

# Configuring Weekdone

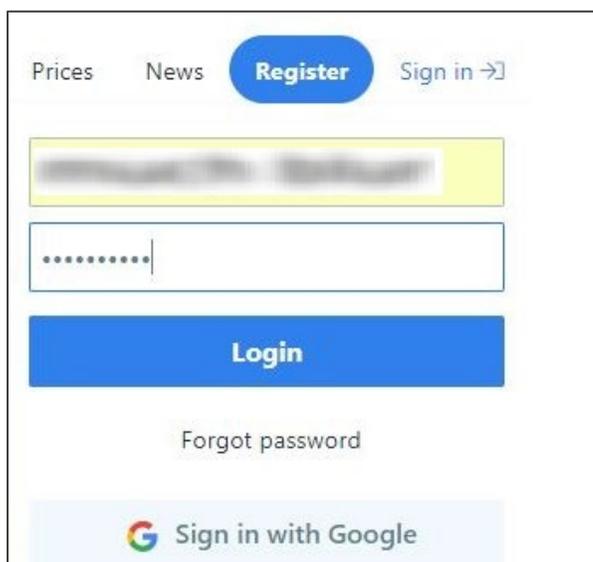
Configuring Weekdone for single sign-on (SSO) enables administrators to manage users using Citrix ADC. Users can securely log on to Weekdone by using the enterprise credentials.

## Prerequisite

Browser Requirements: Internet Explorer 11 and above

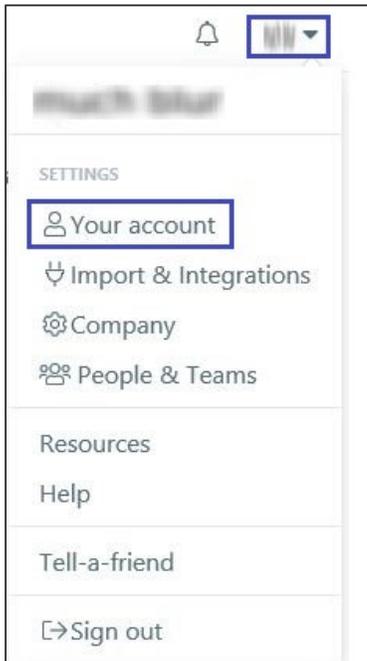
## To configure Weekdone for SSO by using SAML:

1. In a browser, type <https://www.weekdone.com> and press **Enter**.
2. Type your Weekdone admin account credentials (**Email** and **Password**) and click **Login**.

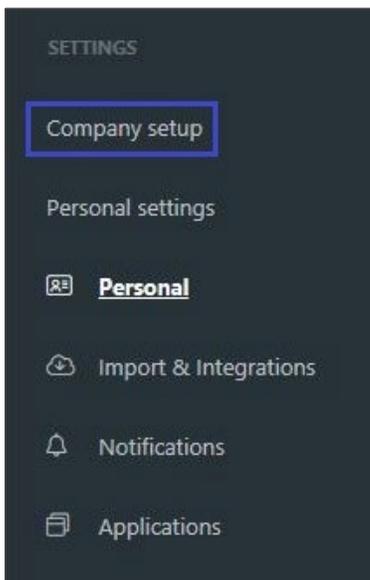


The screenshot shows the Weekdone login interface. At the top, there are navigation links for 'Prices', 'News', and a blue 'Register' button, followed by a 'Sign in →' link. Below this is a yellow rectangular box containing a blurred email address. Underneath is a password input field with a masked password of seven dots. A large blue 'Login' button is positioned below the password field. Below the 'Login' button is a link for 'Forgot password'. At the bottom of the form is a light blue button with the Google logo and the text 'Sign in with Google'.

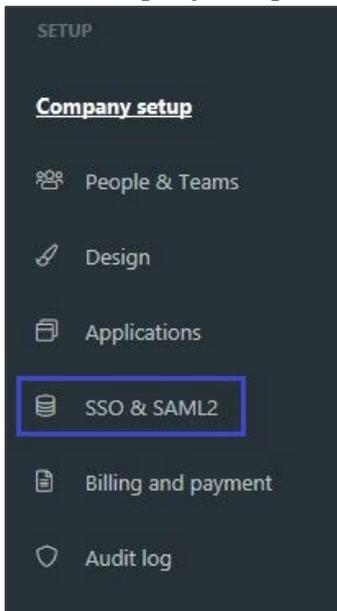
3. On the profile page, click the user profile icon at the top-right corner and select **Your account** under **Settings**.



