RSA SecurID Access SAML Configuration for Dome9

Last Modified: August 24, 2016

Dome9 is the security operations console for cloud infrastructure. It is a purpose-built security and compliance solution for public and hybrid clouds. It has a complete set of security controls including firewall management, visualization, file integrity monitoring, configuration monitoring, and dynamic access leases and tamper protection.

Before You Begin

- Acquire an administrator account for both RSA SecurID Access and Dome9.
- Obtain the Dome9 Login URL, ACS URL and Service Provider Issuer ID from your Dome9 service provider.

The instructions in this guide use the following login URL, ACS URL and issuer ID (entity ID) values:

Login URL	*https://secure.dome9.com/account/logon*
ACS URL	*https://secure.dome9.com/sso/saml/gslab*
Service Provider Issuer ID	*https://secure.dome9.com/*

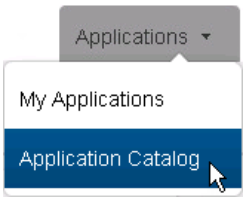
Procedure

1. Add the Application in RSA SecurID Access
2. Configure Dome9 to Use RSA SecurID Access as an Identity Provider

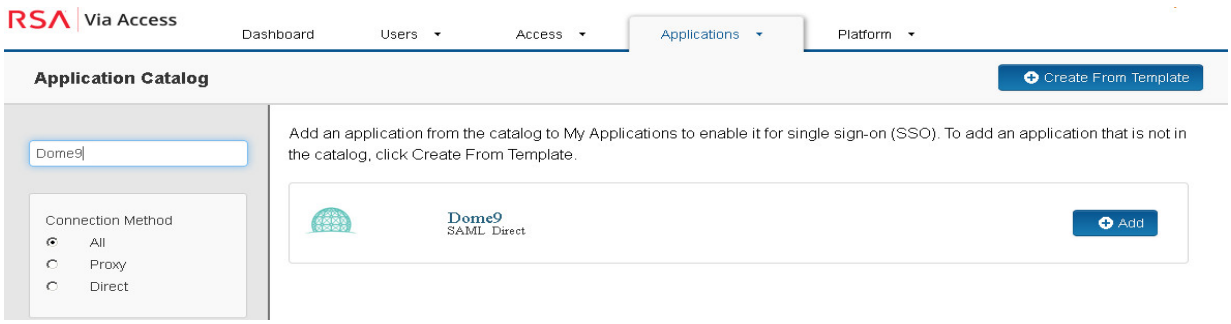
Add the Application in RSA SecurID Access

Procedure

1. Log in to the RSA SecurID Access Administration Console, click the **Applications** tab and select *Application Catalog* from the **Application** tab dropdown list.

