Service Provider Administrator	✖
ccc	Service Provider Operator	✖
R1	Service Provider Operator	✖
custom	Service Provider Administrator	✖
Custom	Copy_of_Service Provider Administrator	✖
SPA	Role3	✖
custom-ecp	Service Provider Operator	✖

Showing **1-10** of **10** entries 10 rows ‹ Previous 1 Next ›

Unlock a User Account

For Releases 10.2.1 and later.

If a user account becomes locked, you can unlock the account from the Concerto Users lifecycle screen. In the following screen, user pu36 has been locked, as indicated by the lock icon. To unlock the user's account, click the More icon in the row for that user pu36 and select Unlock. The user account is unlocked.



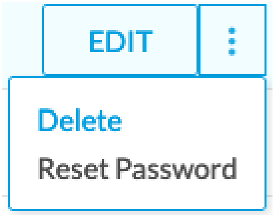
pu36	pu36	pu36 🔒	Yes	Admin_Custom_Monitor	No	
UserTest	user	UserTest	Yes	Role-Test	No	

Delete a User or Reset a User Password

You can delete a user or reset a user's password from both the Users lifecycle on the service provider home screen and the Users lifecycle within a tenant home screen.

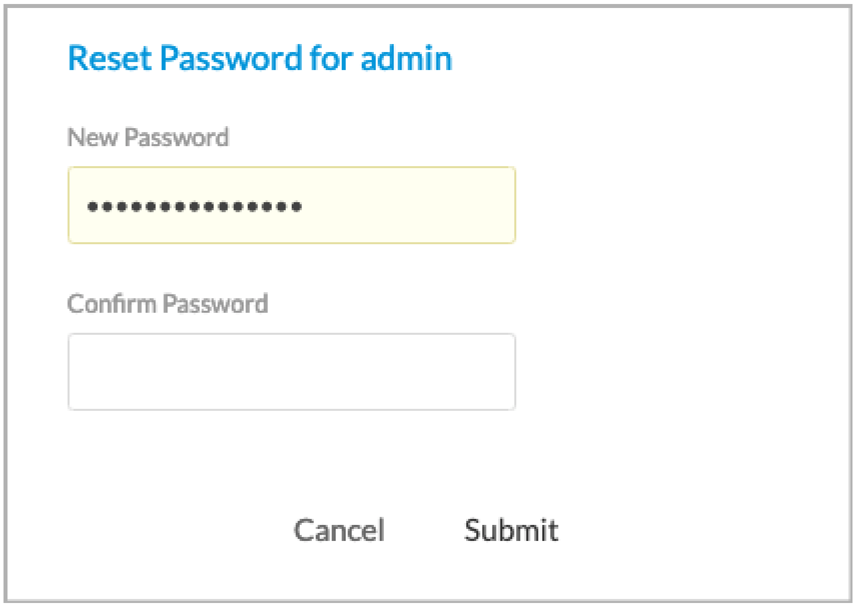
To delete a user:

1. Click the ⋮ More icon in the row for that user on the Users lifecycle screen.
2. Click Delete and enter information as prompted.



To reset a user password:

1. Click the ⋮ More icon in the row for that user on the Users lifecycle screen.
2. Click Reset Password. The Reset Password screen displays.



Reset Password for admin

New Password

•••••••••••••••

Confirm Password

3. Enter the new password and confirm the new password.
4. Click Submit. If you reset a user password, the user is prompted to change their password the next time they attempt to log in. For more information, see Change Your Initial User Password.

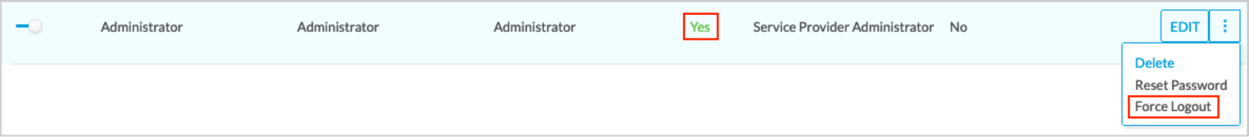
Force a User Logout

For Releases 10.2.1 and later.

You can force an active user to be logged out of Concerto.

To perform a forced logout on an active user:

1. Click the More icon in the row for that user on the Users lifecycle screen.



2. Select Force Logout. The user is logged out immediately.

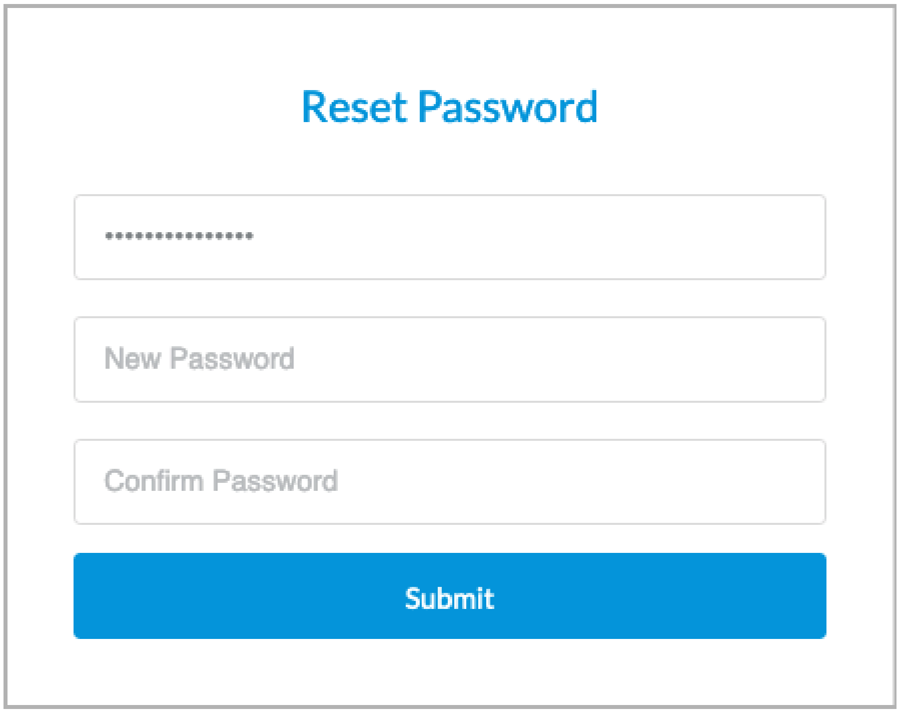
Change Your Initial User Password

For Releases 10.2.1 and later.

