Kerberos-tillägg för enkel inloggning

Användarhandledning

December 2019

Innehåll

Introduktion

Med Kerberos-tillägget för enkel inloggning (SSO) är det enkelt att använda Kerberos-baserad enkel inloggning med företagets Apple-enheter.

Förenklad Kerberos-autentisering

Kerberos-tillägget för enkel inloggning förenklar processen för att få en biljettbeviljande Kerberos-biljett (TGT) från företagets Active Directory-domän, så att användarna smidigt kan autentisera sig på webbplatser, i appar, på filservrar och i andra resurser. I macOS skaffar Kerberos-tillägget för enkel inloggning en Kerberos-TGT proaktivt när nätverkets status ändras så att användaren kan autentisera när det behövs.

Hantera Active Directory-konton

Med Kerberos-tillägget för enkel inloggning blir det enklare för användarna att hantera sina Active Directory-konton. I macOS kan användarna ändra sina Active Directory-lösenord och de meddelas när ett lösenord snart löper ut. Användarna kan även ändra sina lokala kontolösenord så att de stämmer med Active Directory-lösenorden.

Stöd för Active Directory

Kerberos-tillägget för enkel inloggning ska användas med en Active Directory-domän på plats. Det har inte stöd för Azure Active Directory. Enheterna behöver inte vara kopplade till en Active Directory-domän för att använda Kerberos-tillägget för enkel inloggning. Användarna behöver inte heller logga in på sin Mac med Active Directory eller mobila konton. Apple rekommenderar istället att man använder lokala konton.

Krav

- iOS 13, iPadOS eller macOS Catalina.
- En Active Directory-domän som kör Windows Server 2008 eller senare. Kerberos-tillägget för enkel inloggning ska inte användas med Azure Active Directory. Det kräver en traditionell Active Directory-domän på plats.
- Tillgång till nätverket som är värd för Active Directory-domänen. Man kan ansluta till nätverket via wifi, Ethernet eller VPN.
- Enheterna måste hanteras med en MDM-lösning (Mobile Device Management) med stöd för nyttolasten till konfigurationsprofilen för utökningsbar enkel inloggning (SSO). Fråga din MDM-leverantör om de har stöd för den här konfigurationsprofilens nyttolast.

Enterprise Connect

Kerberos-tillägget för enkel inloggning är tänkt att ersätta Enterprise Connect. Läs avsnittet Övergå från Enterprise Connect i det här dokumentet för mer information om ni för närvarande använder Enterprise Connect och vill gå över till Kerberos-tillägget för enkel inloggning.

Komma igång

Skapa och driftsätta en konfigurationsprofil

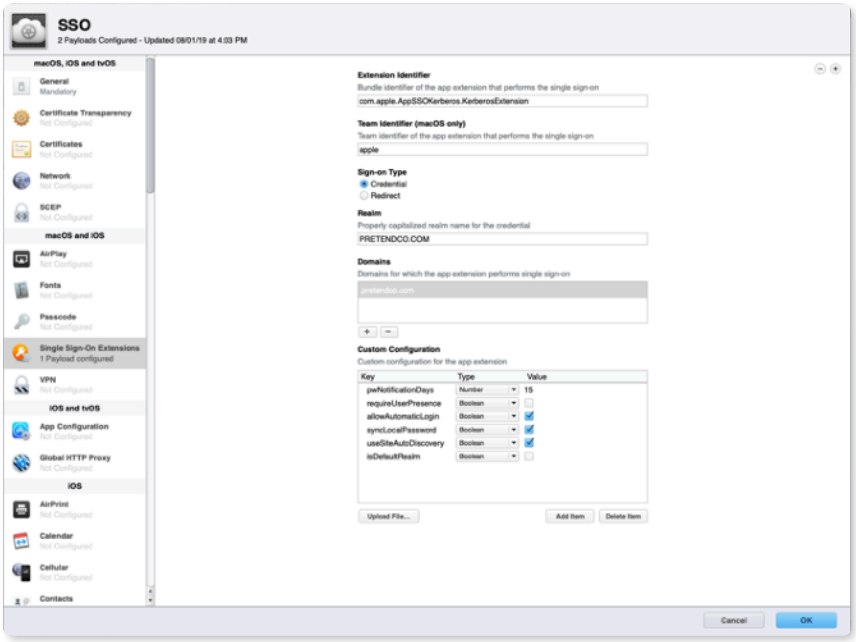
För att använda Kerberos-tillägget för enkel inloggning måste man konfigurera det med en konfigurationsprofil som levereras till enheten från en MDM-lösning.

