Configuring Unifi

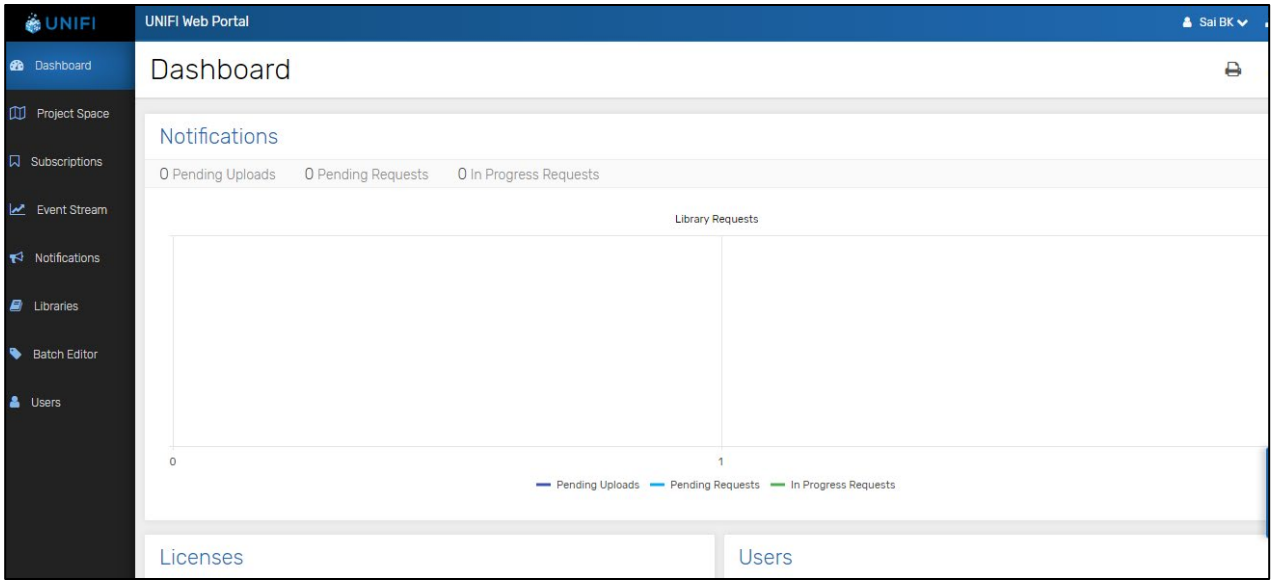
Configuring Unifi for SSO enables administrators to manage their users using Citrix Gateway. Users can securely log on to Unifi using their enterprise credentials.

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

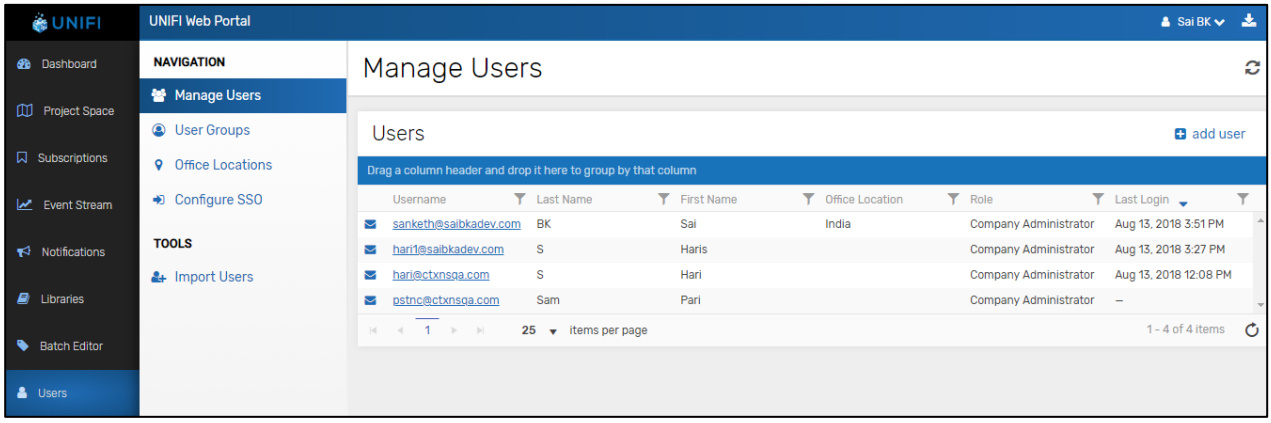
1. In a browser, type the URL, https://app.discoverunifi.com/ and press **Enter.**

2. Type the credentials, and click **Log in**.

The Dashboard page appears.



