Kerberos SSO-extensie

Gebruikershandleiding

December 2019

Inhoud

Inleiding

Met de Kerberos Single Sign-on-extensie (SSO) kunnen de Apple devices in uw organisatie gebruikmaken van op Kerberos gebaseerde eenmalige aanmelding.

Vereenvoudigde Kerberos-identiteitscontrole

De Kerberos SSO-extensie vereenvoudigt het proces voor het ophalen van een Kerberos-TGT (ticket-granting ticket) uit het Active Directory-domein van uw organisatie. Gebruikers kunnen dan naadloos inloggen bij onder meer websites, apps en bestandsservers. De Kerberos SSO-extensie in macOS haalt proactief bij elke wijziging in de status van het netwerk een Kerberos-TGT op, zodat de identiteit van de gebruiker meteen kan worden gecontroleerd.

Beheer van Active Directory-accounts

Uw gebruikers profiteren ook bij het beheer van hun Active Directory-account van de Kerberos SSO-extensie. Ze kunnen in macOS namelijk hun Active Directory-wachtwoord wijzigen en krijgen een melding wanneer een wachtwoord bijna verloopt. Verder kunnen ze voor hun lokale account hetzelfde wachtwoord gebruiken als voor hun Active Directory-account.

Ondersteuning van Active Directory

De Kerberos SSO-extensie moet met een lokaal Active Directory-domein worden gebruikt. Azure Active Directory wordt niet ondersteund. Devices hoeven niet aan een Active Directory-domein gekoppeld te zijn om de Kerberos SSO-extensie te kunnen gebruiken. Bovendien hoeven gebruikers niet met een Active Directory- of mobiele account in te loggen bij hun Mac. Apple adviseert gebruik te maken van lokale accounts.

Vereisten

- iOS 13, iPadOS of macOS Catalina.
- Een Active Directory-domein dat op Windows Server 2008 of later draait. De Kerberos SSO-extensie kan niet met Azure Active Directory worden gebruikt, maar vereist een traditioneel lokaal Active Directory-domein.
- Toegang tot het hostnetwerk van het Active Directory-domein (via wifi, Ethernet of VPN).
- Devices moeten worden beheerd met een MDM-oplossing (mobile device management) die de payload van het configuratieprofiel ‘Extensible Single Sign-on’ ondersteunt. U kunt bij uw MDM-leverancier navragen of dit wordt ondersteund.

Enterprise Connect

De Kerberos SSO-extensie komt in de plaats van Enterprise Connect. Maakt u gebruik van Enterprise Connect en wilt u overstappen naar de Kerberos SSO-extensie? In het gedeelte ‘Overstappen van Enterprise Connect’ verderop vindt u meer informatie.

Aan de slag

Een configuratieprofiel maken en implementeren

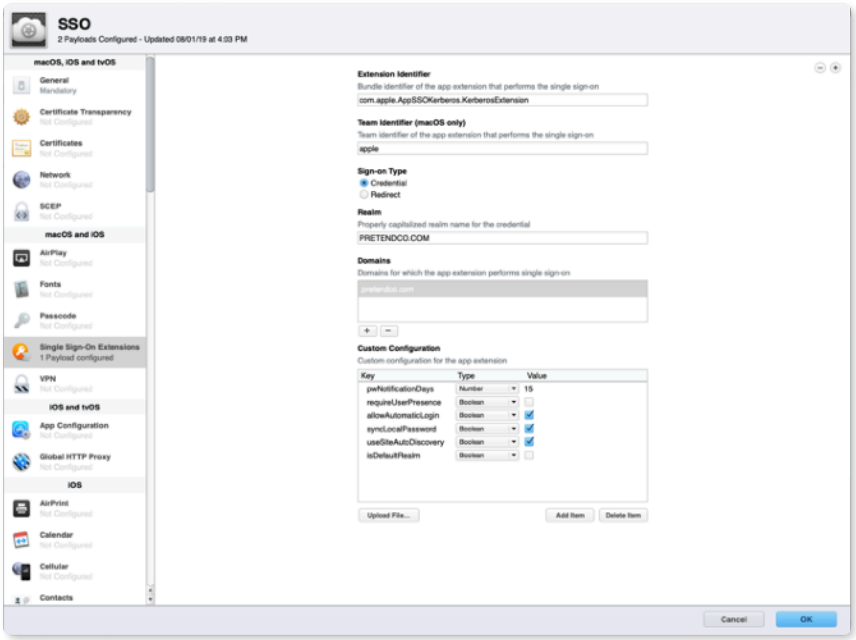
Om de Kerberos SSO-extensie te kunnen gebruiken, moet deze worden geconfigureerd op basis van een configuratieprofiel dat via een MDM-oplossing op het device wordt gezet.

Opmerking: Het configuratieprofiel moet via een MDM-oplossing op het device worden gezet. In macOS moet dat een door de gebruiker goedgekeurde MDM-aanmelding zijn en moet het in de System Scope geïnstalleerd zijn. Het profiel handmatig toevoegen wordt niet ondersteund.

