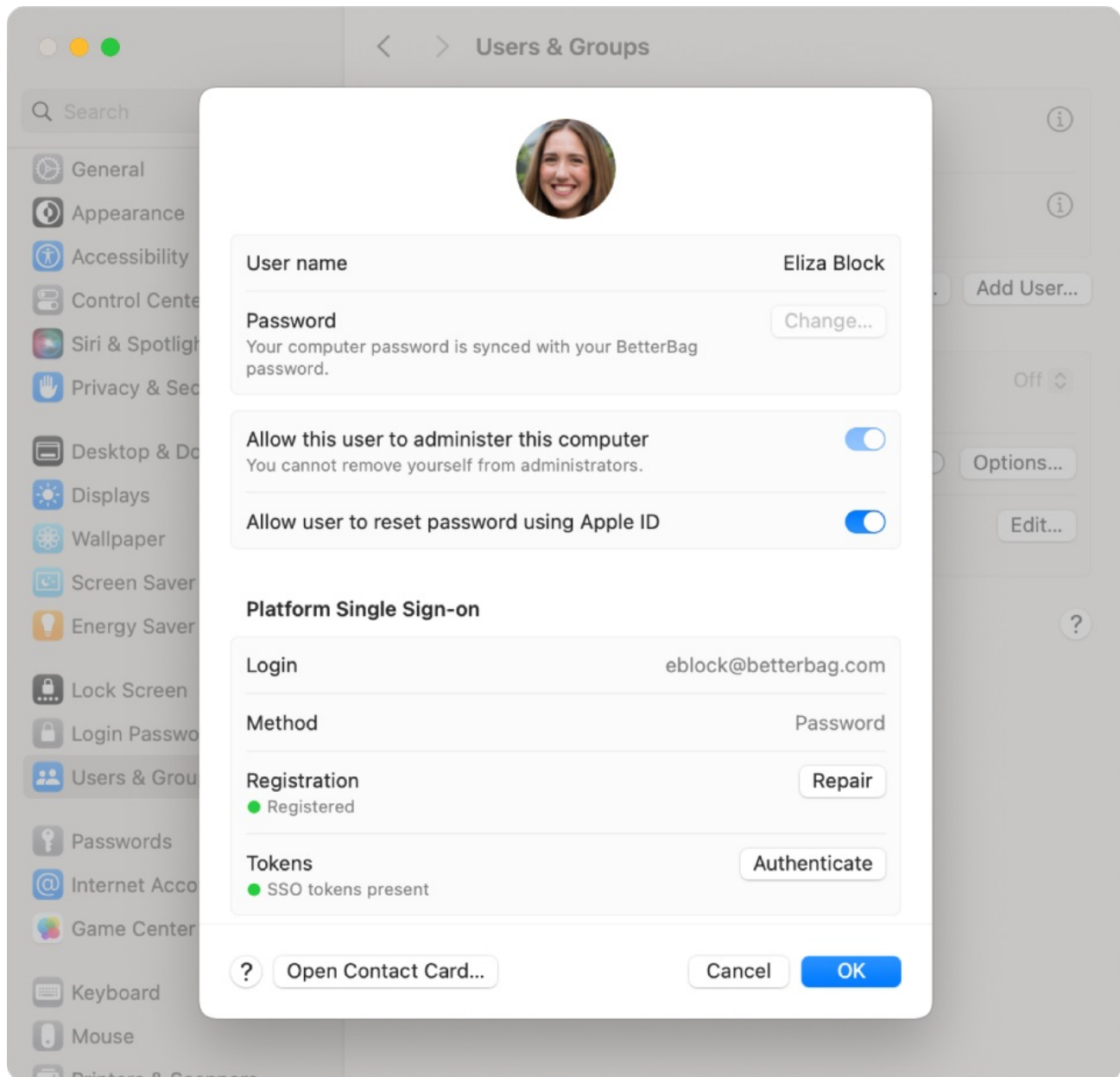


Microsoft Enterprise Platform Single Sign-on for macOS

What

With Platform Single Sign-on (Platform SSO), we can utilize SSO extensions that extend to the macOS login window, allowing users to synchronize local account credentials with an identity provider (IdP). In this case, we are combining what is provided here: [Microsoft Enterprise SSO | FileWave KB](#) with [Platform Single Sign-on for macOS - Apple Support](#). The local account password is automatically kept in sync after this configuration, so the cloud password and local passwords will match. Users will also still be able to unlock their Mac with Touch ID and Apple Watch. The end result will allow the user to login with their Entra ID and password or their local account username with their synced Entra ID's password.



When/Why

An Administrator who is managing a fleet of MacBooks may want to use this for another level of security or for taking advantage of the full integration that macOS now offers with SSO. You are offered the same benefits as listed in: [Microsoft Enterprise SSO | FileWave KB](#) except with the added layer of further syncing the local account with your identity provider account.

How

Below are the following requirements and configuration creation steps for deployment.

Platform SSO Requirements:

- macOS 13 or later
