Kerberos Single Sign-on-udvidelse

Brugervejledning

December 2019

Indhold

Introduktion

Med Kerberos Single Sign-on-udvidelsen (SSO) bliver det nemt at bruge Kerberos-baseret single sign-on sammen med din organisations Apple-enheder.

Forenklet Kerberos-godkendelse

Kerberos SSO-udvidelsen forenkler processen med at hente en Kerberos-billet med tildeling af billet (TGT) fra din organisations Active Directory-domæne, der giver brugere mulighed for problemfrit at godkende ressourcer som websites, programmer og filservere. På macOS henter Kerberos SSO-udvidelsen proaktivt en Kerberos TGT ved ændringer i netværksstatus for at sikre, at brugeren er klar til at godkende, når det kræves.

Administration af Active Directory-konto

Kerberos SSO-udvidelsen hjælper også brugerne til at administrere deres Active Directory-konti. På macOS giver den brugerne mulighed for at ændre deres Active Directory-adgangskode og giver dem besked, når en adgangskode er ved at udløbe. Brugere kan også ændre deres adgangskode til deres lokale konto, så den er den samme som deres Active Directory-adgangskode.

Understøttelse af Active Directory

Kerberos SSO-udvidelsen bør bruges sammen med et lokalt Active Directory-domæne. Azure Active Directory understøttes ikke. For at bruge Kerberos SSO-udvidelsen behøver enhederne ikke at være knyttet til et Active Directory-domæne. Desuden behøver brugerne ikke at logge ind på deres Mac-computer med Active Directory eller mobilkonti; i stedet anbefaler Apple at bruge lokale konti.

Krav

- iOS 13, iPadOS eller macOS Catalina.
- Et Active Directory-domæne med Windows Server 2008 eller nyere installeret. Kerberos SSO-udvidelsen er ikke beregnet til at blive brugt sammen med Azure Active Directory. Den kræver et traditionelt Active Directory-domæne i det lokale miljø.
- Adgang til netværket, hvor Active Directory-domænet er hostet. Denne netværksadgang kan ske gennem Wi-Fi, Ethernet eller VPN.
- Enheder skal administreres med en løsning til administration af mobile enheder (MDM) med understøttelse af Extensible Single Sign-on-konfigurationsbeskrivelse for payload (SSO). Kontakt jeres MDM-leverandør for at høre om dennes understøttelse af konfigurationsbeskrivelsen for payload.

Enterprise Connect

Hensigten med Kerberos SSO-udvidelsen er at erstatte Enterprise Connect. Hvis I bruger Enterprise Connect og ønsker at overgå til Kerberos SSO-udvidelsen, henvises I til afsnittet "Transitioning from Enterprise Connect" i dette dokument for yderligere oplysninger.

Kom godt i gang

Udarbejdelse og anvendelse af en konfigurationsbeskrivelse

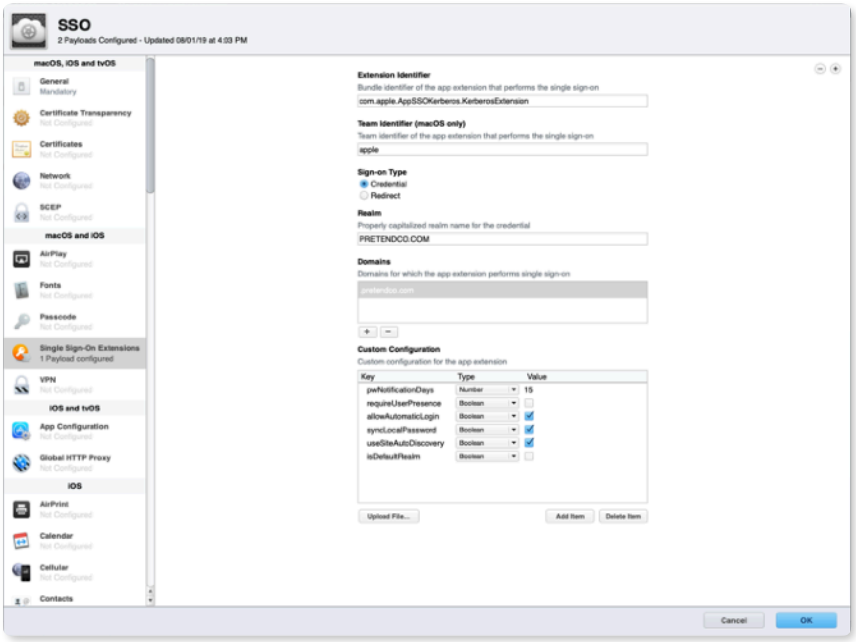
For at bruge Kerberos SSO-udvidelsen skal I konfigurere den ved hjælp af en konfigurationsbeskrivelse, der leveres til enheden fra en MDM-løsning.