Obs! Konfigurationsprofilen måste levereras till enheten via MDM. I macOS måste det vara en användargodkänd MDM-registrering som installeras i systemet. Det går inte att lägga till profilen manuellt.

För att konfigurera med en konfigurationsprofil ska du använda nyttolasten till utökningsbar enkel inloggning som lanserades i iOS 13, iPadOS och macOS 10.15. Profilhanteraren, en del av macOS Server, har stöd för nyttolasten till utökningsbar enkel inloggning. Det kan hända att du kan skapa den nödvändiga profilen i Profilhanteraren om din MDM-lösning inte har stöd för den här nyttolasten ännu. Importera sedan profilen till MDM-lösningen för distribution. Kontakta din MDM-leverantör för mer information.

Följ de här stegen för att skapa en konfigurationsprofil med Profilhanteraren:

1. Logga in i Profilhantereran.
2. Skapa en profil för en grupp enheter eller en specifik enhet.
3. Välj tillägg för enkel inloggning i listan med nyttolaster. Klicka sedan på plusknappen för att lägga till en ny nyttolast.
4. Ange ”com.apple.AppSSOKerberos.KerberosExtension” i fältet Extension Identifier.
5. Ange ”apple” i fältet Team Identifier.



6. Välj Credential under Sign-on Type.
7. Ange namnet på den Active Directory-domän där dina konton finns i fältet Realm. Skriv namnet med versaler. Använd aldrig namnet till din Active Directory-skog, bara om dina konton finns på skogsnivå.

8. Klicka på plusknappen under Domains och lägg till domäner till alla resurser som använder Kerberos. Lägg till exempel till ”.us.pretendco.com.” om Kerberos-autentisering används med resurser på us.pretendco.com. (Glöm inte punkten i början.)
9. Lägg till följande värden under Custom Configuration:

Key	Type	Value
pwNotificationDays	Number	15
requireUserPresence	Boolean	Inte markerad
allowAutomaticLogin	Boolean	Markerad
syncLocalPassword	Boolean	Markerad
useSiteAutoDiscovery	Boolean	Markerad
isDefaultRealm	Boolean	Inte markerad

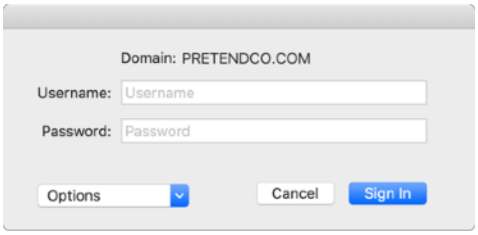
10. Klicka på OK för att spara den nya konfigurationsprofilen. Den installeras automatiskt på den valda enheten eller enhetsgruppen.

Användarinställning – iOS och iPadOS

1. Anslut enheten till ett nätverk där organisationens Active Directory-domän finns.
2. Gör något av följande:
   - Använd Safari för att öppna en webbplats med stöd för Kerberos-autentisering.
   - Öppna en app med stöd för Kerberos-autentisering.
3. Ange användarnamnet och lösenordet till Kerberos eller Active Directory.
4. Man uppmanas då att meddela om man alltid vill logga in automatiskt. De flesta användare svarar ja.
5. Logga in. Webbplatsen eller appen laddas efter en kort paus. Man behöver inte ange sina inloggningsuppgifter igen förrän man byter lösenord, om man väljer att logga in i Kerberos-tillägget för enkel inloggning automatiskt. Om man väljer att inte logga in automatiskt behöver man bara ange inloggningsuppgifterna när Kerberos-uppgifterna slutar att gälla, vanligtvis efter 10 timmar.

Användarinställning – macOS

1. Man måste autentisera Kerberos-tillägget för enkel inloggning. Det går att börja på flera sätt:
   - Man uppmanas att autentisera direkt efter att konfigurationsprofilen för utökningsbar enkel inloggning installeras om Mac-datorn är ansluten till det nätverk där Active Directory-domänen finns.
   - Man uppmanas att autentisera om man använder Safari för att öppna en webbplats som godkänner Kerberos-autentisering eller om man använder en app som kräver Kerberos-autentisering.
   - Man uppmanas direkt att autentisera varje gång man ansluter sin Mac till ett nätverk där Active Directory är tillgängligt.
   - Man kan välja menytillbehöret till Kerberos-tillägget för enkel inloggning och sedan klicka för att logga in.
2. Man uppmanas att ange Kerberos-inloggningsuppgifterna. Ange användarnamnet och lösenordet till Kerberos eller Active Directory.



