Configure AAA

For supported software information, click here.

This article describes how to configure authentication, authorization, and accounting (AAA) for users who access a Director node.

Authentication identifies users to determine whether they can access a Director node and to perform operations on it, including accessing an Analytics node. To authenticate a user, you use a user database on an external server or within Director. The external authentication server can be Active Directory, LDAP, RADIUS, or TACACS+. For Releases 22.1.1 and later, you can use two-factor authentication (2FA) in conjunction with using external authentication servers.

After a user is authenticated on a Director node, each user action that they perform must be authorized. Authorization provides remote access control, including one-time authorization and service authorization based on user or user account and profile. The Director software provisions two user types, provider and tenant (or organization), and for each user type the Director software provides different roles, which determine the access level for individual users. When you create a user, you assign them to the desired role.

When you have a topology with more than one Director node, you can configure one of the Director nodes to be the central authentication Director node. This node processes all the authentications requests received by any of the Director nodes.

Authorization uses a database to define the authorization methods. The database can be located locally on the access server or on a router, or it can be hosted remotely on a RADIUS or TACACS+ server. The authorization process assembles a set of attributes that describe what the user is authorized to perform, compares them to the information in the authorization database, and then returns to AAA the user's permissions and restrictions.

Configure User Authentication

To authenticate a user in Versa Director, the user database can be internal or external. If the users are added directly in Versa Director, no user configuration is required. However, to access an external user database, perform the configuration procedure explained in this article.

You can connect Versa Director to the following external servers:

- Active Directory
- LDAP

- RADIUS
- TACACS+

For Releases 20.2.1 and later, you can configure multiple redundant authentication servers. If you configure multiple servers, authentication is performed in the configured order. If the first configured authentication server is not reachable, the second authentication server is tried, and so on.

For Releases 22.1.1 and later, you can incorporate two-factor authentication (2FA) into the process of logging in to a Director node while using external authentication servers.

To configure user authentication for a Director node, you do the following:

1. Optionally, configure two-factor authentication.
2. Configure an authentication connector to link the Director node to an authentication server.
3. Configure the AAA authentication.
4. Associate organizations with the authentication connector.

Director User Login Conventions

When you configure login to a Director node, you can configure local or remote login, or both. Local login allows a user to log in directly to the Director node, authenticating the user based on a local username and password database. Remote login authentication uses a remote AAA authentication server.

For local authentication, you create a user on the Director node.

For remote authentication, you create a user on an Active Directory, an LDAP, a RADIUS, or a TACACS+ server. If the remote server is unreachable, the login operation falls back to local authentication. For the local authentication to succeed in this situation, you must create a local user with the same username as the remote user. For example, if the remote username is VersaSupport, you must create the username VersaSupport on the local Director node. Note that if you configure a remote server as a default authentication connector, only remote users can log in to the Director node; local Director users cannot log in.

You can configure the order in which the Director node tries different authentication methods, having it start with either local or remote authentication and then having it try the other method if the first one fails. These two methods are called local-then-remote, which is the default, and remote-then-local.

In the local-then-remote method:

1. When a user enters a username and password, the Director node checks whether the local user exists.
2. If the user exists, local authentication is initiated.
3. If the local user exists but the password is different, external (remote) authentication is initiated.
4. If the local user does not exist, external authentication is initiated.

In the remote-then-local method:

1. When a user enters a username and password, the Director node checks whether the remote user exists.
2. If the remote authentication server is not reachable, local authentication is initiated.
3. If the user exists on the remote server, remote authentication is initiated.
4. If the remote user does not exist, the authentication fails.

The following table are the username conventions for logging in to Versa Director UI:

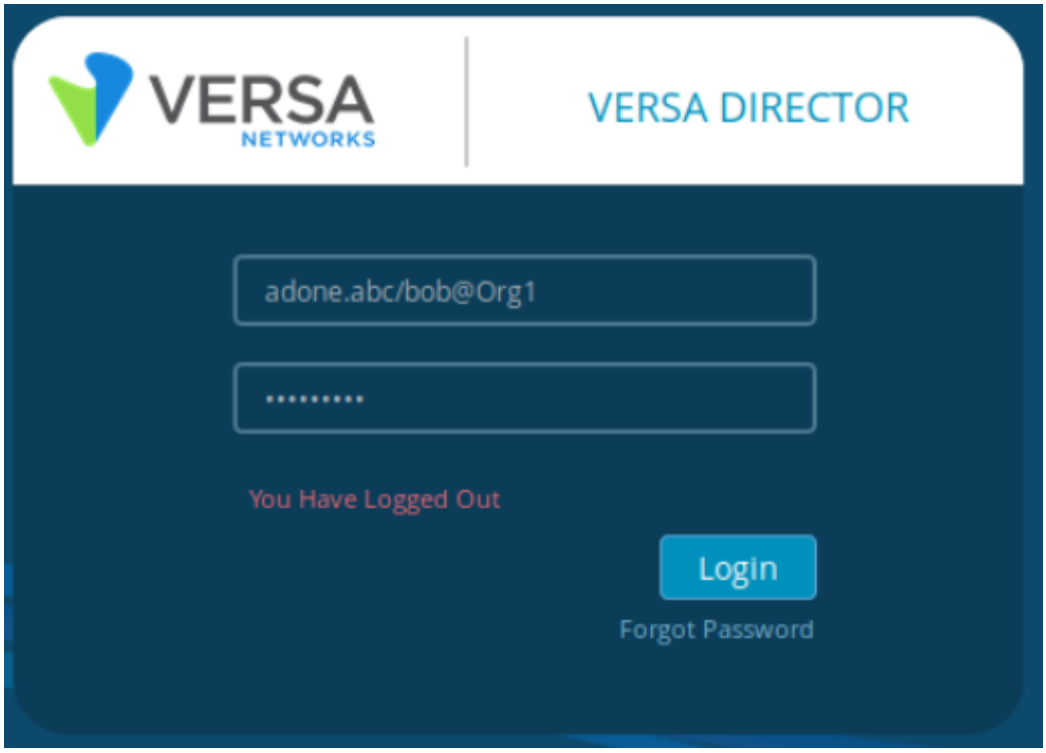
When connecting to an Active Directory global catalog server using LDAP, RADIUS, and TACACS+, the following are the login conventions:

User Type	**Local Authentication**	**External (Remote) Authentication**
Provider	*username* For example: James	*username* (for all external authentication types) For example: James *username@system* (the *@system* is optional) (for RADIUS and TACACS+ only) For example: James@System
Organization (Tenant)	*username* For example: Admin	*username@organization-name* For example: thomas@TelecomProvider

When connecting to an Active Directory global catalog server for the Active Directory connector configured on port 3268 or 3269, the following are the login conventions:

User Type	**Internal**	**External**
Provider	*username* For example: Admin	*domain-name*/*username* For example: adone.abc/admin
Organization (Tenant)	*username* For example: Admin	*domain-name*/*username@organization-name* For example: adone.abc/ Bob@TelecomProvider).

The following is an example login screenshot for an external provider user:



Central Authentication

For Releases 22.1.3 and later.

When you have a topology with more than one Director node, you can configure one of the Director nodes to be the central authentication Director node. This node processes all the authentications requests received by any of the Director nodes. Central authentication is useful when customer branches are geographically dispersed. For example, suppose you have a deployment with three Director nodes—DC1, DC2, and DC3—that are located in three data centers. If you configure the DC1 Director node to be the central authentication node for all three Director nodes, an administrator can access customer branches that are managed by any of the three Director nodes.

You can use the following authentication methods on the central authentication Director node to authenticate users:

- Basic authentication
- Basic external server authentication, such as Active Directory, LDAP, RADIUS, and TACACS+
- OAuth
- OAuth with an external server
- Single sign-on (SSO) from any providers, including Okta, Ping Identity, and Azure AD.

You can use any SSO authentication service that allows a user to use a single set of login credentials to access multiple applications and to use an external authentication server to authenticate a user. If you use SSO for login, you are

redirected to an identity provider (IdP) authentication page using SAML or OpenID.

To use SSO with a central authentication Director node, you configure the SSO information, which is the IP address or FQDN and hostname of the other Director nodes. Then, you can log out from the Director node, and log in again using SSO. For more information, see Configure an SSO Connector, below.

If you use central authentication, you cannot configure a connector to a single IDP connector in connector mode. If you do not use central authentication, single IDP connector mode is used for authentication.

If the central authentication Director node and the other Director nodes are in different locations, it is strongly recommended that you configure central authentication for each tenant to avoid latency. For this to work, you must first create organization (tenant) users on both the central authentication server and the organization server. Then you configure the central authentication Director node on the organization servers, and you configure the supported user roles for the organization users. With this configuration, authentication requests from all Director nodes and organization users are sent to the central authentication Director node for validation.

To use central authentication for all system users, you configure the central authentication connector as the default connector. If you configure a default connector, local users cannot log in to central authentication servers. If you enable external authentication, only users authenticated by external servers can log in to tenant servers.

To use central authentication for tenant users, create an organization, add supported user roles, and associate external authentication connector with the organization. For more information, see Associate an Authentication Connector with an Organization, below.

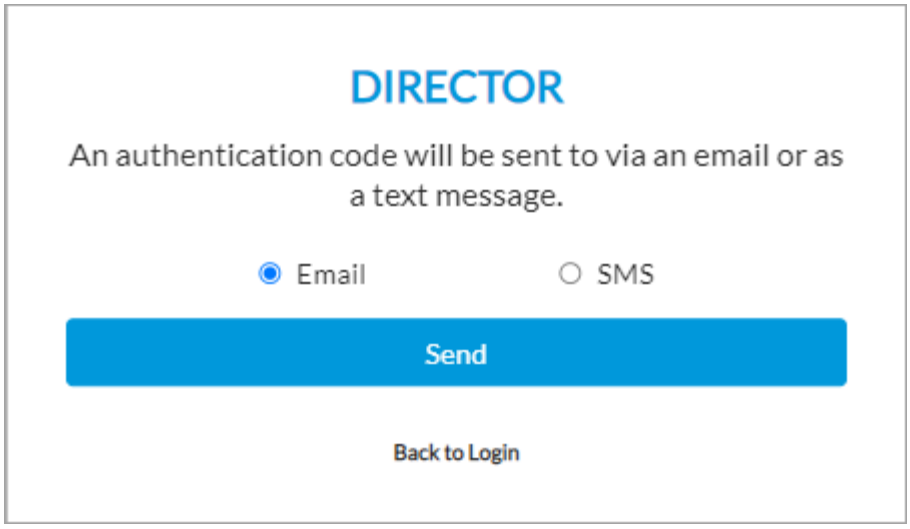
Configure Two-Factor Authentication

For Releases 22.1.1 and later.

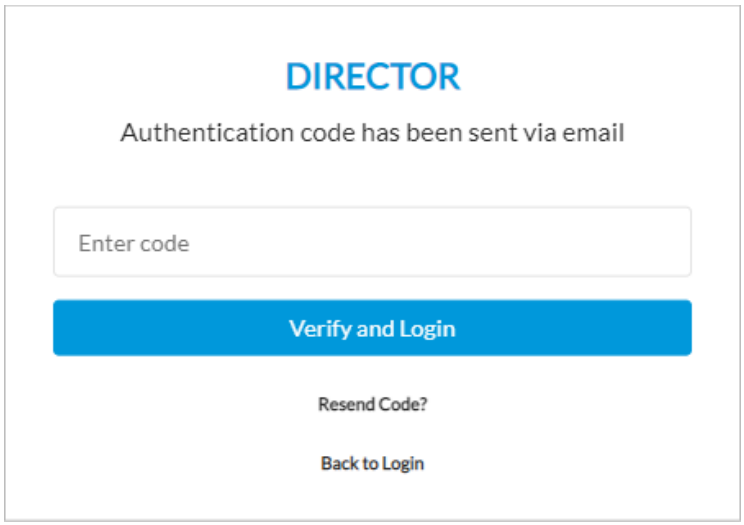
When you use external authentication, you can configure two-factor authentication to provide additional authentication for users who log in to Director nodes. With two-factor authentication, the user receives an authentication code either in email or as an SMS.

By default, two-factor authentication is disabled for all users, and an administrator or authorized user can enable it. If an administrator has enabled two-factor authentication, a user cannot disable it.

When a user is logging in to a Director node, the Director node checks the username and password and also checks whether two-factor authentication is enabled for the user. If two-factor authentication is required, the Director login screen displays a two-factor authentication window in which the user must select how to receive the authentication code.



The user then enters the authentication code.



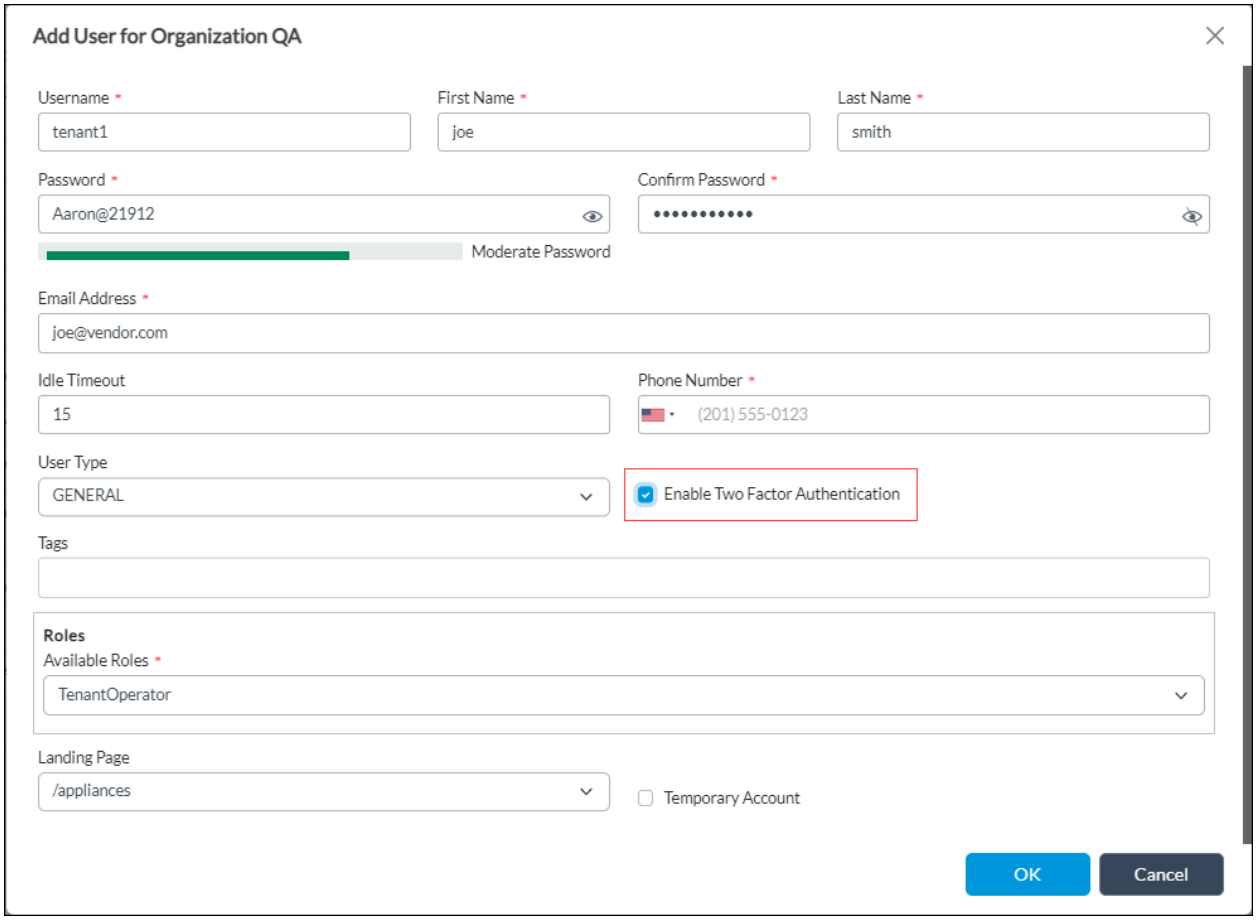
After the Director node validates the authentication code, the two-factor authentication process is complete.

An administrator or an authorized user can enable or disable two-factor authentication. By default, two-factor authentication is disabled for all users. Users cannot disable two-factor authentication if it is enabled by an administrator. In addition to your username and password login, Director checks if two-factor authentication is enabled for the user. If two-factor authentication is required, Director displays the two-factor authentication window where you enter the authentication code received through email or mobile message server. After the authentication code is validated, the two-factor authentication process is complete.

Enable Two-Factor Authentication on the Director Node

To enable two-factor authentication for a user:

1. In Director view, select the Administration tab in the top menu bar.
2. Select an organization in the horizontal menu bar.
3. Select Director User Management > Organization Users in the left menu bar.
4. Click the Add icon. In the Add User for Organization popup window, enter information for the following fields.



5. For information about configuring the other fields, see Add Tenant (Organization) Users.
6. Click OK.

Configure External Authentication Servers for Two-Factor Authentication

You can configure users and assign them roles using Active Directory, LDAP, RADIUS, or TACACS+ external authentication servers. In the configuration for the external authentication server, you must enable two-factor authentication, and you must include email address and mobile number attributes so that the user can receive the authentication code. This section provides the information required for configuring each type of external authentication server to support two-factor authentication.

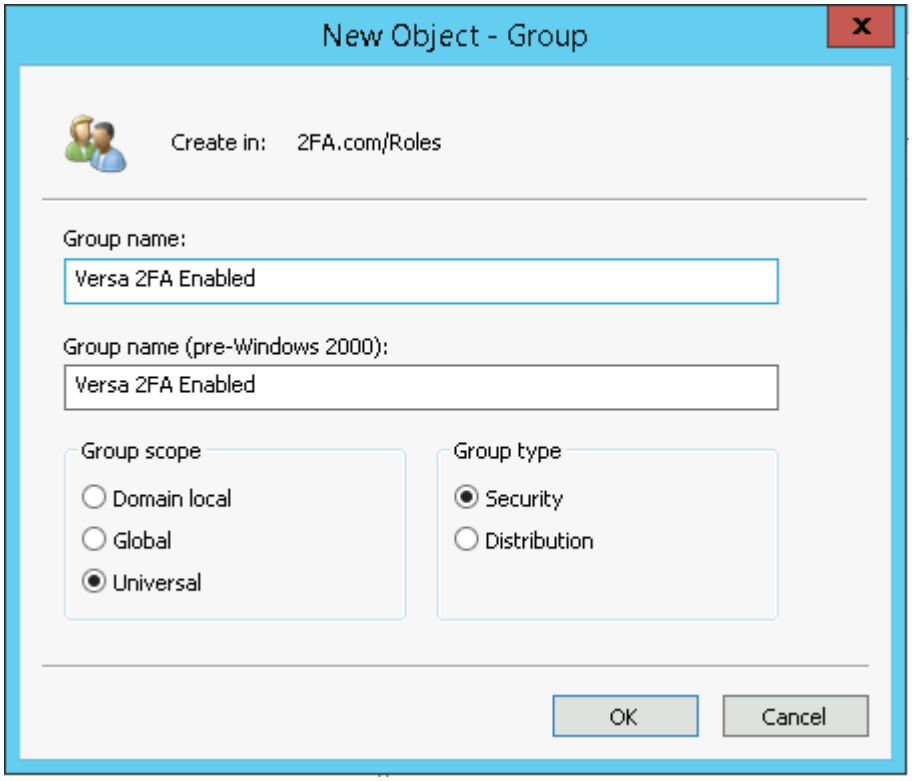
Configure an Active Directory Server for Two-Factor Authentication

For an Active Directory server, you create a group named Versa-2FA-Enabled and then you add two-factor

authentication users to this group.

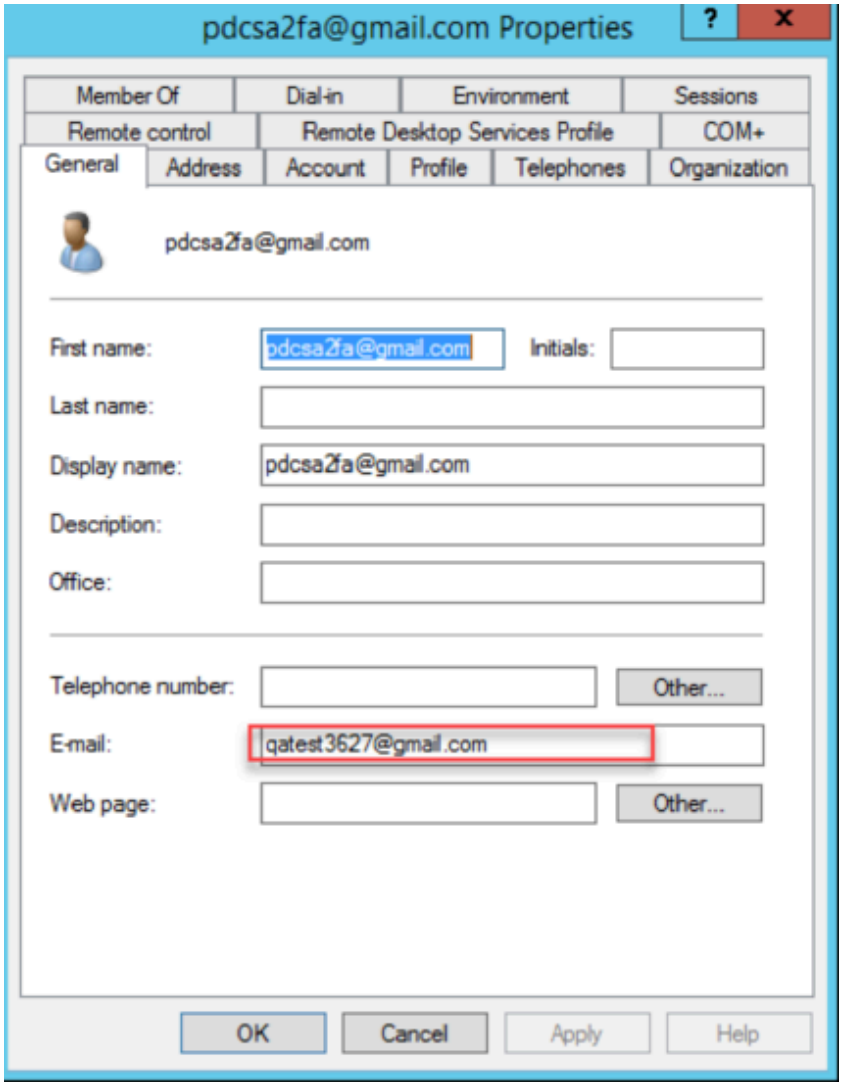
To configure two-factor authentication on an Active Directory server:

1. Create the Versa-2FA-Enabled group on the Active Directory server.



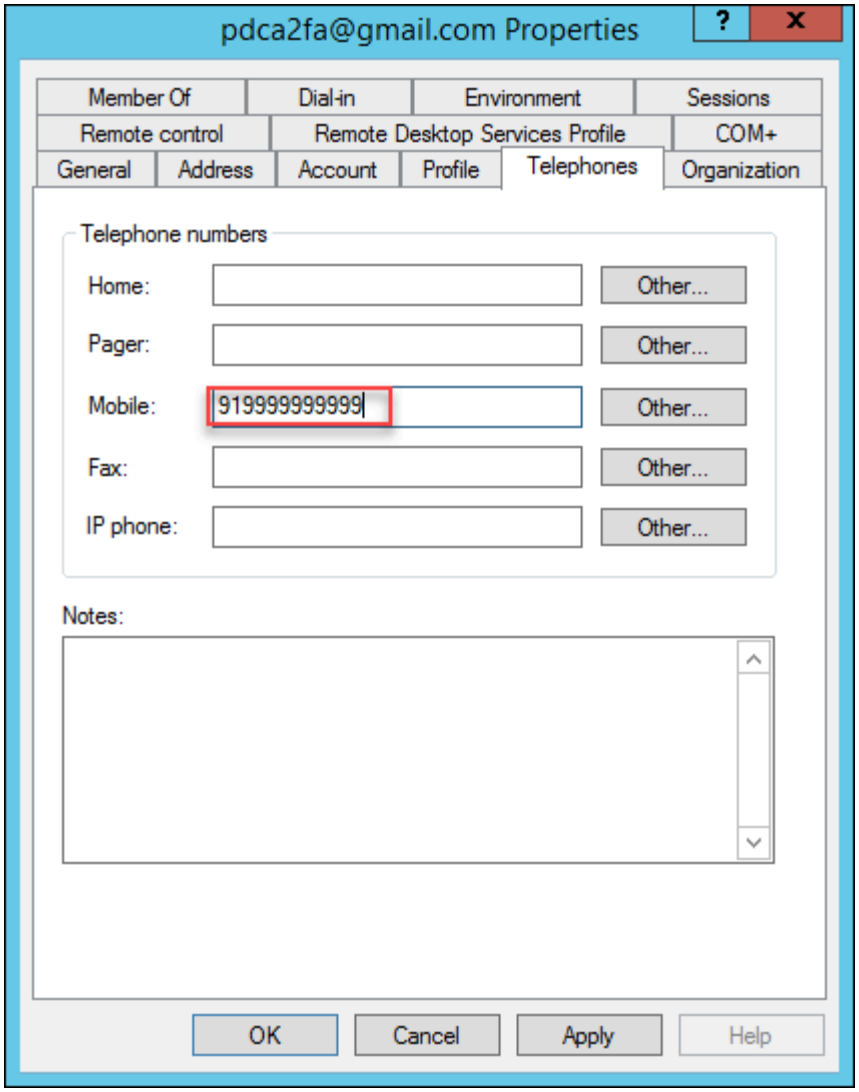
2. Select the General tab, and then enter the email address of the user to receive the two-factor authentication code.