When you log in as a new user to Concerto for the first time, or if the administrator changes your password, you are prompted to change your password.

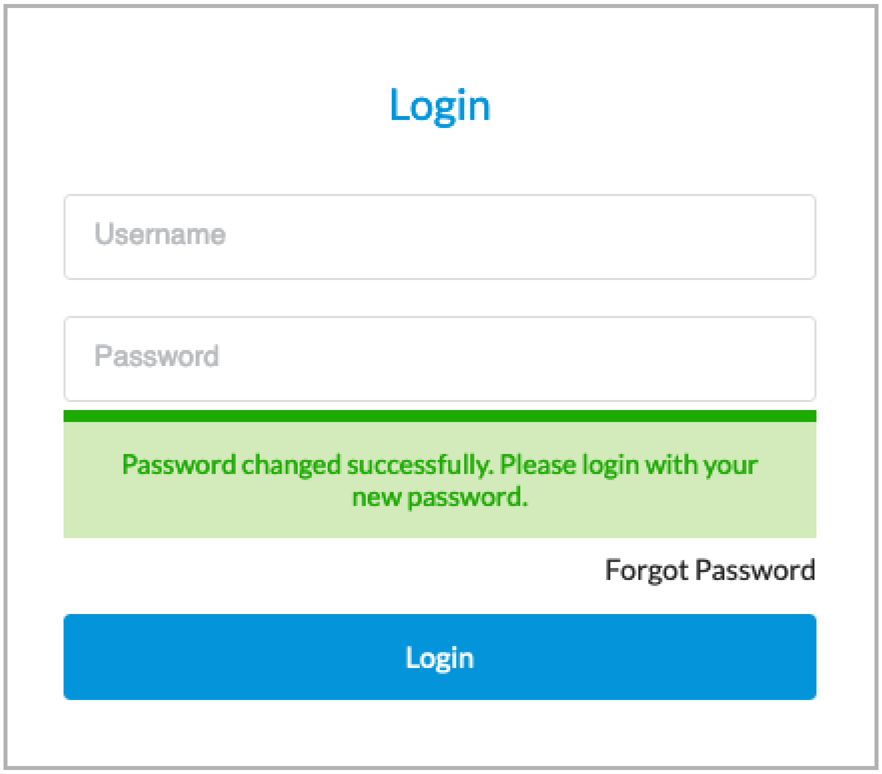
To change your password:

1. Log in to Concerto using your configured password. The following screen displays, prompting you to change your password.



2. Enter your current password, enter a new password, and confirm the new password by entering it again.

3. Click Submit. The following screen displays, and you can now log in with your new password.



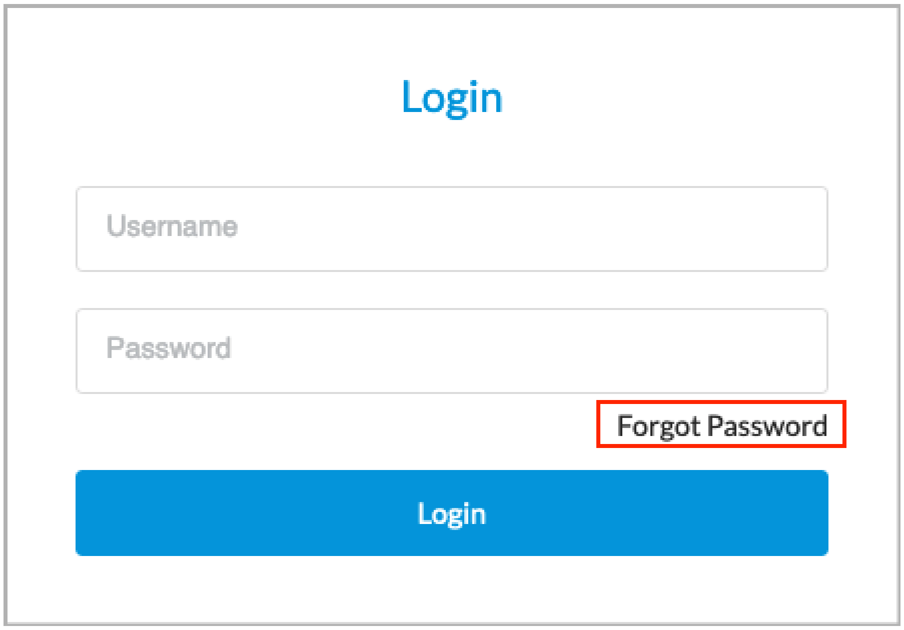
Password changed successfully. Please login with your new password.

Reset a Forgotten Password

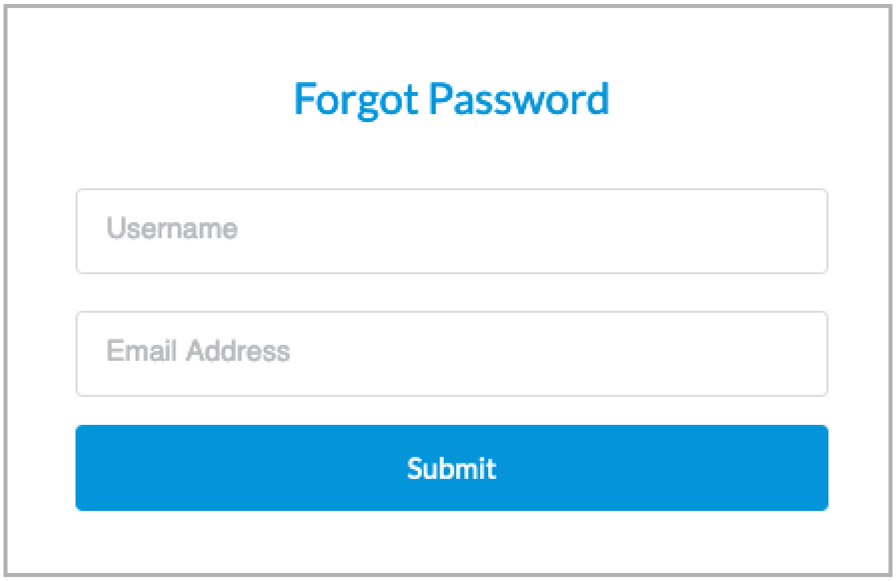
For Releases 10.2.1 and later.

