White Paper

Privakey SSO: Revolutionizing Passwordless Authentication

January 2024

Table of Contents

Introduction

Overview of Privakey SSO

Privakey SSO represents a paradigm shift in the field of Identity and Access Management (IAM). By leveraging passwordless technology, it offers organizations a secure and user-friendly solution for securely accessing multiple cloud accounts and SaaS services.

This white paper delves into the intricacies of Privakey SSO, highlighting its importance in the modern digital landscape.

Importance of Passwordless SSO

In an era where cybersecurity threats are escalating, passwordless authentication has emerged as a critical solution. It not only enhances security but also simplifies the user experience, thereby increasing efficiency and reducing the risk of system breaches.

The Problem with Passwords

Over 80% of system breaches are attributed to stolen credentials.[1] Why are passwords such poor credentials?

Poor user password hygiene

Managing multiple IDs and passwords has become increasingly complex for the average user. To deal with the challenge, users become complacent:

1. 50% of Internet users use the same password for all their accounts[2]
2. 60% of people reuse the same passwords often[3].
3. People also rely on easily hacked passwords. According to NordPass the top 5 passwords in 2023 were 123456, admin, 12345678, 123456789 and 1234.[4]

This complacency leaves systems vulnerable to unauthorized access by bad actors.

Vulnerable Password Recovery

Passwords are, by definition, something a user knows. And users forget things. When a user forgets a password a recovery process is initiated.

[1] 2022 Verizon Data Breach Report, 2022
[2] Last Pass 2021
[3] MSN 2021
[4] https://nordpass.com/most-common-passwords-list

This vulnerable recovery process is often exploited by hackers. The group behind the widely reported MGM Resorts breach in 2023 have claimed on X, "All ALPHV ransomware group did to compromise MGM Resorts was hop on LinkedIn, find an employee, then call the Help Desk [to get a password]."

Passwords are insufficient

Passwords are vulnerable to numerous attack vectors from reuse, interception and servier-side breaches. Common password attacks include: Phishing, Credential Stuffing, Keylogging, Man-in-the-Middle Attacks, Pharming, Brute Force Attacks, Dictionary Attacks. These are all easily executed ways bad actors gain access to users' credentials that can be mitigated by passwordless, .

Multi-factor Authentication – It is not always enough

> ***Multi Factor Authentication refers to using more than one factor ("Something you know", "Something you Have" and "Something You Are") to access a system. When an authentication requires one or more of these components it is considered multi-factor.***

A common mitigation against the weaknesses of Username and Password authentication is the addition of an additional factor. However, enhancing security through the addition of extra factors, while crucial, often presents genuine challenges and costs, sometimes compromising user convenience in the process.

Temporary One Time Passcodes (TOTPs), delivered via a text or generated on an app, are a common way to add another step. However, these 'factors', while an improvement, are susceptible to several of the same attacks as password-based authentication, including Pharming and Replay Attacks. Further, SIM swaps can allow one to gain access to TOTPs delivered via text.

Hardware Tokens reduce the attack surface but require investment. And, in some implementations, they can be compromised by Pharming and Keylogging.

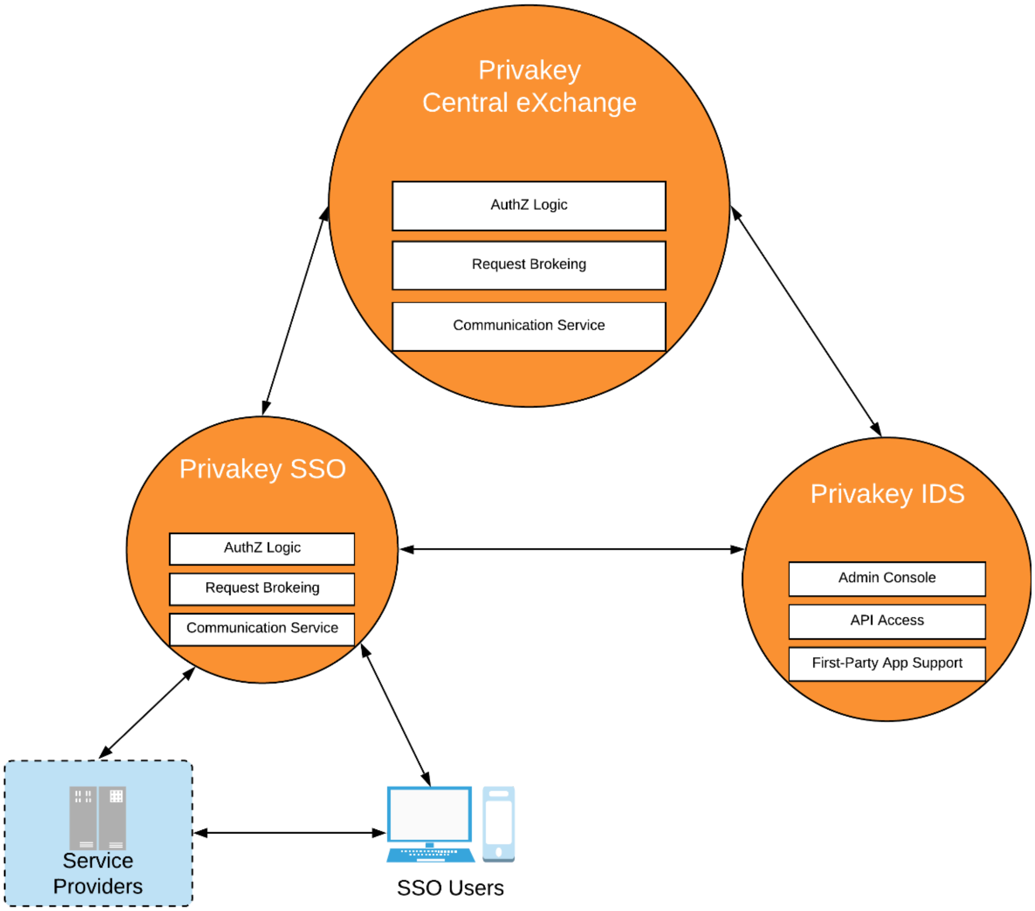
The Emergence of Passwordless Authentication

Passwordless Authentication is rooted in the principle that a secure and trusted token, stored on a secure user device, protected locally by a traditional authentication factor such as biometrics or passphrases, can be used to confirm a user's identity without relying on a user transmitting a password.

Passwordless Authentication effectively removes the most exploited element, the password, from authentication.

The team that founded Privakey were previously working at a company that issued highly secure, passwordless smart-card tokens to US Federal agencies. Noting that the exorbitant costs and challenges associated with implementing highly trusted smart-card ecosystems would hinder its adoption at scale by other organizations and consumers, the team initiated an innovation initiative to explore the most effective way to deliver this level of security on a larger scale and at a reasonable expense.

Privakey, Privakey CX, Privakey Identity Services (IDS) and the Privakey SSO were born from these endeavors.

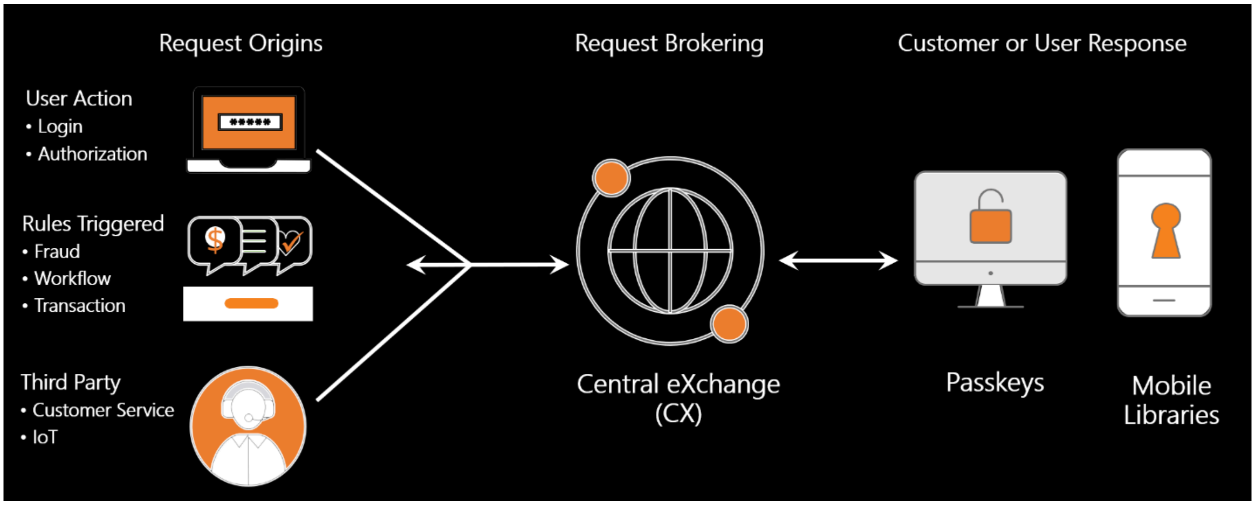


Privakey CX is a highly scalable platform for plug-and-play passwordless identity and authentication. Privakey CX enabled services can instantly identify any trusted, provisioned user. Additionally, services can challenge users with on-demand Step-Up authentications and Privakey Event authorizations. The Privakey IDS API enables the following Privakey CX interactions:

