SOCIAL INNOVATION MANAGEMENT

BRIGHTIDEA®

Overview

Brightidea Single Sign-on

1. Single Sign-on

Single sign-on (SSO) is a method of access control between multiple independent software systems. Integration with Brightidea software using SSO permits users access without using a Brightidea user ID and password.

Below are some of the benefits of SSO:

- It provides users a seamless cross-site navigating experience, hence increase site participation rate.
- It eliminates the need for users to remember brightidea application access credential.
- It allows company's identity management system to have complete user access control. Once user leaves the company, access to Brightidea system is taken away automatically.

2. How does SSO work

There are 3 parties involved in SSO integration:

Service Provider (SP)

The Service Provider (SP) is the party that owns and maintains an application. In this case, it's Brightidea.

Identity Provider (IDP)

The Identity Provider (IDP) is the party that creates, maintain and manage user identity information, and provide user authentication to other Service Provider. In this case, it's a company's identity management system.

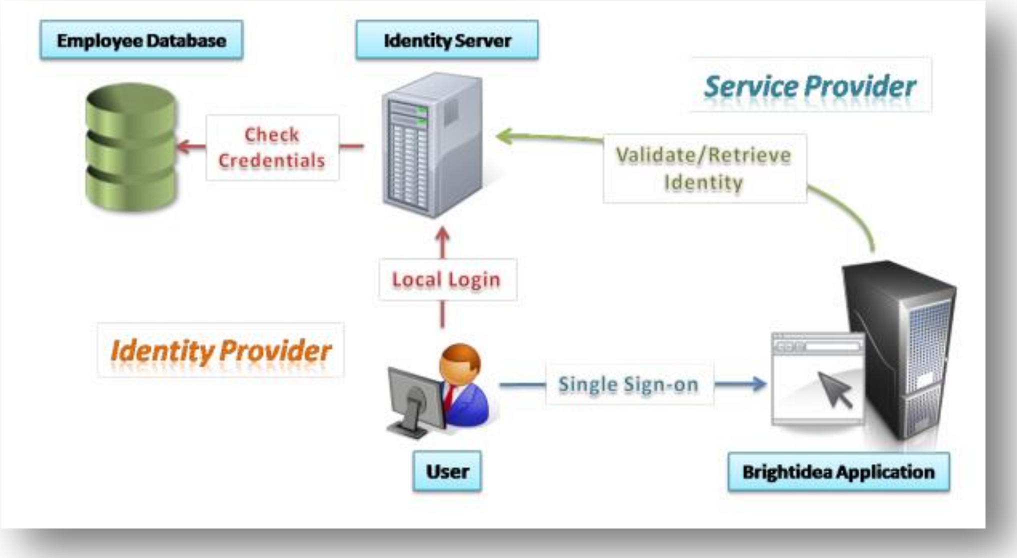
User

A person who has an account in IDP and wishes to access SP.

If SSO integration is setup between Brightidea and a company's identity management system and a user clicks on a Brightidea URL:

- He will first be redirected to the IDP for authentication.
- If successful, he will then be redirected back to Brightidea for account processing.
- Once complete, the web browser will send user into the application.

Much of the redirect is not obvious at the front end. End user will land into Brightidea application without the need of ever entering Brightidea credential.



3. Brightidea via SAML

Brightidea's Single Sign-On implementation is a proprietary developed and in-house maintained solution. The solution is built base on an industry standard protocol named SAML. To know about more about the protocol, visit: http://en.wikipedia.org/wiki/Security_Assertion_Markup_Language

3.1 SAML Spec

Brightidea SAML requirements are:

- Version - SAML 2.0
- Initiation Type – SP-initiated
- Binding Method – POST
- Signature Algorithm – Choose between RSA_SHAA1 or RSA_SHA246
- NameId – Most use company's unique employee ID
- Assertion Attribute – Must send user Email and Screen Name

Optional:

- Sign Authentication – Choose to sign authentication request using RSA_SHAA1, RSA_SHA246 or leave it un-signed.
- Assertion Encryption – Choose to encrypt assertion element

3.2 Security

Brightidea SSO framework performs multiple levels of security verification in its SSO process.

- All communication must use SSL encryption
- Assertion Signature must be validated
- Assertion attribute presence and expiration timeframe must be validated
- IDP has the option to receive signed Authentication
- IDP has the option can choose to encryption Assertion

4. User Account Management

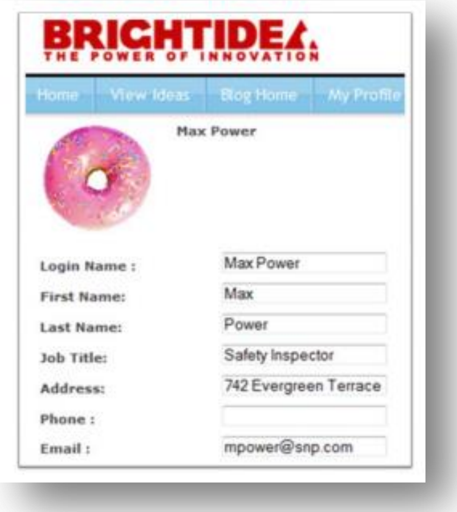
If using SSO, user account is process on every access. So there is no need to perform addition account pre-population or Active Directory synchronized process. User account information is synchronized between Brightidea and company's directory automatically.

Account Creation & Synchronization

Brightidea creates account for user on initial access, and updates the account information on every subsequent access.

User Profile

Besides Email and Screen Name, additional user profile data can be passed through SSO process.



Max Power

Login Name :	Max Power
First Name:	Max
Last Name:	Power
Job Title:	Safety Inspector
Address:	742 Evergreen Terrace
Phone :	
Email :	mpower@snp.com