If you forget your Concerto password, you can reset it:

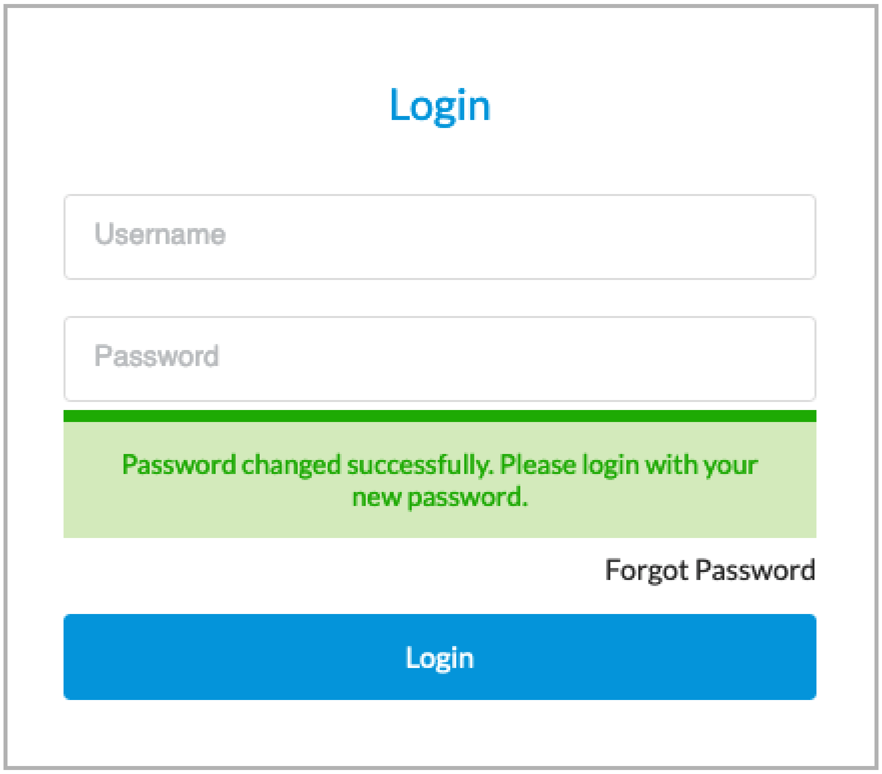
1. In the log in screen, click Forgot Password.



2. In the next screen, enter your username and email address.



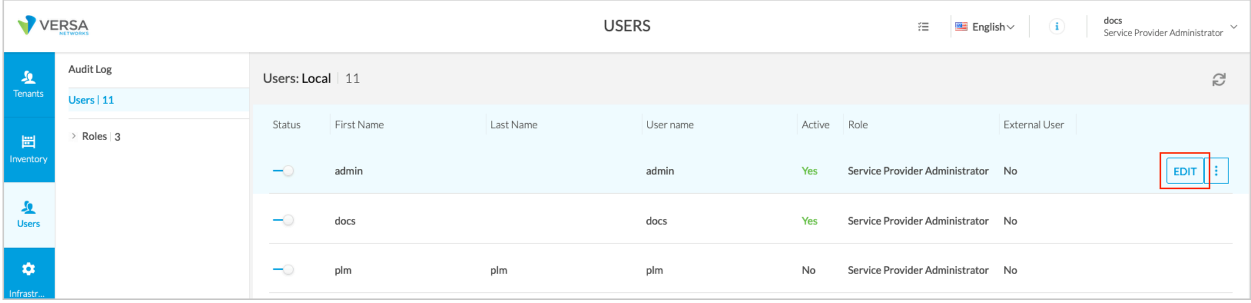
3. Click Submit. You then receive an email with a temporary password.
4. Enter the temporary password. You are then prompted to create a new password, as described in [Change Your Initial User Password](). After you reset your password, the following screen displays.



Password changed successfully. Please login with your new password.