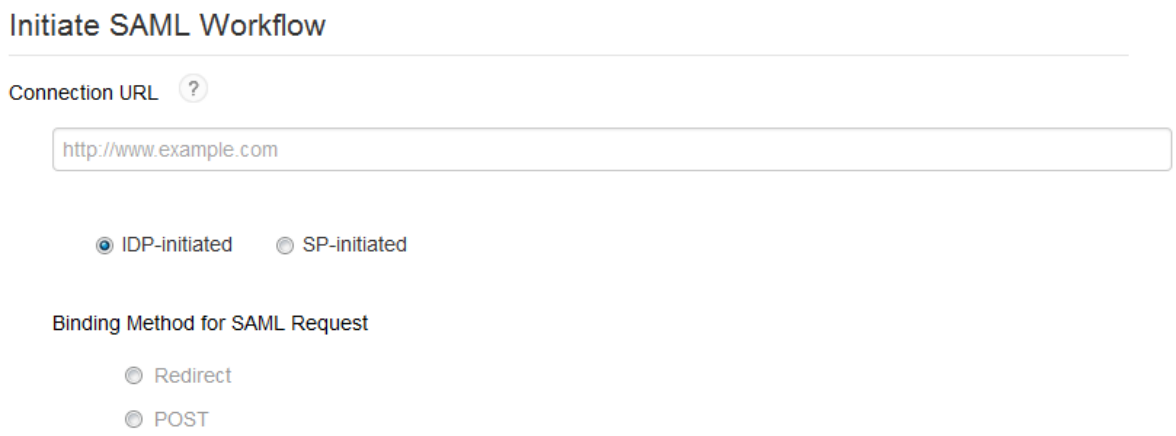


2. Search for *Dome9* in the list of applications and click the **+Add** button.



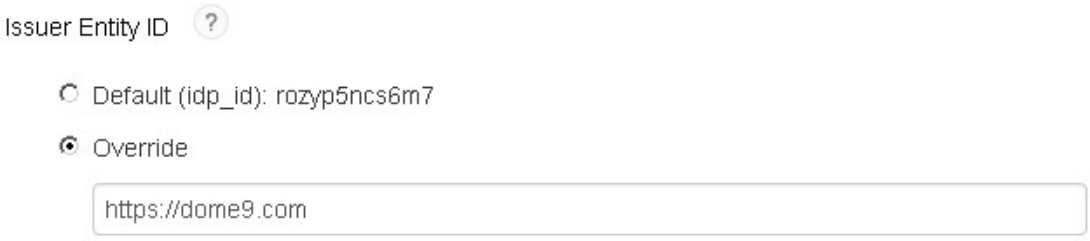
3. Enter a name for the application in the **Name** field on the Basic Information page and click the **Next Step** button.
4. Select the **IDP-initiated** radio button in the Initiate SAML Workflow section.

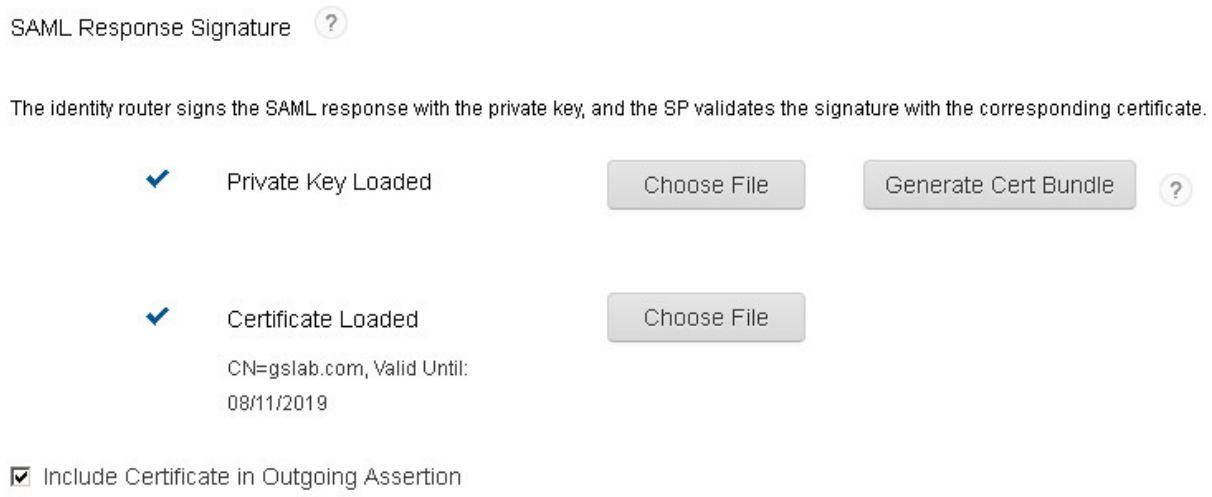
Note: The following IDP-initiated configuration works for SP-initiated Dome9 connections as well.



5. Scroll to SAML Identity Provider (Issuer) section, copy the value in the **Identity Provider URL** field and paste it into a temporary file. You will need the URL when you configure your Dome9 service provider.

