A Kerberos egyszeri bejelentkezéses bővítménye

Felhasználói útmutató

2019. december

Tartalom

Bevezetés

A Kerberos egyszeri bejelentkezési (SSO) bővítmény megkönnyíti a Kerberos egyszeri bejelentkezés használatát a vállalata Apple-eszközein.

Egyszerűsített Kerberos-hitelesítés

A Kerberos SSO-bővítmény leegyszerűsíti a Kerberos jegymegadási jegyek (TGT) beszerzésének folyamatát a szervezet Active Directory-tartományától, így lehetővé téve, hogy a felhasználók zökkenőmentesen hitelesíthessék magukat az olyan erőforrások felé, mint amilyenek a webhelyek, az alkalmazások és a fájlszerverek. A macOS-alapú rendszereken a Kerberos SSO-bővítmény a hálózati állapot változásakor proaktívan beszerez egy Kerberos TGT-t, ezzel biztosítva, hogy a felhasználó készen álljon a hitelesítésre, amikor az szükségessé válik.

Active Directory-fiókkezelés

A Kerberos SSO-bővítmény segíti a felhasználókat az Active Directory-fiókjuk kezelésében is. A macOS-alapú rendszereken lehetővé teszi a felhasználók számára az Active Directory-jelszavuk módosítását, és értesíti őket, ha egy jelszó hamarosan lejár. A felhasználók ezenkívül a helyi fiókjelszavukat is módosíthatják, hogy az megegyezzen az Active Directory-jelszavukkal.

Active Directory-támogatás

A Kerberos SSO-bővítmény helyszíni Active Directory-tartománnyal való használatra van tervezve. Az Azure Active Directory használata nem támogatott. A Kerberos SSO-bővítmény használatához nincs szükség az eszközök Active Directory-tartományhoz való csatlakoztatására. Arra sincs továbbá szükség, hogy a felhasználók a Mac gépükön Active Directory- vagy mobilfiókokkal jelentkezzenek be – az Apple ehelyett a helyi fiókok használatát javasolja.

Követelmények

- iOS 13, iPadOS, vagy macOS Catalina.
- Windows Server 2008 vagy annál újabb rendszert használó Active Directory-tartomány. A Kerberos SSO-bővítmény nem az Azure Active Directoryval való használatra van tervezve. Az üzemeltetéséhez hagyományos, helyszíni Active Directory-tartományra van szükség.
- Hozzáférés ahhoz a hálózathoz, ahol az Active Directory-tartomány található. A hálózati hozzáférés történhet Wi-Fi-, Ethernet- vagy VPN-kapcsolat használatával.
- Az eszközök felügyeletéhez Mobile Device Management- (MDM-) megoldásra van szükség, amely támogatja a bővíthető egyszeri bejelentkezési (SSO) konfigurációs profilcsomagot. A konfigurációs profilcsomag támogatásáról érdeklődjön MDM-beszállítójánál.

Enterprise Connect

A Kerberos SSO-bővítmény az Enterprise Connectet váltja le. Ha Ön jelenleg Enterprise Connectet használ, és át szeretne térni a Kerberos SSO-bővítményre, további információkért tekintse meg e dokumentum „Áttérés az Enterprise Connectről” című szakaszát.

Első lépések

Konfigurációs profil létrehozása és üzembe helyezése

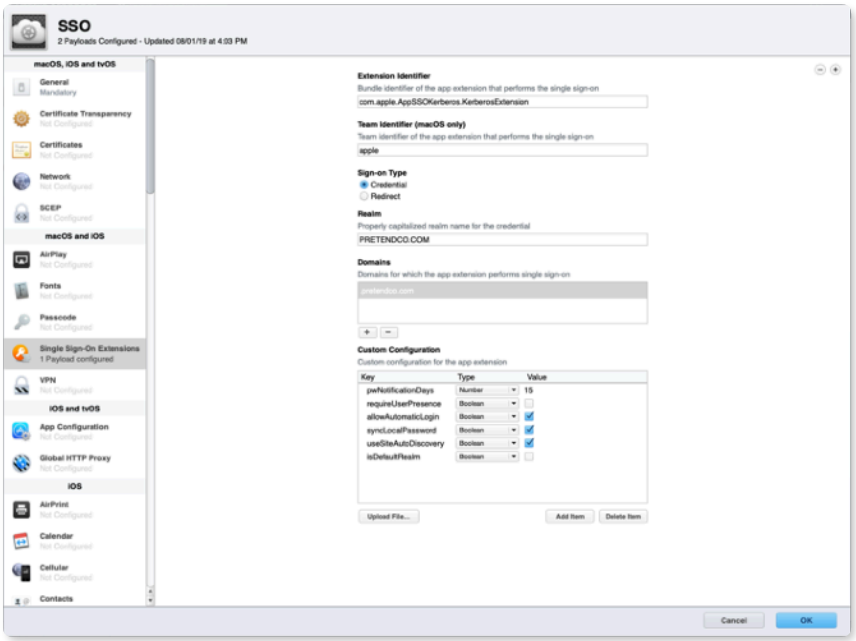
A Kerberos SSO-bővítmény használatához konfigurálnia kell azt egy konfigurációs profil használatával, amely egy MDM-megoldáson keresztül küldhető el az eszközre.