Om de configuratie via een configuratieprofiel te regelen, gebruikt u de payload van Extensible Single Sign-on die in iOS 13, iPadOS en macOS 10.15 is ingevoerd. Deze wordt door Profile Manager (onderdeel van macOS Server) ondersteund. Als uw MDM-oplossing deze payload nog niet ondersteunt, kunt u het benodigde profiel in Profile Manager maken, in uw MDM-oplossing importeren en vervolgens distribueren. Neem voor meer informatie contact op met uw MDM-leverancier.

Volg deze stappen om in Profile Manager een configuratieprofiel te maken:

1. Log in bij Profile Manager.
2. Maak een profiel voor een specifiek device of een groep devices.
3. Selecteer ‘Single Sign-On Extensions’ in de lijst met payloads. Klik op de +-knop om een nieuwe payload toe te voegen.
4. Ga naar het veld ‘Extension Identifier’ en vul ‘com.apple.AppSSOKerberos.KerberosExtension’ in.
5. Ga naar het veld ‘Team Identifier’ en vul ‘apple’ in.



6. Selecteer ‘Credential’ onder ‘Sign-on Type’.
7. Ga naar het veld ‘Realm’ en voer in hoofdletters de naam in van het Active Directory-domein van uw gebruikersaccounts. Voer hier niet de naam van uw Active Directory-forest in, tenzij uw gebruikersaccounts daar beheerd worden.

8. Klik onder ‘Domains’ op de +-knop en voeg voor alle resources die gebruikmaken van Kerberos een domein toe. Als u de Kerberos-identiteitscontrole bijvoorbeeld voor resources in us.pretendco.com wilt gebruiken, vult u ‘.us.pretendco.com’ in. (Let op de punt aan het begin.)
9. Kies onder ‘Custom Configuration’ de volgende waarden:

Key	Type	Value
pwNotificationDays	Getal	15
requireUserPresence	Boolean	Niet ingeschakeld
allowAutomaticLogin	Boolean	Ingeschakeld
syncLocalPassword	Boolean	Ingeschakeld
useSiteAutoDiscovery	Boolean	Ingeschakeld
isDefaultRealm	Boolean	Niet ingeschakeld

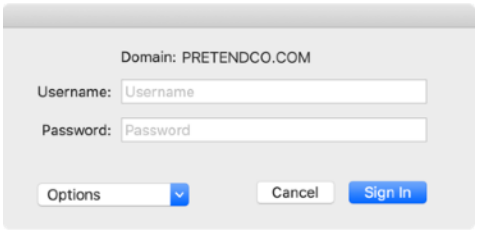
10. Klik op ‘OK’ om het nieuwe configuratieprofiel te bewaren. Dit wordt automatisch op het geselecteerde device of de geselecteerde groep devices geïnstalleerd.

Configuratie door de gebruiker – iOS en iPadOS

1. Verbind uw device met een netwerk waarop het Active Directory-domein van uw organisatie beschikbaar is.
2. Doe een van deze dingen:
   - Open Safari en ga naar een website die Kerberos-identiteitscontrole ondersteunt.
   - Open een app die Kerberos-identiteitscontrole ondersteunt.
3. Voer uw Kerberos- of Active Directory-gebruikersnaam en -wachtwoord in.
4. U wordt gevraagd of u altijd automatisch aangemeld wilt worden. Voor de meeste gebruikers geldt dat ze dit bevestigend moeten beantwoorden.
5. Tik op de aanmeld- of inlogknop. Even later wordt de website geladen of wordt de app geopend. Als u ervoor hebt gekozen automatisch in te loggen via de Kerberos SSO-extensie, hoeft u hierna niet meer handmatig in te loggen, tenzij u uw wachtwoord verandert. Als u ervoor hebt gekozen niet automatisch in te loggen, hoeft u pas opnieuw in te loggen wanneer uw Kerberos-inloggegevens verlopen (meestal na tien uur).

Configuratie door de gebruiker – macOS

1. Uw identiteit moet via de Kerberos SSO-extensie worden gecontroleerd. Dat kan op diverse manieren:
   - Wanneer uw Mac verbonden is met een netwerk waarop uw Active Directory-domein beschikbaar is, moet u uw inloggegevens invoeren zodra het configuratieprofiel 'Extensible SSO' is geïnstalleerd.
   - Wanneer u in Safari naar een website gaat die Kerberos-identiteitscontrole ondersteunt of een app gebruikt die Kerberos-identiteitscontrole vereist, moet u op dat moment uw inloggegevens invoeren.
   - U moet uw inloggegevens invoeren zodra u uw Mac verbindt met een netwerk waarop uw Active Directory-domein beschikbaar is.
   - U kunt het menu 'Extra' van de Kerberos SSO-extensie selecteren, waarna u op 'Sign In' klikt.
2. U moet uw Kerberos-inloggegevens invoeren. Voer uw Kerberos- of Active Directory-gebruikersnaam en -wachtwoord in.