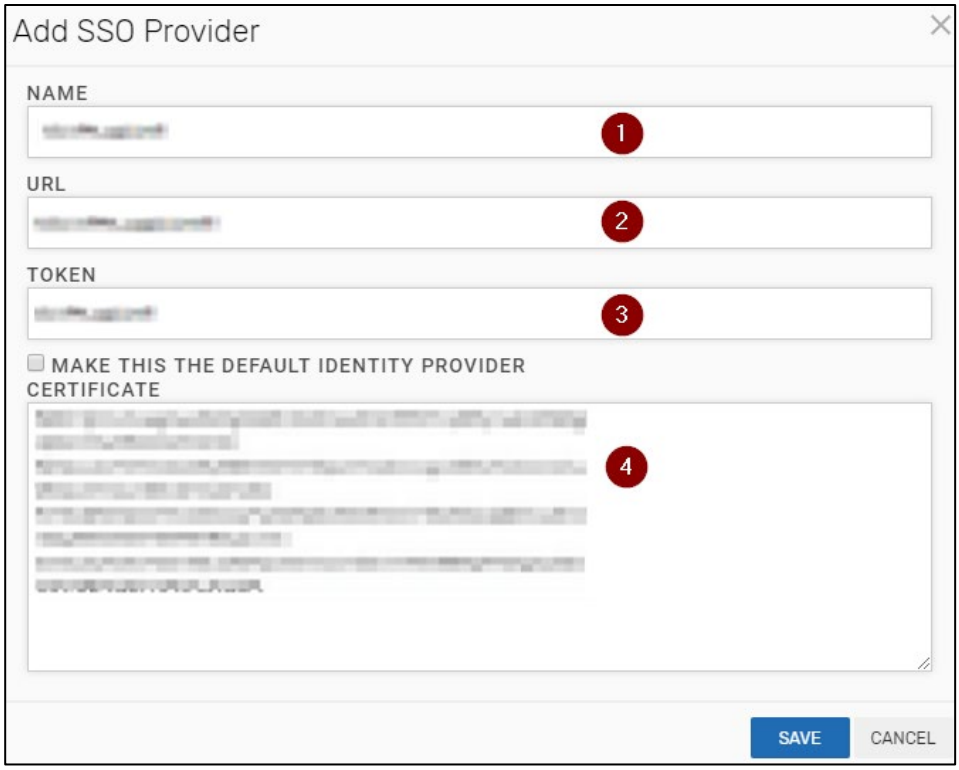
3. On the Dashboard page, click **Users** in the left pane.



4. Under the Navigation pane, click **Configure SSO**.

5. On the SSO Identity Providers page, click **Add Provider**.

6. On the Add SSO Provider dialog box, type the following information:



i. **Name**: Type the name for the IDP provider.

ii. **URL**: Enter the IdP URL, SAML 2.0 endpoint, for example, https://example.com/saml/login.

iii. **Token**: Type the issuer name.

iv. **Certificate**: Select the checkbox, to make the uploaded certificate as the default 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**.

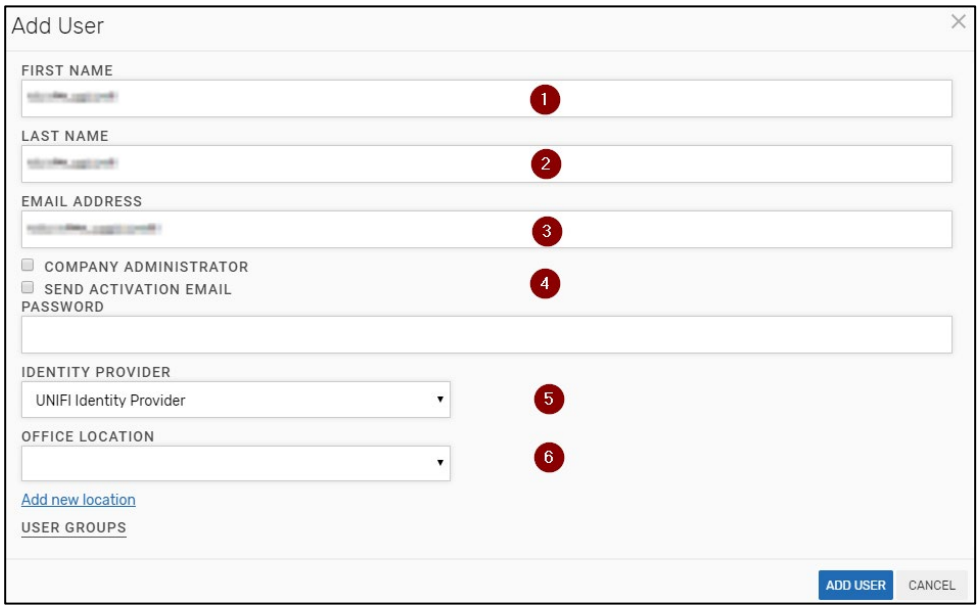
d. Copy the text between -----BEGIN CERTIFICATE----- and -----END CERTIFICATE-----

7. Click **Save**.

8. Under the Navigation pane, click **Manage Users**.

9. On the Manage Users page, click **Add User**.

10. On the Add User dialog box, type the following information:



i. **First Name**: First name of the user.

ii. **Last Name**: Last name of the user.

iii. **Email Address**: Email address of the user.

iv. **Company Administrator/Send Activation Email:** Select the appropriate checkbox.

v. **Identity Provider**: Select the appropriate identity provider option from the drop-down list.

vi. **Office Location**: Select the appropriate location option from the drop-down list.

11. Click **Add User**.

The configuration is successful.