Extensión de inicio de sesión único de Kerberos

Manual del usuario

Diciembre de 2019

Contenido

Introducción

Con la extensión de inicio de sesión único (SSO) de Kerberos es más fácil usar el inicio de sesión único basado en Kerberos con los dispositivos Apple de tu organización.

Autenticación Kerberos más sencilla

La extensión de SSO de Kerberos simplifica la adquisición de un ticket de otorgamiento de tickets (TGT) de Kerberos desde el dominio de Active Directory de tu organización, y esto permite que los usuarios se autentiquen sin problemas en recursos como sitios web, apps y servidores de archivos. En macOS, la extensión de SSO de Kerberos adquiere de forma proactiva un TGT de Kerberos cuando cambia el estado de la red para asegurarse de que el usuario pueda autenticarse cuando quiera.

Gestión de cuentas de Active Directory

La extensión de SSO de Kerberos también ayuda a tus usuarios a gestionar sus cuentas de Active Directory. En macOS, permite que los usuarios cambien sus contraseñas de Active Directory y les enviará una notificación cuando estén a punto de caducar. Además, los usuarios pueden modificar las contraseñas de sus cuentas locales para utilizar las mismas que tienen en Active Directory.

Compatibilidad con Active Directory

La extensión de SSO de Kerberos se debe utilizar con un dominio local de Active Directory. No se admite el uso de Azure Active Directory. No es necesario que los dispositivos estén vinculados a un dominio de Active Directory para poder usar la extensión de SSO de Kerberos. Además, los usuarios no tienen que iniciar sesión en sus ordenadores Mac con Active Directory o cuentas móviles; Apple recomienda usar cuentas locales.

Requisitos

- iOS 13, iPadOS o macOS Catalina.
- Un dominio de Active Directory con Windows Server 2008 o posterior. La extensión de SSO de Kerberos no está destinada a utilizarse con Azure Active Directory. Requiere un dominio local de Active Directory típico.
- Acceso mediante wifi, Ethernet o VPN a la red en la que se aloja el dominio de Active Directory.
- Los dispositivos se deben gestionar con una solución de gestión de dispositivos móviles (Mobile Device Management, MDM) que admita la carga útil de perfil de configuración Extensible Single Sign-On (SSO). Ponte en contacto con tu proveedor de MDM para consultarle si admite esta carga útil de perfil de configuración.

Enterprise Connect

La finalidad de la extensión de SSO de Kerberos es sustituir a Enterprise Connect. Si usas Enterprise Connect y quieres pasarte a la extensión de SSO de Kerberos, consulta más información en el apartado «Transición desde Enterprise Connect» de este documento.

Primeros pasos

Creación e implantación de un perfil de configuración

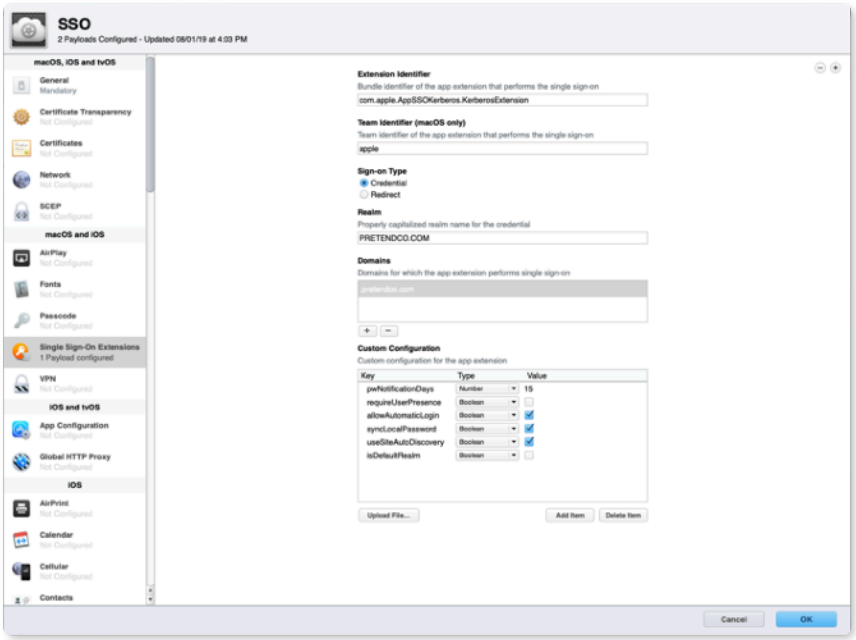
Para usar la extensión de SSO de Kerberos, debes configurarla con un perfil de configuración proporcionado al dispositivo desde una solución de MDM.

Nota: El perfil de configuración debe proporcionarse al dispositivo mediante MDM. En macOS, debe ser una inscripción en MDM aprobada por el usuario e instalada en el ámbito del sistema. No se puede añadir manualmente el perfil.

