Kerberos Single Sign-on-utvidelse

Brukerhåndbok

Desember 2019

Innhold

Introduksjon **3**

Kom i gang **4**

Avanserte funksjoner **8**

Bytte fra Enterprise Connect **13**

Tillegg **16**

Introduksjon

Med Kerberos Single Sign-on-utvidelsen (SSO) blir det enkelt å bruke Kerberos-basert SSO med organisasjonens Apple-enheter.

Forenklet Kerberos-autentisering

Kerberos SSO-utvidelsen forenkler prosessen med å skaffe en Kerberos tilgangsbillett (TGT) fra organisasjonens Active Directory-domene, slik at brukere kan bli sømløst autentisert for ressurser som nettsteder, apper og filtjenere. I macOS vil Kerberos SSO-utvidelsen proaktivt hente en Kerberos TGT ved endringer i nettverkstilstand, slik at brukeren er klar til autentisering ved behov.

Administrering av Active Directory-kontoer

Kerberos SSO-utvidelsen hjelper også brukere med å administrere Active Directory-kontoene sine. I macOS kan brukere endre Active Directory-passord, og de blir også varslet når et passord utløper snart. Brukere kan også endre sitt lokale passord for å tilpasse det til Active Directory-passordet.

Støtte for Active Directory

Kerberos SSO-utvidelsen skal brukes med et lokalt Active Directory-domene. Azure Active Directory støttes ikke. Enheter trenger ikke å være koblet til et Active Directory-domene for å kunne bruke Kerberos SSO-utvidelsen. Apple anbefaler at brukerne logger på Macen med lokal konto i stedet for med Active Directory- eller mobilkonto.

Krav

- iOS 13, iPadOS eller macOS Catalina.
- Et Active Directory-domene som kjører Windows Server 2008 eller nyere. Kerberos SSO-utvidelsen er ikke utviklet for Azure Active Directory. Den krever et tradisjonelt lokalt Active Directory-domene.
- Tilgang til nettverket der Active Directory-domene ligger. Tilgang til nettverket kan være via Wi-Fi, Ethernet eller VPN.
- Enhetene må administreres med en MDM-løsning (administrering av mobile enheter) som støtter Extensible Single Sign-on (SSO) konfigurasjonsprofilnyttelast. Kontakt MDM-leverandøren for å få hjelp med denne konfigurasjonsprofilnyttelasten.

Enterprise Connect

Kerberos SSO-utvidelsen skal erstatte Enterprise Connect. Hvis du bruker Enterprise Connect og vil bytte til Kerberos SSO-utvidelsen, finner du mer informasjon i delen «Bytte fra Enterprise Connect».

Kom i gang

Lage og rulle ut en konfigurasjonsprofil

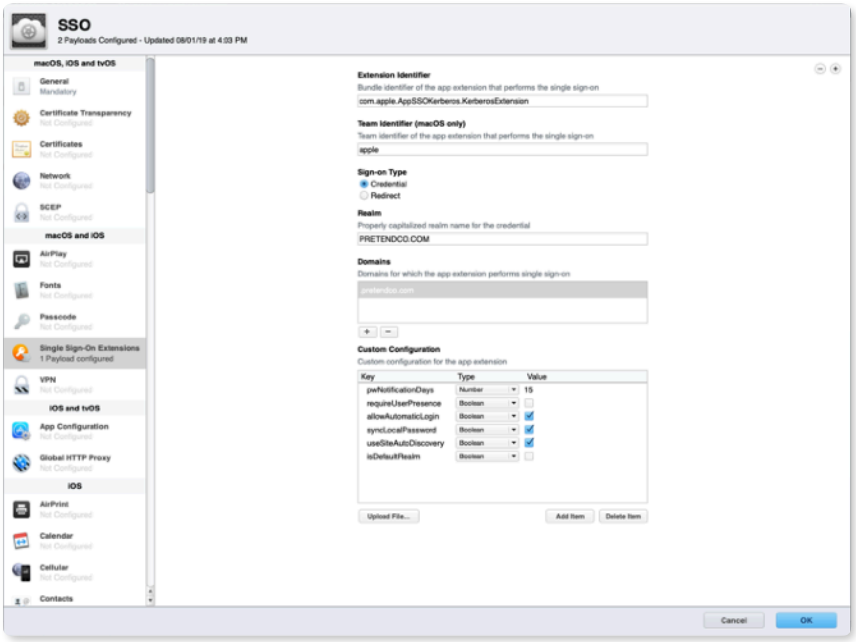
For å bruke Kerberos SSO-utvidelsen må du konfigurere den ved hjelp av en konfigurasjonsprofil som leveres til enheten fra en MDM-løsning.