Bemærk: Konfigurationsbeskrivelsen skal leveres til enheden af MDM. På macOS skal det være en brugergodkendt MDM-registrering og installeret i systemet. Manuel tilføjelse af beskrivelsen understøttes ikke.

For at konfigurere med en konfigurationsbeskrivelse skal I bruge det Extensible Single Sign-on-payload, der blev introduceret i iOS 13, iPadOS og macOS 10.15. Profile Manager, der er en del af macOS Server, omfatter understøttelse af Extensible Single Sign-on-payload. Hvis jeres MDM-løsning endnu ikke understøtter dette payload, vil I muligvis kunne udarbejde den nødvendige beskrivelse i Profile Manager og derefter importere den i jeres MDM-løsning til distribution. Kontakt jeres MDM-leverandør for at få flere oplysninger.

For at udarbejde en konfigurationsbeskrivelse ved hjælp af Profile Manager skal I følge disse trin:

1. Log ind på Profile Manager.
2. Opret en profil for en enhedsgruppe eller en specifik enhed.
3. Vælg Single Sign-On-udvidelserne i Payload-listen, og klik dernæst på knappen Add (+) for at tilføje et nyt payload.
4. I feltet Extension Identifier skal I indtaste "com.apple.AppSSOKerberos.KerberosExtension."
5. Indtast "apple" i feltet Team Identifier.



6. Vælg Credential under Sign-on Type.
7. I feltet Realm skal I indtaste navnet på det Active Directory-domæne, hvor jeres brugerkonti er. Skriv navnet med store bogstaver. Brug ikke navnet på jeres Active Directory-skov, medmindre jeres brugerkonti er på skovniveau.

8. Klik på knappen Add (+) under Domains, og tilføj domæner for alle ressourcer, der bruger Kerberos. Hvis I f.eks. bruger Kerberos-godkendelse med ressourcer i us.pretendco.com, skal I tilføje ".us.pretendco.com." (Glem ikke punktummet i starten.)
9. Tilføj følgende værdier under Custom Configuration:

Key	Type	Value
pwNotificationDays	Number	15
requireUserPresence	Boolean	Ikke kontrolleret
allowAutomaticLogin	Boolean	Kontrolleret
syncLocalPassword	Boolean	Kontrolleret
useSiteAutoDiscovery	Boolean	Kontrolleret
isDefaultRealm	Boolean	Ikke kontrolleret

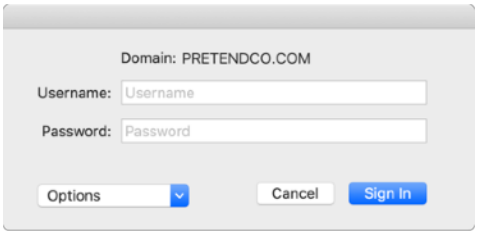
10. Klik på OK for at gemme den nye konfigurationsbeskrivelse. Den vil automatisk blive installeret på den valgte enhed eller enhedsgruppe.

Brugerindstilling – iOS og iPadOS

1. Tilslut din enhed til et netværk, hvor jeres organisations Active Directory-domæne er tilgængeligt.
2. Gør ét af følgende:
   - Brug Safari til at få adgang til et website, der understøtter Kerberos-godkendelse.
   - Åbn et program, der understøtter Kerberos-godkendelse.
3. Indtast brugernavn og adgangskode til Kerberos eller Active Directory.
4. Du vil blive spurgt, om du ønsker at logge automatisk på fremover. De fleste brugere trykker Yes.
5. Tryk på Sign In. Efter en kort pause indlæses websitet eller programmet. Hvis du vælger at logge ind automatisk på Kerberos SSO-udvidelsen, vil du kun blive bedt om brugeroplysninger, hvis du skifter adgangskode. Hvis du ikke har valgt at logge ind automatisk, vil du kun blive bedt om brugeroplysninger, når dine Kerberos-brugeroplysninger udløber – normalt efter 10 timer.

Brugerindstilling – macOS

1. Du skal godkende Kerberos SSO-udvidelsen. Du kan begynde processen på flere måder:
   - Hvis din Mac er forbundet med det netværk, hvor jeres Active Directory-domæne er tilgængeligt, vil du blive bedt om at godkende umiddelbart efter, at Extensible SSO-konfigurationsbeskrivelsen er installeret.
   - Hvis du bruger Safari til at tilgå et website, som accepterer Kerberos-godkendelse, eller du bruger et program, der kræver Kerberos-godkendelse, vil du blive bedt om at godkende.
   - Du vil øjeblikkeligt blive bedt om at godkende, hver gang du forbinder din Mac med et netværk, hvor jeres Active Directory er tilgængeligt.
   - Du kan vælge Kerberos SSO-udvidelsens ekstramenu, og dernæst klikke på Sign In.
2. Du vil blive bedt om Kerberos-brugeroplysninger. Indtast brugernavn og adgangskode til Kerberos eller Active Directory.