Para configurar la extensión con un perfil de configuración, deberás utilizar la carga útil Extensible Single Sign-On que se introdujo en iOS 13, iPadOS y macOS 10.15. El Gestor de Perfiles —incluido en macOS Server— admite la carga útil Extensible Single Sign-On. Si tu solución de MDM no admite esta carga útil de momento, puedes crear el perfil que necesites en el Gestor de Perfiles e importarlo después a tu solución de MDM para distribuirlo. Ponte en contacto con tu proveedor de MDM para obtener más información.

Sigue estos pasos para crear un perfil de configuración con el Gestor de Perfiles:

1. Inicia sesión en el Gestor de Perfiles.
2. Crea un perfil para un grupo de dispositivos o un dispositivo determinado.
3. Selecciona Single Sign-On Extensions en la lista Payload. A continuación, haz clic en el botón Add (+) para añadir una carga útil nueva.
4. En el campo Extension Identifier, introduce «com.apple.AppSSOKerberos.KerberosExtension».
5. En el campo Team Identifier, introduce «apple».



6. Selecciona Credential en Sign-on Type.
7. En el campo Realm, escribe en mayúsculas el nombre del dominio de Active Directory en el que residen tus cuentas de usuario. Usa el nombre de tu bosque de Active Directory solo si tus cuentas residen en el nivel del bosque.

8. En Domains, haz clic en el botón Add (+) y añade los dominios de todos los recursos que utilicen Kerberos. Por ejemplo, si usas la autenticación de Kerberos con recursos de us.pretendco.com, añade «.us.pretendco.com». (No olvides incluir el punto inicial.)
9. Añade estos valores en Custom Configuration:

Key	Type	Value
pwNotificationDays	Number	15
requireUserPresence	Boolean	No comprobado
allowAutomaticLogin	Boolean	Comprobado
syncLocalPassword	Boolean	Comprobado
useSiteAutoDiscovery	Boolean	Comprobado
isDefaultRealm	Boolean	No comprobado

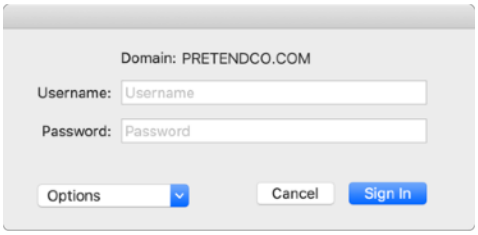
10. Haz clic en OK para guardar el nuevo perfil de configuración. Se instalará automáticamente en el dispositivo o grupo de dispositivos seleccionado.

Configuración de usuario: iOS y iPadOS

1. Conecta tu dispositivo a una red en la que esté disponible el dominio de Active Directory de la organización.
2. Haz una de estas opciones:
   - Utiliza Safari para acceder a un sitio web que admita la autenticación Kerberos.
   - Abre una app que sea compatible con la autenticación Kerberos.
3. Introduce tu nombre de usuario y contraseña de Kerberos o Active Directory.
4. Se te preguntará si quieres iniciar sesión automáticamente a partir de ese momento. La mayoría de los usuarios deben tocar Yes.
5. Toca Sign In. Tras una breve pausa, se cargará el sitio web o la app. Si elegiste iniciar sesión automáticamente en la extensión de SSO de Kerberos, no se te pedirán las credenciales hasta que cambies de contraseña. Si no elegiste el inicio de sesión automático, solo se te pedirán las credenciales cuando te caduque la de Kerberos (normalmente, al cabo de 10 horas).

Configuración de usuario: macOS

1. Debes autenticarte en la extensión de SSO de Kerberos. Hay distintas formas de iniciar este proceso:
   - Si tu Mac está conectado a la red en la que esté disponible tu dominio de Active Directory, se te pedirá que te autentiques justo después de que se instale el perfil de configuración del SSO extensible.
   - Si utilizas Safari para acceder a un sitio web que admita la autenticación Kerberos, o si usas una app que requiera dicha autenticación, se te pedirá que te autentiques.
   - Tendrás que autenticarte inmediatamente cada vez que conectes tu Mac a una red en la que tu Active Directory esté disponible.
   - Puedes seleccionar el menú extra de la extensión de SSO de Kerberos y hacer clic después en Sign In.
2. Se te pedirán las credenciales de Kerberos. Introduce tu nombre de usuario y contraseña de Kerberos o Active Directory.



3. Se te preguntará si quieres iniciar sesión automáticamente. La mayoría de los usuarios deben hacer clic en Yes.
4. Haz clic en Sign In. Tras una breve pausa, se cargará el sitio web o la app. Si elegiste iniciar sesión automáticamente en la extensión de SSO de Kerberos, no se te pedirán las credenciales hasta que cambies de contraseña. Si no elegiste el inicio de sesión automático, solo se te pedirán las credenciales cuando te caduque la de Kerberos (normalmente, al cabo de 10 horas).
5. Si tu contraseña está a punto de caducar, recibirás una notificación indicándote los días que quedan para que caduque. Puedes hacer clic en la notificación y cambiar la contraseña.
6. Si has activado la función de sincronización de contraseñas, se te pedirán las contraseñas local y de Active Directory que tengas. Introduce las dos y haz clic en OK para sincronizarlas. Aparecerá esa pantalla cada vez que inicies sesión aunque ya estén sincronizadas las contraseñas.

