Kerberos-kertakirjautumislaajennus

Käyttöopas

Joulukuu 2019

Sisältö

Johdanto

Kerberos-kertakirjautumislaajennus (SSO) tekee Kerberos-pohjaisen kertakirjautumisen käytöstä helppoa organisaatiosi Apple-laitteilla.

Yksinkertaisempi Kerberos-todentautuminen

Kerberos SSO -laajennuksen ansiosta Kerberos TGT -lipun (ticket-granting ticket) hakeminen organisaatiosi Active Directory -domainista on yksinkertaisempaa, ja käyttäjät voivat todentautua vaivattomasti esimerkiksi verkkosivustoille, appeihin ja tiedostopalvelimille. macOS:ssä Kerberos SSO -laajennus hankkii ennakoivasti Kerberos TGT:n verkon tilan vaihtuessa varmistaakseen, että käyttäjä on valmis todentautumaan aina tarvittaessa.

Active Directory -tilin hallinta

Kerberos SSO -laajennus auttaa käyttäjiä myös hallitsemaan Active Directory -tilejään. macOS:ssä se antaa käyttäjien muuttaa Active Directory -salasanansa ja ilmoittaa heille, kun salasana on vanhenemassa. Käyttäjät voivat myös muuttaa paikallisten tilien salasanat vastaamaan Active Directory -salasanoja.

Active Directoryn tuki

Kerberos SSO -laajennusta tulee käyttää paikan päällä olevan Active Directory -domainin kanssa. Azure Active Directorya ei tueta. Kerberos SSO -laajennusta käyttääkseen laitteiden ei tarvitse olla liitetty Active Directory -domainiin. Lisäksi käyttäjien ei tarvitse kirjautua sisään Mac-tietokoneisiin Active Directory- tai mobiilitileillä. Sen sijaan Apple suosittelee paikallisten tilien käyttämistä.

Vaatimukset

- iOS 13, iPadOS tai macOS Catalina.
- Active Directory -domain, joka käyttää Windows Server 2008:aa tai uudempaa. Kerberos SSO -laajennusta ei ole tarkoitettu käytettäväksi Azure Active Directoryn kanssa. Se vaatii perinteisen, paikan päällä olevan Active Directory -domainin.
- Pääsy verkkoon, jossa Active Directory -domainia ylläpidetään. Verkkoon voi olla muodostettu Wi-Fi-, Ethernet- tai VPN-yhteys.
- Laitteita on hallittava mobiililaitteiden hallintaratkaisulla (mobile device management, MDM), joka tukee laajennettavan kertakirjautumisen (SSO) asetusprofiilin tietosisältöä. Kysy MDM-toimittajaltasi, tukevatko he tämän asetusprofiilin tietosisältöä.

Enterprise Connect

Kerberos SSO -laajennuksen on tarkoitus korvata Enterprise Connect. Jos käytät tällä hetkellä Enterprise Connectia ja haluat siirtyä käyttämään Kerberos SSO -laajennusta, löydät lisätietoa aiheesta tämän dokumentin osiosta ”Siirtyminen Enterprise Connectista”.

Alkuun pääseminen

Asetusprofiilin luominen ja käyttöönotto

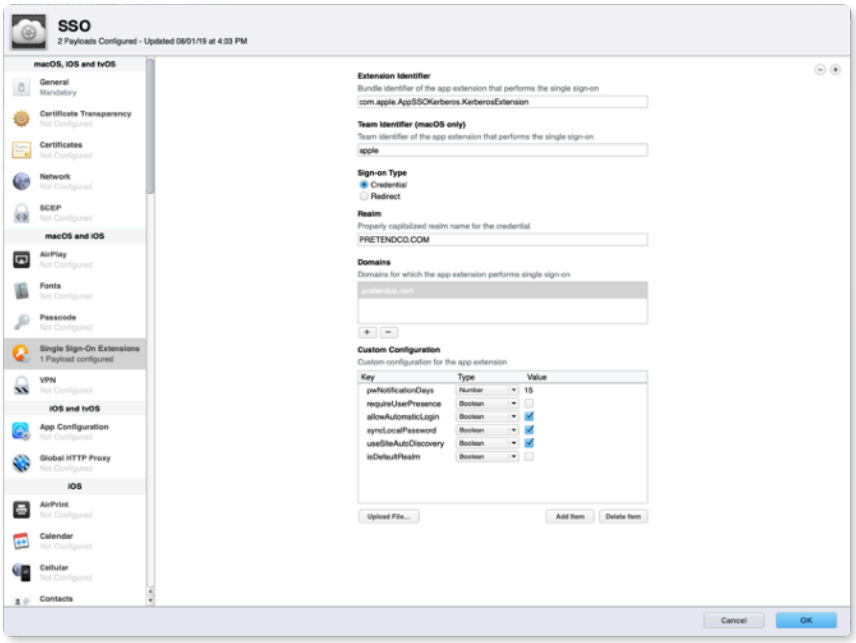
Kerberos SSO -laajennusta käyttääksesi sinun täytyy määrittää se käyttämällä asetusprofiilia, joka on toimitettu laitteelle MDM-ratkaisulla.