Merk: Konfigurasjonsprofilen må leveres til enheten fra MDM. I macOS må det være en brukergodkjent MDM-registrering, og den må være installert i systemdefinisjonsområdet. Profilen kan ikke legges til manuelt.

For å konfigurere med en konfigurasjonsprofil må du bruke Extensible Single Sign-on-nyttelasten som ble innført i iOS 13, iPadOS og macOS 10.15. Profile Manager, som er en del av macOS Server, støtter Extensible Single Sign-on-nyttelast. Hvis MDM-løsningen din ikke støtter denne nyttelasten, kan du bygge den nødvendige profilen i Profile Manager og importere den inn i din MDM-løsning for distribusjon. Kontakt MDM-leverandøren for mer informasjon.

Følg disse trinnene for å lage en konfigurasjonsprofil med Profile Manager:

1. Logg på Profile Manager.
2. Lag en profil for en enhetsgruppe eller for en enhet.
3. Velg Single Sign-On Extensions i listen Payload, og klikk på knappen Add (+) for å legge til en ny nyttelast.
4. I feltet Extension Identifier skriver du «com.apple.AppSSOKerberos.KerberosExtension».
5. Skriv inn «apple» i feltet Team Identifier.



6. Velg Credential under Sign-on Type.
7. I feltet Realm skriver du inn navnet på Active Directory-området der brukerkontoene ligger. Bruk store bokstaver. Ikke bruk navnet på Active Directory-skogen, med mindre brukerkontoene ligger på skognivå.

8. Klikk på Add-knappen (+) under Domains, og legg til domener for ressurser som bruker Kerberos. Hvis du for eksempel bruker Kerberos-autentisering med ressurser i us.pretendco.com, legger du til «.us.pretendco.com». (Ikke glem punktumet i starten.)
9. Legg til disse verdiene under Custom Configuration:

Key	Type	Value
pwNotificationDays	Number	15
requireUserPresence	Boolean	Ikke kontrollert
allowAutomaticLogin	Boolean	Kontrollert
syncLocalPassword	Boolean	Kontrollert
useSiteAutoDiscovery	Boolean	Kontrollert
isDefaultRealm	Boolean	Ikke kontrollert

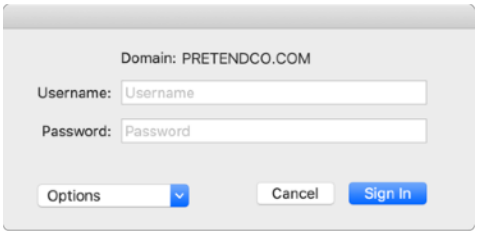
10. Klikk på OK for å lagre den nye konfigurasjonsprofilen. Den installeres automatisk på valgt enhet eller enhetsgruppe.

Brukeroppsett – iOS og iPadOS

1. Koble enheten til et nettverk der organisasjonens Active Directory-domene er tilgjengelig.
2. Gjør ett av følgende:
   - Bruk Safari til å åpne et nettsted som støtter Kerberos-autentisering.
   - Start en app som støtter Kerberos-autentisering.
3. Angi brukernavn og passord for Kerberos eller Active Directory.
4. Du blir spurt om du vil logge på automatisk. De fleste brukere bør velge Ja.
5. Trykk på Sign in (Logg på). Nettstedet eller appen lastes inn etter en kort pause. Hvis du velger å logge på Kerberos SSO-utvidelsen automatisk, blir du ikke bedt om å oppgi brukernavn og passord igjen før du endrer passord. Hvis du ikke velger å logge på automatisk, blir du bedt om å oppgi brukernavn og passord når din Kerberos-pålogging utløper, vanligvis etter 10 timer.

