

Configure Dome9 Arc for Single Sign-On

Configuring Dome9 Arc for SSO enables administrators to manage their users using Citrix Gateway service. Users can securely log on to Dome9 Arc using their enterprise credentials.

To configure Dome9 Arc for SSO through SAML, follow the steps below:

1. In a browser, type the URL, <https://secure.dome9.com/v2/login> and press **Enter**.
2. Type the credentials and click **Login**.

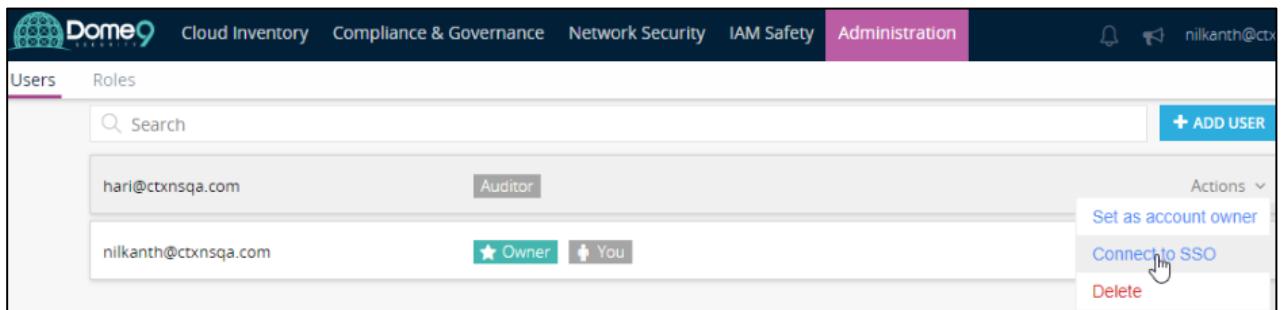


3. On the Landing page, navigate to **Administration > Users**.

4. Click on the **Actions** drop-down list against the required user and click **Connect to SSO**.

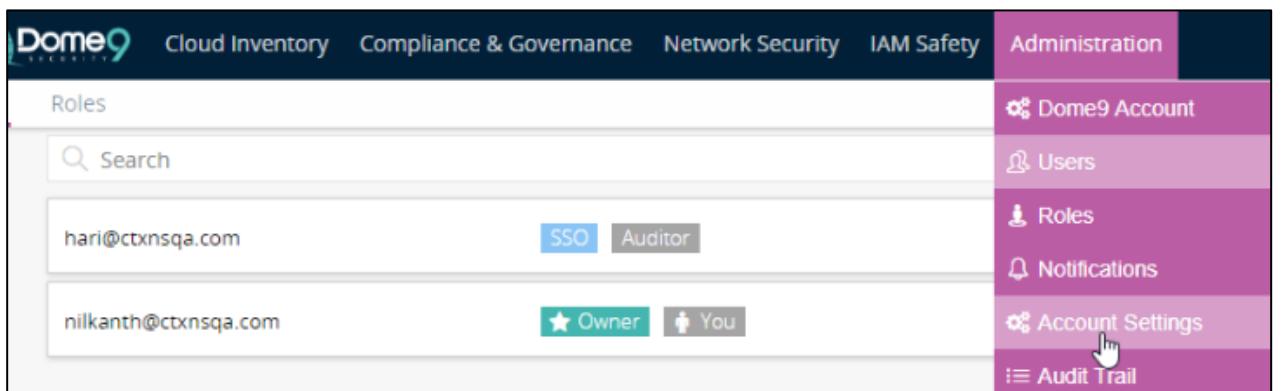
Note: Administrator can configure the SSO settings but cannot perform the SSO authentication. Administrator can add users and enable SSO authentication for them.

istrator



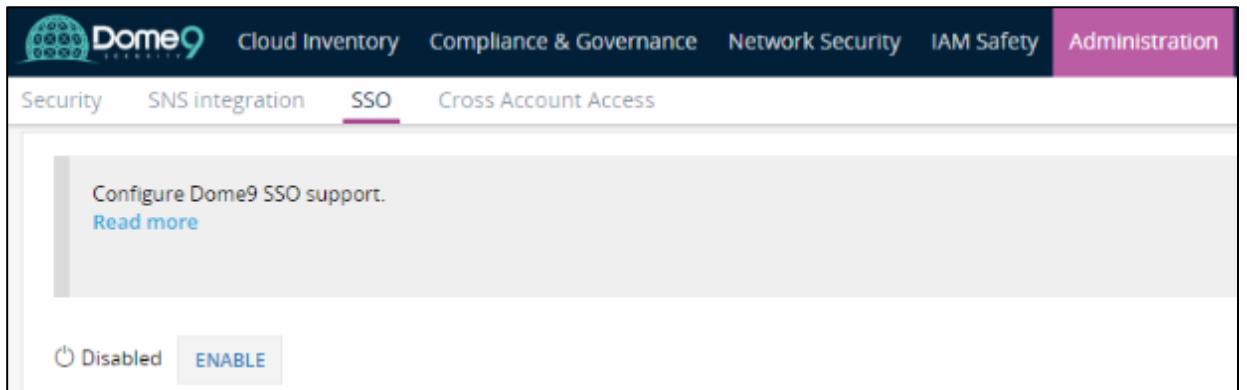
The screenshot shows the Dome9 Administration interface. The top navigation bar includes Cloud Inventory, Compliance & Governance, Network Security, IAM Safety, and Administration. The Administration tab is selected. Below the navigation is a search bar and a 'ADD USER' button. The main area is titled 'Users' and shows two entries: 'hari@ctxnsqa.com' with the role 'Auditor' and 'nilkanth@ctxnsqa.com' with the roles 'Owner' and 'You'. A context menu is open for the second user, with the 'Connect to SSO' option highlighted.