Huomaa: Asetusprofiili on toimitettava laitteelle MDM-ratkaisulla. macOS:ssä sen on oltava käyttäjän hyväksymä MDM-rekisteröinti ja asennettu järjestelmään. Profiilin lisäämistä manuaalisesti ei tueta.

Asetusprofiilin avulla määrittämisessä käytetään iOS 13:n, iPadOS:n ja macOS 10.15:n mukana tullutta laajennettavan kertakirjautumisen tietosisältöä. Profile Manager, joka on osa macOS Serveriä, sisältää laajennettavan kertakirjautumisen tietosisällön tuen. Jos MDM-ratkaisusi ei vielä tue tätä tietosisältöä, saatat pystyä luomaan tarvittavan profiilin Profile Managerissa ja tuomaan sen MDM-ratkaisuusi jaettavaksi. Kysy lisätietoja MDM-toimittajaltasi.

Näin luot asetusprofiilin Profile Managerilla:

1. Kirjaudu Profile Manageriin.
2. Luo profiili laiteryhmälle tai tietylle laitteelle.
3. Valitse Payload-luettelosta Single Sign-On Extensions ja lisää sitten uusi tietosisältö klikkaamalla lisäyspainiketta (+).
4. Kirjoita Extension Identifier -kenttään ”com.apple.AppSSOKerberos.KerberosExtension”.
5. Kirjoita Team Identifier -kenttään ”apple”.



6. Valitse Sign-on Type -kohdassa Credential.
7. Syötä Realm-kenttään isoilla kirjaimilla sen Active Directory -domainin nimi, jossa käyttäjätilisi ovat. Älä käytä Active Directory -metsän nimeä, paitsi jos käyttäjätilisi sijaitsevat metsätasolla.
8. Klikkaa Domains-kohdan alla olevaa lisäyspainiketta (+) ja lisää resursseja, jotka käyttävät Kerberosta. Jos esimerkiksi käytät Kerberos-todentautumista osoitteen us.pretendco.com resursseihin, lisää ”.us.pretendco.com”. (Älä unohda alun pistettä.)

9. Lisää seuraavat arvot kohdan Custom Configuration alle:

10. Tallenna uusi asetusprofiili klikkaamalla OK. Se asennetaan automaattisesti valittuun laitteeseen tai laiteryhmään.

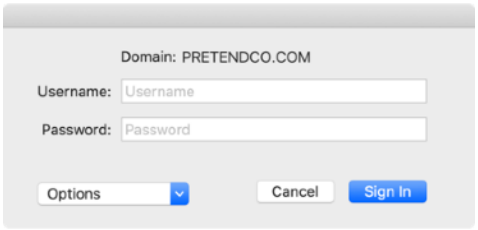
Key	Type	Value
pwNotificationDays	Numero	15
requireUserPresence	Boolean	Ei valittu
allowAutomaticLogin	Boolean	Valittu
syncLocalPassword	Boolean	Valittu
useSiteAutoDiscovery	Boolean	Valittu
isDefaultRealm	Boolean	Ei valittu

Käyttöönotto – iOS ja iPadOS

1. Yhdistä laitteesi verkkoon, jossa organisaatiosi Active Directory -domain on saatavilla.
2. Tee jokin seuraavista:
   - Avaa Safarissa verkkosivusto, joka tukee Kerberos-todentautumista.
   - Avaa appi, joka tukee Kerberos-todentautumista.
3. Kirjoita Kerberos- tai Active Directory -käyttäjätunnuksesi ja -salasanasi.
4. Sinulta kysytään haluatko kirjautua automaattisesti sisään pysyvästi. Useimpien käyttäjien kannattaa napauttaa Yes.
5. Napauta Sign In. Hetken kuluttua verkkosivustosi tai appisi latautuu. Jos valitsit automaattisen kirjautumisen Kerberos SSO -laajennukseen, sinulta ei kysytä tunnuksia ennen kuin muutat salasanasi. Jos et valinnut automaattista kirjautumista, sinulta kysytään tunnuksia vain kun Kerberos-tunnuksesi vanhenee – yleensä 10 tunnin kuluessa.

Käyttöönotto – macOS

1. Sinun täytyy todentautua Kerberos SSO -laajennukseen. Voit aloittaa tämän prosessin monella eri tavalla:
   - Jos Mac on yhteydessä verkkoon, jossa Active Directory -domainisi on saatavilla, sinua pyydetään todentautumaan heti kun laajennettavan kertakirjautumisen asetusprofiili on asennettu.
   - Jos avaat Safarissa verkkosivuston, joka hyväksyy Kerberos-todentautumisen, tai käytät appia, joka vaatii Kerberos-todentautumista, sinua pyydetään todentautumaan.
   - Sinua pyydetään heti todentautumaan aina, kun yhdistät Macisi verkkoon, jossa Active Directorysi on saatavilla.
   - Voit valita Kerberos SSO -laajennuksen valikkoekstran ja klikata sitten Sign In.
2. Sinulta kysytään Kerberos-tunnuksiasi. Kirjoita Kerberos- tai Active Directory -käyttäjätunnuksesi ja -salasanasi.