Megjegyzés: A konfigurációs profilt az MDM-en keresztül kell elküldeni az eszközre. macOS-alapú rendszerek esetében felhasználó által jóváhagyott MDM-regisztrációra van szükség, amely a Rendszer hatókörben van telepítve. A profilok manuális hozzáadása nem támogatott.

A konfigurációs profillal történő konfiguráláshoz az iOS 13, iPadOS, illetve macOS 10.15 által tartalmazott bővíthető egyszeri bejelentkezési csomagot kell használni. A macOS Server részét képező Profilkezelő támogatja a bővíthető egyszeri bejelentkezési csomagot. Ha az MDM-megoldása még nem támogatja ezt a csomagot, előfordulhat, hogy létrehozhatja a szükséges profilt a Profilkezelőben, majd importálhatja az MDM-megoldásba terjesztés céljából. További információért lépjen kapcsolatba MDM-beszállítójával.

A konfigurációs profilok Profilkezelővel történő létrehozásához kövesse ezeket a lépéseket:

1. Jelentkezzen be a Profilkezelőbe.
2. Hozzon létre egy eszközcsoporthoz vagy egy adott eszközhöz tartozó profilt.
3. Kattintson a Single Sign-On Extensions (Egyszeri bejelentkezési bővítmények) elemre a Payload (Csomagok) listáján, majd kattintson a Hozzáadás (+) gombra egy új csomag hozzáadásához.
4. Az Extension Identifier (Bővítményazonosító) mezőbe gépelje be a következőt: „com.apple.AppSSOKerberos.KerberosExtension”.
5. A Team Identifier (Csapatazonosító) mezőbe írja be a következőt: „apple”.



6. A Sign-on Type (Bejelentkezés típusa) alatt válassza ki a Credential (Hitelesítő adatok) lehetőséget.
7. A Realm (Tartomány) mezőbe gépelje be annak az Active Directory-tartománynak a nevét, ahol a felhasználói fiókjai találhatóak, csupa nagybetűt használva. Ne az Active Directory-erdő nevét használja, kivéve, ha a felhasználói fiókok az erdő szintjén helyezkednek el.

8. A Domains (Tartományok) alatt kattintson a Hozzáadás (+) gombra, és adja hozzá a Kerberost használó összes erőforrás tartományát. Ha például Kerberos-hitelesítést használ a us.pretendco.com webhelyen található erőforrásokhoz, adja hozzá a „.us.pretendco.com” tartományt. (Ügyeljen a pontra a kifejezés elején.)
9. A Custom Configuration (Egyéni konfiguráció) területen adja hozzá a következő értékeket:

Key	Type	Value
pwNotificationDays	Number	15
requireUserPresence	Boolean	Nincs bejelölve
allowAutomaticLogin	Boolean	Be van jelölve
syncLocalPassword	Boolean	Be van jelölve
useSiteAutoDiscovery	Boolean	Be van jelölve
isDefaultRealm	Boolean	Nincs bejelölve

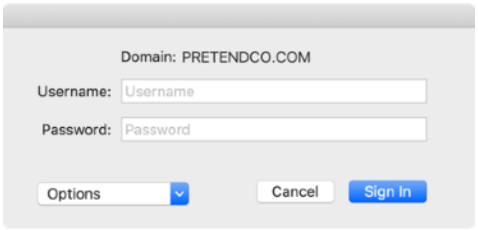
10. Kattintson az OK gombra az új konfigurációs profil mentéséhez. A profil automatikusan telepítve lesz a kiválasztott eszközön vagy eszközcsoporton.

Felhasználó beállítása – iOS és iPadOS

1. Csatlakoztassa az eszközét egy olyan hálózathoz, ahol a szervezete Active Directory-tartománya elérhető.
2. Tegye a következők valamelyikét:
   - Safari használatával nyissa meg a Kerberos-hitelesítést támogató webhelyet.
   - Indítson el egy alkalmazást, amely támogatja a Kerberos-hitelesítést.
3. Adja meg a Kerberos- vagy Active Directory-felhasználónevét és -jelszavát.
4. A rendszer rá fog kérdezni, hogy szeretne-e minden alkalommal automatikusan bejelentkezni. A legtöbb felhasználó esetében érdemes a Yes (Igen) lehetőségre koppintani.
5. Koppintson a Sign In (Bejelentkezés) parancsra. Kis idő elteltével betölt a webhely vagy alkalmazás. Ha a Kerberos SSO-bővítménybe való automatikus bejelentkezést választotta, nem kell újból megadnia a hitelesítő adatait, ameddig nem módosítja a jelszavát. Ha nem az automatikus bejelentkezést választotta, csak azután kell újból megadnia a hitelesítő adatait, hogy a Kerberos-beli hitelesítő adatai lejárnak (általában 10 óra elteltével).

