

# Configure HelloSign for Single Sign-On

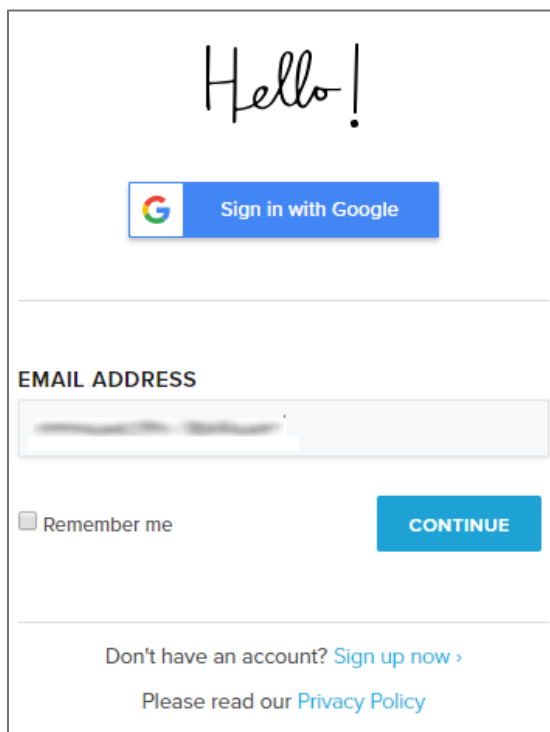
Configuring HelloSign for single sign-on (SSO) enables administrators to manage users of Citrix ADC. Users can securely log on to HelloSign by using the enterprise credentials.

## Prerequisite

Browser Requirements: Internet Explorer 11 and above

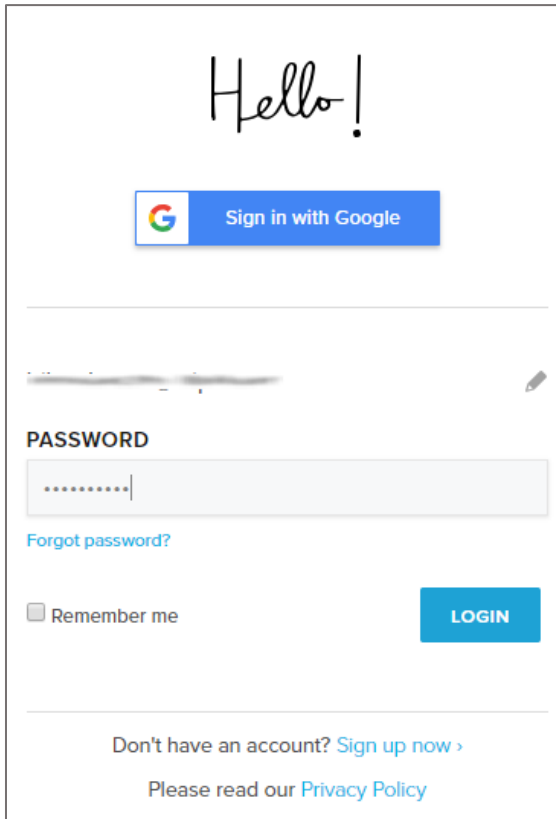
## To configure HelloSign for SSO by using SAML:

1. In a browser, type <https://app.hellosign.com/account/login> and press **Enter**.
2. Type your HelloSign admin email address and click **CONTINUE**.



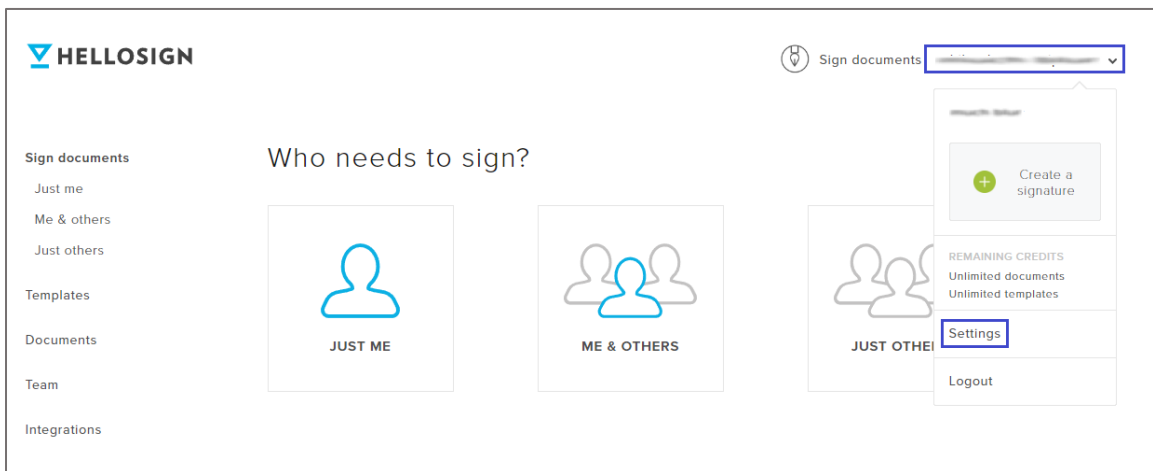
The screenshot shows the HelloSign login interface. At the top, the word "Hello!" is written in a large, handwritten-style font. Below it is a blue button with the Google logo and the text "Sign in with Google". A horizontal line separates this from the main login area. The label "EMAIL ADDRESS" is positioned above a text input field. Below the input field is a checkbox labeled "Remember me" and a blue button labeled "CONTINUE". At the bottom of the form, there are two links: "Don't have an account? Sign up now >" and "Please read our Privacy Policy".