3. Sinulta kysytään haluatko kirjautua sisään automaattisesti. Useimpien käyttäjien kannattaa klikata Yes.
4. Klikkaa Sign In. Hetken kuluttua verkkosivustosi tai appisi latautuu. Jos valitsit automaattisen kirjautumisen Kerberos SSO -laajennukseen, sinulta ei kysytä tunnuksia ennen kuin muutat salasanasi. Jos et valinnut automaattista kirjautumista, sinulta kysytään tunnuksia vain kun Kerberos-tunnuksesi vanhenee – yleensä 10 tunnin kuluessa.
5. Jos salasanasi on vanhenemassa, saat ilmoituksen siitä, kuinka monta päivää sen vanhenemiseen on. Voit klikata ilmoitusta ja muuttaa salasanasi.
6. Jos olet ottanut käyttöön salasanojen synkronointiominaisuuden, sinulta kysytään nykyistä Active Directory -salasanaasi ja paikallista salasanaasi. Syötä molemmat ja synkronoi salasanasi klikkaamalla OK. Näet tämän kehotuksen ensimmäisen kirjautumisen kohdalla, myös siinä tapauksessa, että salasanasi on jo synkronoitu.

Salasanamuutokset – macOS

Voit myös muuttaa Active Directory -salasanasi Kerberos SSO -laajennuksella:

1. Varmista, että olet kirjautunut sisään Kerberos SSO -laajennukseen.
2. Valitse Kerberos SSO -valikkoekstra ja valitse Change Password. Voit myös saada ilmoituksen siitä, että salasanasi on vanhenemassa.
3. Syötä nykyinen salasanasi ja sitten uusi salasanasi. Varmista, että käyttämäsi uusi salasana vastaa organisaatiosi salasanavaatimuksia. Klikkaa OK.
4. Hetken päästä näet viestin, joka kertoo salasanan vaihdon onnistuneen. Jos salasanojen synkronointiominaisuus on käytössä, paikallisen tilisi salasana päivitetään vastaamaan uutta Active Directory -salasanaasi.

Kerberos SSO -valikkoekstran käyttäminen – macOS

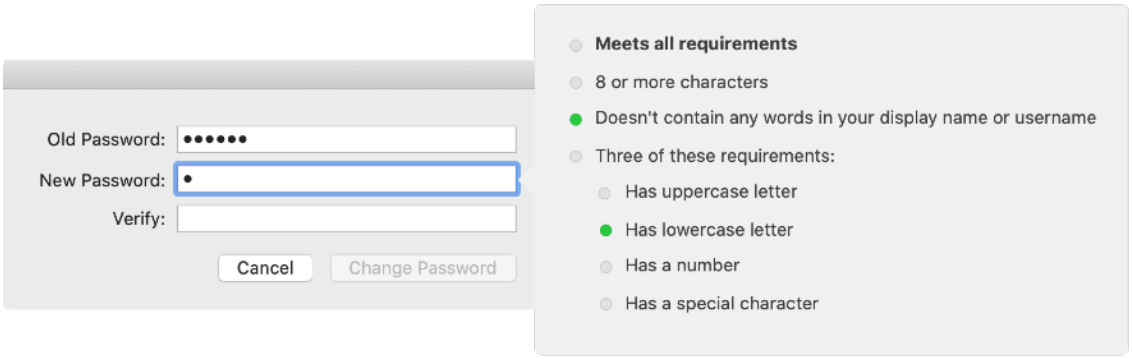
Kerberos SSO -valikkoekstrasta pääset helposti katsomaan hyödyllisiä tietoja tilistäsi ja laajennuksen toiminnoista. Näet sen valikkorivin oikeassa yläkulmassa harmaana tai mustana avaimena.

Jos haluat tietää tilisi tilanteen, aloita katsomalla Kerberos SSO -valikkoekstran kuvaketta ja panemalla merkille sen värin. Jos avain on harmaa, et ole kirjautuneena laajennukseen. Jos avain on musta, olet kirjautunut sisään. Avaimen valittuasi näet tilin, jolla olet kirjautunut sisään sekä sen, kuinka monta päivää salasanasi vanhenemiseen on jäljellä. Valikossa pääset myös kirjautumaan sisään, kirjautumaan ulos ja muuttamaan salasanasi.

Edistykselliset toiminnot

Salasanojen live-testaus

Monissa Active Directory -määrityksissä Kerberos SSO -laajennus voi testata käyttäjien uudet salasanat heidän syöttäessään ne ja kertoa käyttäjille, mitä muutoksia salasanoihin on tehtävä, jotta ne täyttäisivät salasanavaatimukset. Kun määritys on tehty, uutta salasanaa syöttävä käyttäjä näkee tämän näkymän:



Voit käyttää tätä ominaisuutta, jos Active Directory -domainisi käyttää vain tavallisia Active Directory -salasanakäytäntöjä. Active Directory antaa oletusarvoisesti ylläpitäjille oikeuden vaatia monimutkaisia ja tietyn pituisia salasanoja. Lisätietoa siitä, mikä tekee salasanasta monimutkaisen löydät osoitteesta technet.microsoft.com/en-us/library/cc786468(v=ws.10).aspx.