Cambios de contraseña: macOS

También puedes utilizar la extensión de SSO de Kerberos para cambiar tu contraseña de Active Directory:

1. Comprueba que has iniciado sesión en la extensión de SSO de Kerberos.
2. Selecciona el menú extra de SSO de Kerberos y elige Change Password. Es posible que recibas una notificación avisándote de que tu contraseña está a punto de caducar.
3. Introduce primero tu contraseña actual y luego la nueva. Asegúrate de que la nueva contraseña cumpla los requisitos de tu organización al respecto. Haz clic en OK.
4. Tras una breve pausa, aparecerá un cuadro de diálogo indicando que la contraseña se ha modificado correctamente. Si está activada la función de sincronización de contraseñas, la contraseña de tu cuenta local se actualizará con tu nueva contraseña de Active Directory.

Uso del menú extra de SSO de Kerberos: macOS

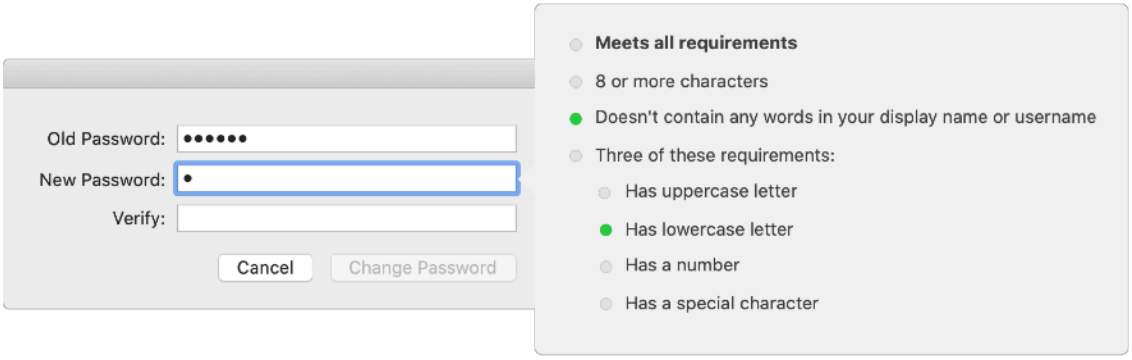
El menú extra de SSO de Kerberos permite acceder fácilmente a información útil sobre tu cuenta y a las funciones de la extensión. Aparecerá como una tecla gris o negra en la barra de menús que hay arriba a la derecha.

Para conocer el estado de tu cuenta, fíjate en el color del icono del menú extra de SSO de Kerberos. Si la tecla es de color gris, significa que no has iniciado sesión en la extensión. Si es negra, sí has iniciado sesión. Después de seleccionar la tecla, verás con qué cuenta has iniciado sesión y los días que quedan para que caduque tu contraseña. Con el menú también puedes iniciar y cerrar sesión y cambiar tu contraseña.

Funciones avanzadas

Comprobación de contraseñas en tiempo real

En muchas configuraciones de Active Directory, la extensión de SSO de Kerberos puede comprobar las nuevas contraseñas de los usuarios a medida que las introducen e indicarles los requisitos que deben cumplir. Si está activada esta función, el usuario verá esto cuando introduzca una nueva contraseña:



Para poder usar esta prestación, tu dominio de Active Directory debe usar solamente las políticas de contraseñas estándar de Active Directory. De manera predeterminada, Active Directory permite que un administrador exija que las contraseñas sean complejas y tengan determinada longitud. Puedes consultar más información sobre los requisitos de complejidad que deben cumplir las contraseñas en technet.microsoft.com/en-us/library/cc786468(v=ws.10).aspx.

Nota: Es posible que no puedas usar esta prestación si tu dominio utiliza herramientas o DLL de terceros para ampliar la política de contraseñas estándar de Active Directory. Por ejemplo, si no tienes permiso para incluir determinadas palabras aparte de tu nombre de usuario en tu contraseña o esta debe tener una cantidad específica de caracteres especiales, es posible que estés usando ampliaciones de las políticas de contraseñas de terceros. Si no lo sabes con seguridad, pídele más información a tu administrador de Active Directory.