3. Du vil blive spurgt, om du ønsker at logge automatisk på. De fleste brugere trykker Yes.
4. Klik på Sign In. Efter en kort pause indlæses websitet eller programmet. Hvis du vælger at logge ind automatisk på Kerberos SSO-udvidelsen, vil du kun blive bedt om brugeroplysninger, hvis du skifter adgangskode. Hvis du ikke har valgt at logge ind automatisk, vil du kun blive bedt om brugeroplysninger, når dine Kerberos-brugeroplysninger udløber – normalt efter 10 timer.
5. Hvis din adgangskode er tæt på at udløbe, får du besked om, hvor mange dage du har, til den udløber. Du kan klikke på notifikationen og ændre din adgangskode.
6. Hvis du har slået funktionen til adgangskodesynkronisering til, vil du blive bedt om din nuværende adgangskode til Active Directory og din lokale adgangskode. Indtast begge, og klik dernæst på OK for at synkronisere adgangskoderne. Du vil se denne anmodning, første gang du logger ind, også selvom dine adgangskoder allerede er synkroniserede.

Ændring af adgangskode – macOS

Du kan også ændre din Active Directory-adgangskode med Kerberos SSO-udvidelsen:

1. Sørg for, at du har logget ind på Kerberos SSO-udvidelsen.
2. Vælg Kerberos SSO-ekstramenuen, og vælg Change Password. Du får muligvis en notifikation om, at din adgangskode er ved at udløbe.
3. Indtast din nuværende adgangskode, og dernæst din nye adgangskode. Sørg for, at den nye adgangskode opfylder din organisations krav til adgangskoder. Klik på OK.
4. Efter en kort pause vil du se en dialogboks, der fortæller dig, at adgangskoden er ændret. Hvis funktionen adgangskodesynkronisering er slået til, vil adgangskoden til din lokale konto blive opdateret, så den er den samme som din nye Active Directory-adgangskode.

Brug af Kerberos SSO-ekstramenuen – macOS

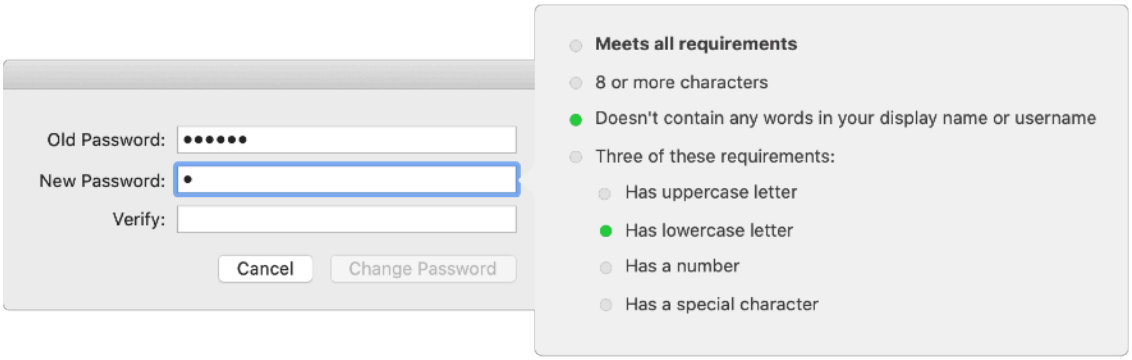
Kerberos SSO-ekstramenuen giver nem adgang til nyttige oplysninger om din konto og udvidelsens funktioner. Den vises som en grå eller sort tast i menulinjen øverst til højre.

For at få statusinformation om din konto skal du først se, hvilken farve Kerberos-ekstramenuens ikon har. Hvis tasten er grå, er du ikke logget ind på Kerberos SSO-udvidelsen. Hvis tasten er sort, er du logget ind. Når du har valgt tasten, vil du se den konto, du er logget ind på, samt hvor mange dage der er, til din adgangskode udløber. Du kan også logge ind, logge ud og ændre adgangskode via menuen.