Huomaa: Et välttämättä voi käyttää tätä ominaisuutta, jos domainisi käyttää muiden valmistajien työkaluja tai DLL:iä laajentaakseen tavallista Active Directory -salasanakäytäntöä. Jos salasanassa ei saa esimerkiksi käyttää käyttäjätunnuksen ohella muita sanoja tai salasanassa on oltava erikoismerkkejä, saatat käyttää muiden valmistajien salasanakäytännön laajennuksia. Jos et ole varma, pyydä lisätietoja Active Directory -ylläpitäjältä.

Jos organisaatiosi Active Directory -domain on vaatimusten mukainen, voit ottaa käyttöön salasanojen live-testauksen. Aseta nämä parametrit Kerberos SSO -laajennuksen asetusprofiilissa:

Parametri	Key	Type	Value	Valinnainen
Vaadi monimutkaisia salasanoja	pwReqComplexity	Boolean	KYLLÄ	Ei
Salasanan vaadittu pituus	pwReqLength	Integer	Numero	Kyllä
Käytä aiempaa salasanarajaa	pwReqHistory	Integer	Numero	Kyllä
Salasanan vähimmäisikä	pwReqMinAge	Integer	Numero	Kyllä

Salasanojen live-testauksessa on tiettyjä rajoituksia. Se ei voi tarkistaa, onko salasanaa käytetty jo aiemmin. Se ei voi myöskään tarkistaa, sisältääkö salasanasi Active Directory -nimesi, jos sinulla ei ole jo Kerberos TGT:tä. Näin saattaa käydä, jos asetat salasanaa ensimmäistä kertaa tai jos salasanasi on vanhentunut. Kaikki muut testit toimivat normaalisti.

Salasanavaatimusnäyttö

Jos et voi käyttää salasanojen live-testausta, voit määrittää Kerberos SSO -laajennuksen näyttämään tekstin, joka kertoo organisaatiosi salasanavaatimukset käyttäjien syöttäessä uusia salasanojaan. Aseta Kerberos SSO -laajennuksen asetusprofiilissa kohtaan ”pwReqText” merkkijono, joka sisältää sen tekstin, jonka haluat näkyvän käyttäjän muuttaessa salasanaansa.

Salasanatoimintojen muuttaminen tai poistaminen käytöstä

Jotkin organisaatiot eivät välttämättä pysty käyttämään Kerberos SSO -laajennuksen tavallista salasanan vaihtotoimintoa, jos ne eivät salli salasanan muuttamista Active Directoryn kautta. Voit ottaa tämän toiminnon pois käytöstä asettamalla Kerberos SSO -laajennuksen asetusprofiilissa kohdan ”allowPasswordChanges” arvoksi FALSE.

Salasanan vaihtosivuston tuki – macOS

Kerberos SSO -laajennus voidaan määrittää avaamaan salasanan vaihtosivusto oletusselaimessa, kun käyttäjä päättää vaihtaa salasanan tai vastaa ilmoitukseen salasanan vanhenemisesta. Apple suosittelee tämän ominaisuuden käyttöä vain paikallista tiliä käytettäessä, sillä mobiilitilejä ei tueta.

Aseta Kerberos SSO -laajennuksen asetusprofiilissa ”pwChangeURL” ohjaamaan salasanan vaihtosivustosi verkko-osoitteeseen. Kun käyttäjät ovat vaihtaneet salasanansa, heidän on kirjauduttava ulos Kerberos-laajennuksesta ja kirjauduttava takaisin sisään uusilla salasanoillaan. Jos paikallisten salasanojen synkronointi on käytössä, käyttäjät ohjataan synkronoimaan salasanansa.

Salasanojen synkronointi – macOS

Kerberos SSO -laajennus voi muuttaa paikallisen tilin salasanan vastaamaan käyttäjän Active Directory -salasanaa. Voit ottaa tämän ominaisuuden käyttöön asettamalla Kerberos SSO -laajennuksen asetusprofiilin Custom Configuration -osiossa kohdan ”syncLocalPassword” arvoksi TRUE.

