Kerberos Single Sign-On Erweiterung

Benutzerhandbuch

Dezember 2019

Inhalt

Einführung **3**

Erste Schritte **4**

Erweiterte Funktionen **8**

Der Wechsel von Enterprise Connect **13**

Anhang **16**

Einführung

Die Kerberos Single Sign-On (SSO) Erweiterung macht es einfach, die Kerberos basierte Gesamtauthentifizierung auf den Apple Geräten des Unternehmens zu nutzen.

Vereinfachte Kerberos Authentifizierung

Die Kerberos SSO Erweiterung vereinfacht den Prozess, ein Kerberos Ticket-Granting Ticket (TGT) aus der Active Directory Domain des Unternehmens zu erhalten, und ermöglicht Benutzern eine nahtlose Authentifizierung bei Ressourcen wie Websites, Apps und Dateiservern. In macOS fordert die Kerberos SSO Erweiterung bei Änderungen des Netzwerkstatus proaktiv ein Kerberos TGT an, um dafür zu sorgen, dass der Benutzer sich bei Bedarf authentifizieren kann.

Active Directory Accountverwaltung

Die Kerberos SSO Erweiterung hilft den Benutzern außerdem, ihre Active Directory Accounts zu verwalten. In macOS ermöglicht sie Benutzern, ihre Active Directory Passwörter zu ändern und benachrichtigt sie, wenn ein Passwort bald abläuft. Benutzer können außerdem die Passwörter ihrer lokalen Accounts ändern, um sie mit ihren Active Directory Passwörtern abzugleichen.

Active Directory Unterstützung

Die Kerberos SSO Erweiterung sollte mit einer Active Directory Domain vor Ort verwendet werden. Azure Active Directory wird nicht unterstützt. Um die Kerberos SSO Erweiterung zu nutzen, müssen die Geräte nicht mit einer Active Directory Domain verbunden sein. Außerdem müssen sich Benutzer nicht mit Active Directory oder mobilen Accounts bei ihren Mac Computern anmelden. Apple empfiehlt, stattdessen lokale Accounts zu verwenden.

Voraussetzungen

- iOS 13, iPadOS oder macOS Catalina.
- Eine Active Directory Domain mit Windows Server 2008 oder neuer. Die Kerberos SSO Erweiterung ist nicht für die Verwendung mit Azure Active Directory vorgesehen. Sie erfordert eine herkömmliche Active Directory Domain vor Ort.
- Zugriff auf das Netzwerk, in dem die Active Directory Domain gehostet wird. Dieser Zugriff auf das Netzwerk kann über WLAN, Ethernet oder VPN erfolgen.
- Die Geräte müssen mit einer Lösung für die mobile Geräteverwaltung (Mobile Device Management, MDM) mit Unterstützung für die Konfigurationsprofil-Payload für das erweiterbare Single Sign-On (SSO) verwaltet werden. Erkundigen Sie sich bei Ihrem MDM-Anbieter bezüglich der Unterstützung dieser Konfigurationsprofil-Payload.

Enterprise Connect

Die Kerberos SSO Erweiterung soll Enterprise Connect ersetzen. Wenn Sie aktuell Enterprise Connect verwenden und zur Kerberos SSO Erweiterung wechseln möchten, finden Sie im Abschnitt „Wechsel von Enterprise Connect“ in diesem Dokument weitere Informationen.