Avancerede funktioner

Livetesting af adgangskode

I mange Active Directory-konfigurationer kan Kerberos SSO-udvidelsen teste nye brugeradgangskoder, samtidig med at de indtastes, og oplyse brugerne om, hvilke krav til adgangskoder de skal overholde, når de ændrer deres adgangskode. Når den er konfigureret, vil brugeren se dette, når han/hun indtaster den nye adgangskode:



For at bruge denne funktion må jeres Active Directory-domæne kun have standardpolitikker om brug af adgangskoder til Active Directory. Som standard giver Active Directory mulighed for, at en administrator kan kræve, at en adgangskode skal være kompleks og af en vis længde. På technet.microsoft.com/en-us/library/cc786468(v=ws.10).aspx kan du se, hvad en kompleks adgangskode består af.

Bemærk: Du kan muligvis ikke se denne funktion, hvis dit domæne bruger værktøjer fra tredjeparter, eller DLL til at udvide standardpolitikken for adgangskoder til Active Directory. Hvis du, ud over dit brugernavn, ikke kan anvende visse ord i din adgangskode, eller du skal bruge et bestemt antal særlige tegn i adgangskoden, bruger du sandsynligvis udvidede adgangskodepolitikker fra tredjeparter. Hvis du er usikker, kan du bede din Active Directory-administrator om yderligere oplysninger.

Hvis din organisations Active Directory-domæne opfylder kravene, kan du slå livetesting af adgangskode til. I konfigurationsbeskrivelsen til Kerberos SSO-udvidelse skal I indstille følgende parametre:

Parameter	Key	Type	Value	Valgfrit
Kræv komplekse adgangskoder	pwReqComplexity	Boolean	JA	Nej
Påkrævet adgangskodelængde	pwReqLength	Integer	Tal	Ja
Genbrug tidligere adgangskodegrænse	pwReqHistory	Integer	Tal	Ja
Minimumsalder for adgangskode	pwReqMinAge	Integer	Tal	Ja

Livetesting af adgangskode har nogle begrænsninger. Det kan ikke teste, om en adgangskode allerede er i brug. Det kan heller ikke teste, om din adgangskode indeholder dit Active Directory-visningsnavn, medmindre du allerede har en Kerberos-TGT. Det kan være tilfældet, hvis du indstiller din adgangskode for første gang, eller hvis din adgangskode er udløbet. Alle andre tests vil virke normalt.

Visning af adgangskodekrav

Hvis du ikke kan bruge livetesting af adgangskode, kan du konfigurere Kerberos SSO-udvidelsen til at vise en tekststreng med din organisations krav til adgangskoder, når brugeren indtaster den nye adgangskode. I konfigurationsbeskrivelsen til Kerberos SOS-udvidelsen sættes "pwReqText" til en streng, der indeholder den tekst, som du ønsker, en bruger skal se i forbindelse med ændring af adgangskode.

Ændring eller deaktivering af adgangskodefunktionalitet

Nogle organisationer kan måske ikke bruge standardfunktionaliteten for ændring af adgangskode i Kerberos SSO-udvidelsen, da de ikke tillader adgangskodeændringer til Active Directory. I jeres konfigurationsbeskrivelse for Kerberos SSO-udvidelsen skal I indstille "allowPasswordChanges" til FALSE for at deaktivere funktionen.

Websitesupport til ændring af adgangskode – macOS

Kerberos SSO-udvidelsen kan konfigureres til at åbne et website i standardbrowseren, hvor adgangskode kan ændres, når brugeren vælger "Change password" eller bekræfter en besked om udløb af adgangskode. Apple anbefaler, at man kun bruger denne funktion, når man bruger en lokal konto, da mobilkonti ikke er understøttet.

I jeres konfigurationsbeskrivelse for Kerberos SSO-udvidelse skal I angive "pwChangeURL" som URL for det website, hvor adgangskode kan ændres. Når brugerne har ændret deres adgangskode, skal de logge ud af Kerberos-udvidelsen, og dernæst logge ind igen med deres opdaterede adgangskode. Hvis lokal synkronisering af adgangskode er slået til, kan brugerne guides med hensyn til, hvordan de får synkroniseret deres adgangskoder igen.

Synkronisering af adgangskode – macOS

Kerberos SSO-udvidelsen kan sætte adgangskoden til den lokale konto til at være den samme som brugerens adgangskode til Active Directory. Denne funktion aktiveres ved at sætte "syncLocalPassword" til TRUE i afsnittet Custom Configuration i konfigurationsbeskrivelsen for Kerberos SSO-udvidelsen.