Salasanojen synkronointi muodostuu kahdesta perustoiminnosta. Ensin, kun käyttäjä muuttaa salasanaa Kerberos SSO -laajennuksen avulla, tämä ominaisuus muuttaa paikallisen salasanan vastaamaan Active Directory -salasanaa. Jos paikallinen salasana ja Active Directory -salasana eivät ole synkronoituna, Kerberos SSO -laajennus synkronoi ne seuraavalla tavalla:

- Kun salasanojen synkronointi otetaan käyttöön ja jatkossa aina kun Kerberos SSO -laajennus yrittää muodostaa yhteyden, niitä päivämääriä, joina käyttäjät viimeksi muuttivat paikallista salasanaansa ja Active Directory -salasanaansa, verrataan välimuistissa oleviin arvoihin. Jos arvot vastaavat toisiaan, salasanat ovat synkronoituna eikä muita toimia tarvita. Jos ne eivät vastaa toisiaan, Kerberos SSO -laajennus pyytää käyttäjien paikallista ja Active Directory -salasanaa. Kun käyttäjät antavat paikallisen salasanansa, Kerberos SSO -laajennus muuttaa paikallisen salasanan vastaamaan Active Directory -salasanaa.
- Salasanamuutokset toimivat samanlaisella tavalla. Kun käyttäjät muuttavat salasanaa Kerberos SSO -laajennuksella, heidän vanhoja Active Directory -salasanojaan verrataan paikallisiin tileihin. Jos vanha Active Directory -salasana ja paikallinen salasana vastaavat toisiaan, Kerberos SSO -laajennus muuttaa molemmat salasanat. Jos ne eivät vastaa toisiaan, vain Active Directory -salasana muutetaan. Käyttäjiä pyydetään sitten antamaan paikallinen salasana seuraavan kerran, kun yhteyttä yritetään muodostaa.

Ominaisuus vaatii seuraavia seikkoja:

- Jos käyttäjät ovat kirjautuneena Mac-tietokoneilleen Active Directory -tileillä paikallisten tilien sijaan, salasanojen synkronointi on pois käytöstä. Tämä ominaisuus on tarkoitettu käytettäväksi vain paikallisten tilien kanssa: jos käyttäjät ovat kirjautuneet Mac-tietokoneilleen Active Directory -tileillä, ominaisuus on tarpeeton.
- Jos paikallisilla tileillä on käytössä jokin salasanakäytäntö esimerkiksi käyttämällä asetusprofiilia tai pwpolicy-komentoa, varmista, että paikallinen salasanakäytäntö on sama tai vähemmän tiukka kuin Active Directory -salasanakäytäntö. Jos paikallinen salasanakäytäntö on tiukempi kuin Active Directory -käytäntö, Kerberos SSO -laajennus saattaa hyväksyä salasanan, joka täyttää Active Directoryn vaatimukset, mutta ei onnistu asettamaan paikallista salasanaa, koska salasana ei vastaa paikallisia salasanavaatimuksia. Jos paikallisen salasanakäytännön täytyy olla tiukempi kuin Active Directory -salasanakäytännön, sinun ei tule käyttää tätä ominaisuutta.
- Paikallinen käyttäjätunnus on eri kuin Active Directory -käyttäjätunnus, vain salasanat muutetaan vastaamaan toisiaan.

Älykorttien tuki – macOS

Kerberos SSO -laajennus tukee todentautumisessa älykortteihin perustuvia identiteettejä. Älykortteihin on oltava saatavilla CryptoTokenKit-ajuri, tokend-pohjaisia ajureita ei tueta. macOS 10.15 sisältää Yhdysvaltain valtionhallinnossa laajalti käytössä olevan PIV-standardin tuen.

Ennen kuin aloitat, varmista, että Active Directory -domain on määritetty tukemaan älykortilla todentautumista. Älykortilla Active Directoryyn todentautumisen sallimista ei käsitellä tässä dokumentissa. Lisätietoja aiheesta saat tutustumalla Microsoftin dokumentaatioon.

Näin kirjaudut Kerberos SSO -laajennukseen älykortilla:

1. Klikkaa Options-valikkoa ja valitse sitten ”Use a smart card”.
2. Kun näet Identity-painikkeen, syötä älykorttisi ja klikkaa painiketta.
3. Valitse identiteetti, jolla haluat todentautua, klikkaa OK ja klikkaa sitten Sign In.
4. Anna PIN-numero pyydettäessä.

Jos Kerberos SSO -laajennus vaatii Kerberos TGT:n, sinua pyydetään syöttämään älykorttisi ja kirjoittamaan PIN-numerosi. Saat lisätietoja macOS:n älykorttituesta suorittamalla Päätteessä komennon ”man SmartCardServices”.

Jaetut ilmoitukset – macOS

Kerberos SSO -laajennus julkaisee jaettuja ilmoituksia erilaisista tapahtumista. macOS:n apit ja palvelut kertovat jaettujen ilmoitusten avulla muille apeille ja palveluille, että jotain on tapahtunut. Tätä tapahtumaa odottava appi tai palvelu voi reagoida tapahtumaan jollain tavalla.

Ylläpitäjä voi käyttää tätä toimintoa suorittaakseen jonkin tehtävän tiettyjen tapahtumien kohdalla. Ylläpitäjä voi vaikkapa haluta suorittaa jonkin skriptin aina kun Kerberos SSO -laajennukseen lisätään uusi Kerberos-tunnus.

Kerberos SSO -laajennus vain julkaisee jaettuja ilmoituksia tiettyjen asioiden tapahtuessa. Se ei suorita toimintoja kyseisten tapahtumien aikana. Ylläpitäjän on tarjottava työkalu näiden ilmoitusten seuraamiseen ja toimintojen suorittamiseen, kun ne julkaistaan.