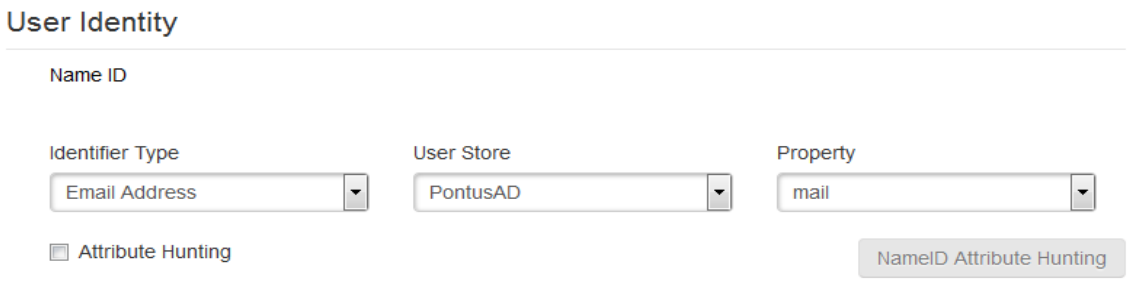
6. In the **Issuer Entity ID** section, enter *https://dome9.com*, copy this value and paste it into a temporary file. You will need this value when you configure your Dome9 service provider.





7. Click the **Choose File** button on the left of the **Generate Certificate Bundle** button, locate and select a private key for signing the SAML assertions and click the **Open** button.
8. Click the **Choose File** button underneath the **Generate Certificate Bundle** button, locate and select your public certificate and click the **Open** button.
9. Select the **Include Certificate in Outgoing Assertion** checkbox.
10. Scroll to the Service Provider section and enter your Dome9 ACS URL in the **Assertion Consumer Service (ACS) URL** field. The URL should be formatted as follows: *https://secure.dome9.com/sso/saml/<COMPANY_NAME>*.
    The ACS URL in this example is *https://secure.dome9.com/sso/saml/gslab*.
11. Enter *https://secure.dome9.com/ in* the **Audience (Service Provider Entity ID)** field.

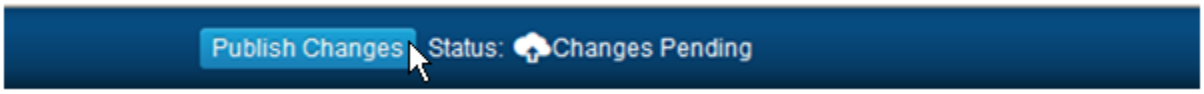
12. Scroll to the User Identity section, select **EmailAddress** from the Identifier Type dropdown list and select the name of your user identity source from the User Store dropdown list. In this example, user accounts are stored in an identity source named Pontus*AD*.
13. Select the identity source's attribute that will be used as the NameID from the **Property** dropdown list. In this example, the identity source's **mail** attribute will be used to uniquely identify a user in SAML assertions.



14. Click the **Next Step** button.

15. On the User Access page, select the access policy the identity router will use to determine which users can access the Dome9 service provider from the portal. If you want to allow access to all users who are signed in to the portal, select the **Allow All Authenticated Users** radio button. Otherwise, select the **Select Custom Policy** radio button and select the policy you want to use from the dropdown list.

16. Click the **Next Step** button.
17. Select the **Display in Portal** checkbox on the Portal Display page.
18. Click the **Save and Finish** button.
19. Click the **Publish Changes** button in the top left corner of the page.

