



Single sign-on Authentication and Identity Integration

Migration and Implementation Services

Single sign-on (SSO) is a user authentication process that enables users to securely access multiple applications and services using just one set of credentials. With single sign-on, users sign in once with one account to access company resources, software as a service (SaaS) applications, and web applications. Administrators can centralize user account management, and automatically add or remove user access to applications based on group membership. Without single sign-on, users must remember application-specific passwords and sign in to each application. IT staff needs to create and update user accounts for each application such as Microsoft 365, Box, Slack and Salesforce. Users need to remember their passwords, plus spend the time to sign in to each application. The benefits of onboarding becomes the simple and secure method to off-board users.

Apple announced End Of Life support for Enterprise Connect with the release of macOS Monterey back in October, 2021. Apple will no longer provide any updates to Enterprise Connect going forward and Apple recommends using the Kerberos Single Sign-on Extension, which is free of charge, and supported on macOS Catalina and later.

The Kerberos Single Sign-on (SSO) extension makes it easy to use Kerberos-based single sign-on with your organization's Apple devices. The Kerberos SSO extension should be used with an on-premise Active Directory domain. Azure Active Directory isn't supported. To use the Kerberos SSO extension, devices don't need to be joined to an Active Directory domain. Additionally, users don't need to log in to their Mac computers with Active Directory or mobile accounts; instead, Apple recommends using local accounts.

HCS offers two services for Single sign-on Authentication and Identity Integration:

- Migration from Apple Enterprise Connect to a Kerberos Single Sign-on Extension workflow.
- Implementation of a Kerberos Single Sign-on Extension workflow.

HCS can perform a documented audit of your current Enterprise Connect workflow and provide a Kerberos Single Sign-on Extension workflow to meet those needs. A Kerberos Single Sign-on Extension workflow will provide a modern and supportable solution for Single Sign-on in your environment.

The Kerberos Single Sign-on Extension provides similar features to Enterprise Connect such as:

- Mounting of Network Shares
- Password Syncing with the local macOS user account
- Live Password Testing with complex Active Directory Password Policies
- External Password Change Website URL
- Run scripts based on a successful password change
- Run scripts based on a successful network connection
- Run scripts based on a failed network connection

Benefits of using the Kerberos Single Sign-on Extension:

- Provided by Apple at no additional cost
- Supported on macOS Catalina and later
- Supported on iOS / iPadOS 13 and later
- Deployed via an MDM solution for easier management
- Enforced settings using configuration profiles
- Smart Card Support

On premises Microsoft Active Directory Kerberos SSO Features:

- Securely access multiple applications and services using just one set of credentials
- Leveraging Kerberos extensions
- Apps that support Kerberos authentication
- Sync local user passwords with AD
- Access to native apps