Liitteessä on esimerkki skriptistä ja launchd-ominaisuusluettelosta (.plist), joka voi seurata ilmoituksia ja suorittaa toimintoja. Muokkaa tätä esimerkkiä tarvittaessa käyttöönottoosi sopivaksi.

Alla ovat Kerberos SSO -laajennuksen jakamat ilmoitukset:

Nimi	Julkaistaessa
com.apple.KerberosPlugin.ConnectionCompleted	Kerberos SSO -laajennus on suorittanut liittymisprosessinsa.
com.apple.KerberosPlugin.ADPasswordChanged	Käyttäjä on muuttanut Active Directory -salasanaa laajennuksen avulla.
com.apple.KerberosPlugin.LocalPasswordSynced	Käyttäjä on synkronoinut Active Directory -salasanan ja paikallisen salasanan.
com.apple.KerberosPlugin.InternalNetworkAvailable	Käyttäjä on yhdistänyt laitteensa verkkoon, jossa Active Directory -domain on saatavilla.
com.apple.KerberosPlugin.InternalNetworkNotAvailable	Käyttäjä on yhdistänyt laitteensa verkkoon, jossa Active Directory -domain ei ole saatavilla.
com.apple.KerberosExtension.gotNewCredential	Käyttäjä on hankkinut uuden Kerberos TGT:n.
com.apple.KerberosExtension.passwordChangedWithPasswordSync	Käyttäjä on muuttanut Active Directory -salasanan, ja paikallinen salasana on päivitetty vastaamaan uutta Active Directory -salasanaa.

Komentorivin tuki – macOS

Ylläpitäjät voivat käyttää komentorivityökalua nimeltä *app-sso* Kerberos SSO -laajennuksen hallintaan ja tarpeellisten tietojen tarkasteluun. He voivat esimerkiksi kirjautua sisään, tehdä salasanamuutoksia ja kirjautua ulos kyseisellä työkalulla. Se voi myös tulostaa hyödyllisiä tietoja, kuten tällä hetkellä kirjautuneena olevan käyttäjän, tietokoneen tämänhetkisen Active Directory -sivuston, käyttäjän verkon kotijaon, käyttäjän salasanan vanhenemisajankohdan ja paljon muita hyödyllisiä tietoja ominaisuusluettelona tai JSON-muodossa. Nämä tiedot voidaan jäsentää ja ladata Macin hallintaratkaisuun inventaario- ja muihin tarkoituksiin.

Jos haluat lisätietoja app-sso-työkalun käytöstä, suorita komento ”app-sso -h” Pääte-apissa.

Mobiilitilit – macOS

Kerberos SSO -laajennus ei vaadi, että Macisi olisi liitetty Active Directoryyn tai että käyttäjä olisi kirjautunut Macille mobiilitilillä. Apple suosittelee Kerberos SSO -laajennuksen käyttöä paikallisella tilillä. Paikalliset tilit toimivat parhaiten macOS:lle suositellulla käyttöönottomallilla ja ne ovat paras vaihtoehto tämän päivän Macin käyttäjille, jotka saattavat ajoittain liittyä organisaatiosi verkkoon. Kerberos SSO -laajennus luotiin varta vasten parantamaan Active Directory -integrointia paikalliselta tililtä.

Jos kuitenkin haluat jatkaa mobiilitilien käyttöä, voit silti käyttää Kerberos SSO -laajennusta. Ominaisuus vaatii seuraavia seikkoja:

- Salasanojen synkronointi ei toimi mobiilitileillä. Jos muutat Active Directory -salasanasi Kerberos SSO -laajennuksen avulla ja olet kirjautunut sisään Maciisi samalla käyttäjätilillä, jota käytät Kerberos SSO -laajennuksella, salasanamuutokset toimivat samalla tavalla kuin Käyttäjät ja ryhmät -järjestelmäasetuksissa. Mutta jos teet ulkoisen salasanamuutoksen, eli muutat salasanaasi verkkosivustolla tai tukipalvelu nollaa sen, Kerberos SSO -laajennus ei voi synkronoida mobiilitilisi salasanaa uudestaan Active Directory -salasanasi kanssa.
- Verkko-osoitteen käyttämistä salasanan muuttamiseen Kerberos-laajennuksella ja mobiilitilillä ei tueta.

Domain-alueen kartoitus

Ylläpitäjän on ehkä määriteltävä oma domain-alue Kerberosille. Organisaatiolla saattaa olla esimerkiksi Kerberos-alue nimeltä ”ad.pretendco.com”, mutta sen pitäisi käyttää Kerberos-todentautumista resursseille, jotka sijaitsevat domainissa ”fakecompany.com”.

Huomaa: Kerberosin toteuttaminen Applen käyttöjärjestelmissä voi määrittää domain-alueen automaattisesti lähes joka tilanteessa. Ylläpitäjät muuttavat näitä asetuksia hyvin harvoin.

