ATABASCA
POWERED BY WWPASS TECHNOLOGY

Multi-Faktor Login für Zoom

Wer sollte dieses Whitepaper lesen:

IT-Experten und Manager, die auf Datensicherheit und Risikomanagement spezialisiert sind.

Eine Voraussetzung dafür ist, dass der Leser mit den grundlegenden Konzepten der Authentifizierung, des Identitätsmanagements und der SSO Anmeldung für webbasierte Anwendungen vertraut ist.

Dank seiner hervorragenden Audio- und Videoqualität, der gut gestalteten Benutzeroberfläche und der angemessenen Preise hat sich **Zoom** zur führenden Videokonferenzplattform entwickelt. Leider mangelt es der Plattform an Qualität der Sicherheit, was die Benutzer vor zahlreiche Herausforderungen stellt.

Einer der anfälligsten Teile der Zoom-Sicherheit ist die Benutzerauthentifizierung. Die integrierte Benutzerverwaltung basiert sich auf der Verwendung von E-Mails als Benutzernamen und Passwörter für die Benutzerüberprüfung. Diese schwache Authentifizierungsmethode setzt Benutzer einem ernsthaften Risiko für unbefugten Zugriff, Phishing und andere Sicherheitsbedrohungen aus. Für Business- und Enterprisebenutzer, bei denen die Benutzerverwaltung auf dem Active Directory (AD) des Unternehmens basiert, macht die Verwendung derselben Benutzernamen und Passwörter für Zoom und AD die Infrastruktur des Unternehmens für Hackerangriffe anfällig. Benutzer mit Business oder Enterprise Zoom-Konten können jedoch die Sicherheit erheblich verbessern, indem sie Zoom in eine robuste Single Sign-On-Plattform mit Multi-Faktor-Authentifizierung integrieren.

Gluu SSO + WWPass bietet ein viel höheres Maß an Sicherheit, ohne auf Komfort zu verzichten. In Kombination mit allen LDAP-basierten Benutzerverwaltungssystemen (wie Microsoft Active Directory und anderen) bietet Gluu SSO + WWPass einen sicheren Anmeldedienst für SAML-kompatible webbasierte Geschäftsanwendungen. Mit dieser Lösung können Unternehmen ein Höchstmaß an

starker Authentifizierung gemäß DSGVO (Allgemeine Datenschutzgrundverordnung (EU) 2016/679) und NIST (SP 800-63-1) erreichen. Diese Lösung ist sowohl konform als auch sicher und trägt zu der Widerstandsfähigkeit gegen externe Angriffe bei.

Die Verwaltung von Gluu SSO + WWPass auf VMware vSphere® Appliance- und Benutzerrechten ist unkompliziert für erfahrene IT-Profis. Erstellung einer Zoom-Benutzergruppe erlauben Administratoren einen sofortigen Zugriff auf Zoom-Konten für alle vordefinierten Mitarbeiter mit Optionen zur Feinabstimmung bestimmter Zugriffsrechte.

1. Was ist Gluu SSO+ WWPass?

Gluu SSO + WWPass

Erhöhen die Sicherheit von SAML und Oauth2-konformen Anwendungen durch Ersetzen von Benutzername / Passwort basierten Logins mit einer starken Multi-Faktor Authentifizierung.

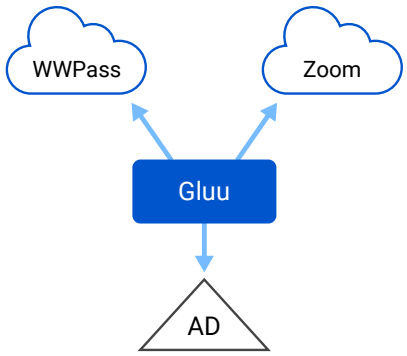
Bieten Benutzern eine einfachere, sicherere und schnellere Anmeldung für Zoom und andere SAML / Oauth2 basierte Anwendungen und andere wichtige Unternehmensdienste wie z.B. VPN.

Vereinfachen die Verwaltung von Benutzerzugriffsrechten durch Integration in das LDAP-Verzeichnis, einschließlich MS AD.