Adgangskodesynkronisering omfatter to basale funktioner. Hvis brugerne bruger Kerberos SSO-udvidelsen til at ændre adgangskoden, indstiller funktionen brugerens lokale adgangskode til at være den samme som deres Active Directory-adgangskode. Hvis den lokale adgangskode og adgangskoden til Active Directory kommer ud af sync, synkroniserer Kerberos SSO-udvidelsen dem igen således:

- Ved at slå synkronisering af adgangskoder til, og når Kerberos SSO-udvidelsen efterfølgende forsøger at oprette forbindelse, bliver de datoer, hvor brugeren sidst ændrede lokal adgangskode og adgangskode til Active Directory sammenlignet med cached værdier. Hvis værdierne stemmer overens, er adgangskoderne synkroniserede, og yderligere handling er ikke påkrævet. Hvis de ikke stemmer overens, vil Kerberos SSO-udvidelsen bede brugerne om deres lokale adgangskode og adgangskoden til Active Directory. Når brugerne angiver deres lokale adgangskode, indstiller Kerberos SSO-udvidelsen den lokale adgangskode til at være den samme som deres adgangskode til Active Directory.
- Ændringer af adgangskode sker på samme måde. Når brugerne ændrer adgangskode med Kerberos SSO-udvidelsen, tjekkes deres gamle adgangskode til Active Directory op mod den lokale konto. Hvis en gammel adgangskode til Active Directory og den lokale adgangskode er den samme, ændrer Kerberos SSO-udvidelsen begge adgangskoder. Hvis de ikke er ens, er det kun adgangskoden til Active Directory, der ændres. Brugerne bliver bedt om at angive deres lokale adgangskode ved næste forsøg på at oprette forbindelse.

Denne funktion har følgende krav:

- Hvis brugerne har logget ind på deres Mac-computer med en Active Directory-kontoen og ikke en lokal konto, slås synkronisering af adgangskode fra. Funktionen er kun til brug sammen med lokale konti; hvis brugerne har logget ind på deres Mac-computer med en Active Directory-konto, er denne funktion ikke nødvendig.
- Hvis der gælder en politik for adgangskoder til lokale konti – f.eks. som følge af en konfigurationsbeskrivelse eller ved at bruge pwpolicy-kommandoen – så sørg for, at den lokale adgangskodepolitik matcher eller er mindre streng end adgangskodepolitikken for Active Directory. Hvis den lokale adgangskodepolitik er strengere end politikken for Active Directory, kan Kerberos SSO-udvidelsen acceptere en adgangskode, som opfylder Active Directory-kravene, men kan ikke indstille den lokale adgangskode, da den ikke opfylder kravene til lokale adgangskoder. Hvis politikken for lokale adgangskoder skal være strengere end adgangskodepolitikken for Active Directory, bør I ikke bruge denne funktion.
- Det lokale brugernavn er forskelligt fra Active Directory-brugernavnet – kun adgangskoder kan være de samme.

Understøttelse af smartcard – macOS

Kerberos SSO-udvidelsen understøtter brugen af smartcard-baserede identiteter til godkendelse. Smartcards skal have adgang til en CryptoTokenKit-driver; token-baserede drivere understøttes ikke. macOS 10.15 understøtter PIV-standarden, som i vid udstrækning bruges af den amerikanske regering.

Inden I begynder, skal I sikre jer, at jeres Active Directory-domæne er konfigureret til at understøtte smartcard-godkendelse. Processen med at aktivere smartcard-godkendelse til Active Directory falder uden for dette dokuments rammer. Se Microsofts dokumentation for yderligere oplysninger.

For at logge ind på Kerberos SSO-udvidelsen med et smartcard skal du følge disse trin:

1. Klik på menuen Options, og vælg dernæst "Use a smart card".
2. Når du ser knappen Identity, skal du sætte dit smartcard i og trykke på knappen.
3. Vælg den identitet, du ønsker at godkende med, klik på OK, og dernæst på Sign In.
4. Indtast din PIN-kode, når du bliver bedt om det.

Hvis Kerberos SSO-udvidelsen kræver en Kerberos-TGT, vil du blive bedt om at sætte dit smartcard i og indtaste din PIN-kode. I kan se flere oplysninger om understøttelse af smartcard i macOS ved at køre "man SmartCardServices" i Terminal.

Distribuerede notifikationer – macOS

Kerberos SSO-udvidelsen viser distribuerede notifikationer, når diverse hændelser indtræffer. Programmer og tjenester i macOS bruger distribuerede notifikationer for at fortælle andre programmer og tjenester, at en hændelse er indtruffet. Et program eller en tjeneste, der lytter efter en sådan hændelse, kan reagere, når den indtræffer.

En administrator kan bruge denne funktionalitet til at udføre en handling, når visse hændelser indtræffer. For eksempel kan en administrator ønske at køre et script, hver gang Kerberos SSO-udvidelsen kræver en ny Kerberos-brugeroplysning.

