IndustrySafe Single Sign-on Specification
Revision 2: 11/18/2011

1 Single Sign-on Specifications

1.1 Overview

A Single sign-on (SSO) solution allows a user to validate their identity to an initial single system, and have that system pass access authentication credentials to other, independent systems. This document describes the method and specifications of how IndustrySafe, the Service Provider can accept SSO credentials from a remote authenticating system, the Identity Provider (IdP). IndustrySafe uses SSO that is SAML 2.0 Compliant.

The SSO process utilized by IndustrySafe authenticates for a valid user identity from the IdP. Once that user identity has been validated, the IndustrySafe application controls the user's privileges and access within IndustrySafe. If IndustrySafe cannot validate the user's identity successfully then no access to IndustrySafe is allowed. Users authenticated by the IdP must also be valid users within the IndustrySafe application. A technical specification to automate the integration of user information to IndustrySafe is available upon request.

1.2 Single Sign-on Process

IndustrySafe implements SSO by using SAML 2.0. To insure that IndustrySafe meets all SAML 2.0 standards, IndustrySafe uses "ASP.NET SAML Component" by www.atp-inc.net. ATP's "BuildAuthenticationRequest" component requires the client to provide the following when single sign-on is first setup (or if there is a change at the IdP server):

> The X509 certificate used by the IdP.
>
> The single sign-on ID Provider URL – the web address of the IdP Server that accepts HTTP Binding Authentication Requests.

IndustrySafe will provide the client with the URL for the initial request. The client will publish this URL internally to their IndustrySafe Users. No UserID specific information is provided at this initial request.

When the client's users access this initial URL, IndustrySafe will send an Authentication Request to the Client's SAML IdP using SAML's HTTP Binding method. Using the "BuildAuthenticationRequest" component in the ATP software, IndustrySafe will generate and send a valid SAML 2.0 Authentication Request.

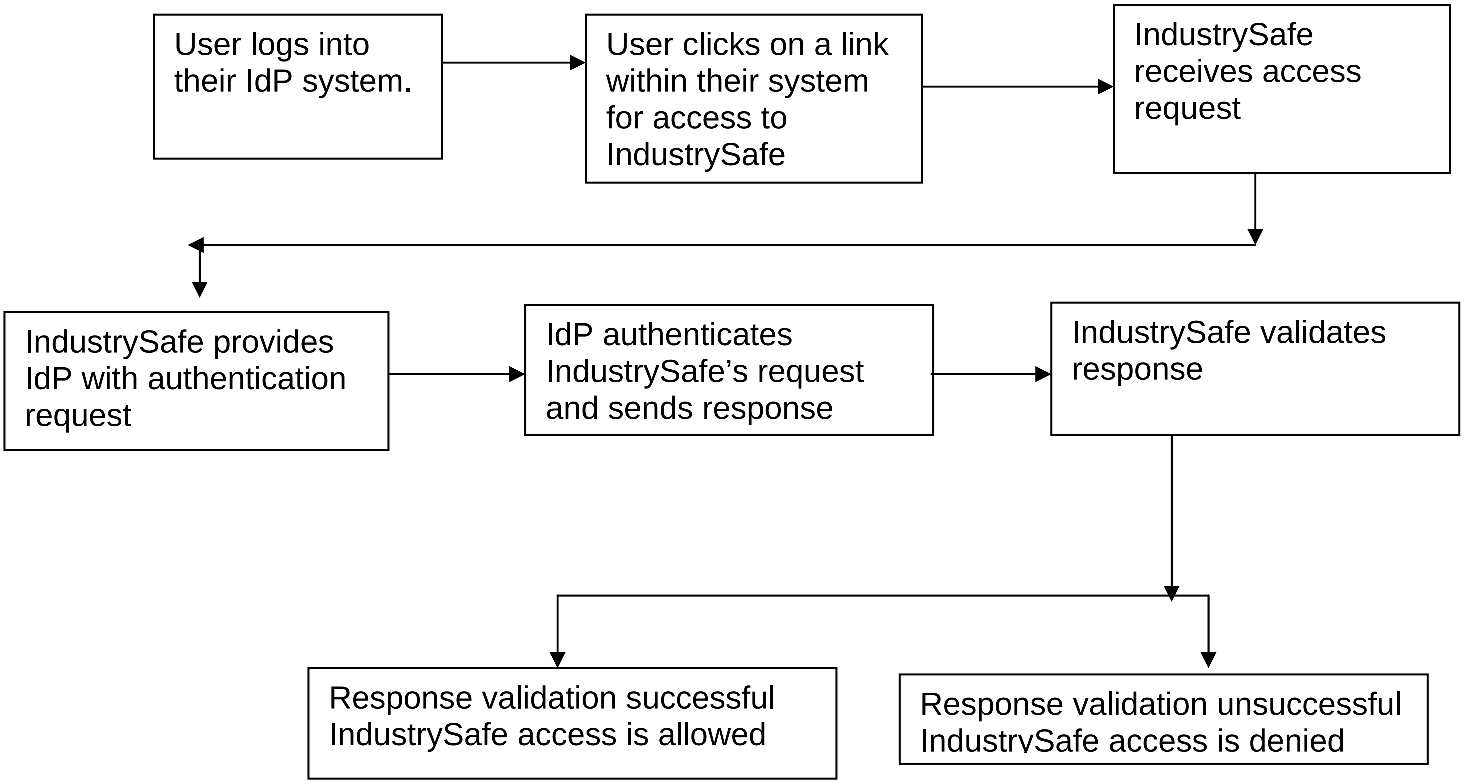
The client's SAML IdP server will process the Authentication Request and respond with an SAML 2.0 Assertion Response using SMAL's HTTP Binding method. This response must include the UserID and the NotBefore and NotOnOrAfter conditions for the response.

IndustrySafe will receive the response from the Client’s IdP, and use the “Atp.Saml2.Response” Object in ATP Components to validate the response with the X509 Certificate and parse out the UserID and the valid times for this response.

> The UserID will be parsed out of the “Atp.Saml2.Response” (an ATP component) using the code “Atp.Saml2.Response.samlAssertion.Subject.NameId.NameIdentifier”
>
> The Valid times will be parsed out of the “Atp.Saml2.Response” (an ATP component) using the codes “Atp.Saml2.Response.Conditions.NotBefore” and “Atp.Saml2.Response.Conditions.NotOnOrAfter”

IndustrySafe will attempt to use the UserID provided in a Valid Assertion Response to log into the IndustrySafe application. If the UserID does not exist in the IndustrySafe application, or is not an enabled user, an error message will be displayed and the user will not gain access to IndustrySafe. The UserID returned in the Assertion Response is typically the user’s email address or Employee ID. When setting up the Users in IndustrySafe, the IndustrySafe User ID must match the UserID that will be provided by the IdP server. In IndustrySafe, the User ID is case sensitive.

1.3 SSO Process Flow Diagram


User logs into their IdP system.
User clicks on a link within their system for access to IndustrySafe
IndustrySafe receives access request
IndustrySafe provides IdP with authentication request
IdP authenticates IndustrySafe’s request and sends response
IndustrySafe validates response
Response validation successful IndustrySafe access is allowed
Response validation unsuccessful IndustrySafe access is denied