Gluu-Integration mit WWPass-Hardware oder –Software basierter kryptografischen Multi-Faktor-Authentifizierung bietet DSGVO und NIST-konformes starkes SSO basierend auf SAML oder Oauth2 Protokolle für viele wie Zoom und andere Geschäftsanwendungen an.

Um sich anzumelden, verwenden Benutzer einen WWPass-PassKey anstelle eines Benutzernamens.

Der WWPass PassKey ist ein kryptografischer Token, der in Form von einer praktischen mobilen App, USB / NFC-Anhänger oder einer Smartcard verfügbar ist. Mit einer Zusatzeingabe einer PIN ist der WWPass PassKey eine starke Zwei-Faktor-Authentifizierungslösung.



Der WWPass PassKey ist anonym und enthält keine persönliche Identifikation oder Informationen, Zertifikate, oder andere Identitätsattribute. Der WWPass PassKey

Abkürzungen in diesem Dokument

AD Microsoft Active Directory

IdP-Identitätsanbieter

LDAP Lightweight Directory Access Protocol

RP Relying Party (Anmerkung: In SAML, eine Relying Party ist als Dienstanbieter (SP) bezeichnet)

SAML 2.0 Security Assertion Markup Language 2.0

SP Dienstanbieter (SAML Bezeichnung für eine vertrauende Partei -RP)

SPID WWPass-Dienstanbieter Identifikator (Dienstanbieter ID)

PUID Persönliche Benutzer-ID (Anonymisierter Identifikator eines Benutzers) gespeichert in dem WWPass verteilten Netzwerk

SSO Single Sign-on

UPN AD-User Principal Name

Gluu Gluu SSO-platform

VPN Virtuelles privates Netzwerk

bietet eine einfache und sichere, anonyme Methode zur Multi-Faktor-Authentifizierung für jede VPN- Verbindung, Web- oder PC / Mobile-basierte Anwendung. Er bietet auch gleichzeitig eine beispiellose Bequemlichkeit für den Benutzer, der jetzt ein einziges Gerät für Anmeldungen aller Art einsetzen kann.

Für das IT-Team Gluu-Integration mit Active Directory bietet eine vertraute Verwaltungsschnittstelle für zentral verwaltete Benutzerzugriffsrechte. Das On- und Offboarding von Benutzern erfolgt über die AD-Benutzerverwaltung. Das Software von Gluu SSO + WWPass läuft als virtuelle Appliance auf einer VMware vSphere-Infrastruktur des Unternehmens - einer Virtualisierung Technologie, die vielen IT-Fachleuten bereits bekannt ist. Das Design von Gluu vereinfacht die Bereitstellung und reduziert die IAM Verwaltungskosten.

Risikomanagement-Profis und Datenschutzbeauftragte können sich zurücklehnen, denn wenn ein WWPass PassKey verloren geht oder gestohlen wird, die Datensicherheit der Firma dabei in keiner Weise beeinträchtigt wird. Ein einfaches webbasiertes Dienstprogramm ermöglicht dem Benutzer oder einem autorisierten IT-Administrator (fungiert als Wiederherstellungsagent des Benutzers), den verlorenen WWPass PassKey zu annullieren und einen Ersatz zu erstellen. Die Wiederherstellungsverfahren für die mobile WWPass PassKeys ermöglicht Benutzern eine Wiederherstellung der ursprüngliche WWPass PassKey auf dem neuen Telefon, während die App auf dem alten Telefon dauerhaft deaktiviert wird.

2. Wie funktioniert Gluu SSO + WWPass für Zoom?

Gluu SSO+ WWPass ist sowohl für Endbenutzer als auch für die IT- Administratoren einfach zu verwenden. Eine Kombination von Gluu, WWPass-Clouddienste und die LDAP-Verzeichnisdienste unter einer Haube erstellt die SAML Identity Provider (IdP) -Funktion.