3. Type your HelloSign admin password and click **LOGIN**.



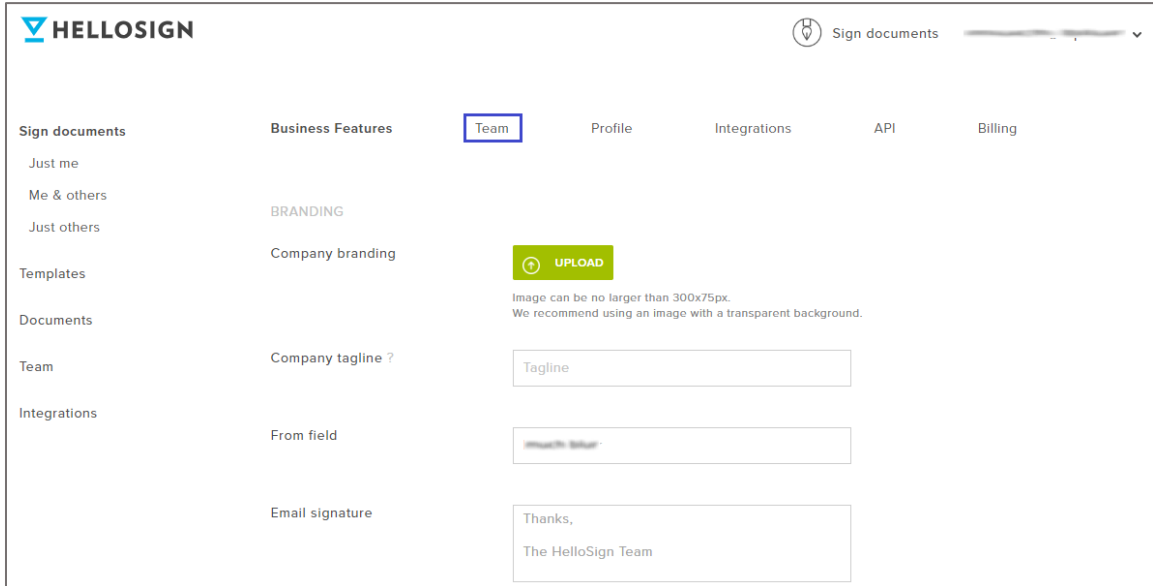
The image shows the HelloSign login page. At the top, it says "Hello!" in a handwritten font. Below that is a "Sign in with Google" button. There is a blurred input field for the email address. Below the email field is a "PASSWORD" label and a password input field with masked characters. To the left of the password field is a "Forgot password?" link. Below the password field is a "Remember me" checkbox. To the right of the password field is a blue "LOGIN" button. At the bottom, there are links for "Don't have an account? Sign up now >" and "Please read our Privacy Policy".

4. In the dashboard page, click the username in the top-right corner and select **Settings**.



The image shows the HelloSign dashboard. On the left is a navigation menu with items: Sign documents, Templates, Documents, Team, and Integrations. The "Sign documents" item is selected. The main content area is titled "Who needs to sign?" and has three options: "JUST ME" (one person icon), "ME & OTHERS" (two people icon), and "JUST OTHERS" (three people icon). The "JUST OTHERS" option is selected. On the right, there is a user profile dropdown menu. The menu is open and shows a "Create a signature" button, "REMAINING CREDITS" (Unlimited documents, Unlimited templates), "Settings" (highlighted with a blue box), and "Logout".

5. Click **Team**.



6. In the **TEAM SETTINGS** page, scroll down and select **Enable SAML SSO** check box under **SAML SSO**.

7. Enter the values for the following fields:

Required Information	Description
Identity Provider Single Sign-On URL	IdP logon URL
Identity Provider Issuer	Issuer URL
X.509 Certificate	Copy and paste the IdP certificate. The IdP certificate must begin and end with -----Begin Certificate----- and -----End Certificate----- <b>Note:</b> The IdP metadata URL is provided by Citrix and can be accessed from the link below. The link is displayed while configuring SSO settings for your app. <a href="https://gateway.cloud.com/idp/saml/&lt;citrixcloudcust id&gt;/&lt;app id&gt;/idp_metadata.xml">https://gateway.cloud.com/idp/saml/&lt;citrixcloudcust id&gt;/&lt;app id&gt;/idp_metadata.xml</a>