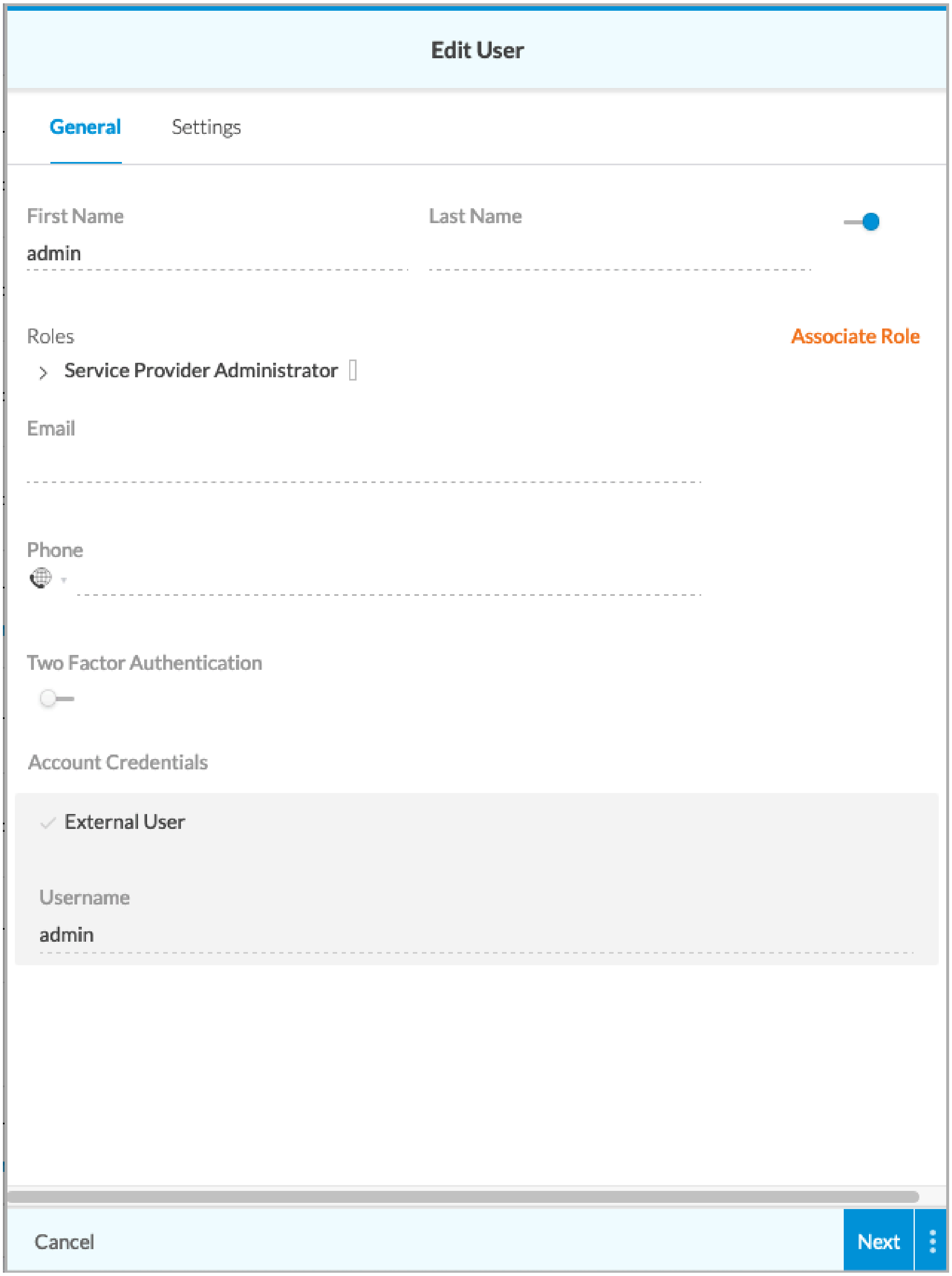
Edit User Information

1. On the Users lifecycle screen, hover over a row and click the Edit box, or click a row to display the Edit User screen for that user.



Status	First Name	Last Name	User name	Active	Role	External User
	admin		admin	Yes	Service Provider Administrator	No
	docs		docs	Yes	Service Provider Administrator	No
	plm	plm	plm	No	Service Provider Administrator	No

2. Select the General tab, and make the desired changes.



Edit User

First Name: admin

Last Name:

Roles: Service Provider Administrator

Email:

Phone:

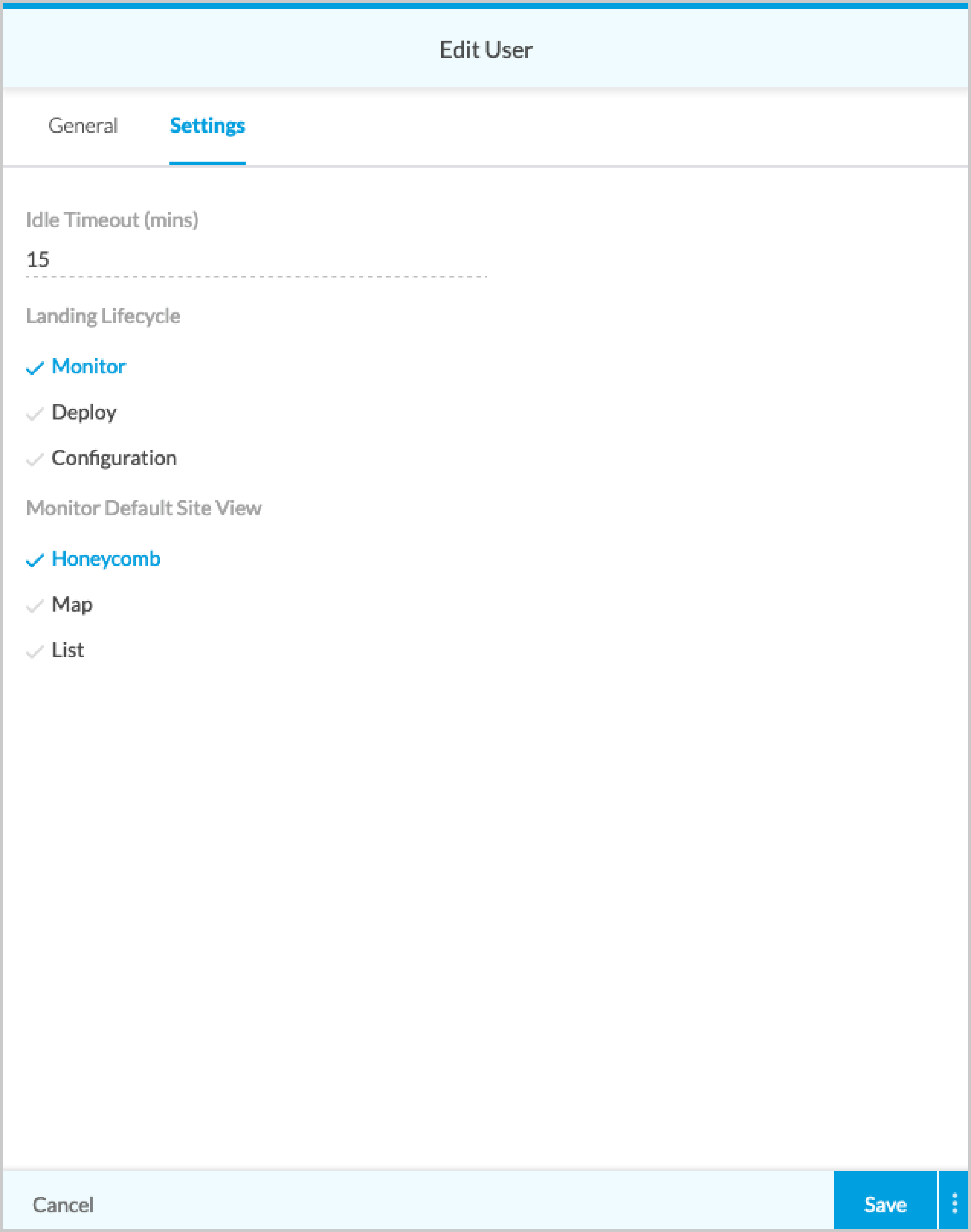
Two Factor Authentication

Account Credentials

✓ External User

Username: admin

3. Select the Settings tab, and make the desired changes.



Edit User

Idle Timeout (mins)
15

Landing Lifecycle

✓ Monitor
Deploy
Configuration

Monitor Default Site View

✓ Honeycomb
Map
List

4. Click Save.

View Audit Logs

For Releases 11.4.1 and later.