3. Man uppmanas då att meddela om man vill logga in automatiskt. De flesta användare svarar ja.
4. Klicka för att logga in. Webbplatsen eller appen laddas efter en kort paus. Man behöver inte ange sina inloggningsuppgifter igen förrän man byter lösenord, om man väljer att logga in i Kerberos-tillägget för enkel inloggning automatiskt. Om man väljer att inte logga in automatiskt behöver man bara ange inloggningsuppgifterna när Kerberos-uppgifterna slutar att gälla, vanligtvis efter 10 timmar.
5. När lösenordet snart går ut får man ett meddelande med information om hur många dagar det är kvar till att lösenordet går ut. Man kan då klicka på meddelandet och byta lösenord.
6. Man uppmanas att ange de aktuella lokala och Active Directory-lösenorden om man har aktiverat funktionen för synkning av lösenord. Ange båda och klicka sedan på OK för att synka lösenorden. Det här meddelandet visas när man först loggar in, även om lösenorden redan är synkade.

Byta lösenord – macOS

Man kan även byta sitt Active Directory-lösenord med Kerberos-tillägget för enkel inloggning:

1. Kontrollera att du är inloggad i Kerberos-tillägget för enkel inloggning.
2. Välj menytillbehöret till Kerberos-tillägget för enkel inloggning och välj Change Password. Det kan även hända att man får ett meddelande när lösenordet är på väg att gå ut.
3. Ange det nuvarande lösenordet och ange sedan det nya lösenordet. Se till att det nya lösenordet uppfyller företagets lösenordskrav. Klicka på OK.
4. Efter en kort stund visas en dialogruta som bekräftar att lösenordet har ändrats. Lösenordet till det lokala kontot uppdateras för att stämma med det nya Active Directory-lösenordet om funktionen för synkning av lösenord är aktiverad.

Använda menytillbehöret till Kerberos-tillägget för enkel inloggning – macOS

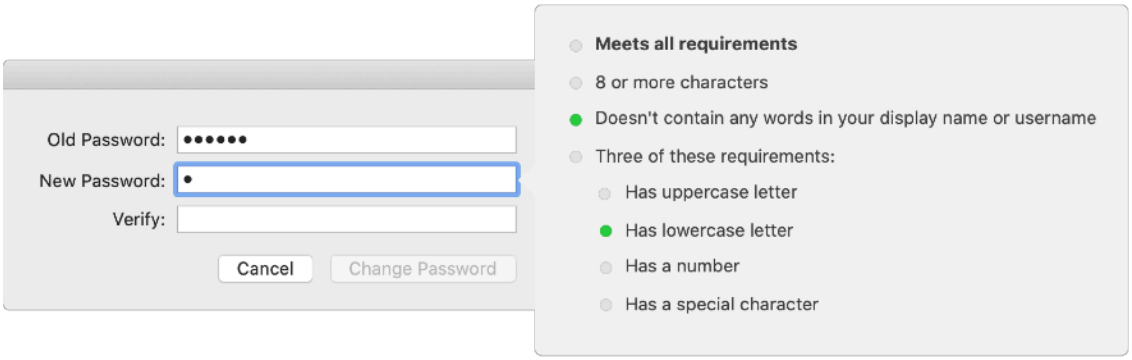
Menytillbehöret till Kerberos-tillägget för enkel inloggning erbjuder enkel tillgång till användbar information om kontot och tilläggets funktioner. Det visas som en grå eller svart nyckel i menyraden högst upp till höger.

Börja med att kontrollera färgen på symbolen till Kerberos-tilläggets menytillbehör för att få statusinformation om kontot. Om nyckeln är grå är du inte inloggad i tillägget. Om nyckeln är svart är du inloggad. När du har valt nyckeln visas det konto som du är inloggad med samt hur många dagar som är kvar till att lösenordet går ut. Från menyn kan man även logga in, logga ut och byta lösenord.

