SSO FOR Huddle

Customer Datasheet

# 1. Overview of SSO (Single Sign On) for Huddle

Single Sign-On (SSO) is an enterprise feature that allows administrators to connect Huddle to their organisation’s network directory service (be it Microsoft Active Directory, LDAP or Workday). Once connected, users can sign in to Huddle using just their existing network authentication infrastructure. Result: a secure solution where users don’t have to remember passwords and IT spends less time on password resets.

Our SSO is enabled by a technology called SAML 2.0, the industry standard for communicating identities over the Internet. Huddle has supported this for some time but we’ve now integrated with four of the leading cloud identity providers (IDPs), each of whom simplify the process and provide many additional security and management features. Huddle also supports Microsoft Active Directory Federation Service (AD FS).

|  |  |  |  |
| --- | --- | --- | --- |
| http://livehiveapp.com/cms/wp-content/uploads/2013/07/OneLogin-Logo.png?cc8d28 | http://blog.box.com/wp-content/uploads/2012/08/OKTA-1024x767.jpg | https://www.pingidentity.com/images/media-kit/PI_SQLogo.png | http://www.chippewa.ca/wp-content/uploads/2013/01/CentrifyLogoVerticalColorwithWhiteBackgroundHighRes1133x746.jpg |

# 2. Key benefits

|  |  |  |  |
| --- | --- | --- | --- |
| C:\Users\james.pipe\Documents\Helveticons\Helveticons Basic (png)\128x128\Lock 128x128.png | Security Allows password complexity to be set centrally by enterprise IT, users can be required to sign-in to Huddle via SAML. Disabling a user centrally through their identify provider (such as Active Directory) will then prevent them from accessing Huddle the next time they attempt to authenticate. | C:\Users\james.pipe\Documents\Helveticons\Helveticons Basic (png)\48x48\Fingerprint 48x48.png | Even more security Users can be required to use a strong authentication factor in addition to their password when they sign in. Our partners offer a plethora of options including native mobile apps, PKI certificates or any of the pre-integrated solutions from RSA, Symantec, VASCO and Yubico. |
| C:\Users\james.pipe\Downloads\like.png | User ConvenienceHuddle users can access business content, accept invitations and respond to notifications without needing to remember a further username and password. Huddle can be quickly adopted and becomes a seamless resource in the enterprise environment. |  | Works across the cloudHuddle’s SSO partners all natively support thousands of cloud and on-premise applications. This means that IT can roll out one set of usernames and passwords for virtually every single tool their users access. This means more productive users and less time wasted by IT on resetting forgotten passwords. |

# 3. Types of Single Sign On

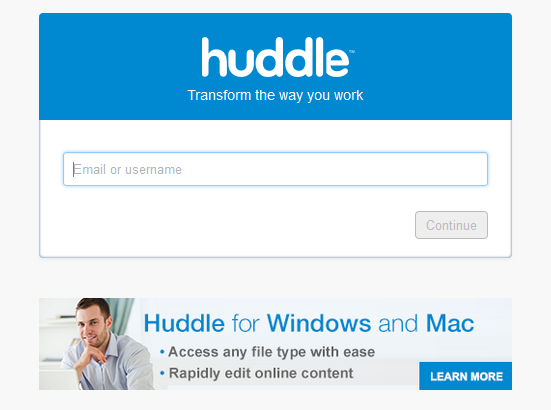
We have three types of Single Sign On flow available to our users. They have the same level of security and the choice of which to use is largely a question of user experience preference.

1. *SP (Service Provider) Initiated SSO*, which involves a user first going to the Huddle login page to kick off the SSO flow.
2. *IDP (Identity Provider) Initiated SSO for the web*, which involves a user first clicking on a link that takes them directly to the Identity Provider (IDP) like Active Directory, which in turn redirects them to the Huddle web application, so that they never see the login page.
3. *IDP Initiated SSO for the API*, which allows client applications to make use of the SSO flow to ensure their users do not need to see the Huddle login page first.