3. U wordt gevraagd of u zich automatisch wilt aanmelden. Voor de meeste gebruikers geldt dat ze dit bevestigend moeten beantwoorden.
4. Klik op de aanmeld- of inlogknop. Even later wordt de website geladen of wordt de app geopend. Als u ervoor hebt gekozen automatisch in te loggen via de Kerberos SSO-extensie, hoeft u hierna niet meer handmatig in te loggen, tenzij u uw wachtwoord verandert. Als u ervoor hebt gekozen niet automatisch in te loggen, hoeft u pas opnieuw in te loggen wanneer uw Kerberos-inloggegevens verlopen (meestal na tien uur).
5. Wanneer uw wachtwoord bijna verloopt, krijgt u een melding met daarin het aantal dagen totdat het wachtwoord verloopt. Als u op de melding klikt, kunt u meteen uw wachtwoord veranderen.
6. Als u wachtwoordsynchronisatie hebt ingeschakeld, moet u uw huidige Active Directory-wachtwoord en lokale wachtwoord invoeren. Voer deze in en klik op 'OK' om uw wachtwoorden te synchroniseren. U ziet deze melding bij de allereerste keer dat u inlogt, ook als uw wachtwoorden al gesynchroniseerd zijn.

Wachtwoord veranderen – macOS

Met de Kerberos SSO-extensie kunt u ook uw Active Directory-wachtwoord veranderen:

1. Zorg dat u bij de Kerberos SSO-extensie bent ingelogd.
2. Selecteer het Kerberos SSO-menu 'Extra' en kies 'Change Password'. Mogelijk krijgt u een melding dat uw wachtwoord verlopen is.
3. Voer uw huidige wachtwoord en een nieuw wachtwoord in. Zorg dat het nieuwe wachtwoord voldoet aan de eisen die uw organisatie aan wachtwoorden stelt. Klik op 'OK'.
4. Even later krijgt u een melding dat het wachtwoord is veranderd. Als u wachtwoordsynchronisatie hebt ingeschakeld, wordt het wachtwoord van uw lokale account aangepast zodat dit hetzelfde is als het nieuwe Active Directory-wachtwoord.

Het Kerberos SSO-menu ‘Extra’ gebruiken – macOS

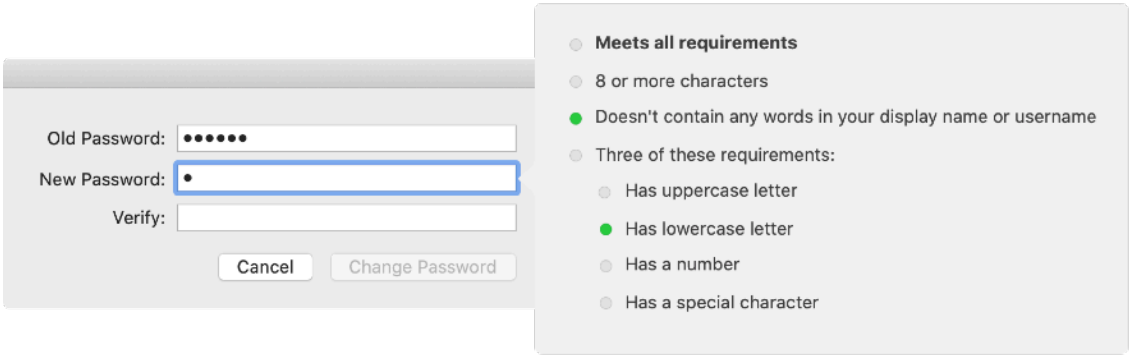
In het Kerberos SSO-menu ‘Extra’ vindt u nuttige informatie over uw account en over de functies van de extensie. U vindt dit menu in de menubalk rechtsboven (grijze of zwarte sleutel).

Als u de status van uw account wilt weten, kijkt u om te beginnen naar de kleur van het symbool van het menu ‘Extra’ in Kerberos SSO. Bij een grijze sleutel bent u niet ingelogd bij de extensie. Bij een zwarte sleutel bent u wel ingelogd. Nadat u de sleutel hebt geselecteerd, ziet u de account waarmee u bent ingelogd en hoeveel dagen het nog duurt voordat uw wachtwoord verloopt. Via dit menu kunt u ook inloggen, uitloggen en uw wachtwoord veranderen.

Geavanceerde functies

Wachtwoorden live testen

In veel Active Directory-configuraties kan de Kerberos SSO-extensie nieuwe wachtwoorden van gebruikers testen zodra ze worden ingevoerd en aangeven aan welke eisen een nieuw wachtwoord moet voldoen. Wanneer dit is geconfigureerd, ziet de gebruiker het volgende bij het invoeren van een nieuw wachtwoord:



Om deze feature te kunnen gebruiken, mag uw Active Directory-domein alleen gebruikmaken van standaardwachtwoordbeleid in Active Directory. Beheerders mogen in Active Directory standaard afdwingen dat complexe wachtwoorden met een bepaalde lengte worden gebruikt. Wilt u weten wat onder een complex wachtwoord wordt verstaan? Ga dan naar technet.microsoft.com/en-us/library/cc786468(v=ws.10).aspx.