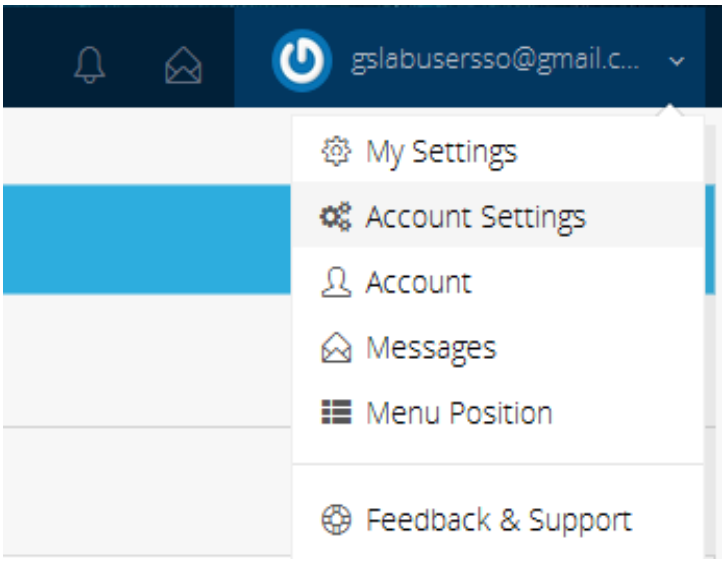


Configure Dome9 to Use RSA SecurID Access as an Identity Provider

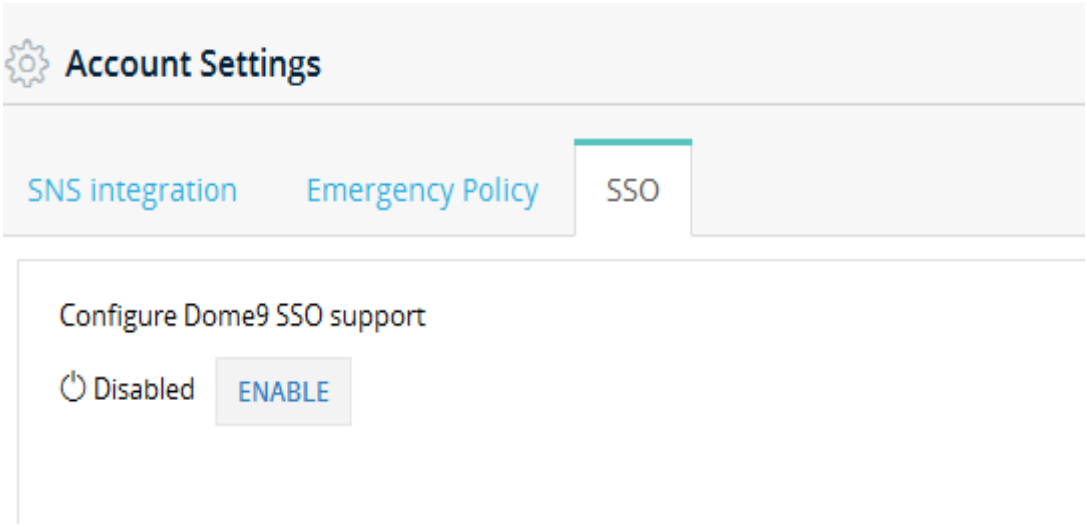
Follow below steps to configure Dome9 as service provider.