5. Navigate to **Administration > Account Settings**.



The screenshot shows the Dome9 Administration interface with the 'Roles' tab selected. It lists two users: 'hari@ctxnsqa.com' with the roles 'SSO' and 'Auditor', and 'nilkanth@ctxnsqa.com' with the roles 'Owner' and 'You'. The right sidebar contains navigation links: Dome9 Account, Users, Roles, Notifications, Account Settings (which is highlighted with a mouse cursor), and Audit Trail.

6. On the SSO page, click **Enable**.



The screenshot shows the SSO configuration page. The top navigation bar includes Cloud Inventory, Compliance & Governance, Network Security, IAM Safety, and Administration. The Administration tab is selected. Below the navigation is a sub-navigation bar with Security, SNS Integration, SSO (which is selected and highlighted in blue), and Cross Account Access. The main content area displays a message: 'Configure Dome9 SSO support.' with a 'Read more' link. At the bottom is a control panel with a 'Disabled' button and an 'ENABLE' button.

7. On the SSO Configuration page, specify the following details:

SSO Configuration

Obtain the following items from the Identity Provider and enter them below [?](#)

Account ID 1

Issuer 2

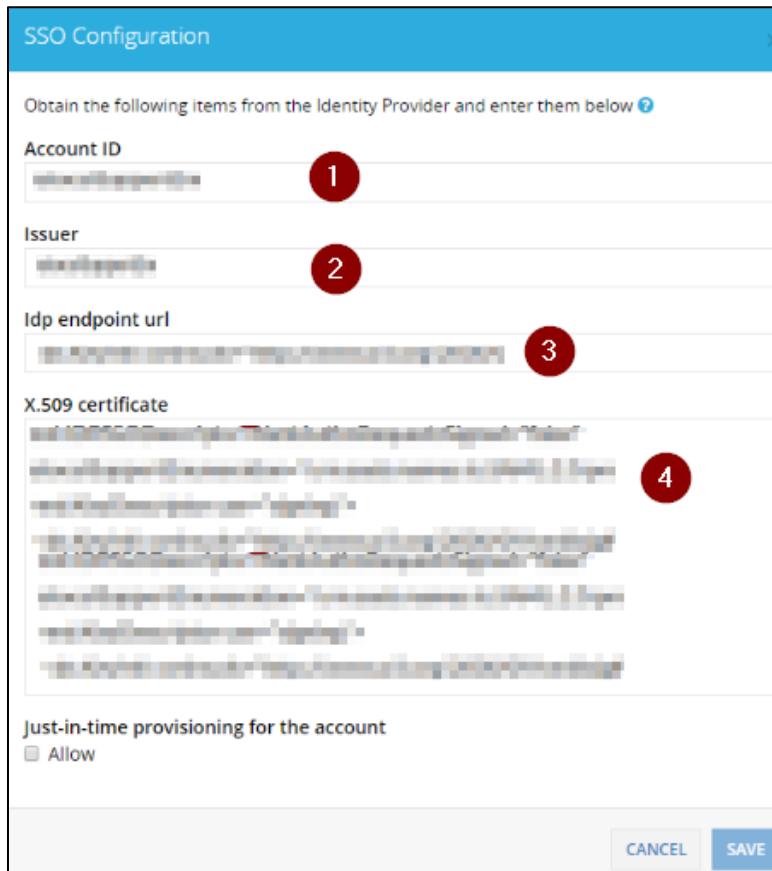
Idp endpoint url 3

X.509 certificate 4

Just-in-time provisioning for the account

Allow

CANCEL SAVE



- i. **Account ID:** Enter the account ID.
- ii. **Issuer:** Type a unique issuer ID.
- iii. **Idp endpoint url:** Enter the IdP URL, SAML 2.0 endpoint, for example, <https://example.com/saml/login>
- iv. **X.509 certificate:** To upload the certificate:
 - a. Remotely access your NetScaler instance using PuTTY.
 - b. Navigate to `/nsconfig/ssl` folder (using shell command `cd /nsconfig/ssl`) and press **Enter**.
 - c. Type `cat <certificate-name>` and press **Enter**.

```
1 -----BEGIN CERTIFICATE-----
2 MIIFPzCCBegIApJY189Tw/6/mHRS5nGDUzANBgkqhkiG9w0BAQsFADBN
3 HQs=-----  
4 aWc=-----  
5 NTE=-----  
6 BAc=-----  
7 Lje=-----  
8 ADC=-----  
9 yVj=-----  
10 Kjf=-----  
11 vdE=-----  
12 RK2=-----  
13 Ryc=-----  
14 NBA=-----  
15 +Cc=-----  
16 Y2v=-----  
17 BBY=-----  
18 Ly9=-----  
19 Oi8=-----  
20 Mdc=-----  
21 dC5=-----  
22 GGK=-----  
23 Y2v=-----  
24 dDA=-----  
25 PA6=-----  
26 +Xz=-----  
27 gSf=-----  
28 C+H=-----  
29 UOZurwimopre1chajfor3mwnCZCKp000051wq1hWQ0d12/m7WzQbAzy4NQ
30 6ED5
31 -----END CERTIFICATE-----
32
```

d. Copy the text between -----BEGIN CERTIFICATE----- and -----END CERTIFICATE-----

8. Click **Save**.

The SSO configuration is saved.