Opmerking: U kunt deze feature waarschijnlijk niet gebruiken wanneer uw domein DLL-bestanden of tools van derden gebruikt om het standaardwachtwoordbeleid in Active Directory uit te breiden. Als er bijvoorbeeld behalve uw gebruikersnaam nog meer woorden zijn die u niet in uw wachtwoord mag gebruiken of als u een bepaald aantal speciale tekens in uw wachtwoord moet gebruiken, maakt u waarschijnlijk gebruik van extensies voor wachtwoordbeleid van derden. Als u dit niet zeker weet, kunt u dit navragen bij uw Active Directory-beheerder.

Als het Active Directory-domein van uw organisatie aan de eisen voldoet, kunt u het live testen van wachtwoorden inschakelen. Stel in het configuratieprofiel van de Kerberos SSO-extensie de volgende parameters in:

Parameter	Key	Type	Value	Optioneel
Complexe wachtwoorden afdwingen	pwReqComplexity	Boolean	JA	Nee
Vereiste lengte van wachtwoorden	pwReqLength	Integer	Getal	Ja
Limiet voor hergebruik eerdere wachtwoorden	pwReqHistory	Integer	Getal	Ja
Minimale gebruiksduur van wachtwoorden	pwReqMinAge	Integer	Getal	Ja

Het live testen van wachtwoorden kent een paar beperkingen. Er kan niet worden getest of een wachtwoord al eerder is gebruikt. Als u nog geen Kerberos-TGT hebt, kan evenmin worden getest of uw wachtwoord uw weergavenaam voor Active Directory bevat. Dit kan gebeuren wanneer u uw wachtwoord voor het eerst instelt of wanneer uw wachtwoord is verlopen. Alle andere tests werken zoals het hoort.

Eisen voor wachtwoorden weergeven

Als u het live testen van wachtwoorden niet kunt gebruiken, kunt u de Kerberos SSO-extensie zo configureren dat gebruikers bij het invoeren van een nieuw wachtwoord een tekststring zien met de eisen die uw organisatie aan wachtwoorden stelt. Stel in het configuratieprofiel van de Kerberos SSO-extensie voor 'pwReqText' een string in met de tekst die u wilt weergeven wanneer een gebruiker zijn wachtwoord verandert.

Wachtwoordfunctionaliteit veranderen of uitschakelen

Sommige organisaties kunnen de standaardfunctionaliteit voor het veranderen van wachtwoorden van de Kerberos SSO-extensie niet gebruiken omdat ze het veranderen van Active Directory-wachtwoorden niet toestaan. Als u deze functionaliteit wilt uitschakelen, gaat u naar het configuratieprofiel van de Kerberos SSO-extensie en zet u 'allowPasswordChanges' op 'FALSE'.

Wachtwoord veranderen op een website – macOS

U kunt de Kerberos SSO-extensie zo instellen dat er in de standaardbrowser een website voor het veranderen van het wachtwoord wordt geopend zodra de gebruiker op een knop voor het veranderen van zijn wachtwoord klikt of zodra de gebruiker de melding over het verlopen van zijn wachtwoord bevestigt. Apple raadt aan deze feature alleen bij lokale accounts te gebruiken, aangezien mobiele accounts niet worden ondersteund.

Ga naar het configuratieprofiel van de Kerberos SSO-extensie en stel 'pwChangeURL' in op de url van uw website voor het veranderen van wachtwoorden. Zodra een gebruiker zijn wachtwoord heeft veranderd, moet hij uitloggen bij de Kerberos-extensie en opnieuw inloggen met het nieuwe wachtwoord. Als u wachtwoordsynchronisatie hebt ingeschakeld, krijgt de gebruiker instructies om zijn wachtwoorden opnieuw te synchroniseren.

Wachtwoorden synchroniseren – macOS

De Kerberos SSO-extensie kan het wachtwoord van een lokale account aanpassen zodat dit hetzelfde is als het Active Directory-wachtwoord van de gebruiker. U schakelt deze feature in door naar het configuratieprofiel van de Kerberos SSO-extensie te gaan en 'syncLocalPassword' in het gedeelte 'Custom Configuration' in te stellen op 'TRUE'.

