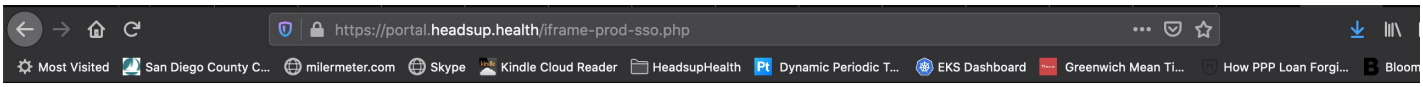
Hosting Heads Up in a Browser Iframe

(Updated 2021/10/20)

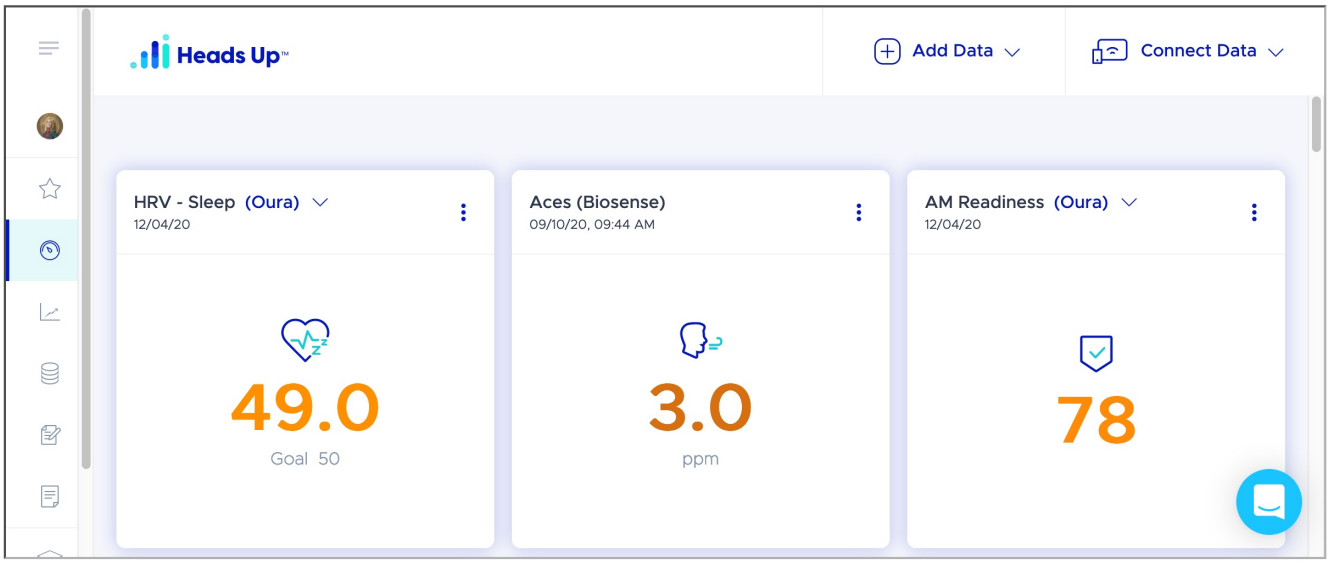
Overview

The Heads Up application can be configured to be hosted within an iframe on a customer portal page when used with the Encrypted Single Sign-on Link functionality to load the iframe content with an authenticated user session.