Brukeroppsett – macOS

1. Du må autentisere deg i Kerberos SSO-utvidelsen. Denne prosessen kan gjøres på flere måter:
   - Hvis Macen er koblet til nettverket der Active Directory-domenet er tilgjengelig, blir du bedt om å autentisere deg umiddelbart etter at Extensible SSO-profilen er installert.
   - Hvis du bruker Safari til å få tilgang til et nettsted som bruker Kerberos-autentisering, eller hvis du bruker en app som krever Kerberos-autentisering, blir du bedt om å autentisere deg.
   - Du blir umiddelbart bedt om å autentisere deg når du kobler Macen til et nettverk der din Active Directory er tilgjengelig.
   - Du kan velge Kerberos SSO-utvidelsesmenytillegget, og deretter klikke på Sign in (Logg på).
2. Du blir bedt om å logge deg på. Angi brukernavn og passord for Kerberos eller Active Directory.



3. Du blir spurt om du vil logge på automatisk. De fleste brukere bør velge Ja.
4. Klikk på Sign in (Logg på). Nettstedet eller appen lastes inn etter en kort pause. Hvis du velger å logge på Kerberos SSO-utvidelsen automatisk, blir du ikke bedt om å oppgi brukernavn og passord igjen før du endrer passord. Hvis du ikke velger å logge på automatisk, blir du bedt om å oppgi brukernavn og passord når din Kerberos-pålogging utløper, vanligvis etter 10 timer.
5. Når passordet nærmer seg utløp, blir du varslet om hvor mange dager du har på deg. Du kan klikke på varslingen for å endre passord.
6. Hvis du har aktivert synkronisering av passord, blir du bedt om å oppgi Active Directory-passord og passord for lokal konto. Angi begge, og klikk på OK for å synkronisere passordene dine. Denne informasjonen vises den første gangen du logger deg på, selv om passordene allerede er synkronisert.

Endre passord – macOS

Du kan også endre Active Directory-passord ved hjelp av Kerberos SSO-utvidelsen:

1. Du må være logget på Kerberos SSO-utvidelsen.
2. Velg Kerberos SSO-menytillegget, og velg Change Password. Det kan hende du blir varslet om at passordet ditt snart utløper.
3. Oppgi gjeldende passord, og deretter nytt passord. Bruk passord som oppfyller organisasjonens krav til passord. Klikk på OK.
4. Etter en kort pause åpnes en dialogrute som bekrefter at passordet er endret. Hvis funksjonen for synkronisering av passord er aktivert, oppdateres passordet for den lokale kontoen for å tilpasse det til Active Directory-passordet.

Bruke Kerberos SSO-menytillegget – macOS

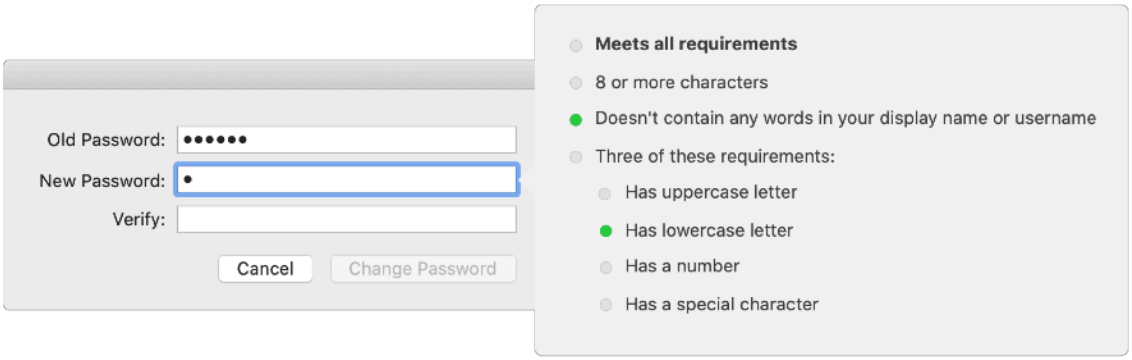
Med Kerberos SSO-menytillegget får du enkelt tilgang til nyttig informasjon om kontoen din og funksjonene i utvidelsen. Den vises som en grå eller svart nøkkel øverst til høyre i menylinjen.

For å finne statusinformasjon om kontoen kan du først se på ikonet for Kerberos SSO-menytillegget og legge merke til fargen på det. Hvis nøkkelen er grå, er du ikke logget på utvidelsen. Hvis nøkkelen er svart, er du logget på. Når du har valgt nøkkelen, vises kontoen du er logget på med, og hvor mange dager som gjenstår før passordet ditt utløper. Du kan også logge på, logge av og endre passord ved hjelp av denne menyen.

