HARVARD UNIVERSITY

Enterprise Architecture

Technology Partner Services
and
Strategy and End User Services

Advisory

Use of Single Sign On (SSO) with Salesforce

Authors: Georgina Prager Greg Charest Raoul Sevier	**Audience Level:** • Solution Architect and Project Manager • Application Developer and Designer
Version: 1.0 **Last Revised:** **Status:** DRAFT **Document Type:**	**Distribution Scope:** Harvard-wide
Workgroup Members:	**Reviewers:** Amy Fairhall

Document Change Log

Rev	Date	Editor	Changes
0.1	1/15/2021	gcharest	first draft
0.2	1/28/2021	gcharest	clean up revisions
1.0	4/14/20221	gcharest	published version

1. Problem Statement

There are currently more than 60 implementations of Salesforce across the University. These platforms use a mix of native and centrally managed authentication services. The lack of a consistent approach to user authentication and authorization leads to increase risk.

2. Key Recommendations

- Use a centrally managed Harvard authentication system, typically Harvard Key, for any Salesforce instance that handles level 3 or higher data. ***Note that this is required by University security policy*** [1]***.***

- Use the Harvard Key SSO system or an equivalent University supported alternative, for any Salesforce instance used by a significant number of Harvard faculty, staff or students in order to provide a better user experience and improve security.

- Use SSO and the new Harvard Key Light system for Salesforce instances that support non-Harvard users including Salesforce Community sites.

- Limit the use of the native Salesforce authentication system to use cases with a small number of trusted users or when centrally managed services cannot meet business or technical needs.

3. Executive Summary

[1] https://policy.security.harvard.edu/requirement-number/sb12
https://security.harvard.edu/data-classification-table

In addition to the native system of user authentication and authorization, Salesforce supports Single sign-on (SSO), an authentication method that enables users to access multiple applications with one login and one set of credentials. The largest SSO system at Harvard is Harvard Key, although some Schools support alternative systems. Salesforce administrators should understand and choose an authentication system based on user experience, security and practical considerations.

4. Discussion

4.1. Security Tools and Configurations

Salesforce includes a variety of security related tools and configuration alternatives. These include:

- User Password Management
- Single Sign-On
- My Domain
- Multi-Factor Authentication
- Network-Based Security
- Device Activation
- Session Security
- Custom Login Flows
- Desktop Client Access

These may be implemented with the Salesforce native authentication system or in combination with a separate identity provider. Each of these should be evaluated and implemented when appropriate in the context of business, technical and policy requirements.

4.2. Authentication Alternatives

4.2.1. Salesforce Native

Salesforce has an internal system of user authentication that utilizes usernames, passwords, and session management. Although functional, the user needs to create, remember, and manage another set of credentials. In add, the org administrator needs to manually provision and deprovision users.

4.2.2. Single-Sign-On (SSO)

Salesforce also supports single sign-on capability to simplify and standardize user authentication. There are two options to implement single sign-on—federated authentication using Security Assertion Markup Language (SAML) and delegated authentication.

- Federated authentication using Security Assertion Markup Language (SAML) lets you send authentication and authorization data between affiliated but unrelated web services. Salesforce enables federated authentication for your org automatically, but it must be configured to use your identify provider.

- Delegated authentication is similar to SSO but offers a different user experience. Both SSO and delegated authentication enable users to log in to multiple apps with one set of credentials. However, with delegated authentication, users must log in to each app separately. Delegated authentication integrates Salesforce with an authentication method that you choose. One advantage to delegated authentication is that it can be managed at the permission level, not at the org level, giving you more flexibility. With permissions, you can require some to use delegated authentication while others use their Salesforce-managed password. A significant disadvantage to delegated authentication is that it requires an external authentication system and custom development to wrap the authentication process in a SOAP [2] based web service that Salesforce can consume.

4.3. SSO Options

4.3.1. Harvard Key

Harvard Key is Harvard University's unified credential for accessing University applications and services with a single, convenient login name and password. The use of Harvard Key with Salesforce is an example of Federated authentication using Security Assertion Markup Language (SAML). Configuring Salesforce to use Harvard Key is beyond the scope of this advisory but documentation is available through the Identity and Access Management Program site[3] and Salesforce [4].

4.3.2. Harvard Key Light

Harvard Key currently supports Harvard employees, faculty, staff, students, and persons-of-interest (POI). Consequently, the use of the Harvard Key SSO system in Salesforce is limited to those user populations. A new Harvard Key service that will support a wider variety of roles, including executive and extended education students, is in development. This will support the use of the enterprise authentication system with Salesforce Communities and other broader user populations.

4.3.3. Other Harvard SSO systems

Although Harvard Key is the primary enterprise SAML identity provider, some schools support their own identity providers. Configuring Salesforce to use an alternative identity provide is similar to using Harvard Key.

---

[2] https://en.wikipedia.org/wiki/SOAP

[3] https://iam.harvard.edu/get-started/authentication

[4] https://developer.salesforce.com/docs/atlas.en-us.sso.meta/sso/sso_saml_setting_up.htm

4.4. Benefits of Single Sign On

The use of centrally managed authentication services and SSO provides several important benefits:

- Mitigate risk because user passwords are not stored or managed within Salesforce
- Reduce user password fatigue from different username and password combinations and reduce time spent re-entering passwords for the same identity
- Reduce IT costs due to lower number of IT help desk calls about passwords

While the use of SSO does create a dependency on the authentication service, Harvard Key is highly available and rivals Salesforce itself in operational performance and uptime.