Näin domain-alue määritetään Kerberos SSO -laajennukselle:

1. Lisää Extensible SSO -profiilin Custom Configuration -osiossa objekti nimeltä domainRealmMapping. Objektityypin pitäisi olla Dictionary.
2. Laita tämän sanakirjan avaimeksi alueen nimi isoilla kirjaimilla.
3. Laita tämän sanakirjan tyypiksi Array. Ensimmäisen arvon tulisi olla Kerberos-alueesi nimi pienillä kirjaimilla, ja sen alussa on piste. Toisen arvon tulisi olla sen domainin nimi, joka vaatii todentautumista tätä aluetta vastaan, ja sekin alkaa pisteellä. Lisää tarvittaessa taulukoita.

Löydät lisätietoja aiheesta Kerberos-dokumentaatiosta.

Siirtyminen Enterprise Connectista

Yleiskatsaus

Kerberos SSO -laajennuksen on tarkoitus korvata Enterprise Connect, samankaltainen työkalu, joka on käytössä jo monissa organisaatioissa. Useimmat Enterprise Connectista Kerberos SSO -laajennukseen siirtyvät organisaatiot noudattavat näitä vaiheita:

1. Luo Kerberos SSO -laajennukselle asetusprofiili, joka toimii samankaltaisella tavalla kuin nykyinen Enterprise Connect -profiilisi.
2. Poista Enterprise Connect.
3. Ota uusi Kerberos SSO -laajennuksen asetusprofiili käyttöön.
4. Pyydä käyttäjiä kirjautumaan Kerberos SSO -laajennukseen.

Kerberos SSO -laajennukseen siirtymistä ei vaadita organisaation Mac-tietokoneiden päivittämiseksi macOS 10.15 -versioon. Enterprise Connect toimii odotetulla tavalla macOS 10.15:n kanssa, mutta organisaatioiden kannattaa silti suunnitella siirtymään pois Enterprise Connectin käytöstä.

Kenen ei kannata siirtyä

Kerberos SSO -laajennus sopii useimpien Enterprise Connectia käyttävien organisaatioiden tarpeisiin. Seuraavat kriteerit täyttävä organisaatio ei kuitenkaan välttämättä pysty siirtymään siihen Enterprise Connectista tai voi mahdollisesti siirtyä siihen vain osittain:

- Organisaation, jossa käytetään tällä hetkellä Mac-tietokoneita ja macOS-versiota 10.14 tai aiempaa, kannattaa jatkaa näissä järjestelmissä Enterprise Connectin käyttöä ja siirtää vain macOS 10.15:llä varustetut Mac-tietokoneet käyttämään Kerberos SSO -laajennusta. Kerberos SSO -laajennus ja sen asetusprofiili toimivat vain macOS 10.15:ttä käyttävissä Mac-tietokoneissa. Pääset käyttämään Kerberos SSO -laajennusta, kun päivität nämä järjestelmät macOS 10.15:een.
- Organisaatio, joka käyttää Macien hallintaan työkalua, joka ei tue käyttäjän hyväksymää MDM-rekisteröitymistä.
- Organisaatio, joka ei käytä mitään hallintatyökalua.
- Organisaatio, joka käyttää Active Directoryn toiminnallista tasoa Windows Server 2003 tai aiempaa.

Kerberos SSO -laajennuksen asetusprofiilin luominen

Sinun on luotava Kerberos SSO -laajennukselle asetusprofiili, joka muistuttaa Enterprise Connectin asetusprofiilia. Monilla Enterprise Connectin asetusprofiilin Preference key -avaimilla on vastinparinsa Kerberos SSO -laajennuksen profiilissa. Aloita tutustumalla alla olevaan taulukkoon, jossa on kartta Kerberos SSO -laajennuksen Enterprise Connectin Preference key -avaimilla vastaavista kohdista:

Enterprise Connect	Kerberos SSO -laajennus	Huomautukset
adRealm	Realm	Alue pitää kirjoittaa isoilla kirjaimilla.
Automatic login (enabled by default)	allowAutomaticLogin	Lisää Custom Configuration -osioon. Sen arvon täytyy olla True, jotta automaattinen kirjautuminen toimii.
disablePasswordFunctions	allowPasswordChange	Lisää Custom Configuration -osioon. Asettamalla sen arvoon False estät salasanamuutokset.
passwordChangeURL	pwChangeURL	Lisää Custom Configuration -osioon.
passwordExpireOverride	pwExpireOverride	Lisää Custom Configuration -osioon.
passwordNotificationDays	pwNotificationDays	Lisää Custom Configuration -osioon.
prepopulatedUsername	principalName	Lisää Custom Configuration -osioon.
pwReqComplexity	pwReqComplexity	Lisää Custom Configuration -osioon.
pwReqHistory	pwReqHistory	Lisää Custom Configuration -osioon.
pwReqLength	pwReqLength	Lisää Custom Configuration -osioon.
pwReqMinimumPasswordAge	pwReqMinAge	Lisää Custom Configuration -osioon.
pwReqText	pwReqText	Lisää Custom Configuration -osioon. Anna teksti, joka tulee näkyviin RTF-tiedostoon johtavan polun sijaan.
syncLocalPassword	syncLocalPassword	Lisää Custom Configuration -osioon.

