API Collection

Platform single sign-on (SSO)

Use credentials from macOS login to perform single sign-on with an identity provider.

Overview

Platform single sign-on (SSO) is a replacement for binding to directory services. It builds on enterprise SSO capabilities so SSO extensions can also perform single sign-on for apps and websites. It integrates with macOS and doesn't use JavaScript or render webpages for authentication.

The system stores the SSO tokens in the keychain and only shares them with the SSO extension. The SSO extension then uses the SSO tokens to authenticate the user to their on-premises apps and on websites as needed. If the SSO tokens are missing, expired, or more than four hours old, platform SSO attempts to refresh or retrieve new tokens from the IdP.

Platform SSO supports the following authentication methods with an identity provider (IdP):

Password and encrypted password
: The IdP uses the local account password and keeps it in sync, including password updates from the login window and screensaver unlock.

Password with WS-Trust
: A federated IdP, meaning an IdP that facilitates federated authentication across multiple security domains, can use the local account password for authentication.

User secure enclave key
: A secure enclave-backed key can authenticate with the IdP without a password and without changing the local account password.

SmartCard
: High-security customers can use a SmartCard to authenticate with the IdP.

Platform SSO can create new local user accounts on demand at the login window using IdP credentials, and also integrate IdP group membership with macOS. You can use network accounts for authorization, and groups can also authorize network accounts.

Use Device Management to securely configure platform SSO, including device and user registration, configuring groups, and managing account permissions.

The system can also retrieve Kerberos ticket-granting tickets (TGTs), import them to a credential cache, and optionally share them with the Kerberos SSO extension.

Topics

Essentials

- Creating extensions that support platform SSO

  Configure capabilities and authentication options for extensions.

- Registering devices and users

  Implement device and user registration.

`protocol` `ASAuthorizationProviderExtensionRegistrationHandler`

An interface through which a single sign-on (SSO) authentication provider extension registers users and devices for platform SSO.

`enum` `ASAuthorizationProviderExtensionAuthenticationMethod`

The platform single sign-on method for the user.

`struct` `ASAuthorizationProviderExtensionRequestOptions`

The options for the extension to obtain the status of the registration.

`enum` `ASAuthorizationProviderExtensionRegistrationResult`

The registration result.

Configuration

- Configuring Device Management

  Configure Device Management to support device and user registration for platform SSO.

- Configuring authentication with the identity provider (IdP)

  Specify how platform SSO authenticates with the identity provider.

`class` `ASAuthorizationProviderExtensionLoginConfiguration`

An interface for configuring platform single sign-on.

`class` `ASAuthorizationProviderExtensionLoginManager`

An interface to maintain platform single sign-on (SSO) during authentication and registration.

Authentication

Authentication process

Use a system-supported method to authenticate with an identity provider.

`class` `ASAuthorizationProviderExtensionKerberosMapping`

A set of Kerberos mappings that the system login process uses.

See Also

Single sign-on (SSO)

Enterprise single sign-on (SSO)