

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/

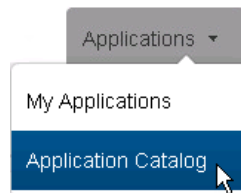
Procedure

1. [Add the Application in RSA SecurID Access](#)
2. [Configure Dome9 to Use RSA SecurID Access as an Identity Provider](#)

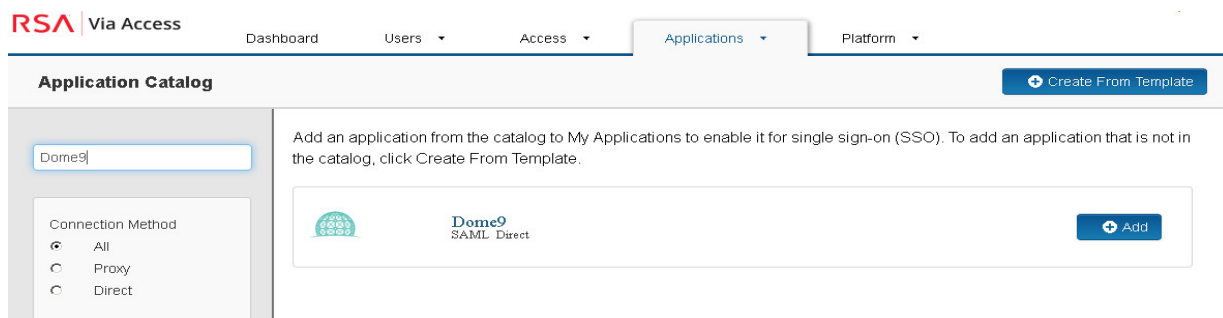
Add the Application in RSA SecurID Access

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.

Initiate SAML Workflow

Connection URL

IDP-initiated SP-initiated

Binding Method for SAML Request

Redirect

POST

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](#).

SAML Identity Provider (Issuer)

Identity Provider URL

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](#).

Issuer Entity ID

Default (idp_id): rozyp5ncs6m7

Override

SAML Response Signature ?

The identity router signs the SAML response with the private key, and the SP validates the signature with the corresponding certificate.

<input checked="" type="checkbox"/>	Private Key Loaded	<input type="button" value="Choose File"/>	<input type="button" value="Generate Cert Bundle"/> ?
<input checked="" type="checkbox"/>	Certificate Loaded	<input type="button" value="Choose File"/>	
	CN=gslab.com, Valid Until: 08/11/2019		

Include Certificate in Outgoing Assertion

- 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.
- Click the **Choose File** button underneath the **Generate Certificate Bundle** button, locate and select your public certificate and click the **Open** button.
- Select the **Include Certificate in Outgoing Assertion** checkbox.
- 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*.
- Enter *https://secure.dome9.com/* in the **Audience (Service Provider Entity ID)** field.

Service Provider

Assertion Consumer Service (ACS) URL ?

Audience (Service Provider Entity ID) ?

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 PontusAD.
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.

User Identity

Name ID

Identifier Type

Email Address

User Store

PontusAD

Property

mail

Attribute Hunting

NameID Attribute Hunting

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

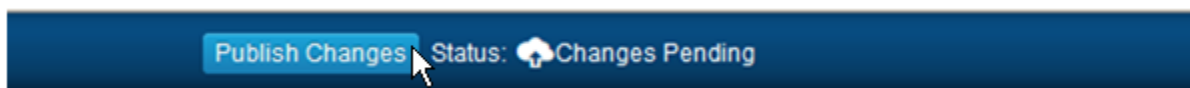
15. On the User Access page, select the access policy the identity router will use to determine which users can access the Dome9 service provider from the portal. If you want to allow access to all users who are signed in to the portal, select the **Allow All Authenticated Users** radio button. Otherwise,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

Allow All Authenticated Users

Select Custom Policy ?

No Access Allowed

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.