Felhasználó beállítása – macOS

1. Hitelesítésre van szükség a Kerberos SSO-bővítmény felé. Ezt a folyamatot többféleképpen is megkezdheti:
   - Ha a Mac gépe csatlakoztatva van ahhoz a hálózathoz, amelyen az Active Directory-tartománya elérhető, a rendszer hitelesítést fog kérni rögtön azután, hogy telepítette a bővíthető SSO-konfigurációt.
   - Ha Safarit használ a Kerberos-hitelesítést támogató webhely megnyitásához, vagy olyan alkalmazást használ, amelyhez Kerberos-hitelesítés szükséges, a rendszer hitelesítést fog kérni.
   - A rendszer azonnal hitelesítést fog kérni, ha a Mac gépét olyan hálózathoz csatlakoztatja, ahol az Active Directory-tartománya elérhető.
   - Kiválaszthatja a Kerberos SSO-bővítmény menüextráját is, majd kattinthat a Sign In (Bejelentkezés) parancsra.
2. A rendszer kérni fogja a Kerberos-beli hitelesítő adatait. Adja meg a Kerberos- vagy Active Directory-felhasználónevét és -jelszavát.



3. A rendszer rá fog kérdezni, hogy szeretne-e automatikusan bejelentkezni. A legtöbb felhasználó esetében érdemes a Yes (Igen) lehetőségre kattintani.
4. Kattintson a Sign In (Bejelentkezés) parancsra. Kis idő elteltével betölt a webhely vagy alkalmazás. Ha a Kerberos SSO-bővítménybe való automatikus bejelentkezést választotta, nem kell újból megadnia a hitelesítő adatait, ameddig nem módosítja a jelszavát. Ha nem az automatikus bejelentkezést választotta, csak azután kell újból megadnia a hitelesítő adatait, hogy a Kerberos-beli hitelesítő adatai lejárnak (általában 10 óra elteltével).
5. Ha a jelszava hamarosan lejár, értesítést fog kapni a lejártáig fennmaradó napok számáról. Az értesítésre kattintva módosíthatja a jelszavát.
6. Ha engedélyezte a jelszó-szinkronizálási funkciót, meg kell adnia a jelenlegi Active Directory- és helyi jelszavát. Adja meg mindkettőt, majd kattintson az OK gombra a jelszavak szinkronizálásához. Ez a felkérés akkor is megjelenik az első bejelentkezéskor, ha a jelszavai már szinkronizálva vannak.

Jelszómódosítás – macOS

A Kerberos SSO-bővítménnyel az Active Directory-jelszavát is módosíthatja:

1. Győződjön meg arról, hogy be van jelentkezve a Kerberos SSO-bővítménybe.
2. Válassza ki a Kerberos SSO-bővítmény menüextráját, majd válassza a Change Password (Jelszó módosítása) parancsot. Előfordulhat, hogy értesítést kap a jelszava közelgő lejártáról.
3. Adja meg az aktuális jelszavát, majd az új jelszavát. Ügyeljen rá, hogy az új jelszava megfeleljen a szervezete jelszavakkal kapcsolatos követelményeinek. Kattintson az OK gombra.
4. Kis idő elteltével megjelenik egy párbeszédablak, amely a jelszó sikeres módosításáról tájékoztatja. Ha a jelszó-szinkronizálási funkció engedélyezve van, a rendszer a helyi fiókja jelszavát az új Active Directory-jelszavával megegyezőre frissíti.

A Kerberos SSO menüextrájának használata – macOS

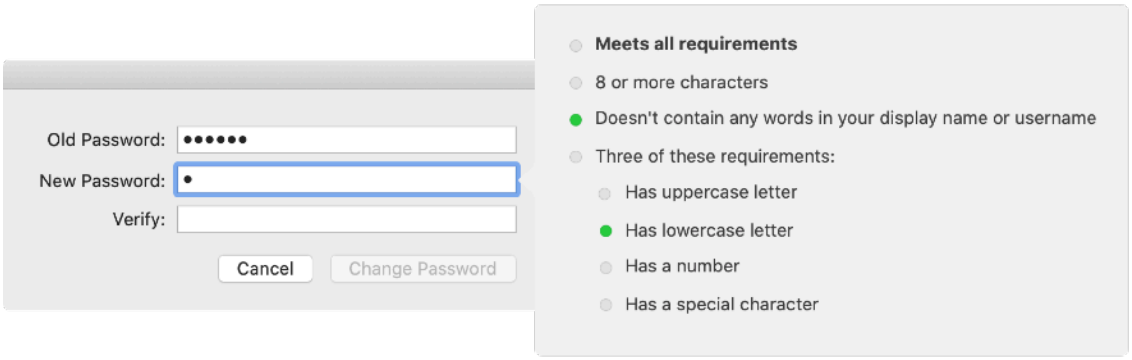
A Kerberos SSO menüextrájának használatával könnyen elérhetők a fiókjára és a bővítmény funkcióira vonatkozó hasznos információk. Szürke vagy fekete kulcs formájában jelenik meg a menüsoron, a jobb felső részen.

Ha a fiókjára vonatkozó állapotinformációkra van szüksége, először tekintse meg, milyen színű a Kerberos SSO menüextrájának ikonja. Ha a kulcs szürke, nincs bejelentkezve a bővítménybe. Ha a kulcs fekete, be van jelentkezve. A kulcs kiválasztása után megjelenik a bejelentkezéshez használt fiók, valamint a jelszó lejártáig fennmaradó napok száma. A menü ezenkívül a bejelentkezést, a kijelentkezést és a jelszó módosítását is lehetővé teszi.

