COMINTELLI®

WHITE PAPER

Single Sign On (SSO) in Intelligence2day® Enterprise

Enabling transparent, simple and secure user authentication

Contents

1. Introduction

Single sign-on (SSO) is a user authentication process that permits a user to enter one name and password in order to access multiple applications/resources. The process authenticates the user for all the applications they have been given rights to and eliminates further prompts when they switch applications during a particular session.

There are many applications that seem to be rich in functionality, but are vulnerable to unwanted intrusions. Unfortunately, this is often something you discover when it is already too late. Web applications must be built with improved security features to fulfill their economic promise and protect organizations against liability and loss.

This White Paper describes how Comintelli's Intelligence2day® Enterprise can interact with available SSO solutions.

2. Advantages

The benefits are understandable with reduction of;

- password fatigue from different user name and password combinations
- time spent re-entering passwords for the same identity
- IT costs due to lower number of calls about passwords

SSO shares centralized authentication servers that all other applications and systems use for authentication purposes and combines this with techniques to ensure that users do not have to actively enter their credentials more than once.
Technologies are being implemented to help detect the attempt to hack a certain system, in which it would lock out the hacker from the remaining systems.

3. Disadvantages

Single sign-on in its nature provides access to many resources once the user is initially authenticated ("keys to the castle"). It might increase the negative impact in case the credentials are available to other persons and misused.

The SSO is a highly-critical tool to keep up always. If the SSO expires, the user would lose access to all sites.

SSO does not come in handy for a multi-user computer, especially if the user stays logged in all the time. This is more prevalent of an issue in plant operations, business floors, etc. where multiple users can access the computer.

4. Security

In an enterprise using SSO software, the user logs on with their id and password. This provides access to information and multiple applications such as the Intelligence2day® Enterprise portal. Single Sign On software is a stronger form of authentication which includes digital certificates.

Single Sign On takes place between enterprises using federated authentication. For example, an employee may successfully log on to their enterprise system and when they click on a link to Intelligence2day® Enterprise, the business partner's Single Sign On system (Federation Server) will provide a digitally signed security assertion token using a protocol (such as SAML as described below). Intelligence2day® Enterprise receives the token, checks it (based on certification signature and time stamp), and then allows the employee to access the application without having to sign on.

5. Different SSO solutions/configurations

There are several different ways of implementing SSO, some of the most common are described below:

- Integrated Windows Authentication (Kerberos based): Initial sign-on prompts the user for credentials to access the network.
- Security Assertion Markup Language (SAML): An XML standard that allows secure web domains to exchange user authentication and authorization data. Using SAML, an online service provider can contact a separate online identity provider to authenticate users who are trying to access secure content.
- Active Directory Federation Services SSO: Windows AD FS supports Web single-sign-on (SSO) technologies that help information technology (IT) organizations collaborate across organizational boundaries.
- SiteMinder Federation SSO: Provides users seamless, easy access to applications with a federated single sign-on (SSO) across the underlying domains.

6. SAML-based SSO in Intelligence2day® Enterprise

Security Assertion Markup Language (SAML) is an XML-based open standard data format for exchanging authentication and authorization data between parties, in particular, between an identity provider and a service provider.

Comintelli offers a SAML-based Single Sign-On (SSO) service that provides customers with full control over the authorization and authentication of hosted user accounts that can access the Intelligence2day® Enterprise application.

Using the SAML model, Comintelli acts as the service provider (SP) and provides the Intelligence2day® Enterprise service. The customer act as identity providers (IdP) and control usernames, passwords and other information used to identify, authenticate and authorize users.

The process of using SAML in Intelligence2day® Enterprise is described in more detail below:

1. The user attempts to reach the Intelligence2day® Enterprise application. The user does not have a valid session (i.e. security context). The SP saves the requested resource URL.

