

Configuring Front

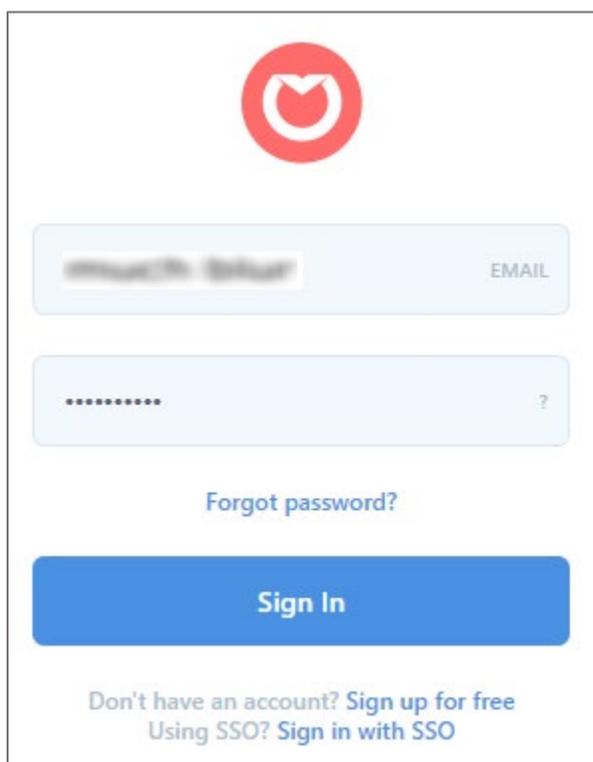
Configuring Front for single sign-on (SSO) enables administrators to manage users of Citrix ADC. Users can securely log on to Front by using the enterprise credentials.

Prerequisite

Browser Requirements: Internet Explorer 11 and above

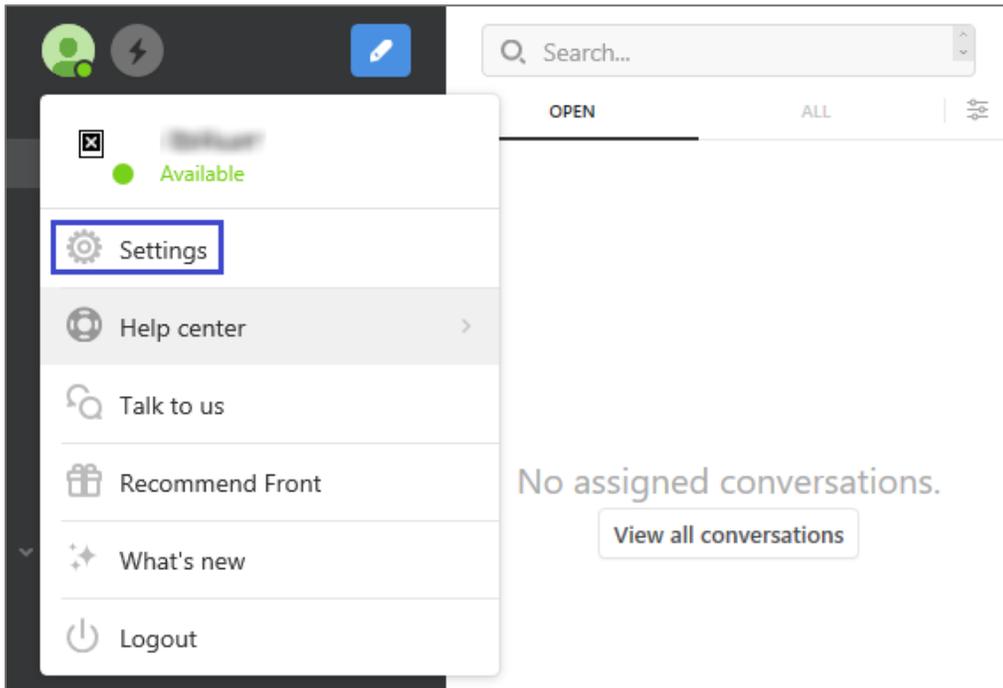
To configure Front for SSO by using SAML:

1. In a browser, type <https://frontapp.com/> and press **Enter**.
2. Type your Front admin credentials (**Your email** and **Your password**) and click **Sign In**.

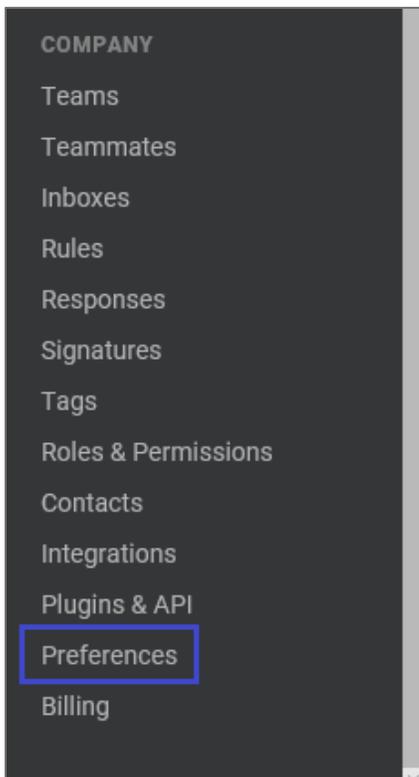


The image shows a screenshot of the Front app login page. At the top center is the Front logo, a red circle with a white stylized 'M' inside. Below the logo are two input fields: the first is for the email address, with a placeholder 'EMAIL' and a small 'EMAIL' label to its right; the second is for the password, with a placeholder of ten dots and a small '?' label to its right. Below the password field is a link that says 'Forgot password?'. At the bottom of the form is a large blue button with the text 'Sign In'. Below the button, there is a link that says 'Don't have an account? Sign up for free' and another link that says 'Using SSO? Sign in with SSO'.

3. In the top-left corner, click the user account icon and select **Settings** from the drop-down menu.



4. In the left panel, scroll down and click **Preferences** under **COMPANY**.



- In the **Company preferences** page, click **Single Sign On**.

The screenshot shows the 'Company preferences' interface. The 'General' section is active, and the 'Single Sign On' sub-tab is highlighted with a blue border. The settings are as follows:

- Bump on comment:** Move a conversation to the top when a new comment is posted.
- Bump on assign:** Move a conversation to the top when it's assigned.
- Allow non-administrators to delete conversations:** Disable if you want regular users to always archive.
- Allow conversations to be moved to all team inboxes:** Enable to let teammates move to team inboxes they cannot access.
- Session idle timeout:** Log out user if idle for more than this period of time.

- Scroll down and enter the values for the following fields in **SAML Integration**:

Field Name	Description
SSO	Select SAML from the drop-down list.
ENTRY POINT	IdP logon URL
Authentication request binding	Select HTTP Post from the drop-down list.
Signing Certificate	Copy and paste the IdP certificate. The IdP certificate must begin and end with -----Begin Certificate----- and -----End Certificate----- Note: The IdP Certificate is provided by Citrix and can be accessed from the link below: https://ssb4.mgmt.netscalergatewaydev.net/idp/saml/templatetest/idp_metadata.xml

Cancel

Save

Single Sign On

SAML ▾

Enabling Single Sign On (SSO) will force Disable SAML the method of your

- Disable
- SAML ✓

[Read our SSO documentation.](#)

ENTRY POINT
[Redacted]

URL of your identity provider which will receive authentication requests

Authentication request binding

Method with which the authentication request will be sent to your identity pro...

HTTP Post ▾

Signing certificate

```
-----BEGIN CERTIFICATE-----  
[Redacted]  
-----END CERTIFICATE-----
```