Updated: Thu, 24 Oct 2024 10:45:19 GMT



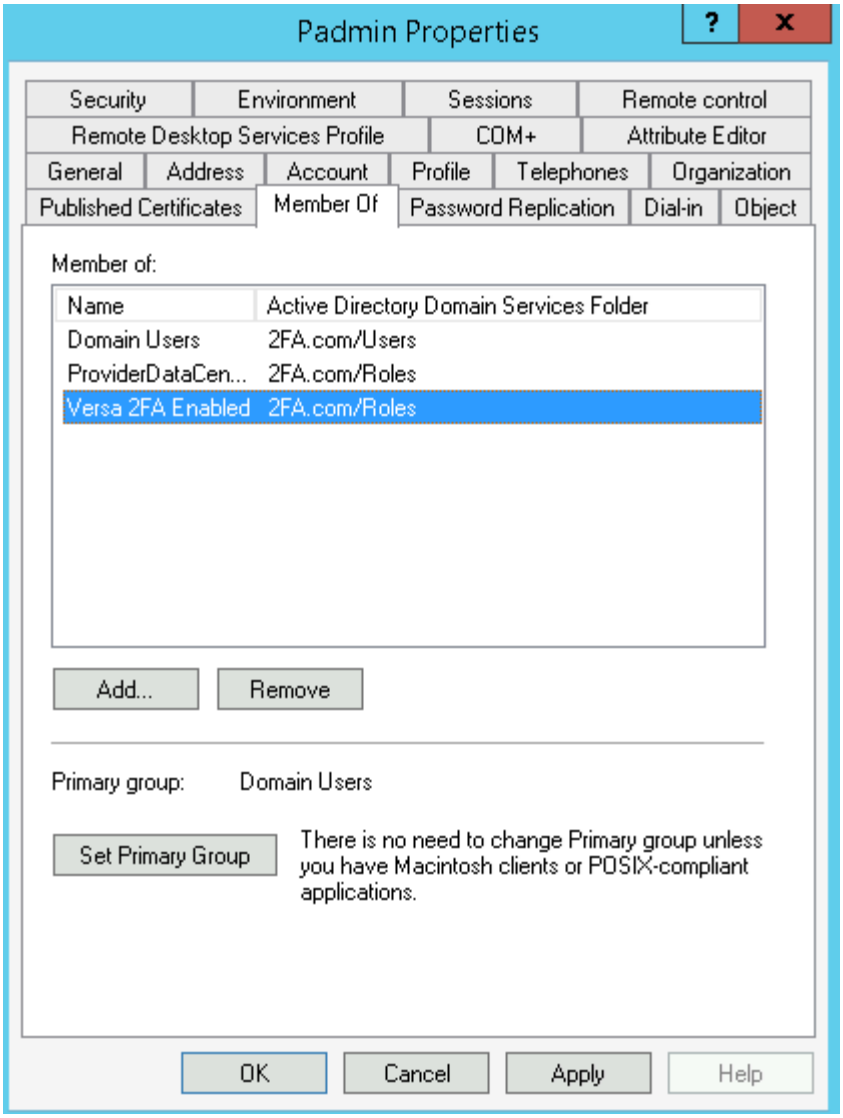
3. Select the Telephones tab, and then enter the mobile number of the user to receive the two-factor authentication code through an SMS.

Updated: Thu, 24 Oct 2024 10:45:19 GMT



4. Select the Member Of tab, and then add the user to the Versa-2FA-Enabled group.

Updated: Thu, 24 Oct 2024 10:45:19 GMT



5. Click Apply.

Note: In the Accounts tab, when you create an Active Directory user account, the @ special character you enter with an email address for the user logon name is considered as the underscore (_) character. This is a known behavior change from Microsoft. For example, if you enter the Active Directory user account name as abc@xxx.com, it is replaced with abc_xxx.com.

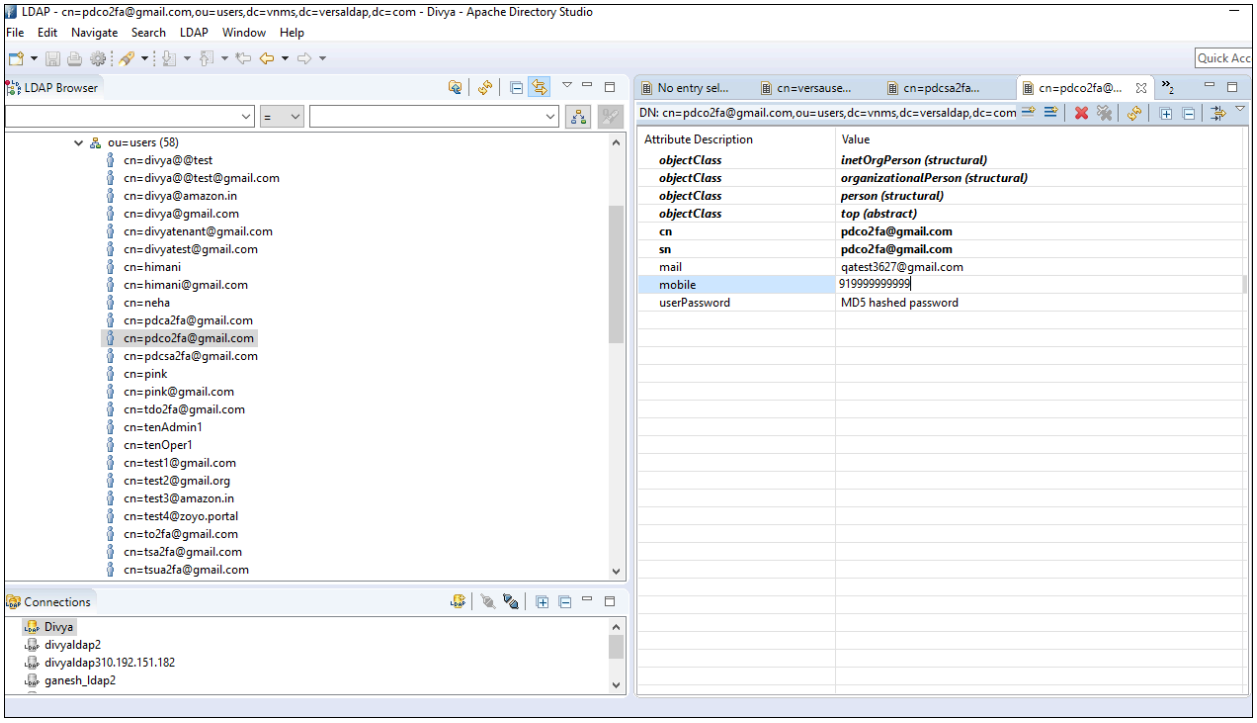
Configure an LDAP Server for Two-Factor Authentication

For LDAP authentication server, you create a group named Versa-2FA-Enabled and then you add two-factor authentication users to this group. The users must belong to the inetOrgPerson object class so that you can add the email address and mobile number attributes for them to receive the authentication code.

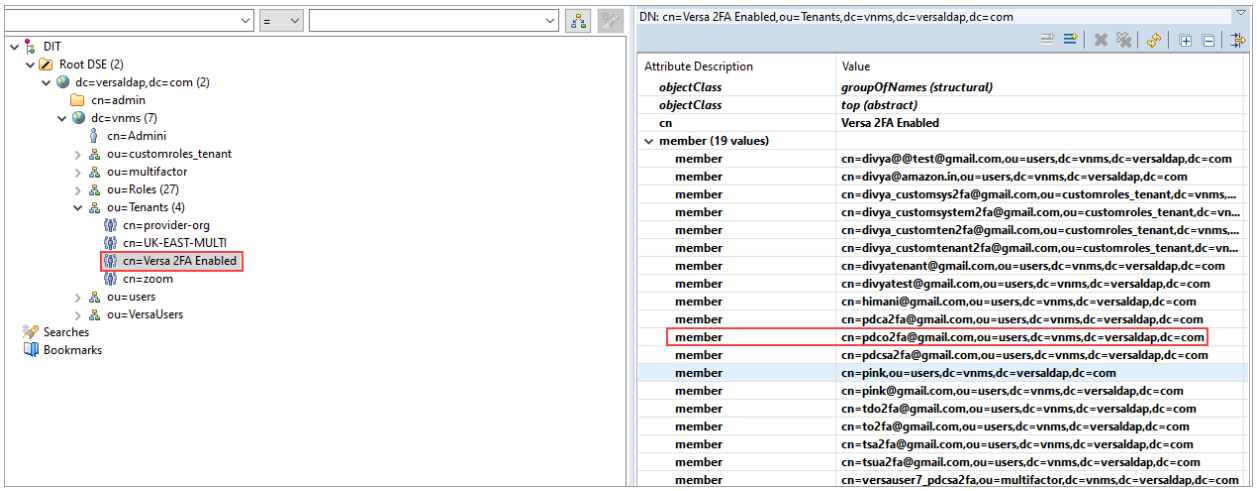
Note that you can add only new users to the LDAP two-factor authentication group, because LDAP does not allow you to change the person object to the inetOrgPerson object.

To configure two-factor authentication on an LDAP server:

1. Create a user in the inetOrgPerson object class, and enter the following information.



   a. For the Mail attribute, enter an email address in the Value field.
   b. For the Mobile attribute, enter a mobile number in the Value field.
2. Create the Versa-2FA-Enabled group, and then add the user to this group.



Configure a RADIUS Server for Two-Factor Authentication

To configure two-factor authentication on a RADIUS server, enter information similar to the following to the RADIUS

authentication configuration file:

```
TSA1 Cleartext-Password := "versa123"
  Versa-Role = "TenantSuperAdmin",
  Versa-Tenant = Org1,
  Versa-Email-Id = "abc.xxx@versa-networks.com",
  Versa-Phone-No = "91xxxxxxxx",
  Versa-2FA-Enabled = "true"
  Versa-GUI-Idle-TimeOut= 20
```

Configure a TACACS+ Server for Two-Factor Authentication

To configure two-factor authentication on a TACACS+ server, enter information similar to the following to the RADIUS authentication configuration file:

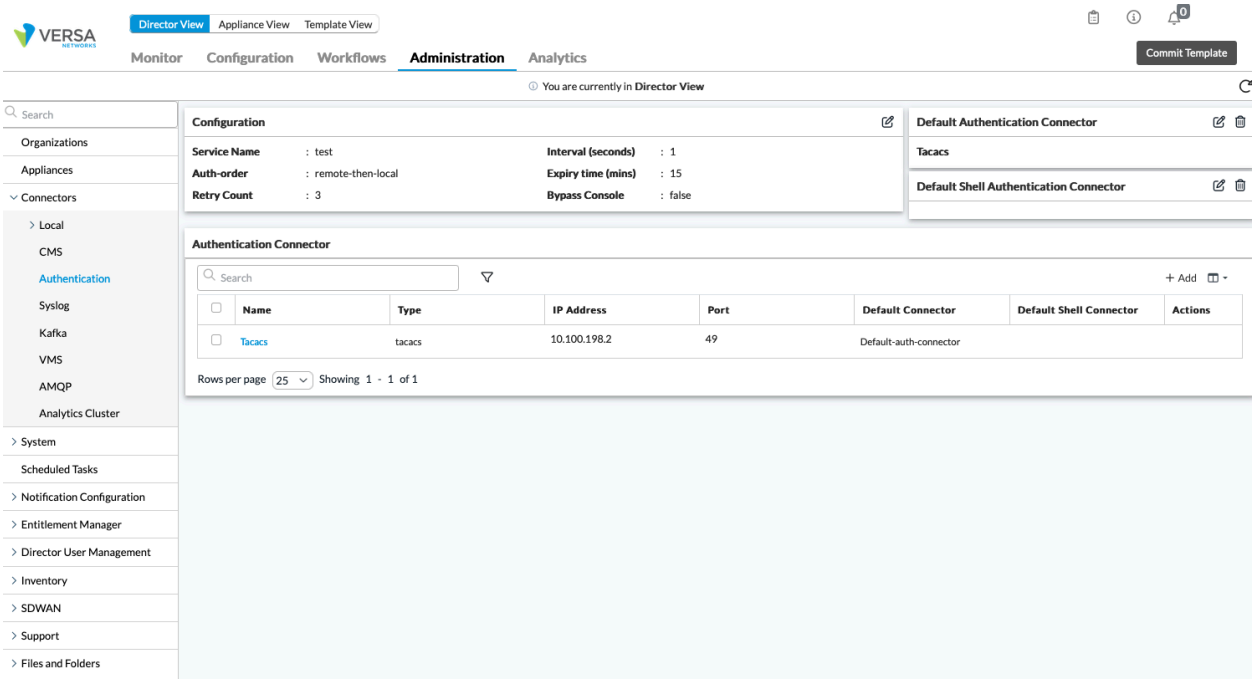
```
group = TSA_2FA {
   login = PAM
    service = test {
       Versa-Role = "TenantSuperAdmin"
       Versa-UserId = "9009"
       Versa-Tenant = "Org1"
       Versa-GUI-Idle-TimeOut = "60"
       Versa-Email-Id = "abc.xxx@versa-networks.com",
       Versa-Phone-No = "91xxxxxxxx",
       Versa-2FA-Enabled = "true"
    }
}

user = TSA1 {
     member = TSA_2FA
     login = cleartext "versa1234" #des 2OkHxsq6VYVig # versa123
     global = cleartext "versa1234"
     pap   = cleartext "versa1234"
}
```

Configure Authentication Connectors

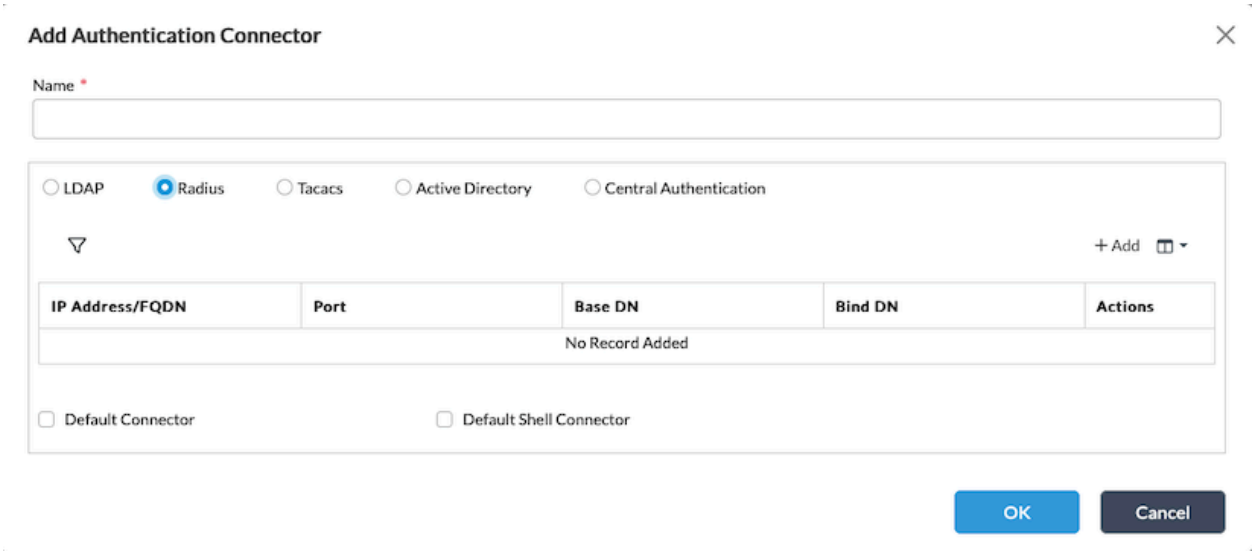
You configure one or more authentication connectors, which link the Director node to authentication servers. For each authentication connector, you define the type of external (remote) AAA authentication server, the server's IP address or FQDN, the port to connect to, and password credential information.

To configure an authentication connector:

1. In Director view, select the Administration tab in the top menu bar.
2. Select Connectors > Authentication in the left menu bar.

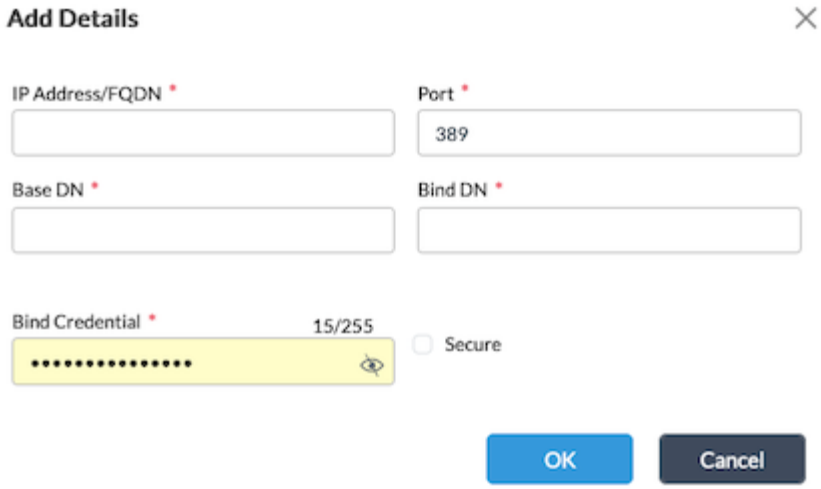


3. In the Authentication Connectors pane, click the Add icon to add a connector. In the Add Authentication Connector window, enter information for the following fields.



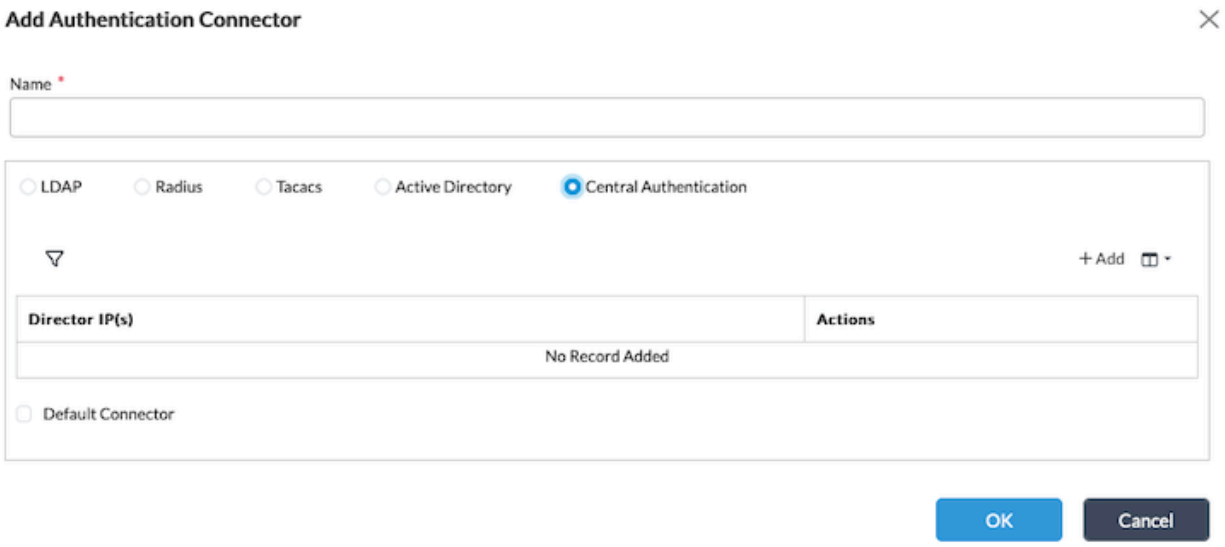
Field	Description
Name (Required)	Enter a name for the authentication connector.
Type of Server (Required)	Select the type of external (remote) authentication server: ◦ Active Directory. Note that you can configure an authentication connector only to a Domain in a single Forest. ◦ Central authentication ◦ LDAP ◦ RADIUS ◦ TACACS+
Add icon	Click to add a connector and configure the external authentication server. For more information, see Step 4.
Default Connector	Click to set the connector as the default connector. If you configure an external server to be the default authentication connector, local authentication is disabled, and users can be authenticated for login only by using that external AAA authentication server.
Default Shell Connector	(For releases 22.1.4 and later.) For RADIUS and TACACS+ servers, click to set the connector as the default shell connector. This can be the same server as the default connector, or it can be a different server. The default shell connector authenticates users logging in using the shell, and the server that you configure as the default connector authenticates GUI logins and API calls.

4. Click the Add icon to add a connector.
    a. For Active Directory, LDAP, RADIUS, or TACACS+, in the Add Details popup window, enter information for the following fields. Note that the fields displayed depend on the type of external authentication server. The following screenshot is for Active Directory. Note that for a single authentication connector, you can configure only one type of authentication, either Active Directory, LDAP, RADIUS, or TACACS+. All authentication servers work in an active–active manner. If one of them becomes unavailable, the system automatically switches to the next available one.