Unterstützte Funktionalität und Anforderungen

Virtualisierung
VMWare vSphere v6.0 und höher

Verzeichnis
Microsoft Active Directory 2008/2012/2016

Unterstützte Browser
Chrome ™; Mozilla Firefox®; Opera ™; Safari®; Microsoft Edge

Unterstützte Protokolle
SAML 2.0, Oauth 2

Mindestanforderungen
50+ GB Speicherplatz; 8+ GB RAM; ein 64-Bit-Intel®- oder AMD®-Prozessor (2+ Kerne)

2.1. Was der Benutzer sieht

1. Der Benutzer navigiert zum Zoom Corporate Portal (Vanity URL) Corp.zoom.us (wobei Corp die Unternehmens-ID ist, die bei Zoom registriert ist) oder wählt im Zoom-Client „Mit SSO anmelden".
2. Nach dem Klicken auf Host oder Anmeldeschaltfläche (Funktionen welche eine Authentifizierung abfragen), wird dem Benutzer das WWPass-Anmeldebild angezeigt. Der Benutzer verwendet seinen WWPass PassKey (über USB- oder NFC-Schnittstelle) oder scannt das QR-Code mit der WWPass PassKey App.
3. Wenn es die allererste Anmeldung des Benutzers auf Zoom mit WWPass Key ist, Gluu SSO + WWPass identifiziert den unbekannten Token und bietet dem Benutzer die Möglichkeit an, sich mit in AD (oder einem anderen LDAP) gespeicherten Benutzername und Passwort des Benutzers anzumelden.
4. Nachdem der WWPass PassKey an das Benutzer-AD-Konto gebunden ist, wird die Kombination Benutzername / Passwort nie wieder verwendet.
5. Nach der erstmaligen Registrierung meldet sich der Benutzer bei Zoom nun mit WWPass PassKey an.
6. Systemadministratoren (entsprechend der Unternehmenssicherheit Richtlinien) können den zweiten Authentifizierungsfaktor aktivieren. Im WWPass Fall handelt es sich um eine PIN, die diesem bestimmten WWPass PassKey zugeordnet ist. Auf modernen Mobilgeräten kann eine PIN durch eine Gerätebiometrie (Fingerabdruck oder FaceID) ersetzt werden.

2.2. Unter der Haube

Die einmalig einfache Erfahrung des Benutzers mit Gluu SSO und WWPass PassKey wird durch leistungsstarke Sicherheitstechnologien unterstützt.

Abhängig von der IAM-Unternehmensstrategie kann die Benutzerverwaltung der Active Directory übertragen oder vollständig von Gluu ausgeführt werden. Da die meisten

Organisationen bereits über ein IAM-System verfügen, werden wir die Microsoft AD-Integration hier beschreiben.

Zur Verdeutlichung werden die folgenden SAML-definierten Rollen innerhalb der Gluu-Architektur ausgeführt:

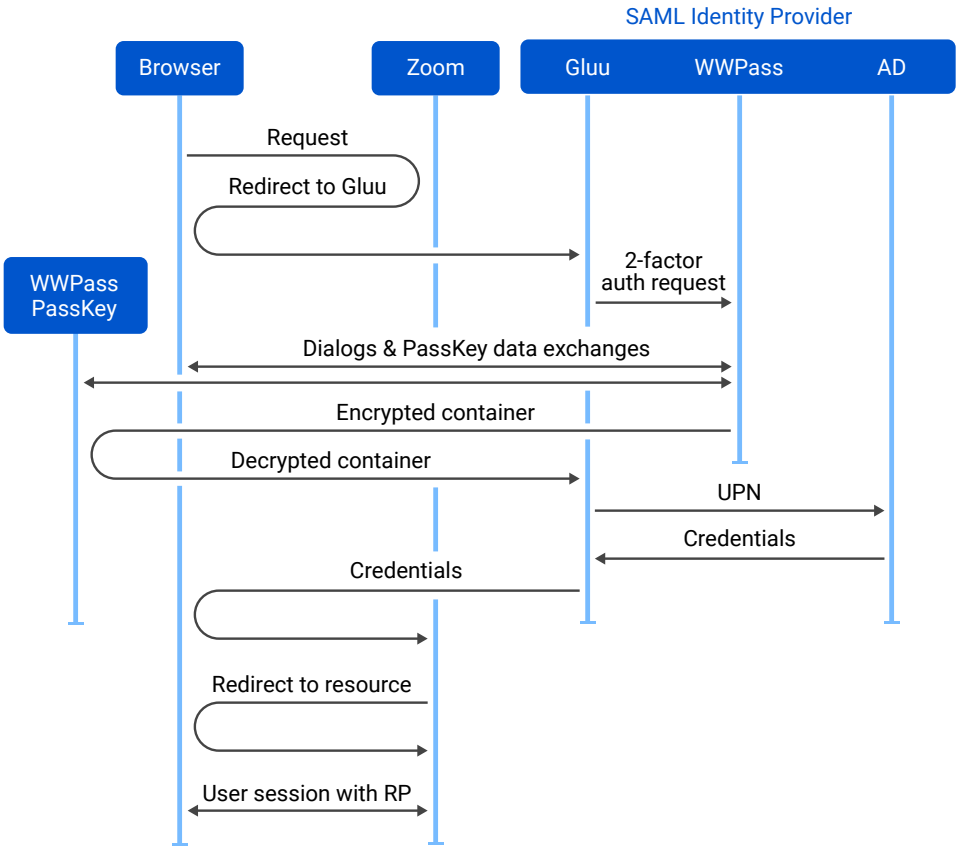
- **SAML SP (auch bekannt als RP):** Die Ziel-Web-App.
- **SAML User Agent:** Der Webbrowser des Benutzers.
- **SAML IdP** Die Kombination von Gluu-, AD- und WWPass-Diensten. Gluu implementiert den SAML-Nachrichtenaustausch mit der Web-App und dem Browser des Benutzers.