Speciális funkciók

Élő jelszóellenőrzés

A Kerberos SSO-bővítmény sok Active Directory-konfiguráció esetében képes tesztelni az új felhasználói jelszavakat a begépelésük közben, és ismertetni a felhasználóval a jelszó módosításának követelményeit. Ha ez a funkció be van állítva, a felhasználó a következő nézetet fogja látni az új jelszó megadásakor:



E funkció használatának feltétele, hogy az Active Directory-tartománya csak szabványos Active Directory-jelszószabályzatokat használjon. Az Active Directory alapértelmezett esetben lehetővé teszi, hogy a rendszergazda a jelszavak összetettségére és hosszára vonatkozó követelményeket adjon meg. Az összetett jelszavak mibenlétére vonatkozó információkért lásd: technet.microsoft.com/hu-hu/library/cc786468(v=ws.10).aspx.

Megjegyzés: Ha a tartománya harmadik féltől származó eszközöket vagy DLL-eket használ a szabványos Active Directory-jelszószabályzatok kibővítésére, előfordulhat, hogy nem fogja tudni használni ezt a funkciót. Ha például a felhasználóneve, vagy bizonyos más szavak a jelszóban történő használata is tiltott, vagy a jelszónak adott számú különleges karaktert kell tartalmaznia, lehetséges, hogy harmadik féltől származó jelszószabályzat-bővítményeket használ. Ha bizonytalan ebben, kérjen további tájékoztatást Active Directory-rendszergazdájától.

Ha a szervezete Active Directory-tartománya megfelel a követelményeknek, engedélyezheti az élő jelszóellenőrzést. A Kerberos SSO-bővítmény konfigurációs profiljában adja meg a következő paramétereket:

Paraméter	Key	Type	Value	Választható
Összetett jelszavak megkövetelése	pwReqComplexity	Boolean	IGEN	Nem
Jelszó kötelező hossza	pwReqLength	Integer	Számérték	Igen
Előző jelszókorlát újbóli felhasználása	pwReqHistory	Integer	Számérték	Igen
Jelszó minimális élettartama	pwReqMinAge	Integer	Számérték	Igen

Az élő jelszóellenőrzésre bizonyos korlátozások vonatkoznak. Nem tudja ellenőrizni, hogy a felhasználó egy adott jelszót használt-e már korábban. Azt sem képes ellenőrizni, hogy a jelszó tartalmazza-e a felhasználó Active Directoryban megjelenített nevét, ha még nem rendelkezik Kerberos TGT-vel. Ez akkor fordulhat elő, ha első alkalommal állítja be a jelszavát, vagy a jelszava lejárt. Minden más ellenőrzés normál módon működik.

Jelszókövetelmények megjelenítése

Ha nem tudja használni az élő jelszóellenőrzést, beállíthatja, hogy a Kerberos SSO-bővítmény az új jelszavak megadásakor megjelenítsen egy szöveges karakterláncot, amely a szervezete jelszavakra vonatkozó követelményeit tartalmazza. A Kerberos SSO-bővítmény konfigurációs profiljában állítsa be a „PwReqText" értékét a felhasználó számára a jelszó módosításakor megjelenítendő karakterláncra.

A jelszómódosítási funkció letiltása

Előfordulhat, hogy egyes szervezetek nem tudják használni a Kerberos SSO-bővítmény jelszómódosítási funkcióját, mivel nem engedélyezik az Active Directory-jelszó módosítását. Ha az „allowPasswordChanges" értékét FALSE-ra (HAMIS) állítja a Kerberos SSO-bővítmény konfigurációs profiljában, azzal letilthatja a funkció használatát.

Jelszómódosítási webhely támogatása – macOS

A Kerberos SSO-bővítmény beállítható úgy, hogy egy jelszómódosítási webhelyet nyisson meg az alapértelmezett böngészőben, amikor a felhasználó a „Jelszó módosítása" elemet választja, vagy a jelszó lejártára figyelmeztető értesítésre kattint. Az Apple csak helyi fiók használata esetén javasolja ennek a funkciónak a használatát, mivel a mobilfiókok nem támogatottak.

A Kerberos SSO-bővítmény konfigurációs profiljában állítsa be a „pwChangeURL" értékét a jelszómódosítási webhely URL-címére. Miután a felhasználó módosította a jelszót, ki kell jelentkeznie a Kerberos-bővítményből, majd újra be kell jelentkeznie az új jelszóval. Ha engedélyezve van a helyi jelszóval való szinkronizálás, a rendszer végigvezeti a felhasználót a jelszavak szinkronizálásán.

Jelszó-szinkronizálás – macOS

A Kerberos SSO-bővítmény képes a helyi fiók jelszavát egy felhasználó Active Directory-jelszavával megegyezőre állítani. A funkció engedélyezéséhez állítsa a „syncLocalPassword" értékét TRUE-ra (IGAZ) a Kerberos SSO-bővítmény konfigurációs profiljának Egyéni beállítások szakaszában.

