Multi-factor Login to Salesforce

Who should read this white paper:

IT professionals and managers specializing in data security and risk management.

This paper assumes the reader is familiar with basic concepts of authentication, identity management, and single sign-on for web-based applications.

Web-based applications are the most critical part of the corporate IT infrastructure. The steady growth of web-based applications in the enterprise IT infrastructure has made corporate accounts common attack vectors for hackers. Using a username as the first step in a login process invites hackers, weakens security, and jeopardizes the whole authentication process.

One of the most vulnerable parts of Salesforce security is user authentication. Built-in user management is based on the use of e-mails as usernames and passwords for user verification. These weak means of authentication puts users at serious risk of unauthorized access, phishing, and other security threats. For business and enterprise users, where user management is based on the company's Active Directory (AD), utilization of the same usernames and passwords for Salesforce and AD makes the company's infrastructure vulnerable to hacker attacks. However, users with corporate Salesforce accounts can significantly improve the security by integrating Salesforce with a robust Single Sign-on platform featuring multi-factor authentication.

WWPass SSO authentication provides a much higher level of security without sacrificing convenience. When combined together and integrated with any LDAP-based user management systems (like Microsoft Active Directory), WWPass SSO provides a secure login service for SAML compliant web-based business applications. By adopting this solution, enterprises can achieve the highest level of strong authentication in accordance with GDPR (General Data Protection Regulation (EU) 2016/679) and

NIST (SP 800-63-1). Being both compliant and secure, this solution further increases resistance to external attacks.

1. What is WWPass SSO?

WWPass SSO

Increases security of SAML and OAuth2 compliant business applications by replacing username/password based login with strong multi-factor authentication.

Gives users a simpler, safer, and faster sign-on for Salesforce, and other SAML/OAuth2 enabled applications, and other key enterprise services such as VPN.

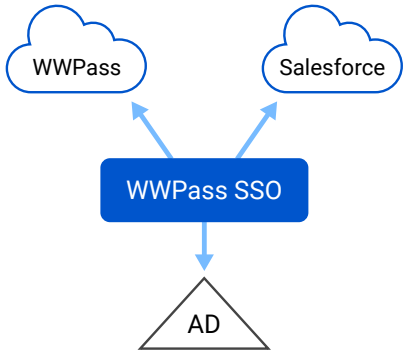
Simplifies administration of user access rights by integrating with LDAP directory services, including MS AD.

Gluu server integration with WWPass hardware or software based cryptographic multi-factor authentication provides GDPR and NIST compliant strong SSO based on SAML or OAuth2 protocols for many business applications, such as Salesforce and many others.

To log in, users employ a WWPass Key in place of a username.

The WWPass Key is a cryptographic token available in convenient mobile app, USB/NFC fob, or a smart card. With the addition of a PIN, the WWPass Key serves as a strong two-factor authentication solution.

WWPass Key is anonymous, contains no personal identifying information, certificates, or any other identity attributes. The WWPass Key provides a single-credential, secure, and anonymous method for multi-factor authentication into any enabled VPN, web or PC/mobile-based application. It features unprecedented convenience for users, who can now employ a single device to quickly log into many other network services.



For the IT team, WWPass SSO integration with Active Directory provides a familiar administrative interface for centrally managed user access rights. User onboarding and off-boarding is done through AD user management. WWPass SSO runs as a virtual appliance on an enterprise's VMware vSphere infrastructure — a virtualization technology already familiar to many IT professionals.

Acronyms in this document

AD Microsoft Active Directory

IdP Identity Provider

LDAP Lightweight Directory Access Protocol

RP Relying Party (note: In SAML, a Relying Party is referred to as a Service Provider)

SAML 2.0 Security Assertion Markup Language 2.0

SP Service Provider (SAML term for a Relying Party)

SPID WWPass Service Provider Identifier

PUID Personal User ID (user anonymous identifier) stored in WWPass distributed network

SSO Single Sign-on

UPN AD User Principal Name

Gluu Gluu SSO platform

VPN Virtual Private Network

WWPass's design simplifies deployment and reduces Identity Access Management (IAM) costs.

Risk management professionals can also rest easy knowing that if a WWPass Key is lost or stolen, corporate data security is in no way compromised. A simple web-based utility allows the user or authorized IT administrator (acting as the user's recovery agent) to invalidate the lost WWPass Key and create a replacement. The recovery procedure for WWPass Key mobile app allows users to restore the original key on the new phone, while the app on the old phone becomes permanently disabled.