Configure Dome9 SSO support

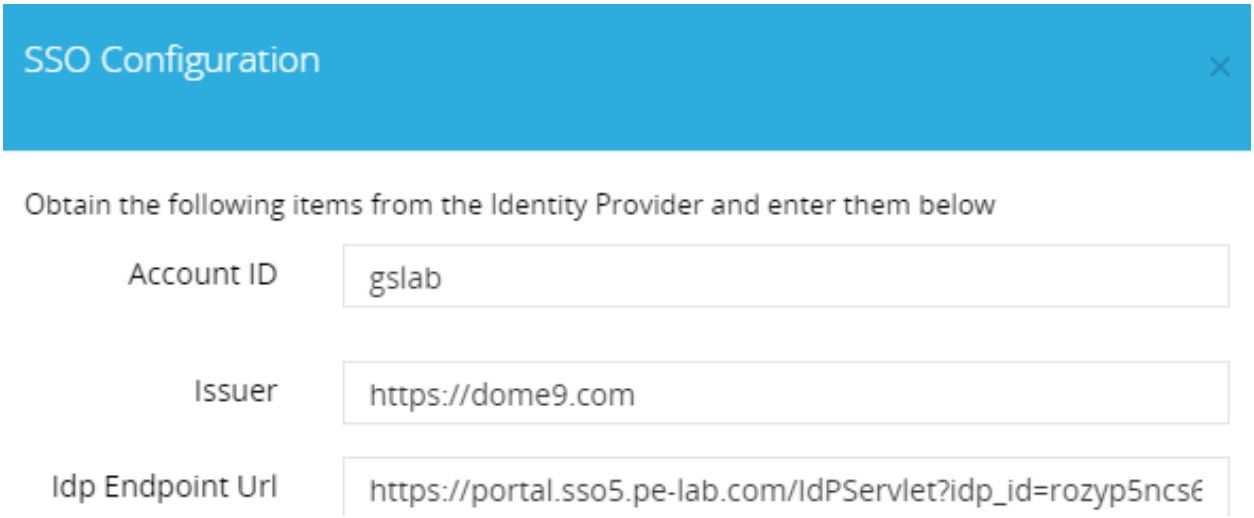
1. Login into Dome9 console at *https://secure.dome9.com/account/logon.* In the upper right corner, click on **Account Settings**.



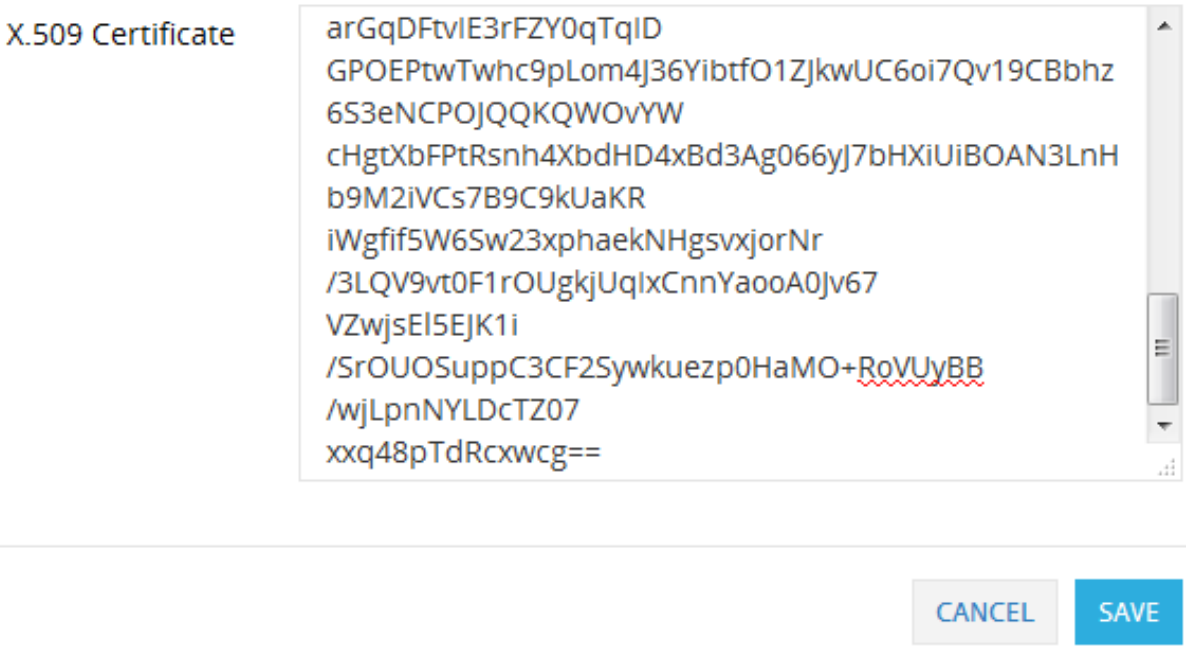
2. Go to SSO tab in Account Settings. Click on **Enable** to configure Dome9 for SSO support.



