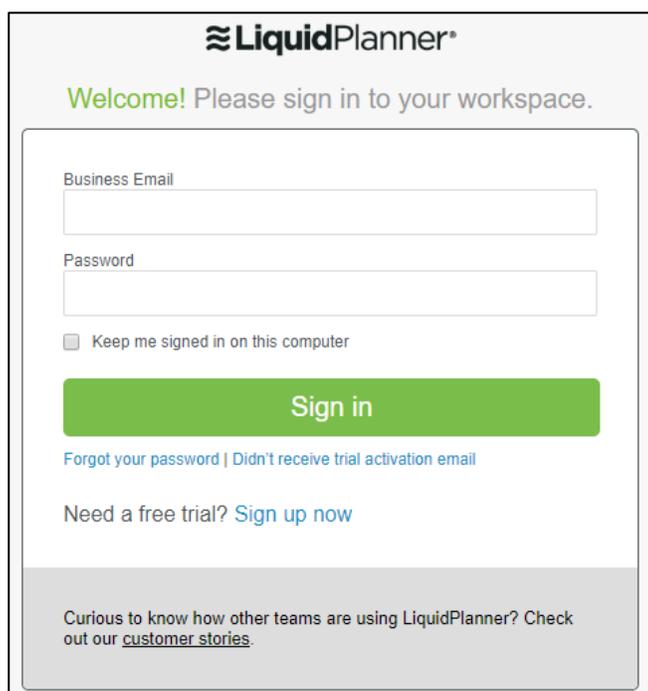


Configuring LiquidPlanner

Configuring LiquidPlanner for SSO enables administrators to manage their users using Citrix Gateway. Users can securely log on to LiquidPlanner using their enterprise credentials.

To configure LiquidPlanner for SSO through SAML, follow the steps below:

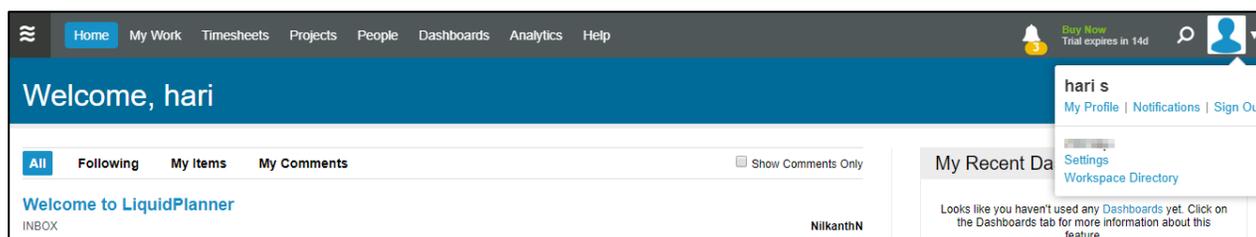
1. In a browser, type the URL, <https://app.liquidplanner.com/login> and press **Enter**.
2. Type the credentials, and click **Sign in**.



The screenshot shows the LiquidPlanner login interface. At the top, the LiquidPlanner logo is displayed. Below it, a green message says "Welcome! Please sign in to your workspace." The main form contains two input fields: "Business Email" and "Password". Below these fields is a checkbox labeled "Keep me signed in on this computer". A prominent green "Sign in" button is centered below the form. Underneath the button are two links: "Forgot your password" and "Didn't receive trial activation email". At the bottom of the form area, there is a link that says "Need a free trial? Sign up now". A footer section at the very bottom of the page contains the text: "Curious to know how other teams are using LiquidPlanner? Check out our [customer stories](#)."

The Home page appears.

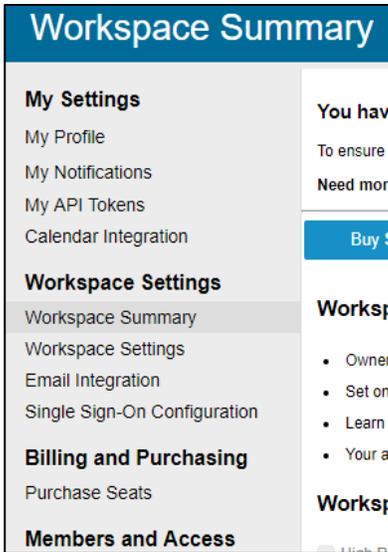
3. On the Home page, click on the profile image in the top right corner. Click **Settings**.