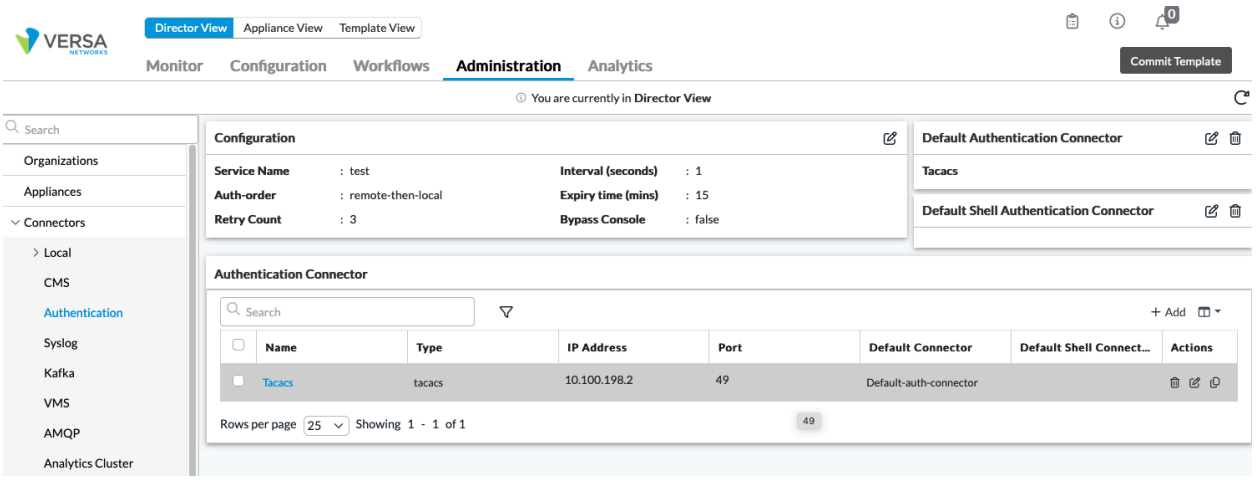


Field	Description
IP Address/FQDN	Enter the IP address or fully qualified domain name of the authentication server.
Port	Enter the port number on the server to connect to. For Active Directory, use one of the following port numbers to connect to global catalog: ▪ 3268—Connect to the global catalog server. ▪ 3269—Connect securely to the global catalog server.
Secret String	For RADIUS and TACACS+, enter the password to access the authentication server. Do not include the following characters in the password: [ ] ; : \
Bind DN	For Active Directory and LDAP server, enter the bind domain name.
Bind Credentials	For Active Directory and LDAP, enter the bind domain password.
Base DN	For Active Directory and LDAP, enter the bind domain name.
Secure	For Active Directory, click to enable secure connectivity to the Active Directory server. In the popup window, click Choose File and browse for the SSL certificate, which must be in .pem format. Then click Upload.

b. (For Releases 22.1.3 and later.) For central authentication, in the Add Details popup window, enter the IP address of the central authentication Director node. For high availability Director nodes, enter the IP addresses of the active and standby Director nodes, separated by a comma.



5. Click OK. The Authentication Connectors pane displays the configured authentication connectors.



Configure Default Authentication Connectors

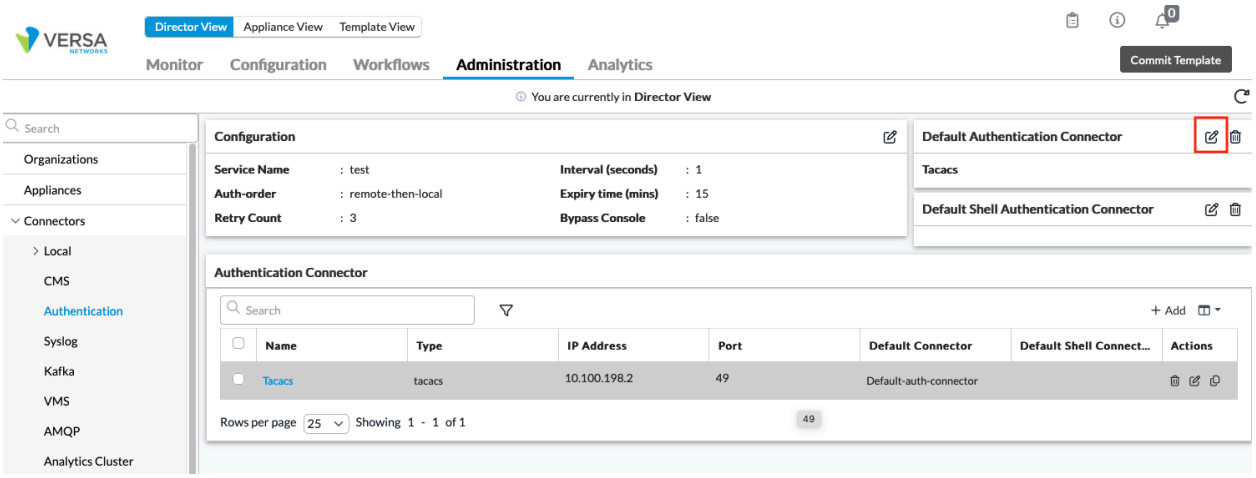
You can configure an external server to be the default authentication connector. If you do this, local authentication is disabled, and users can be authenticated for login only by using an external AAA authentication server.

For releases 22.1.4 and later, you can configure an external RADIUS or TACACS server to authenticate users logging in to the Director node using the shell. This can be the same server as the default authentication connector, or it can be a different server. The default shell connector authenticates users logging in using the shell, and the server that you configure as the default connector authenticates GUI logins and API calls.

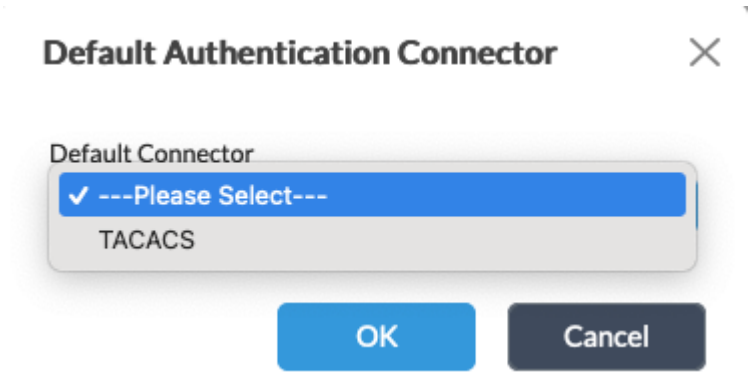
To configure an external server as a default authentication connector:

1. In Director view, select the Administration tab in the top menu bar.

2. Select Connectors > Authentication in the left menu bar.
3. Click the name of the server in the Authentication Connectors pane and select the Default Connector field, or click the Edit icon in the Default Connector pane.

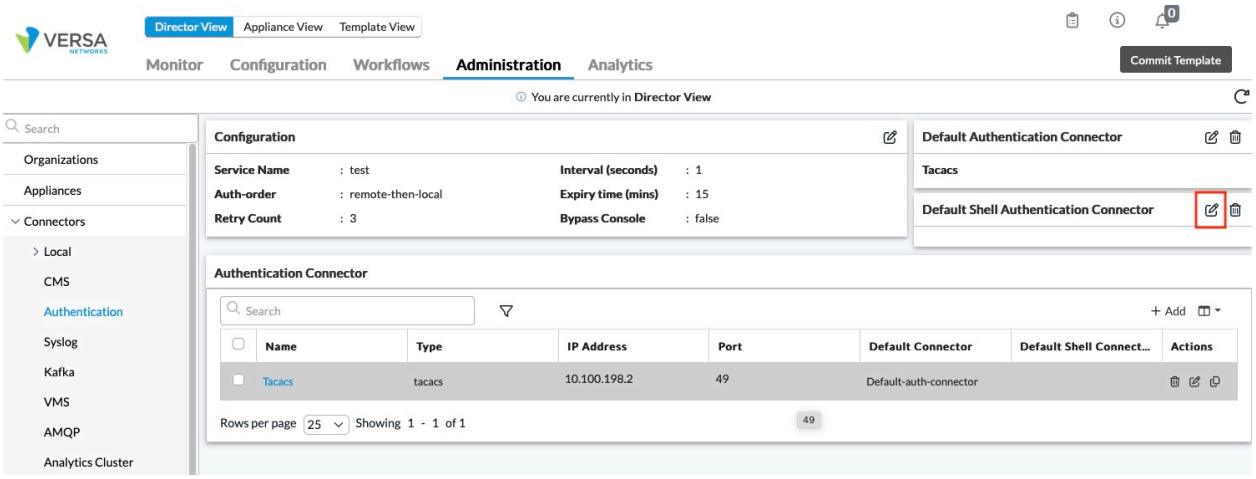


4. In the Default Connector field, select the connector, and then click OK.

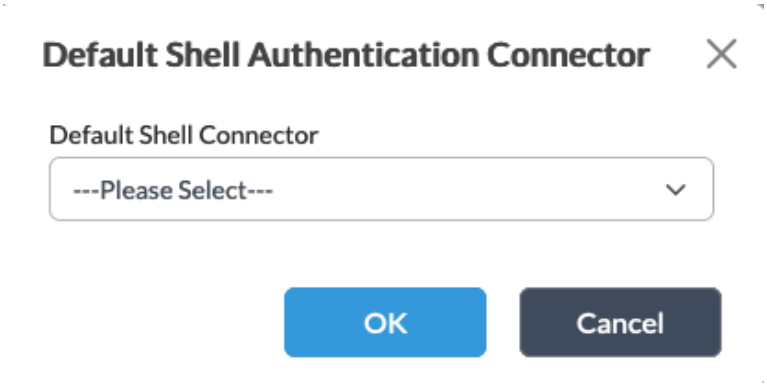


5. To configure a RADIUS or TACACS+ server as the default shell authentication connector, click the name of the server in the Authentication Connectors pane and select the Default Shell Connector field, or click the Edit icon in the Default Shell Connector pane.

Updated: Thu, 24 Oct 2024 10:45:19 GMT

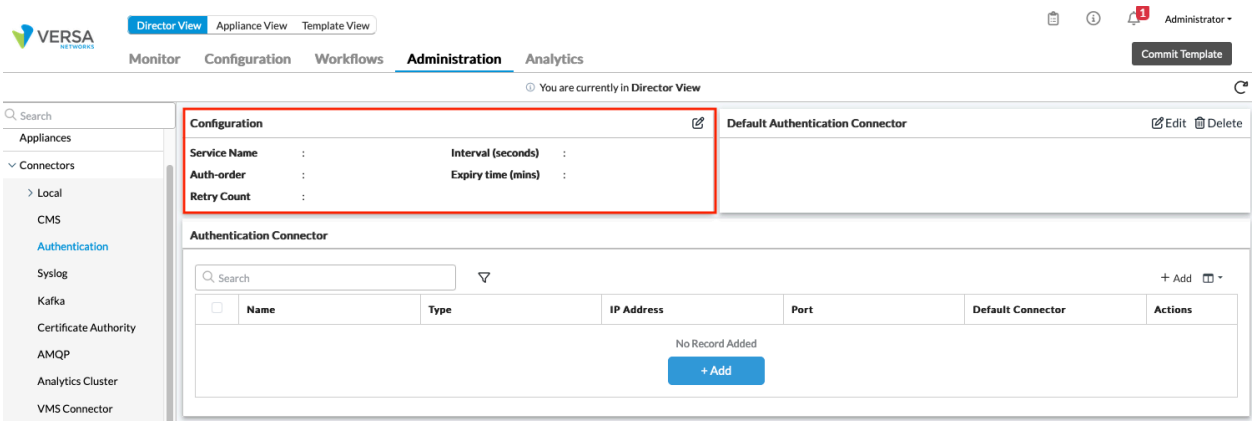


6. In the Default Shell Connector field, select the connector, and then click OK.

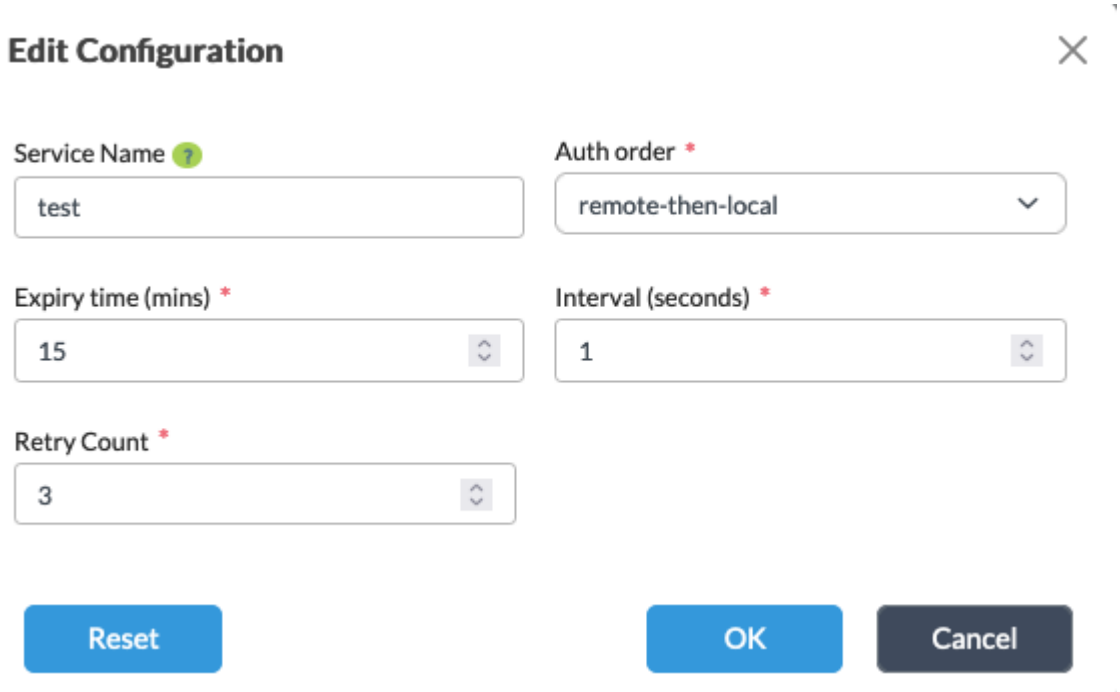


Rename the Default Connector

1. In Director view, select the Administration tab in the top menu bar.
2. Select Connectors > Authentication in the left menu bar.
3. In the Configuration pane, click the Edit icon.



4. In the Edit popup window, enter information for the following fields.



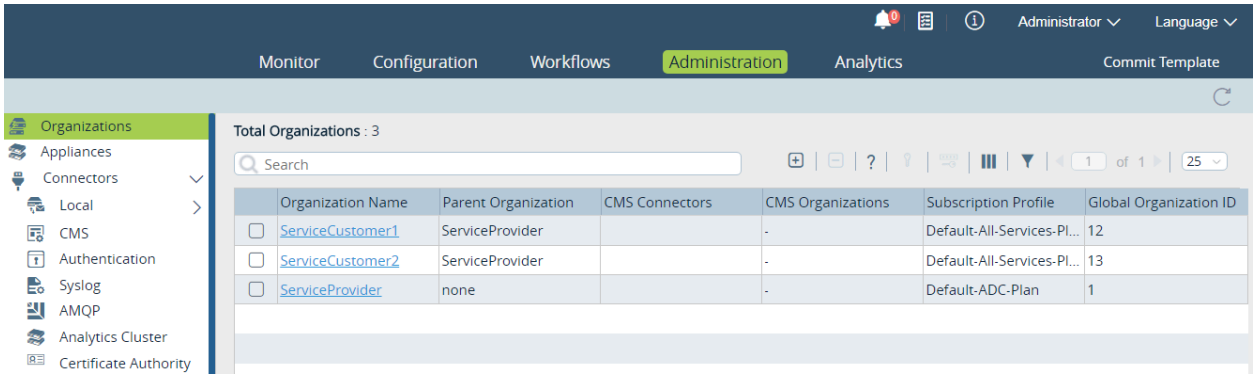
Field	Description
Service Name	For TACACS+, enter the external server service name that has vendor-specific attributes. By default, the service name is "test."
Authentication Order	Select the authentication order: ◦ local-then-remote—Allow a user to log in directly to the Director node, authenticating the user based on a local username and password database. ◦ remote-then-local—Use a remote AAA authentication server to log in to the Director node.
Expiry Time	Enter the expiration time for retrying authentication, in minutes. *Default:* 15 minutes *Range:* 1 through 1440

Field	Description
Interval	Enter the sleep time between retries, in seconds. *Default:* 1 second
Retry Count	Enter number of retries before marking the server unreachable. *Default:* 3

5. Click OK.

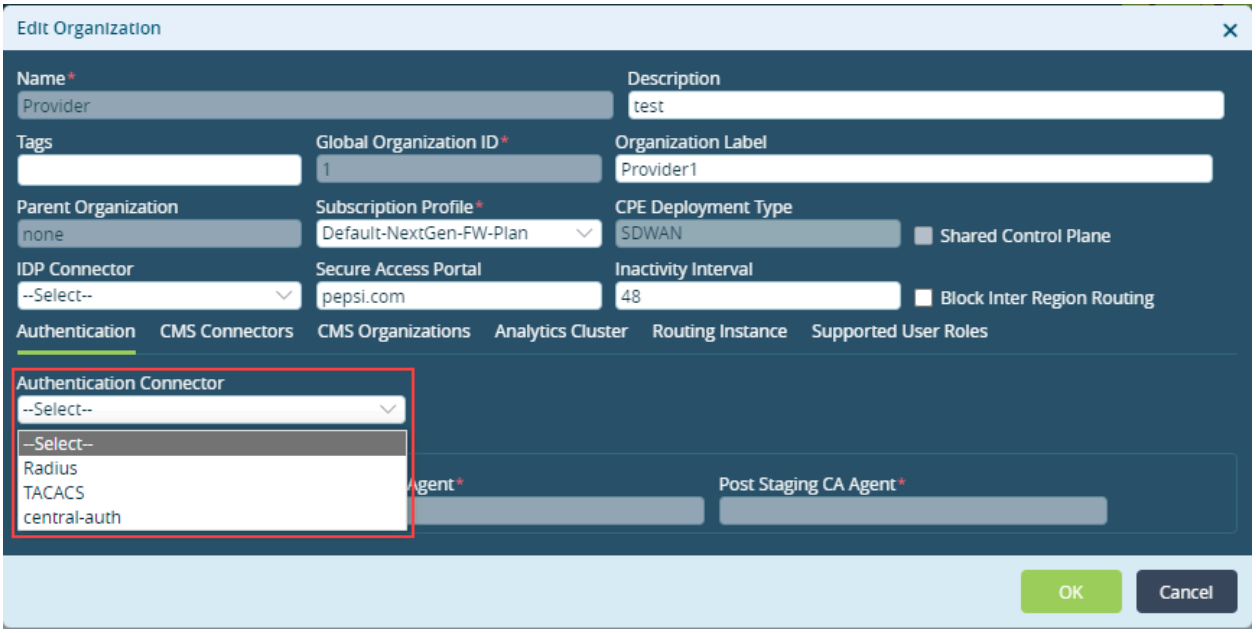
Associate an Authentication Connector with an Organization

1. In Director view, select the Administration tab in the top menu bar.
2. Select Organizations in the left menu bar.



3. Select an organization in the main pane. The Edit Organization popup window displays.

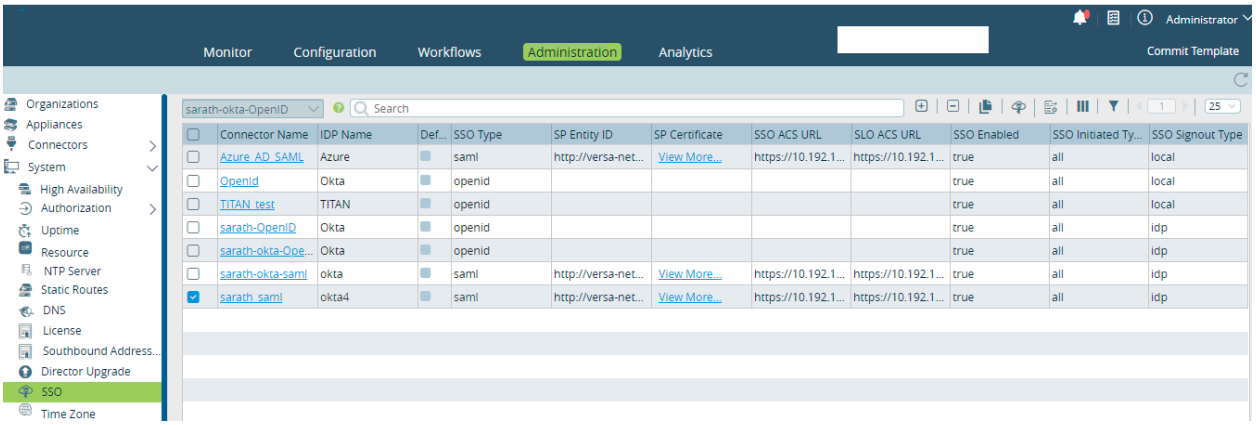
Updated: Thu, 24 Oct 2024 10:45:19 GMT



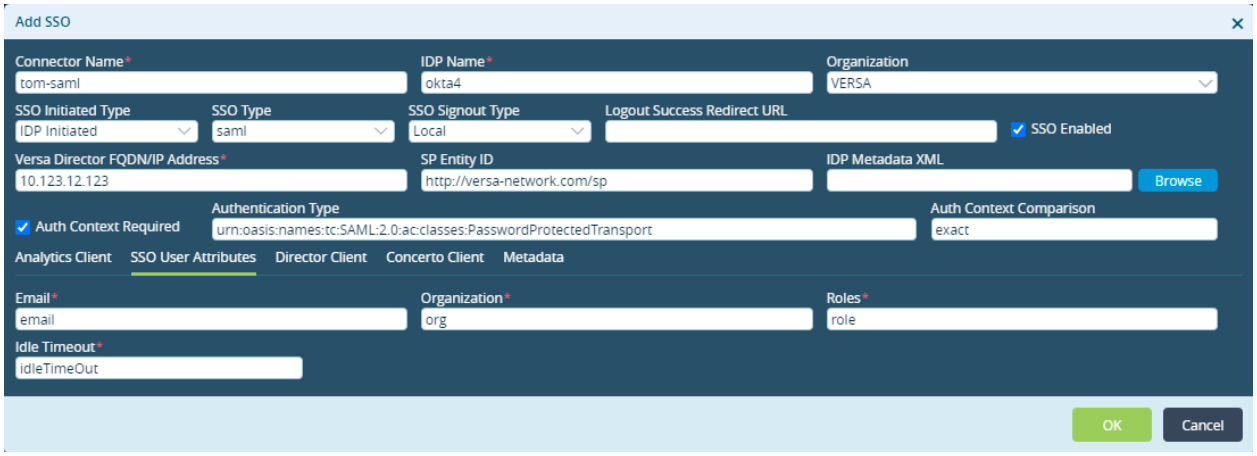
4. Select the Authentication tab.
5. in the Authentication Connector field, select the server type.
6. Click OK.

Configure an SSO Connector

1. In Director view, select the Administration tab in the top menu bar.
2. Select System > SSO in the left menu bar. The main pane displays the currently configure SSO connectors.