- A mobile device management (MDM) solution that supports the Extensible Single Sign-on payload which includes support for Platform SSO (enrolled in FileWave via DEP or User approved enrollment in our case)
- Support from the IdP for the Platform SSO authentication protocol
- One of two supported authentication methods:
 - Authentication with a Secure Enclave-backed key: With this method, a user who logs in to their Mac can use a Secure Enclave-backed key to authenticate with the IdP without a password. The Secure Enclave key is set up with the IdP during the user registration process
 - Password authentication: With this method, a user authenticates with a local password or an IdP password

Note: If the Mac is unenrolled from the MDM solution, it's also unregistered from the IdP.

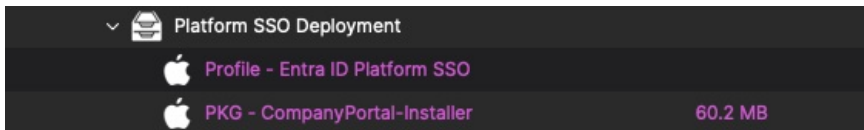
WS-Trust federation

WS-Trust federation is supported in macOS 13.3 or later. This allows Platform SSO to successfully authenticate users when their account is managed by an IdP federated with Microsoft Entra ID.

Deployment:

Here is an example Profile Fileset ready to deploy in your environment with the default configuration:

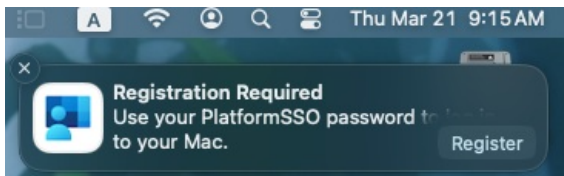
- [Profile - Entra ID Platform SSO.fileset.zip](#)
- The Microsoft Company Portal app must be installed on the device. It can be installed manually by users or deployed over FileWave. You can download the Company Portal app here: [Company Portal app](#)