- Zero-trust authentication and authorization
- Two-way trusted interactions between systems and users
- Interactive, contextual, and digitally signed interactions

All Privakey authentications, transactions, and events are secured using:

- Asymmetric cryptography is generated on a user-possessed device's secure element.
- Privakey key is stored on a user-possessed device's secure element.
- Public key stored on Privakey Central eXchange Server (Privakey cloud or customer premised).
- Leverages device native biometrics.
- No passwords (phishing-proof, and no honey pots).
- All sensitive transactions exchanged over TLS with AES 256-bit encryption and device-App=key encryption
- All transactions are digitally signed and auditable (immutable logs)



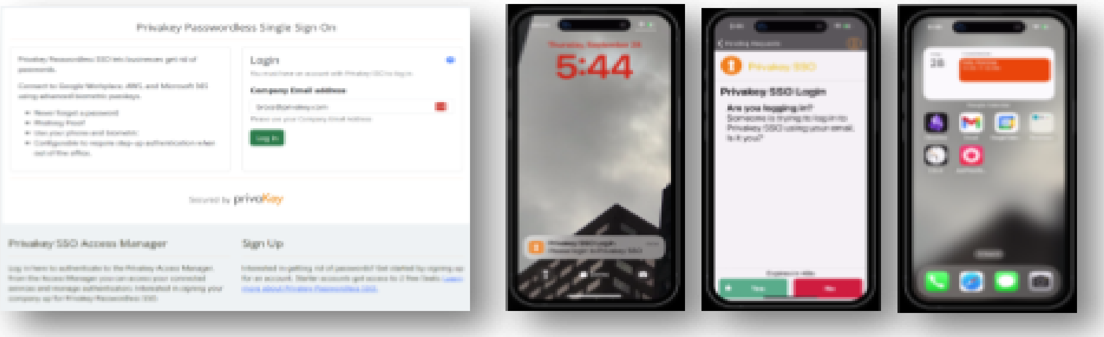
With the Privakey IDS API any kind of authentication or authorization can be supported, including:

1. Privakey ID: Simple Authentications
2. Privakey Step-Up: Re-authentications and third-party approvals
3. Privakey Events: Detailed, interactive call-and-responses that enable contextually rich and dynamic digitally signed exchanges between systems and their securely identified end users.

A Passwordless SSO

The Privakey Passwordless SSO combines the feature-set of a light-weight Identity Provider with the security of Privakey CX. Privakey's SSO is designed to be the simplest way for companies and their employees to gain access to their critical cloud accounts, data, and resources.

Figure 3: The Privakey SSO



Privakey Passwordless Single Sign On

Login

Company Email address

Log In

Secured by privaKey

Privakey SSO Access Manager

Sign Up

5:44

Privakey SSO

Privakey SSO Login

Are you logging in?

Someone is trying to login to Privakey SSO using your email. Is it you?

Yes

No

Simple to administer and even easier to user, the Privakey SSO allows organizations to do away with passwords and enable passwordless access to their critical SaaS tools.

Access all your day-to-day productivity tools with secure passwordless Privakey Authenticators. Getting to Google, Microsoft, Okta, Salesforce, AWS, Zoom, Box, and many, many more is made easy with Privakey SSO.

Companies can set Privakey SSO up in minutes and protect their critical business assets while making getting to work easier for all their users.

Privakey SSO: A Detailed Overview

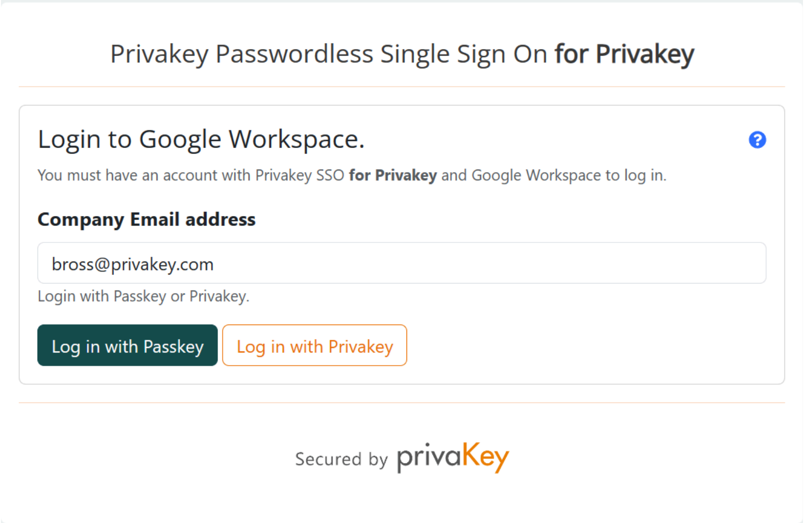
Concept and Design Philosophy

Privakey SSO is designed with the user's convenience and security in mind. By eliminating traditional passwords, it reduces the attack surface, while also streamlining the login process.

Key Features and Benefits

Passwordless Authentication:

Using the Privakey App, Passkeys or both, users will access the Privakey SSO and connected services without passwords.



Privakey Passwordless Single Sign On **for Privakey**

Login to Google Workspace.

You must have an account with Privakey SSO **for Privakey** and Google Workspace to log in.

Company Email address

bross@privakey.com

Login with Passkey or Privakey.

Figure 4: Multiple Passwordless Authenticators

Users in Privakey never set up a password, rather they configure either or both secure Passwordless modality offered by Privakey: The Privakey Authenticator or framework-based Passkeys. Both technologies are deeply integrated within Privakey CX and the SSO. All adopters of Privakey SSO need to do to benefit from their convenience and security is invite their users to the platform.

Providing 2 secure, passwordless modalities ensures both convenience and strong recovery.

Single Sign-On

Privakey SSO allows users to authenticate once and gain access to all linked cloud and SaaS services, enhancing productivity. Instead of remembering and maintaining countless passwords and MFA tokens, users of Privakey SSO just need to enter their username and provide a biometric (or PIN) to access all the services.

C

Google Workspace
Office 365
okta
zoom
Azure
slack
Trello
asana
ZOHO
Dropbox
box
salesforce essentials
GitHub
GitLab
freshdesk
mailchimp
monday.com
intuit quickbooks
xero
gusto
bambooHR
HubSpot
LastPass
zendesk
DocuSign
Airtable
Adobe Creative Cloud
webex

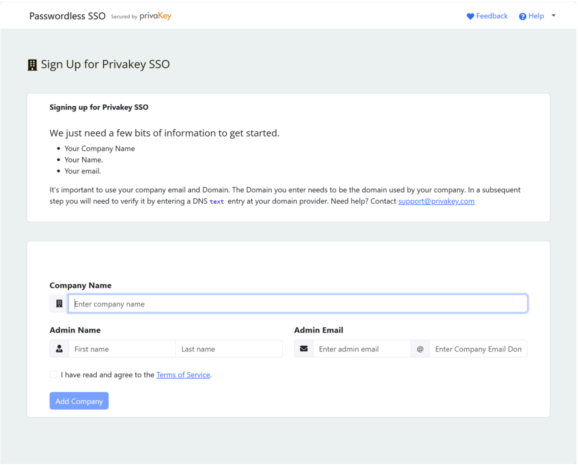
Leveraging standard federated authentication protocols, Privakey SSO lets administrators connect downstream services, such as Office 365, Google, Okta and more with simple, straight-forward configuration.

User-Friendly Interface

Designed for ease of use, set-up and administration ensuring a straight-forward experience from day one. The Privakey SSO has the following easy to use features:

Administration Functions

Self-Sign-Up



Sign Up for Privakey SSO

Signing up for Privakey SSO

We just need a few bits of information to get started.

- Your Company Name
- Your Name.
- Your email.

It's important to use your company email and Domain. The Domain you enter needs to be the domain used by your company. In a subsequent step you will need to verify it by entering a DNS `text` entry at your domain provider. Need help? Contact support@privakey.com

Company Name

Enter company name

Admin Name

First name | Last name

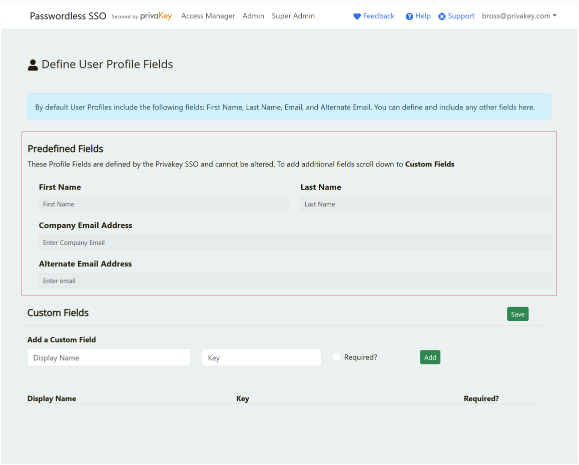
Admin Email

Enter admin email @ Enter Company Email Don

□ I have read and agree to the Terms of Service.