3. In Account ID field, enter your <COMPANY_NAME>. The <COMPANY_NAME> in this example is gslab.
4. In Issuer field, enter Issuer as **https://dome9.com**.
5. Enter your RSA SecurID Access Identity Provider URL in the Identity Endpoint URL field. Refer to page 2 step 5.

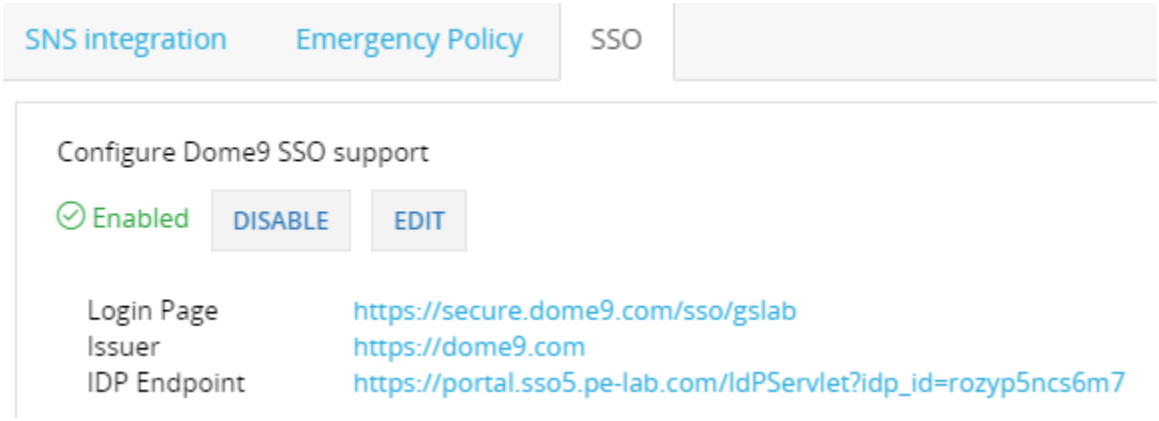


6. Copy and paste the X509 certificate from RSA SecurID Access into the X.509 Certificate textbox.



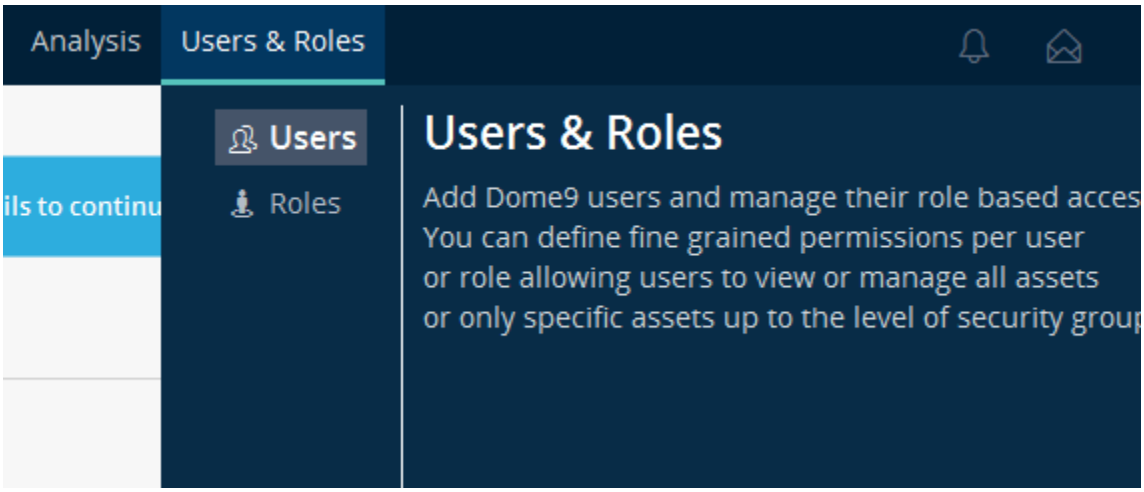
7. Click the **Save** button.