Het synchroniseren van wachtwoorden bestaat uit twee basisfuncties. Wanneer de gebruiker om te beginnen de Kerberos SSO-extensie gebruikt om een wachtwoord te veranderen, zorgt deze feature ervoor dat het lokale wachtwoord van de gebruiker wordt aangepast aan diens Active Directory-wachtwoord. Wanneer het lokale wachtwoord en het Active Directory-wachtwoord niet meer gesynchroniseerd zijn, zorgt de Kerberos SSO-extensie er als volgt voor dat ze opnieuw gesynchroniseerd worden:

- Bij het inschakelen van wachtwoordsynchronisatie en bij elke volgende verbindingspoging van de Kerberos SSO-extensie worden de datums waarop de gebruiker zijn lokale wachtwoord en Active Directory-wachtwoord voor het laatst heeft veranderd, vergeleken met de waarden die in de cache zijn opgeslagen. Als de waarden met elkaar overeenkomen, zijn de wachtwoorden gesynchroniseerd en hoeft er verder niets te worden gedaan. Als de waarden niet met elkaar overeenkomen, vraagt de Kerberos SSO-extensie de gebruiker om zijn lokale wachtwoord en Active Directory-wachtwoord in te voeren. Zodra de gebruiker zijn lokale wachtwoord heeft opgegeven, verandert de Kerberos SSO-extensie dat lokale wachtwoord in zijn Active Directory-wachtwoord.

- Het veranderen van een wachtwoord werkt ongeveer hetzelfde. Wanneer de gebruiker zijn wachtwoord via de Kerberos SSO-extensie verandert, wordt zijn oude Active Directory-wachtwoord vergeleken met zijn lokale account. Als het oude Active Directory-wachtwoord en het lokale wachtwoord met elkaar overeenkomen, verandert de Kerberos SSO-extensie beide wachtwoorden. Als ze niet met elkaar overeenkomen, wordt alleen het Active Directory-wachtwoord veranderd. De gebruiker moet dan bij de eerstvolgende verbindingspoging zijn lokale wachtwoord opgeven.

Voor deze feature gelden de volgende eisen:

- Wanneer gebruikers niet met hun lokale account, maar met hun Active Directory-account bij hun Mac zijn ingelogd, is wachtwoordsynchronisatie uitgeschakeld. Deze feature werkt namelijk alleen met lokale accounts. Als gebruikers met hun Active Directory-account bij hun Mac zijn ingelogd, is deze feature overbodig.
- Als voor lokale accounts een wachtwoordbeleid wordt afgedwongen (bijvoorbeeld door een configuratieprofiel of het commando 'pwpolicy'), moet dat beleid net zo streng of minder streng zijn dan het beleid voor Active Directory-wachtwoorden. Als het beleid voor lokale accounts strenger is dan het Active Directory-beleid, kan het namelijk voorkomen dat de Kerberos SSO-extensie een wachtwoord toestaat dat aan de Active Directory-eisen voldoet, maar dat het lokale wachtwoord niet wordt ingesteld omdat het niet aan de eisen voor lokale wachtwoorden voldoet. Als uw beleid voor lokale wachtwoorden strenger moet zijn dan het beleid voor Active Directory-wachtwoorden, moet u deze feature niet gebruiken.
- De lokale gebruikersnaam is anders dan de gebruikersnaam in Active Directory. Alleen de wachtwoorden worden gesynchroniseerd.

Ondersteuning van smartcards – macOS

De Kerberos SSO-extensie ondersteunt identiteitscontrole op basis van smartcards. Smartcards moeten wel een CryptoTokenKit-driver hebben; op tokenD gebaseerde drivers worden niet ondersteund. macOS 10.15 ondersteunt de PIV-standaard, die veel wordt gebruikt door Amerikaanse overheidsinstanties.

Voordat u hiermee aan de slag gaat, moet u controleren of uw Active Directory-domein identiteitscontrole op basis van smartcards ondersteunt. Zo ja, dan kunt u dit inschakelen in Active Directory. Hoe u dat precies moet doen, valt buiten het kader van dit document. Raadpleeg de desbetreffende documentatie van Microsoft als u hier meer over wilt weten.

Volg deze stappen om met een smartcard in te loggen bij de Kerberos SSO-extensie:

1. Klik op het menu 'Options' en selecteer 'Use a smart card'.
2. Zodra u de knop 'Identity' ziet, plaatst u uw smartcard en klikt u op de knop.
3. Kies de gewenste identiteit en klik achtereenvolgens op 'OK' en 'Sign In'.
4. Voer desgevraagd uw pincode in.

Als de Kerberos SSO-extensie een Kerberos-TGT moet ophalen, moet u uw smartcard plaatsen en uw pincode invoeren. Als u in Terminal het commando 'man SmartCardServices' uitvoert, krijgt u meer informatie te zien over de ondersteuning van smartcards in macOS.

Gedistribueerde meldingen – macOS

De Kerberos SSO-extensie post een gedistribueerde melding zodra zich bepaalde events voordoen. De apps en voorzieningen in macOS wijzen andere apps en voorzieningen met zo'n gedistribueerde melding op een event. Een app of voorziening die alert is op dat event, kan dan actie ondernemen.

Beheerders kunnen deze feature gebruiken om een actie te laten uitvoeren zodra zich een bepaald event voordoet. Een beheerder kan bijvoorbeeld een script laten uitvoeren zodra de Kerberos SSO-extensie nieuwe Kerberos-inloggegevens ophaalt.