Add Company

Customizable User Profile Fields.



Define User Profile Fields

By default User Profiles include the following fields: First Name, Last Name, Email, and Alternate Email. You can define and include any other fields here.

Predefined Fields

These Profile Fields are defined by the Privakey SSO and cannot be altered. To add additional fields scroll down to **Custom Fields**

First Name

First Name

Last Name

Last Name

Company Email Address

Enter Company Email

Alternate Email Address

Enter email

Custom Fields

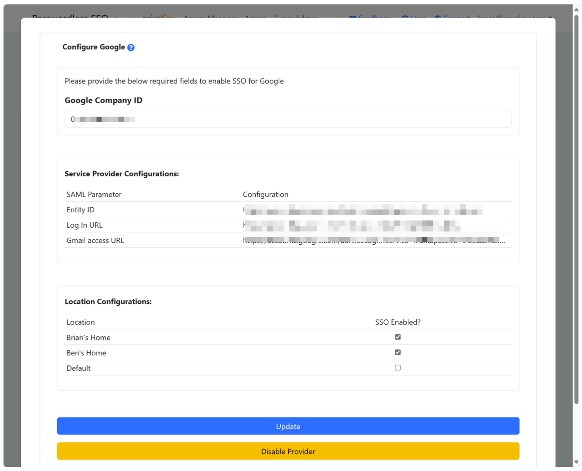
Save

Add a Custom Field

Display Name | Key | □ Required? | Add

Display Name	Key	Required?

Simple Service Provider Configuration.



Configure Google

Please provide the below required fields to enable SSO for Google

Google Company ID

[redacted]

Service Provider Configurations:

SAML Parameter	Configuration
Entity ID	[redacted]
Log In URL	[redacted]
Gmail access URL	[redacted]

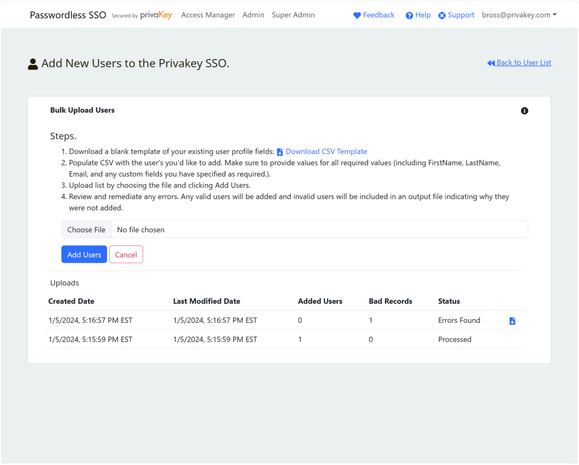
Location Configurations:

Location	SSO Enabled?
Brian's Home	☑
Ben's Home	☑
Default	□

Update

Disable Provider

Ability to add batches of users.



Add New Users to the Privakey SSO.

Back to User List

Bulk Upload Users

Steps.

1. Download a blank template of your existing user profile fields: Download CSV Template
2. Populate CSV with the user's you'd like to add. Make sure to provide values for all required values (including FirstName, LastName, Email, and any custom fields you have specified as required.).
3. Upload list by choosing the file and clicking Add Users.
4. Review and remediate any errors. Any valid users will be added and invalid users will be included in an output file indicating why they were not added.

Choose File No file chosen

Add Users | Cancel

Uploads

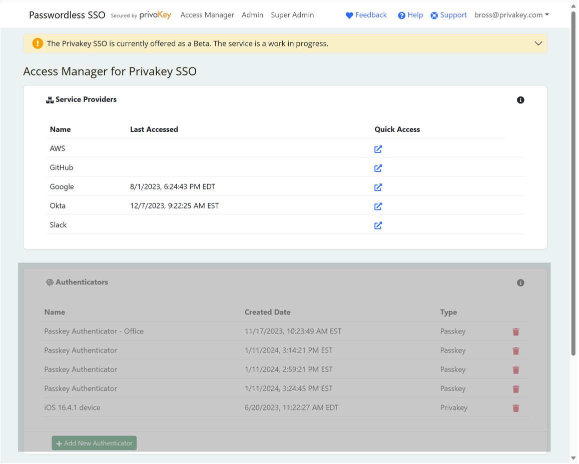
Created Date	Last Modified Date	Added Users	Bad Records	Status
1/5/2024, 5:16:57 PM EST	1/5/2024, 5:16:57 PM EST	0	1	Errors Found
1/5/2024, 5:15:59 PM EST	1/5/2024, 5:15:59 PM EST	1	0	Processed

And much more, including:

- Ability to configure locations.
- Ability to define SSO behaviors for specific services at locations.
- Administer account recovery, token removal and session termination.

User Functions

Quick Links to connected Services.



The Privakey SSO is currently offered as a Beta. The service is a work in progress.

Access Manager for Privakey SSO

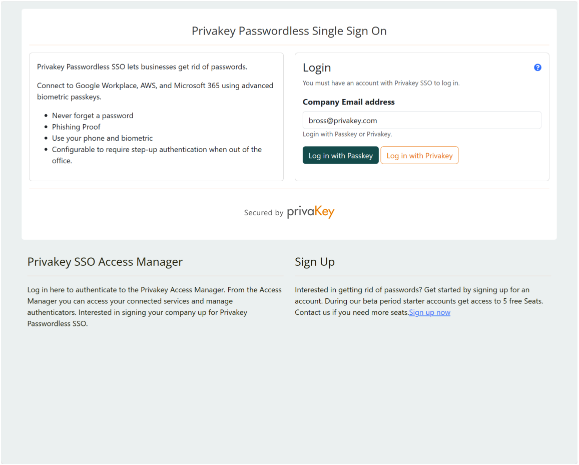
Service Providers

Name	Last Accessed	Quick Access
AWS		↗
GitHub		↗
Google	8/1/2023, 6:24:43 PM EDT	↗
Okta	12/7/2023, 9:22:25 AM EST	↗
Slack		↗

Authenticators

Name	Created Date	Type	
Passkey Authenticator - Office	11/17/2023, 10:23:49 AM EST	Passkey	🗑
Passkey Authenticator	1/11/2024, 3:14:21 PM EST	Passkey	🗑
Passkey Authenticator	1/11/2024, 2:59:21 PM EST	Passkey	🗑
Passkey Authenticator	1/11/2024, 3:24:45 PM EST	Passkey	🗑
iOS 16.4.1 device	6/20/2023, 11:22:27 AM EDT	Privakey	🗑

Direct Access to Connected Services



Privakey Passwordless Single Sign On

Privakey Passwordless SSO lets businesses get rid of passwords.

Connect to Google Workplace, AWS, and Microsoft 365 using advanced biometric passkeys.

- Never forget a password
- Phishing Proof
- Use your phone and biometric
- Configurable to require step-up authentication when out of the office.

Login

You must have an account with Privakey SSO to log in.

Company Email address

bross@privakey.com

Login with Passkey or Privakey.

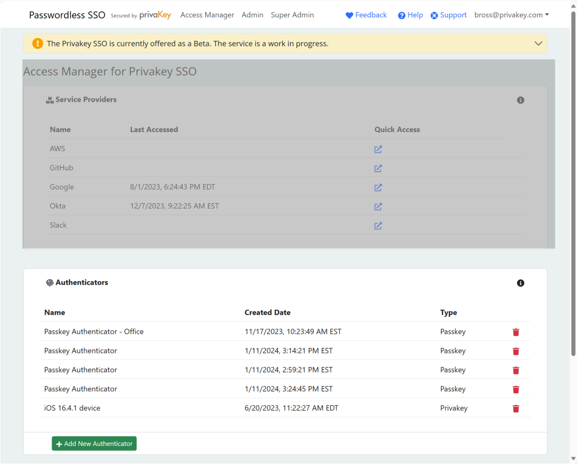
Privakey SSO Access Manager

Log in here to authenticate to the Privakey Access Manager. From the Access Manager you can access your connected services and manage authenticators. Interested in signing your company up for Privakey Passwordless SSO.

Sign Up

Interested in getting rid of passwords? Get started by signing up for an account. During our beta period starter accounts get access to 5 free Seats. Contact us if you need more seats.Sign up now

Manage Authenticators



The Privakey SSO is currently offered as a Beta. The service is a work in progress.