Avanserte funksjoner

Testing av passord i sanntid

I mange Active Directory-konfigurasjoner kan Kerberos SSO-utvidelsen teste nye passord når brukerne oppgir dem, for å fortelle brukerne hvilke passordkrav som må oppfylles når de skal endre passord. Når funksjonen er konfigurert, ser brukerne følgende når de oppgir det nye passordet:



For å kunne bruke denne funksjonen må ditt Active Directory-domene bare bruke standard passordregler for Active Directory. Som standard lar Active Directory administratoren kreve at passordet er komplekst og av en bestemt lengde. Mer om komplekse passord: technet.microsoft.com/en-us/library/cc786468(v=ws.10).aspx.

Merk: Det er ikke sikkert du kan bruke denne funksjonen hvis domenet bruker tredjepartsverktøy eller DLL-er for å utvide standard passordregler for Active Directory. Hvis du for eksempel ikke har lov til å bruke bestemte ord, bortsett fra brukernavnet ditt, i passordet, eller hvis du må bruke et bestemt antall spesialtegn i passordet, kan det hende du bruker en passordregelutvidelse fra tredjepart. Kontakt Active Directory-administratoren for mer informasjon.

Hvis organisasjonens Active Directory-domene oppfyller kravene, kan du aktivere testing av passord i sanntid. Angi følgende parametre i konfigurasjonsprofilen for Kerberos SSO-utvidelsen:

Parameter	Key	Type	Value	Valgfritt
Krev komplekse passord	pwReqComplexity	Boolean	JA	Nei
Påkrevd passordlengde	pwReqLength	Integer	Nummer	Ja
Bruk forrige passord på nytt	pwReqHistory	Integer	Nummer	Ja
Minimum passordalder	pwReqMinAge	Integer	Nummer	Ja

Testing av passord i sanntid har enkelte begrensninger. Funksjonen tester ikke om passordet har blitt brukt tidligere. Den tester heller ikke om passordet inneholder ditt visningsnavn i Active Directory hvis du ikke allerede har en Kerberos TGT. Dette kan skje hvis du velger passord for første gang, eller hvis passordet har utløpt. Alle andre tester fungerer normalt.

Visning av krav til passord

Hvis du ikke kan bruke testing av passord i sanntid, kan du konfigurere Kerberos SSO-utvidelsen for å vise en tekststreng med organisasjonens krav til passord når brukerne velger sitt nye passord. I din konfigurasjonsprofil for Kerberos SSO-utvidelsen angir du en streng for «pwReqText» som inneholder teksten brukerne skal se når de endrer passord.

Funksjonalitet for å endre eller deaktivere passord

Enkelte organisasjoner kan ha behov for å bruke standardfunksjonaliteten for endring av passord fra Kerberos SSO-utvidelsen fordi de ikke ønsker passordendringer mot Active Directory. I konfigurasjonsfilen for Kerberos SSO-utvidelsen setter du «allowPasswordChanges» til FALSE for å deaktivere denne funksjonaliteten.

Støtte for å endre passord ved hjelp av nettsted – macOS

Kerberos SSO-utvidelsen kan konfigureres til å åpne et nettsted for å endre passord i standardnettleseren når brukeren velger «Change password» (Endre passord) eller klikker på en varsling om at passordet utløper. Apple anbefaler at denne funksjonen bare brukes sammen med en lokal konto, siden mobile kontoer ikke støttes.

I konfigurasjonsprofilen i Kerberos SSO-utvidelsen setter du «pwChangeURL» til adressen til nettstedet for å endre passord. Når brukere har endret passord, må de logge av Kerberos-utvidelsen, og deretter logge på igjen med det nye passordet. Hvis synkronisering av lokalt passord er aktivert, får brukerne informasjon om hvordan de skal gå frem for å synkronisere passordene igjen.

Synkronisere passord – macOS

Kerberos SSO-utvidelsen kan endre passordet for den lokale kontoen, slik at det stemmer med brukerens Active Directory-passord. Denne funksjonen aktiveres ved å sette «syncLocalPassword» til TRUE i delen Custom Configuration av konfigurasjonsprofilen for Kerberos SSO-utvidelsen.