Während die Kombination aus Gluu, WWPass-Authentifizierung und AD die Rolle des SAML-Identitätsanbieters übernimmt, hat jedes dieser Systeme eine bestimmte Funktion:

- WWPass authentifiziert die Basisidentität des Benutzers*. Die Basisidentität unterscheidet den Benutzer von allen anderen Maschinen und Personen, ohne persönliche Benutzerinformationen zu enthalten.
- AD fungiert als autorisierender Attributanbieter, der die Zugriffsrechte des Benutzers und andere persönliche Identifikationsinformationen besitzt.
- Gluu bindet die von AD erhaltenen Attribute an die Sitzung des Benutzers und übermittelt dem RP eine SAML-Sicherheitszusicherung.

In der folgenden Abbildung sehen Sie eine Darstellung des Gluu-Authentifizierungsworkflows in Aktion gemäß den folgenden Schritten:

1. Ein Benutzer navigiert in einem Browser zu einer Web-App (Zoom).
2. Der RP leitet die Verbindung zu Gluu um.
3. Gluu kommuniziert mit dem WWPass-Interceptor-Skript, das WWPass-Server kontaktiert, um eine Zwei-Faktor-Benutzerauthentifizierung anzufordern. WWPass-Server kommunizieren mit einem Browser auf dem Computer des Benutzers und fordern den Benutzer auf, einen QR-Code mit der WWPass PassKey-App zu scannen und eine PIN einzugeben. Gleichzeitig wird die Zustimmung des Benutzers zur Anmeldung bei Gluu SSO bestätigt.



Hinweis: Die gesamte Kommunikation zwischen WWPass-Servern, Gluu und dem Computer des Benutzers verwendet verschlüsselte SSL-Sitzungen.

4. WWPass-Server überprüfen, ob der WWPass PassKey des Benutzers gültig und die PIN korrekt sind. In diesem Fall setzen die WWPass-Server eine verschlüsselte Benutzerkennung -PUID aus dem fragmentierten, global verteilten WWPass-Speicher** wieder zusammen und liefern die PUID an Gluu.
5. Gluu findet mit dieser PUID einen LDAP-Datensatz. Es prüft, ob das Konto aktiviert ist und ruft alle erforderlichen Attribute ab.
6. Wenn die PUID dem LDAP unbekannt ist, führt WWPass einen Bindungsprozess durch. Es fordert die AD-Anmeldeinformationen des Benutzers an, die nur einmal verwendet werden, um das AD-Konto mit der PUID zu verknüpfen. Wenn die Anmeldeinformationen gültig sind, wird der Benutzer aktiviert und sein Konto wird mit dieser PUID verknüpft. Domänenanmeldeinformationen werden für nachfolgende Anmeldungen nie wieder verwendet.

7. Gluu überträgt die Attribute in einem SAML XHTML-Formular an den Browser.
8. Der Browser des Benutzers sendet eine SAML Request Assertion Consumer Service-Nachricht mit den Anmeldeinformationen an Zoom.
9. Zoom überprüft die SAML-Antwort, autorisiert den Benutzer zum Zugriff auf die App und leitet den Browser dann zur entsprechenden Zielseite “Willkommen” oder “Zugriff verweigert” weiter.