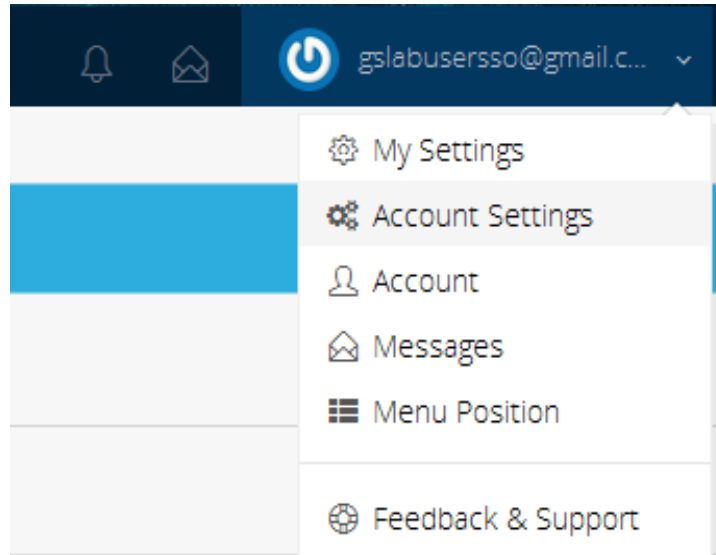


Configure Dome9 to Use RSA SecurID Access as an Identity Provider

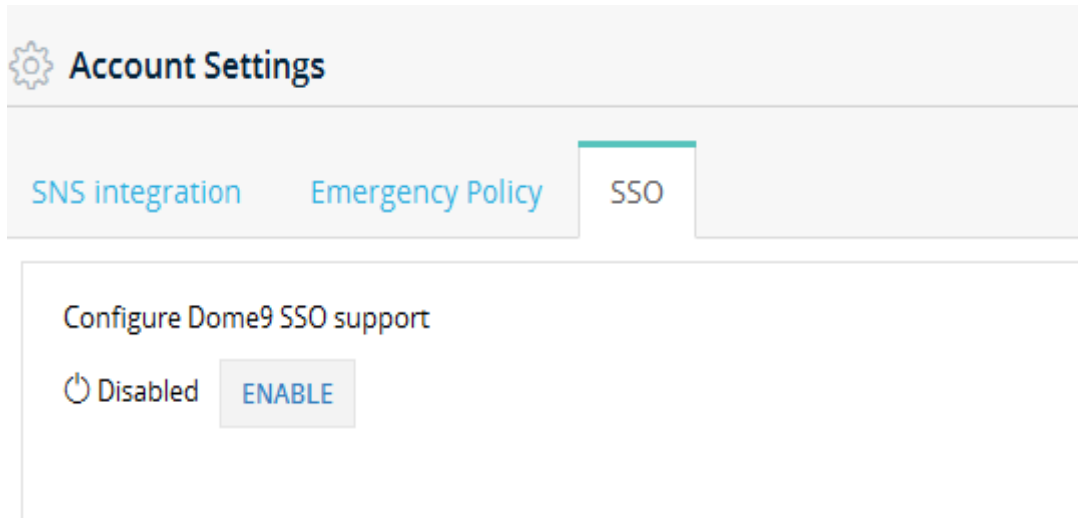
Follow below steps to configure Dome9 as service provider.

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.

SSO Configuration ×

Obtain the following items from the Identity Provider and enter them below

Account ID

gslab

Issuer

https://dome9.com

Idp Endpoint Url

https://portal.sso5.pe-lab.com/IdPServlet?idp_id=rozyp5ncs6

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

X.509 Certificate

```
arGqDFtvIE3rFZY0qTqID
GPOEPtwTwhc9pLom4J36Yibtfo1ZJkwUC6oi7Qv19CBbhz
6S3eNCPOJQQKQWovYW
cHgtXbFPtRsnh4XbdHD4xBd3Ag066yj7bHXiUiBOAN3LnH
b9M2iVCs7B9C9kUaKR
iWgfif5W6Sw23xphaekNHgsvxjorNr
/3LQV9vt0F1rOUgkjUqixCnnYaooA0Jv67
VZwjsEI5EJK1i
/SrOUOSuppC3CF2Sywkuezp0HaMO+RoVUyBB
/wjLpnNYLDcTZ07
xxq48pTdRcxwcg==
```