Avancerade funktioner

Testa lösenord live

I många Active Directory-konfigurationer kan Kerberos-tillägget för enkel inloggning testa nya användarlösenord när man skriver in dem och tala om för användarna vilka krav de måste uppfylla för att kunna byta lösenord. Den här vyn visas när man anger ett nytt lösenord om det är konfigurerat:



Active Directory-domänen kan bara ha standardriktlinjer för Active Directory-lösenord för att man ska kunna använda den här funktionen. Som standard tillåter Active Directory att en administratör kräver att lösenord ska vara komplexa och en viss längd. Besök technet.microsoft.com/en-us/library/cc786468(v=ws.10).aspx för att läsa mer om vad ett komplext lösenord innebär.

Obs! Det kan hända att man inte kan använda den här funktionen om domänen använder verktyg från andra utvecklare eller DLL:er för att utöka standardriktlinjerna för Active Directory-lösenord. Det kan till exempel vara så att ni använder tillägg för lösenordskrav från andra utvecklare om man inte kan använda vissa ord utöver sitt användarnamn i lösenordet eller om man måste ha ett visst antal specialtecken i lösenordet. Be Active Directory-administratören om mer information om du är osäker.

Du kan aktivera test av lösenord live om organisationens Active Directory-domän uppfyller kraven. Ställ in följande parametrar i konfigurationsprofilen till Kerberos-tillägget för enkel inloggning:

Parameter	Key	Type	Value	Valfritt
Kräv komplexa lösenord	pwReqComplexity	Boolean	JA	Nej
Kräv en viss längd på lösenorden	pwReqLength	Integer	Siffra	Ja
Återanvänd den tidigare lösenordsgränsen	pwReqHistory	Integer	Siffra	Ja
Minsta tid för lösenord	pwReqMinAge	Integer	Siffra	Ja

Test av lösenord live har vissa begränsningar. Funktionen kan inte testa om ett lösenord redan har använts. Det går heller inte att testa om lösenordet innehåller Active Directory-namnet om man inte redan har en Kerberos-TGT. Det kan hända när man ställer in lösenordet första gången eller om lösenordet har gått ut. Alla andra test fungerar som vanligt.

Ruta med lösenordskrav

Man kan konfigurera Kerberos-tillägget så att en textsträng med organisationens lösenordskrav visas när användarna anger nya lösenord, om man inte kan använda test av lösenord live. Lägg till ”pwReqText” i en sträng med texten som du vill ska visas för användarna när man byter lösenord i konfigurationsprofilen till Kerberos-tillägget.

Ändra eller avaktivera lösenordsfunktionen

Vissa organisationer kanske inte kan använda standardfunktionen för byte av lösenord i Kerberos-tillägget för enkel inloggning på grund av att de inte tillåter att man byter lösenord via Active Directory. Ställ in ”allowPasswordChanges” som FALSE för att avaktivera den här funktionen i konfigurationsprofilen till Kerberos-tillägget för enkel inloggning.

Stöd för webbplats för lösenordsbyte – macOS

Kerberos-tillägget för enkel inloggning kan konfigureras för att öppna en webbplats för lösenordsbyte i standardwebbläsaren när användare väljer Change password eller klickar på ett meddelande om att lösenordet snart går ut. Apple rekommenderar att man endast använder den här funktionen när man använder ett lokalt konto, eftersom mobila konton inte stöds.

Ställ in ”pwChangeURL” som URL-länk till webbplatsen för lösenordsbyte i konfigurationsprofilen till Kerberos-tillägget. Man måste logga ut från Kerberos-tillägget när man har bytt lösenord och sedan logga in på nytt med det nya lösenordet. Användarna får stegvisa anvisningar för att synka lösenordet igen om synkronisering av lokala lösenord är aktiverat.

Synka lösenord – macOS

Kerberos-tillägget för enkel inloggning kan ställa in det lokala kontolösenordet så att det är samma som en användares Active Directory-lösenord. Aktivera den här funktionen genom att ställa in ”syncLocalPassword” som TRUE i avsnittet Custom Configuration i konfigurationsprofilen till Kerberos-tillägget för enkel inloggning.