Huomaa: Joitakin Enterprise Connectin asetusprofiilin Preference key -avaimilla ei ole välttämättä mainittu tässä. Ne saattavat liittyä toimintoihin, jotka eivät ole enää tarpeellisia Kerberos SSO -laajennuksessa tai joita ei tueta enää.

Enterprise Connectin poistaminen

Kerberos SSO -laajennuksen ja Enterprise Connectin käyttämistä rinnakkain samalla tietokoneella ei tueta. Kun olet siirtynyt Kerberos SSO -laajennukseen, poista Enterprise Connect. Poistaaksesi sen tarvitset ylläpito-oikeudet. Noudata seuraavia ohjeita poistaaksesi Enterprise Connect:

Enterprise Connect 2.0 ja uudemmat

1. Poista Enterprise Connect -agentti avaamalla Pääte-appi ja suorittamalla komento ”launchctl unload /Library/LaunchAgents/com.apple.ecAgent” järjestelmään tällä hetkellä kirjautuneena käyttäjänä.
2. Lopeta Enterprise Connect -valikkoekstra avaamalla Pääte-appi ja syöttämällä Pääte-appiin komento ”killall Enterprise\ Connect\ Menu”.
3. Poista Enterprise Connect -appi Ohjelmat-kansiosta.
4. Poista Enterprise Connect launchd .plist -ominaisuusluettelo kohteesta /Library/LaunchAgents/com.apple.ecAgent.plist.

Enterprise Connect 1.9.5 ja aiemmat

1. Lopeta Enterprise Connect syöttämällä komento ”killall Enterprise\ Connect” Pääte-appiin.
2. Poista Enterprise Connect -appi Ohjelmat-kansiosta.

Liitteessä on esimerkkiskripti, joka poistaa minkä tahansa Enterprise Connect -version.

Enterprise Connectin skriptin laukaisijat

Enterprise Connect voi suorittaa skriptejä, kun tietyt asiat tapahtuvat. Enterprise Connect voi esimerkiksi suorittaa skriptin, kun se saa liittymisprosessin suoritettua tai kun käyttäjä muuttaa salasanaa. Kerberos SSO -laajennus käyttää skriptejä eri tavalla kuin Enterprise Connect. Se ei suorita skriptejä suoraan. Sen sijaan se julkaisee jaetun ilmoituksen, kun jotain tapahtuu, ja toinen prosessi odottaa ilmoitusta ja suorittaa sen havaitessaan skriptin. Löydät lisätietoja aiheesta tämän dokumentin kohdasta ”Edistykselliset toiminnot”.

Alla on viittaukset Enterprise Connectin skriptin laukaisijoihin ja niitä vastaaviin jaettuihin ilmoituksiin Kerberos SSO -laajennuksessa:

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

Jaetut verkkoresurssit

Kerberos SSO -laajennus ei tue jaettujen verkkoresurssien käsittelyä, kuten käyttäjän verkon kotihakemistoa. Voit korvata tämän toiminnon suurelta osin skripteillä.

Liite

Laitehallintaprofiili: ExtensibleSingleSignOnKerberos

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

Mobiililaitteiden hallinnan (MDM) protokollaopas

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

Laitehallintaprofiili: ExtensibleSingleSignOnKerberos.ExtensionData

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

Esimerkkiskripti – Jaettujen ilmoitusten prosessointi

Kerberos SSO -laajennus julkaisee jaettuja ilmoituksia erilaisten asioiden tapahtuessa, esimerkiksi kun käyttäjä muuttaa salasanaa tai kun yrityksen verkko muodostaa yhteyden. Ylläpitäjänä voit skriptin tai apin avulla seurata näitä ilmoituksia ja reagoida niiden julkaisuun esimerkiksi suorittamalla skriptin tai shell-komennon.

Alla on esimerkkiskripti, joka voi suorittaa skriptejä tai komentoja, kun ilmoituksia julkaistaan. Se tulee toteuttaa joko LaunchAgent-skriptinä, jolloin se suoritetaan kirjautuneena käyttäjänä, tai LaunchDaemon-skriptinä, jos se halutaan suorittaa pääoikeuksilla. Skriptissä on kaksi tarvittavaa parametriä:

- **-notification** on sen jaetun ilmoituksen nimi, jota seuraat. Löydät esimerkkejä sivulta 11.
- **-action** on toiminto, jonka haluat suorittaa, kun jaettu ilmoitus julkaistaan. Esimerkiksi ”sh /path/to/script.sh.”

Suorittaaksesi skriptin sinun täytyy asentaa kehittäjien komentorivityökalut. Näiden työkalujen asennuspaketti on saatavilla Apple Developer -verkkosivustolta.

```
#!/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()
```

Esimerkkiskripti – Enterprise Connectin poistaminen

Tämä esimerkkiskripti poistaa minkä tahansa Enterprise Connect -version. Suorita se Macin hallintaratkaisusta tai manuaalisesti. Skripti on suoritettava pääoikeuksilla.

```
#!/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
```