Het enige wat de Kerberos SSO-extensie bij een event doet, is een gedistribueerde melding posten. De extensie zet niet de bijbehorende actie in gang. De beheerder moet zorgen voor een tool die dit soort meldingen oppikt en de benodigde actie uitvoert.

In de bijlage staat een voorbeeld van een script en een launchd .plist die voor dit doel kunnen worden gebruikt. U kunt dit voorbeeld als uitgangspunt gebruiken en naar wens aanpassen.

Hieronder staan de gedistribueerde meldingen die de Kerberos SSO-extensie kan posten:

Naam	Op het moment van posten
com.apple.KerberosPlugin.ConnectionCompleted	De Kerberos SSO-extensie heeft het verbindingsproces voltooid.
com.apple.KerberosPlugin.ADPasswordChanged	De gebruiker heeft zijn Active Directory-wachtwoord met de extensie veranderd.
com.apple.KerberosPlugin.LocalPasswordSynced	De gebruiker heeft zijn Active Directory-wachtwoord en lokale wachtwoord gesynchroniseerd.
com.apple.KerberosPlugin.InternalNetworkAvailable	De gebruiker heeft verbinding gemaakt met een netwerk waar het geconfigureerde Active Directory-domein beschikbaar is.
com.apple.KerberosPlugin.InternalNetworkNotAvailable	De gebruiker heeft verbinding gemaakt met een netwerk waar het geconfigureerde Active Directory-domein niet beschikbaar is.
com.apple.KerberosExtension.gotNewCredential	De gebruiker heeft een nieuwe Kerberos-TGT opgehaald.
com.apple.KerberosExtension.passwordChangedWithPasswordSync	De gebruiker heeft zijn Active Directory-wachtwoord veranderd en zijn lokale wachtwoord is aangepast zodat dit hetzelfde is als het nieuwe Active Directory-wachtwoord.

Ondersteuning voor de commandoregel – macOS

Met de commandoregeltool *app-sso* kunnen beheerders de Kerberos SSO-extensie beheren en nuttige informatie inzien. Zo kunnen ze met deze tool een inlog- of uitlogproces of het veranderen van een wachtwoord initiëren. Via de tool kunnen ze ook nuttige informatie afdrukken, zoals de gebruiker die op dat moment is ingelogd, de huidige Active Directory-site van de computer, de homeshare van het netwerk van de gebruiker of de verloopdatum van het wachtwoord van de gebruiker. Dit kan in de vorm van een .plist- of .json-bestand. Deze informatie kan voor inventarisatie- en andere doeleinden worden geparst en naar een Mac-beheeroplossing worden geüpload.

Als u in de Terminal-app het commando 'app-sso -h' uitvoert, krijgt u meer informatie te zien over het gebruik van app-sso.

Mobiele accounts – macOS

Om de Kerberos SSO-extensie te kunnen gebruiken, hoeft uw Mac niet aan Active Directory gekoppeld te zijn. De gebruiker hoeft ook niet met een mobiele account bij de Mac ingelogd te zijn. Apple raadt aan de Kerberos SSO-extensie met een lokale account te gebruiken. Lokale accounts werken het beste bij het aanbevolen implementatiemodel voor macOS. Voor uw Mac-gebruikers is dit ook de beste keuze, want zij maken waarschijnlijk met tussenpozen verbinding met het netwerk van uw organisatie. De Kerberos SSO-extensie is specifiek gemaakt voor een betere integratie van Active Directory via een lokale account.

Als u wilt, kunt u de Kerberos SSO-extensie echter ook met mobiele accounts gebruiken. Voor deze feature gelden de volgende eisen:

- Wachtwoordsynchronisatie werkt niet bij mobiele accounts. Als u uw Active Directory-wachtwoord verandert via de Kerberos SSO-extensie en u bent op uw Mac ingelogd met dezelfde gebruikersaccount als voor de Kerberos SSO-extensie, werkt het wijzigen van wachtwoorden hetzelfde als via het paneel 'Gebruikers en groepen' in Systeemvoorkeuren. Als u uw wachtwoord echter buiten de extensie om verandert (bijvoorbeeld op een website of bij een reset door uw helpdesk), kan de Kerberos SSO-extensie het nieuwe wachtwoord van uw mobiele account niet synchroniseren met uw Active Directory-wachtwoord.
- Het gebruik van een url voor het wijzigen van een wachtwoord met de Kerberos-extensie en een mobiele account wordt niet ondersteund.

Domeinen en realms aan elkaar koppelen

Mogelijk moet een beheerder voor Kerberos een aangepaste koppeling tussen domein en realm maken. Een organisatie kan bijvoorbeeld een Kerberos-realm met de naam 'ad.pretendco.com' hebben, maar de Kerberos-identiteitscontrole nodig hebben voor resources in het domein 'fakecompany.com'.