CANCEL

SAVE

7. Click the **Save** button.

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

SNS integration Emergency Policy SSO

Configure Dome9 SSO support

✓ Enabled DISABLE EDIT

Login Page <https://secure.dome9.com/sso/gslab>

Issuer <https://dome9.com>

IDP Endpoint https://portal.sso5.pe-lab.com/IdPServlet?idp_id=rozyp5ncs6m7

Creating user for SSO

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

Analysis Users & Roles

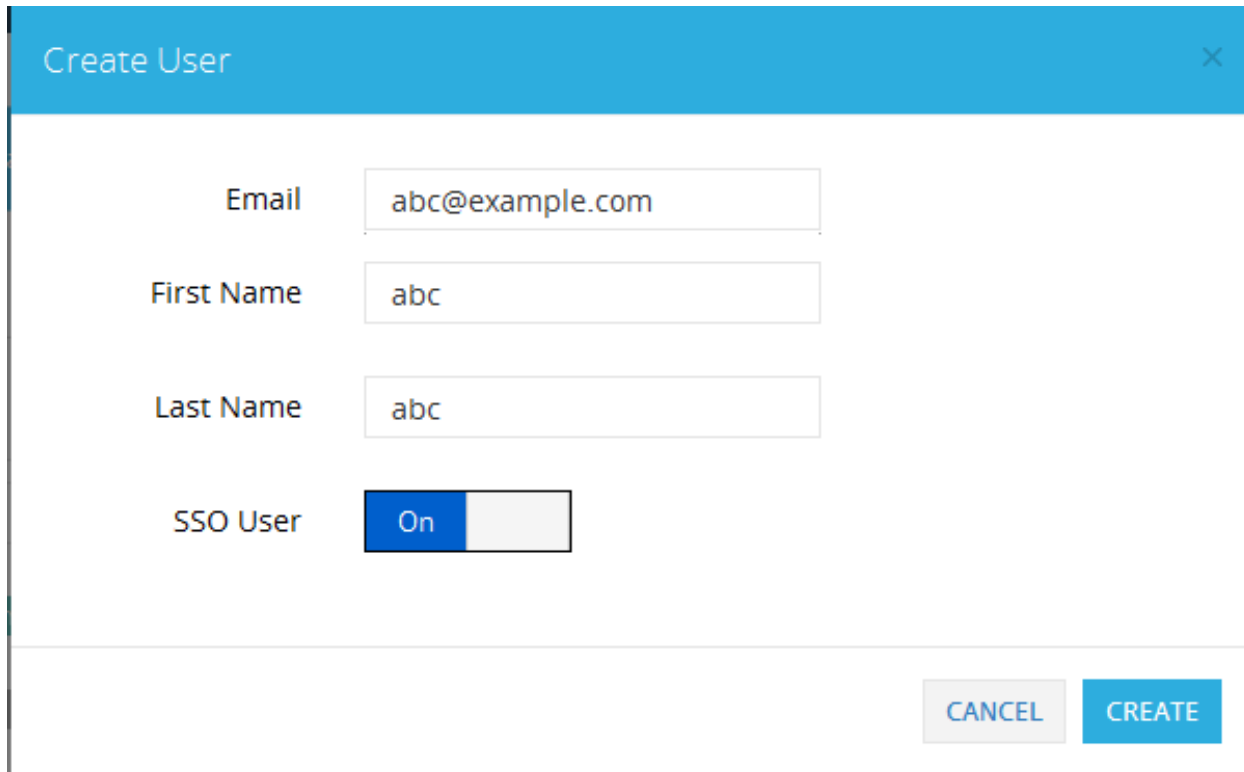
Users & Roles

Add Dome9 users and manage their role based access. You can define fine grained permissions per user or role allowing users to view or manage all assets or only specific assets up to the level of security group.

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



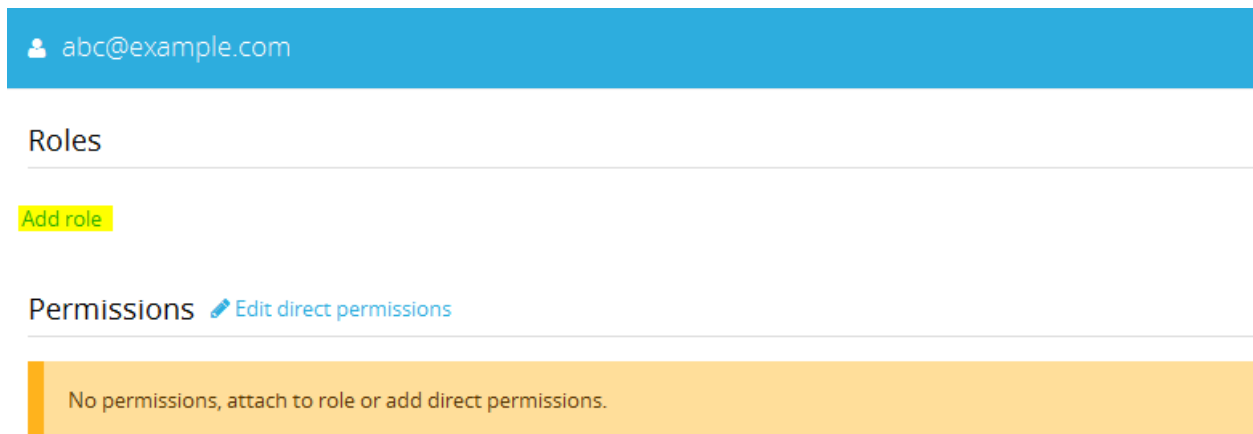
3. In the Create User section, fill in all the details of your user. Make sure that SSO User field is **On**.



The screenshot shows the 'Create User' form. The form has a blue header with the text 'Create User' and a close button (X) on the right. The form contains four input fields: 'Email' with the value 'abc@example.com', 'First Name' with the value 'abc', and 'Last Name' with the value 'abc'. Below these fields is a toggle switch for 'SSO User', which is currently set to 'On'. At the bottom right of the form, there are two buttons: 'CANCEL' and 'CREATE'.

4. Click on **Create**.

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



abc@example.com

Roles

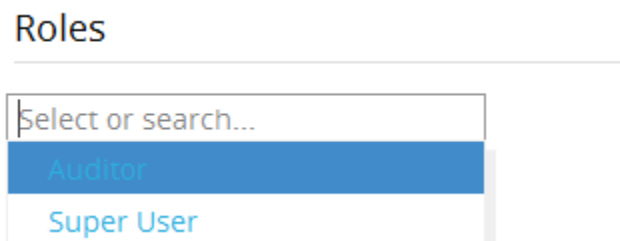
Add role

Permissions

[Edit direct permissions](#)

No permissions, attach to role or add direct permissions.

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



Roles

Select or search...

Auditor

Super User

7. Click on **Close**.