Synkning av lösenord omfattar två grundläggande funktioner. Den första är att när användaren byter lösenord med Kerberos-tillägget för enkel inloggning ställer funktionen in det så att det ska vara samma som Active Directory-lösenordet. Om det lokala lösenordet och Active Directory-lösenordet skulle sluta att synkas ser Kerberos-tillägget för enkel inloggning till att de synkas igen på följande sätt:

- När man aktiverar synkning av lösenordet och varje gång Kerberos-tillägget försöker att ansluta, så jämförs datumen då användaren senast ändrade sitt lokala lösenord och sitt Active Directory-lösenord med de cachelagrade värdena. Om värdena stämmer överens är lösenorden synkade och ingen åtgärd behövs. Om de inte stämmer överens uppmanar Kerberos-tillägget för enkel inloggning användaren att ange det lokala lösenordet och Active Directory-lösenordet. När användaren anger sitt lokala lösenord ställer Kerberos-tillägget in det så att det ska stämma med Active Directory-lösenordet.
- Lösenordsändringar fungerar på ungefär samma sätt. När användaren ändrar lösenord med Kerberos-tillägget kontrolleras det gamla Active Directory-lösenordet mot det lokala kontot. Kerberos-tillägget för enkel inloggning ändrar båda lösenorden om det gamla Active Directory-lösenordet och det lokala lösenordet är samma. Om de inte är samma ändras bara Active Directory-lösenordet. Man uppmanas sedan att ange det lokala lösenordet nästa gång man försöker att ansluta.

Den här funktionen har följande krav:

- Synkningen av lösenord avaktiveras för användare som är inloggade på sin Mac med Active Directory-kontot, inte det lokala. Den här funktionen ska endast användas med lokala konton. Funktionen är onödig om man är inloggad på sin Mac med sitt Active Directory-konto.
- Se till att riktlinjerna för lokala lösenord är samma eller mindre strikta än riktlinjerna för Active Directory-lösenord om det finns särskilda riktlinjer för lokala konton, till exempel med en konfigurationsprofil eller pwpolicy-kommandot. Om riktlinjerna för lokala lösenord är striktare än de för Active Directory kan Kerberos-tillägget för enkel inloggning godkänna ett lösenord som uppfyller Active Directory-kraven, men misslyckas med att ställa in det lokala lösenordet eftersom det inte uppfyller kraven för lokala lösenord. Använd inte den här funktionen om riktlinjerna för lokala lösenord måste vara striktare än riktlinjerna för Active Directory-lösenord.
- Det lokala användarnamnet är inte samma som användarnamnet till Active Directory. Det är bara lösenordet som är samma.

Stöd för smartkort – macOS

Kerberos-tillägget för enkel inloggning har stöd för att använda smartkortbaserade identiteter för autentisering. Smartkort måste ha en CryptoTokenKit-drivenhet. Tokenbaserade drivenheter stöds inte. macOS 10.15 har stöd för PIV-standarden, som i stor utsträckning används av myndigheter i USA.

Kontrollera att Active Directory-domänen är konfigurerad för att ha stöd för smartkortautentisering innan du börjar. Det här dokumentet beskriver inte hur man aktiverar smartkortautentisering för Active Directory. Mer information finns i Microsofts material.

Följ de här stegen för att logga in i Kerberos-tillägget för enkel inloggning med ett smartkort:

1. Klicka på alternativmenyn och välj sedan Use a smart card.
2. Sätt i smartkortet när Identity-knappen visas och klicka på den.
3. Välj den identitet som du vill autentisera med, klicka på OK och sedan på logga in.
4. Ange pin-koden när meddelandet visas.

Man uppmanas att sätta i smartkortet och ange pin-koden om Kerberos-tillägget för enkel inloggning behöver en Kerberos-TGT. Kör ”man SmartCardServices” i Terminal för mer information om stöd för smartkort i macOS.

Distribuerade notiser – macOS

Kerberos-tillägget för enkel inloggning publicerar distribuerade notiser när olika händelser sker. Appar och tjänster i macOS använder distribuerade notiser för att meddela andra appar och tjänster om att en händelse har skett. En app eller tjänst som lyssnar efter den här händelsen kan då vidta en åtgärd.

En administratör kan använda den här funktionen för att utföra en åtgärd när vissa händelser sker. En administratör vill kanske till exempel köra ett skript varje gång som Kerberos-tillägget får en ny Kerberos-inloggningsuppgift.

Kerberos-tillägget för enkel inloggning publicerar bara distribuerade notiser när angivna händelser sker. Det kör inga åtgärder när dessa händelser sker. Administratören måste ange ett verktyg för att lyssna efter dessa notiser och köra åtgärder när de sker.

I bilagan finns ett exempel på ett skript och en launchd-egenskapslista (.plist) som kan lyssna efter notiser och köra åtgärder. Ändra exemplet efter behov så att det passar driftsättningen.