Access Manager for Privakey SSO

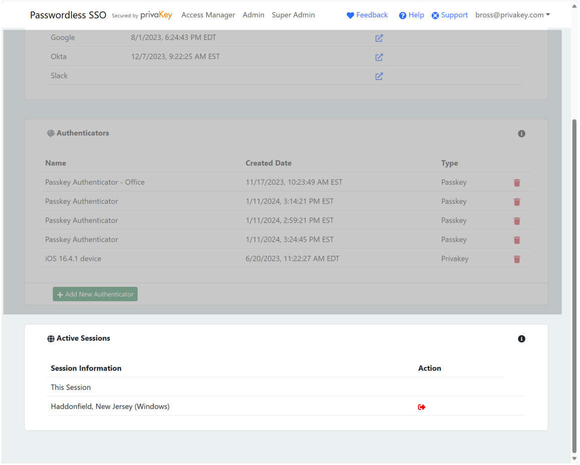
Service Providers

Name	Last Accessed	Quick Access
AWS		↗
GitHub		↗
Google	8/1/2023, 6:24:43 PM EDT	↗
Okta	12/7/2023, 9:22:25 AM EST	↗
Slack		↗

Authenticators

Name	Created Date	Type	
Passkey Authenticator - Office	11/17/2023, 10:23:49 AM EST	Passkey	🗑
Passkey Authenticator	1/11/2024, 3:14:21 PM EST	Passkey	🗑
Passkey Authenticator	1/11/2024, 2:59:21 PM EST	Passkey	🗑
Passkey Authenticator	1/11/2024, 3:24:45 PM EST	Passkey	🗑
iOS 16.4.1 device	6/20/2023, 11:22:27 AM EDT	Privakey	🗑

Manage Sessions



Google	8/1/2023, 6:24:43 PM EDT	↗
Okta	12/7/2023, 9:22:25 AM EST	↗
Slack		↗

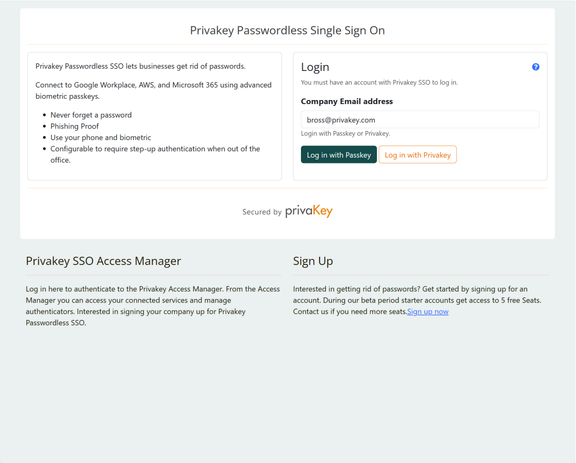
Authenticators

Name	Created Date	Type	
Passkey Authenticator - Office	11/17/2023, 10:23:49 AM EST	Passkey	🗑
Passkey Authenticator	1/11/2024, 3:14:21 PM EST	Passkey	🗑
Passkey Authenticator	1/11/2024, 2:59:21 PM EST	Passkey	🗑
Passkey Authenticator	1/11/2024, 3:24:45 PM EST	Passkey	🗑
iOS 16.4.1 device	6/20/2023, 11:22:27 AM EDT	Privakey	🗑

Active Sessions

Session Information	Action
This Session	
Haddonfield, New Jersey (Windows)	↪

Flexible Sign-on: Privakey or Passkey



Privakey Passwordless Single Sign On

Privakey Passwordless SSO lets businesses get rid of passwords.

Connect to Google Workplace, AWS, and Microsoft 365 using advanced biometric passkeys.

- Never forget a password
- Phishing Proof
- Use your phone and biometric
- Configurable to require step-up authentication when out of the office.

Login

You must have an account with Privakey SSO to log in.

Company Email address

bross@privakey.com

Login with Passkey or Privakey.

Privakey SSO Access Manager

Log in here to authenticate to the Privakey Access Manager. From the Access Manager you can access your connected services and manage authenticators. Interested in signing your company up for Privakey Passwordless SSO.

Sign Up

Interested in getting rid of passwords? Get started by signing up for an account. During our beta period starter accounts get access to 5 free Seats. Contact us if you need more seats.Sign up now

Technical Architecture

Overview

The technical architecture of the Privakey stack is a unique blend of modern technologies and protocols, designed to provide a seamless and secure user experience. This architecture is built to support the robust requirements of passwordless authentication, single sign-on (SSO) capabilities, and alternative authentication methods like PINs and Passkey logins across various platforms and services.

Security Principles of Privakey

Privakey relies on patented IP, standard protocols and several core constructs to ensure the integrity of the SSO.

Privakey Central eXchange.

The Central eXchange Service (CX) is an application server that brokers authentication and authorization requests from relying parties to and from users' devices. Based on patented intellectual property, Privakey CX is responsible for verifying and relaying users' intents from their secure devices to services.

Privakey CX can connect to the Privakey App (available for iOS or Android) or first-party applications enabled through the Privakey IDS (see below). It is the central hub that handles all authentication and authorization verification.

Privakey IDS

The IDS is a service that allows first-party applications and services to interact with Privakey CX. The Privakey IDS exposes API access to Privakey CX. The IDS also allows companies to white label Privakey interactions. By imbedding Privakey's core technologies in first-party applications developers can provide advanced authentication and authorization to their users.

Privakey CX and the Privakey IDS can be licensed or access via the Privakey Cloud. The SSO leverages the Privakey Cloud.

Privakey CX Components

Request Origins

Request Origins are the current processes and workflows of an application or service that would benefit from strong and definitive user authorizations. Multiple different services can connect to a single Privakey instance. Each company configured within the Privakey SSO becomes a request origin with Privakey IDS.

Authenticators

Privakey relies on the Privakey App and device Passkeys as authenticators. By providing multiple passwordless authenticators Privakey IDS provides flexible access, secure recovery and the convenience of local Passkeys and the portability of Privakey Authenticator.

The Privakey App

Available for iOS and Android, the Privakey App is a mobile authenticator designed to be installed on a user's mobile phone. Secure, convenient, and always available the Privakey App is great for day-to-day use, perfect for accessing services from a new or different computer and a great way to ensure one will always have access to their services.

The Privakey App supports push authentications as well as more advanced authorizations.

Passkeys

Passkeys are an emerging web standard for passwordless authentication. Initially developed by the FIDO organization and later adopted by the World Wide Web Consortium (W3C) and major hardware manufacturers and OS's,

Passkeys are a way to directly authenticate services using keys generated and stored on a computer or mobile device. Passkeys rely on browser standards, operating system controls and secure elements in modern computers to generate secure authenticators.

Passkeys, when available on a computer, are great for one's daily workstation. However, they are typically bound the computer on which they're generated, so they have limited use accessing a service from a different or new computer.

Privakey Label

Privakey IDS offers libraries that can be leveraged by developers to extend the capabilities of existing apps to enable Privakey CX Authentication and Authorization Challenges. By enhancing existing ecosystems with Privakey CX Authentication and Authorization first-party application developers can create unique, bilaterally trusted interactions. For example, a bank could dynamically challenge a user to confirm a remotely initiated wire transfer.

Privakey CX Key Principles

Multi-Factor Authorizations

Privakey's simple process for approving authentication and authorization challenges rests in the inherent strength of multi-factor identity assertion. By combining something the user has (their cryptographically bound Passkey or Privakey App on their mobile device) with something they know (a PIN) or something they are (a fingerprint or face biometric), Privakey enables strong, password-free challenge responses.

Asymmetric Cryptography

Asymmetric Cryptography is leveraged in Privakey to strongly bind a device to a user and to digitally sign and verify request challenge responses processed by Privakey CX. During the Privakey App initialization several asymmetric key pairs are generated on the device to ensure the integrity of both device to server interactions and user authentication and authorization assertions. Critically – user's authentication keys are generated on and never leave secure elements of the device. Public keys are transferred to Privakey CX. Authentication keys are rotated frequently.

Device Biometrics

Privakey leverages the native device biometrics of modern mobile devices to ensure user-familiarity, edge processing of biometric challenges and to ensure deep access to device hardware security elements.

PINs are better than Passwords.

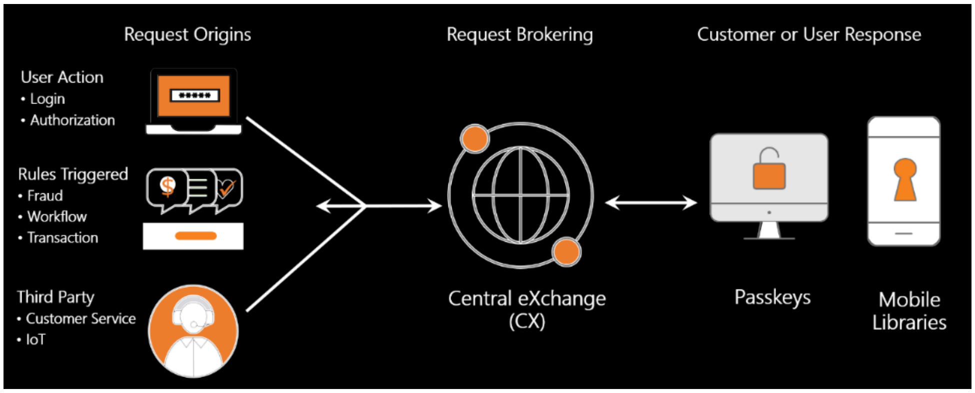
Privakey allows services to rapidly enable authentication and authorizations without shared-secrets — no need for passwords or knowledge-based authorizations.