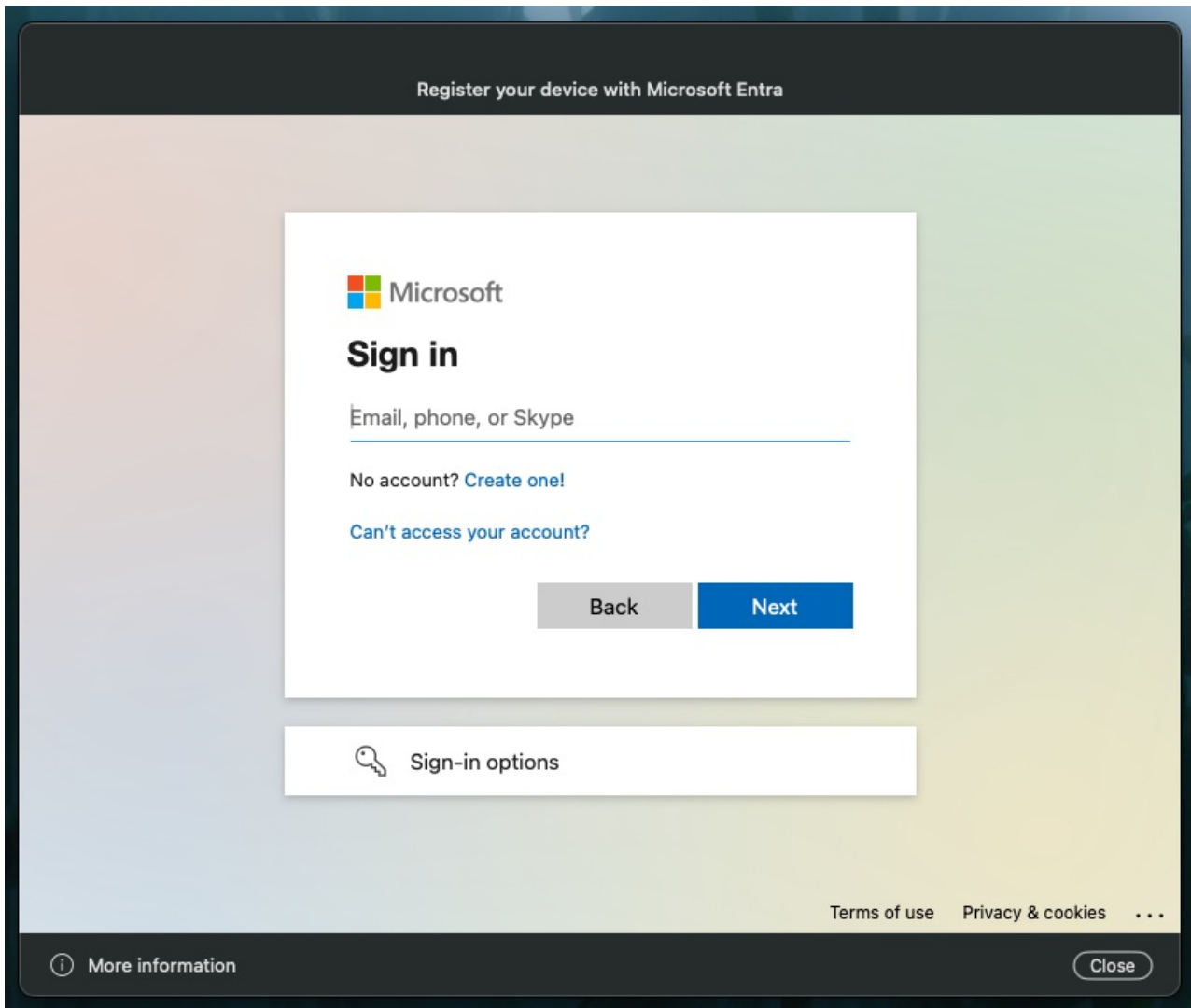
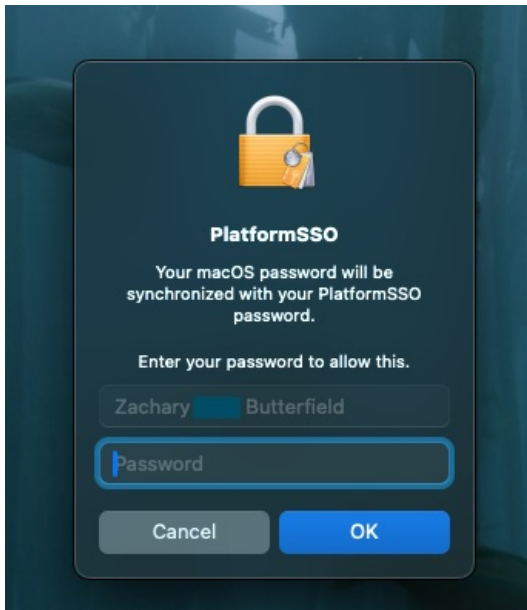