Opmerking: Bij een Kerberos-implementatie in Apple besturingssystemen worden domeinen en realms in vrijwel elk scenario automatisch aan elkaar gekoppeld. Een beheerder hoeft deze instellingen zelden aan te passen.

Volg deze stappen om de koppeling tussen domein en realm voor de Kerberos SSO-extensie te configureren:

1. Ga in het profiel 'Extensible SSO' naar het gedeelte 'Custom Configuration' en voeg een object met de naam 'domainRealmMapping' toe. Kies bij 'Type' de optie 'Dictionary'.
2. Stel de key van deze dictionary in op de naam van uw realm in hoofdletters.
3. Stel de waarde van deze dictionary in op 'Array'. De eerste waarde is de naam van uw Kerberos-realm in kleine letters, met een punt ervoor. De tweede waarde is de naam van het domein dat de identiteitscontrole tegen dit realm moet uitvoeren, ook met een punt ervoor. Voeg het benodigde aantal array's toe.

Raadpleeg voor meer informatie de documentatie over Kerberos.

Overstappen van Enterprise Connect

Overzicht

De Kerberos SSO-extensie komt in de plaats van Enterprise Connect, een soortgelijke tool die in veel organisaties wordt gebruikt. De meeste organisaties die van Enterprise Connect willen overstappen naar de Kerberos SSO-extensie, kunnen deze stappen volgen:

1. Maak een configuratieprofiel voor de Kerberos SSO-extensie met (ongeveer) dezelfde functionaliteit als uw huidige Enterprise Connect-profiel.
2. Verwijder Enterprise Connect.
3. Implementeer het nieuwe configuratieprofiel voor de Kerberos SSO-extensie.
4. Vraag de gebruikers om in te loggen bij de Kerberos SSO-extensie.

Overstappen op de Kerberos SSO-extensie is geen vereiste om de Macs in uw organisatie te upgraden naar macOS 10.15. Enterprise Connect werkt namelijk nog steeds met macOS 10.15. Toch is het verstandig om de vervanging van Enterprise Connect alvast in uw planning mee te nemen.

Wie niet moeten overstappen

De Kerberos SSO-extensie voldoet aan de behoeften van het overgrote deel van de organisaties die nu Enterprise Connect gebruiken. Organisaties die nu Enterprise Connect gebruiken en aan de volgende criteria voldoen, kunnen echter mogelijk niet of slechts deels overstappen:

- Een organisatie met Macs die nog op macOS 10.14 of ouder draaien, moet op die systemen Enterprise Connect blijven gebruiken. Ze kunnen de Kerberos SSO-extensie alleen in gebruik nemen voor Macs die op macOS 10.15 draaien. De Kerberos SSO-extensie en het bijbehorende configuratieprofiel werken namelijk alleen op Macs met macOS 10.15. Als u ook op de Macs met een ouder besturingssysteem gebruik wilt maken van de Kerberos SSO-extensie, moet u die eerst upgraden naar macOS 10.15.
- Een organisatie die een Mac-beheertool gebruikt die door de gebruiker goedgekeurde MDM-aanmelding niet ondersteunt.
- Een organisatie die geen Mac-beheertool gebruikt.
- Een organisatie met Active Directory op het functieniveau van Windows Server 2003 of ouder.

Een configuratieprofiel voor de Kerberos SSO-extensie maken

U moet een configuratieprofiel voor de Kerberos SSO-extensie maken dat (ongeveer) hetzelfde is als uw Enterprise Connect-configuratieprofiel. Veel Preference Keys in uw huidige Enterprise Connect-configuratieprofiel hebben een equivalente key in een Kerberos SSO-extensieprofiel. In de tabel hieronder ziet u welke key in de Kerberos SSO-extensie equivalent zijn aan de Preference Keys in Enterprise Connect:

Enterprise Connect	Kerberos SSO-extensie	Opmerkingen
adRealm	Realm	Het realm moet in hoofdletters worden ingevoerd.
Automatic login (enabled by default)	allowAutomaticLogin	Voeg dit toe onder 'Custom Configuration'. Stel deze waarde in op 'True' om automatisch inloggen in te schakelen.
disablePasswordFunctions	allowPasswordChange	Voeg dit toe onder 'Custom Configuration'. Stel deze waarde in op 'False' om wachtwoordwijzigingen uit te schakelen.
passwordChangeURL	pwChangeURL	Voeg dit toe onder 'Custom Configuration'.
passwordExpireOverride	pwExpireOverride	Voeg dit toe onder 'Custom Configuration'.
passwordNotificationDays	pwNotificationDays	Voeg dit toe onder 'Custom Configuration'.
prepopulatedUsername	principalName	Voeg dit toe onder 'Custom Configuration'.
pwReqComplexity	pwReqComplexity	Voeg dit toe onder 'Custom Configuration'.
pwReqHistory	pwReqHistory	Voeg dit toe onder 'Custom Configuration'.
pwReqLength	pwReqLength	Voeg dit toe onder 'Custom Configuration'.
pwReqMinimumPasswordAge	pwReqMinAge	Voeg dit toe onder 'Custom Configuration'.
pwReqText	pwReqText	Voeg dit toe onder 'Custom Configuration'. Geef een string op met weer te geven tekst in plaats van een pad naar een .rtf-bestand.
syncLocalPassword	syncLocalPassword	Voeg dit toe onder 'Custom Configuration'.