The PIN used by both Passkeys and the Privakey App (relied on when biometrics are unavailable, not configured or failed) are never stored on the users' devices or the Privakey Auth Service. Nor are they ever transmitted or shared with the Privakey Auth Service. The PIN is used computationally to protect and gain access to the private key store on the device. If a bad actor had a user's PIN, they would also need access to the user's device to execute any authorizations.

Secure Data Flow

The communication process within the Privakey CX architecture is both secure and efficient, accommodating various authentication methods:

Initiation of Authentication Request: An authentication request is initiated when a user attempts to access a cloud service or application. The request is an authenticated server-server request generated by a Relying Party to the Privakey CX via Privakey IDS API endpoints.



Notification of Authentication: A user is notified of a challenge either locally on the originating device (when using Passkeys) or via a framework notification to the Privakey App. The Notification delivered to the device does not include any sensitive information. This notification is used to advise the user and the App that there is a pending challenge. The App then securely connects to Privakey CX to access the encrypted payload.

Biometric Verification or PIN/Passkey Entry: After the App access the request and the user views it they are provided context to assess the validity of the request. The user can Accept or Reject the request. If they to the user's device, where biometric verification or PIN/Passkey entry is performed.

Authentication Response: The device sends a signed authentication response payload back to Privakey CX, confirming the user's identity and intent.

Granting Access: Privakey CX communicates the outcome of the interaction to the requested cloud service or application.

Extending Privakey IDS with SSO

Single Sign-On is a process that allows a user to access multiple services with one set of credentials. Further, Single-Sign-On can allow users to access the multitude of applications after they have single authentication.

The Privakey SSO is an independent, multi-tenant SaaS service that leverages Privakey CX.

The SSO is intentionally designed as a lightweight Identity and Authentication provider, providing the key capabilities of an SSO while ensuring it is easy to set up and use.

Key SSO Concepts

Companies

The Privakey SSO is a multi-tenant platform. When a new entity signs up, they sign up as a Company. A company is defined as a domain-joined entity, such as *ssousingcompany.co*m with domain-based users who have domain-based emails, such as *boss@ssousingcompany.com*. To complete sign-up an individual must validate domain ownership.

Users

The Privakey SSO is designed to support employees of organizations. Once set-up these users will use the Privakey SSO to access all configured services (see Services below).

Services

Services are the online applications connected to the SSO (such as Google Workspace, Microsoft 365, AWS, Okta, etc.). Privakey SSO makes connecting the SSO to Services as easy as possible. For most services only one or two bits of data a required to configure Privakey. While configuration on the Service itself may be more complicated Privakey SSO Documentation makes it easy.

Privakey federates access to services by using standards-based protocols including SAML and JWT.

Authenticators

Privakey SSO uses Privakey IDS authenticators - the Privakey App and device Passkeys - as authenticators. By providing multiple passwordless authenticators the Privakey SSO provides flexible access, secure recovery and the convenience of local Passkeys and the portability of Privakey Authenticator.

Locations

Optionally, Locations can be configured when setting up the Privakey SSO. Locations are defined by CIDRs (Classless Inter-Domain Routing definitions). It is a notation that represents a range of IP addresses and can be used to specify a physical location. By enabling Locations, a Company can specify different SSO rules for services. For example, if a company wants to make a resource harder to get to when a User is not in the office, they will use Locations to set specific rule requiring the user re-authenticate when accessing the service outside the office.

Summary

The expanded technical architecture of Privakey SSO demonstrates its versatility and adaptability in the face of evolving authentication needs. By supporting biometric, PIN, and Passkey authentication methods, it offers a secure, scalable, and user-friendly platform for a wide range of applications and user preferences. This comprehensive approach to authentication positions Privakey SSO as a leading solution in the realm of modern cybersecurity and identity management.

Setting Up Privakey SSO

Enabling passwordless access

The Privakey Passwordless SSO is designed to make managing enterprise class, passwordless authentication easy for small to mid-size business managers to manage. If you are already administering, for example, Google Workspace or Microsoft 365 you can administer Privakey.

Prerequisites

A verifiable Domain:

Privakey Passwordless SSO currently requires companies to have a registered domain. For example, for Acme Co this might be acme.co. During sign-up one will need to verify control of the domain.

Domain-based Email

Privakey Passwordless SSO shares your user's email addresses with connected services. The requirement to have this email be associated with a domain you own and manage is often a requirement of online applications and services that accept third party authentication. To facilitate this connection all users in the system must use a domain email. So, if you were acme.co, all users must have an email structured like: user@acme.co.

Access The Privakey Passwordless SSO

One can sign up for Privakey passwordless SSO at Privakey SSO - Signup (https://sso.privakey.com/signup).

To get started one will need to:

1. Provide basic information including Name, Email, Domain, and phone number.
2. Create your passwordless authenticator.
3. Verify control of your domain by entering a txt record in your DNS registry.

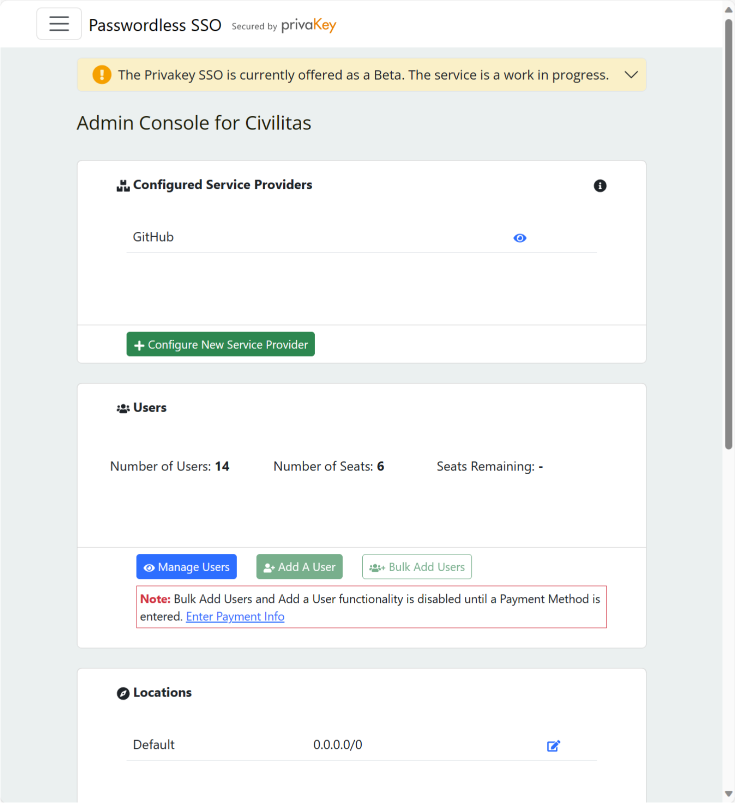
Administering Activities

There are three main components to configuring the Privakey Passwordless SSO:

1. **Users:** These are company employees who will leverage the Privakey Passwordless SSO to access company resources.
2. **Service Providers:** These are the services that you will use Privakey to access. Examples include Google Workspace, Microsoft 365, Octa, AWS, Dropbox, Box and Zoom.

1. **Locations:** Locations can be used to define Single Sign On rules for services. For example, you may want to require your users to always log into a service when they are not in the office but enable SSO access when they are in the office.

These capabilities can be managed from the Privakey Passwordless SSO Admin console.



The Privakey SSO is currently offered as a Beta. The service is a work in progress.

Admin Console for Civilitas

Configured Service Providers

GitHub

Users

Number of Users: **14** Number of Seats: **6** Seats Remaining: **-**

Note: Bulk Add Users and Add a User functionality is disabled until a Payment Method is entered. Enter Payment Info

Locations

Default	0.0.0.0/0

Adding Users

Adding users is a great place to start and it is very easy to do. Once added to the system users will be prompted to create an authenticator which they will use to access Service Providers.