Erste Schritte

Ein Konfigurationsprofil erstellen und implementieren

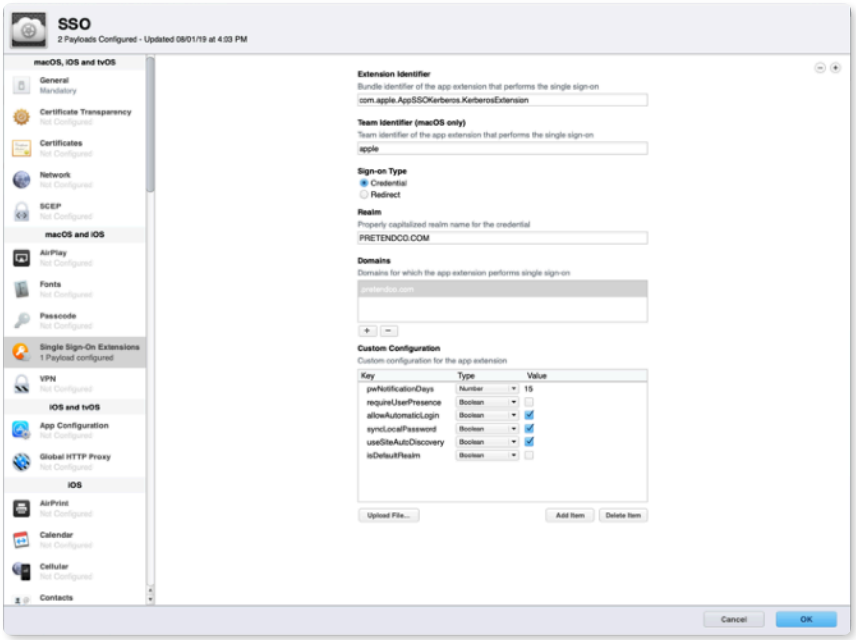
Um die Kerberos SSO Erweiterung zu nutzen, brauchen Sie ein Konfigurationsprofil, das von einer MDM-Lösung auf das Gerät übertragen wird.

Hinweis: Das Konfigurationsprofil muss über MDM auf das Gerät übertragen werden. In macOS muss das eine vom Benutzer genehmigte MDM-Registrierung sein und im Systemumfang installiert werden. Das manuelle Hinzufügen des Profils wird nicht unterstützt.

Die Konfiguration mit einem Konfigurationsprofil ist mit der erweiterbaren SSO Payload möglich, die in iOS 13, iPadOS und macOS 10.15 eingeführt wurde. Der Profilmanager – Teil von macOS Server – unterstützt die erweiterbare SSO Payload. Wenn Ihre MDM-Lösung diese Payload noch nicht unterstützt, können Sie eventuell das erforderliche Profil im Profilmanager erstellen und es dann zum Verteilen in Ihre MDM-Lösung importieren. Kontaktieren Sie Ihren MDM-Anbieter für weitere Informationen.

Führen Sie die folgenden Schritte aus, um ein Konfigurationsprofil mit dem Profilmanager zu erstellen:

1. Melden Sie sich beim Profilmanager an.
2. Erstellen Sie ein Profil für eine Gerätegruppe oder ein bestimmtes Gerät.
3. Wählen Sie „Single Sign-On Extensions“ in der Payload-Liste und klicken Sie dann auf die Taste zum Hinzufügen (+), um eine neue Payload hinzuzufügen.
4. Geben Sie „com.apple.AppSSOKerberos.KerberosExtension“ im Feld „Extension Identifier“ ein.
5. Geben Sie „apple“ im Feld „Team Identifier“ ein.



6. Wählen Sie unter „Sign-on Type“ die Option „Credential“ aus.
7. Geben Sie im Feld „Realm“ in Großbuchstaben den Namen Ihrer Active Directory Domain ein, wo Ihre Benutzeraccounts zu finden sind. Geben Sie nicht den Namen Ihrer Active Directory Gesamtstruktur an, es sei denn, Ihre Benutzeraccounts befinden sich auf der Ebene der Gesamtstruktur.

8. Klicken Sie unter „Domains“ auf die Taste zum Hinzufügen (+) und fügen Sie für alle Ressourcen, die Kerberos verwenden, Domains hinzu. Wenn Sie z. B. die Kerberos Authentifizierung für Ressourcen auf us.pretendco.com nutzen, fügen Sie „.us.pretendco.com“ hinzu. (Vergessen Sie nicht den Punkt am Anfang.)
9. Fügen Sie unter „Custom Configuration“ die folgenden Werte hinzu:

Key	Type	Value
pwNotificationDays	Number	15
requireUserPresence	Boolean	Nicht markiert
allowAutomaticLogin	Boolean	Markiert
syncLocalPassword	Boolean	Markiert
useSiteAutoDiscovery	Boolean	Markiert
isDefaultRealm	Boolean	Nicht markiert