Si el dominio de Active Directory de tu organización cumple los requisitos, puedes activar la comprobación de contraseñas en tiempo real. Define estos parámetros en el perfil de configuración de tu extensión de SSO de Kerberos:

Parámetro	Key	Type	Value	Opcional
Requerir contraseñas complejas	pwReqComplexity	Boolean	SÍ	No
Longitud de contraseña requerida	pwReqLength	Integer	Número	Sí
Reutilizar límite de contraseña anterior	pwReqHistory	Integer	Número	Sí
Antigüedad mínima de la contraseña	pwReqMinAge	Integer	Número	Sí

La comprobación de contraseñas en tiempo real tiene ciertas limitaciones. No puede comprobar si las contraseñas se han usado anteriormente ni si la tuya contiene tu nombre visible de Active Directory en caso de que aún no tengas un TGT de Kerberos. Esto puede suceder la primera vez que definas tu contraseña o si esta ha caducado. El resto de las comprobaciones funcionarán con normalidad.

Visualización de los requisitos de las contraseñas

Si no puedes usar la comprobación de contraseñas en tiempo real, puedes configurar la extensión de SSO de Kerberos para que muestre una cadena de texto con los requisitos que deben cumplir las contraseñas de tu organización a medida que las introducen los usuarios. En tu perfil de configuración de la extensión de SSO de Kerberos, define «pwReqText» como una cadena con el texto que verán los usuarios mientras cambian sus contraseñas.

Modificación o desactivación de las funciones de las contraseñas

Es posible que algunas organizaciones no puedan utilizar la función estándar para modificar contraseñas de la extensión de SSO de Kerberos porque no permiten que se cambien las contraseñas de Active Directory. En el perfil de configuración de tu extensión de SSO de Kerberos, asigna el valor FALSE a «allowPasswordChanges» para desactivar esta función.

Compatibilidad con sitios web de modificación de contraseñas: macOS

La extensión de SSO de Kerberos se puede configurar para que abra un sitio web de modificación de contraseñas en el navegador predeterminado cuando el usuario seleccione Change Password o confirme un aviso de caducidad de la contraseña. Apple recomienda utilizar esta prestación solo con cuentas locales porque no se admiten las cuentas móviles.

En tu perfil de configuración de la extensión de SSO de Kerberos, define «pwChangeURL» como la URL de tu sitio web para modificar contraseñas. Cuando los usuarios hayan cambiado sus contraseñas, deben cerrar sesión en la extensión de Kerberos y volver a iniciarla con sus nuevas contraseñas. Si está activada la sincronización de contraseñas locales, los usuarios recibirán instrucciones paso a paso para volver a sincronizar las suyas.

Sincronización de contraseñas: macOS

La extensión de SSO de Kerberos puede definir la contraseña de la cuenta local para que coincida con la contraseña de Active Directory de un usuario. Para activar esta función, asigna el valor TRUE a «syncLocalPassword» en la sección Custom Configuration del perfil de configuración de tu extensión de SSO de Kerberos.

La sincronización de contraseñas incluye dos funciones básicas. Primero, cuando un usuario cambia su contraseña con la extensión de SSO de Kerberos, esta función le permite definir su contraseña local para que coincida con la de Active Directory. Si las contraseñas local y de Active Directory dejan de estar sincronizadas, la extensión de SSO de Kerberos hace lo siguiente para volver a sincronizarlas:

- Una vez activada la sincronización de contraseñas y cada vez que la extensión de SSO de Kerberos intente conectarse después, las fechas correspondientes a la última vez que los usuarios cambiaron sus contraseñas locales y de Active Directory se compararán con los valores almacenados en caché. Si los valores coinciden, las contraseñas se sincronizarán y no será necesario hacer nada más. Si no coinciden, la extensión de SSO de Kerberos solicitará a los usuarios sus contraseñas locales y de Active Directory. Cuando los usuarios introduzcan sus contraseñas locales, la extensión de SSO de Kerberos las definirá para que coincidan con las de Active Directory.

- Los cambios de contraseña funcionan de manera parecida. Cuando los usuarios cambian sus contraseñas con la extensión de SSO de Kerberos, se comparan sus contraseñas anteriores de Active Directory con las de las cuentas locales. Si una contraseña anterior de Active Directory coincide con la local, la extensión de SSO de Kerberos cambiará las dos. Si no coinciden, solo se modificará la de Active Directory. Después, se pedirá a los usuarios que introduzcan sus contraseñas locales la próxima vez que intenten conectarse.

Esta prestación tiene los siguientes requisitos:

- Si los usuarios inician sesión en sus ordenadores Mac con sus cuentas de Active Directory —no con sus cuentas locales—, se desactivará la sincronización de contraseñas. Esta prestación solo se puede utilizar con cuentas locales y no es necesaria si los usuarios inician sesión en sus ordenadores Mac con sus cuentas de Active Directory.
- Si se aplica una política de contraseñas a las cuentas locales —por ejemplo, usar un perfil de configuración o el comando pwpolicy—, asegúrate de que la política de contraseñas locales sea menos estricta que la de Active Directory o que ambas coincidan. Si una política de contraseñas locales es más estricta que la de Active Directory, es posible que la extensión de SSO de Kerberos acepte una contraseña que cumpla los requisitos de Active Directory, pero no se definirá la contraseña local por no cumplir los requisitos pertinentes. No deberías usar esta prestación si la política de contraseñas locales debe ser más estricta que la de Active Directory.
- El nombre del usuario local es diferente al de Active Directory; solo las contraseñas están definidas para que coincidan.