Kerberos SSO-udvidelsen viser ganske enkelt distribuerede notifikationer, når angivne hændelser indtræffer. Den foretager ikke handlinger, når disse hændelser indtræffer. Administratoren skal levere et værktøj, der lytter efter disse notifikationer og kører handlinger, når de vises.

Appendikset indeholder et eksempel på et script og en åbnet egenskabsliste (.plist), der kan lytte efter notifikationer og køre handlinger. Hvis du ønsker det, kan I ændre dette eksempel, så det passer til jeres implementering.

Se de distribuerede notifikationer, som Kerberos SSO-udvidelsen viser, nedenfor.

Navn	Når det sendes ud
com.apple.KerberosPlugin.ConnectionCompleted	Kerberos SSO-udvidelsen har kørt forbindelsesprocessen.
com.apple.KerberosPlugin.ADPasswordChanged	Brugeren har ændret Active Directory-adgangskoden med udvidelsen.
com.apple.KerberosPlugin.LocalPasswordSynced	Brugeren har synkroniseret Active Directory-adgangskoden og den lokale adgangskode.
com.apple.KerberosPlugin.InternalNetworkAvailable	Brugeren har oprettet forbindelse til et netværk, hvor det konfigurerede Active Directory-domæne er tilgængeligt.
com.apple.KerberosPlugin.InternalNetworkNotAvailable	Brugeren har oprettet forbindelse til et netværk, hvor det konfigurerede Active Directory-domæne ikke er tilgængeligt.
com.apple.KerberosExtension.gotNewCredential	Brugeren har erhvervet et nyt Kerberos-TGT.
com.apple.KerberosExtension.passwordChangedWithPasswordSync	Brugeren har ændret adgangskoden til Active Directory, og den lokale adgangskode er blevet opdateret, så den er den samme som den nye Active Directory-adgangskode.

Understøttelse af kommandolinje – macOS

Administratorer kan bruge en kommandolinje, som hedder *app-sso*, til at styre Kerberos SSO-udvidelsen og tilgå nyttig information. De kan for eksempel bruge værktøjet til at starte login, ændring af adgangskode og logud. Det kan også udskrive nyttig information, som f.eks. hvilken bruger der aktuelt er logget ind, computerens nuværende Active Directory-site, brugerens netværksdeling, når brugerens adgangskode udløber og en række andre nyttige oplysninger i en egenskabsliste eller i JSON-format. Disse oplysninger kan analyseres og uploades til en Mac-administrationsløsning for status og andre formål.

Kør "app-sso -h" i programmet Terminal for at få flere oplysninger om, hvordan app-sso bruges.

Mobilkonti – macOS

Kerberos SSO-udvidelsen kræver ikke, at din Mac er knyttet til Active Directory, eller at brugeren er logget på Mac-computeren med en mobilkonto. Apple foreslår, at I bruger Kerberos SSO-udvidelsen med en lokal konto: Lokale konti fungerer bedst med den anbefalede implementeringsmodel til macOS og er det bedste valg for moderne Mac-brugere, som skal oprette sporadisk forbindelse til jeres organisations netværk. Kerberos SSO-udvidelsen blev specielt udviklet for at styrke integrationen af Active Directory fra en lokal konto.

Men selvom I vælger fortsat at bruge mobilkonti, kan I stadig bruge Kerberos SSO-udvidelsen. Denne funktion har følgende krav:

- Synkronisering af adgangskoder fungerer ikke med mobilkonti. Hvis du bruger Kerberos SSO-udvidelsen til at ændre din Active Directory-adgangskode, og du er logget ind på din Mac med samme brugerkonto, som du bruger til Kerberos SSO-udvidelsen, fungerer adgangskodeændringer på samme måde som fra indstillingsvinduet for Users & Groups. Men hvis du ændrer adgangskoden eksternt, dvs. hvis du ændrer din adgangskode på et website, eller din helpdesk nulstiller den, kan Kerberos SSO-udvidelsen ikke synkronisere adgangskoden til din mobilkonto med Active Directory-adgangskoden igen.
- Brug af en URL til ændring af adgangskode med Kerberos-udvidelsen og en mobilkonto understøttes ikke.

Kortlægning af domæne-område

En administrator kan have brug for at definere en specialkortlægning af et domæne-område for Kerberos. En organisation kan f.eks. have et Kerberos-område, der hedder "ad.pretendco.com", men kan have behov for at bruge Kerberos-godkendelse til ressourcer i"fakecompany.com"-domænet.

Bemærk: Implementering af Kerberos på Apples styresystemer kan automatisk fastlægge kortlægning af domæne-område i næsten alle situationer. Det er meget sjældent, at en administrator tilpasser disse indstillinger.