Här visas de distribuerade notiserna som publiceras av Kerberos-tillägget:

Namn	När den publiceras
com.apple.KerberosPlugin.ConnectionCompleted	Kerberos-tillägget för enkel inloggning har kört anslutningsprocessen.
com.apple.KerberosPlugin.ADPasswordChanged	Användaren har ändrat Active Directory-lösenordet med tillägget.
com.apple.KerberosPlugin.LocalPasswordSynced	Användaren har synkroniserat Active Directory-lösenordet och det lokala lösenordet.
com.apple.KerberosPlugin.InternalNetworkAvailable	Användaren har anslutit till ett nätverk där den konfigurerade Active Directory-domänen är tillgänglig.
com.apple.KerberosPlugin.InternalNetworkNotAvailable	Användaren har anslutit till ett nätverk där den konfigurerade Active Directory-domänen inte är tillgänglig.
com.apple.KerberosExtension.gotNewCredential	Användaren har fått en ny Kerberos-TGT.
com.apple.KerberosExtension.passwordChangedWithPasswordSync	Användaren har ändrat Active Directory-lösenordet, och det lokala lösenordet har uppdaterats för att vara samma som det nya Active Directory-lösenordet.

Stöd för kommandorader – macOS

Administratörer kan använda ett kommandoradsverktyg som heter *app-sso* till att styra Kerberos-tillägget för enkel inloggning och få tillgång till användbar information. De kan till exempel använda verktyget för att starta inloggningar, lösenordsändringar och utloggningar. Verktyget kan även skriva ut användbar information, till exempel aktuell inloggad användare, datorns aktuella Active Directory-plats, användarens arbetsresurs på nätverket, när användarens lösenord går ut och mängder av annan användbar information i en egenskapslista eller JSON-format. Den här informationen kan tolkas och laddas upp till en Mac-hanteringslösning för lager och andra syften.

Kör ”app-sso -h” i Terminal-appen för mer information om hur man använder app-sso.

Mobila konton – macOS

Kerberos-tillägget för enkel inloggning kräver inte att Mac-datorn är bunden till Active Directory eller att användaren är inloggad på Mac-datorn med ett mobilt konto. Apple föreslår att man använder Kerberos-tillägget med ett lokalt konto. Lokala konton fungerar bäst med den rekommenderade driftsättningsmodellen för macOS och är det bästa alternativet för dagens Mac-användare, som kanske ansluter till organisationens nätverk regelbundet. Kerberos-tillägget för enkel inloggning skapades specifikt för att förbättra Active Directory-integreringen från ett lokalt konto.

Man kan dock ändå använda Kerberos-tillägget även om man väljer att fortsätta att använda mobila konton. Den här funktionen har följande krav:

- Synkning av lösenord fungerar inte med mobila konton. Om man använder Kerberos-tillägget för att ändra sitt Active Directory-lösenord och man är inloggad på Mac med samma användarkonto som man använder med Kerberos-tillägget så fungerar lösenordsändringar på samma sätt som de gör från inställningspanelen Users & Groups. Om man däremot ändrar ett lösenord externt, det vill säga om man ändrar lösenordet på en webbplats eller om helpdesken återställer det, så kan inte Kerberos-tillägget synka det mobila kontots lösenord med Active Directory-lösenordet igen.
- Det går inte att att använda en URL för att ändra lösenord med Kerberos-tillägget och ett mobilt konto.

Domänområdeskoppling

En administratör kan behöva definiera en anpassad domänområdeskoppling för Kerberos. Organisationen kanske till exempel har ett område som heter ”ad.pretendco.com”, men kanske behöver använda Kerberos-autentisering för resurser i domänen ”fakecompany.com”.

Obs! Kerberos på Apple-operativsystem kan i de allra flesta fall avgöra domänområdeskopplingen automatiskt. Det är väldigt ovanligt att en administratör anpassar de här inställningarna.

Följ de här stegen för att konfigurera domänområdeskoppling för Kerberos-tillägget för enkel inloggning:

1. Lägg till ett objekt som heter domainRealmMapping i avsnittet Custom Configuration i profilen till den utökningsbara enkla inloggningen. Objekttypen ska vara Dictionary.
2. Ställ in nyckeln till ordboken som namnet på området i versaler.
3. Ordbokens värde ska vara av typen Array. Det första värdet ska vara namnet på Kerberos-området i gemener och inledas med punkt. Det andra värdet ska vara namnet på domänen som måste autentiseras mot det här området. Inled även detta med punkt. Lägg till fler arrayer efter behov.