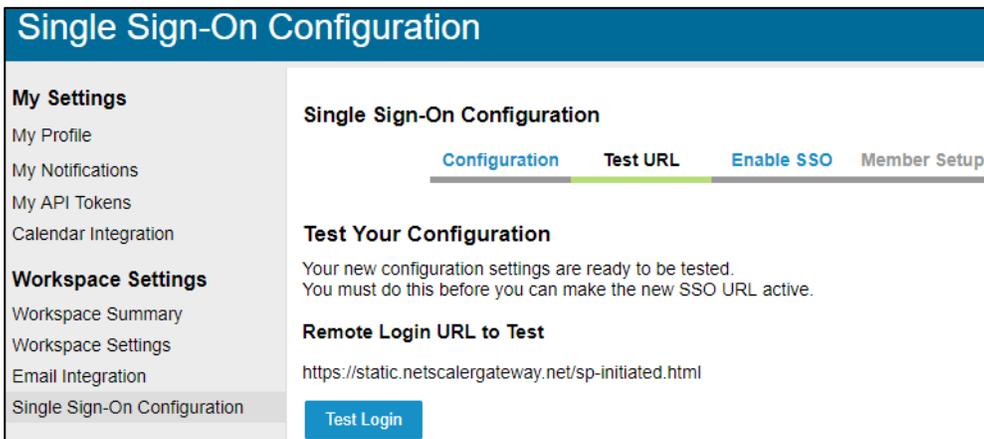
The screenshot shows the LiquidPlanner Home page. The top navigation bar includes links for Home, My Work, Timesheets, Projects, People, Dashboards, Analytics, and Help. On the right side of the navigation bar, there is a notification bell icon with a "3" badge, a "Buy Now" button with "Trial expires in 14d", and a user profile icon. Below the navigation bar, a large blue banner says "Welcome, hari". To the right of the banner is a user profile dropdown menu for "hari s" with options for "My Profile", "Notifications", and "Sign Out". Below the banner, there are tabs for "All", "Following", "My Items", and "My Comments", along with a "Show Comments Only" checkbox. The main content area shows "Welcome to LiquidPlanner" and "INBOX". On the right side, there is a "My Recent Data" section with links for "Settings" and "Workspace Directory". At the bottom right, there is a message: "Looks like you haven't used any Dashboards yet. Click on the Dashboards tab for more information about this feature."

The Workspace Summary page appears.

4. On the Workspace Summary page, under Workspace Settings, click **Single Sign-On Configuration** in the left pane.



The Single Sign-On page appears.



5. On the Single Sign-On page, click **Configuration** sub tab.
6. Type the following information:

Single Sign-On Configuration

Configuration Test URL Enable SSO Member Setup

Custom Subdomain Link ?
 https://app.liquidplanner.com/sso_login/ 196627

SAML Identity Provider Certificate ?

Fingerprint:

Or Upload Certificate File (currently "MIIG6zCCBN0gAwIBAgIJA1b8os82USoPMA0GCS...") **1**

No file chosen

Current Remote Login URL ?
 https://app.liquidplanner.com/saml/login

New Login URL to Test: ? **2**

Logout Landing URL (Optional) ? **3**

Service Provider Details ?

Metadata URL	https://app.liquidplanner.com/196627/sso/saml/metadata
SAML Version	2.0
Entity ID	https://app.liquidplanner.com/196627
Assertion Consumer URL	https://app.liquidplanner.com/196627/auth/saml/callback
Name ID Format	urn:oasis:names:tc:SAML:2.0:nameid-format:transient

Troubleshooting Notification:

Enter content to be displayed to end users so that they can easily contact someone to help them troubleshoot any issues.

- i. **SAML Identity Provider Certificate:** Click **Choose File**, and then follow prompts to select and save the file. You can also simply copy and paste (or type) in your SHA1 fingerprint.
- ii. **New Login URL to test:** Enter the new IdP URL, SAML 2.0 endpoint, for example, https://example.com/saml/login.
- iii. **Logout Landing URL:** Type the URL to be displayed after logout, for example, https://www.example.com.

7. Click **Save**.

8. Click **Enable SSO** sub tab. Click the appropriate radio button, and click **Save**.

Enable SSO for All Members:

Yes All full members and portal guests (excluding dashboard guests) added to this workspace will be required to use SAML 2.0 to authenticate.

No You can configure which members will be required to use SAML 2.0 and which will use an email address and password stored in LiquidPlanner to login.

The configuration is saved.