Standard Iframe Example



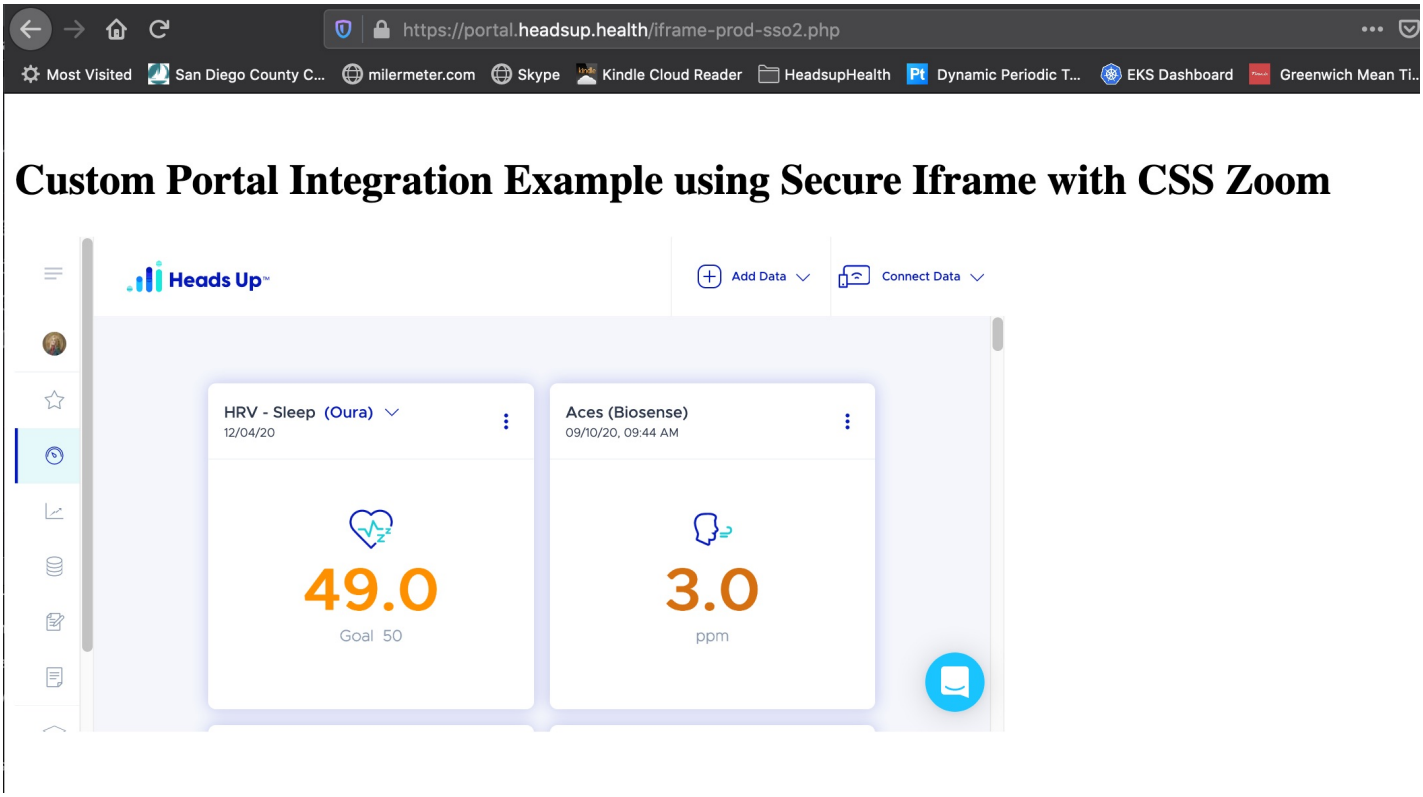
Custom SSO Secure Iframe Example



An iframe (short for inline frame) is an HTML element that allows an external webpage to be embedded in an HTML document. Unlike traditional frames, which were used to create the structure of a webpage, iframes can be inserted anywhere within a webpage layout. Iframes are used for several different purposes, such as online advertising and multimedia and usually contain an entire webpage.

The content of an iframe is usually independent of the parent website container page and the browser maintains strict security boundaries between the parent and any iframes contained on the page. Additionally, the layout and style of the iframe content cannot be controlled or changed by the parent website either. There are some CSS features that can be used by the parent website to shrink the content of the iframe, but those capabilities vary by browser.

Iframe Example using CSS to use the browser zoom capability



Security and Subdomain Usage

One of the benefits of using an iframe within an existing website is that the iframe content (Heads Up) operates independently of the hosting web application (your portal or website) and Heads Up will manage its own set of cookies and local storage that are secure and not sharable with the parent website. While this is a very powerful capability, it is often abused by bad actors, so browsers such as Chrome, Firefox, and Safari have implemented an additional level of security controls specific to securing iframe content and data.

When the Heads Up web application is included as an iframe on your site, it is considered to be cross-site domain content if the domain of those hosting page is different than the domain of the Heads Up web application in the iframe. This means that the browser will block the Heads Up content and cookies by default, which will prevent the Heads Up web application from working properly.

In order to enable a secure experience for the user, the owner of the parent website will have to contact Heads Up and purchase a license, which will provide the following in return:

- enable the Iframe capabilities that will allow the cross-site security headers,
- implement an endpoint to be used with a subdomain DNS entry
- register an SSL certificate in order to securely access the Heads Up website from with their page.

Iframe Entitlement Verification

If the Practitioner's Organization has not yet been entitled for the Iframe feature, the browser will block and not display any content from Heads Up or a subdomain. As previously mentioned, the owner of the Organization must ***contact someone from Heads Up Sales*** to purchase the appropriate license to enable and use this functionality.

There is a secure endpoint available to verify if the Organization has been entitled to access the Iframe feature or not. Using the API key and the unique Organization UUID that is provided by the owner of the Organization, this endpoint is available to verify if the capability has been enabled or not, and will return **true** or **false**, respectively. If **true**, then the Iframe should display the content from the Heads Up platform, assuming the subdomain and SSL cert have been properly configured and the SSO link is being generated correctly. If **false**, then the browser will block content from displaying in the Iframe. The API can be used by the host site to display alternative content in the iframe if the value is set to **false**.