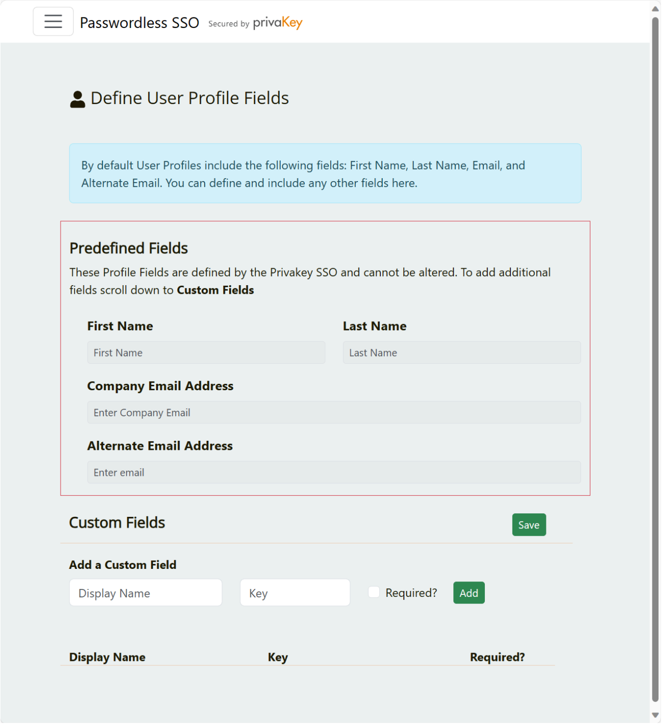
One can simply add users individually by clicking Add A User in the Users section of the main Admin screen. Alternatively, one can Bulk Add Users by uploading a csv file by clicking Bulk Add Users.

Configuring Profile Fields

By default, the following Fields are available for users:

Field	**Required?**
First Name	✅
Last name	✅
Company Email Address	✅
Alternate Email Address	

If additional fields are desired or required one can customize fields by configuring User Profile Settings. This may be required for certain Service Providers (for example, Microsoft 365 requires users have an Immutable ID set).



Passwordless SSO Secured by privaKey

Define User Profile Fields

By default User Profiles include the following fields: First Name, Last Name, Email, and Alternate Email. You can define and include any other fields here.

Predefined Fields

These Profile Fields are defined by the Privakey SSO and cannot be altered. To add additional fields scroll down to **Custom Fields**

First Name: First Name

Last Name: Last Name

Company Email Address: Enter Company Email

Alternate Email Address: Enter email

Custom Fields

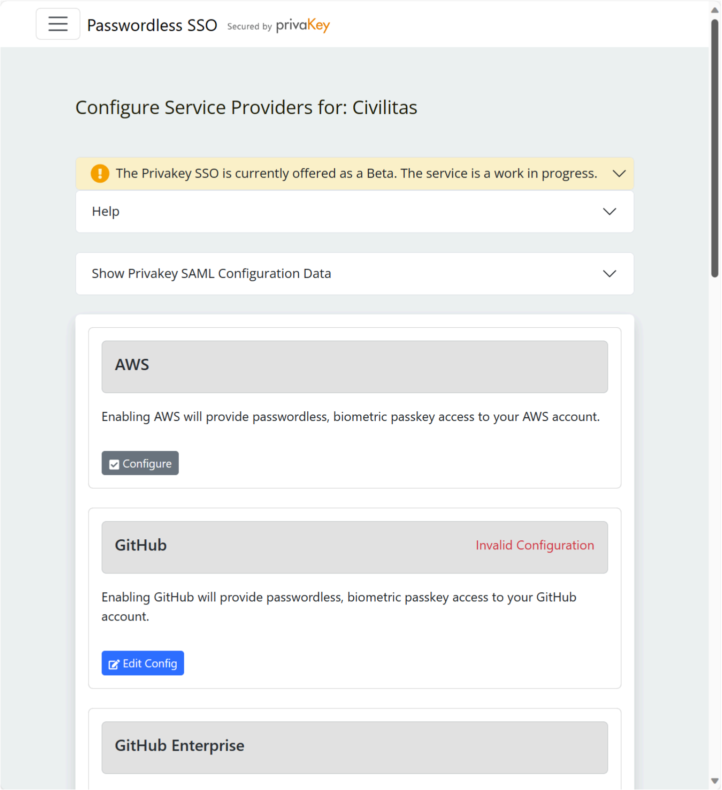
Add a Custom Field

Display Name | Key | □ Required?

Display Name	**Key**	**Required?**

Adding Service Providers

Next you should add a service provider. After familiarizing yourself with the SSO it is recommended one add a core email and productivity application such as Google Workspace of Microsoft 365 first. Detailed instructions are provided in Administration - Service Provider Configuration.



Passwordless SSO Secured by privaKey

Configure Service Providers for: Civilitas

The Privakey SSO is currently offered as a Beta. The service is a work in progress.

Help
Show Privakey SAML Configuration Data

AWS

Enabling AWS will provide passwordless, biometric passkey access to your AWS account.

GitHub Invalid Configuration

Enabling GitHub will provide passwordless, biometric passkey access to your GitHub account.

GitHub Enterprise

Note: While adding a service such as Google Workspace is a great place to jump-start ones passwordless journey, care should be taken when Privakey-enabling them. As Privakey Passwordless SSO currently uses Email to invite Users to the platform they will need to have access to their email to create a Privakey Authenticator. Google, Microsoft, and others facilitate this requirement by allowing you to create organizational units with different authentication rules. We provide detailed instructions in the help sections dedicated to configuring Google and Microsoft services for use with the Privakey SSO.

Adding Locations

Configuring locations is an optional but powerful feature.

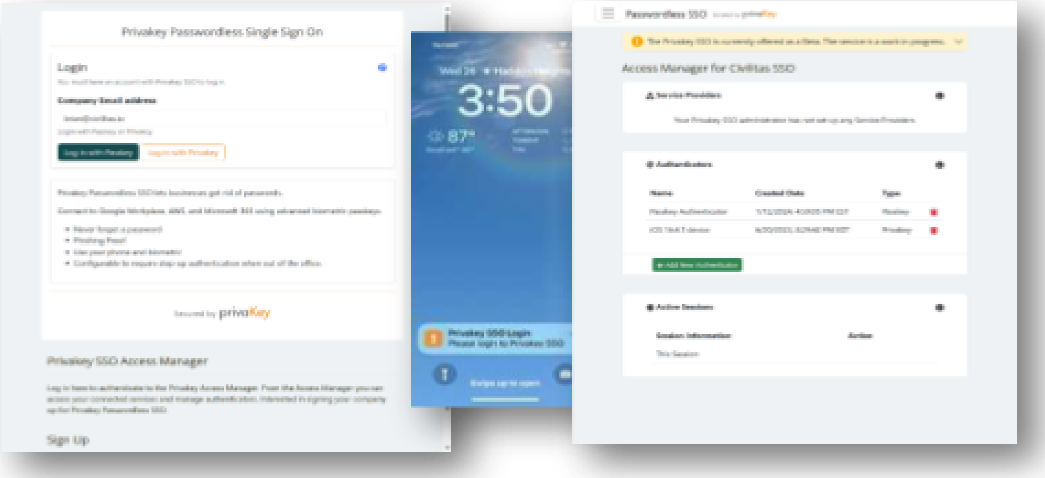
In a secure facility such as your office it may make sense to let users login once and access all of their online business accounts. But how do you want the SSO to behave when they're working remotely, or from a coffee shop? You may want them to re-authenticate to the Privakey Passwordless SSO when accessing sensitive accounts such as AWS even though they've already accessed Box.

Privakey's Location feature enables this capability. However, broad rules can be set for the entire SSO without ever configuring a location. It's up to you.

Using Privakey SSO

Administering Privakey is easy. Using Privakey to access services is even easier.

To log-in to all SSO-enabled services a user will simply enter their email and approve the authentication on the Privakey App or by using a native Passkey. Further, with that one authentication they will automatically be able to access any SSO-enabled service. That's it.



Privakey Passwordless Single Sign On

Login

You must have an account with Privakey SSO to log in.

Company Email address: brian@civitas.io

Login with Passkey or Privakey

Privakey Passwordless SSO lets businesses get rid of passwords.

Connect to Google Workplace, AWS, and Microsoft 365 using advanced biometric passkeys.

- Never forget a password
- Phishing Proof
- Use your phone and biometric
- Configurable to require step up authentication when out of the office.

Secured by privaKey

Privakey SSO Access Manager

Log in here to authenticate to the Privakey Access Manager. From the Access Manager you can access your connected services and manage authenticators. Interested in signing your company up for Privakey Passwordless SSO

The Privakey SSO is currently offered as a Beta. The service is a work in progress.

Access Manager for Civitas SSO

Service Providers

Your Privakey SSO administrator has not set up any Service Providers.