4. In the left panel, select **Company setup** under **Settings**.



5. In the **Company setup** menu, select **SSO & SAML2**.



6. In the **Single sign-on SAML2** page, enter the values for the following fields:

Field Name	Description
SAML Name	Sign-in URL.
SAML SSO URL	IdP logon URL.
SAML Logout URL	Logout 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 Certificate is provided by Citrix and can be accessed from the link below: <a href="https://ssb4.mgmt.netscalergatewaydev.net/idp/saml/templatedes/t/idp_metadata.xml">https://ssb4.mgmt.netscalergatewaydev.net/idp/saml/templatedes/t/idp_metadata.xml</a>

The screenshot shows the 'Single sign-on SAML2' configuration page. At the top, there's a navigation bar with 'Settings' and a breadcrumb 'Setup > Company setup'. Below that, the title 'Single sign-on SAML2' is centered. A descriptive paragraph explains that SAML2 enables communication with an organization's IDP. The configuration fields are as follows:

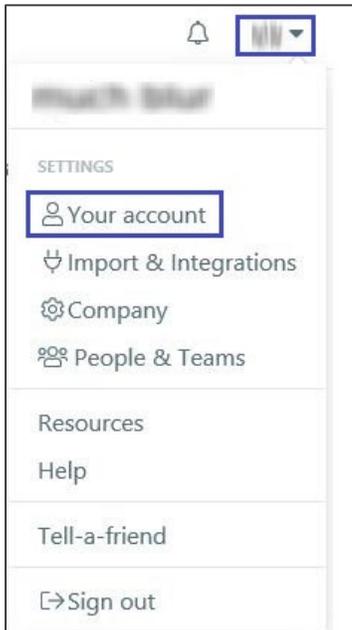
- SAML name:** Input field containing 'https://weekdone.com/a/'. Below it, a note says 'This is your sign-in URL. Please choose something unique and related to your company'.
- SAML SSO URL:** Input field containing a blurred URL. Below it, a note says 'This is the login URL of your Identity Provider'.
- SAML Logout URL:** Input field containing a blurred URL. Below it, a note says 'This is the URL where users will be redirected after they log out'.
- X509 Certificate:** Input field containing '-----BEGIN CERTIFICATE-----' followed by a long alphanumeric string 'MIIG6zCCBN0gAwIBAgJAlb8os82UsoPMA0GCSqGSIb3DQEBCwUAMI'. Below it, a note says 'Get this from your Identity Provider'.

A blue 'Save changes' button is located at the bottom center of the form.

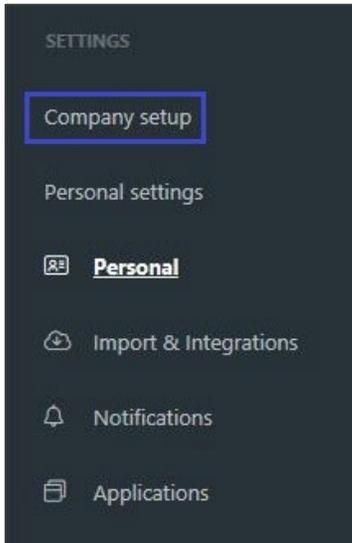
- 7 Finally, click **Save Changes**.

## To configure Weekdone for User Account:

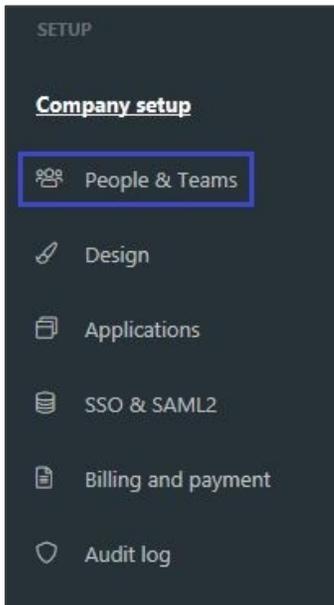
1. On the profile page, click the user profile icon at the top-right corner and select **Your account** under **Settings**.



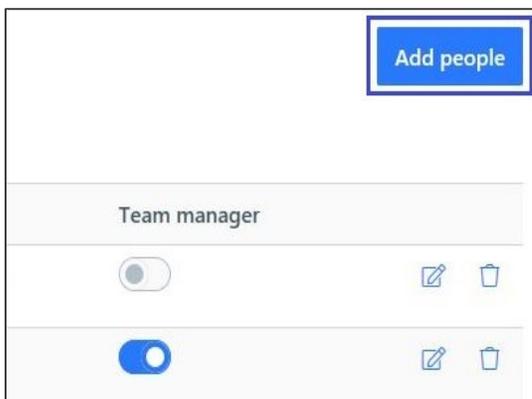
2. In the left panel, select **Company setup** under **Settings**.



3. In the **Company setup** menu, select **People & Teams**.



4. In the **People & Teams** page, click **Add people**.



5. In the **INVITE PEOPLE BY EMAIL** section, type the email address of the user and click **Invite**.

