

Configuring Ximble

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

Prerequisite

Browser Requirements: Internet Explorer 11 and above

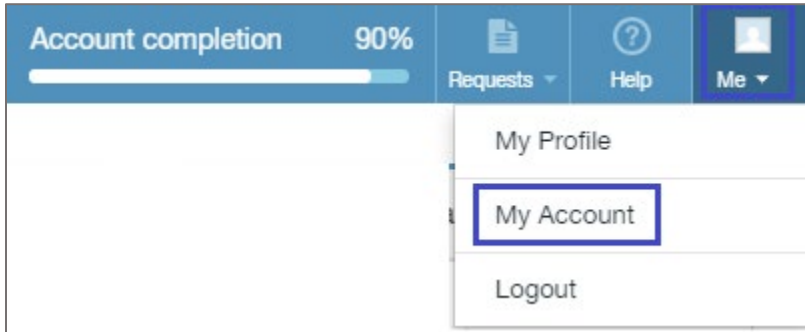
To configure Ximble for SSO by using SAML:

1. In a browser, type <https://app.ximble.com/login> and press **Enter**.
2. Type your Ximble admin account credentials (**Username** and **Password**) and click **Sign In**.

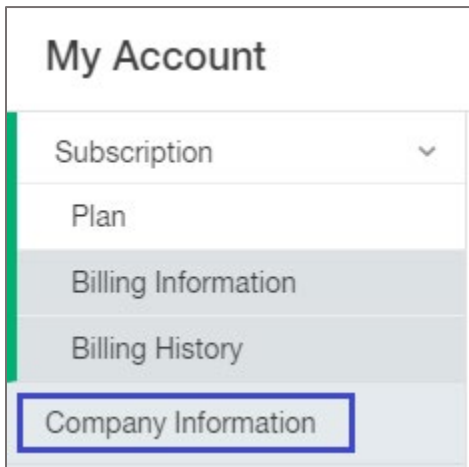


The screenshot shows the Ximble login interface. At the top left is the Ximble logo. Below it, the text "Sign In" is displayed. There are two input fields: the first is for the username, and the second is for the password, which is masked with dots. Below the password field is a checkbox labeled "Remember me". A large green button with the text "Sign In" is positioned below the checkbox. At the bottom of the form, there is a link that says "Other sign in options" with a downward-pointing arrow.

- In the top-right corner, click the user account and select **My Account** from the drop-down list.



- In the left panel, click **Company Information**.



- In the **Company Information** page, click the **Single Sign on Information** tab and enter the values for the following fields:

Field Name	Description
Identity Provider	Citrix
AppUrl	IdP logon URL
AppMetadataUrl	Copy and paste the IdP certificate URL. Note: The IdP Certificate URL is provided by Citrix and can be accessed from the below: https://ssb4.mgmt.netscalergatewaydev.net/idp/saml/templatetest/idp_metadata.xml

Company Information

Primary Contact Localization API Information **Single Sign on Information**

Identity Provider

AppUrl

AppMetadataUrl

Disable username and password modifications in Ximble for all users

Save

6. Finally, click **Save**.