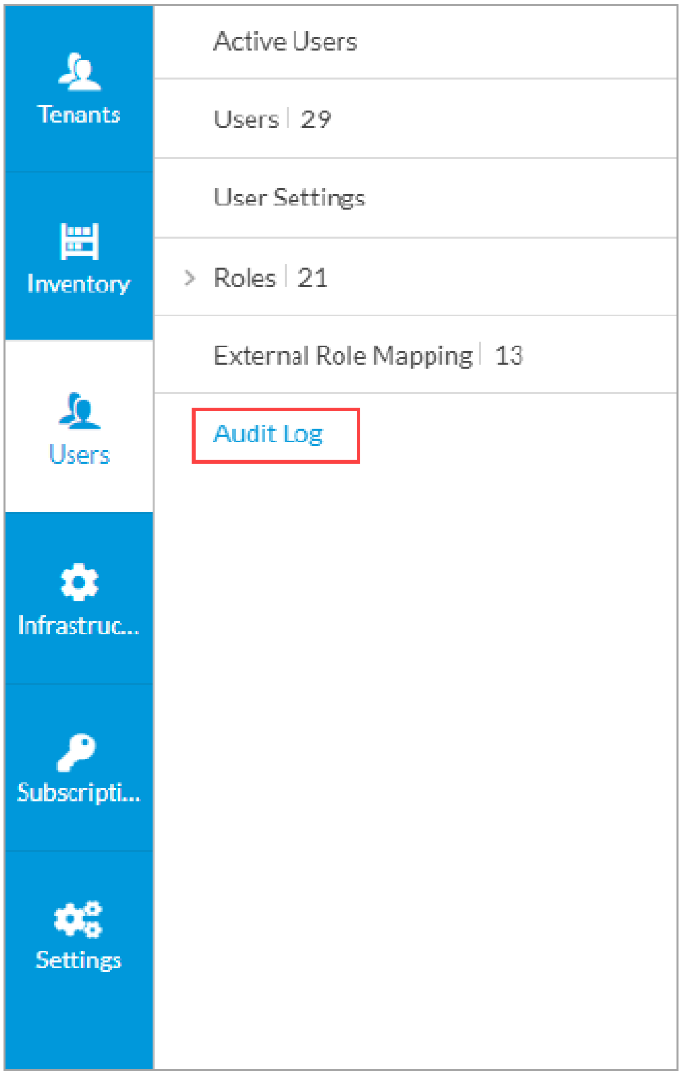
Internal audit logs capture information about all activity on Concerto, including all internal URLs that were visited, the payloads for each request, the actions that occur as a result of the request, and all errors that were encountered. The logs are placed in the Concerto audit tables, and they are also sent to Versa Director.

You use audit logs to view activity history on Concerto and to perform debugging.

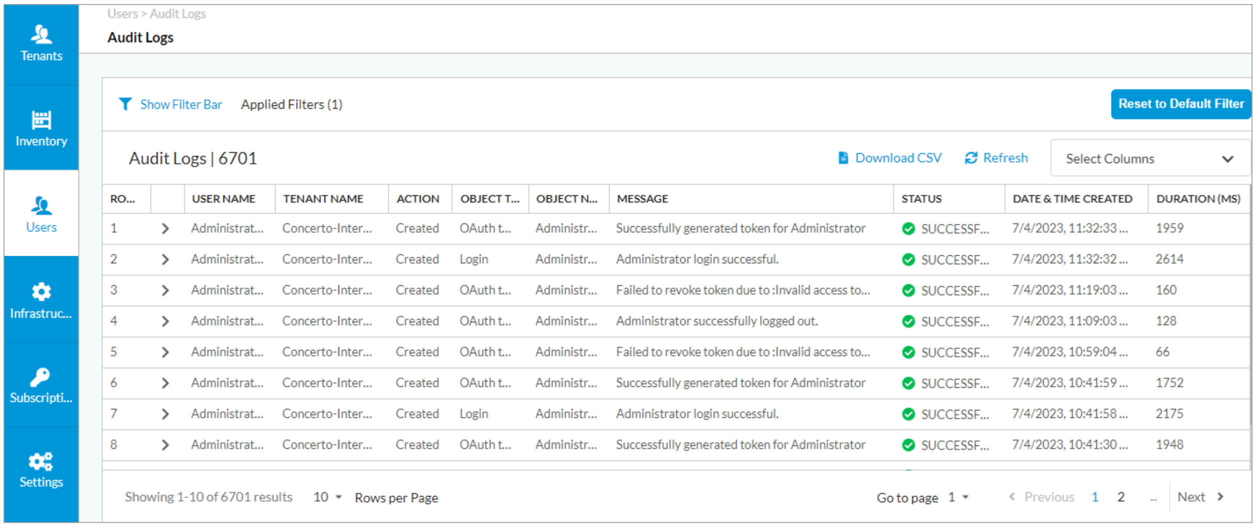
You view the audit logs in the Users lifecycle screen either at the system or tenant level. Note that to view the audit logs, you must be a Service Provider Administrator or an Enterprise Administrator.

To view audit logs:

