Getting Started with Single Sign-On

I. Introduction

NobleHour sets out to incentivize civic engagement by enabling users within companies, educational institutions, and organizations to conduct and coordinate their social and economic impact; fostering positive change within their community. From coordinating volunteer work to the exchange of groundbreaking research, efficient collaboration between users is a necessity.

Users require a simple and unified access method across multiple or disparate networks. This means interoperability, automation, and the seamless use of a **Single Sign-On (SSO)** policy to reduce the burden of multiple account authentication processes. With SSO, only the existing credentials of an organization will be necessary for users while eliminating the need for creating and managing a separate NobleHour account.

In order to offer SSO within your organization, NobleHour embraces **Security Assertion Markup Language (SAML 2.0).**

II. SSO/SAML Overview

SAML is an XML-based format for exchanging authorization data between systems. It's widely adopted in private enterprises worldwide and considered the first choice for managing SSO authentication. This is due to its flexible configuration, multiple platform support, and ability to interoperate with widely used core protocols and authentication methods.

Regardless of SAML's rapid adoption, every system is different. There's always customization involved depending on the architecture, protocol, and mechanisms used by your organization. Our team is dedicated to working within your parameters, laying the groundwork for a seamless SSO implementation. As a result of this process, we will establish a SAML-based registration and login for use by your organization.

You can learn more about SAML by viewing the official Security Assertion Markup Language website. This provides a complete overview of SAML's requirements, specifications, and deployment profile.

Before implementing SSO, we require information about your organization's current system. This consists of two steps:

1. Complete the SSO Initial Assessment Help which you can access here.

   In *III: SSO Initial Assessment Help*, we'll walk you through this questionnaire and clarify what's required.

2. Email develop@noblehour.com with information specified in *IV: SAML2 Identity Provider Setup*.

To assist in the information collection process, we've included two additional sections:

V: NobleHour SSO Flowchart - provides a graphical representation of the SSO authentication process for previously established and newly linked accounts.

VI: Reference - Includes helpful definitions, links, and metadata for the SSO/SAML2 implementation.

III. SSO Initial Assessment Help

Below we've included additional clarification on each question asked within the SSO Initial Assessment Questionnaire. As you enter data into the online form, please use this document as a reference. It will help frame any relevant information required and help expedite your SSO implementation.

Page 1

Basic Information

Q.1: Enter the name of your organization, educational institution, or company.

Q.2-Q.4: Provide us with the contact information for your IT Manager or SSO Project Team Leader.

System Information

Q.5: The IdP (Identity Provider) solution currently in use by your organization.

Q.6: Help us determine if your system is capable of federation with external systems. This information is typically provided by your software partner or vendor.

Page 2

Q.7: List all supported federations, solutions, protocols used by your organization.

> Please include all current versions as well as future versions, upgrades, or platform changes planned within the next 90 days.
>
> In order for us to implement SAML, we'll need to understand protocol information such as authentication context, attributes, and bindings. NobleHour supports a variety of solutions for the SAML protocol such as **LDAP, Shibboleth, ADFS, and Ping Federate.**

Q.8: Help us identify your preferred protocol.

> We understand that our clients use different technologies. We've designed NobleHour to pass an array of attributes during the authentication process.

Q.9: Provide us with all necessary account information used during the federation process.

> While we have the ability to receive basic account information such as *firstname*, *lastname*, *email*, and *age*, NobleHour can accommodate additional data when necessary.

An API is required to dissociate federated logons. This is typically provided by your current software partner or vendor. Regardless, our team will be on hand to understand and plan API specifics with you.

Q.10: Inform us of the steps required to become a service provider.

Help us understand the process involved in becoming an official service provider within your organization.

Q.11: We require a test environment used as a staging area for dummy accounts that will simulate and verify authentication flow. We can work with simple test accounts or full production environments.

Page 3

Additional Information

Q.12: Briefly explain the primary security concerns shared within your organization. Security is always an important component to us, especially the authentication process.

At NobleHour, we take all security concerns seriously and will adhere to any organizational standards required during the entire project cycle.

Q.13: Provide us with any internal support documentation that can help us work more effectively or will clarify any potential incompatibilities.

Q.14: Include example data fields or headers that we can use for reference, especially within the test environment.

Q.15-Q.16: Please define your role, as well as of participating team members, along with their contact information to help streamline the SSO implementation process.

Q.17: Help us define your ideal timeline for rolling out NobleHour at your organization.

*When complete, please select **Submit Questionnaire** at the end of the online form.*

Proceed to IV: SAML2 Identity Provider Setup.