This is an example of requesting the status of the Iframe entitlement: `curl -k -H "Content-type: application/json" -H "Authorization: Bearer <API Key>" https://app.headsuphealth.com/api/v1/organizations/<org_id>/entitlements/iframe_access_allowed`

A successful API request will return **true** or **false**.

Workaround for Testing

The steps outlined above are required for the iframe to work with Heads Up by default for users. However, users can also whitelist the Heads Up domain within their individual browser settings. This workflow is not ideal for most end users, but we recommend using it for testing the Heads Up iframe in your website before the subdomain is configured. To do this, use your browser settings to whitelist *.headsuphealth.com.

Optional Development Browser Configuration

During development, the browser can be manually configured to accept third party cookies from the Heads Up website: app.headsuphealth.com until the subdomain and SSL certificates have been configured.

Instructions for whitelisting the Heads Up application domain are available upon request.

Whitelisting The HeadUp Domain in Browsers

HIPAA Compliance

The data center environment used by the Heads Up application is fully HIPAA compliant and adheres to standard security practices which includes the encryption of data in transit and at rest, employs multi-factor authentication and data access logging. Heads Up also maintains a required Business Associate Agreement (BAA) with Amazon AWS Service which is also a requirement for HIPAA compliance. The use of an iframe and the single-sign-on functionality should have no impact on this as the security boundaries provided by the browsers maintain a secure connection within the iframe and the Heads Up web application.

Organization Setup Steps

These steps need to be completed by your development team:

Configure a Subdomain to Use for Hosting Iframe Content

If your hosting website address is something like *www.myhealth.com*, then a subdomain like *headsup.myhealth.com* would need to be created and registered with your website domain provider and an an associated SSL certificate will need to be register on your behalf with AWS.

Follow these steps:

1. Create a CNAME record with your DNS provider pointing your subdomain to *app.headsuphealth.com*
2. Verify that you can access the Heads Up platform using your subdomain in a browser tab.
3. Notify Heads Up Support of the subdomain(s) that you intend to use to access the Heads Up platform.
4. Heads Up will request an SSL certificate on your behalf with the AWS Certificate Manager and then return instructions from AWS about an additional CNAME record that you will need to add to your DNS provider to verify that you own the domain.
5. Once it has been verified by AWS, your SSL cert will need to be configured in our AWS infrastructure before it can be used.

6. After the SSL cert has been configured by Heads Up personnel, you should be able to use your secure subdomain address to access Heads Up.

HTML Implementation

Adding an iframe to an existing web page is very straightforward. The same generated encrypted SSO link as described in the SSO documentation should be used with the SRC attribute of the IFRAME tag.

```
<IFRAME src="http://<subdomain>/dashboard?org_uuid=600d9184-0460-4b81-a54a-b0baad1369e9&sec_p=lUb5fotCtfh836q7TJLLTkyTDUIoV2jvmTbotWzKqY2UVFPYss7WAUuRkV9ZWyRVZ2I5cHFvWUlvRFBiQ0JZL1" height="500" width="750" title="Heads Up Dashboard" name="heads_up_dashboard">
</IFRAME>
```

> One thing to keep in mind when adding an Iframe tag to your hosting page, is that the browser page load performance for the Iframe is greatly affected by the order and amount of other pages that are also loaded on the hosting page. It is highly recommended to include the Iframe tag as close to the top of the hosted page as possible and load other javascript links below it.

> This article describes the problem well: https://www.ernestojpg.com/2018/05/how-to-load-iframes-faster.html

Note: you can modify the link above to direct to a different page within Heads Up, if desired. For example, to direct the user directly to the Lab Results page rather than the Dashboard, use this link:

```
<IFRAME src="http:/<subdomain>/biomarkers?org_uuid=600d9184-0460-4b81-a54a-b0baad1369e9&sec_p=lUb5fotCtfh836q7TJLLTkyTDUIoV2jvmTbotWzKqY2UVFPYss7WAUuRkV9ZWyRVZ2I5cHFvWUlvRFBiQ0JZL1" height="500" width="750" title="Heads Up Dashboard" name="heads_up_dashboard">
</IFRAME>
```

When running in an iframe, the Heads Up web application will only allow access for authenticated client users of a specific Org. The SSO link provides an authenticated user session, so general access is not allowed.

Heads Up Setup Steps

These steps must be completed on the backend by a Heads Up administrator

Enabling Iframe Access for an Org

By default, the Heads Up web application and the browsers do not allow cross domain access, so it must be enabled for the customer's Organization.

The **iframe_access_allowed** entitlement must be added for the customer's organization and set to *true* to allow Iframe access.

Changelog

2021/10/20

- Updated with new section about page loading performance

2021/4/3

- Added section on iframe entitlement API
- Changed date formats

2021/3/9

- Updated instructions for CNAME record configuration to reflect the new pointer to app.headsuphealth.com
- Added subdomain setup steps details