Compatibilidad con tarjetas inteligentes: macOS

La extensión de SSO de Kerberos admite el uso de identidades basadas en tarjetas inteligentes en el proceso de autenticación. Las tarjetas inteligentes deben tener un driver CryptoTokenKit disponible; no se admite el uso de drivers basados en identificadores. macOS 10.15 admite el estándar PIV, muy utilizado por el gobierno de Estados Unidos.

Antes de empezar, asegúrate de que tu dominio de Active Directory esté configurado para admitir la autenticación mediante tarjetas inteligentes. En este documento no se describe el proceso para activar la autenticación en Active Directory mediante tarjetas inteligentes. Consulta más información al respecto en la documentación pertinente de Microsoft.

Sigue estos pasos para iniciar sesión en la extensión de SSO de Kerberos con una tarjeta inteligente:

1. Haz clic en el menú Options. A continuación selecciona Use a Smart Card.
2. Cuando aparezca el botón Identity, inserta tu tarjeta inteligente y haz clic en él.
3. Elige la identidad que quieras usar para autenticarte y haz clic en OK. A continuación, haz clic en Sign In.
4. Introduce tu PIN cuando se te solicite.

Si la extensión de SSO de Kerberos tiene que adquirir un TGT de Kerberos, se te pedirá que insertes tu tarjeta inteligente e introduzcas tu PIN. Si necesitas más información sobre la compatibilidad con tarjetas inteligentes en macOS, ejecuta «man SmartCardServices» en la app Terminal.

Notificaciones distribuidas: macOS

La extensión de SSO de Kerberos publica notificaciones distribuidas cuando se producen diferentes eventos. Los servicios y apps de macOS utilizan notificaciones distribuidas para avisar a otros servicios y apps cuando se ha producido un evento. Los servicios o apps que escuchan notificaciones de eventos pueden tomar diferentes medidas.

Los administradores pueden usar esta función para adoptar distintas medidas cuando se producen determinados eventos. Por ejemplo, es posible que un administrador decida ejecutar un script cada vez que la extensión de SSO de Kerberos adquiera una nueva credencial de Kerberos.

Lo único que hace la extensión de SSO de Kerberos es publicar notificaciones distribuidas cuando se producen eventos concretos; no ejecuta ninguna acción en esos casos. El administrador debe proporcionar una herramienta que escuche esas notificaciones y ejecute las acciones pertinentes en ese momento.

El apéndice incluye el ejemplo de un script y una lista de propiedades launchd (.plist) que pueden escuchar notificaciones y ejecutar acciones. Modifica este ejemplo para adaptarlo a tu implantación.

Estas son las notificaciones distribuidas que publica la extensión de SSO de Kerberos:

Nombre	Momento de la publicación
com.apple.KerberosPlugin.ConnectionCompleted	La extensión de SSO de Kerberos ha ejecutado su proceso de conexión.
com.apple.KerberosPlugin.ADPasswordChanged	El usuario ha cambiado la contraseña de Active Directory con la extensión.
com.apple.KerberosPlugin.LocalPasswordSynced	El usuario ha sincronizado las contraseñas local y de Active Directory.
com.apple.KerberosPlugin.InternalNetworkAvailable	El usuario se ha conectado a una red en la que está disponible el dominio de Active Directory configurado.
com.apple.KerberosPlugin.InternalNetworkNotAvailable	El usuario se ha conectado a una red en la que no está disponible el dominio de Active Directory configurado.
com.apple.KerberosExtension.gotNewCredential	El usuario ha adquirido un nuevo TGT de Kerberos.
com.apple.KerberosExtension.passwordChangedWithPasswordSync	El usuario ha cambiado la contraseña de Active Directory, y la local se ha actualizado para que coincida con la nueva contraseña de Active Directory.

Compatibilidad con la línea de comandos: macOS

Los administradores pueden utilizar una herramienta de línea de comandos llamada *app-sso* para controlar la extensión de SSO de Kerberos y acceder a información útil. Por ejemplo, pueden utilizar la herramienta para iniciar procesos de inicio y cierre de sesión y de cambio de contraseña. Además, la herramienta permite imprimir información útil, como el usuario que tiene una sesión iniciada, el sitio de Active Directory actual del ordenador, el recurso compartido principal de red del usuario, la fecha de caducidad de su contraseña y otra información útil y variada en formato de lista de propiedades o JSON. Esta información se puede analizar y subir a una solución de gestión del Mac para realizar tareas de inventario, entre otras.

Si necesitas más información sobre el uso de app-sso, ejecuta «app-sso -h» en la app Terminal.