A jelszó-szinkronizálásnak két alapvető funkciója van. Az egyik, ha a felhasználó a Kerberos SSO-bővítmény használatával módosítja a jelszavát, ez a funkció az Active Directory-jelszavával megegyezőre állítja a helyi jelszavát. Ha a helyi és az Active Directory-jelszó közül valamelyik megváltozik, a Kerberos SSO-bővítmény ismét szinkronizálja őket a következő módon:

- A jelszó-szinkronizálás engedélyezésekor, valamint a Kerberos SSO-bővítmény minden ezt követő kapcsolódási kísérletekor a rendszer összehasonlítja a felhasználó helyi és Active Directory-jelszavának legutóbbi módosítási dátumát a tárolt értékekkel. Ha az értékek megegyeznek, a jelszavak szinkronban vannak, és nincs szükség intézkedésre. Ha nem egyeznek, a Kerberos SSO-bővítmény felkéri a felhasználót a helyi és Active Directory-jelszava megadására. Ha a felhasználó megadta a helyi jelszót, a Kerberos SSO-bővítmény úgy állítja át azt, hogy az egyezzen az Active Directory-jelszavával.
- A jelszómódosítás hasonlóan működik. Ha a felhasználó jelszómódosítást végez a Kerberos SSO-bővítmény használatával, a rendszer összehasonlítja a régi Active Directory-jelszavát a helyi fiókjáéval. Ha a helyi jelszó egyezik egy régi Active Directory-jelszóval, a Kerberos SSO-bővítmény mindkettőt módosítja. Ha nem egyeznek, csak az Active Directory-jelszó módosul. Ezt követően a felhasználónak a következő csatlakozási kísérletkor meg kell adnia a helyi jelszavát.

Ez a funkció a következő követelményekkel rendelkezik:

- Ha a felhasználók a Mac gépükre Active Directory-fiókkal – és nem helyi fiókkal – vannak bejelentkezve, a jelszó-szinkronizálás le van tiltva. Ez a funkció csak helyi fiókokkal való használatra lett tervezve. Ha a felhasználó Active Directory-fiókkal van bejelentkezve a Mac gépén, a funkcióra nincs szükség.
- Valamely jelszószabályzat helyi fiókokon kikényszerített alkalmazása esetén – például konfigurációs profil vagy a pwpolicy parancs használatakor – gondoskodjon arról, hogy a helyi szabályzat megegyezzen az Active Directory jelszószabályzatával, vagy kevésbé legyen szigorú annál. Ha valamely helyi jelszószabályzat szigorúbb az Active Directory szabályzatánál, a Kerberos SSO-bővítmény elfogadhatja az Active Directory követelményeinek megfelelő jelszót, de nem lesz képes beállítani a helyi jelszót, mivel a jelszó nem felel meg a helyi jelszavakkal kapcsolatos követelményeknek. Ha a helyi jelszószabályzatnak szigorúbbnak kell lennie az Active Directory-jelszószabályzatnál, ne használja ezt a funkciót.
- A helyi felhasználónév különbözik az Active Directory-felhasználónévtől – csak a jelszavak szinkronizálása van beállítva.

Intelligens kártyák támogatása – macOS

A Kerberos SSO-bővítmény támogatja az intelligens kártyákon alapuló hitelesítési identitásokat. Az intelligens kártyáknak rendelkezniük kell a CryptoTokenKit illesztőprogrammal. A tokenalapú illesztőprogramok nem támogatottak. A macOS 10.15 tartalmazza a PIV szabvány támogatását, amelyet az Egyesült Államok kormánya széles körben használ.

A kezdés előtt győződjön meg arról, hogy az Active Directory-tartomány konfigurálva van az intelligens kártyás hitelesítés támogatására. Az Active Directory felé történő intelligens kártyás hitelesítés engedélyezése nem tartozik e dokumentum tárgykörébe. A további részletekért tekintse meg a Microsoft dokumentációját.

A Kerberos SSO-bővítménybe történő intelligenskártya-alapú bejelentkezéshez kövesse ezeket a lépéseket:

1. Kattintson az Options (Beállítások) menüre, majd válassza a „Use a smart card” (Intelligens kártya használata) elemet.
2. Ha megjelenik az Identitás gomb, helyezze be az intelligens kártyát, és kattintson a gombra.
3. Válassza ki a hitelesítéshez használni kívánt identitást, kattintson az OK gombra, majd a Sign In (Bejelentkezés) parancsra.
4. Amikor a rendszer kéri, adja meg a PIN-kódját.

Ha a Kerberos SSO-bővítménynek Kerberos TGT-t kell beszereznie, a rendszer megkéri, hogy helyezze be az intelligens kártyáját, és adja meg a PIN-kódját. Az intelligens kártyák macOS rendszer általi támogatásáról további információt a Terminálon a „man SmartCardServices” parancs futtatásával tudhat meg.

Terjesztett értesítések – macOS

A Kerberos SSO-bővítmény terjesztett értesítéseket tesz közzé, amikor különböző események következnek be. A macOS alkalmazásai és szolgáltatásai terjesztett értesítésekkel közlik a többi alkalmazással és szolgáltatással, hogy egy esemény történt. Az eseményt figyelő alkalmazások vagy szolgáltatások műveletet végezhetnek, amikor ez bekövetkezik.

A rendszergazdák ezzel a funkcióval elvégeztethetnek műveleteket, amikor bizonyos események bekövetkeznek. Előfordulhat például, hogy egy rendszergazda mindig egy szkriptet kíván futtatni, amikor a Kerberos SSO-bővítmény új Kerberos-beli hitelesítő adatokat szerez be.