8. Verify your configurations. You can use Login Page value for SP initiated SSO.

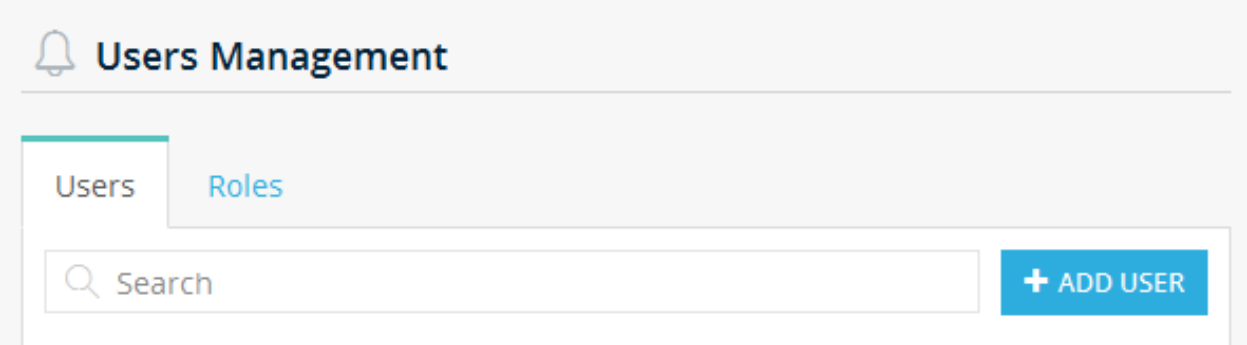


Creating user for SSO

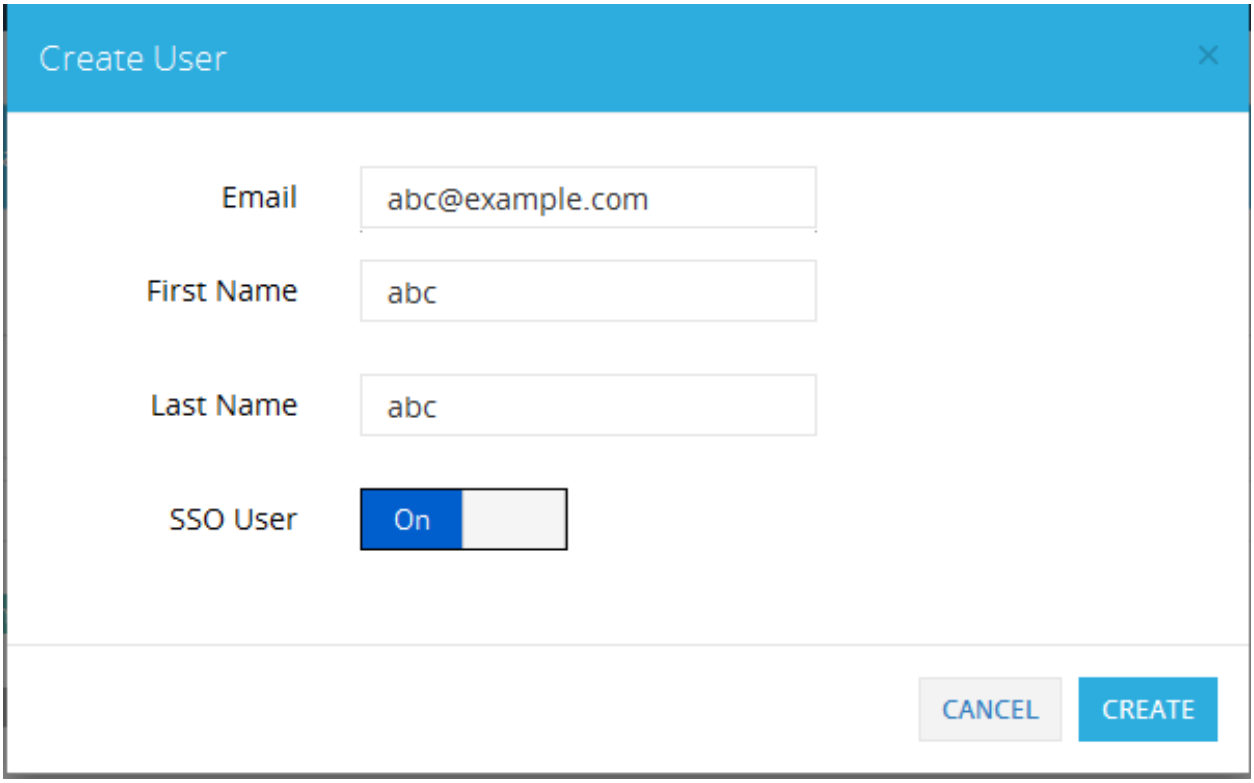
1. Click on **Users & Roles** in the top.