Synkronisering av passord består av to grunnfunksjoner. Når brukerne bruker Kerberos SSO-utvidelsen til å endre passord, sørger denne funksjonen for at det lokale passordet stemmer overens med Active Directory-passordet. Hvis det lokale passordet og Active Directory-passordet ikke stemmer overens, vil Kerberos SSO-utvidelsen synkronisere dem igjen på følgende måte:

- Når synkronisering av passord aktiveres, og alle påfølgende ganger Kerberos SSO-utvidelsen forsøker å logge seg på, sammenlignes datoene for når brukeren sist endret det lokale passordet og Active Directory-passordet med lagrede verdier. Hvis verdiene samsvarer, er passordene synkroniserte, og det kreves ingen handling. Hvis de ikke samsvarer, vil Kerberos SSO-utvidelsen be brukeren om å oppgi både lokalt passord og Active Directory-passord. Når brukerne oppgir sitt lokale passord, vil Kerberos SSO-utvidelsen endre det lokale passordet, slik at det stemmer overens med Active Directory-passordet.
- Endring av passord fungerer på en liknende måte. Når brukere endrer passord ved hjelp av Kerberos SSO-utvidelsen, kontrolleres det gamle Active Directory-passordet mot den lokale kontoen. Hvis et eldre Active Directory-passord og det lokale passordet samsvarer, endrer Kerberos SSO-utvidelsen begge passordene. Hvis de ikke samsvarer, endres bare Active Directory-passordet. Deretter blir brukerne bedt om å oppgi sitt lokale passord ved neste påloggingsforsøk.

Denne funksjonen har følgende krav:

- Hvis brukerne er logget på Macen med Active Directory – ikke lokal konto – er synkronisering av passord deaktivert. Denne funksjonen skal bare brukes med lokale kontoer. Hvis brukerne er logget på Macen med Active Directory-kontoen sin, er det ikke behov for denne funksjonen.
- Hvis det brukes regler for passord for lokale kontoer, for eksempel ved hjelp av en konfigurasjonprofil eller kommandoen pwpolicy, må reglene for lokale passord tilsvare eller være mindre streng enn reglene for Active Directory-passord. Hvis reglene for lokale passord er strengere enn reglene for Active Directory-passord, kan Kerberos SSO-utvidelsen godkjenne et passord som oppfyller kravene for Active Directory, men ikke kunne endre det lokale passordet, siden det ikke oppfyller reglene for lokale passord. Hvis reglene for lokale passord må være strengere enn reglene for Active Directory-passord, bør du ikke bruke denne funksjonen.
- Det lokale brukernavnet avviker fra Active Directory-brukernavnet – bare passordene endres for å samsvare.

Støtte for smartkort – macOS

Kerberos SSO-utvidelsen støtter smartkort-baserte identiteter for autentisering. Smartkort må ha CryptoTokenKit-driver tilgjengelig. Tokend-baserte drivere støttes ikke. macOS 10.15 støtter PIV-standarden, som brukes av offentlige myndigheter i USA.

Active Directory-domenet må være konfigurert for å støtte smartkort-autentisering før du kan begynne. Prosessen for å aktivere smartkort-autentisering i Active Directory beskrives ikke i dette dokumentet. Se Microsofts dokumentasjon for mer detaljert informasjon.

Følg disse trinnene for å logge på Kerberos SSO-utvidelsen ved hjelp av et smartkort:

1. Klikk på menyen Options, og velg «Use a smart card».
2. Når du ser Identity-knappen, setter du inn smartkortet og klikker på knappen.
3. Velg identiteten du vil autentisere deg med, klikk på OK og klikk deretter på Sign In (Logg på).
4. Oppgi PIN-koden din når du blir bedt om det.

Hvis Kerberos SSO-utvidelsen trenger en Kerberos TGT, blir du bedt om å sette inn smartkortet og oppgi PIN-koden. Du får mer informasjon om støtte for smartkort i macOS ved å kjøre «man SmartCardServices» i Terminal.

Distribuerte varslinger – macOS

Kerberos SSO-utvidelsen poster distribuerte varslinger når forskjellige hendelser oppstår. Apper og tjenester i macOS bruker distribuerte varslinger til å varsle andre apper og tjenester når det har oppstått en hendelse. En app eller tjeneste som lytter etter denne hendelsen, kan iverksette en handling når den oppstår.

En administrator kan bruke denne funksjonaliteten til å utføre en handling når enkelte hendelser oppstår. For eksempel kan administratoren kjøre et skript hver gang Kerberos SSO-utvidelsen henter ny Kerberos-påloggingsinformasjon.