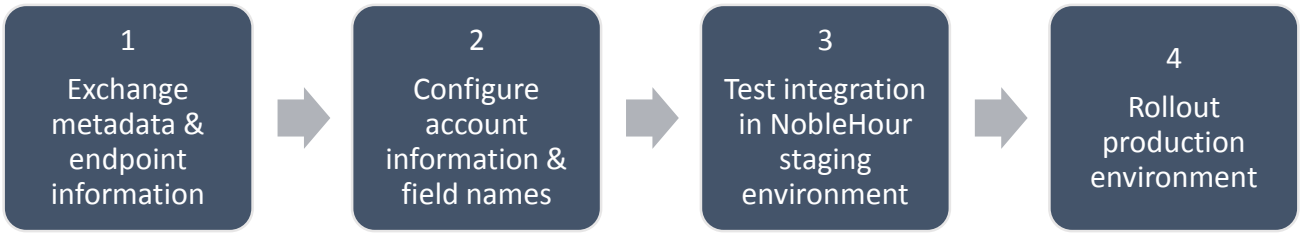
IV. SAML2 Identity Provider Setup

Now that you've completed the SSO Initial Assessment Questionnaire, the next step is to reply to us at develop@noblehour.com with four important prerequisites for your SAML2 setup and configuration. This email will mark the second and final component of our information collection process. Once it's sent to us, we'll contact you to establish an implementation timeline.

For the implementation of SSO, we assume that your organization will already have an Identity Provider (IdP) and that users have an existing account (Principal Identity) with that specific IdP.

SAML2 SSO Timeline Synopsis

In order to set your organization up as a SAML2 Identity Provider, our team will perform the following:



1. **Exchange metadata and endpoint information with your team.**

   Provide us with the IdP metadata, certificate or fingerprint information, single logon endpoint credentials, and entity ID. Additionally, please inform us if messages are digitally signed.

   A. Our staging environment metadata can be found here.

   B. Our production environment metadata can be found here.

2. **Configure the account information & field names you're able to provide.**

   When a user authenticates with IdP, a federated identity must be created in the NobleHour system. This entails a process within NobleHour that establishes the account using the Principle Identity provided by the IdP.

   While NobleHour's SSO requires several basic attributes from the assertion within the authentication response, additional attributes can be used to establish a more detailed user profile. On the next page, our table identifies and defines the expected attributes, mapping them to two common Identity Providers for your reference:

Attribute Table

Attribute	Required	Shibboleth	PingFederate
uuid	FALSE	eduPersonTargetedID	<varies>
email	TRUE	eduPersonPrincipalName, mail	email
firstname	TRUE	givenName	firstname
lastname	TRUE	sn	lastname
over13	TRUE	<n/a>	over13
affiliation	FALSE	eduPersonAffiliation	<n/a>
birthdate	FALSE	<n/a>	birthdate

Note: *The requirement on the* **birthdate** *and* **over13** *attributes are mutually exclusive. If* **birthdate** *is provided, then the* **over13** *attribute does not need to be provided, and vice-versa.*

Below is an example set of acceptable attributes:

```
<saml:AttributeStatement xmlns:xs="http://www.w3.org/2001/XMLSchema">!
<saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrnameformat:
basic" Name="over13">!
<saml:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchemainstance"
xsi:type="xs:string">Y</saml:AttributeValue>!
</saml:Attribute>!
<saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrnameformat:
basic" Name="email">!
<saml:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchemainstance"
xsi:type="xs:string">user@institution.edu</saml:AttributeValue>!
</saml:Attribute>!
<saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrnameformat:
basic" Name="lastname">!
<saml:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchemainstance"
xsi:type="xs:string">Smith</saml:AttributeValue>!
</saml:Attribute>!
<saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrnameformat:
basic" Name="firstname">!
<saml:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchemainstance"
xsi:type="xs:string">John</saml:AttributeValue>!
</saml:Attribute>!

  </saml:AttributeStatement>!
```

3. **Deploy and test integration in NobleHour staging environment.**

    A. Test SP-initiated logins and account claiming.

    B. Test IdP-initiated logins and account claiming.

    Here we'll communicate with your team to ascertain what's necessary and/or available for using test credentials within your environment. A security analysis and deployment schedule will also be discussed, helping us understand when we can begin.

4. **Rollout our production environment.**

    We will configure your Identity Provider (IdP) with your portal.