Mer information finns i Kerberos-materialet.

Övergå från Enterprise Connect

Översikt

Kerberos-tillägget för enkel inloggning är tänkt att ersätta Enterprise Connect, som är ett liknande verktyg som många organisationer redan använder. Det flesta organisationer som övergår från Enterprise Connect till Kerberos-tillägget för enkel inloggning kommer att följa de här stegen:

1. Skapa en konfigurationsprofil till Kerberos-tillägget för enkel inloggning som fungerar på liknande sätt som den nuvarande Enterprise Connect-profilen.
2. Avinstallera Enterprise Connect.
3. Driftsätt den nya konfigurationsprofilen till Kerberos-tillägget för enkel inloggning.
4. Be användarna att logga in i Kerberos-tillägget för enkel inloggning.

Det är inte ett krav att övergå till Kerberos-tillägget för enkel inloggning för att uppgradera organisationens Mac-datorer till macOS 10.15. Enterprise Connect fungerar som vanligt med macOS 10.15, men man bör ändå planera för att så småningom övergå från Enterprise Connect.

När bör man inte övergå?

Kerberos-tillägget för enkel inloggning tillgodoser behoven för de allra flesta organisationer som använder Enterprise Connect. Det kan dock hända att organisationer som uppfyller följande kriterier inte kan övergå från Enterprise Connect eller bara kan göra det delvis:

- Organisationer som för närvarande har Mac-datorer som kör macOS 10.14 eller tidigare ska fortsätta att köra Enterprise Connect på de datorerna och bara övergå till Kerberos-tillägget för enkel inloggning på Mac-datorer som kör macOS 10.15. Kerberos-tillägget för enkel inloggning och den tillhörande konfigurationsprofilen fungerar bara på Mac-datorer som kör macOS 10.15. Uppgradera datorerna till macOS 10.15 för att använda Kerberos-tillägget för enkel inloggning.
- Organisationer som använder ett Mac-hanteringsverktyg som inte har stöd för användargodkänd MDM-registrering.
- Organisationer som inte använder ett hanteringsverktyg.
- Organisationer som använder en Active Directory-funktionsnivå för Windows Server 2003 eller tidigare.

Skapa en konfigurationsprofil till Kerberos-tillägget för enkel inloggning

Man behöver skapa en konfigurationsprofil till Kerberos-tillägget för enkel inloggning som påminner om konfigurationsprofilen till Enterprise Connect. Många inställningsnycklar (Preference Keys) i den nuvarande konfigurationsprofilen till Enterprise Connect har motsvarigheter i en profil till Kerberos-tillägget för enkel inloggning. Börja med att gå igenom den här tabellen som visar Kerberos-tilläggets motsvarigheter till Preference Keys i Enterprise Connectr:

Enterprise Connect	Kerberos-tillägg för enkel inloggning	Anteckningar
adRealm	Realm	Området ska skrivas helt med versaler.
Automatic login (enabled by default)	allowAutomaticLogin	Lägg till i avsnittet Custom Configuration. Det måste ställas in som True för att automatisk inloggning ska fungera.
disablePasswordFunctions	allowPasswordChange	Lägg till i avsnittet Custom Configuration. Ställ in som False för att avaktivera lösenordsändringar.
passwordChangeURL	pwChangeURL	Lägg till i avsnittet Custom Configuration.
passwordExpireOverride	pwExpireOverride	Lägg till i avsnittet Custom Configuration.
passwordNotificationDays	pwNotificationDays	Lägg till i avsnittet Custom Configuration.
prepopulatedUsername	principalName	Lägg till i avsnittet Custom Configuration.
pwReqComplexity	pwReqComplexity	Lägg till i avsnittet Custom Configuration.
pwReqHistory	pwReqHistory	Lägg till i avsnittet Custom Configuration.
pwReqLength	pwReqLength	Lägg till i avsnittet Custom Configuration.
pwReqMinimumPasswordAge	pwReqMinAge	Lägg till i avsnittet Custom Configuration.
pwReqText	pwReqText	Lägg till i avsnittet Custom Configuration. Ange en textsträng som ska visas istället för en sökväg till en RTF-fil.
syncLocalPassword	syncLocalPassword	Lägg till i avsnittet Custom Configuration.