Kerberos SSO-utvidelsen distribuerer varslinger når bestemte hendelser oppstår. Den gjør ikke noe aktivt når hendelsene oppstår. Administratoren må velge et verktøy som lytter etter disse varslingene, og gjennomfører en handling når de oppstår.

I vedlegget finner du et eksempel på en skript og en launchd egenskapsliste (.plist) som kan brukes til å lytte etter varslinger og gjennomføre handlinger. Dette eksempelet kan tilpasses dine behov.

Nedenfor finner du de distribuerte varslingene fra Kerberos SSO-utvidelsen:

Navn	Ved publisering
com.apple.KerberosPlugin.ConnectionCompleted	Kerberos SSO-utvidelsen har gjennomført tilkoblingsprosessen.
com.apple.KerberosPlugin.ADPasswordChanged	Brukeren har endret Active Directory-passord ved hjelp av utvidelsen.
com.apple.KerberosPlugin.LocalPasswordSynced	Brukeren har synkronisert Active Directory-passordet og det lokale passordet.
com.apple.KerberosPlugin.InternalNetworkAvailable	Brukeren har koblet seg til et nettverk det det konfigurerte Active Directory-domenet er tilgjengelig.
com.apple.KerberosPlugin.InternalNetworkNotAvailable	Brukeren har koblet seg til et nettverk der det konfigurerte Active Directory-domenet ikke er tilgjengelig.
com.apple.KerberosExtension.gotNewCredential	Brukeren har hentet ny Kerberos TGT.
com.apple.KerberosExtension.passwordChangedWithPasswordSync	Brukeren har endret Active Directory-passord, og det lokale passordet er oppdatert i samsvar med det nye Active Directory-passordet.

Støtte for kommandolinje – macOS

Administratorer kan bruke kommandolinjeverktøyet *app-sso* til å kontrollere Kerberos SSO-utvidelsen og få tilgang til nyttig informasjon. De kan for eksempel bruke verktøyet for å initiere pålogging, endring av passord og avlogging. Det kan også vise nyttig informasjon, for eksempel hvilken bruker som er logget på, datamaskinens Active Directory-område, brukerens hjem på nettverket, når brukerens passord utløper og mye annen informasjon i egenskapsliste eller JSON-format. Denne informasjonen kan overføres og lastes opp til en Mac-administrasjonsløsning for å få oversikt, eller for andre formål.

For mer informasjon om bruk av app-sso, kan du kjøre kommandoen «app-sso -h» i Terminal.

Mobile kontoer – macOS

Kerberos SSO-utvidelsen krever ikke at Macen er knyttet til Active Directory, eller at brukeren er logget på Macen med en mobil konto. Apple anbefaler at Kerberos SSO-utvidelsen brukes med en lokal konto. Lokale kontoer er det beste valget for anbefalt distribusjonsmodell for macOS, og de er det beste valget for dagens Mac-brukere, som kobler seg til organisasjonens nettverk fra tid til annen. Kerberos SSO-utvidelsen ble utviklet for å forbedre Active Directory-integrering fra en lokal konto.

Men du kan fortsatt bruke Kerberos SSO-utvidelsen hvis du velger å bruke mobile kontoer. Denne funksjonen har følgende krav:

- Synkronisering av passord fungerer ikke med mobile kontoer. Hvis du bruker Kerberos SSO-utvidelsen til å endre Active Directory-passordet og du er logget på Macen med den samme brukerkontoen du bruker med Kerberos SSO-utvidelsen, vil endring av passord fungere på samme måte som i Brukere og grupper-valgpanelet. Hvis du endrer passordet eksternt, for eksempel via et nettsted eller ved å la brukerstøtte tilbakestille det, vil ikke Kerberos SSO-utvidelsen kunne synkronisere passordet for din mobile konto med passordet for Active Directory.
- Nettstedsadresse for å endre passord med Kerberos-utvidelsen og en mobil konto støttes ikke.

Domeneområdetilordning

Administratoren kan definere en tilpasset domeneområdetilordning for Kerberos. For eksempel kan en organisasjon ha Kerberos-området «ad.pretendco.com», men også behov for å bruke Kerberos-autentisering for ressurser på domenet «fakecompany.com».

Merk: Kerberos-implementeringen i operativsystemer fra Apple kan definere domenetilordning automatisk i de aller fleste tilfeller. Administratorer trenger svært sjelden å tilpasse disse innstillingene.