1. Go to the Users lifecycle, and then click Audit Log.



2. The Audit Logs screen displays the audit log information.



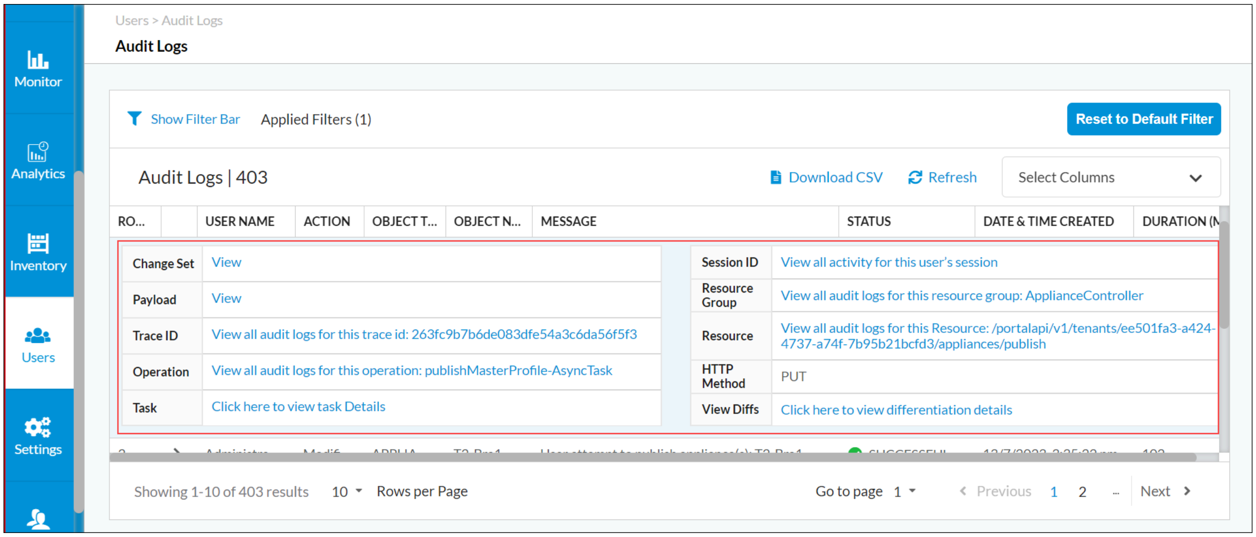
Audit Logs

Audit Logs | 6701

RO...		USER NAME	TENANT NAME	ACTION	OBJECT T...	OBJECT N...	MESSAGE	STATUS	DATE & TIME CREATED	DURATION (MS)
1	>	Administrat...	Concerto-Inter...	Created	OAuth t...	Administr...	Successfully generated token for Administrator	✓ SUCCESSF...	7/4/2023, 11:32:33 ...	1959
2	>	Administrat...	Concerto-Inter...	Created	Login	Administr...	Administrator login successful.	✓ SUCCESSF...	7/4/2023, 11:32:32 ...	2614
3	>	Administrat...	Concerto-Inter...	Created	OAuth t...	Administr...	Failed to revoke token due to :Invalid access to...	✓ SUCCESSF...	7/4/2023, 11:19:03 ...	160
4	>	Administrat...	Concerto-Inter...	Created	OAuth t...	Administr...	Administrator successfully logged out.	✓ SUCCESSF...	7/4/2023, 11:09:03 ...	128
5	>	Administrat...	Concerto-Inter...	Created	OAuth t...	Administr...	Failed to revoke token due to :Invalid access to...	✓ SUCCESSF...	7/4/2023, 10:59:04 ...	66
6	>	Administrat...	Concerto-Inter...	Created	OAuth t...	Administr...	Successfully generated token for Administrator	✓ SUCCESSF...	7/4/2023, 10:41:59 ...	1752
7	>	Administrat...	Concerto-Inter...	Created	Login	Administr...	Administrator login successful.	✓ SUCCESSF...	7/4/2023, 10:41:58 ...	2175
8	>	Administrat...	Concerto-Inter...	Created	OAuth t...	Administr...	Successfully generated token for Administrator	✓ SUCCESSF...	7/4/2023, 10:41:30 ...	1948

Showing 1-10 of 6701 results 10 Rows per Page Go to page 1 Previous 1 2 ... Next

3. To view details for a log entry, click the > Toggle Row Expanded icon next to the username. The log entry detail display. For example:



Audit Logs

Audit Logs | 403

RO...		USER NAME	ACTION	OBJECT T...	OBJECT N...	MESSAGE	STATUS	DATE & TIME CREATED	DURATION (M

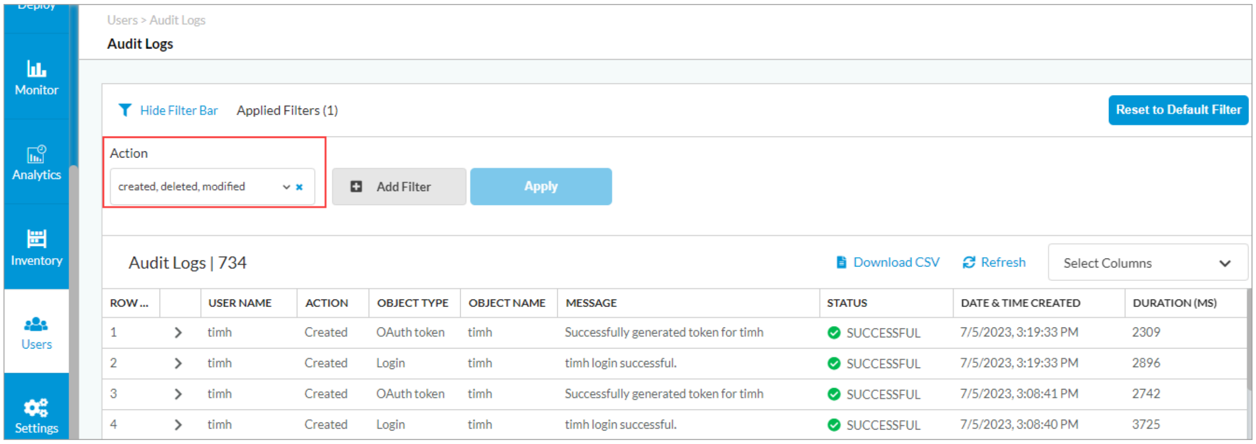
Change Set	View	Session ID	View all activity for this user's session
Payload	View	Resource Group	View all audit logs for this resource group: ApplianceController
Trace ID	View all audit logs for this trace id: 263fc9b7b6de083dfe54a3c6da56f5f3	Resource	View all audit logs for this Resource: /portalapi/v1/tenants/ee501fa3-a424-4737-a74f-7b95b21bcfd3/appliances/publish
Operation	View all audit logs for this operation: publishMasterProfile-AsyncTask	HTTP Method	PUT
Task	Click here to view task Details	View Diffs	Click here to view differentiation details

Showing 1-10 of 403 results 10 Rows per Page Go to page 1 Previous 1 2 ... Next

Field	Description
Payload	Displays the content of the request. To maintain user privacy, sensitive user information is replaced with asterisks (****).
Trace ID	Displays the trace ID associated with the request. When a user clicks a link in Concerto, Concerto generates a trace ID for the request.

Field	Description
Operation	Displays the action that was initiated by the request.
Session ID	Displays all the activity for a user during the session.
Resource Group	Displays the collection of resources that match the resource types specified in a query.
Resource	Displays all the audit logs for a user.
HTTP Method	Displays the HTTP method: ◦ DELETE ◦ GET ◦ HEAD ◦ PATCH ◦ POST ◦ PUT
Task	Displays all the task details. This option displays in the audit log only after you publish the SD-WAN branch.
View Diffs	Displays the differences between last published configuration and the current published configuration. This option displays in the audit log only after you publish the SD-WAN branch.

4. To run audit log queries, click Show Filter Bar icon.
5. In the Action field, select an audit log actions. By default, audit logs show create, modify, and delete actions. To view read calls, select the Read action. To view the CLI commands that were issued, select the None action.