2. In the Users Management section, click on **+ADD USER**.

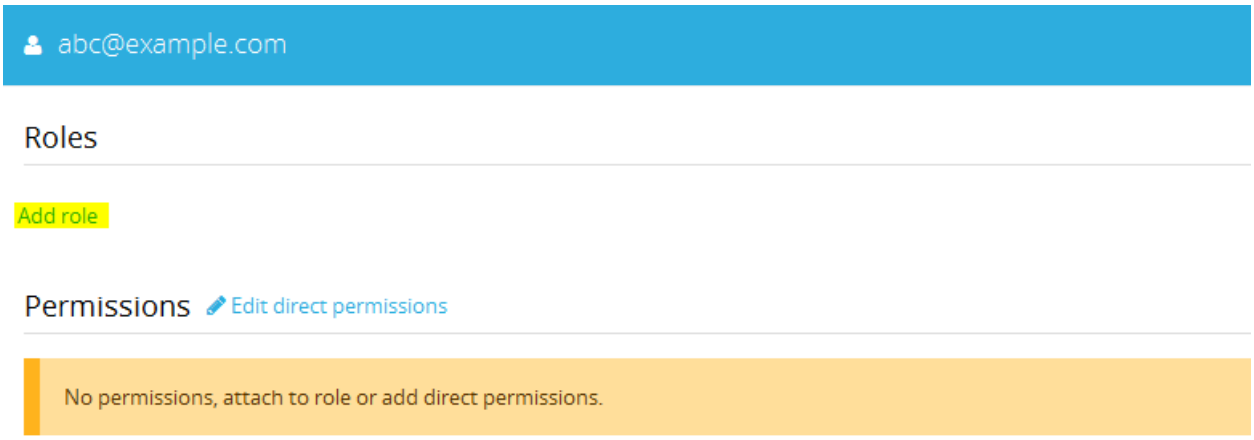


3. In the Create User section, fill in all the details of your user. Make sure that SSO User field is **On**.

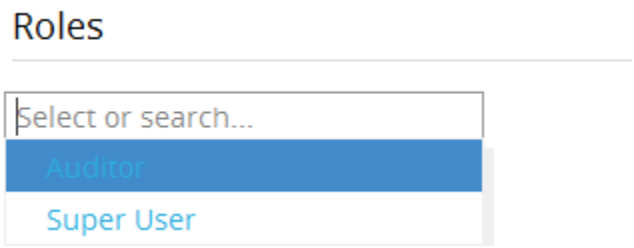


4. Click on **Create**.

5. Roles and Permissions will pop-up. Click on **Add Role**.



6. Use the Roles pulldown and select a role for the user.



7. Click on **Close**.

AB