2. How does WWPass SSO for Salesforce work?

WWPass SSO is easy to use for both end-users and IT administrators. Under the hood, the combination of Gluu, WWPass cloud services, and the LDAP directory services creates a SAML's Identity Provider (IdP) function.

2.1. What the User Sees

1. User navigates to Salesforce corporate portal (vanity URL) https://domain.my.salesforce.com (where domain is the corporate ID, registered with Salesforce).
2. After clicking on host or sign-in button (functions which require authentication), the user is presented with the WWPass login screen. The user employs their WWPass Key (through USB or NFC interface) or scans the displayed QR code with the WWPass Key app.
3. If it is the user's first access to Salesforce with their WWPass Key, WWPass SSO identifies the unknown token and offers the option to log in with AD (or other LDAP) username and password provided by system administrators.
4. After WWPass Key is bound to the user AD account his/her username/password will never be used again.

Supported functionality and requirements

Virtualization
VMWare vSphere v6.0 and above

Directory stores
Microsoft Active Directory 2008/2012/2016

Supported browsers
Chrome™; Mozilla Firefox®; Opera™; Safari®; Microsoft Edge

Supported federation protocols
SAML 2.0, OAuth2

Minimum requirements
50+ GB storage space; 8+ GB RAM; one 64-bit Intel® or AMD® processor (2+ cores)

5. After initial enrollment, the user will log in to Salesforce with WWPass Key.
6. System administrators (according to corporate security policies) may enable a second authentication factor. In WWPass case, it's a PIN associated with that particular WWPass Key. On modern mobile devices, a PIN can be substituted with device biometrics (fingerprint or FaceID).

2.2. Under the Hood

The user's seamless experience with WWPass SSO and WWPass Key is backed up with powerful security technologies.

Depending on the corporate IAM strategy, user management may be vested into Active Directory or be completely performed by WWPass SSO server. Given that most organizations have an IAM system in place already, we will describe AD integration.

For purposes of clarification, the following SAML-defined roles are performed within the Gluu architecture:

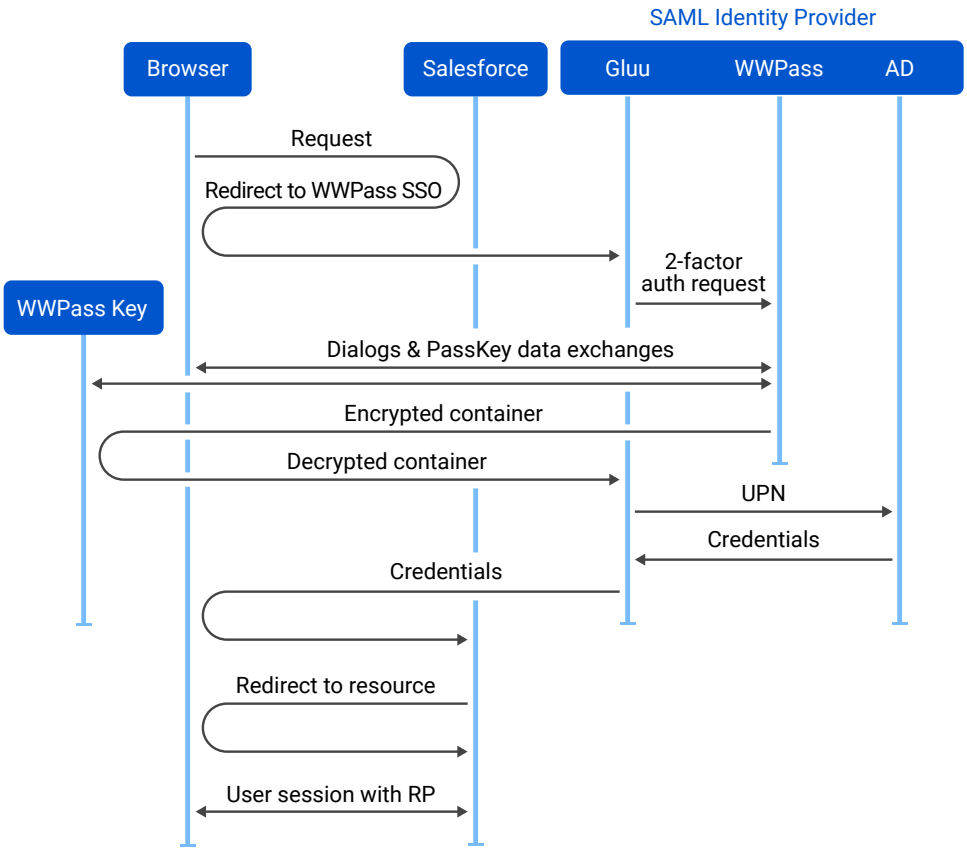
- **SAML SP (aka RP):** The target web app.
- **SAML User Agent:** The user's web browser.
- **SAML IdP** The combination of Gluu, AD, and WWPass services. WWPass SSO implements the SAML message interchanges with the web app and the user's browser.