Cuentas móviles: macOS

La extensión de SSO de Kerberos no necesita que tu Mac esté vinculado a Active Directory ni que el usuario inicie sesión en el Mac con una cuenta móvil. Apple sugiere que utilices la extensión de SSO de Kerberos con una cuenta local. Las cuentas locales funcionan mejor con el modelo de implantación recomendado para macOS y son la mejor opción para los usuarios de Mac hoy en día, que suelen conectarse de forma intermitente a la red de tu organización. La extensión de SSO de Kerberos está especialmente diseñada para mejorar la integración de Active Directory desde una cuenta local.

No obstante, puedes usar la extensión de SSO de Kerberos aunque decidas seguir utilizando cuentas móviles. Esta prestación tiene los siguientes requisitos:

- La sincronización de contraseñas no funciona con cuentas móviles. Si utilizas la extensión de SSO de Kerberos para cambiar tu contraseña de Active Directory y has iniciado sesión en tu Mac con la misma cuenta de usuario que usas con la extensión de SSO de Kerberos, los cambios de contraseña funcionan igual que en el panel de preferencias Users & Groups. Sin embargo, si tu contraseña se modifica desde una ubicación externa —la cambias tú desde un sitio web o la restablece el equipo de asistencia—, la extensión de SSO de Kerberos no puede volver a sincronizar la contraseña de tu cuenta móvil con tu contraseña de Active Directory.
- No se admite el uso de una URL para modificar contraseñas con la extensión de Kerberos y una cuenta móvil.

Asociación de dominio-reino

Es posible que los administradores tengan que definir una asociación personalizada de dominio-reino para Kerberos. Por ejemplo, puede que una organización tenga un reino de Kerberos llamado «ad.pretendco.com», pero que tenga que usar la autenticación Kerberos para acceder a los recursos del dominio «fakecompany.com».

Nota: La implementación de Kerberos en sistemas operativos Apple puede determinar automáticamente la asociación de dominio-reino en casi todos los casos. Es muy poco habitual que los administradores personalicen estos ajustes.

Estos son los pasos que se deben seguir para configurar la asociación de dominio-reino de la extensión de SSO de Kerberos:

1. En la sección Custom Configuration del perfil del SSO extensible, añade un objeto llamado domainRealmMapping. El objeto debe ser de tipo Dictionary.
2. Define la clave de este diccionario con el nombre de tu reino en mayúsculas.
3. Define el valor de este diccionario con el tipo Array. El primer valor debe ser el nombre de tu reino de Kerberos en minúsculas con un punto inicial. El segundo valor debe ser el nombre del dominio que se debe autenticar en este reino y también debe empezar con un punto. Ve añadiendo matrices conforme las necesites.

Consulta más información en la documentación de Kerberos.

Transición desde Enterprise Connect

Descripción

La finalidad de la extensión de SSO de Kerberos es sustituir a Enterprise Connect, una herramienta parecida que ya se utiliza en muchas organizaciones. Estos son los pasos que deberán seguir la mayoría de las organizaciones que decidan pasarse de Enterprise Connect a la extensión de SSO de Kerberos:

1. Crea un perfil de configuración para la extensión de SSO de Kerberos que proporcione funciones similares a tu perfil actual de Enterprise Connect.
2. Desinstala Enterprise Connect.
3. Implementa el nuevo perfil de configuración de la extensión de SSO de Kerberos.
4. Indica a los usuarios que deben iniciar sesión en la extensión de SSO de Kerberos.

No es obligatorio pasarse a la extensión de SSO de Kerberos para actualizar los ordenadores Mac de tu organización a macOS 10.15. Aunque Enterprise Connect funciona según lo previsto con macOS 10.15, las organizaciones deberían planificar el proceso de transición desde Enterprise Connect más adelante.

A quién no está destinada la transición

La extensión de SSO de Kerberos cubrirá las necesidades de la gran mayoría de las organizaciones que utilicen Enterprise Connect. No obstante, es posible que una organización que cumpla los criterios indicados a continuación no pueda hacer la transición desde Enterprise Connect o que solo pueda hacerla parcialmente:

- Las organizaciones que tengan ordenadores Mac con macOS 10.14 o versiones anteriores deben seguir utilizando Enterprise Connect en esos sistemas y pasarse a la extensión de SSO de Kerberos solo en los ordenadores Mac con macOS 10.15. La extensión de SSO de Kerberos y su perfil de configuración asociado solo funcionarán en ordenadores Mac con macOS 10.15. Actualiza esos sistemas a macOS 10.15 para aprovechar las ventajas de la extensión.
- Organizaciones que utilicen una herramienta de gestión para Mac que no admita la inscripción mediante MDM aprobada por el usuario.
- Organizaciones que no utilicen una herramienta de gestión.
- Organizaciones que utilicen un nivel funcional de Active Directory de Windows Server 2003 o versiones anteriores.