Følg disse trinnene for å konfigurere domenetilordning for Kerberos SSO-utvidelsen:

1. Legg til et objekt med navn domainRealmMapping i delen Custom Configuration i Extensible SSO-profilen. Objekttypen skal være Dictionary.
2. Nøkkelen for denne ordboken skal være navnet på området, i store bokstaver.
3. Verdien for denne ordboken skal være av typen Array. Den første verdien skal være navnet på Kerberos-området, med små bokstaver og med et punktum først. Den andre verdien skal være navnet på domenet som trengs for å autentisere dette området, igjen med et punktum først. Legg til flere arrays ved behov.

Du finner mer informasjon i dokumentasjonen for Kerberos.

Bytte fra Enterprise Connect

Oversikt

Kerberos SSO-utvidelsen skal erstatte Enterprise Connect, et liknende verktøy som brukes av mange organisasjoner. De fleste organisasjoner som bytter fra Enterprise Connect til Kerberos SSO-utvidelsen, kommer til å følge disse trinnene:

1. Lag en konfigurasjonsprofil for Kerberos SSO-utvidelsen som tilbyr liknende funksjonalitet som dagens Enterprise Connect-profil.
2. Avinstaller Enterprise Connect.
3. Distribuer den nye konfigurasjonsprofilen for Kerberos SSO-utvidelsen.
4. Be brukerne logge på Kerberos SSO-utvidelsen.

Det er ikke nødvendig å bytte til Kerberos SSO-utvidelsen for å oppgradere organisasjonens Macer til macOS 10.15. Enterprise Connect fungerer som forventet med macOS 10.15, men organisasjoner bør likevel planlegge et fremtidig bytte fra Enterprise Connect.

Disse trenger ikke å bytte

Kerberos SSO-utvidelsen oppfyller behovene til de aller fleste organisasjoner som bruker Enterprise Connect. Men det er ikke sikkert at organisasjoner som oppfyller disse kriteriene, kan bytte fra Enterprise Connect:

- Organisasjoner som har Macer med macOS 10.14 eller eldre, bør fortsette å bruke Enterprise Connect på disse systemene. Macer med macOS 10.15, kan bytte til Kerberos SSO-utvidelsen. Kerberos SSO-utvidelsen og den tilknyttede konfigurasjonsprofilen fungerer bare på Macer med macOS 10.15. Oppgrader systemene til macOS 10.15 for å kunne bruke Kerberos SSO-utvidelsen.
- Organisasjoner som bruker et verktøy for administrering av Mac som ikke støtter brukergodkjent MDM-registrering.
- Organisasjoner som ikke bruker et verktøy for administrering.
- Organisasjoner som bruker Active Directory-funksjonalitetsnivå som tilsvarer Windows Server 2003 eller eldre.

Lage en konfigurasjonsprofil for Kerberos SSO-utvidelsen

Du må lage en konfigurasjonsprofil for Kerberos SSO-utvidelsen som tilsvarer konfigurasjonsprofilen for Enterprise Connect. Mange preference keys i konfigurasjonsprofilen for Enterprise Connect har tilsvarende valg i profilen for Kerberos SSO-utvidelsen. Start med å lese tabellen nedenfor. Der finner du en oversikt over hvilke innstillinger for Kerberos SSO-utvidelsen som tilsvarer Enterprise Connect preference keys:

Enterprise Connect	Kerberos SSO-utvidelse	Notater
adRealm	Realm	Område skal være i store bokstaver.
Automatic login (enabled by default)	allowAutomaticLogin	Legg til delen Custom Configuration. Må settes til True for at automatisk pålogging skal fungere.
disablePasswordFunctions	allowPasswordChange	Legg til delen Custom Configuration. Settes til False for å deaktivere endring av passord.
passwordChangeURL	pwChangeURL	Legg til delen Custom Configuration.
passwordExpireOverride	pwExpireOverride	Legg til delen Custom Configuration.
passwordNotificationDays	pwNotificationDays	Legg til delen Custom Configuration.
prepopulatedUsername	principalName	Legg til delen Custom Configuration.
pwReqComplexity	pwReqComplexity	Legg til delen Custom Configuration.
pwReqHistory	pwReqHistory	Legg til delen Custom Configuration.
pwReqLength	pwReqLength	Legg til delen Custom Configuration.
pwReqMinimumPasswordAge	pwReqMinAge	Legg til delen Custom Configuration.
pwReqText	pwReqText	Legg til delen Custom Configuration. Oppgi en tekststreng som skal vises istedenfor en bane til en RTF-fil.
syncLocalPassword	syncLocalPassword	Legg til delen Custom Configuration.