Most users will use the SP-initiated flow, but some organizations prefer to implement IDP-initiated SSO and have a one stop “portal” for all applications a user can access.

# 4. SP Initiated SSO: What does a user see?

Whenever a user needs to log into Huddle they simply type in their username or email address, and Huddle will redirect them to their Identity Provider (IDP) e.g. Active Directory Federated Services, for authentication.



If they are authorized, they will immediately be redirected into Huddle on the appropriate page. This might be their dashboard, the target of a notification, or a workspace that they we accepting an invitation to.

# 5. How does it work?

Here comes the science: Huddle supports the browser SSO profile of SAML 2.0 with HTTP POST bindings. The example below shows the flow for SP Initiated SSO.

Huddle checks for a unique user with that email – will create a user account if just-in-time provisioning is enabled, else show an error if no user by that name or if duplicate users on that email address.

my.huddle.net

/login

Customer Identity Provider System (e.g. ADFS)

Customer identity system checks that this user is trusted and should be allowed to access Huddle

User provided with authentication token and taken to the appropriate page inside Huddle.

User visits Huddle, enters their email address on the login page and clicks “Continue”.

If SSO is enabled for that domain, Huddle sends a signed user identification request (POST) to the customer system.

**1**

**2**

**3**

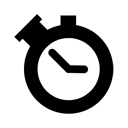
Claims their email address and sends this back to Huddle as a securely signed POST request.

**4**

**5**

**6**

Whole process takes less than a second and is largely invisible to the user.



# 6. Just-in-Time Provisioning

Huddle also provides a powerful way to easily add new users into Huddle. If a company has SSO set up for their users, a user will be automatically provisioned into Huddle without having to sign up, the first time they try to log in. The authentication with their IDP acts as the sign up process. This makes it very easy to invite somebody into a workspace and get working right away. A user will receive a normal Huddle invitation, click to accept, be prompted for their email address, will input their SSO credentials, and will go straight into the workspace they need to access.

In order to switch on Just-in-Time provisioning, SSO needs to be enabled and a ticket should be raised with support.

# 7. Getting started

The easiest and most common method is via Active Directory Federation Services (AD FS) and steps are outlined below. For our cloud SSO partners, please refer to their documentation.

1. Your technical team should be put in touch with Huddle’s Product Engineering Team, and all further steps will occur in consultation.
2. Choose which email domains can be authenticated e.g. *@example.com*
3. Will add Huddle as a “*partner*” on ADFS and send us a digital security certificate.
4. Configure ADFS to “*claim email address*” for users authenticated for Huddle.

Full documentation for your technical team is provided here: <https://github.com/Huddle/huddle-apis/wiki/SingleSignIn#single-sign-in-with-saml>

Next, we’ll need the following information from you in order to set up SSO on our end.

For security, we recommend that you upload the following via a Huddle workspace shared with our team.

1. The Encode Certificate
2. Issuer Name on the Certificate (Name of the SsoService)
3. SSO Service URL
4. Email Domains that you control (we may need to run a quick check to prove ownership).

# 8. Client support for SSO

SSO is supported in all Huddle client applications including:

* Huddle for iOS
* Huddle for Android
* Huddle for Windows / Mac
* Huddle for Outlook
* Huddle for Office
* 3rd party apps using Huddle’s API

# 9. Price and Availability

The SSO for Huddle capability is only available on Plus, Premier and Government/Public Sector packages.

Our SSO partners will provide their Huddle connector for free to new customers (i.e. where the customer does not currently use the given partner for SSO on any other applications) but there may be a cost to add Huddle to an existing SSO implementation.

You can read more about each provider and sign up to their service at:

* **Okta:** <http://www.okta.com/huddle>
* **Centrify:** <http://www.centrify.com/cloud/apps/single-sign-on-for-huddle.asp>
* **OneLogin:** <http://www.onelogin.com/partners/app-partners/Huddle/>
* **Ping Identity**: <http://www.pingone.com/huddle>