Kortlægning af domæne-område kan konfigureres for Kerberos SSO-udvidelsen ved at følge disse trin:

1. I afsnittet Custom Configuration i Extensible SSO-beskrivelsen tilføjes et objekt benævnt domainRealmMapping. Objekttypen bør være Dictionary.
2. Angiv nøglen til dette dictionary til at være navnet på dit område skrevet med store bogstaver.
3. Indstil dictionary-værdien til typen Array. Den første værdi skal være navnet på dit Kerberos-område skrevet med små bogstaver og startende med et punktum. Den anden værdi skal være navnet på det domæne, der skal godkendes i forhold til området, og igen startende med et punktum. Tilføj arrays efter behov.

Se Kerberos-dokumentation for flere oplysninger.

Overgang fra Enterprise Connect

Oversigt

Det er hensigten, at Kerberos SSO-udvidelsen skal erstatte Enterprise Connect, et lignende værktøj, som mange organisationer allerede bruger. De fleste organisationer, der overgår fra Enterprise Connect til Kerberos SSO-udvidelsen, vil følge disse trin:

1. Udarbejd en konfigurationsbeskrivelse for Kerberos SSO-udvidelsen, som giver en lignende funktionalitet som konfigurationsbeskrivelsen for jeres nuværende Enterprise Connect har.
2. Afinstaller Enterprise Connect.
3. Implementer konfigurationsbeskrivelsen for den nye Kerberos SSO-udvidelse.
4. Få brugerne til at logge ind på Kerberos SSO-udvidelsen.

Det er ikke nødvendigt at overgå til Kerberos SSO-udvidelsen for at opgradere jeres organisations Mac-computere til macOS 10.15. Enterprise Connect fungerer som ventet med macOS 10.15, men organisationer bør stadig planlægge en eventuel overgang fra Enterprise Connect.

Hvem skal ikke overgå

Kerberos SSO-udvidelsen opfylder behovene hos langt størstedelen af de organisationer, der bruger Enterprise Connect. Imidlertid kan en organisation, som opfylder følgende kriterier, muligvis ikke overgå fra Enterprise Connect, eller kan måske kun overgå delvist:

- En organisation, som for nuværende har Mac-computere med macOS 10.14 eller ældre, skal lade Enterprise Connect fortsat køre på disse systemer, og kun lade Mac-computere med macOS 10.15 overgå til Kerberos SSO-udvidelsen. Kerberos SSO-udvidelsen og dens tilhørende konfigurationsbeskrivelse fungerer kun på Mac-computere med macOS 10.15. Opgrader disse systemer til macOS 10.15 for at kunne benytte Kerberos SSO-udvidelsen.
- En organisation, der bruger et Mac-administrationsværktøj, som ikke understøtter brugergodkendt MDM-registrering.
- En organisation, der ikke bruger et administrationsværktøj.
- En organisation, der bruger et Active Directory-funktionsniveau af Windows Server 2003 eller ældre.

Udarbejdelse af en konfigurationsbeskrivelse for Kerberos SSO-udvidelse.

I skal udarbejde en konfigurationsbeskrivelse for Kerberos SSO-udvidelsen, som svarer til konfigurationsbeskrivelsen for Enterprise Connect. Mange preference keys i jeres nuværende konfigurationsbeskrivelse til Enterprise Connect har tilsvarende preference keys i en konfigurationsbeskrivelse til Kerberos SSO-udvidelsen. Start med at se nedenstående tabel, som indeholder et kort over Kerberos SSO-udvidelsens preference keys svarende til preference keys I Enterprise Connect.

Enterprise Connect	Kerberos SSO-udvidelse	Noter
adRealm	Realm	Realm skal skrives udelukkende med store bogstaver.
Automatic login (enabled by default)	allowAutomaticLogin	Tilføj til afsnittet Custom Configuration. Det skal sættes til True, for at automatisk login virker.
disablePasswordFunctions	allowPasswordChange	Tilføj til afsnittet Custom Configuration. Sæt til False for at deaktivere adgangskodeændringer.
passwordChangeURL	pwChangeURL	Tilføj til afsnittet Custom Configuration.
passwordExpireOverride	pwExpireOverride	Tilføj til afsnittet Custom Configuration.
passwordNotificationDays	pwNotificationDays	Tilføj til afsnittet Custom Configuration.
prepopulatedUsername	principalName	Tilføj til afsnittet Custom Configuration.
pwReqComplexity	pwReqComplexity	Tilføj til afsnittet Custom Configuration.
pwReqHistory	pwReqHistory	Tilføj til afsnittet Custom Configuration.
pwReqLength	pwReqLength	Tilføj til afsnittet Custom Configuration.
pwReqMinimumPasswordAge	pwReqMinAge	Tilføj til afsnittet Custom Configuration.
pwReqText	pwReqText	Tilføj til afsnittet Custom Configuration. Lav en tekststreng, der skal vises i stedet for en sti til en RTF-fil.
syncLocalPassword	syncLocalPassword	Tilføj til afsnittet Custom Configuration.

