

# Configure 4me

Configuring 4me for single sign-on (SSO) enables administrators to manage users of Citrix ADC. Users can securely log on to 4me by using the enterprise credentials.

## Prerequisite

Browser Requirements: Internet Explorer 11 and above

## To configure 4me for SSO by using SAML:

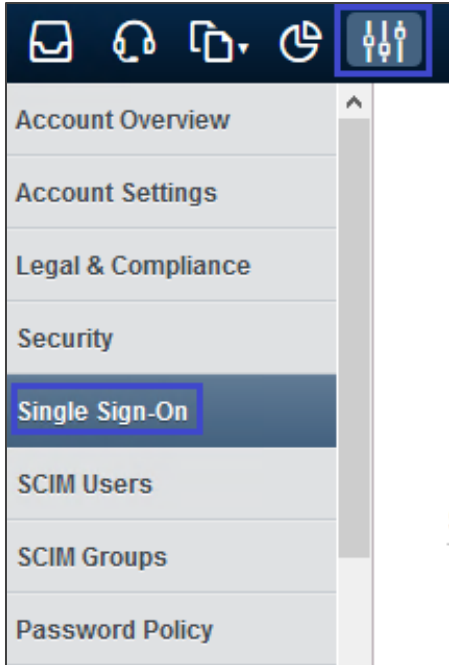
1. In a browser, type <https://www.4me.com/> and press **Enter**.
2. Provide all the necessary details with the 4me team to set up an account with SSO settings.
3. Paste the link given by 4me in a browser and press **Enter**.
4. Type your 4me admin account credentials (**Email** and **Password**) and click **Sign In**.



The screenshot shows a login form with the following elements:

- Email** label above a text input field.
- Password** label above a text input field.
- A blue **Sign In** button.
- A blue hyperlink labeled [Need help signing in?](#)

5. Select **Settings** icon in the navigation bar and click **Single Sign-On**.




6. In the **Single Sign-On** section, select **Enabled** check box and enter the values for the following fields.

Field Name	Description
Remote logout URL	Remote logout URL
IP Ranges	IP Ranges

### Single Sign-On

---



**Enabled**  
 Single Sign-On allows you to use an existing authentication mechanism with 4me such that you can provide centralized, fast and convenient access for your specialists and customers.

⚠ **Should you manage to somehow lock yourself out of 4me once you enable remote authentication, you can bypass single sign-on and access 4me using this URL:**  
**https://[redacted]/access/normal**

Remote logout URL

Your users will return to this URL after they logout.

IP ranges

Requests from these IP ranges will always be routed via remote authentication. Requests from IP addresses outside these ranges will be routed to the normal login page. To route all requests through remote authentication, simply leave this field blank. An IP range is represented as an IPv4 or IPv6 address or using the **CIDR** notation where both IPv4 and IPv6 subnets are supported. Separate multiple IP ranges with commas or spaces.

Your current IP address is: 115.110.156.50/32

7. In the **SAML** section, enter the values for the following fields.

Field Name	Description
SAML SSO URL	Identity provider SSO URL
Certificate fingerprint	Copy and paste the IdP certificate fingerprint from the <a href="https://www.samltool.com/fingerprint.php">https://www.samltool.com/fingerprint.php</a> link, select <b>SHA1 Algorithm</b> and <b>CALCULATE FINGERPRINT</b>
Secondary fingerprint	Copy and paste the IdP certificate fingerprint from the <a href="https://www.samltool.com/fingerprint.php">https://www.samltool.com/fingerprint.php</a> link, select <b>SHA1 Algorithm</b> and <b>CALCULATE FINGERPRINT</b>

**SAML**

SAML SSO URL

This is the URL that 4me will invoke to redirect users to your Identity Provider.

Note that our Assertion Consumer Service (ACS) URL is:  
`https://[redacted]/access/saml/consume`

To assist with troubleshooting, our SAML 2.0 metadata is located at:  
`https://[redacted]/access/saml/metadata`

Certificate fingerprint

The SHA1 fingerprint of the SAML certificate. Obtain this from your SAML identity provider.

Secondary fingerprint

The SHA1 fingerprint of the secondary SAML certificate, used for certificate rollover purposes. Obtain this from your SAML identity provider.

8. Finally, click **Save**.