Merk: Det er ikke sikkert at alle preference keys fra din Enterprise Connect vises her. Det kan skyldes at funksjonaliteten ikke lenger er nødvendig i Kerberos SSO-utvidelsen, eller at den ikke lenger støttes.

Avinstallere Enterprise Connect

Kerberos SSO-utvidelsen og Enterprise Connect kan ikke kjøres samtidig på samme enhet. Når du har byttet til Kerberos SSO-utvidelsen, må Enterprise Connect avinstalleres. Du må ha administratortilgang for å kunne gjøre dette. Følg disse trinnene for å avinstallere Enterprise Connect:

Enterprise Connect 2.0 og nyere

1. Last ut Enterprise Connect-agenten ved å starte Terminal-appen og kjøre «launchctl unload /Library/LaunchAgents/com.apple.ecAgent» som brukeren som er logget på.
2. Avslutt Enterprise Connect-menytillegget ved å starte Terminal-appen og skrive inn «killall Enterprise\ Connect\ Menu» i Terminal-appen.
3. Slett Enterprise Connect-appen fra Programmer-mappen.
4. Slett Enterprise Connect launchd .plist fra /Library/LaunchAgents/com.apple.ecAgent.plist.

Enterprise Connect 1.9.5 og eldre

1. Avslutt Enterprise Connect ved å skrive inn «killall Enterprise\ Connect» i Terminal-appen.
2. Slett Enterprise Connect-appen fra Programmer-mappen.

I vedlegget finner du et eksempelskript som fjerner alle versjoner av Enterprise Connect.

Enterprise Connect skriptutløsere

Enterprise Connect kan kjøre skript når enkelte hendelser oppstår. For eksempel kan Enterprise Connect kjøre et skript når tilkoblingen er fullført, eller når brukeren endrer passord. Kerberos SSO-utvidelsen bruker skript på en annen måte enn Enterprise Connect. Den kjører ikke skript. I stedet distribuerer den varslinger når en hendelse oppstår, som andre hendelser kan lytte etter for å kjøre skript. Se delen «Avanserte funksjoner» for mer informasjon.

Under ser du referanser for Enterprise Connects skriptutløsere og tilsvarende distribuerte varslinger i Kerberos SSO-utvidelsen:

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

Delte nettverksressurser

Kerberos SSO-utvidelsen støtter ikke håndtering av delte nettverksressurser, for eksempel brukerens Hjem-mappe. Mye av denne funksjonaliteten kan erstattes av skript.

Tillegg

Profil for enhetsadministrering: ExtensibleSingleSignOnKerberos

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

Protokollreferanse for administrering av mobile enheter

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

Profil for enhetsadministrering: ExtensibleSingleSignOnKerberos.ExtensionData

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

Eksempelskript – behandle distribuerte varslinger

Kerberos SSO-utvidelsen distribuerer en rekke varslinger når forskjellige hendelser oppstår, for eksempel når brukeren endrer passord eller bedriftens nettverk kobles til. Som administrator kan du bruke et skript eller en app til å lytte etter disse varslingene, slik at du kan iverksette en handling når de distribueres, for eksempel kjøre et skript eller en shell-kommando.

Under finner du et eksempelskript som kan kjøre skript eller kommandoer når varslinger distribueres. Det må kjøres som en LaunchAgent for å kunne kjøres som brukeren som er logget på, eller som LaunchDaemon for å kunne kjøres som rot. Skriptet krever to parametre:

- **-notification** er navnet på den distribuerte varslingen du skal lytte etter. Se side 11 for eksempler.
- **-action** er handlingen som skal kjøres når den distribuerte varslingen registreres. For eksempel «sh /path/to/script.sh».

Du må installere kommandolinjeverktøyene for utviklere for å kunne kjøre skriptet. Du finner installasjonspakke for disse verktøyene på nettstedet Apple Developer.

```
#!/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()
```

Eksempelskript – avinstallere Enterprise Connect

Dette eksempelskriptet fjerner alle versjoner av Enterprise Connect. Kjør det fra en Mac-administrasjonsløsning eller manuelt. Skriptet må kjøres med rotrettigheter.

```
#!/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
```