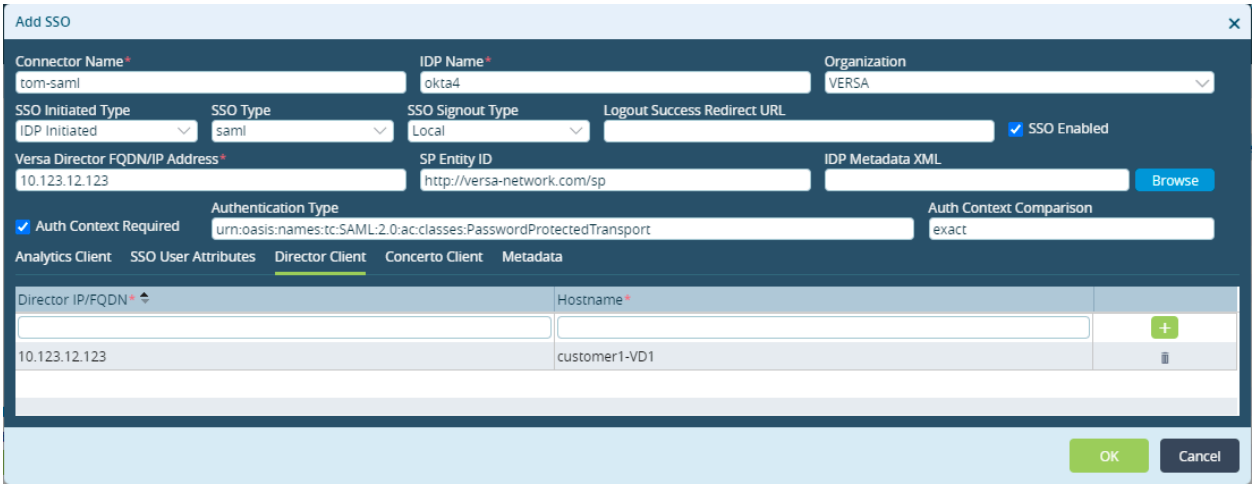
3. Click the Add icon. In the Add SSO popup window, enter information for the following fields.



Field	Description
Connector Name (Required)	Enter a name for the connector.
IDP Name (Required)	Enter a name for the IDP service.
Organization	Select the name of the organization.
SSO Initiated Type	Select the SSO initiator: ◦ All ◦ IDP Initiated ◦ SP Initiated
SSO Type	Select the SSO type markup language: ◦ OpenID—OpenID is an open-standard data format for exchanging authenticati provider and a service provider. ◦ SAML—SAML is an XML-based, open-standard data format for exchanging au identity provider and a service provider.
SSO Signout Type	Select the SSO signout type: ◦ Local—Only the SP session is cleared. ◦ IDP—Both the SP and the IDP sessions are cleared.
Logout Success Redirect URL	Enter the URL to which to be redirected after successful IDP logout.
SSO Enabled	Click to enable SSO.
Versa Director FQDN/IP Address	Enter the FQDN or IP address of Director node to which to connect.

Field	Description
(Required)	
SP Entity ID	Enter the entity ID of the service provider (that is, the VOS device).
IDP Metadata XML	Click Browse and select the IDP (Okta, in this case) metadata. This is generated fr
Authentication Context Required (Group of Fields)	(For Releases 22.1.3 and later.) Click to set the authentication type and context co
◦ Authentication Type	Enter the type of authentication that the IDP is using. The default value is urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport. The Passw principal authenticates to an authentication authority through the presentation of a
◦ Authentication Context Comparison	Enter the comparison to use for the authentication: ◦ exact—Authentication context in the authentication statement must exactly ma ◦ minimum—Authentication context in the authentication statement must be as s contexts.
SSO User Attribute Tab	The following attribute fields must be the same as the user configured in IDP: ◦ Email ◦ Idle Timeout ◦ Organization ◦ Roles

4. (For Releases 22.1.3 and later.) To configure the Director client, click the Director Client tab, and then enter information for the following fields.



Updated: Thu, 24 Oct 2024 10:45:19 GMT

Field	Description
Director IP/FQDN	Enter the FQDN or IP address of Director node to which to connect.
Hostname	Enter the hostname of Director node to which to connect. Click Add icon.

5. Click OK.

Configure User Authorization

Each user action that an authenticated user can perform on a Director node must be authorized. The Director software provisions two user types, provider and tenant (or organization). Each user type has different roles that determine the access level for individual users. When you create a user, you assign them to the desired role. You can use a preconfigured role or create a custom role.

The following preconfigured provider and tenant roles are available:

- Provider users
  - ProviderDataCenterAdmin—Super-admin role with no access to the certain system-level resources.
  - ProviderDataCenterOperator—Read-only access to all resources.
  - ProviderDataCenterSystemAdmin—Super-admin role with access to the entire Director system for all tenants.
- Tenant users
  - TenantDashboardOperator—Read-only access to the resources.
  - TenantOperator—Read-only access for the tenant to which the user belongs.
  - TenantSecurityAdmin—Can perform all security operations for the tenant to which the user belongs and can perform operations for features such as firewall, zones, and ZTP.
  - TenantSuperAdmin—Super-admin role that can perform all operations for the tenant.

The following table describes the resources accessible by the provider role.

Resource	Provider Data CenterAdmin	Provider Data CenterOperator	Provider Data CenterSystemAdmin
ADC_MANAGEMENT	X	X	X
ALARM_MANAGEMENT	X	X	X
AMQP_CONNECTOR_MANAGEMENT	X	X	X
ANALYTICS_CONNECTOR_MANAGEMENT	X	X	X

Resource	Provider Data CenterAdmin	Provider Data CenterOperator	Provider Data CenterSystemAdmin
ANALYTICS_MANAGEMENT	X	X	X
APPLIANCE_CONFIGURATION_MANAGEMENT	X	X	X
APPLIANCE_HA_MANAGEMENT	X	X	X
APPLIANCE_ORGANIZATION_ALG_MANAGEMENT	X	X	X
APPLIANCE_ORGANIZATION_AUTHENTICATION_PROFILE_MANAGEMENT	X	X	X
APPLIANCE_ORGANIZATION_DOT1X_MANAGEMENT	X	X	X
APPLIANCE_ORGANIZATION_LIMITS	X	X	X
APPLIANCE_ORGANIZATION_PROFILES_STORAGE_PROFILES	X	X	X
APPLIANCE_ORGANIZATION_RADIUS_SERVER_MANAGEMENT	X	X	X
APPLIANCE_ORGANIZATION_SETTINGS	X	X	X
APPLIANCE_ORG_MANAGEMENT	X	X	X
APPLIANCE_PROVIDER_USER_MANAGEMENT	X	X	X
APPLIANCE_SNMP_MANAGEMENT	X	X	X
APPLIANCE_SYSTEM_MANAGEMENT	X	X	X
APPLIANCE_TENANT_USER_MANAGEMENT	X	X	X
APPLICATION_CLIENT_MANAGEMENT	X	X	X
ASSET_MANAGEMENT	X	X	X
AUTH_CONNECTOR_MANAGEMENT	X	X	X
CGNAT_MANAGEMENT	X	X	X
CMS_CONNECTOR_MANAGEMENT	X	X	X
CONTROLLER_WORKFLOW_MANAGEMENT	X	—	X
COS_MANAGEMENT	X	X	X
CUSTOM_TEMPLATE_MANAGEMENT	X	—	X

Resource	Provider Data CenterAdmin	Provider Data CenterOperator	Provider Data CenterSystemAdmin
DATA_COLLECTION_MANAGEMENT	X	—	X
DEVICE_GROUP_MANAGEMENT	X	X	X
DEVICE_WORKFLOW_MANAGEMENT	X	X	X
DHCP_MANAGEMENT	X	X	X
DHCP_PROFILE_MANAGEMENT	X	X	X
DIRECTOR_INFO	X	X	X
DIRECTOR_MANAGEMENT	X	X	X
DNS_PROXY_MANAGEMENT	X	X	X
GLOBAL_TRANSPORT_DOMAIN_MANAGEMENT	X	X	X
HA_MANAGEMENT	X	X	X
HW_INVENTORY_MANAGEMENT	X	X	X
INVENTORY_MANAGEMENT	X	X	X
IPSEC_MANAGEMENT	X	X	X
LOG_EXPORT_MANAGEMENT	X	X	X
MONITOR_MANAGEMENT	X	X	X
NETWORK_ADMINISTRATION	X	X	X
NEXTGEN_FIREWALL_MANAGEMENT	X	X	X
NOTIFICATION_RULES_MANAGEMENT	X	X	X
ORGANIZATION_MANAGEMENT	X	X	X
ORG_WORKFLOW_MANAGEMENT	X	—	X
OS_SPACK_MANAGEMENT	X	X	X
PBF_MANAGEMENT	X	X	X
PROVIDER_USER_MANAGEMENT	X	X	X

Resource	Provider Data CenterAdmin	Provider Data CenterOperator	Provider Data CenterSystemAdmin
REGISTRATION_TOKEN_MANAGEMENT	X	X	X
SDWAN_GLOBAL_SETTINGS	X	X	X
SDWAN_MANAGEMENT	X	X	X
SDWAN_PROVIDER_MANAGEMENT	X	X	X
SECURE_ACCESS_MANAGEMENT	X	X	X
SECURITY_MANAGEMENT	X	X	X
SERVICE_CHAIN_MANAGEMENT	X	X	X
SERVICE_CHAIN_WORKFLOW_MANAGEMENT	X	X	X
SMTP_SMS_NOTIFICATION_MANAGEMENT	X	X	X
SNAPSHOT_MANAGEMENT	X	X	X
SPACK_MANAGEMENT	X	X	X
SPOKEGROUP_WORKFLOW_MANAGEMENT	X	X	X
SSO_MANAGEMENT	X	X	X
STATEFUL_FIREWALL_MANAGEMENT	X	X	X
SUBSCRIPTION_MANAGEMENT	X	X	X
SYSLOG_SERVER_MANAGEMENT	X	X	X
SYSTEM_SSL_CERTIFICATE_MANAGEMENT	X	—	X
TASKS_MANAGEMENT	X	X	X
TDF_MONITORING_MANAGEMENT	X	X	X
TEMPLATE_MANAGEMENT	X	X	X
TEMPLATE_WORKFLOW_MANAGEMENT	X	X	X
TENANT_USER_MANAGEMENT	X	X	X
TROUBLE_SHOOTING_MANAGEMENT	—	—	X

Resource	Provider Data CenterAdmin	Provider Data CenterOperator	Provider Data CenterSystemAdmin
UNKNOWN_DEVICE_MANAGEMENT	X	X	X
WAN_NETWORK_MANAGEMENT	X	X	X
WEB_PROXY_MANAGEMENT	X	X	X

The following table describes the resources accessible by the tenant (organization) role.

Resource	TenantDashboard Operator	TenantOperator	Tenant SecurityAdmin	Tenant SuperAdmin
ADC_MANAGEMENT	—	X	—	X
ALARM_MANAGEMENT	X	X	X	X
ANALYTICS_MANAGEMENT	X	X	X	X
APPLIANCE_CONFIGURATION_MANAGEMENT	X	X	X	X
APPLIANCE_HA_MANAGEMENT	—	X	—	X
APPLIANCE_ORGANIZATION_ALG_MANAGEMENT	X	X	—	X
APPLIANCE_ORGANIZATION_AUTHENTICATION_PROFILE_MANAGEMENT	X	X	—	X
APPLIANCE_ORGANIZATION_DOT1X_MANAGEMENT	X	X	—	X
APPLIANCE_ORGANIZATION_LIMITS	X	X	—	X
APPLIANCE_ORGANIZATION_PROFILES_STORAGE_PROFILES	X	X	—	X
APPLIANCE_ORGANIZATION_RADIUS_SERVER_MANAGEMENT	X	X	—	X
APPLIANCE_ORGANIZATION_SETTINGS	X	X	—	X
APPLIANCE_ORG_MANAGEMENT	—	X	—	X
APPLIANCE_PROVIDER_USER_MANAGEMENT	X	X	—	X
APPLIANCE_SNMP_MANAGEMENT	—	X	—	X
APPLIANCE_SYSTEM_MANAGEMENT	—	X	—	X
APPLIANCE_TENANT_USER_MANAGEMENT	X	X	—	X
ASSET_MANAGEMENT	—	X	—	X
CGNAT_MANAGEMENT	—	X	—	X
CMS_CONNECTOR_MANAGEMENT	—	X	—	X
COS_MANAGEMENT	—	X	—	X
DEVICE_GROUP_MANAGEMENT	—	X	—	X
DEVICE_WORKFLOW_MANAGEMENT	—	X	—	X

DHCP_MANAGEMENT	—	X	—	X
DHCP_PROFILE_MANAGEMENT	X	—	X	
DNS_PROXY_MANAGEMENT	X	—	X	
GLOBAL_TRANSPORT_DOMAIN_MANAGEMENT	X	—	X	
HW_INVENTORY_MANAGEMENT	X	—	X	
IPSEC_MANAGEMENT	—	X	—	X
LOG_EXPORT_MANAGEMENT	X	X	X	
MONITOR_MANAGEMENT	X	X	X	
NETWORK_ADMINISTRATION	X	—	X	
NEXTGEN_FIREWALL_MANAGEMENT	X	X	X	
NOTIFICATION_RULES_MANAGEMENT	X	—	X	
ORGANIZATION_MANAGEMENT	X	X	X	
ORG_WORKFLOW_MANAGEMENT	—	—	X	
OS_SPACK_MANAGEMENT	—	X	X	
PBF_MANAGEMENT	—	X	—	X
SDWAN_MANAGEMENT	—	X	—	X
SDWAN_PROVIDER_MANAGEMENT	X	—	X	
SECURE_ACCESS_MANAGEMENT	X	X	X	
SECURITY_MANAGEMENT	X	X	X	
SERVICE_CHAIN_MANAGEMENT	X	—	X	
SERVICE_CHAIN_WORKFLOW_MANAGEMENT	X	—	X	
SNAPSHOT_MANAGEMENT	X	—	X	
SPACK_MANAGEMENT	—	—	X	X
SPOKEGROUP_WORKFLOW_MANAGEMENT	X	—	X	
STATEFUL_FIREWALL_MANAGEMENT	X	X	X	
TASKS_MANAGEMENT	—	X	X	X

TDF_MONITORING_MANAGEMENT		X	—	X
TEMPLATE_MANAGEMENT		X	X	X
TEMPLATE_WORKFLOW_MANAGEMENT		X	—	X
TENANT_USER_MANAGEMENT		X	—	X
WAN_NETWORK_MANAGEMENT		X	—	X
WEB_PROXY_MANAGEMENT		X	X	X

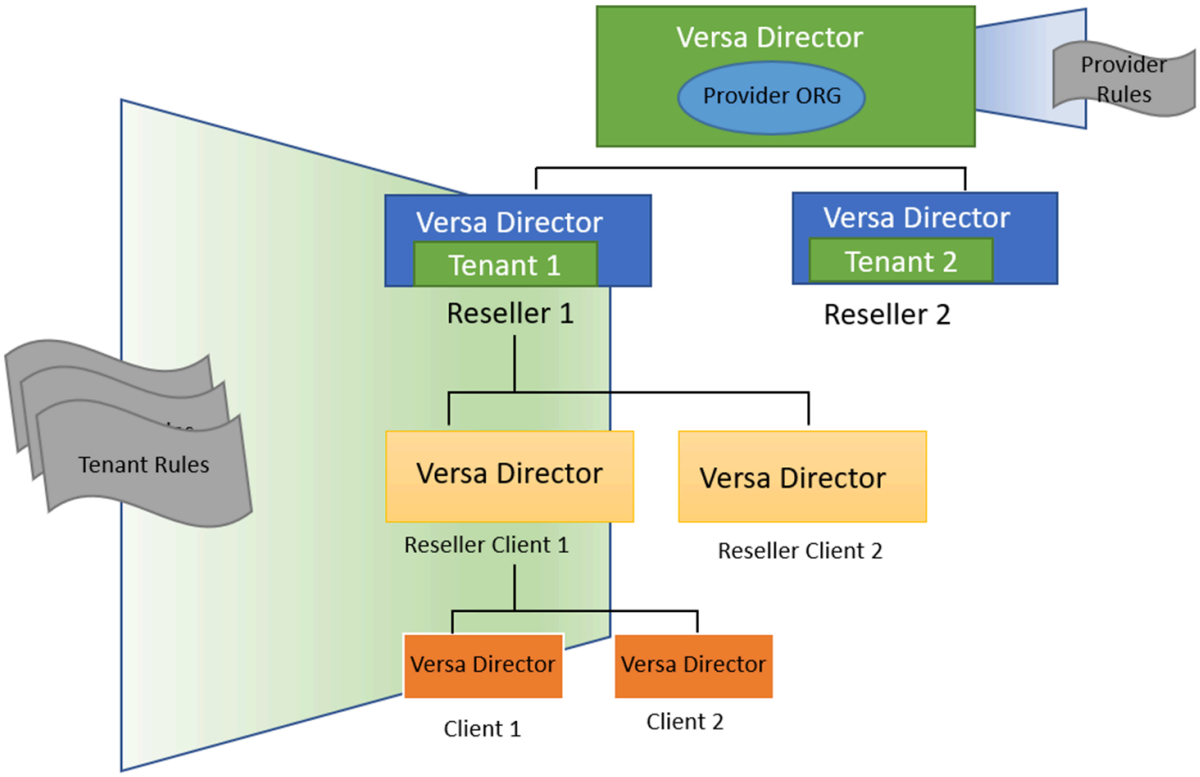
Configure RBAC

Versa Director is shipped with a default set of provider roles and tenant roles for use with role-based access control (RBAC). These provider roles and tenant roles are created by default when you create an organization in the Versa Director.

- Provider Roles—This is independent of the organization and tenant and can access other tenant information.
- Tenant Roles—This is specific to the tenant and has access to tenant specific information only.

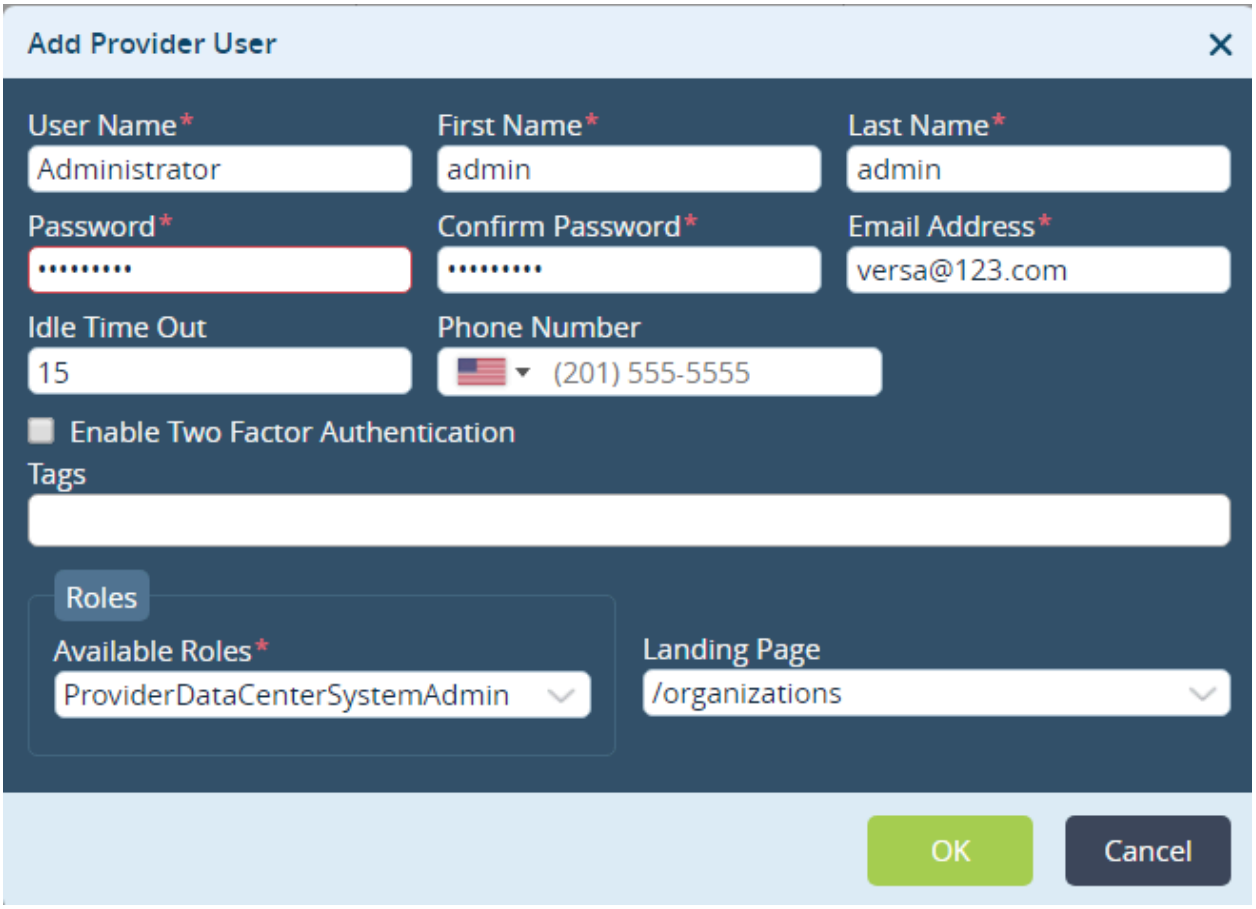
Multiple roles are created every time you create an organization on Versa Director. You can select the roles of interest when you are creating organizations and tenants.

The Director node supports multitenancy RBAC, which allows you to select the roles for a tenant and extend the same to all its subtenants.



Add Provider Users

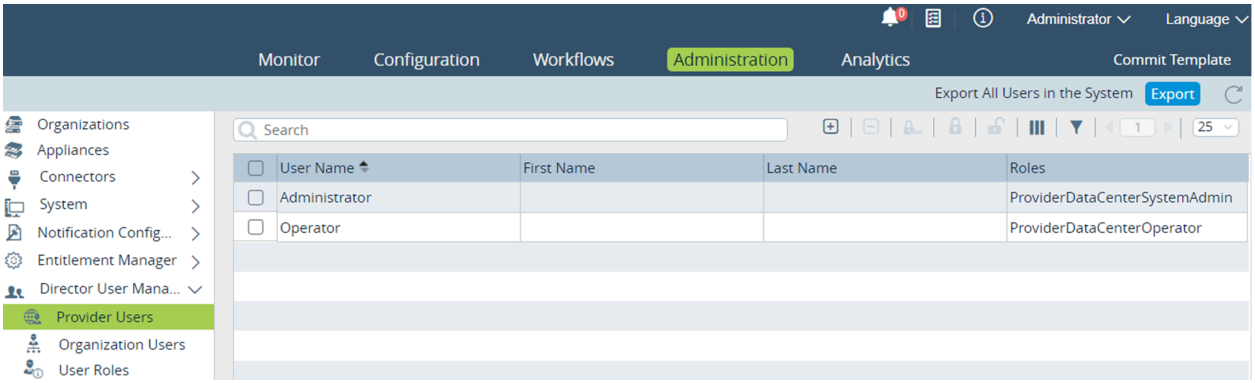
1. In Director view, select the Administration tab in the top menu bar.
2. Select Director User Management > Provider Users in the left menu bar.
3. Click the Add icon. In the Add Provider User popup window, enter information for the following fields.



Field	Description
Username	Enter the login name for the provider user.
First Name	Enter the first name of the provider user.
Last Name	Enter the last name of the provider user.
Password	Enter the password for the provider user.
Confirm Password	Re-enter the password for the provider user.
Email Address	Enter the email address of the provider user
Idle Time Out	Enter the duration after which the login session expires, in minutes. *Range:* 15 through 1440 minutes (24 hours) *Default:* 15 minutes
Phone Number	Enter the contact telephone number of the provider user.