2.3. Für den IT-Administrator: Hinzufügen und Entfernen von Benutzern

Da Gluu in unserem Fall so eng in vorhandene Active Directory integriert ist, ist das Hinzufügen und Entfernen von Benutzern schnell und einfach.

Damit vorhandene Benutzer auf ein Zoom-Unternehmenskonto zugreifen können, müssen sie der Gruppe ZOOM USERS hinzugefügt werden. Wenn sie auch einer Untergruppe ZOOM LICENSED USERS hinzugefügt werden, wird versucht, ihren Benutzerstatus bei jeder Anmeldung bei Zoom auf “Licensed” zu setzen. Wenn der Benutzer diesen Status bereits hat, wird er nicht geändert. Wenn dies nicht der Fall ist und kostenlose Lizenzen verfügbar sind, wird dem Benutzer der Status “lizenziert” zugewiesen.

Wenn ein Benutzer nicht zur Untergruppe Zoom Licensed User gehört, wird sein Status bei jeder Anmeldung auf Basic herabgestuft.

Der Administrator löscht einen Zoom-Benutzer, indem er den Benutzer aus der AD-Gruppe der Zoom-Benutzer entfernt. Weder mit Gluu noch mit dem WWPass PassKey des Benutzers sind zusätzliche Aktionen erforderlich, da weder personenbezogene Daten noch Sicherheitszertifikate bei Gluu oder WWPass PassKey enthalten sind.

Über WWPass

WWPass behebt die größte Schwäche der Informationss-cherheitsinfrastruktur, indem Benutzer und Daten bequem und sicher geschützt werden. Mit nur einem einzigen selbstverwalteten WWPass PassKey können sich Benutzer problemlos für eine Reihe aktivierter lokaler oder Cloud-basierter Anwendungen authentifizieren, ohne sich schwer zu merkende Kombinationen aus Benutzername und Kennwort zu merken. Die patentierten Authentifizierungs- und Cloud-Speichertechnologien von WWPass halten sowohl die Daten der Anwendung als auch die Benutzeridentität von allen anderen Anwendungen separiert und verborgen, wodurch sowohl die Privatsphäre von Benutzern als auch von Anwendungen geschützt wird. Durch die Integration der WWPass-Technologie in ihre Anwendungen schützen Unternehmen zwei wichtige Ressourcen: ihre Daten und ihre Benutzer.

Erfahren Sie mehr unter wwpass.com.

Atabasca Systems AG

Rubisacherrain 25
CH-6440 Brunnen
Phone +41 (0) 41 820 57 20
Fax +41 (0) 41 820 57 21
atabasca.ch

3. Kann Gluu SSO+ WWPass zum Schutz von Anmeldungen bei anderen Diensten verwendet werden?

Gluu SSO+ WWPass ist für die Verwendung in Organisationen mit 10 bis 100.000 Benutzern vorgesehen und kann genau den gleichen Workflow für andere Webdienste bereitstellen, welche SAML- oder Oauth2-Protokolle für die SSO-Integration verwendet, z.B.

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

Es ist auch möglich, den Remotezugriff auf das Unternehmens-LAN über Cisco-, Fortinet- und Juniper-VPN-Clients sicher zu machen, sodass die Risiken die mit der herkömmlichen Authentifizierung verbunden sind dabei beseitigt werden. Alles mit ein und demselben WWPass PassKey.

Bereit für den nächsten Schritt?

Da die Benutzersicherheit im Vordergrund jedes Geschäfts steht, gab es nie einen besseren Zeitpunkt, um in den Schutz Ihres Unternehmens zu investieren. Um mehr über Gluu SSO + WWPass zu erfahren oder eine maßgeschneiderte Lösung für Ihr Unternehmen zu erhalten, wenden Sie sich bitte an sales@atabasca.ch oder sales@wwpass.com.

---

* Towards a Trustworthy Digital Infrastructure for Core Identities and Personal Data Stores by Hardjono, Greenwood and Pentland https://www.wwpass.com/wp-content/uploads/hardjono-greenwood-coreid.pdf

** How WWPass Works https://www.wwpass.com/wp-content/uploads/WWPass_Authentication_How_It_Works.pdf