Users > Audit Logs

Audit Logs

Action: created, deleted, modified

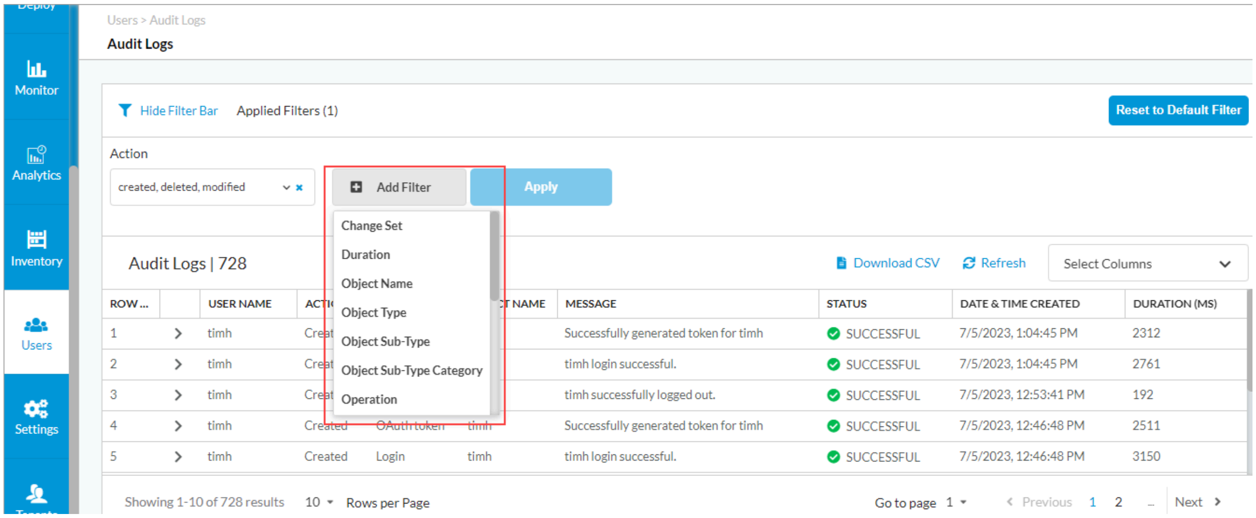
Audit Logs | 734

ROW ...		USER NAME	ACTION	OBJECT TYPE	OBJECT NAME	MESSAGE	STATUS	DATE & TIME CREATED	DURATION (MS)
1	>	timh	Created	OAuth token	timh	Successfully generated token for timh	✓ SUCCESSFUL	7/5/2023, 3:19:33 PM	2309
2	>	timh	Created	Login	timh	timh login successful.	✓ SUCCESSFUL	7/5/2023, 3:19:33 PM	2896
3	>	timh	Created	OAuth token	timh	Successfully generated token for timh	✓ SUCCESSFUL	7/5/2023, 3:08:41 PM	2742
4	>	timh	Created	Login	timh	timh login successful.	✓ SUCCESSFUL	7/5/2023, 3:08:40 PM	3725

- Created—Select to view audit logs when a new user, tenant, profile, or rule was created and added in the database.

- Deleted—Select to view audit logs when an existing user, tenant, profile, or rule was deleted.
- Modified—Select to view audit logs when an existing user, tenant, profile, or rule was modified.
- Read—Select to view audit logs when existing content from database, such as visits to tenant, user page, and profile pages, was read.
- None—Select to view audit logs at the service provider level for CLI operations, such as upgrade and show commands.

6. Click the ⊞ Add Filter icon, and then select one of the following query types for filtering the log information.



Action: created, deleted, modified

Audit Logs | 728

ROW ...		USER NAME	ACTI		T NAME	MESSAGE	STATUS	DATE & TIME CREATED	DURATION (MS)
1	>	timh	Creat			Successfully generated token for timh	✓ SUCCESSFUL	7/5/2023, 1:04:45 PM	2312
2	>	timh	Creat			timh login successful.	✓ SUCCESSFUL	7/5/2023, 1:04:45 PM	2761
3	>	timh	Creat			timh successfully logged out.	✓ SUCCESSFUL	7/5/2023, 12:53:41 PM	192
4	>	timh	Created	OAuth token	timh	Successfully generated token for timh	✓ SUCCESSFUL	7/5/2023, 12:46:48 PM	2511
5	>	timh	Created	Login	timh	timh login successful.	✓ SUCCESSFUL	7/5/2023, 12:46:48 PM	3150

Showing 1-10 of 728 results 10 Rows per Page

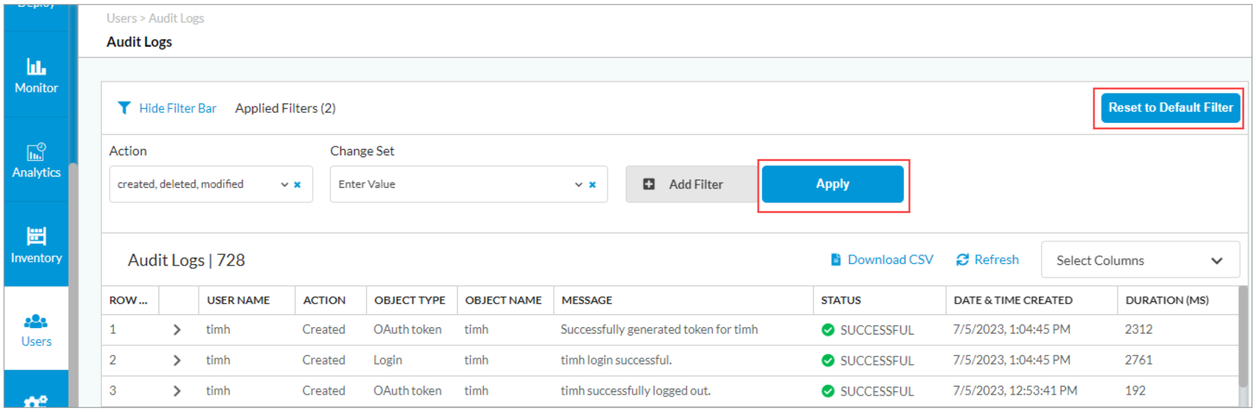
Query	Description
Change Set	Search on a string of characters in an error message. Select the string search type: ◦ Contains—Results contain the search string that you enter. This is the default. ◦ RegEx—Results match a regular expression that you enter.
Duration	Search on the duration of the requests: ◦ Seconds—Click to enter a search duration in seconds. This is the default. ◦ Milliseconds—Click to enter a search duration in milliseconds.
Object Name	Search on an object name such as master profile, appliance, rule, element, profile, or subprofile name. Select the string search type: ◦ Contains—Results contain the search string that you enter. This is the default. ◦ Exact—Results contain the exact search string that you enter. ◦ RegEx—Results match a regular expression that you enter.
Object Type	Search on an object type.
Object Subtype	Search on an object subtype.
Object Subtype Category	Search on an object subtype category.
Operation	Select the type of operation to query. Select the string search type: ◦ Contains—Results contain the search string that you enter. This is the default. ◦ Exact—Results contain the exact search string that you enter. ◦ RegEx—Results match a regular expression that you enter.