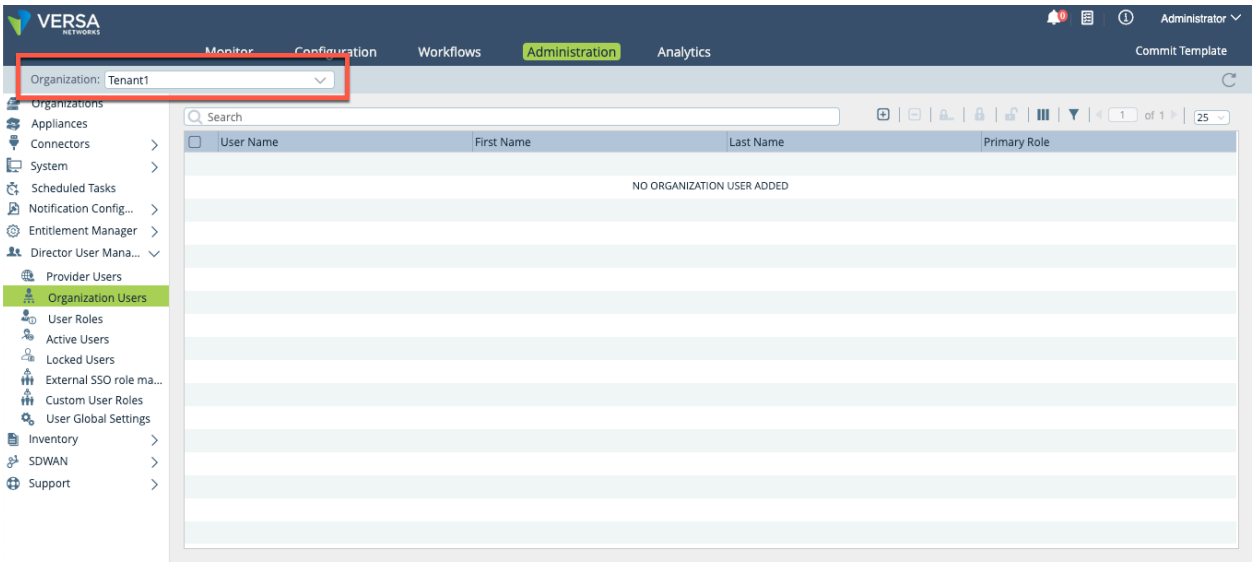
Field	Description
Roles (Group of Fields)	
◦ Available Roles	Select the role to assign to the provider user.
Landing Page	Select the first page to appear when the provider user logs int o the application.

3. Click OK. The main pane displays the provider user and their assigned role.



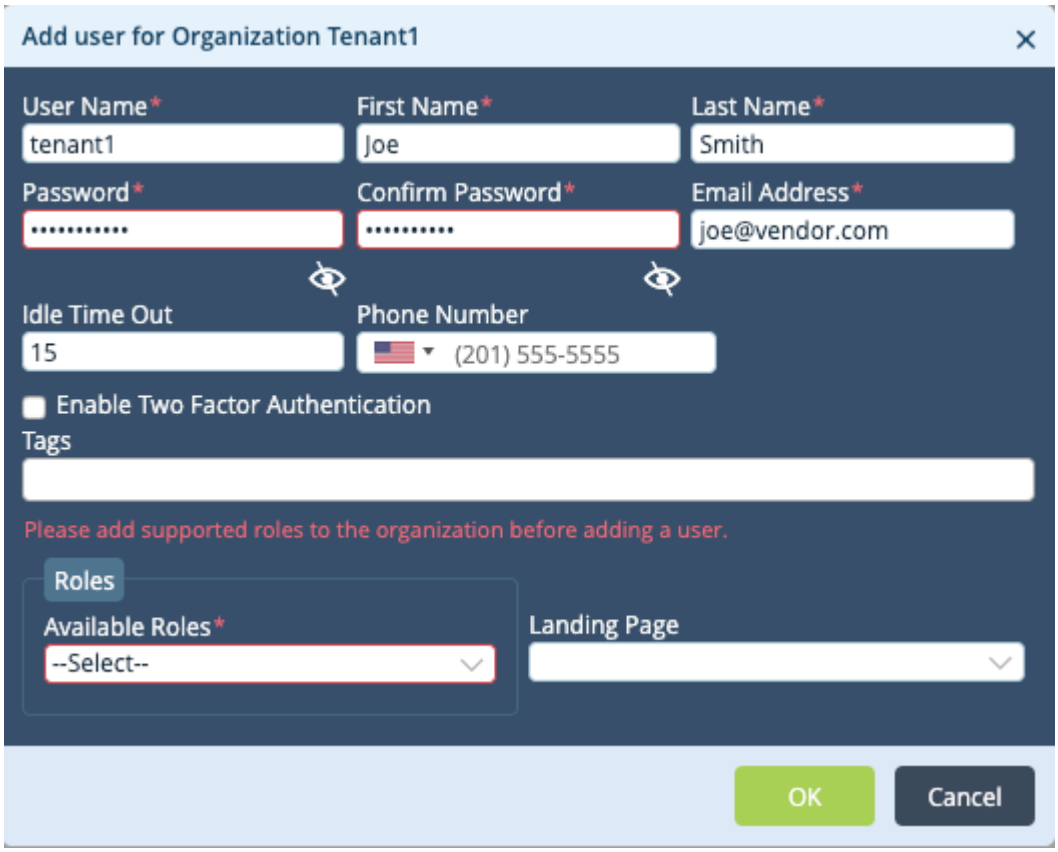
Add Tenant (Organization) Users

1. In Director view, select the Administration tab in the top menu bar.
2. Select an organization in the horizontal menu bar.
3. Select Director User Management > Organization Users in the left menu bar.



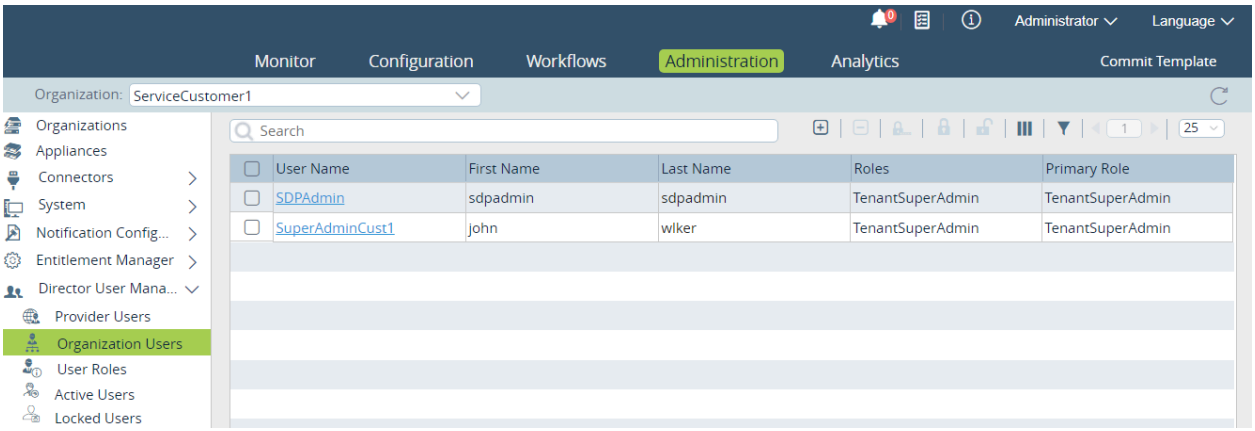
Updated: Thu, 24 Oct 2024 10:45:19 GMT

4. Click the Add icon. In the Add User for Organization popup window, enter information for the following fields.



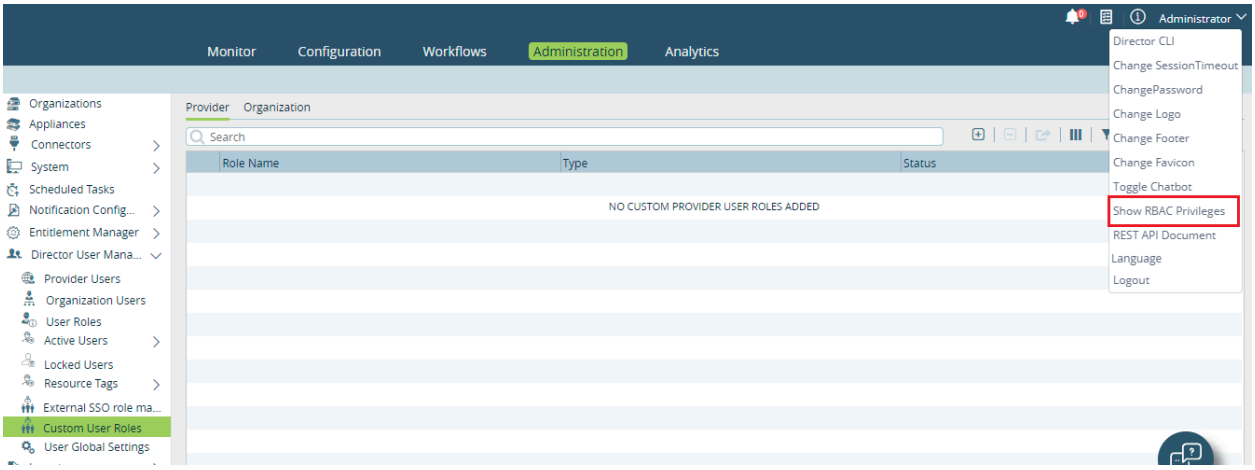
Field	Description
Username	Enter the username for the tenant user.
First Name	Enter the first name of the tenant user.
Last Name	Enter the last name of the tenant user.
Password	Enter the password for the tenant user.
Confirm Password	Re-enter the password for the tenant user.
Email Address	Enter the email address of the tenant user
Idle Time Out	Enter the duration after which the login session expires, in minutes. *Range:* 15 through 1440 minutes (24 hours) *Default:* 15 minutes
Enable Two-Factor Authentication	Click to enable or disable two-factor authentication of the user.
Roles (Group of Fields)	
◦ Available Roles	Select the role to assign to the tenant user. You cannot create organization or tenant users if you do not select RBAC roles. For more information, see Configure RBAC. For information about associating roles with a tenant, see Associate Roles with a Tenant or Organization.
Landing Page	Select the first page to appear when the tenant user logs in to the application.

5. Click OK. The main pane displays the tenant (organization) user and their assigned role.

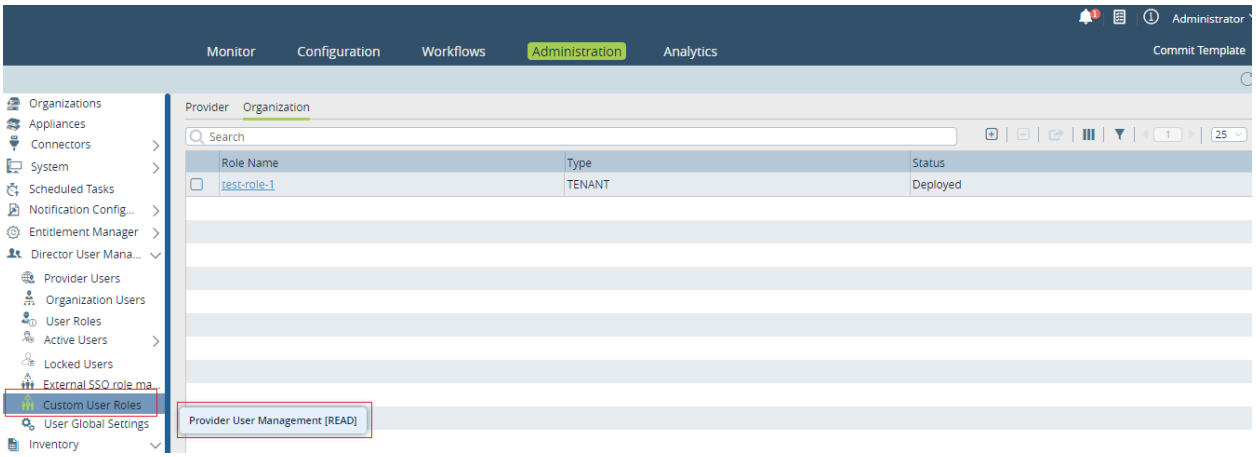


Display RBAC Privileges

1. Log in to the Director as the user Administrator.
2. In the Administrator user drop-down, select Show RBAC Privileges.



3. In the left menu bar, hover the cursor over a menu item to display the privileges for that option. For example:



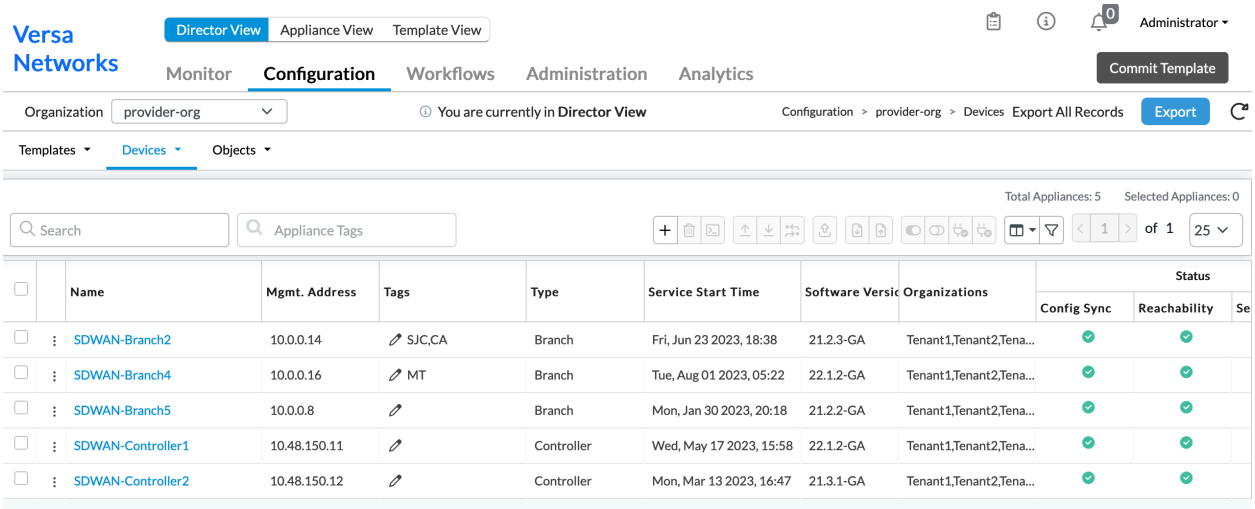
4. To hide the display of RBAC privileges, select Hide RBAC Privileges in the Administrator user drop-down.

To configure custom provider and tenant user roles, see Configure Custom User Roles, below.

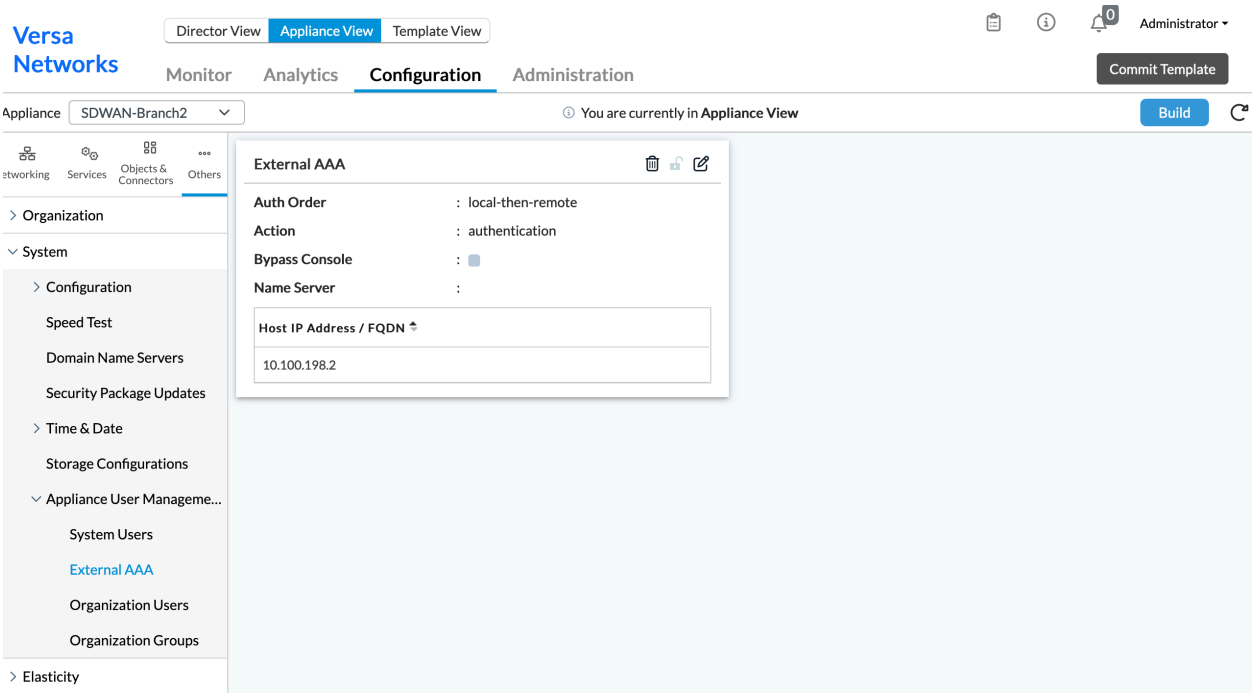
Configure External AAA for a Device

To configure external authentication, authorization, and accounting (AAA) for a device:

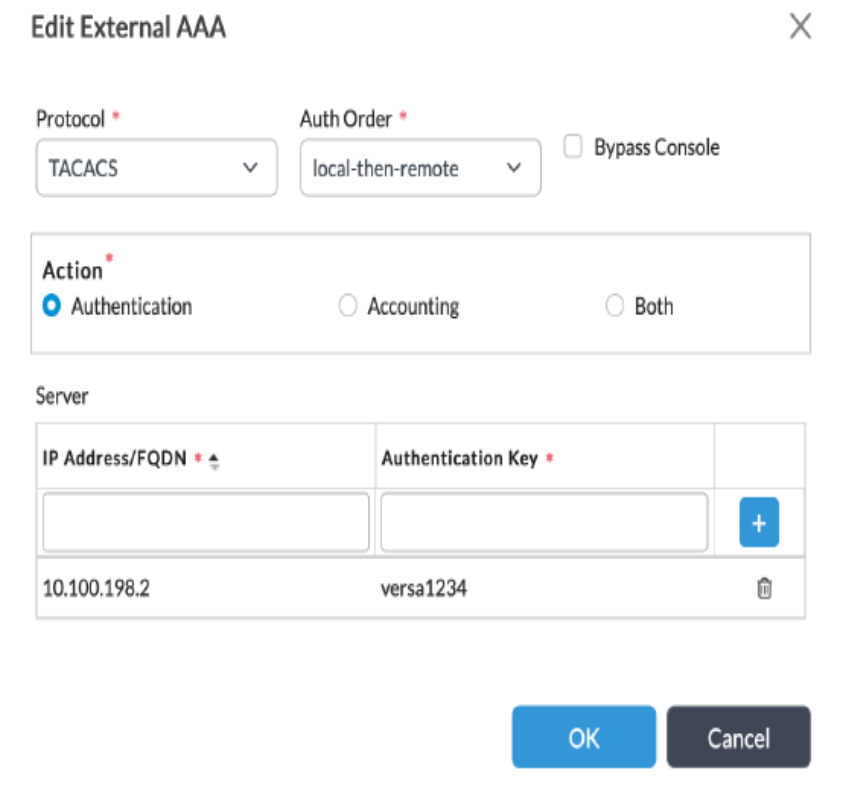
1. In Director view:
   a. Select the Configuration tab in the top menu bar.
   b. Select Devices > Devices in the horizontal menu bar.
   c. Select a device in the main pane. The view changes to Appliance view.



2. Select the Configuration tab in the top menu bar.
3. Select Others > System > Appliance User Management > External AAA in the left menu bar.



4. Click the Edit icon. In the Edit External AAA popup window, enter information for the following fields.



Field	Description
Protocol	Select the protocol: ◦ RADIUS ◦ TACACS+
Authentication Order	Select the authentication order: ◦ local-then-remote—Allow a user to log in directly to the Director node, authenticating the user based on a local username and password database. ◦ remote-then-local—Use a remote AAA authentication server to log in to the Director node.
Bypass Console	(For Releases 22.1.2 and later.) Click to bypass external authentication for console login.
Action	Click to select the AAA action: ◦ Accounting ◦ Authentication ◦ Both
Server (Group of Fields)	
◦ Key	Enter the password to use to access the server.
◦ IP Address	Enter the IP address of the server.

5. Click OK.

Configure Users and Roles

You can configure Director users and assign them roles using RADIUS, TACACS+, or LDAP. This section provides sample configurations that show the file information required for each server type.

Note: The vendor ID assigned for Versa Network is 42359. It is recommended that you use this ID whenever a third-party RADIUS vendor looks for the vendor ID attribute for its RADIUS configuration. This is not a Versa Director configuration requirement.

RADIUS

```
Alex Cleartext-Password:= "admin123"
   Versa-Role= "TenantSuperAdmin",
   Versa-Tenant= Customer1,
   Versa-GUI-Idle-TimeOut= 20

Tony Cleartext-Password:= "admin123"
   Versa-Role= "TenantOperator",
   Versa-Tenant= Customer1,
   Versa-GUI-Idle-TimeOut= 20

Andy Cleartext-Password:= "admin123"
   Versa-Role= "TenantSecurityAdmin",
   Versa-Tenant= Customer1,
   Versa-GUI-Idle-TimeOut= 20

Clark Cleartext-Password:= "admin123"
   Versa-Role= "ProviderDataCenterAdmin",
   Versa-GUI-Idle-TimeOut= 20

Bill Cleartext-Password:= "admin123"
   Versa-Role= "ProviderDataCenterOperator",
   Versa-GUI-Idle-TimeOut= 20

Suri Cleartext-Password:= "admin123"
   Versa-Multi-Tenant-Roles= "Customer1:TenantSuperAdmin;Customer2:TenantOperator",
   Versa-GUI-Idle-TimeOut= 20
```

TACACS+

```
group = TenantSuperAdminGroup {
   login = PAM
   service = test{
      Versa-Role = "TenantSuperAdmin"
      Versa-Tenant = "Galaxy-Foods"
      Versa-GUI-Idle-TimeOut = "300"
      }
}

group = TenantOperatorGroup {
   login = PAM
   service = test {
      Versa-Role = "TenantOperator"
      Versa-Tenant = "Galaxy-Foods"
      Versa-GUI-Idle-TimeOut = "300"
      }
}

group = TenantSecurityAdminGroup {
   login = PAM service = test {
      Versa-Role = "TenantSecurityAdmin"
```

```
        Versa-Tenant = "Galaxy-Foods"
        Versa-GUI-Idle-TimeOut = "300"
        }
}

group = ProviderDataCenterAdminGroup {
    login = PAM
    service = test {
        Versa-Role = "ProviderDataCenterAdmin"
        Versa-GUI-Idle-TimeOut = "300"
        }
}

group = ProviderDataCenterOperatorGroup {
    login = PAM service = test {
        Versa-Role = "ProviderDataCenterOperator"
        Versa-GUI-Idle-TimeOut = "300"
        }
}
```

LDAP

Configuring Roles

```
dn: cn=ProviderDataCenterAdmin,ou=Roles,dc=test,dc=com
objectClass: top
objectClass: organizationalRole
cn: ProviderDataCenterAdmin

dn: cn=TenantSuperAdmin,ou=Roles,dc=test,dc=com
objectClass: top
objectClass: organizationalRole
cn: TenantSuperAdmin

dn: cn=ProviderDataCenterOperator,ou=Roles,dc=test,dc=com
objectClass: top
objectClass: organizationalRole
cn: ProviderDataCenterOperator

dn: cn=TenantSecurityAdmin,ou=Roles,dc=test,dc=com
objectClass: top
objectClass: organizationalRole
cn: TenantSecurityAdmin

dn: cn=TenantOperator,ou=Roles,dc=test,dc=com
objectClass: top
objectClass: organizationalRole
cn: TenantOperator
```

Configuring Tenants

```
dn: ou=testOrg,ou=Tenants,dc=test,dc=com
```

```
objectClass: top
objectClass: organizationalUnit
ou: testOrg
```

Configuring Users

```
dn: cn=org1_user,ou=Users,dc=test,dc=com
objectClass: top
objectClass: person
objectClass: organizationalPerson
cn: org1_user
sn: org1
ou: cn=TenantSuperAdmin,ou=Roles,dc=test,dc=com
userPassword:: e21kNX1OeGJycGpNVXE3K0hJOWVTdi9Jb0lRPT0=
```

Active Directory

Create groups in Active Directory with prefixes for group names that indicate the type of group, such as Versa Role or Versa Tenant.

