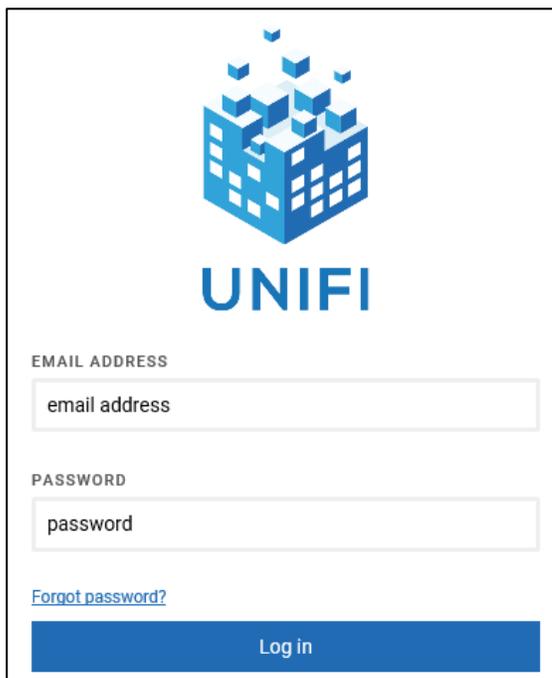


Configuring Unifi

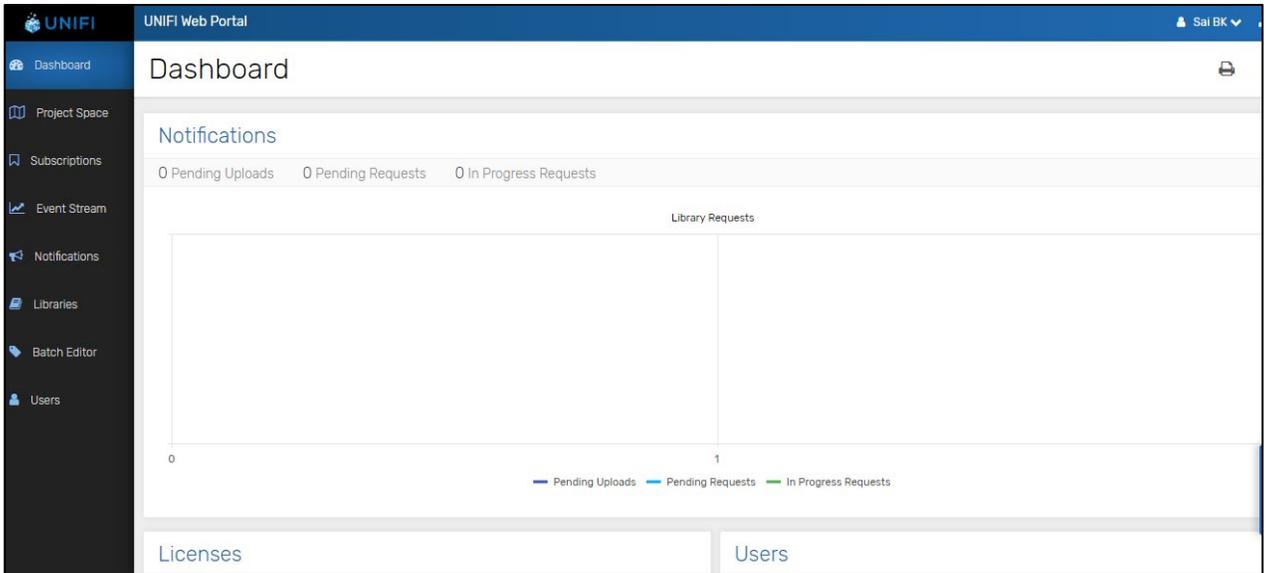
Configuring Unifi for SSO enables administrators to manage their users using Citrix Gateway. Users can securely log on to Unifi using their enterprise credentials.

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

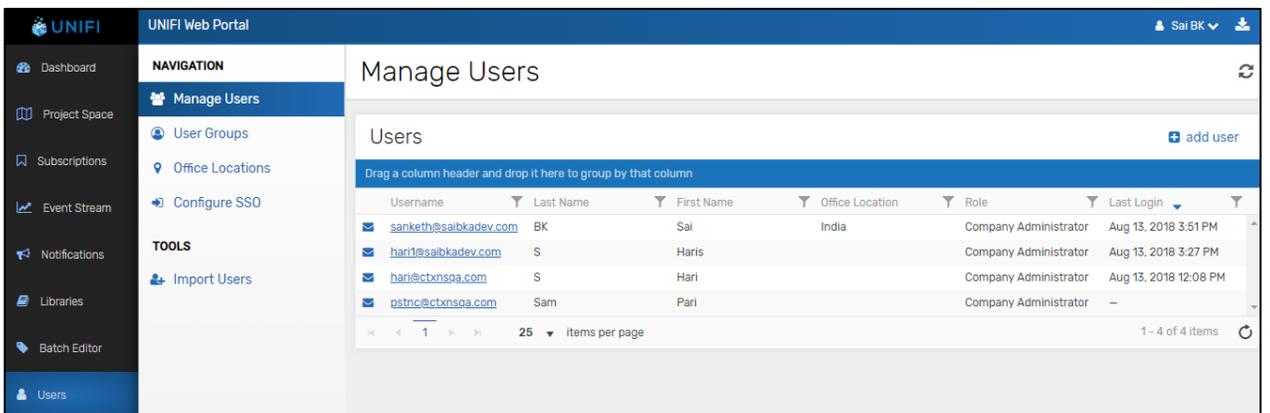
1. In a browser, type the URL, <https://app.discoverunifi.com/> and press **Enter**.
2. Type the credentials, and click **Log in**.



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:

The screenshot shows a dialog box titled "Add SSO Provider". It contains the following fields and controls:

- NAME:** A text input field with a red circle containing the number "1" to its right.
- URL:** A text input field with a red circle containing the number "2" to its right.
- TOKEN:** A text input field with a red circle containing the number "3" to its right.
- CERTIFICATE:** A section with a checkbox labeled "MAKE THIS THE DEFAULT IDENTITY PROVIDER CERTIFICATE" and a large text area for pasting a certificate. A red circle containing the number "4" is to the right of the text area.
- Buttons:** "SAVE" and "CANCEL" buttons at the bottom right.

- 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**.

```

1 -----BEGIN CERTIFICATE-----
2 MIIFPzCCBCEgAwIBAgIQApjY189Tiw/6/mHRS5nGDuzAMBgqhkiG9w0BAQsFADBN
3 NQs=
4 allc
5 HTE
6 BAc
7 LjE
8 ADC
9 yVj
10 Kjf
11 vdE
12 RK2
13 RYC
14 MBa
15 +Cc
16 Y2V
17 BBY
18 LyS
19 Ois
20 MDC
21 dCE
22 GGF
23 Y2V
24 dDA
25 PA6
26 +Xz
27 gSf
28 c+r
29 UOZLmnmupre1cnaJjor3WlCzckp0u9TqenWZwLAdQ0aIz/m7az0qBzy4ND
30 6ED5
31 -----END CERTIFICATE-----
32

```

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:

The screenshot shows the 'Add User' dialog box with the following fields and callouts:

- 1: FIRST NAME
- 2: LAST NAME
- 3: EMAIL ADDRESS
- 4: COMPANY ADMINISTRATOR and SEND ACTIVATION EMAIL
- 5: IDENTITY PROVIDER (dropdown menu)
- 6: OFFICE LOCATION (dropdown menu)

At the bottom of the dialog, there are buttons for 'ADD USER' and 'CANCEL'.

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.