Obs! Några inställningsnycklar (Preference Keys) i konfigurationsprofilen till Enterprise Connect kanske inte listas här. Det kan handla om funktioner som inte längre behövs i Kerberos-tillägget för enkel inloggning eller som inte längre stöds.

Avinstallera Enterprise Connect

Det går inte att köra Kerberos-tillägget för enkel inloggning och Enterprise Connect parallellt på samma dator. Avinstallera därför Enterprise Connect när ni har övergått till Kerberos-tillägget. Man behöver administratörsrättigheter för att kunna avinstallera. Följ de här stegen för att avinstallera Enterprise Connect:

Enterprise Connect 2.0 och senare

1. Ta bort Enterprise Connect-agenten genom att starta Terminal-appen och köra ”aunchctl unload / Library/LaunchAgents/com.apple.ecAgent” som den aktuella inloggade användaren.
2. Avsluta Enterprise Connect-menytillbehöret genom att starta Terminal-appen och köra”killall Enterprise\ Connect\ Menu” i Terminal-appen.
3. Radera appen Enterprise Connect från mappen Applications.
4. Radera launchd-listan till Enterprise Connect (med ändelsen .plist) som finns i /Library/LaunchAgents/ com.apple.ecAgent.plist.

Enterprise Connect 1.9.5 och tidigare

1. Avsluta Enterprise Connect genom att ange ”killall Enterprise\ Connect” i Terminal-appen.
2. Radera appen Enterprise Connect från mappen Applications.

I bilagan finns ett exempel på ett skript för att ta bort valfri version av Enterprise Connect.

Enterprise Connect-skriptutlösare

Enterprise Connect kan köra skript när särskilda händelser sker. Enterprise Connect kan till exempel köra ett skript när anslutningen är klar eller när användaren byter lösenord. Kerberos-tillägget för enkel inloggning hanterar inte skript på samma sätt som Enterprise Connect. Tillägget kör inte skript direkt. Istället publiceras en distribuerad notis när en händelse sker. Andra processer kan då lyssna efter notisen och sedan köra ett skript. Läs mer i avsnittet Avancerade funktioner i det här dokumentet.

Här visas Enterprise Connects skriptutlösare och de motsvarande distribuerade notiserna i Kerberos-tillägget för enkel inloggning:

Enterprise Connect	Kerberos-tillägg för enkel inloggning
auditScriptPath	com.apple.KerberosPlugin.InternalNetworkAvailable
connectionCompletedScriptPath	com.apple.KerberosPlugin.ConnectionCompleted
passwordChangeScriptPath	com.apple.KerberosPlugin.ADPasswordChanged

Nätverksresurser

Kerberos-tillägget för enkel inloggning kan inte hantera nätverksresurser, till exempel användarens arbetskatalog på nätverket. Man kan ersätta många av de här funktionerna med skript.

Bilaga

Enhetshanteringsprofil: ExtensibleSingleSignOnKerberos

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

Protokollreferens för MDM

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

Enhetshanteringsprofil: ExtensibleSingleSignOnKerberos.ExtensionData

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

Skriptexempel – Bearbeta distribuerade notiser

Kerberos-tillägget för enkel inloggning publicerar en rad olika distribuerade notiser när olika händelser sker, till exempel när en användare ändrar ett lösenord eller företagets nätverk blir tillgängligt. Som administratör kan man använda ett skript eller en app för att lyssna efter de här notiserna och vidta åtgärder när de publiceras, till exempel köra ett skript eller en kommandotolk.

Nedan visas ett exempel på ett skript som kan köra skript eller kommandon när notiser publiceras. Det ska köras som en LaunchAgent för att köras som den inloggade användaren eller som LaunchDaemon för att köras som rot. Skriptet har två nödvändiga parametrar:

- **-notification** är namnet på den distribuerade notisen som du vill lyssna efter. Exempel finns på sidan 11.
- **-action** är åtgärden som du vill köra när den distribuerade notisen publiceras. Ett exempel är ”sh /path/to/script.sh”.

Man måste installera kommandoradsverktygen för utvecklare för att köra skriptet. Ett installationspaket till de här verktygen finns på Apple Developer-sajten.

```
#!/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()
```

Skriptexempel – Avinstallera Enterprise Connect

Det här skriptexemplet tar bort alla versioner av Enterprise Connect. Kör det från en Mac-hanteringslösning eller manuellt. Skriptet måste köras med root-privilegier.

```
#!/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
```