For example:

- For a tenant named Org1, provide the group name as Versa Tenant - Org1.
- For the role TenantSuperAdmin, provide group name as Versa Role - TenantSuperAdmin.

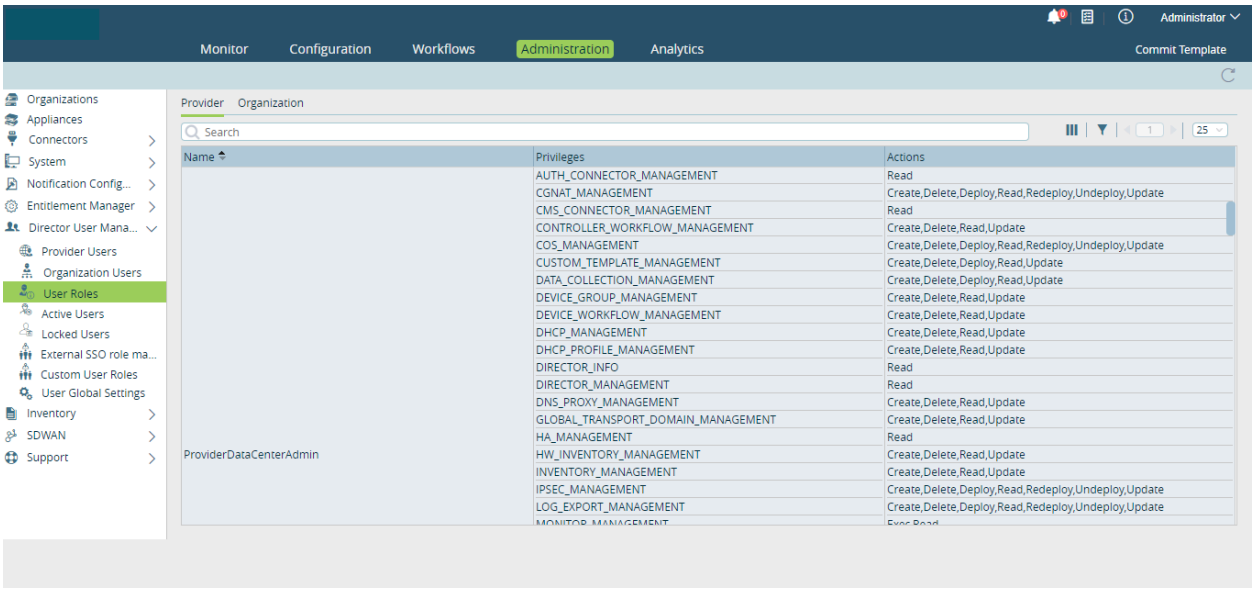
The older format of group names (without prefixes) is also supported.

View User Roles

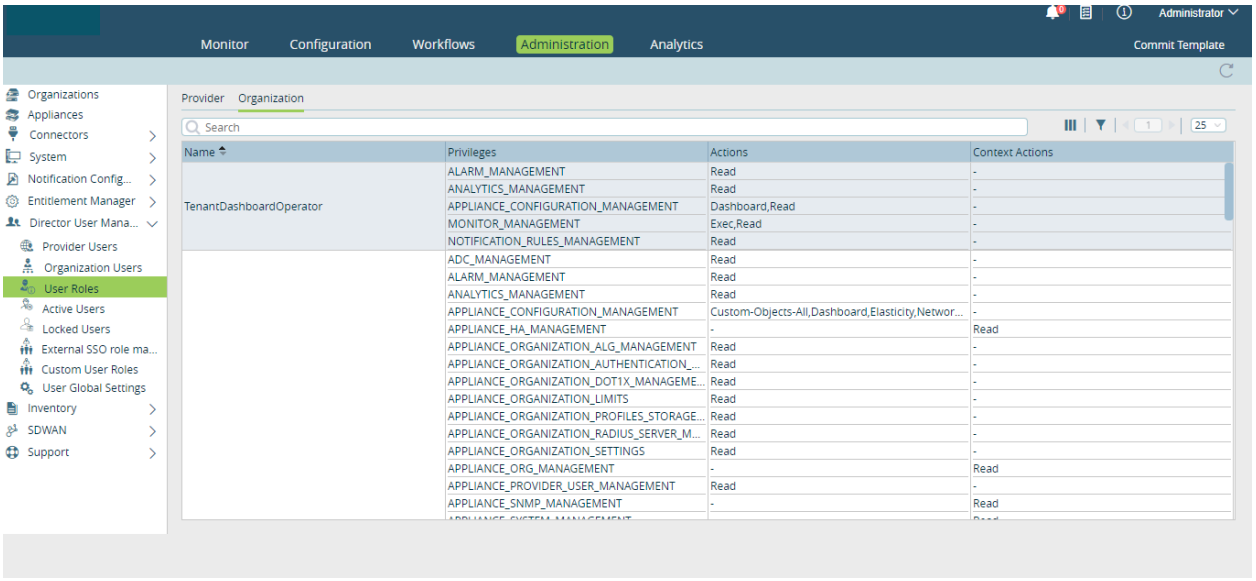
You can view the provider and tenant (organization) user roles, privileges, and actions each user can perform.

To view the user roles:

1. In Director view, select the Administration tab in the top menu bar.
2. Select Director User Management > User Roles in the left menu bar.
3. To view provider user roles, select the Provider tab in the horizontal menu bar.



4. To view tenant (organization) user roles, select the Organization tab in the horizontal menu bar.



View Active Users

To view users who are actively accessing the Director node:

1. In Director view, select the Administration tab in the top menu bar.

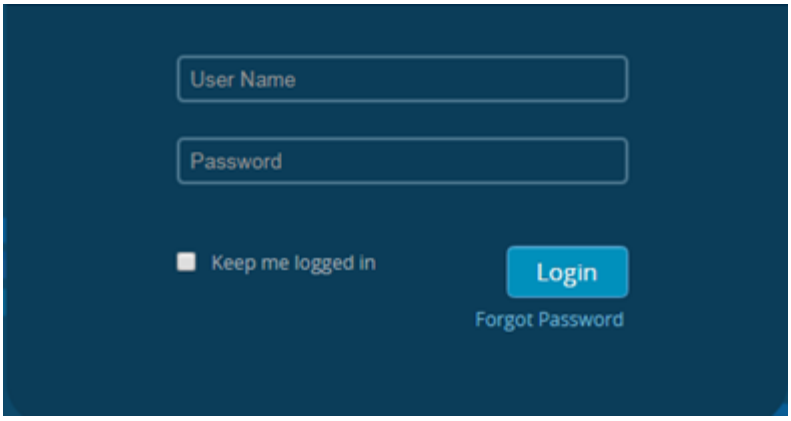
2. Select Director User Management > Active Users in the left menu bar.

Log Out Active Users

To log out an active user from the Director node:

1. In Director view, select the Administration tab in the top menu bar.
2. Select Director User Management > Active Users in the left menu bar.
3. Click the checkbox of the user to log out.

4. Click the Force Logout icon. The active user is logged out, and their login screen displays:



Unlock Users

To unlock a user who has been previously locked out of the Director node:

1. In Director view, select the Administration tab in the top menu bar.
2. Select Director User Management > Locked Users in the left menu bar.
3. Select the checkbox of the user to unlock.

4. Click the Unlock icon.

Configure Resource Tags

For Releases 22.1.1 and later.

For each provider and tenant role, you can configure RBAC resource tags to filter resources such as devices, templates, and device and template workflows. Resource tags allow you to group resources logically and control resources that

belong to the same tenant.

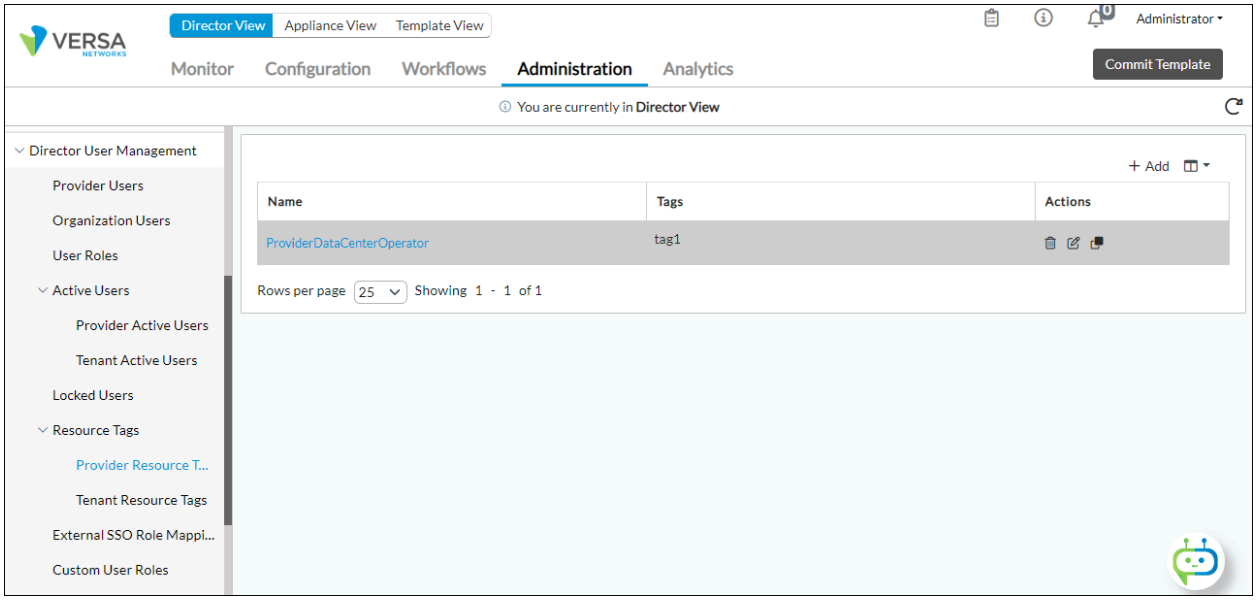
For example, if different user roles are defined to control access to East-Coast and West-Coast devices or templates, a user whose role is East-Coast cannot access any West-Coast devices, and a user whose role is West-Coast cannot access any East-Coast devices. You can define a tag name for the desired role, such as TenantSuperAdmin, and then specify the same tag name for all East-Coast and West-Coast resources, such as devices, templates, and device and template workflows, so that all the objects are logically grouped. Then you apply RBAC on the logical grouping tag.

A resource tag can have multiple names so that same resource can be part of multiple logical groups.

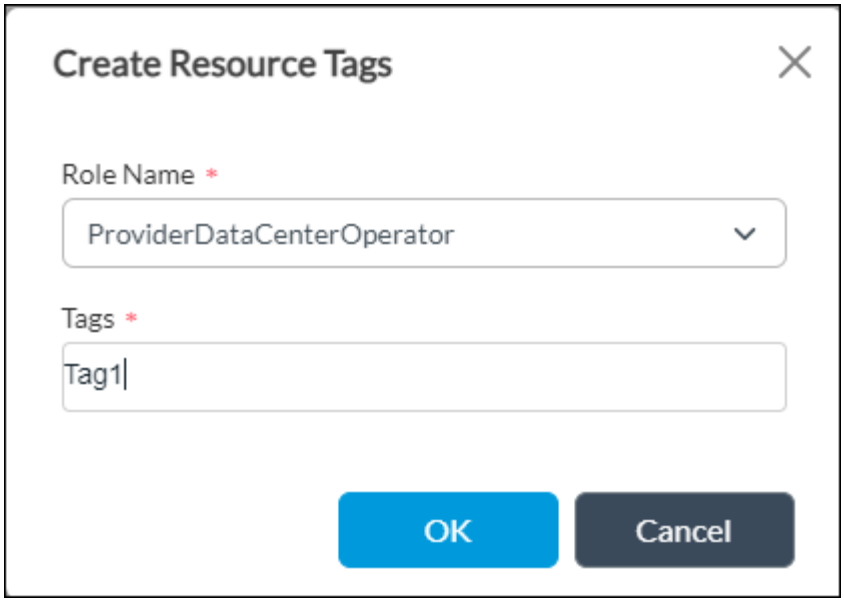
Note: If a user role is configured with no resource tags, the user role can access all resources within its tenant hierarchy. However, if a user role is configured with a resource tag, the user role can access only the resources that match the resource tag.

Configure Resource Tags for Provider Users

1. In Director view, select the Administration tab in the top menu bar.
2. Select Director User Management > Resource Tags > Provider Resource Tags in the left menu bar.



3. Click + Add. In the Create Resource Tags popup window, enter information for the following fields.

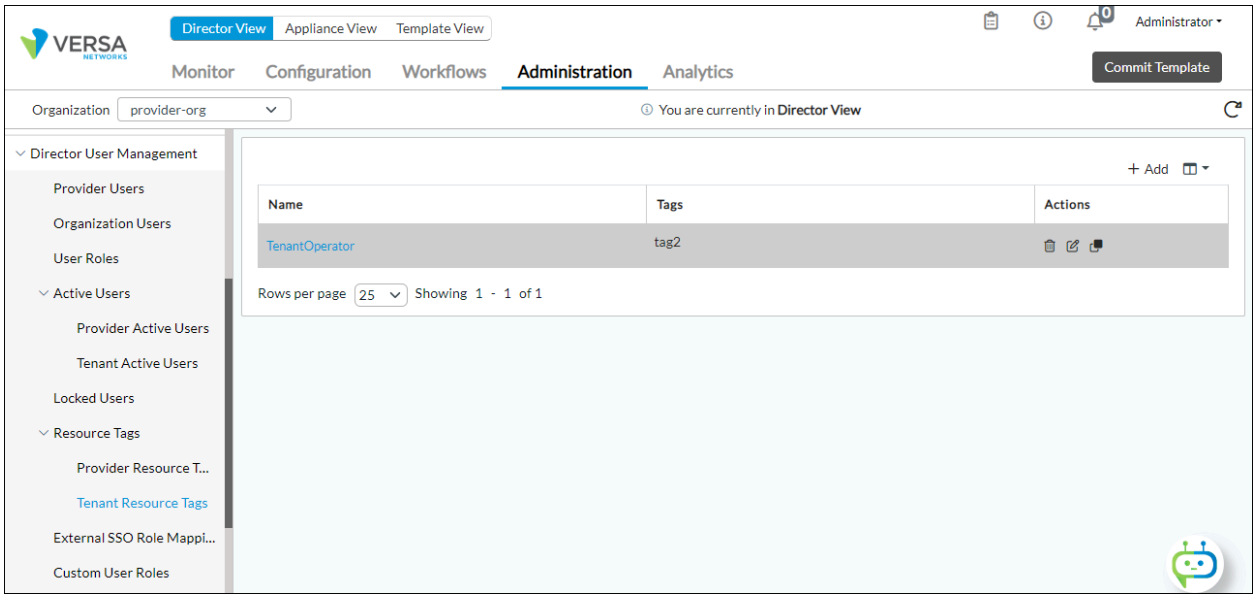


Field	Description
Role Name (Required)	Select a provider role name.
Tags (Required)	Enter one or more names for the resource tag. A resource tag that has multiple names can be part of multiple resource groups.

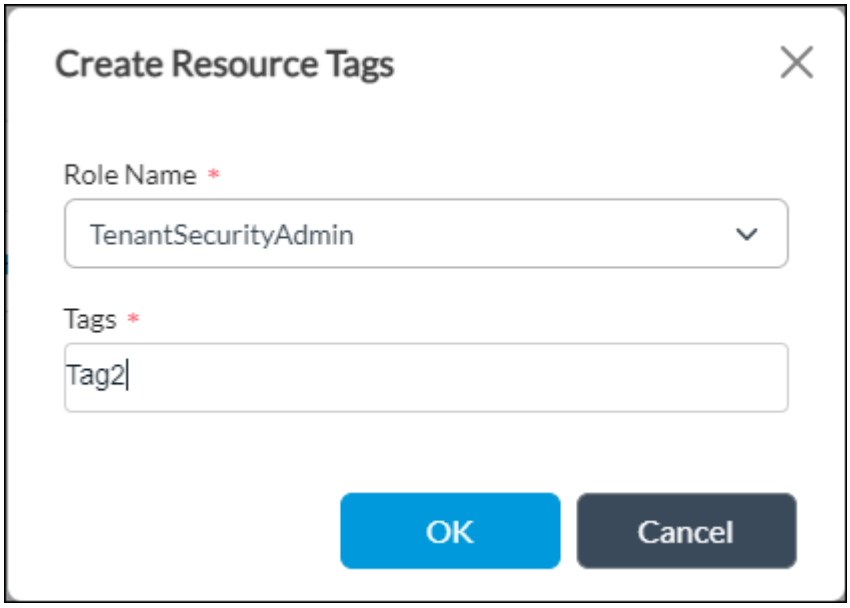
4. Click OK.

Configure Resource Tags for Tenant Users

1. In Director view, select the Administration tab in the top menu bar.
2. Select Director User Management > Resource Tags > Tenant Resource Tags in the left menu bar.



3. Click +Add. In the Create Resource Tags popup window, enter information for the following fields.



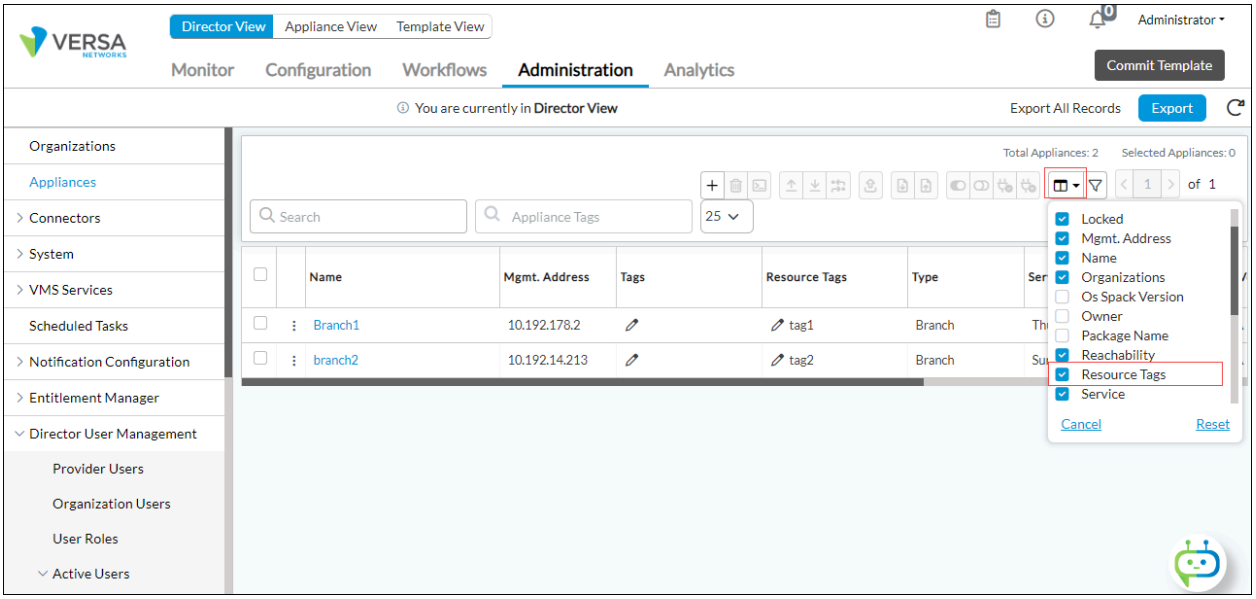
Field	Description
Role Name (Required)	Select a tenant role name.
Tags (Required)	Enter one or more names for the resource tag. A resource tag that has multiple names can be part of multiple resource groups.

4. Click OK.

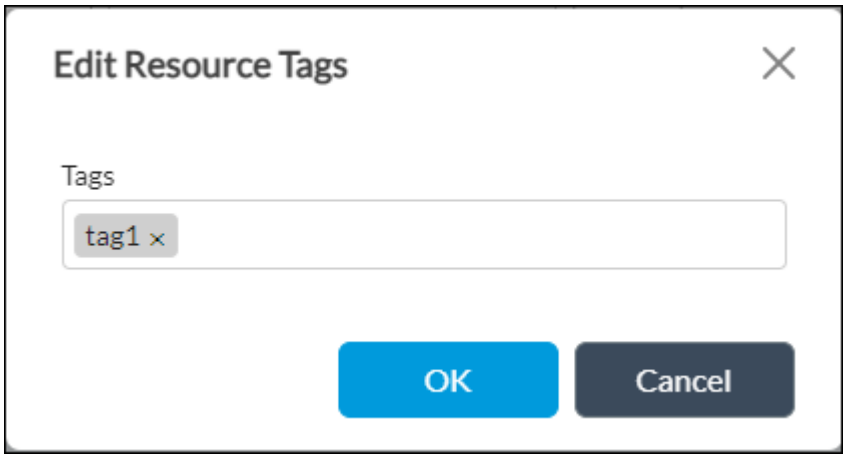
Configure Resource Tags for a Device

For Releases 22.1.1 and later.

1. In Director view, select the Administration tab in the top menu bar.
2. Select Appliances in the left menu bar.
3. In the Filter Columns drop-down list, select Resource Tags to view resource tag column in the appliance main pane. Then click the Edit icon in the Resource Tags column.