Opmerking: Mogelijk staan niet alle Preference Keys in uw Enterprise Connect-configuratieprofiel in dit overzicht. In dat geval gaat het waarschijnlijk over functionaliteit die in de Kerberos SSO-extensie niet meer nodig is of niet meer wordt ondersteund.

Enterprise Connect verwijderen

U kunt de Kerberos SSO-extensie en Enterprise Connect niet tegelijk op dezelfde computer draaien. Nadat u bent overgestapt op de Kerberos SSO-extensie, moet u Enterprise Connect verwijderen. Daar moet u beheerdersrechten voor hebben. Volg deze stappen om Enterprise Connect te verwijderen:

Enterprise Connect 2.0 en nieuwer

1. Voer een Unload-actie uit voor de Enterprise Connect-agent: open de Terminal-app en voer 'launchctl unload /Library/LaunchAgents/com.apple.ecAgent' uit als ingelogde gebruiker.
2. Voer een Quit-actie uit voor het menu 'Extra' in Enterprise Connect: open de Terminal-app en voer daar 'killall Enterprise\ Connect\ Menu' in.
3. Verwijder de Enterprise Connect-app uit de map 'Programma's'.
4. Verwijder het Enterprise Connect launchd .plist-bestand in /Bibliotheek/LaunchAgents/com.apple.ecAgent.plist.

Enterprise Connect 1.9.5 en ouder

1. Voer een Quit-actie uit voor Enterprise Connect: voer in de Terminal-app 'killall Enterprise\ Connect' in.
2. Verwijder de Enterprise Connect-app uit de map 'Programma's'.

In de bijlage staat een voorbeeldscript voor het verwijderen van alle versies van Enterprise Connect.

Enterprise Connect-scripttriggers

Enterprise Connect kan een script uitvoeren zodra zich een bepaald event voordoet. Enterprise Connect kan bijvoorbeeld een script uitvoeren zodra het verbindingsproces is voltooid of wanneer de gebruiker zijn wachtwoord verandert. In de Kerberos SSO-extensie werken scripts anders dan in Enterprise Connect. Ze worden namelijk niet door de extensie zelf uitgevoerd. In plaats daarvan post de extensie een gedistribueerde melding bij een event. Die melding kan door een ander proces worden opgepikt, dat vervolgens het gewenste script uitvoert. Zie het gedeelte 'Geavanceerde functies' elders in dit document voor meer informatie.

Hieronder staat een lijst met scripttriggers in Enterprise Connect en de equivalente gedistribueerde melding in de Kerberos SSO-extensie:

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

Netwerkshares

De Kerberos SSO-extensie ondersteunt geen netwerkshares, zoals de thuismap van het netwerk van de gebruiker. U kunt deze functionaliteit grotendeels vervangen door scripts.

Bijlage

Device Management Profile: ExtensibleSingleSignOnKerberos

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

Mobile Device Management Protocol Reference

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

Device Management Profile: ExtensibleSingleSignOnKerberos.ExtensionData

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

Voorbeeldscript – Gedistribueerde meldingen verwerken

De Kerberos SSO-extensie post een gedistribueerde melding zodra zich een bepaald event voordoet, bijvoorbeeld wanneer de gebruiker zijn wachtwoord verandert of wanneer het bedrijfsnetwerk online komt. Als beheerder kunt u die meldingen laten oppikken door scripts of apps die vervolgens de gewenste actie uitvoeren, zoals een script of shellcommando uitvoeren.

Hieronder staat een voorbeeldscript dat scripts of commando's laat uitvoeren wanneer een melding wordt gepost. Het moet worden uitgevoerd als LaunchAgent (ingelogde gebruiker) of LaunchDaemon (root). Het script moet twee verplichte parameters bevatten:

- **-notification** is de naam van de gedistribueerde melding die voor u van belang is. Zie pagina 11 voor voorbeelden.
- **-action** is de actie die moet worden uitgevoerd voor een geposte melding. Voorbeeld: 'sh /path/to/script.sh'.

Om het script te kunnen uitvoeren, moet u de commandoregeltools voor ontwikkelaars installeren. Op de Apple Developer-website vindt u een installatiepakket voor deze tools.

```
#!/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()
```

Voorbeeldscript – Enterprise Connect verwijderen

Met dit voorbeeldscript verwijdert u alle versies van Enterprise Connect. U kunt het script handmatig of in een Mac-beheeroplossing uitvoeren. Dit script moet met roottoegangsrechten worden uitgevoerd.

```
#!/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
```