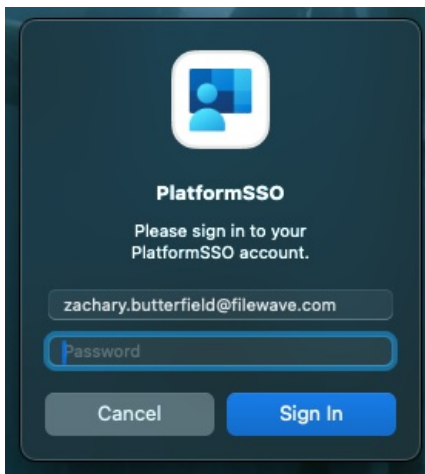
Please Note: On macOS devices, Apple requires the Company Portal app be installed. Users don't need to use or configure the Company Portal app, it just needs to be installed on the device.

End-user Interaction required:

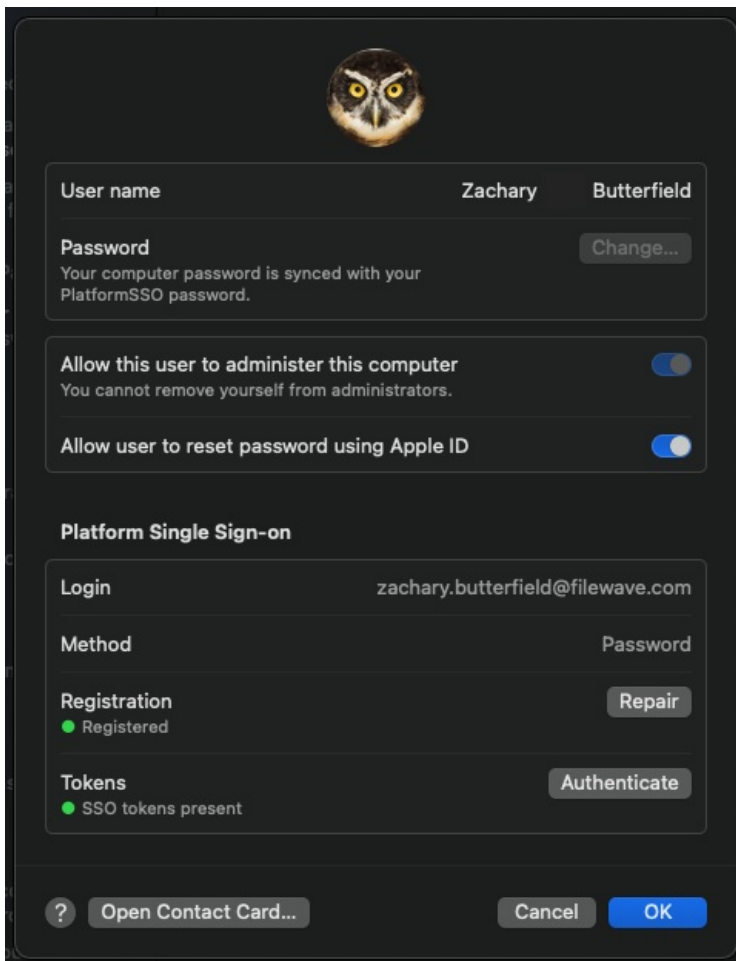
After successful deployment, in the notifications area of the user's device, they should be presented with a message:







After signing in and registering, when you go to System Settings > Users & Groups > click the 'i' next to your Username, you should be able to confirm everything went successfully with the new settings here:



Notes and Observations

- If two-factor authentication is enabled in your environment, whenever your end user opens a Microsoft Application, they will be presented with an 'Approve sign in request' as frequently as what is configured in your Domain's security settings.

Related Content

- [Microsoft Enterprise SSO plug-in for Apple devices KB](#)
- [Apple documentation SSO for macOS](#)

🔄Revision #8

★Created 20 March 2024 16:16:01 by Zachary Butterfield

✍Updated 4 November 2024 13:54:09 by Josh Levitsky