4. In the Edit Resource Tags popup window, enter a name for the resource tag.



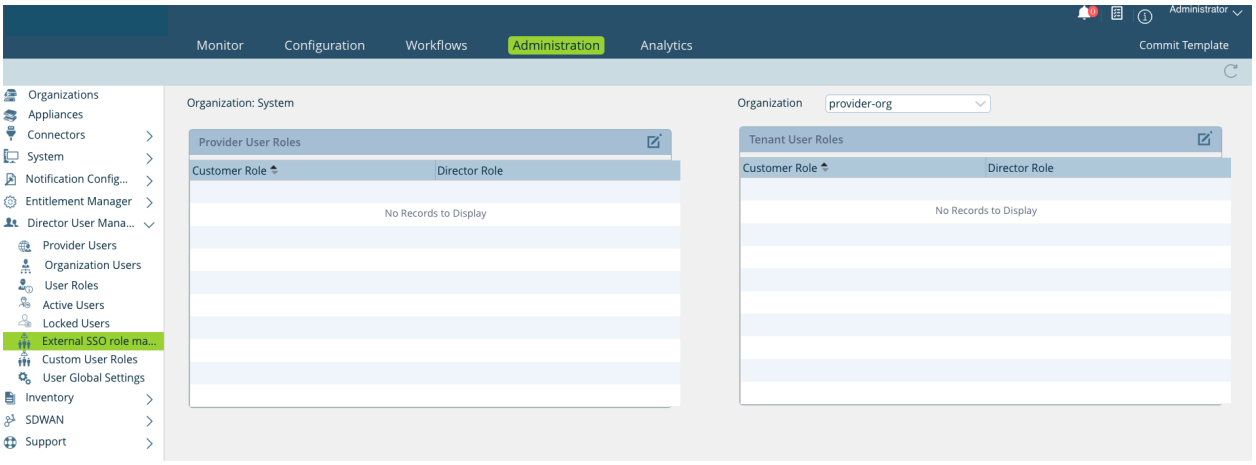
5. Click OK.

Map User SSO Roles

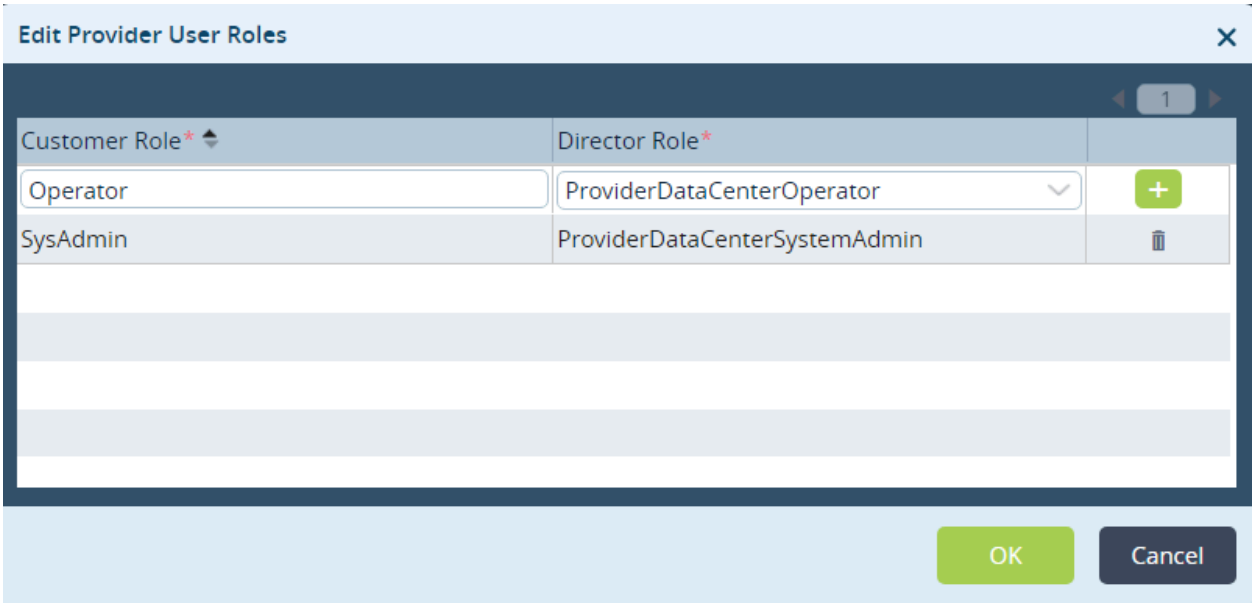
After you configure vendor-specific users and user roles in on a Director node, you map external SSO users with internal Director roles.

To map user SSO roles:

1. In Director view, select the Administration tab in the top menu bar.
2. Select Director User Management > External SSO Role mapping in the left menu bar.



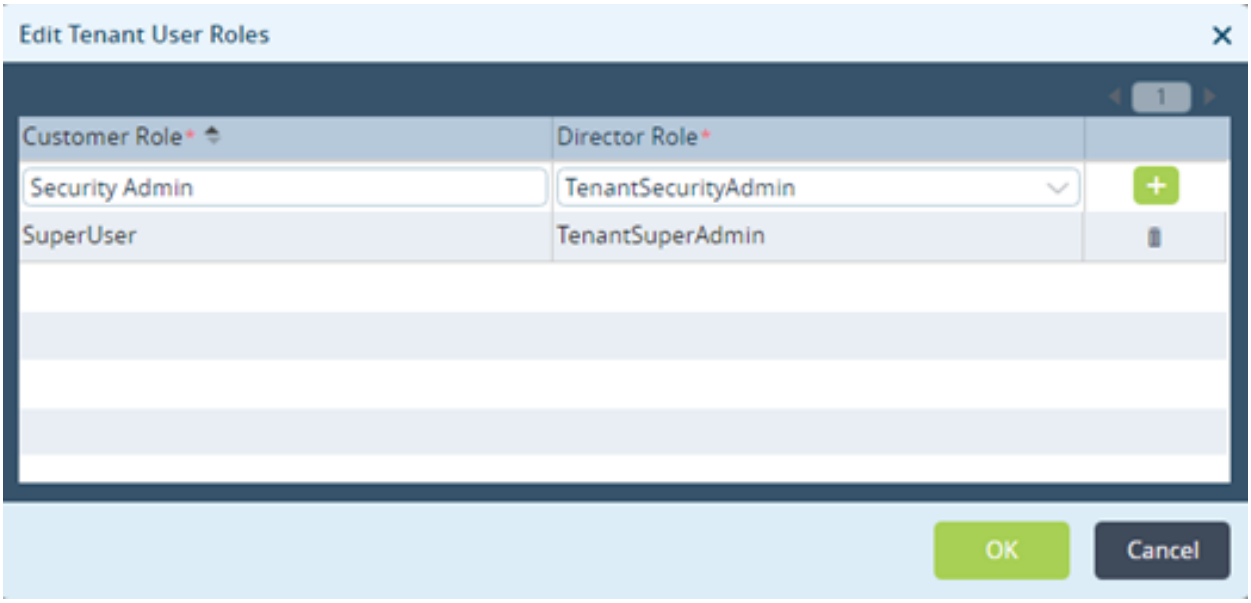
3. In the Provider User Roles pane, click the Edit icon. In the Edit Provider User Roles popup window, enter information for the following fields.



Field	Description
Customer Role	Select the customer role
Director Role	Select the role to associate with the customer role.

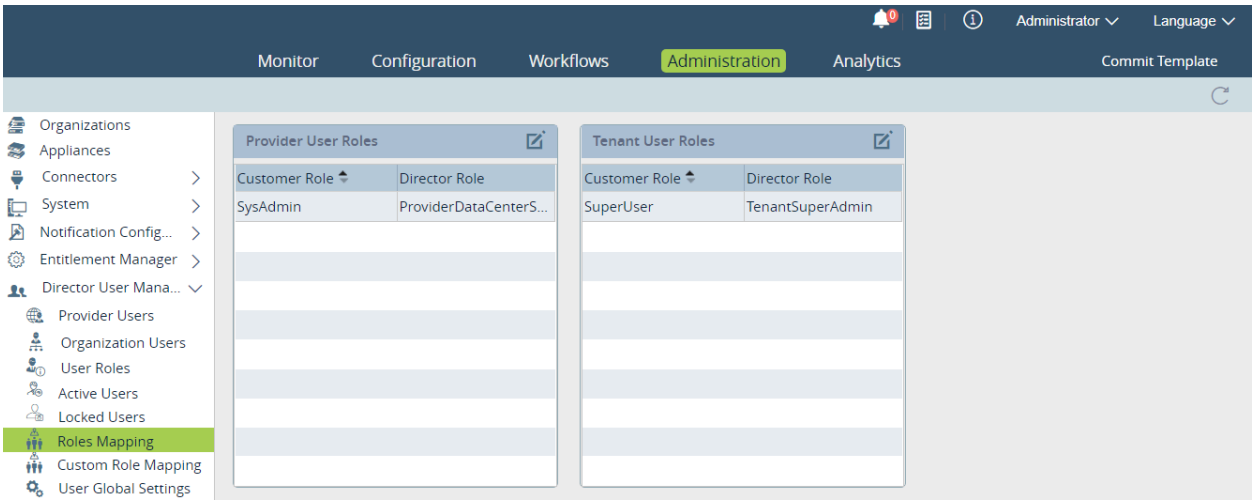
3. Click the Add icon.
4. Click OK.

5. In the Tenant User Roles pane, click the Edit icon. In the Edit Tenant User Roles popup window, enter information for the following fields.



Field	Description
Customer Role	Name of the customer role
Director Role	Role to be associated with the customer role

5. Click OK. The main pane displays the configured mappings between users and roles:



Configure Custom User Roles

For provider and tenant (organization) users, you can configure the custom user roles listed in the following table.

Resource	Provider User	Tenant User
ADC_MANAGEMENT	X	X
ALARM_MANAGEMENT	X	X
AMQP_CONNECTOR_MANAGEMENT	X	X
ANALYTICS_CONNECTOR_MANAGEMENT	X	—
ANALYTICS_MANAGEMENT	X	X
APPLIANCE_CONFIGURATION_MANAGEMENT	X	X
APPLIANCE_HA_MANAGEMENT	X	X
APPLIANCE_ORGANIZATION_ALG_MANAGEMENT	X	X
APPLIANCE_ORGANIZATION_AUTHENTICATION_PROFILE_MANAGEMENT	X	X
APPLIANCE_ORGANIZATION_DOT1X_MANAGEMENT	X	X
APPLIANCE_ORGANIZATION_LIMITS	X	X
APPLIANCE_ORGANIZATION_PROFILES_STORAGE_PROFILES	X	X
APPLIANCE_ORGANIZATION_RADIUS_SERVER_MANAGEMENT	X	X
APPLIANCE_ORGANIZATION_SETTINGS	X	X

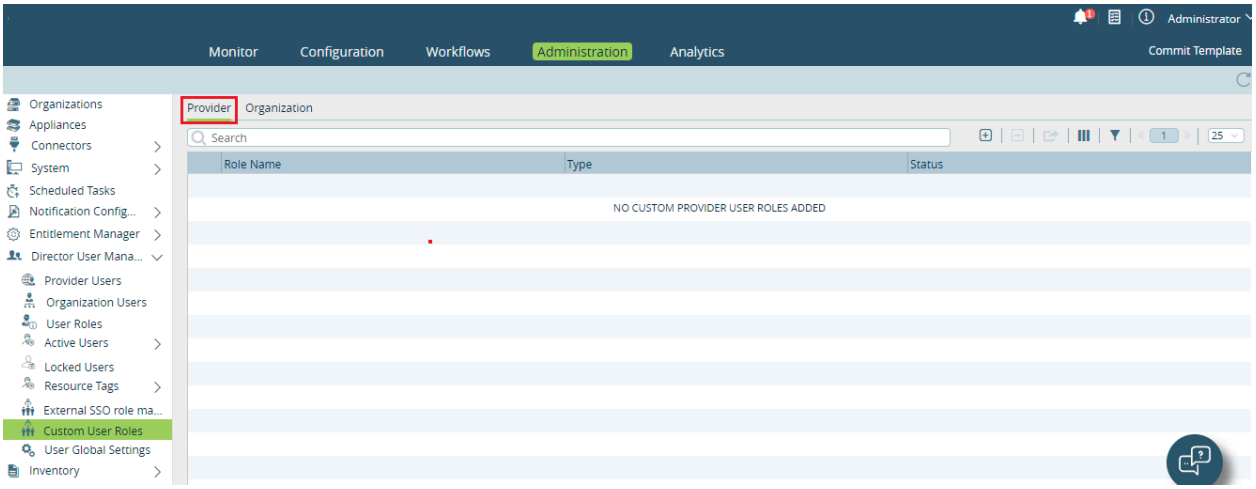
Resource	Provider User	Tenant User
APPLIANCE_ORG_MANAGEMENT	X	X
APPLIANCE_PROVIDER_USER_MANAGEMENT	X	X
APPLIANCE_SNMP_MANAGEMENT	X	X
APPLIANCE_SYSTEM_MANAGEMENT	X	X
APPLIANCE_TENANT_USER_MANAGEMENT	X	X
APPLICATION_CLIENT_MANAGEMENT	X	X
ASSET_MANAGEMENT	X	X
AUTH_CONNECTOR_MANAGEMENT	X	X
CGNAT_MANAGEMENT	X	X
CMS_CONNECTOR_MANAGEMENT	X	X
CONTROLLER_WORKFLOW_MANAGEMENT	X	—
COS_MANAGEMENT	X	X
CUSTOM_TEMPLATE_MANAGEMENT	X	X
DATA_COLLECTION_MANAGEMENT	X	—
DEVICE_GROUP_MANAGEMENT	X	X
DEVICE_WORKFLOW_MANAGEMENT	X	X
DHCP_MANAGEMENT	X	X
DHCP_PROFILE_MANAGEMENT	X	X
DIRECTOR_INFO	X	—
DIRECTOR_MANAGEMENT	X	—
DNS_PROXY_MANAGEMENT	X	X
GLOBAL_TRANSPORT_DOMAIN_MANAGEMENT	X	X
HA_MANAGEMENT	X	—
HW_INVENTORY_MANAGEMENT	X	X
INVENTORY_MANAGEMENT	X	X

Resource	Provider User	Tenant User
IPSEC_MANAGEMENT	X	X
LOG_EXPORT_MANAGEMENT	X	X
MONITOR_MANAGEMENT	X	X
NETWORK_ADMINISTRATION	X	X
NEXTGEN_FIREWALL_MANAGEMENT	X	X
NOTIFICATION_RULES_MANAGEMENT	X	X
ORGANIZATION_MANAGEMENT	X	X
ORG_WORKFLOW_MANAGEMENT	X	X
OS_SPACK_MANAGEMENT	X	X
PBF_MANAGEMENT	X	X
PROVIDER_USER_MANAGEMENT	X	—
REGISTRATION_TOKEN_MANAGEMENT	X	X
SDWAN_GLOBAL_SETTINGS	X	—
SDWAN_MANAGEMENT	X	X
SDWAN_PROVIDER_MANAGEMENT	X	X
SECURE_ACCESS_MANAGEMENT	X	X
SECURITY_MANAGEMENT	X	X
SERVICE_CHAIN_MANAGEMENT	X	X
SERVICE_CHAIN_WORKFLOW_MANAGEMENT	X	X
SMTP_SMS_NOTIFICATION_MANAGEMENT	X	—
SNAPSHOT_MANAGEMENT	X	X
SPACK_MANAGEMENT	X	X
SPOKEGROUP_WORKFLOW_MANAGEMENT	X	X
SSO_MANAGEMENT	X	X
STATEFUL_FIREWALL_MANAGEMENT	X	X

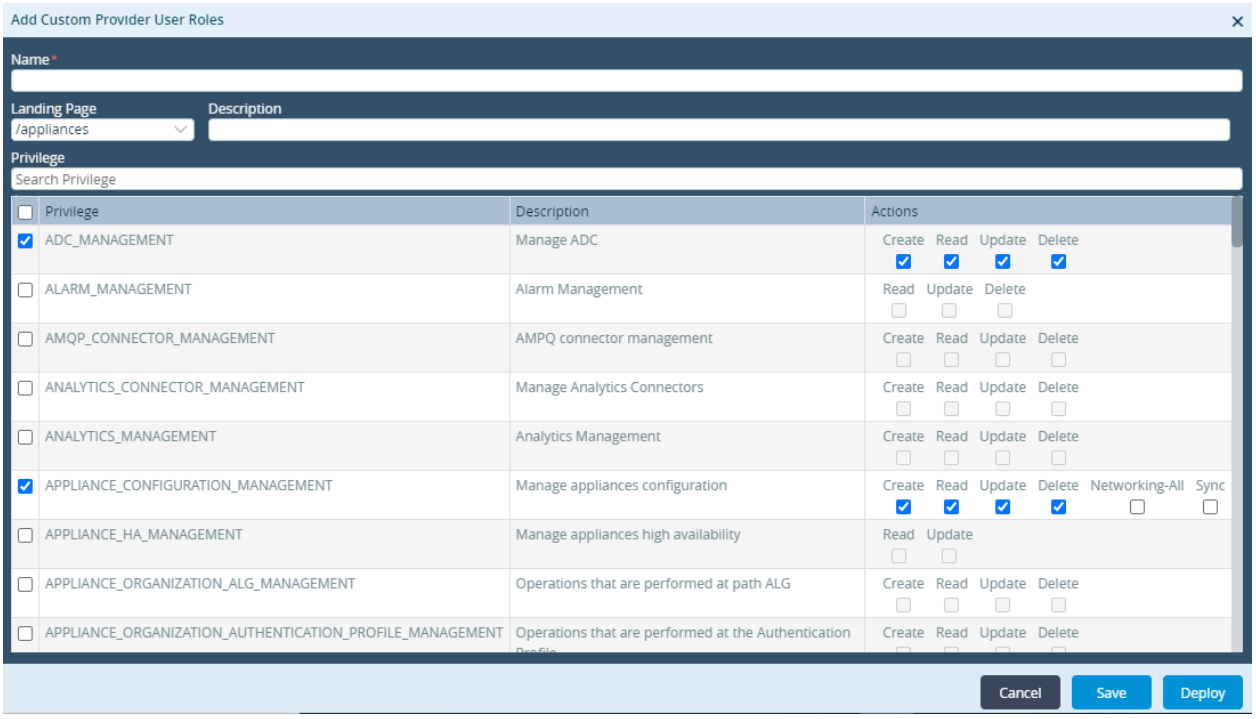
Resource	Provider User	Tenant User
SUBSCRIPTION_MANAGEMENT	X	—
SYSLOG_SERVER_MANAGEMENT	X	—
SYSTEM_SSL_CERTIFICATE_MANAGEMENT	X	—
TASKS_MANAGEMENT	X	X
TDF_MONITORING_MANAGEMENT	X	X
TEMPLATE_MANAGEMENT	X	X
TEMPLATE_WORKFLOW_MANAGEMENT	X	X
TENANT_USER_MANAGEMENT	X	X
TROUBLE_SHOOTING_MANAGEMENT	X	—
UNKNOWN_DEVICE_MANAGEMENT	X	X
USER_OBFUSCATION (For Releases 22.1.2 and later.) When users associated with this resource access Analytics screens, user information in all reports containing usernames is obfuscated.	X	X
USER_MANAGEMENT	X	X
WAN_NETWORK_MANAGEMENT	X	X
WEB_PROXY_MANAGEMENT	X	X

Configure Custom Provider User Roles

1. In Director view, select the Administration tab in the top menu bar.
2. Select Director User Management > Custom User Roles in the left menu bar.
3. Select the Provider tab in the horizontal menu bar, and then click the Add icon.



4. In the Add Custom Provider User Roles popup window, enter information for the following fields.



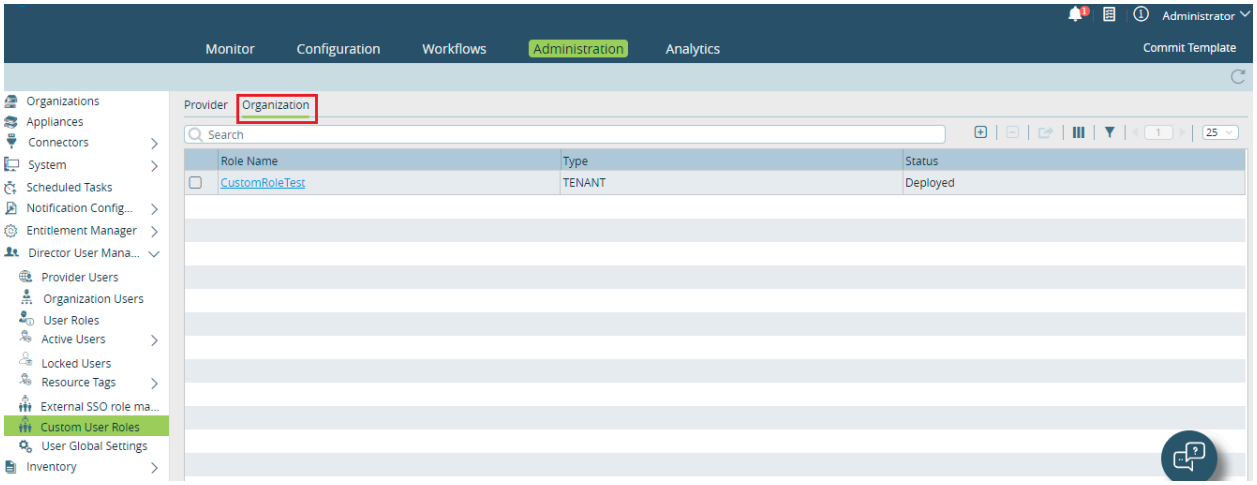
Field	Description
Name	Enter a name for the custom provider user role. For a list of provider and user roles, see Configure User Authorization, above.
Landing Page	Select the first page to display when the user logs in to the application.

Field	Description
Description	Enter a description.
Privileges	In the privilege list, click the required privileges and actions. The actions selected for a privilege are displayed in the Director left menu bar inline help if you have enabled show RBAC privileges. For more information, see Display RBAC Privileges, above.

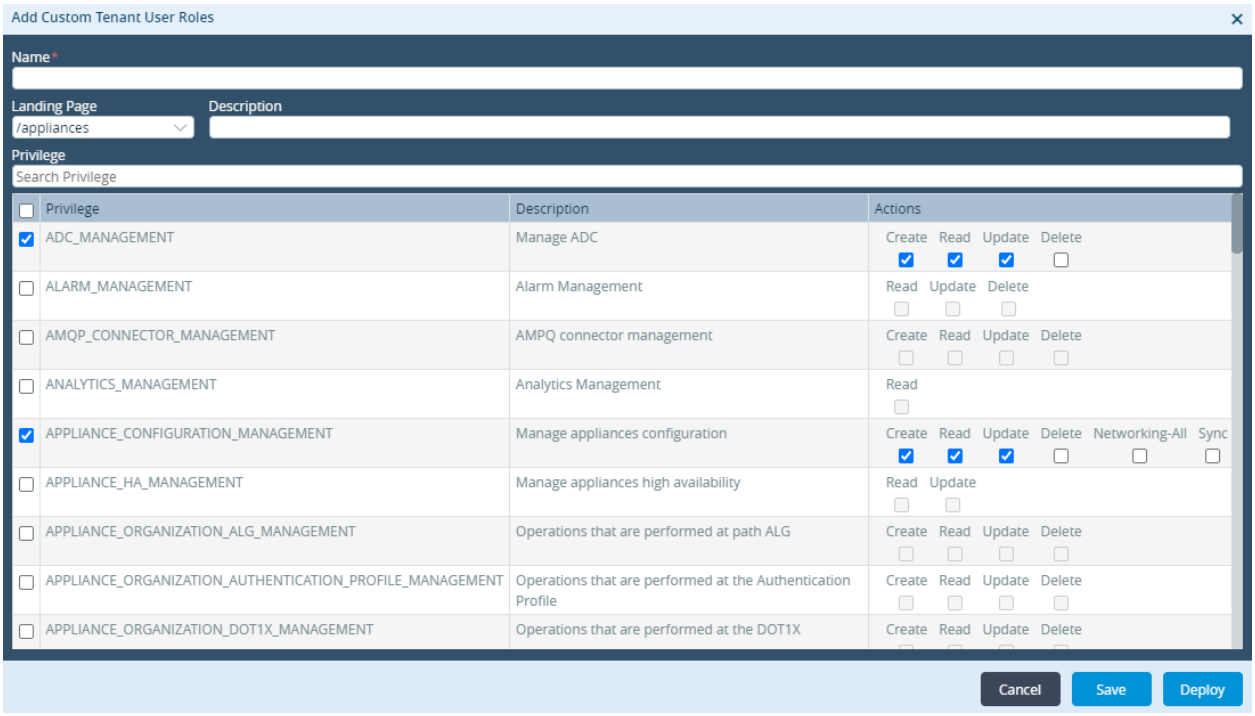
5. Click Save.
6. Click Deploy.

