Secure Login to Microsoft applications

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.

The steady growth of web-based applications in the enterprise IT infrastructure has made corporate accounts common attack vectors for hackers.

One of the most vulnerable parts of Microsoft web-based application`s security is user authentication. Logins to all Microsoft web-based applications are based on usernames in the form of email addresses. A username as the first step in a login process invites hackers and weakens security, putting corporate data at serious risk of unauthorized access, phishing, and other security threats.

WWPass solves the challenge of web-based application security with its unique approach -a login without usernames and passwords eliminating human-readable credentials from the entire authentication process. With WWPass login user identity is no longer the starting point of a login process. It is rather a result of a highly protected authentication and verification process, which utilizes a cryptographic token (**WWPass Key**).

Well protected corporate single sign-on based on WWPass login (**WWPass SSO**) guarantees secure, convenient, and compliant access to all enterprise web-based Microsoft applications.

WWPass SSO provides a much higher level of security. Integrated with any LDAP-based user management systems (like Microsoft Active Directory), WWPass SSO provides a secure login service for Microsoft ADFS enabled web-based business applications such as Outlook Web Access (OWA), Exchange Control Panel (ECP), MS Azure, MS 365, MS Teams, MS SharePoint. By adopting this solution, enterprises can achieve the highest level of strong authentication following 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.

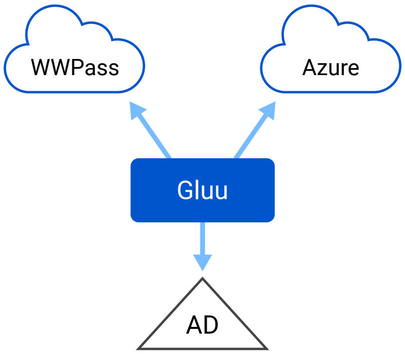
1. What is WWPass SSO?

Gluu server integration with WWPass hardware or software-based cryptographic multi-factor authentication provides SSO based on ADFS, SAML, OAuth2 or RADIUS protocols for many business applications, such as Microsoft and many others.

To log in, users employ a WWPass Key.

The WWPass Key is a cryptographic token available in the form of a mobile app, USB/NFC fob, or a smart card. With the addition of a PIN or biometrics, 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 username-less and passwort-less, secure, and anonymous method for multi-factor authentication into many web, 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, Gluu 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 and Gluu

Increases security of ADFS compatible. Microsoft business applications by replacing username/password-based login with strong multi-factor authentication.

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

Simplifies administration of user access rights by integrating with Active Directory service.

Acronyms in this document

AD Microsoft Active Directory

ADFS Active Directory Federation Services

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 Provider-specific 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

Gluu 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 the 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 Microsoft 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 Active Directory creates a SAML's Identity Provider (IdP) function.

2.1. What the User Sees

1. The user navigates to the Microsoft Azure portal or any other MS web-based app like for example MS Teams.
2. The user clicks on the sign-in button and enters ANY username at the configured corporate domain (i.e. a@contoso.com). The "username" part will be ignored later, only the domain name is important at this stage.
3. 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.
4. If it is the user's first access to the service with this WWPass Key, WWPass SSO identifies the unknown Key and offers the options to bind the Key to their account using either username/password from Active Directory, another WWPass Key or an email, registered in the Active Directory (depending on the options enabled by the administrator).

Supported functionality and requirements

Directory stores
Microsoft Active Directory 2012/2016/2019

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 WWPass Key is bound to the user AD account his/her username/password will never be used again.
6. After initial enrollment, the user will log in to respective Microsoft resources with WWPass Key.
7. System administrators (according to corporate security policies) may enable a second authentication factor. In the WWPass case, it's PIN associated with that particular WWPass Key. On modern mobile devices, 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.

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

- **ADFS SP (aka RP):** The target web app (e.g Microsoft Azure).
- **SAML SP (aka RP):** ADFS server.
- **SAML User-Agent:** The user's web browser.
- **ADFS Claims Provider:** The combination of Gluu, AD, and WWPass services.
- **SAML IdP** The combination of Gluu, AD, and WWPass services.

Gluu implements the SAML message exchange with the web app and the user's browser.