Payload	Search on a string of characters in the payload. Select the string search type: ◦ Contains—Results contain the search string that you enter. This is the default. ◦ RegEx—Results match a regular expression that you enter.
Resource	Search on the type of resource. Select the string search type: ◦ Contains—Returns results that contains search string. This is the default keyword. ◦ Regex—Returns results that matches regular expression search string.
Resource Group	Search on the type of resource group. Select the string search type: ◦ Contains—Returns results that contains search string. This is the default keyword. ◦ Exact—Returns results that matched the exact search string. ◦ RegEx—Returns results that matches regular expression search string.
Date and Time Created	Search on the date and time: ◦ Preset—Returns results within the 7 days or a week. ◦ Custom—Returns results within a custom start date and end date.
Status	Select the status on which to query: ◦ Client Error ◦ Redirection ◦ Server Error ◦ Successful
Status Code	◦ CLI Status Codes: ▪ 0—CLI exit code of 0 means that the CLI

	operation was successful. - 1—CLI exit code of other than 0 means that the CLI operation was not successful. - 126—CLI exit code of 126 means that a command was found but it is not executable. - 127—CLI exit code of 127 means that a command was not found. ◦ HTTP Status Codes: - 200—OK. The request succeeded. - 201—Created. The request succeeded, and a new resource was created as a result. - 204—No content. There is no content to send for this request, but the headers may be useful. - 302—Found. The URI of requested resource was changed temporarily. Further changes in the URI may be made in the future. - 400—Bad request. The server could not understand the request because of invalid syntax. - 401—Unauthorized. The client must authenticate itself to receive the requested response. - 403—Forbidden. The client does not have access rights to the content. - 404—Not found. The server cannot find the requested resource. - 405—Not acceptable. The web server, after performing server-driven content negotiation, found no content that conforms to the criteria given by the user agent. - 500—Internal server error. The server encountered a situation that it does not know how to handle.
Tenant Name	Select the tenant name.
Trace ID	Enter an exact trace ID on which to query.
Session ID	Enter an exact session ID on which to query.
Username	Select the username on which to query. Select the string search type:

	◦ Contains—Returns results that contains search string. This is the default keyword. ◦ Exact—Returns results that matched the exact search string. ◦ RegEx—Returns results that matches regular expression search string.

7. To restore the default filters, click Apply. Click Reset to Default Filter.



Users > Audit Logs

Audit Logs

Hide Filter Bar Applied Filters (2) Reset to Default Filter

Action: created, deleted, modified

Change Set: Enter Value

Add Filter Apply

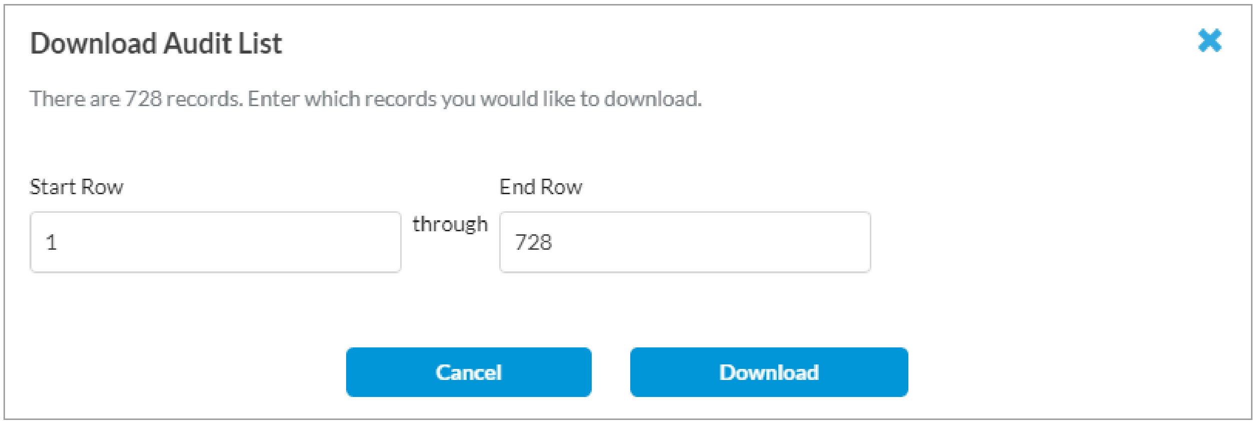
Audit Logs | 728 Download CSV Refresh Select Columns

ROW ...		USER NAME	ACTION	OBJECT TYPE	OBJECT NAME	MESSAGE	STATUS	DATE & TIME CREATED	DURATION (MS)
1	>	timh	Created	OAuth token	timh	Successfully generated token for timh	✓ SUCCESSFUL	7/5/2023, 1:04:45 PM	2312
2	>	timh	Created	Login	timh	timh login successful.	✓ SUCCESSFUL	7/5/2023, 1:04:45 PM	2761
3	>	timh	Created	OAuth token	timh	timh successfully logged out.	✓ SUCCESSFUL	7/5/2023, 12:53:41 PM	192

Download Audit Logs in CSV Format

For Releases 11.4.1 and later.

1. In the Audit Logs screen, click the Download CSV Download CSV icon.
2. In the Download Audit List popup window, enter values for the starting and ending rows. You can download a maximum of 5000 logs at a time.



Download Audit List

There are 728 records. Enter which records you would like to download.

Start Row: 1 through End Row: 728

Cancel Download

3. Click Download.

Supported Software Information

Releases 10.1.1 and later support all content described in this article, except:

- Release 10.2.1 adds the Active column in the Users screen; adds support for the unlocking users from Concerto, changing passwords, resetting forgotten passwords, forcing user logout, and discovering appliances created in Versa Director; adds support for two-factor authentication.
- Release 11.3.1 adds support for mapping an external user role to a local Concerto role.
- Release 11.4.1 adds support for audit logs; adds the User Settings screen; adds support for mapping external custom roles to local Concerto custom roles.

Additional Information

Concerto Home Screen Overview
Configure Single Sign-On Using Director
Configure User Account Settings