Configure Custom Tenant User Roles

1. In Director view, select the Administration tab in the top menu bar.
2. Select Director User Management > Custom User Roles in the left menu bar.
3. Select the Organization tab in the horizontal menu bar, and then click the Add icon.



4. In the Add Custom Tenant User Roles popup window, enter information for the following fields.



Field	Description
Name	Enter a name for the custom user role. For a list of provider and user roles, see Configure User Authorization, above
Landing Page	Select the first page to display when the user logs in to the application.
Description	Enter a description.
Privileges	In the privilege list, click the required privileges and actions. The actions selected for a privilege are displayed in the Director left menu bar inline help if you have enabled show RBAC privileges. For more information, see Display RBAC Privileges, above.

5. Click Save.
6. Click Deploy.

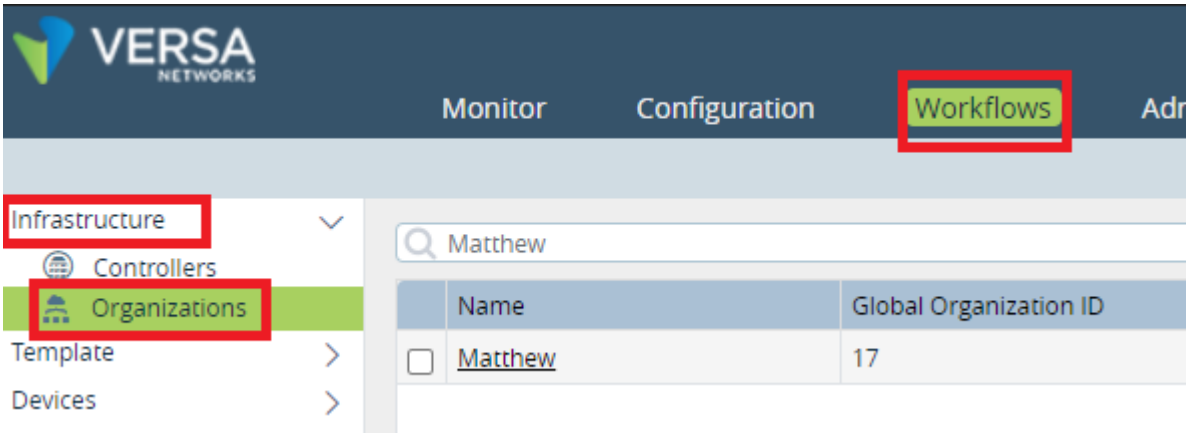
Enable or Remove a Custom User Role for a Tenant

When you create a custom user role, by default, organizations (tenants) cannot use the created custom user role. You

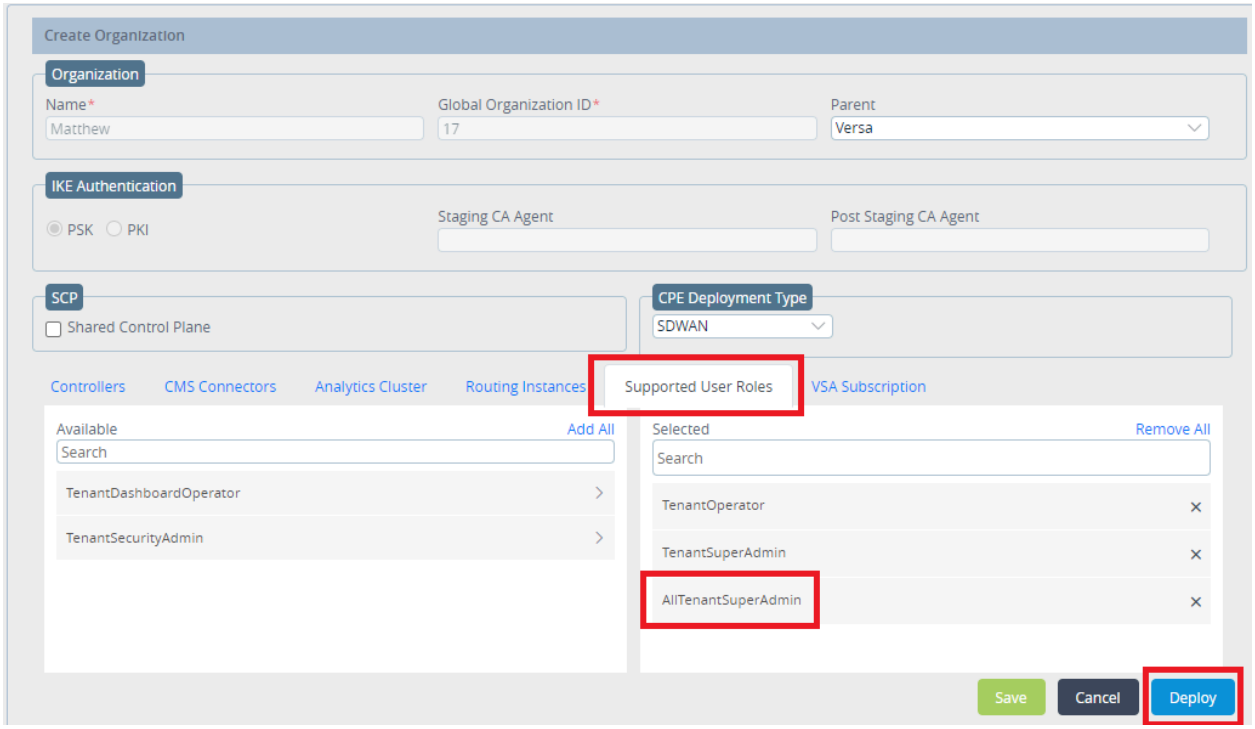
must associate the custom user roles with the organizations in which you create users with new privileges. You can also remove custom user roles from an organization.

To add a custom user role to, or delete a custom user role from, an organization:

1. In Director view, select the Workflows tab in the top menu bar.
2. Select Infrastructure > Organizations in the left menu bar.



3. In the main pane, select the organization for which you want to add or remove a custom user role. The Create Organization popup window displays.
4. Select the Supported User Roles tab.
5. Add the custom user role that you created in Step 3 in Configure Custom Tenant User Roles, above. For example, in the following screenshot, the AllTenantSuperAdmin custom user role is added.

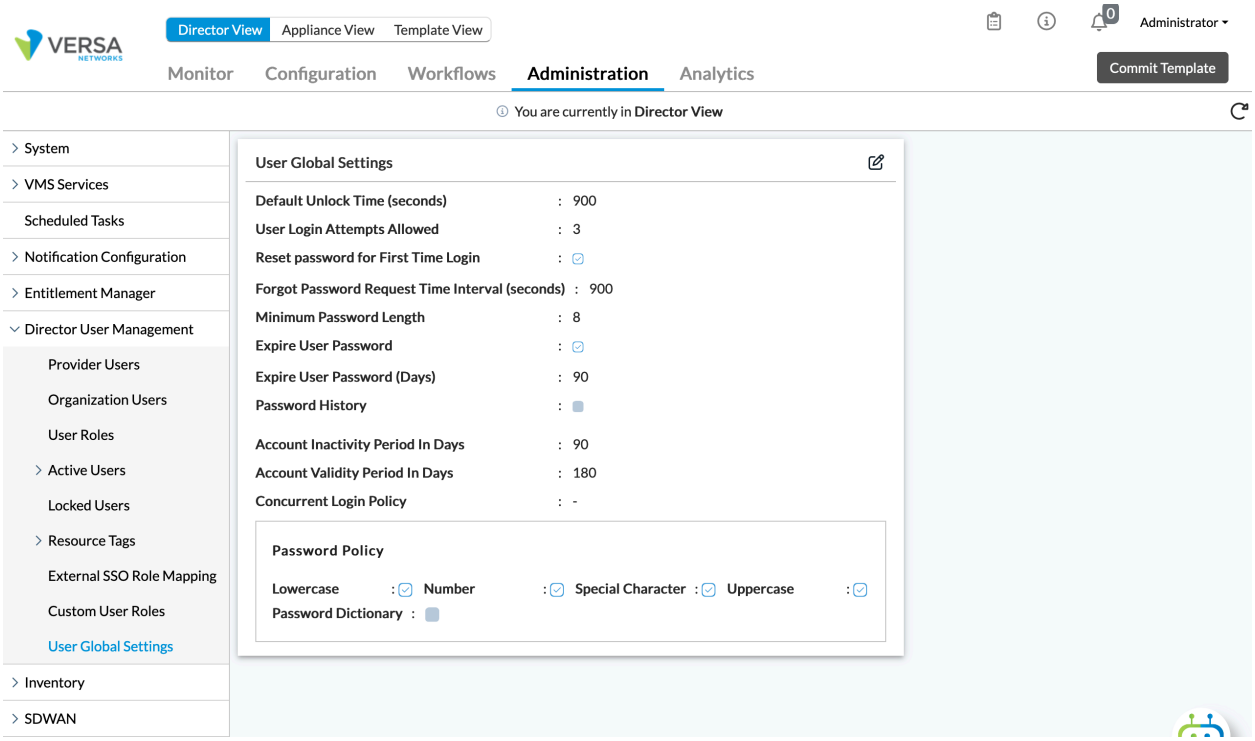


6. To delete a custom user role from an organization, click the X next to the name of the user role.
7. Click Deploy.

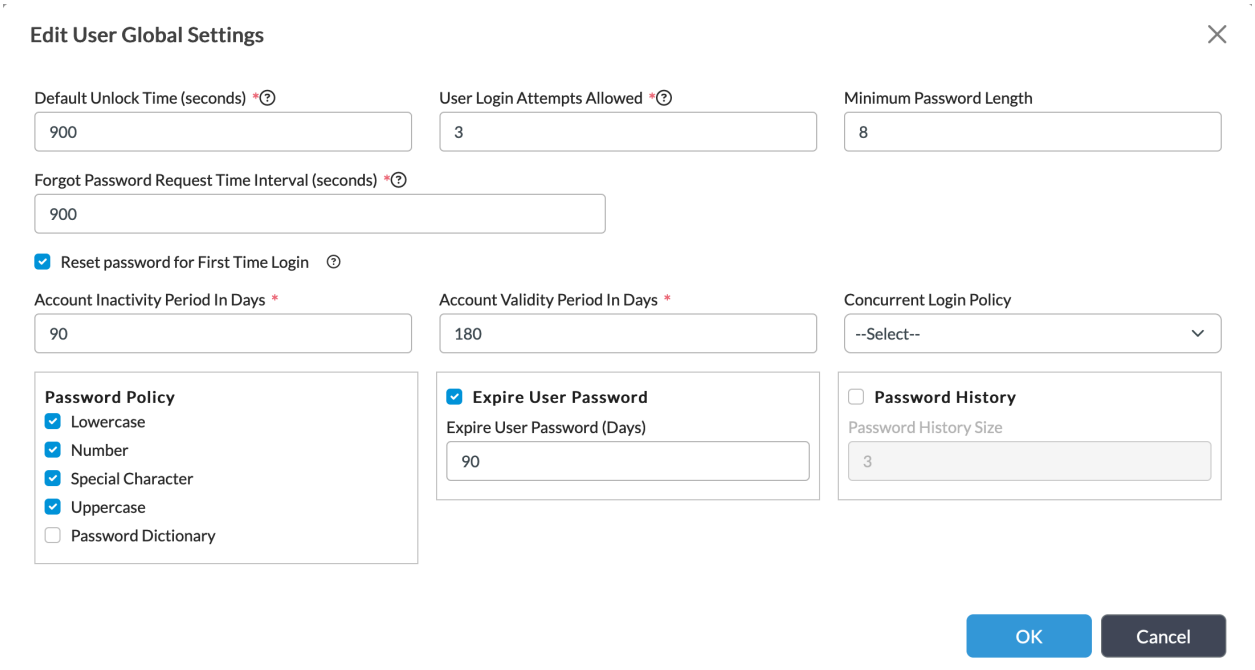
Configure User Global Settings

For Releases 20.2 and later.

1. In Director view, select the Administration tab in the top menu bar.
2. Select Director User Management > Global Settings in the left menu bar. The following screen displays.



3. Click the Edit icon. In the Edit User Global Settings popup window, enter information for the following fields.



Field	Description
Default Unlock Time (Required)	When the user enters the incorrect password and has been locked out and prevented from logging in, enter how long the user must wait, in seconds, before they are unlocked and are again able to log in to the Director node. *Default:* 900 seconds (15 minutes)
User Login Attempts Allowed (Required)	Enter how many times the user is allowed to enter the incorrect password before they are locked out and can no longer log in to the Director node. Configuring the maximum number of login attempts can protect against brute force login attacks. *Default:* 3
Minimum Password Length	(For Releases 22.1.2 and later.) Enter the minimum length of password for logging in to the Director node. Default: 8
Forgot Password Request Time Interval (Required)	(For Releases 22.1.2 and later.) When the user enters the incorrect password, enter how long to wait, in seconds, before they are locked out and are no longer able to log in to the Director node. *Default:* 900 seconds (15 minutes)
Reset Password for First-Time Login	Click to prompt the user to reset their password when they first log in.
Account Inactivity Period (Required)	(For Releases 22.1.2 and later.) Enter the number of days that a user's login account is inactive, after which the user's account is disabled. Default: 90 days
Account Validity Period (Required)	(For Releases 22.1.2 and later.) Enter the number of

Field	Description
	days that a user's login account is valid, after which the user's account is disabled. Default: 180 days
Concurrent Login Policy	(For Releases 22.1.2 and later.) Select how to handle multiple concurrent login sessions on the Director node: ◦ Allow—Allow multiple users to log in to the Director node at the same time. ◦ Deny—Allow only a single user to log in to the Director node at the same time. ◦ Force Logout—For a user who is already logged in to the Director node from one location or browser and who logs in from a second location or browser, log out the user from the first location or browser when they log in to the second.
Password Policy	Click one or more items to select the characters that configure the password policy: ◦ Lowercase—Password must include at least one lowercase letter. ◦ Number—Password must include at least one digit. ◦ Password Dictionary—Check the password against those found in the password dictionary. ◦ Special Character—Password must include at least one special character, such as !, @, #, and &. ◦ Uppercase—Password must include at least one uppercase letter
Expire User Password	Click to have the user's password expire.
◦ Days to Expire User Password	Enter the number of days that a user's password is valid. After this number of days passes, the user is prompted to reset their password when they attempt to log in. *Default:* 90 days
Password History	Click to store the user's password history.

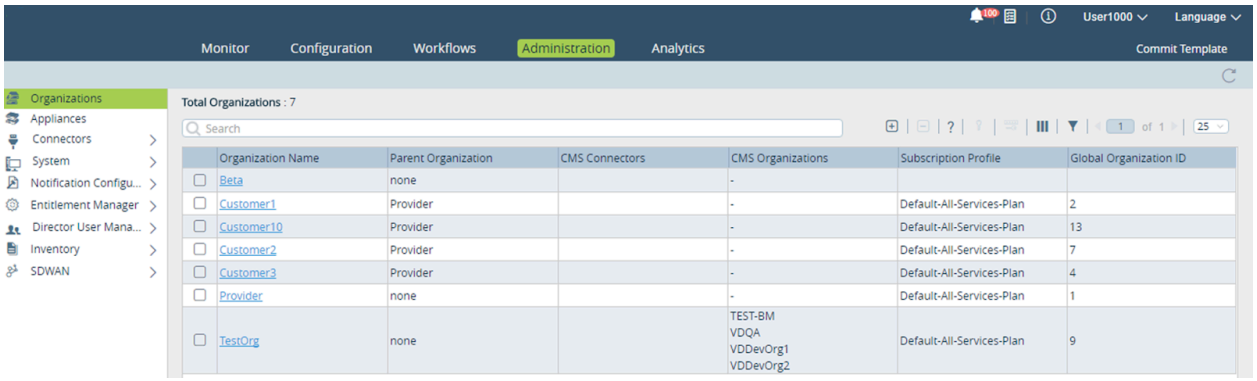
Field	Description
◦ Password History Size	Enter the number of previous passwords to remember. When the user resets their password, they cannot reuse these previous passwords. *Default:* 3

4. Click OK.

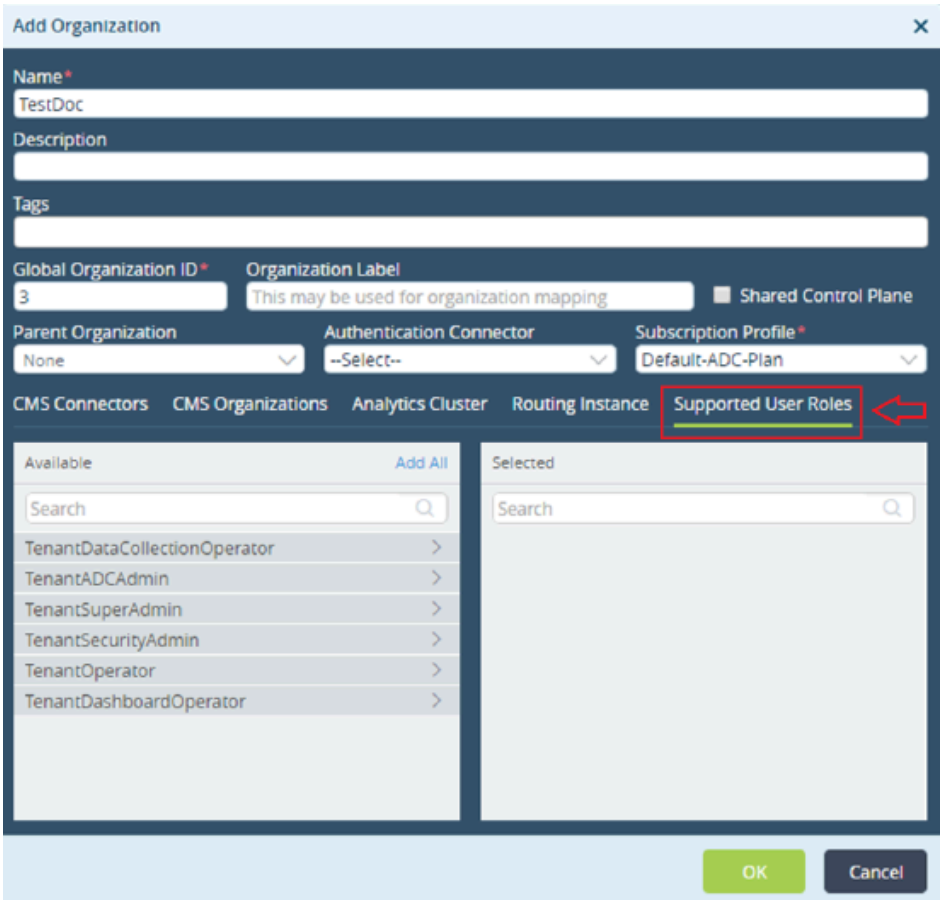
Associate Roles with a Tenant or an Organization

You can select the roles when you create an organization or a tenant.

1. In Director view, select the Administration tab in the top menu bar.
2. Select Organizations in the left menu bar.
3. Click the Add icon to create an organization (tenant).



4. In the Add Organization popup window, select the Supported User Roles tab.

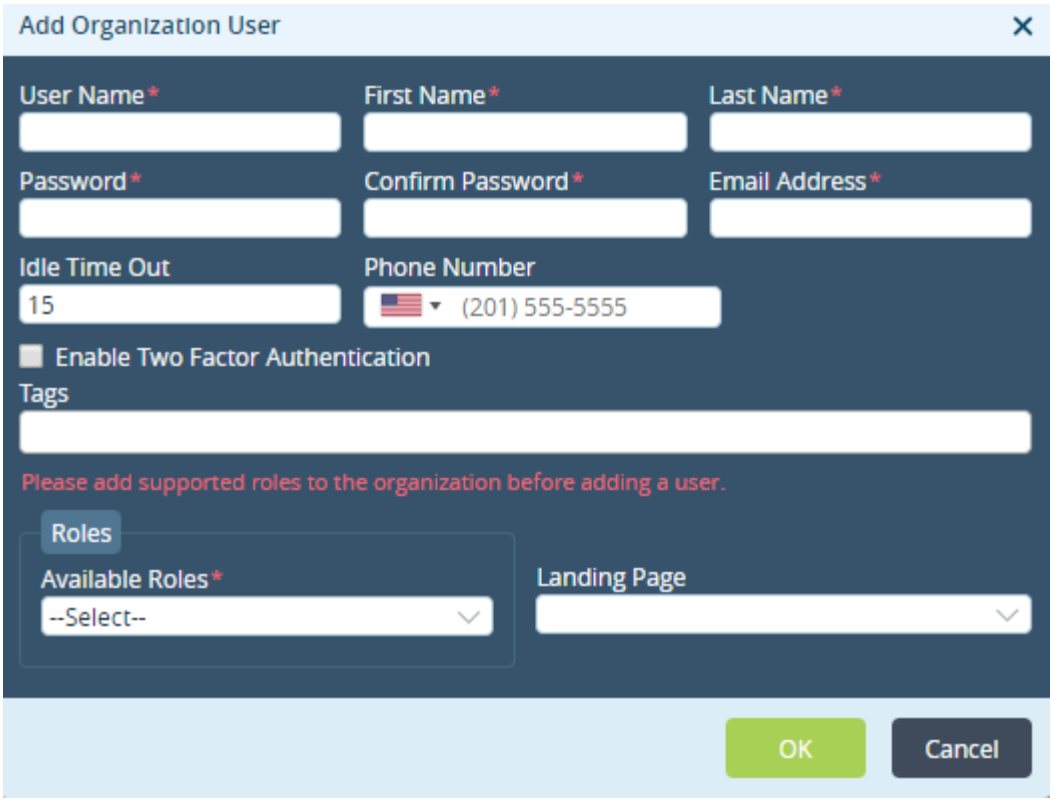


5. Move the available user roles from the Available table to the Select table.
6. Click OK.

Create Organization and Tenant Users

You cannot create organization or tenant users if you do not select RBAC roles.

1. In Director view, select the Administration tab in the top menu bar.
2. Select Director User Management > Organization Users in the left menu bar.
3. Select an organization in the main pane.
4. Click to the Add icon add a user.



5. Click OK.

Supported Software Information

Releases 20.2 and later support all content described in this article, except:

- Release 20.2.1 adds support for redundant authentication servers for Active Directory, LDAP, RADIUS, and TACACS+.
- Release 21.1 adds support for connecting to Active Directory global catalogs.
- Release 22.1.1 adds support for two-factor authentication for external authentication servers and resource tags for user roles and appliances.
- Release 22.1.2 adds support for bypass external authentication for console login; adds fields in the Edit User Global Settings popup window; adds support for USER_OBFUSCATION resource for custom user roles.
- Release 22.1.3 adds support for central authentication server; adds Director Client tab and Authentication Context Required field in the Add SSO window.

Additional Information

Configure AAA (for VOS Devices)
Configure Basic Features
Configure Single Sign-On Using Director