4.5. SSO Technical Overview

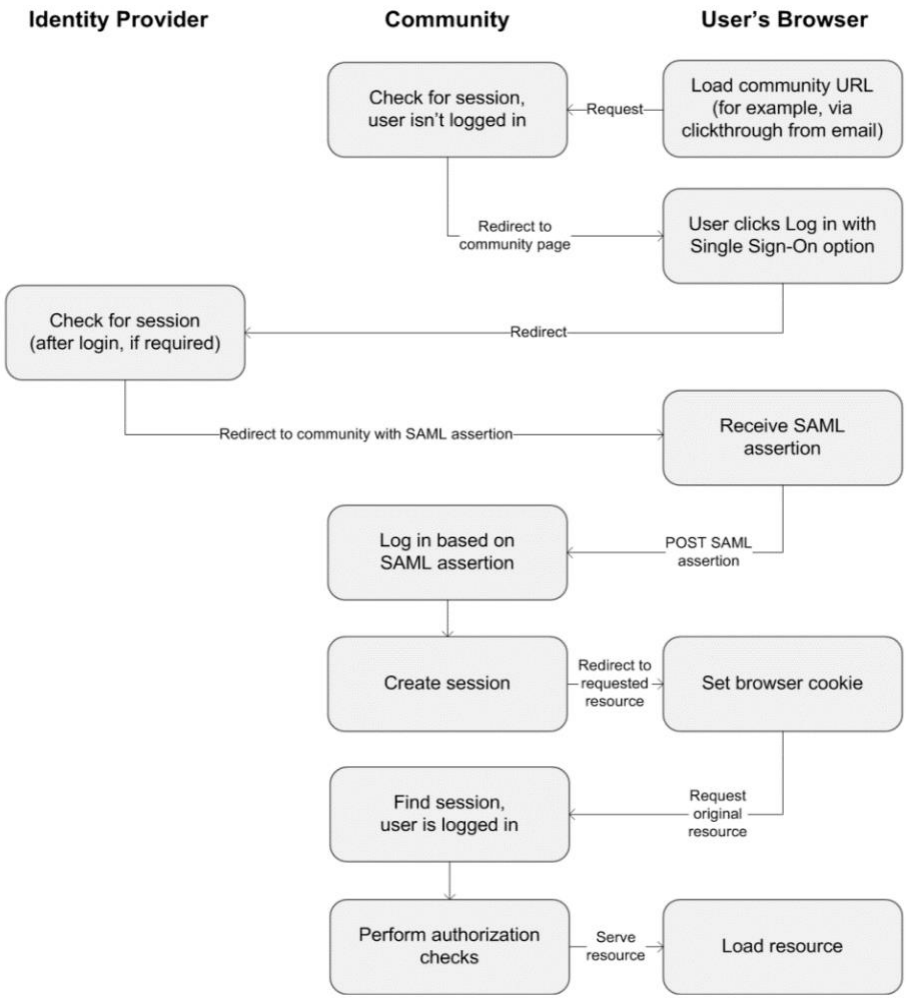
Harvard Key authentication services are available for web applications with two standard protocols: CAS and SAML 2.0.

SAML is an open standard that allows identity providers (IdP) to pass authorization credentials to service providers (SP). This is done through an exchange of digitally signed XML documents. This process allows a Harvard Key user to login to Salesforce using their University username/password and relieves them of the need to re-enter their Harvard Key credential each time they access a different web application.

A simplified description of how the SAML protocol and process works includes the following steps:

- The user attempts to access an application and the application loads
- The application redirects the user to the identity provider, asking for authentication. This is the authentication request
- The user either has an existing active browser session with the identity provider or establishes one by logging into the identity provider
- The identity provider builds the authentication response in the form of an XML-document containing the user's username or email address, signs it using an X.509 certificate, and posts this information to the service provider
- The service provider, which already knows the identity provider and has a certificate fingerprint, retrieves the authentication response and validates it using the certificate fingerprint.
- The identity of the user is established, and the user is provided with app access.

A graphical representation of Salesforce authentication when using SSO is below:



4.6. Certificate Management

SAML authentication relies on public key infrastructure (PKI) and uses digital certificates. These have an expiration dates and must be renewed prior to expiration. The Salesforce default for key expiration is 2 years. Updating certificates must be coordinated with the identity provider.

4.7. Just-in-time (JIT) provisioning

Often SaaS applications and platforms like Salesforce a user must exist (be provisioned) in the application before they are able to login using an SSO system. With Just-in-Time (JIT) provisioning, the identity provider passes user information to a Salesforce org in the SAML assertion to automatically create user accounts. If this option has value in your particular case, work with HUIT's IAM services to determine which user information you want to pass to your org.

5. Salesforce Authentication Recommendations

The use of a Harvard supported central authentication system is required by policy for Salesforce orgs that contain level three or higher data as defined by the Harvard Information Security Office.

The use of an external identity provider and a single sign on system results in improved security and a better user experience. Absent specific business or technical requirements, all Salesforces orgs should use a Harvard supported central authentication system such as Harvard Key.

User provisioning can be done manually but automated provisioning and de-provisioning provide additional value and can reduce costs. Salesforce administrators should work with IAM to understand the available provisioning alternatives.

Harvard Key presently supports Harvard affiliates only but the new capabilities of Harvard Key Light should be considered once the system is available (planned for 6/2021).

When central authentication is not used, the security controls available within Salesforce should be evaluated and used when appropriate.

6. References

https://developer.salesforce.com/docs/atlas.en-us.sso.meta/sso/sso_about.htm
https://en.wikipedia.org/wiki/Single_sign-on
https://developers.onelogin.com/saml
https://resources.docs.salesforce.com/230/latest/en-us/sfdc/pdf/salesforce_single_sign_on.pdf