Bemærk: Nogle preference keys i jeres konfigurationsbeskrivelse til Enterprise Connect er muligvis ikke medtaget her. De kan vedrøre funktioner, som der ikke længere er brug for i Kerberos SSO-udvidelsen, eller som ikke længere er understøttet.

Afinstallering af Enterprise Connect

Kørsel af Kerberos SSO-udvidelsen og Enterprise Connect sideløbende på samme computer understøttes ikke. Efter overgang til Kerberos SSO-udvidelsen skal Enterprise Connect afinstalleres. Du skal have administratorrettigheder for at foretage afinstalleringen. For at afinstallere Enterprise Connect skal du følge nedenstående trin:

Enterprise Connect 2.0 og nyere

1. Fjern Enterprise Connect-agenten ved at åbne programmet Terminal og køre "launchctl unload /Library/LaunchAgents/com.apple.ecAgent" som den bruger, der er logget ind aktuelt.
2. Forlad Enterprise Connect-ekstramenuen ved at åbne programmet Terminal og indtaste "killall Enterprise\ Connect\ Menu" i programmet Terminal.
3. Slet Enterprise Connect-programmet fra mappen Applications.
4. Slet Enterprise Connect launchd .plist på /Library/LaunchAgents/com.apple.ecAgent.plist.

Enterprise Connect 1.9.5 og ældre

1. Afslut Enterprise Connect ved at indtaste "killall Enterprise\ Connect" i programmet Terminal.
2. Slet Enterprise Connect-programmet fra mappen Applications.

Appendikset viser et eksempelscript, der fjerner alle versioner af Enterprise Connect.

Enterprise Connect-scriptudløsere

Enterprise Connect kan køre scripts, når visse hændelser indtræffer. For eksempel kan Enterprise Connect køre et script, når det afslutter forbindelsesoprettelsesprocessen, eller når brugeren ændrer adgangskode. Kerberos SSO-udvidelsen håndterer scripts anderledes end Enterprise Connect. Den kører ikke scripts direkte. I stedet sender den en distribueret notifikation, når en hændelse indtræffer. Andre processer lytter så efter notifikationen og kører derefter et script. Se yderligere oplysninger i afsnittet "Advanced Functions" i dette dokument.

Nedenfor er der henvisninger til Enterprise Connects scriptudløsere og deres tilsvarende distribuerede notifikationer i Kerberos SSO-udvidelsen:

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

Netværksdelinger

Kerberos SSO-udvidelsen understøtter ikke håndteringen af netværksdelinger, f.eks. brugerens netværkshjemmemappe. Du kan erstatte meget af denne funktionalitet med scripts.

Appendiks

Beskrivelse af enhedsadministration: ExtensibleSingleSignOnKerberos

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

Oplysninger om protokol for administration af mobile enheder

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

Beskrivelse af enhedsadministration: ExtensibleSingleSignOnKerberos.ExtensionData

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

Eksempelscript – Behandling af distribuerede notifikationer

Kerberos SSO-udvidelsen sender en række distribuerede notifikationer, når diverse hændelser indtræffer, som f.eks. når brugeren ændrer adgangskode, eller virksomhedsnetværket går online. Som administrator kan du bruge et script eller program til at lytte efter disse notifikationer og handle derpå, når de sendes, f.eks. køre et script eller en shell-kommando.

Nedenfor er der et eksempelscript, som kan køre scripts eller kommandoer, når der sendes notifikationer. Det skal udføres som en LaunchAgent for at køre som brugeren, der er logget ind, eller LaunchDaemon for at køre som rod. Scriptet kræver to nødvendige parametre:

- **-notification** er navnet på den distribuerede notifikation, som du vil lytte efter. Se eksempler på side 11.
- **-action** er den handling, du ønsker at udføre, når den distribuerede notifikation er sendt. Et eksempel er "sh /path/to/script.sh."

For at køre scriptet skal du installere udviklerværktøjer til kommandolinjer. En installationspakke for disse værktøjer er tilgængelig på Apple Developer-websitet.

```
#!/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 = Proces()
        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()
```

Eksempelscript – Afinstallering af Enterprise Connect

Dette eksempelscript fjerner alle versioner af Enterprise Connect. Udfør det fra en Mac-administrationsløsning eller manuelt. Scriptet skal køre med rodprivilegier.

```
#!/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
```