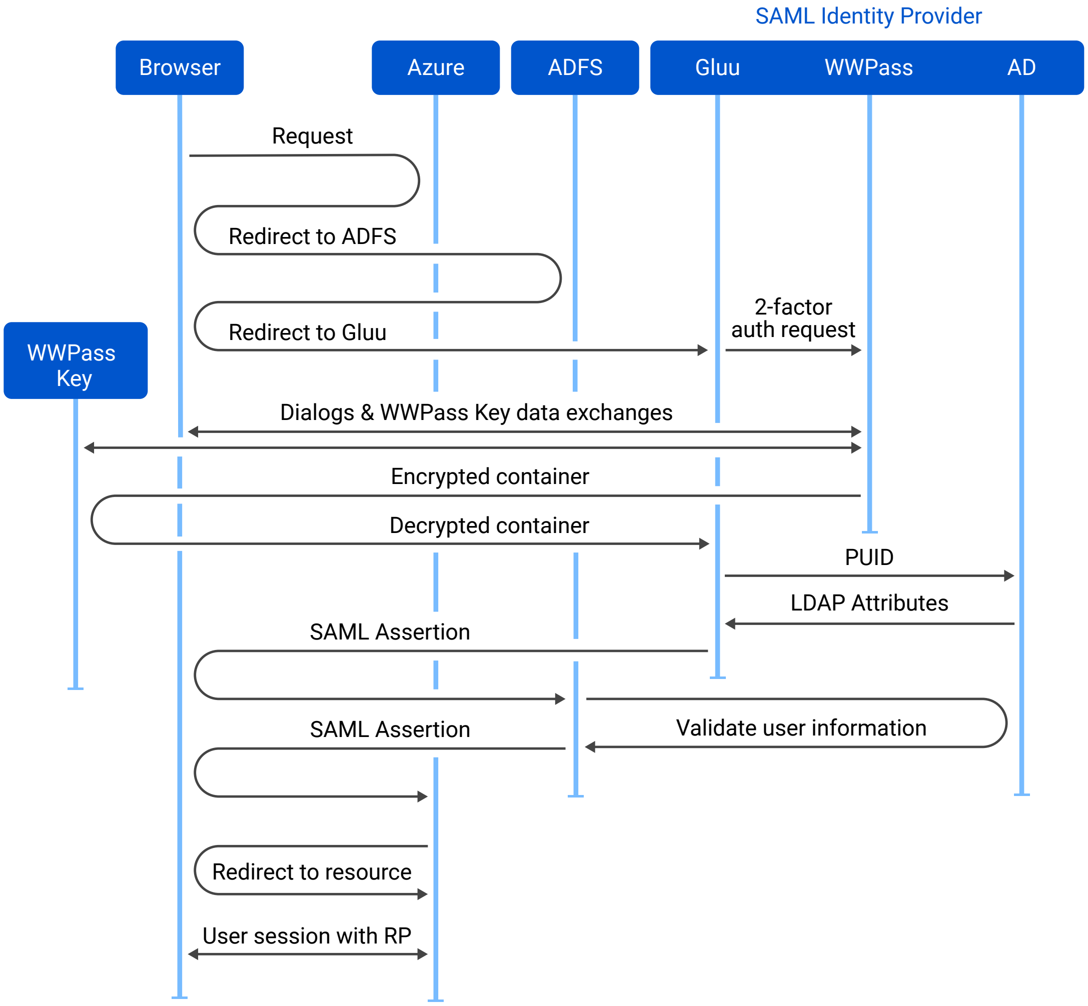
While the combination of Gluu, WWPass authentication, and AD performs the SAML Identity Provider role, each of these systems has a specific function:

- 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 personally-identifying information.
- Gluu binds the attributes obtained from AD to the user's session, delivering a SAML security assertion to the RP.

ADFS is used to translate SAML requests and responses between Microsoft-specific variants used by the Azure portal and more standard implementation in the Gluu Server.

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

1. A user navigates to a web app (Azure portal) in a browser.
2. The RP redirects connection to ADFS.
3. ADFS redirects the user to Gluu.
4. Gluu 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 Gluu SSO.



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

5. 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.
6. Gluu finds an LDAP record with this PUID. It checks if the account is enabled and retrieves all the necessary attributes.
7. If the PUID is unknown to the LDAP, then the WWPass interceptor script performs a binding process. Using one of the three methods (email verification, another WWPass Key, or AD username/password).
8. Gluu transmits the attributes in a SAML XHTML form to the browser.
9. The user's browser transmits a SAML Response containing the user information to ADFS.
10. ADFS checks the SAML Response, modifies it for Azure, and returns the modified response to the browser.
11. The user's browser transmits a SAML Response containing the user information to Azure.
12. Azure checks the SAML response, authorizes the user to access the services, and then redirects the browser to the appropriate welcome or "access denied" landing page.

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 the same workflow for other web services, using SAML or OAuth2 protocols for SSO integration, like:

- Zoom
- Google® Apps for Business™ and Education™
- Salesforce.com®
- Dropbox™ for Business

It is also possible to secure remote access to corporate LAN through Cisco, Fortinet, and Juniper VPN clients, allowing remote users to eliminate risks, associated with traditional authentication. All utilizing 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 WWPass SSO, or to obtain a customized solution for your organization, please contact sales@wwpass.com.

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 many enabled local or cloud-based applications without hard to remember username/password combinations! WWPass's 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

* 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