

Microsoft Enterprise SSO plug-in for Apple devices

What

The Microsoft Single Sign-On (SSO) plug-in for Apple devices is a software extension that allows users to log in to Microsoft services on their Apple devices without needing to enter their credentials each time. This plug-in enables users to authenticate once and use Microsoft services seamlessly across multiple applications and services. For more information, you may visit, [Microsoft Enterprise SSO plug-in for Apple devices](#).

When/Why

Using the Microsoft SSO plug-in for Apple devices offers several advantages. First, it saves time by eliminating the need to enter login credentials each time a user needs to access Microsoft services. This can be particularly useful for users using Microsoft services on their Apple devices.

Second, the Microsoft SSO plug-in provides an added layer of security. Users can use multi-factor authentication (MFA) to secure their login credentials and protect their data from unauthorized access. The plug-in provides a more secure way to access Microsoft services on Apple devices than standard login credentials.

Finally, the Microsoft SSO plug-in offers a more streamlined and user-friendly experience. Users can easily switch between different Microsoft services without needing to log in again and quickly access their files and data on any device.

How

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

Requirements:

- The device must support and have an installed app that has the Microsoft Enterprise SSO plug-in for Apple devices:
 - iOS 13.0 and later: [Microsoft Authenticator app](#)
 - iPadOS 13.0 and later: [Microsoft Authenticator app](#)
 - macOS 10.15 and later: [Intune Company Portal app](#)
- The device must be enrolled in MDM, i.e. DEP enrolled.
- Configuration must be pushed to the device to enable the Enterprise SSO plug-in. Apple requires this security constraint.

✓ 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. You may download here: [Download the Company Portal app installer package](#).

Microsoft Authenticator app deployment:

You may acquire and deploy the Microsoft Authenticator app via your ASM/ABM account. A similar method as any VPP application, search the ASM/ABM, enter in the number of licenses for the VPP application, and click on GET.

Microsoft Authenticator
Microsoft Corporation · iOS App
★★★★★ \$0.00

Authenticator+ App
Rocket Apps GmbH · iOS App
★★★★★ \$0.00

Authenticator App
2Stable · iOS and macOS
★★★★★ \$0.00

Authenticator App™
Codenhagen.IO ApS · iOS App
★★★★☆ \$0.00

Authenticator App, 2FA
CHAMOMILE PTE. LTD. · iOS App
★★★★★ \$0.00

QR, Barcode Scanner for iPhone
Kun Wang · iOS App
★★★★★ \$0.00

Microsoft Authenticator
Microsoft Corporation · iOS App
✓ Device Assignable
[View Details ↗](#)

Buy Licenses

Assign to

Choose a Location

Price	Quantity	Payment Method
\$0.00	0	None

Total Cost **\$0.00**
[Get](#)

Creating the Configuration profile to be deployed to your devices:

- Open FileWave Central
- Select Filesets from the left side menu
- Select New Desktop Fileset
- Click on Profile
- Enter in the name of the Profile, example: Microsoft Single-Sign On
- Select the Single Sign-On Extensions payload
- Enter in the following for specified payload:
 - iOS settings:
 - Extension ID: `com.microsoft.azureauthenticator.ssoextension`
 - Team ID: This field isn't needed for iOS but you can use `UBF8T346G9`
 - macOS settings:
 - Extension ID: `com.microsoft.CompanyPortalMac.ssoextension`
 - Team ID: `UBF8T346G9`
 - Sign-On Type:
 - Type: Redirect
 - URL identity providers:
 - `https://login.microsoftonline.com`
 - `https://login.microsoft.com`
 - `https://sts.windows.net`
 - `https://login.partner.microsoftonline.cn`
 - `https://login.chinacloudapi.cn`
 - `https://login.microsoftonline.us`
 - `https://login-us.microsoftonline.com`
 - Optional Custom Configurations (Not required):
 - Enable SSO for all apps with specific bundle IDs or prefix IDs: Key:AppPreFixAllowList - Type:String - Value:com.microsoft., com.apple., or com.business.travelapp
 - Sign in with browser that don't use MSAL and Safari: Key:browser_sso_interaction_enabled - Type:Number - Value:1
 - Disable OAuth 2 app prompts: Key:disable_explicit_app_prompt - Type:Number - Value:1

Profile Editor

Search

☒ show only configured

macOS, iOS and tvOS

General
Mandatory

iOS 13.0+ and macOS 10.15+

Single Sign-On Extensions
1 payload(s) configured.

Not set

Registration Token
The token this device uses for registration with Platform SSO
[optional]

Extension Identifier
Bundle identifier of the app extension that performs the single sign-on
com.microsoft.azureauthenticator.ssoextension

Team Identifier
Team identifier of the app extension that performs the single sign-on
UBF8T346G9

Sign-on Type
☐ Credential
☒ Redirect

URLs
URL prefixes of identity providers on whose behalf the app extension performs single sign-on

https://login.microsoftonline.com
https://login.microsoft.com
https://sts.windows.net
https://login.partner.microsoftonline.cn
https://login.chinacloudapi.cn
https://login.microsoftonline.us
https://login-us.microsoftonline.com

Custom Configuration
Custom configuration for the app extension

Key	Type	Value
AppPrefixAllowList	String	com.microsoft,c...
browser_sso_interaction_enabled	Number	1
disable_explicit_app_prompt	Number	1

Please check [Apple's Configuration Profile reference](#) for OS compatibility.

Cancel Settings Load Profile Save

Deployment

Next deploy the Microsoft Authenticator app and Configuration profile on a few devices. If you're not deploying the Microsoft Authenticator app using an app policy, then users must install it manually. Users don't need to use the Authenticator app, it just needs to be installed on the device.

▼  **Microsoft Single Sign-On**

 **iOS App - Microsoft Authenticator**

 **Profile - Microsoft Single Sign-On**

Users sign in to any supported app or website to bootstrap the extension.

Bootstrap is the process of signing in for the first time, which sets up the extension. After users sign in successfully, the extension is automatically used to sign in to any other supported app or website.

Meaning the end users will need to sign into their Microsoft account for their first time manually for the extension to authenticate successfully.

You can test single sign-on by opening Safari in private mode (opens Apple's web site) and opening the <https://portal.office.com> site. If configured successfully, no username and password will be required.

Related Content

- [Microsoft SSO for macOS devices](#)

🕒Revision #5
★Created 14 July 2023 13:47:18 by Josh Levitsky
✎Updated 21 March 2024 18:18:29 by Andrew Kloosterhuis