A Kerberos SSO-bővítmény egyszerűen terjesztett értesítéseket tesz közzé, amikor a megadott események megtörténnek. Maga a bővítmény nem futtat semmilyen műveletet, amikor ezek az események bekövetkeznek. A rendszergazdának kell biztosítania egy eszközt ezen értesítések figyeléséhez és a műveletek futtatásához az események előfordulásakor.

A függelék tartalmazza egy szkript példáját és egy launchd-tulajdonságlistát (.plist), amely figyelni tudja az értesítéseket, és műveletetek tud futtatni. A környezet igényei szerint módosítsa ezt a példát.

Alább a Kerberos SSO-bővítmény által közzétett terjesztett értesítéseket találja:

Név	Közzétételkor
com.apple.KerberosPlugin.ConnectionCompleted	A Kerberos SSO-bővítmény futtatta a csatlakozási folyamatát.
com.apple.KerberosPlugin.ADPasswordChanged	A felhasználó módosította az Active Directory-jelszót a bővítménnyel.
com.apple.KerberosPlugin.LocalPasswordSynced	A felhasználó szinkronba állította az Active Directory- és a helyi jelszót.
com.apple.KerberosPlugin.InternalNetworkAvailable	A felhasználó olyan hálózathoz csatlakozott, ahol a konfigurált Active Directory-tartomány elérhető.
com.apple.KerberosPlugin.InternalNetworkNotAvailable	A felhasználó olyan hálózathoz csatlakozott, ahol a konfigurált Active Directory-tartomány nem érhető el.
com.apple.KerberosExtension.gotNewCredential	A felhasználó új Kerberos TGT-t szerzett be.
com.apple.KerberosExtension.passwordChangedWithPasswordSync	A felhasználó módosította az Active Directory-jelszót, és a helyi jelszó frissült, hogy megegyezzen az új Active Directory-jelszóval.

Parancssori támogatás – macOS

A rendszergazdák az *app-sso* parancssori eszközzel vezérelhetik a Kerberos SSO-bővítményt, illetve érhetnek el hasznos adatokat. Az eszközzel például bejelentkezést, jelszómódosításokat és kijelentkezést kezdeményezhetnek. Ezenkívül hasznos információkat tud megjeleníteni, például az aktuálisan bejelentkezett felhasználót, a számítógép aktuális Active Directory-webhelyét, a felhasználó otthoni hálózati megosztását, a felhasználói jelszó lejáratának idejét és sok más hasznos adatot tulajdonságlista vagy JSON formátumban. Ezek az információk leltározási és egyéb célokból elemezhetők és feltölthetők egy maces felügyeleti megoldásba.

Az app-sso használatáról további információt a Terminál alkalmazásban az „app-sso -h” parancsot futtatva szerezhet.

Mobilfiókok – macOS

A Kerberos SSO-bővítményhez nem kell a Mac gépet az Active Directory-hoz kötni, és a felhasználónak nem kell mobilfiókkal bejelentkeznie a Mac gépre. Az Apple azt javasolja, hogy helyi fiókkal használja a Kerberos SSO-bővítményt. A helyi fiókok működnek a legjobban a macOS rendszerhez javasolt üzemeltetési modellel, és manapság ezek a legjobb választások azon Mac-felhasználók számára, akik időnként a szervezet hálózatához csatlakoznak. A Kerberos SSO-bővítmény kifejezetten azért jött létre, hogy javítsa a helyi fiókról végzett Active Directory-integrációt.

Ha azonban továbbra is mobilfiókokat használ, akkor is használhatja a Kerberos SSO-bővítményt. Ez a funkció a következő követelményekkel rendelkezik:

- A jelszó-szinkronizálás nem használható a mobilfiókokkal. Ha a Kerberos SSO-bővítménnyel módosítja az Active Directory-jelszót, és ugyanazzal a felhasználói fiókkal van bejelentkezve a Mac gépre, mint amelyet a Kerberos SSO-bővítménnyel használ, a jelszómódosítás úgy működik, ahogyan a Felhasználók és csoportok beállítási panelen. De ha külső jelszómódosítást végez – vagyis egy webhelyen módosítja a jelszót, vagy az ügyfélszolgálat alaphelyzetbe állítja –, a Kerberos SSO-bővítmény nem tudja szinkronizálni a mobilfiók jelszavát az Active Directory-jelszóval.
- A Kerberos-bővítménnyel és a mobilfiókokkal a jelszómódosítási URL-ek használata nem támogatott.

Tartományleképezés

Előfordulhat, hogy a rendszergazdának egyéni tartományleképezést kell meghatároznia a Kerberoshoz. Egy szervezetben lehet például egy „ad.pretendco.com” nevű Kerberos-tartomány, de lehet, hogy Kerberos-hitelesítést kell használnia a „fakecompany.com” tartományon lévő erőforrásokhoz.

Megjegyzés: Az Apple által készített operációs rendszereken a Kerberos implementációja szinte az összes helyzetben automatikusan meg tudja határozni a tartományleképezést. Nagyon ritka, hogy a rendszergazdák szabják testre ezeket a beállításokat.