While the combination of Gluu, WWPass authentication, and AD performs the SAML Identity Provider role, each of these systems has a specific function:

- WWPass authenticates the user's base identity*. Base identity individuates the user from all other machines and people, without containing any personal user information.
- AD acts as an authoritative attribute provider, holding the user's access rights and other personal identifying information.
- WWPass SSO binds the attributes obtained from AD to the user's session, delivering a SAML security assertion to the RP.

See the figure below for a depiction of the WWPass SSO authentication workflow in action according to the steps below:

1. A user navigates to a web app (Salesforce) in a browser.
2. The RP redirects connection to WWPass SSO.
3. WWPass SSO communicates with the WWPass interceptor script, which contacts WWPass servers to request two-factor user authentication. WWPass servers communicate with a browser on the user's machine, prompting the user to scan a QR code with the WWPass Key app and enter a PIN, simultaneously confirming the user's consent to login to WWPass SSO.
4. WWPass servers verify that the user's WWPass Key is valid and that the PIN is correct. If so, WWPass servers reassemble an encrypted user identifier -PUID from WWPass' fragmented, globally dispersed storage** and deliver the PUID to Gluu.



Note: All communications between WWPass servers, WWPass SSO and the user's machine employ encrypted SSL sessions.

5. WWPass SSO finds an LDAP record with this PUID. It checks if the account is enabled and retrieves all the necessary attributes.
6. If the PUID is unknown to the LDAP, then WWPass performs a binding process. It requests user's AD credentials, which are used only once to associate the AD account with the PUID. If the credentials are valid, the user is enabled, and their account gets linked to that PUID. Domain credentials will never be used again for subsequent logins.
7. WWPass SSO transmits the attributes in a SAML XHTML form to the browser.
8. The user's browser transmits a SAML Request Assertion Consumer Service message containing the credentials to Salesforce.
9. Salesforce checks the SAML response, authorizes the user to access the app, and then redirects the browser to the appropriate welcome or "access denied" landing page.

2.3. For the IT Admin: Adding and Removing Users

Because WWPass SSO integrates so tightly with existing Active Directory records, adding and removing users is speedy and simple.

To allow existing users to access a corporate Salesforce account, they need to be added to the SALESFORCE USERS group. The administrator off-boards a user by removing the user from the Salesforce users AD group. No additional actions are required with either WWPass SSO or the user's WWPass Key, since neither contains personally identifiable information or security certificates.

About WWPass

WWPass solves information security infrastructure's biggest deficiency by conveniently and securely protecting both users and data. With just one self-managed WWPass Key, users can easily authenticate themselves for a number of enabled local or cloud-based applications without hard to remember username/password combinations! WWPass' patented authentication and cloud storage technologies keep both the application's data and user's identity separate and hidden from all other applications, preserving both user and application privacy. By integrating WWPass technology into their applications, organizations protect two critical assets: their data and their users.

Learn more at wwpass.com.

WWPass Corporation

9 Trafalgar Sq. Suite 240

Nashua, NH 03063

+1.603.836.4932 or
+1.888.997.2771

wwpass.com

3. Can WWPass SSO Be Used to Protect Logins to Other Services?

Intended for use in organizations of 10-100,000 users, WWPass SSO can provide exactly the same workflow for other web services, using SAML or OAuth2 protocols for SSO integration, like:

- Google® Apps for Business™ and Education™
- ZOOM.us®
- Dropbox™ for Business
- Microsoft 365, Azure, Teams etc.

It is also possible to secure remote access to corporate LAN through Cisco, Fortinet, Juniper, and Open VPN clients, allowing remote users to eliminate risks, associated with traditional authentication. All by means of one and the same WWPass Key.

Ready to take the next step?

With user security at the forefront of business concerns, there's never been a better time to invest in safeguarding your enterprise. To learn more about Gluu + WWPass, or to obtain a customized solution for your organization, please contact sales@wwpass.com.

---

* Towards a Trustworthy Digital Infrastructure for Core Identities and Personal Data Stores by Hardjono, Greenwood and Pentland https://www.wwpass.com/pdf/docs/HGPCoreId.pdf

** How WWPass Works https://www.wwpass.com/pdf/docs/HowWWPassAuthenticationWorks.pdf