Creación de un perfil de configuración para la extensión de SSO de Kerberos

Debes crear un perfil de configuración para la extensión de SSO de Kerberos que se parezca al que utilizas con Enterprise Connect. Muchas de las preference keys de tu perfil de configuración actual de Enterprise Connect tienen equivalencias con un perfil de la extensión de SSO de Kerberos. Para empezar, revisa la tabla siguiente. En ella se especifican las equivalencias de la extensión de SSO de Kerberos con las preference keys de Enterprise Connect:

Enterprise Connect	Extensión de SSO de Kerberos	Notas
adRealm	Realm	El reino debe aparecer con todas las letras en mayúscula.
Automatic login (enabled by default)	allowAutomaticLogin	Se añade a la sección Custom Configuration. Debe tener asignado el valor True para que el inicio de sesión automático funcione.
disablePasswordFunctions	allowPasswordChange	Se añade a la sección Custom Configuration. Se le asigna el valor False para desactivar los cambios de contraseña.
passwordChangeURL	pwChangeURL	Se añade a la sección Custom Configuration.
passwordExpireOverride	pwExpireOverride	Se añade a la sección Custom Configuration.
passwordNotificationDays	pwNotificationDays	Se añade a la sección Custom Configuration.
prepopulatedUsername	principalName	Se añade a la sección Custom Configuration.
pwReqComplexity	pwReqComplexity	Se añade a la sección Custom Configuration.
pwReqHistory	pwReqHistory	Se añade a la sección Custom Configuration.
pwReqLength	pwReqLength	Se añade a la sección Custom Configuration.
pwReqMinimumPasswordAge	pwReqMinAge	Se añade a la sección Custom Configuration.
pwReqText	pwReqText	Se añade a la sección Custom Configuration. Se proporciona una cadena de texto para que se muestre en lugar de una ruta a un archivo RTF.
syncLocalPassword	syncLocalPassword	Se añade a la sección Custom Configuration.

Nota: Puede que no se incluyan en esta tabla algunas de las preference keys incluidas en tu perfil de configuración de Enterprise Connect. Es posible que hagan referencia a funciones que ya no se necesitan en la extensión de SSO de Kerberos o que ya no se admiten.

Desinstalación de Enterprise Connect

No se admite la ejecución simultánea de la extensión de SSO de Kerberos y Enterprise Connect en un mismo ordenador. Cuando te hayas pasado a la extensión de SSO de Kerberos, debes desinstalar Enterprise Connect. Necesitarás derechos de administrador para hacerlo. Sigue estos pasos para desinstalar Enterprise Connect:

Enterprise Connect 2.0 y versiones posteriores

1. Descarga el agente de Enterprise Connect. Para ello, abre la app Terminal y ejecuta «launchctl unload /Library/LaunchAgents/com.apple.ecAgent» como usuario con sesión iniciada.
2. Sal del menú extra de Enterprise Connect. Para ello, abre la app Terminal e introduce «killall Enterprise\ Connect\ Menu» en ella.
3. Elimina la app Enterprise Connect de la carpeta Applications.
4. Elimina la lista de propiedades launchd con extensión .plist de Enterprise Connect, ubicada en /Library/LaunchAgents/com.apple.ecAgent.plist.

Enterprise Connect 1.9.5 y versiones anteriores

1. Sal de Enterprise Connect. Para ello, introduce «killall Enterprise\ Connect» en la app Terminal.
2. Elimina la app Enterprise Connect de la carpeta Applications.

El apéndice incluye un ejemplo de script que elimina todas las versiones de Enterprise Connect.

Activadores de scripts de Enterprise Connect

Enterprise Connect puede ejecutar scripts cuando se producen determinados eventos. Por ejemplo, Enterprise Connect puede ejecutar un script cuando finalice su proceso de conexión o cuando un usuario cambie de contraseña. La extensión de SSO de Kerberos SSO no gestiona los scripts como Enterprise Connect porque no los ejecuta directamente, sino que publica una notificación distribuida cuando se produce un evento que puede escuchar otro proceso y, después, ejecuta un script. Consulta información más detallada en el apartado «Funciones avanzadas» de este documento.

La tabla siguiente incluye referencias a activadores de scripts de Enterprise Connect y sus notificaciones distribuidas equivalentes en la extensión de SSO de Kerberos:

Enterprise Connect	Extensión de SSO de Kerberos
auditScriptPath	com.apple.KerberosPlugin.InternalNetworkAvailable
connectionCompletedScriptPath	com.apple.KerberosPlugin.ConnectionCompleted
passwordChangeScriptPath	com.apple.KerberosPlugin.ADPasswordChanged

Recursos compartidos de red

La extensión de SSO de Kerberos no admite la gestión de recursos compartidos de red, como el directorio principal de red de un usuario. Puedes suplir gran parte de esta función con scripts.