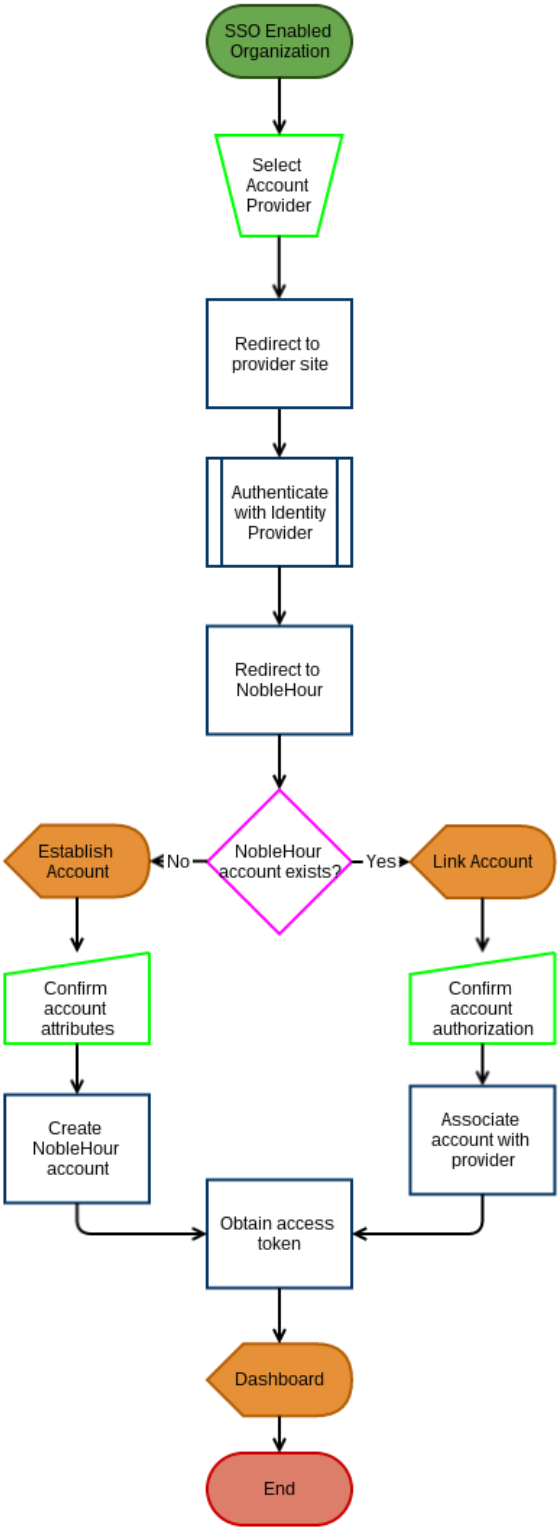
SSO Implementation Complete!

Once everything above has been provided to us, we'll get started with the implementation. Upon completion, users can login to NobleHour with their existing credentials.

In *V: NobleHour SSO Flow Chart*, we graphically illustrate the SSO authentication process for both existing and newly linked accounts.

In *VI: Reference*, we detail important definitions you should become familiar with along with links to help configure your Identity Provider.

V. NobleHour SSO Flow Chart



VI. Reference

SSO Primary Definitions

These definitions lay the groundwork for understanding NobleHour's SSO implementation.

Single Sign-On (SSO) - A process enabling a user to log in once and gain access to related systems without being prompted to log in again at each of them.

Security Assertion Markup Language (SAML) - XML-based data format for exchanging authentication and authorization data between systems.

Identity Provider (IdP) - This is a module that creates, maintains, and manages identity information. IdP will also provide authentication to their service providers within a federation.

Service Provider (SP) - System entity providing services to users or other system entities.

Federation - An association composed of any number of service providers and identity providers.

System Entity - An active element of the system with a distinct set of functionality.

Identity - An entity described by attributes and unique data objects.

Principal - A system entity whose identity can be authenticated.

Principal Identity - A representation of a principal's identity as a unique data object (i.e. *User Account*).

Metadata

1. Our staging environment metadata can be found here.
2. Our production environment metadata can be found here.

Identity Provider Links

SAML: http://saml2int.org/profile/current

LDAP: http://msdn.microsoft.com/en-us/library/aa367008%28v=vs.85%29.aspx

PingFederate: https://www.pingidentity.com/en/products/pingfederate.html

Shibboleth: http://shibboleth.net/

ADFS: http://technet.microsoft.com/en-us/library/cc736690%28v=WS.10%29.aspx

Revision History

3.16.2015	Revised link. Section II SSO/SAML Overview
6.11.2015	New logo added to page header.
1.12.2015	Included link under Part IV: Reference titled **Mapping ADFS Attributes to SAML** located under ADFS.
10.2.2014	Document approved for circulation.