A következő lépésekkel konfigurálható tartományleképezés a Kerberos SSO-bővítményhez:

1. A Bővíthető SSO-profil Egyéni konfiguráció szakaszához adjon hozzá egy domainRealmMapping nevű objektumot. Az objektumnak Szótár típusúnak kell lennie.
2. Adja meg a tartomány nevét nagybetűkkel a szótár kulcsaként.
3. A szótár értékét állítsa Tömb típusúra. Az első értéknek a Kerberos-tartomány nevének kell lennie kisbetűvel, és ponttal kell kezdődnie. A második értéknek azon tartomány nevének kell lennie, amelyet a Kerberos-tartományhoz képest kell hitelesíteni, ismét ponttal kezdve. Igény szerint adjon hozzá tömböket.

További információt a Kerberos dokumentációjában talál.

Áttérés az Enterprise Connectről

Áttekintés

A Kerberos SSO-bővítmény az Enterprise Connectet váltja le, amely egy számos vállalat által már használatba vett, hasonló eszköz. Az Enterprise Connectről a Kerberos SSO-bővítményre áttérő szervezetek legtöbbje az alábbi lépéseket fogja követni:

1. Hozzon létre egy olyan konfigurációs profilt a Kerberos SSO-bővítményhez, amely az aktuális Enterprise Connect-profilhoz hasonló funkciókat nyújt.
2. Távolítsa el az Enterprise Connectet.
3. Telepítse az új Kerberos SSO-bővítmény konfigurációs profilját.
4. Kérje meg a felhasználókat, hogy jelentkezzenek be a Kerberos SSO-bővítménybe.

Nem kell áttérni a Kerberos SSO-bővítményre ahhoz, hogy a szervezet Mac gépeit macOS 10.15-ös verzióra frissítse. Az Enterprise Connect a várt módon működik a macOS 10.15-ös verzióval, de a szervezeteknek így is számítaniuk kell arra, hogy végül át kell majd térniük az Enterprise Connectről.

Akinél ellenjavallt az áttérés

A Kerberos SSO-bővítmény az Enterprise Connectet használó szervezetek legtöbbjénél megfelel az igényeknek. Előfordulhat, hogy a következő feltételeknek megfelelő szervezetek azonban nem tudnak áttérni az Enterprise Connectre, vagy csak részben tudnak áttérni:

- A jelenleg macOS 10.14-es vagy korábbi rendszert futtató Mac gépeket használó szervezeteknek meg kell őrizniük az Enterprise Connectet ezeken a rendszereken, és csak a macOS 10.15-ös rendszert futtató Mac gépeken térhetnek át a Kerberos SSO-bővítményre. A Kerberos SSO-bővítmény és a társított konfigurációs profilja csak a macOS 10.15-ös verziót futtató Mac gépeken működik. A Kerberos SSO-bővítmény használatához frissítse ezeket a rendszereket a macOS 10.15-ös verzióra.
- Azon maces felügyeleti eszközt használó szervezetek, amelyek nem támogatják a felhasználók által jóváhagyott MDM-regisztrációt.
- A felügyeleti eszközt nem használó szervezetek.
- A Windows Server 2003-as vagy korábbi Active Directory-működési szintet alkalmazó szervezetek.

A Kerberos SSO-bővítmény konfigurációs profiljának létrehozása

Olyan konfigurációs profilt kell létrehoznia a Kerberos SSO-bővítményhez, amely hasonló az Enterprise Connect konfigurációs profiljához. Az aktuális Enterprise Connect konfigurációs profilban lévő számos Preference Keynek van megfelelője a Kerberos SSO-bővítmény profiljában. Először tekintse át az alábbi táblázatot, amely az Enterprise Connect Preference Keynek megfelelő Kerberos SSO-bővítményelemek leképezését tartalmazza:

Enterprise Connect	Kerberos SSO-bővítmény	Megjegyzések
adRealm	Realm	A tartománynak nagybetűkből kell állnia.
Automatic login (enabled by default)	allowAutomaticLogin	Az Egyéni konfiguráció szakaszhoz kell hozzáadni. Igaz (True) értékre kell állítani, hogy működjön az automatikus bejelentkezés.
disablePasswordFunctions	allowPasswordChange	Az Egyéni konfiguráció szakaszhoz kell hozzáadni. A jelszómódosítások letiltásához állítsa Hamis (False) értékre.
passwordChangeURL	pwChangeURL	Az Egyéni konfiguráció szakaszhoz kell hozzáadni.
passwordExpireOverride	pwExpireOverride	Az Egyéni konfiguráció szakaszhoz kell hozzáadni.
passwordNotificationDays	pwNotificationDays	Az Egyéni konfiguráció szakaszhoz kell hozzáadni.
prepopulatedUsername	principalName	Az Egyéni konfiguráció szakaszhoz kell hozzáadni.
pwReqComplexity	pwReqComplexity	Az Egyéni konfiguráció szakaszhoz kell hozzáadni.
pwReqHistory	pwReqHistory	Az Egyéni konfiguráció szakaszhoz kell hozzáadni.
pwReqLength	pwReqLength	Az Egyéni konfiguráció szakaszhoz kell hozzáadni.
pwReqMinimumPasswordAge	pwReqMinAge	Az Egyéni konfiguráció szakaszhoz kell hozzáadni.
pwReqText	pwReqText	Az Egyéni konfiguráció szakaszhoz kell hozzáadni. Adjon meg egy megjeleníteni kívánt szöveges karakterláncot egy RTF-fájl útvonala helyett.
syncLocalPassword	syncLocalPassword	Az Egyéni konfiguráció szakaszhoz kell hozzáadni.