Apéndice

Perfil de gestión de dispositivos: ExtensibleSingleSignOnKerberos

developer.apple.com/documentation/devicemanagement/extensiblesinglesignonkerberos?language=objc

Referencia sobre el protocolo de gestión de dispositivos móviles

developer.apple.com/business/documentation/MDM-Protocol-Reference.pdf

Perfil de gestión de dispositivos: ExtensibleSingleSignOnKerberos.ExtensionData

developer.apple.com/documentation/devicemanagement/extensiblesinglesignonkerberos/extensiondata?language=objc

Ejemplo de script: procesamiento de notificaciones distribuidas

La extensión de SSO de Kerberos publica notificaciones distribuidas cuando se producen diferentes eventos, como cuando un usuario cambia de contraseña o la red de una empresa se conecta online. Como administrador, puedes usar un script o una app para escuchar esas notificaciones y tomar las medidas oportunas cuando se publiquen, como ejecutar un script o una shell de comandos.

El ejemplo de script siguiente puede ejecutar scripts o comandos cuando se publican notificaciones. Se debe ejecutar como LaunchAgent para ejecutarse como usuario con sesión iniciada o como LaunchDaemon para ejecutarse como usuario raíz. El script requiere dos parámetros:

- **-notification** es el nombre de la notificación distribuida que quieres escuchar. Puedes consultar algunos ejemplos en la página 11.
- **-action** es la acción que quieres ejecutar cuando se publica la notificación distribuida. Ejemplo: «sh /path/to/script.sh».

Debes tener instaladas las herramientas de línea de comandos para desarrolladores si quieres ejecutar el script. Hay disponible un paquete de instalador con estas herramientas en el sitio web para desarrolladores de Apple.

```
#!/usr/bin/swift

import Foundation

class NotifyHandler {

    // Action we want to run, like a shell command or a script
    public var action = String()

    // Runs every time we receive the specified distributed
    // notification
    @objc func gotNotification(notification: NSNotification){
        let task = Process()
        task.launchPath = "/bin/zsh"
        task.arguments = ["-c", action]
        task.launch()
    }
}

// MAIN

let scriptPath: String = CommandLine.arguments.first!

// -notification is the name of the notification you are listening for
guard let notification = UserDefaults.standard.string(forKey: "notification") else {
    print("\(scriptPath): No notification passed, exiting…")
    exit(1)
}
```

```
// -action is the action you want to run. This can be a shell

// command, script, etc.
guard let action = UserDefaults.standard.string(forKey: "action") else {
    print("\(scriptPath): No action passed, exiting…")
    exit(1)
}

let nh = NotifyHandler()
nh.action = action

print("Action is \(nh.action) and notification is \(notification)")

// Listen for the specified notification
DistributedNotificationCenter.default().addObserver(
    nh,
    selector: #selector(nh.gotNotification),
    name: NSNotification.Name(rawValue: notification),
    object: action)

RunLoop.main.run()
```

Ejemplo de script para desinstalar Enterprise Connect

Con este ejemplo de script se desinstala cualquier versión de Enterprise Connect. Ejecútalo con privilegios de usuario raíz desde una solución de gestión para Mac o manualmente.

```
#!/bin/zsh

# Unload the Kerberos helper from versions of EC prior to 1.6
if [[ -e /Library/LaunchDaemons/com.apple.Enterprise-Connect.kerbHelper.plist ]]; then
  launchctl bootout system /Library/LaunchDaemons/com.apple.Enterprise-Connect.kerbHelper.plist
  rm /Library/LaunchDaemons/com.apple.Enterprise-Connect.kerbHelper.plist
fi

# Remove the privileged helper from versions of EC prior to 1.6
if [[ -e /Library/PrivilegedHelperTools/com.apple.Enterprise-Connect.kerbHelper ]]; then
  rm /Library/PrivilegedHelperTools/com.apple.Enterprise-Connect.kerbHelper
fi

# Remove the authorization db entry from versions of EC prior to 1.6
/usr/bin/security authorizationdb read com.apple.Enterprise-Connect.writeKDCs > /dev/null

if [[ $? -eq 0 ]]; then
  security authorizationdb remove com.apple.Enterprise-Connect.writeKDCs
fi

if [[ -e /Library/LaunchAgents/com.apple.ecAgent.plist ]]; then
  # Enterprise Connect 2.0 or greater is installed
  # Unload ecAgent for logged in user and remove from launchd

  loggedInUser=$(scutil <<< "show State:/Users/ConsoleUser" | awk '/Name :/ && ! /loginwindow/ { print $3 }')
  loggedInUID=$(id -u $loggedInUser)

  launchctl bootout gui/$loggedInUID /Library/LaunchAgents/com.apple.ecAgent.plist
  rm /Library/LaunchAgents/com.apple.ecAgent.plist

  # Quit the menu extra
  killall "Enterprise Connect Menu"
fi

# Finally, remove the Enterprise Connect app bundle
rm -rf /Applications/Enterprise\ Connect.app
```