Authenticators

Name	Created Date	Type
Passkey Authenticator	1/11/2024, 4:03:05 PM EST	Passkey
iOS 16.6.1 device	6/20/2023, 6:29:40 PM EDT	Privakey

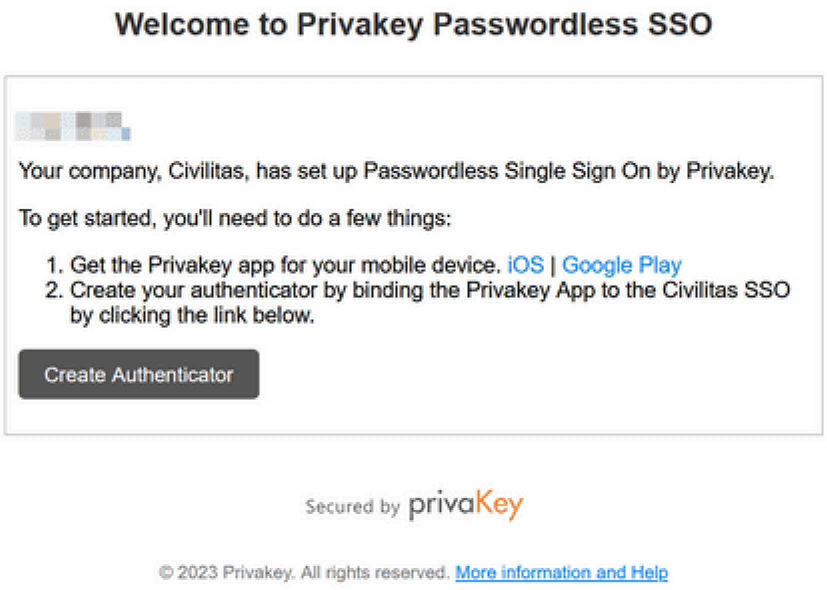
Active Sessions

Session Information	Action
This Session	

How do Users get Access to Privakey?

1. Get Invited by the Company's SSO Administrator

Users must be invited by a company administrator to begin using the Privakey SSO. After an Admin adds the user, they will receive an email with instructions on creating and authenticator and accessing the SSO.



Welcome to Privakey Passwordless SSO

[redacted]

Your company, Civilitas, has set up Passwordless Single Sign On by Privakey.

To get started, you'll need to do a few things:

1. Get the Privakey app for your mobile device. iOS | Google Play
2. Create your authenticator by binding the Privakey App to the Civilitas SSO by clicking the link below.

Secured by privaKey

© 2023 Privakey. All rights reserved. More information and Help

Users can set up the Privakey App or a Passkey (when available) as an authenticator. If possible, users should set up both.

2. Creating an Authenticator

Once invited, users will click on Create Authenticator to get started in their Passwordless journey. Users will have the option to use the Privakey App or device-native Passkeys. Each has merits and it is recommended users set both up. To understand the relative benefits see Technical Architecture – Privakey CX Components - Authenticators above.

The Privakey App

The Privakey App is an authenticator application made for mobile devices. Available on iOS and Android the Privakey App allows you to access the Privakey SSO and your companies resources without using passwords.

Get the App

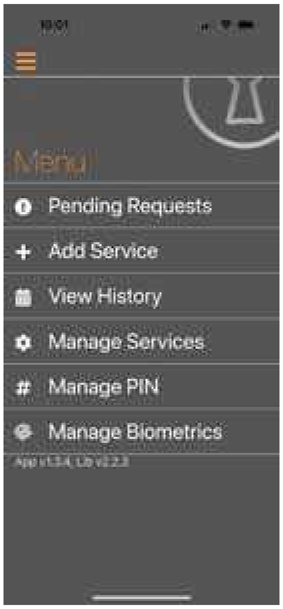
Use your mobile device to search for Privakey in the app store or click the links below.

Android: Link (https://play.google.com/store/apps/details?id=com.privakey.authwallet)

iOS: Link (https://apps.apple.com/us/app/privakey/id1552057206)

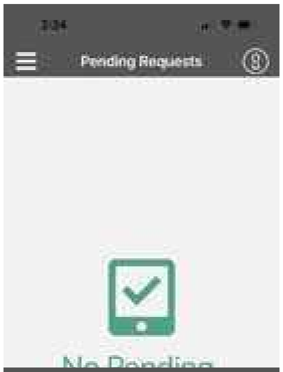
Tour the App

Most of the time you will access the app in response to a notification. The notification resulted from a log-in attempt that you initiated. However, Privakey also proved other capabilities that allow you to manage your authenticator are making there are a host of capabilities provided that allow you to manage your authenticator.



Main Menu:

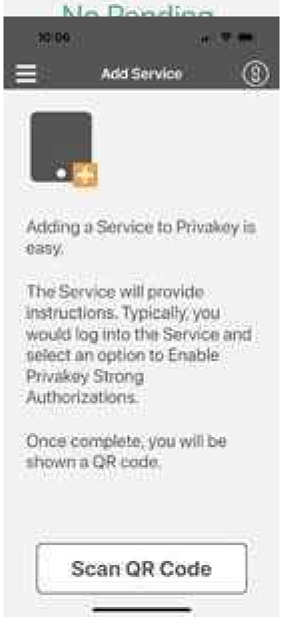
Clicking on the menu displays the different actions you can take. Each action is explained below.



Pending Requests

This accesses the list of any outstanding authentication or authorization requests you have been sent. It is also the default view you will see when launching the app.

Don't worry if you see No Requests Pending. You'll typically access requests directly from the notification, then act on them leaving nothing pending.



Adding a Service to Privakey is easy.

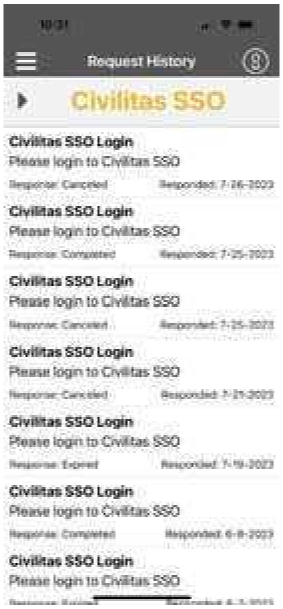
The Service will provide instructions. Typically, you would log into the Service and select an option to Enable Privakey Strong Authorizations.

Once complete, you will be shown a QR code.

Add Service

This is where you connected your SSO service to your Privakey App.

Your administrator will send you an email from the system. Look for an email from noreply@privakey.com. The email will have instructions on how to proceed. Basically - click the Create Authenticator Link in the email, open the Privakey App, select Add a New Service and follow the prompts.



10:31

Request History

Civilitas SSO

Civilitas SSO Login
Please login to Civilitas SSO
Response: Canceled Responded: 7-26-2023

Civilitas SSO Login
Please login to Civilitas SSO
Response: Completed Responded: 7-25-2023

Civilitas SSO Login
Please login to Civilitas SSO
Response: Canceled Responded: 7-25-2023

Civilitas SSO Login
Please login to Civilitas SSO
Response: Canceled Responded: 7-21-2023

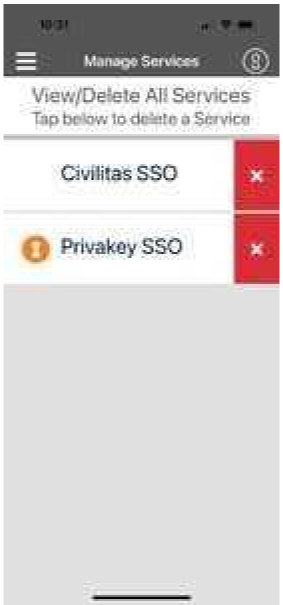
Civilitas SSO Login
Please login to Civilitas SSO
Response: Expired Responded: 7-19-2023

Civilitas SSO Login
Please login to Civilitas SSO
Response: Completed Responded: 6-8-2023

Civilitas SSO Login
Please login to Civilitas SSO

View History

The History page provides you with a log of all of your authorizations. You can review your authentication and authorization history here.



10:31

Manage Services

View/Delete All Services
Tap below to delete a Service

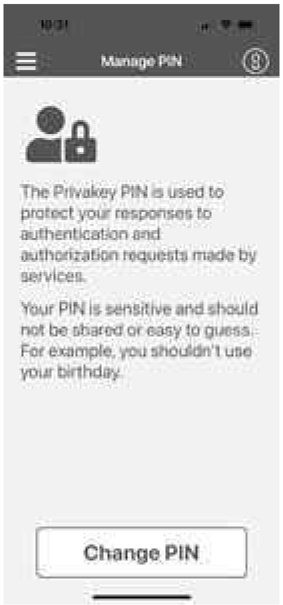
Civilitas SSO ×

Privakey SSO ×

Manage Services

The Privakey App can connect to services other than your Company's SSO. This is where you can review the services that have been connected to this App. If need be, you can remove a service from the App.

Removing a service from the app will preclude you from interacting with that service.



Manage PIN

The Privakey PIN is used to protect your responses to authentication and authorization requests made by services.

Your PIN is sensitive and should not be shared or easy to guess. For example, you shouldn't use your birthday.

Change PIN

Manage PIN

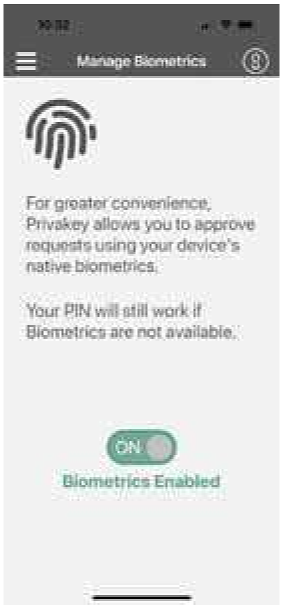
PINs are used in the application as an alternative to Biometrics. Entering a PIN is required when you connect your first service. The PIN, just like the biometric, is used to securely store (and access) private keys used to verify the integrity of your authentications.