Megjegyzés: Előfordulhat, hogy az Enterprise Connect konfigurációs profiljának néhány Preference Keynek nem szerepel itt. Ezek olyan funkciókra hivatkozhatnak, amelyekre már nincs szükség a Kerberos SSO-bővítményben, vagy amelyek már nem támogatottak.

Az Enterprise Connect eltávolítása

Ugyanazon a számítógépen a Kerberos SSO-bővítmény és az Enterprise Connect egyidejű futtatása nem támogatott. A Kerberos SSO-bővítményre való áttérés után távolítsa el az Enterprise Connectet. Az eltávolításhoz rendszergazdai jogosultságokra lesz szüksége. Az Enterprise Connect eltávolításához kövesse az alábbi lépéseket:

Enterprise Connect 2.0 és újabb

1. Az Enterprise Connect eltávolításához indítsa el a Terminál alkalmazást, és futtassa a „launchctl unload /Library/LaunchAgents/com.apple.ecAgent" fájlt a jelenleg bejelentkezett felhasználóként.
2. Lépjen ki az Enterprise Connect menüextrából a Terminál alkalmazás elindításával, majd a „killall Enterprise\ Connect\ Menu" parancs kiadásával.
3. Törölje az Enterprise Connect alkalmazást az Alkalmazások mappából.
4. Törölje az Enterprise Connect launchd .plist-fájlt a /Library/LaunchAgents/com.apple.ecAgent.plist helyről.

Enterprise Connect 1.9.5 és korábbi

1. Az Enterprise Connect bezárásához írja be a „killall Enterprise\ Connect" parancsot a Terminál alkalmazásban.
2. Törölje az Enterprise Connect alkalmazást az Alkalmazások mappából.

A függelékben található egy mintaszkript, amely eltávolítja az Enterprise Connect összes verzióját.

Az Enterprise Connect szkriptindítói

Az Enterprise Connect szkripteket tud futtatni, amikor bizonyos események történnek. Az Enterprise Connect például futtatni tud egy szkriptet, amikor befejeződik a csatlakozási folyamata, vagy amikor a felhasználó jelszómódosítást végez. A Kerberos SSO-bővítmény máshogyan kezeli a szkripteket, mint az Enterprise Connect. Nem futtat közvetlenül szkripteket. Ehelyett terjesztett értesítést tesz közzé, amikor esemény történik, amelyeket egy másik folyamat megfigyelhet, majd az észlelés után futtathatja a szkriptet. Részleteket a jelen dokumentum „Speciális funkciók" szakaszában talál.

Alább az Enterprise Connect szkriptindítóinak referenciáit és a Kerberos SSO-bővítményben az azoknak megfelelő terjesztett értesítéseket találja:

Enterprise Connect	Kerberos SSO-bővítmény
auditScriptPath	com.apple.KerberosPlugin.InternalNetworkAvailable
connectionCompletedScriptPath	com.apple.KerberosPlugin.ConnectionCompleted
passwordChangeScriptPath	com.apple.KerberosPlugin.ADPasswordChanged

Hálózati megosztások

A Kerberos SSO-bővítmény nem támogatja a hálózati megosztások, például a felhasználó hálózati kezdőkönyvtárának a kezelését. A funkció jelentős részét szkriptekkel helyettesítheti.

Függelék

Eszközfelügyeleti profil: ExtensibleSingleSignOnKerberos

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

Mobileszköz-felügyeleti protokoll referenciája

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

Eszközfelügyeleti profil: ExtensibleSingleSignOnKerberos.ExtensionData

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

Mintaszkript – Terjesztett értesítések feldolgozása

A Kerberos SSO-bővítmény különböző terjesztett értesítéseket tesz közzé, amikor egyes események bekövetkeznek, például amikor a felhasználó módosít egy jelszót, vagy ha a vállalati hálózat online állapotba kerül. Rendszergazdaként szkripttel vagy egy alkalmazással megfigyelheti ezeket az értesítéseket, és a közzétételükkor műveletet végezhet, például egy szkriptet vagy parancshéjat indíthat.

Alább egy mintaszkript található, amely szkripteket vagy parancsokat képes futtatni az értesítések közzétételekor. Ezt LaunchAgent ügynökként kell végrehajtani, hogy a bejelentkezett felhasználóként fusson, vagy LaunchDaemon szolgáltatásként, hogy gyökérszintű felhasználói jogosultságokkal fusson. A szkriptnek két kötelező paramétere van:

- A **-notification** a megfigyelni kívánt terjesztett értesítés neve. A 11. oldalon talál erre példákat.
- Az **-action** a terjesztett értesítés közzétételekor végrehajtani kívánt művelet. Például: „sh /path/to/script.sh”.

A szkript futtatásához telepítenie kell a fejlesztői parancssori eszközöket. Ezen eszközök telepítőcsomagja az Apple Developer webhelyen érhető el.

```
#!/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()
```

Mintaszkript – Az Enterprise Connect eltávolítása

Ez a mintaszkript eltávolítja az Enterprise Connect összes verzióját. Egy maces felügyeleti megoldásból vagy manuálisan is végrehajthatja. A szkriptet gyökérszintű felhasználói jogosultságokkal kell futtatni.

```
#!/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
```