2. Intelligence2day® Enterprise re-directs the user to IdP's federation server.

3. Browser re-directs to IdP URL.

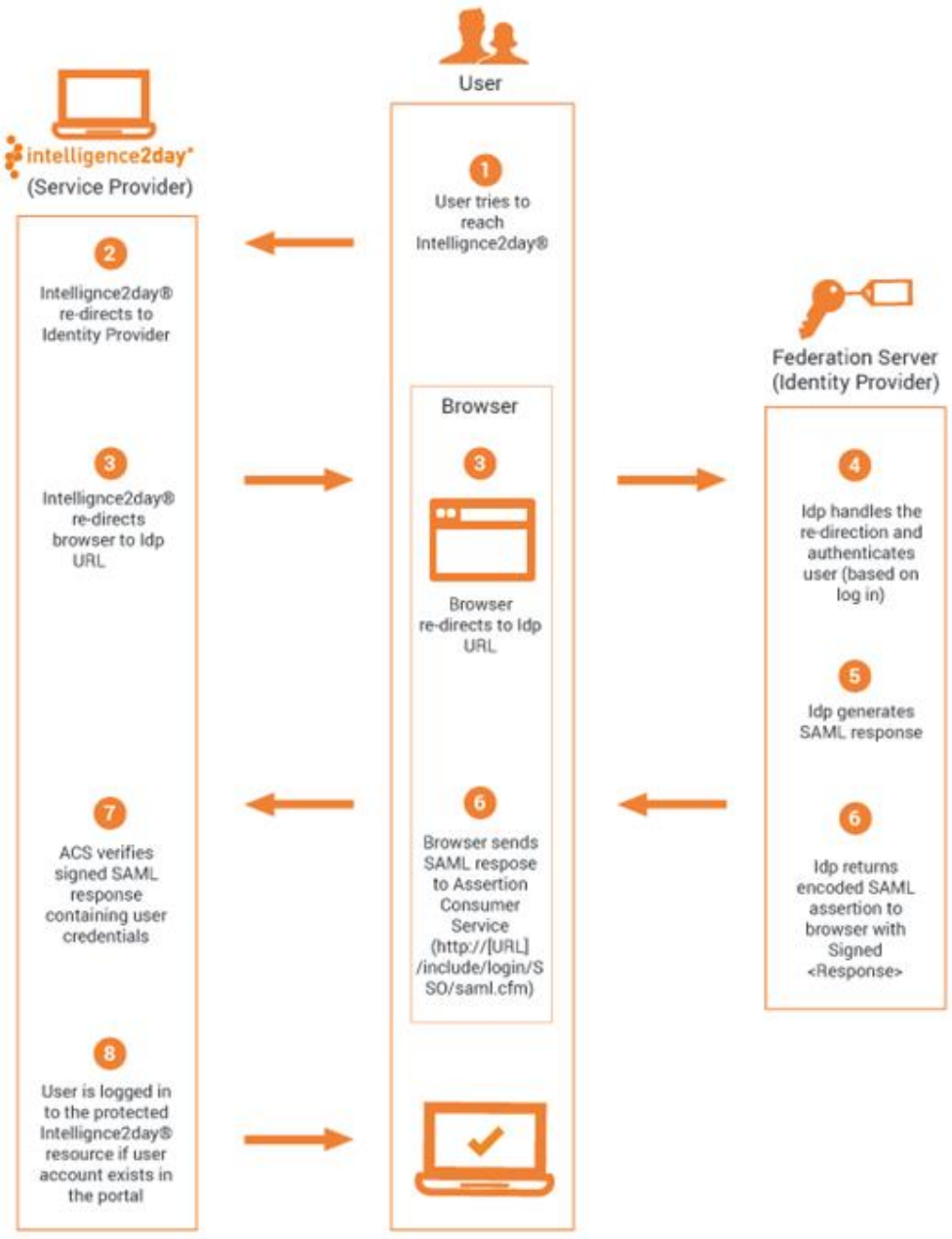
4. Federation server handles the re-direct and authenticates the user by either asking for valid login credentials or by checking for valid session cookies.

5. The IdP generates a SAML response that contains the authenticated users subject = unique ID (not considered as a user name in Intelligence2day®), first name, last name and email address. In accordance with the SAML 2.0 specification, this response is digitally signed with the customer's public and private DSA/RSA keys.

6. The customer encodes the SAML response and the RelayState parameter and returns that information to the user's browser. The customer provides a mechanism so that the browser can forward that information to Intelligence2day® Enterprise Assertion Consumer Service, ACS.
   `entityID: comintelli.sp.saml2`
   `ACS: https://[SITE URL]/include/login/SSO/saml.cfm`

7. Intelligence2day® Enterprise ACS verifies the SAML response using the customer's public key. If the response is successfully verified, ACS redirects the user to the destination URL. Intelligence2day® Enterprise obtains the <Response> message from processing.

8. The user has been verified as valid (if the user account exists) and redirected to the protected destination URL. Each user login is logged in the system with updated statistics.



The process of using SAML in Intelligence2day®

7. About Comintelli

Comintelli is a software company that provides a cloud-based service for information access called Intelligence2day®. It provides solutions for Competitive Intelligence and Knowledge Management that helps customers manage their unstructured information more effectively. Founded in 1999 and with extensive industry experience, Comintelli continues to develop user-friendly solutions that save both time and money.

For more information, please contact:
Phone: +46-8-663 76 00 | 1-800-485-6402 (US/Canada)
E-mail: contact@comintelli.com
Web: www.comintelli.com | www.intelligence2day.com
Visit our Resource Center for more White papers and Cases