Your PIN can be a fall-back for when Biometrics fail or it can be the primary means of authentication if you do not want to use a Biometric. PINS are not stored on the Privakey Server and are only used to access the secure storage on your device.

DO NOT SHARE YOUR PIN WITH ANYONE - IF THEY HAVE ACCESS TO YOUR UNLOCKED PHONE THE PIN WILL GIVE THEM ACCESS TO ALL OF YOUR COMPANY CLOUD ACCOUNTS CONNECTED TO PRIVAKEY'S SSO.

The Privakey PIN does not have to be the same as your device PIN. But, it can be! The Privakey service does not have access to either PIN.

Privakey App - Manage Biometric



Manage Biometrics

For greater convenience, Privakey allows you to approve requests using your device's native biometrics.

Your PIN will still work if Biometrics are not available.

ON

Biometrics Enabled

Privakey uses device biometrics to securely store (and access) private keys used to verify the integrity of your authentications. On this screen you can enable / disable biometrics. You may, for example, want to disable Biometrics and leverage only your PIN if the biometric sensor on your device is unreliable.

Passkeys

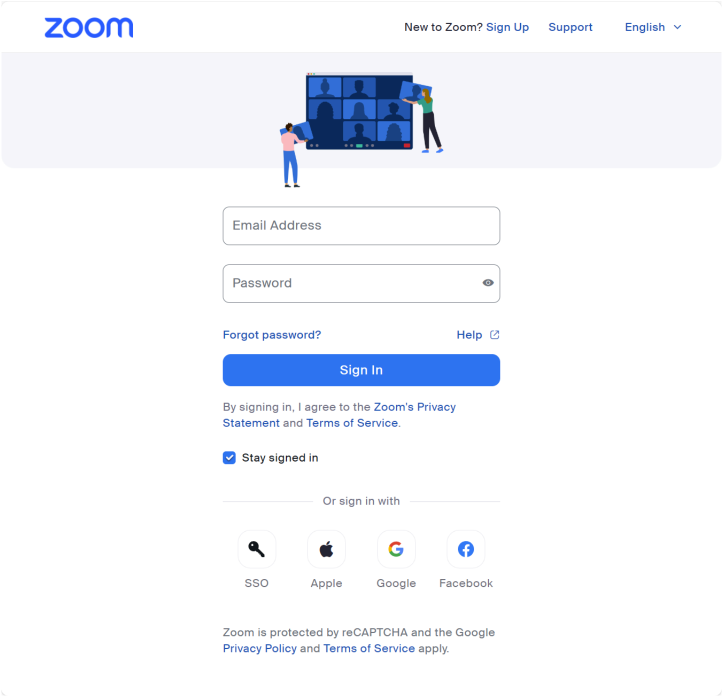
Similar to the Privakey App, Passkeys work by using assymetric key cryptography to authenticate users. Unlike passwords, which are secrets shared and stored both by the user and the service provider, passkeys rely on a pair of cryptographic keys: a private key and a public key. The private key is securely stored on the user's device and never shared, while the public key is stored on the server. During authentication, the user's device proves it has the private key without transmitting it, significantly reducing the risk of phishing or server breaches compromising user credentials.

However, Passkeys are dependent on Computer Hardware, Operating Systems and Browser support. And they can be a bit complicated to set up. If your system supports passkeys they are a great way to access the Privakey SSO.

3. Accessing Services.

Once a user has an Authenticator and an Administrator has configured a service (such as Google), logging in becomes easy. A user will simply go to the SSO or directly to the service and enter their company email address. They will approve the authentication, without a password, using the Privakey App or a Passkey and immediately be granted access.

Note: Some services will have an alternate path for accessing an SSO-enabled service. See the Zoom example below and note they have a link to SSO below the form. For Zoom one will need to click that link to initiate login.



By signing in, I agree to the Zoom's Privacy Statement and Terms of Service.

Zoom is protected by reCAPTCHA and the Google Privacy Policy and Terms of Service apply.

Conclusion

Using Privakey SSO transforms the way users interact with digital services. It offers a secure, efficient, and user-friendly solution for accessing a wide range of applications, significantly enhancing the overall digital experience.

Easy to set up, easy to administer and even easier to use Privakey Passwordless SSO is a perfect way to reduce an organizations to password-based attack vectors while improving the day-to-day life of users.

Appendix: Access Countless Services via Google

Get passwordless access to countless services by just enabling Google.

If you use Google Workspace for Email and Productivity tools it is great place to start your Privakey SSO journey. **Sign in with Google** is supported by many, many services. Once you enable Privakey Passwordless SSO for those services you immediately inherit a passwordless login to those downstream services.

Brands Supported by Google Workspace IdP

The following is a list of notable brands and cloud applications that are pre-integrated with Google Workspace IdP for SSO, along with brief descriptions:

15Five	A performance management software that helps employees grow and develop in their roles.
4me	IT service management application focusing on service level agreement (SLA) management.
7Geese	A performance management tool that facilitates goal setting and feedback.
Accellion	Secure file sharing and collaboration platform.
Adaptive Insights	Business planning software for budgeting, forecasting, and reporting.
Adobe Sign	E-signature solution for fast, secure electronic signatures.
Aha!	Roadmapping software for setting strategy and planning products.
Amazon Web Services	Comprehensive cloud computing platform offering a variety of services.
Andfrankly	Employee engagement and feedback tool.
AppDynamics	Application performance management and IT operations analytics.
Apteligent	Mobile app performance insights and diagnostic tools.
Artifactory	Universal repository manager supporting all major packaging formats.
Asana	Project and task management tool for teams.
Atlassian Cloud	Suite of cloud-based collaboration and productivity tools, including Jira and Confluence.
Automox	Cloud-based patch management and endpoint protection.

AutoTask Workplace	File sync and share solution tailored for businesses.
BambooHR	Human resources management system for small and medium-sized businesses.
BetterWorks	Continuous performance management software.
Bime	Business intelligence and data visualization tool.
Black Duck by Synopsys	Software composition analysis for open source security and license compliance.
BlueJeans	Video conferencing service that facilitates virtual meetings.
Bonusly	Employee recognition and rewards platform.
Boomi	Integration platform as a service (iPaaS) for connecting cloud and on-premises applications.
Box	Cloud content management and file sharing service for businesses.
Brightcove	Video hosting and publishing platform.
Bugcrowd	Crowdsourced security and vulnerability disclosure platform.
Bugsnag	Error monitoring and reporting for application stability.
Buildkite	Continuous integration and delivery platform.
Canva	Graphic design platform for creating social media graphics, presentations, posters, and other visual content.
Canvas LMS	Learning management system for educational institutions and businesses.
Carbonite	Online backup service for personal and business data.
Chartio	Cloud-based data exploration, visualization, and reporting tool.
Cigna	Health services and insurance company.
Cisco Umbrella	Cloud security platform providing the first line of defense against threats on the internet.
Clarizen	Enterprise collaborative work management solution.
Clear Review	Performance management software focusing on continuous feedback.
ClearSlide	Sales engagement platform for presenting and tracking content.
Cloudbees	Enterprise Jenkins and DevOps solutions.
CloudHealth	Cloud management platform for optimizing and governing cloud costs.

Clubhouse	Project management platform for software development.
Comeet	Collaborative recruiting platform.
ComponentSpace	SAML components for ASP.NET and .NET applications.
Concur	Travel, expense, and invoice management software.
Coralogix	Log analytics and cloud monitoring solution.
Coupa	Business spend management (BSM) platform.
CrashPlan	Data backup and recovery solution for businesses.
CyberArk	Security solutions for privileged account management.
Dashlane	Password management and digital wallet application.
Datadog	Monitoring and analytics platform for cloud-scale applications.
Desk	Customer service application from Salesforce.
Deskpro	Helpdesk software for customer support.
Dialpad	Cloud-based business phone system.
Dialpad Sandbox	Testing environment for Dialpad.
Digicert	SSL certificate and digital certificate management.
Docebo	Learning management system (LMS) for online training.
DocuSign	Electronic signature technology and digital transaction management.
Domo	Business intelligence tools and data visualization.
Drift	Conversational marketing and sales platform.
Dropbox	File hosting service offering cloud storage, file synchronization, personal cloud, and client software.
Duo	Security solutions for multi-factor authentication and secure access.
Egencia	Business travel management for modern businesses.
Egnyte	Enterprise file synchronization and sharing.
Elastica	Cloud access security broker (CASB) solutions.
Emburse	Expense management and AP automation.
Engagedly	Performance management software with employee engagement.
Envoy	Workplace platform to manage visitors and deliveries.

Evernote Business	Note-taking, organizing, and archiving.
Expensify	Expense management software for personal and business use.
Federated Directory	Cloud-based directory for managing business contacts.
Firstbird	Employee referral program.
Foodee	Corporate meal delivery