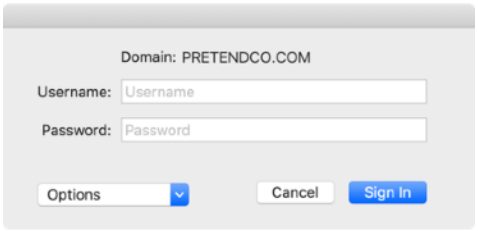
10. Klicken Sie auf „OK“, um das neue Konfigurationsprofil zu speichern. Es wird automatisch auf dem ausgewählten Gerät oder der Gerätegruppe installiert.

Benutzereinrichtung – iOS und iPadOS

1. Verbinden Sie Ihr Gerät mit einem Netzwerk, in dem die Active Directory Domain Ihrer Organisation verfügbar ist.
2. Führen Sie einen der folgenden Schritte aus:
   - Rufen Sie mit Safari eine Website auf, die die Kerberos Authentifizierung unterstützt.
   - Starten Sie eine App, die die Kerberos Authentifizierung unterstützt.
3. Geben Sie Ihren Benutzernamen und Ihr Passwort für Kerberos oder Active Directory ein.
4. Sie werden gefragt, ob Sie sich automatisch dauerhaft anmelden möchten. Die meisten Benutzer sollten „Yes“ auswählen.
5. Tippen Sie auf „Sign In“. Nach einer kurzen Pause wird Ihre Website oder App geladen. Wenn Sie sich für eine automatische Anmeldung bei der Kerberos SSO Erweiterung entschieden haben, werden Sie nicht mehr zur Eingabe Ihrer Anmeldedaten aufgefordert, bis Sie Ihr Passwort ändern. Wenn Sie sich nicht für die automatische Anmeldung entschieden haben, werden Sie erst nach Ablauf Ihrer Kerberos Anmeldedaten zur Eingabe der Anmeldedaten aufgefordert – für gewöhnlich nach 10 Stunden.

Benutzereinrichtung – macOS

1. Sie müssen sich bei der Kerberos SSO Erweiterung authentifizieren. Sie können diesen Prozess auf mehrere Arten beginnen:
   - Wenn Ihr Mac mit dem Netzwerk verbunden ist, in dem Ihre Active Directory Domain verfügbar ist, werden Sie sofort nach der Installation des erweiterbaren SSO Konfigurationsprofils aufgefordert, sich zu authentifizieren.
   - Wenn Sie Safari verwenden, um auf eine Website zuzugreifen, die die Kerberos Authentifizierung akzeptiert, oder wenn Sie eine App nutzen, die eine Kerberos Authentifizierung erfordert, werden Sie aufgefordert, sich zu authentifizieren.
   - Sie werden sofort zur Authentifizierung aufgefordert, wenn Sie Ihren Mac mit einem Netzwerk verbinden, in dem Ihre Active Directory Domain verfügbar ist.
   - Sie können die Menüerweiterung für die Kerberos SSO Erweiterung auswählen und dann auf „Sign In" klicken.
2. Sie werden aufgefordert, Ihre Kerberos Anmeldedaten einzugeben. Geben Sie Ihren Benutzernamen und Ihr Passwort für Kerberos oder Active Directory ein.



3. Sie werden gefragt, ob Sie sich automatisch anmelden möchten. Die meisten Benutzer sollten „Yes" auswählen.
4. Klicken Sie auf „Sign In". Nach einer kurzen Pause wird Ihre Website oder App geladen. Wenn Sie sich für eine automatische Anmeldung bei der Kerberos SSO Erweiterung entschieden haben, werden Sie nicht mehr zur Eingabe Ihrer Anmeldedaten aufgefordert, bis Sie Ihr Passwort ändern. Wenn Sie sich nicht für die automatische Anmeldung entschieden haben, werden Sie erst nach Ablauf Ihrer Kerberos Anmeldedaten zur Eingabe der Anmeldedaten aufgefordert – für gewöhnlich nach 10 Stunden.
5. Wenn Ihr Passwort bald abläuft, erhalten Sie eine Benachrichtigung, in der Ihnen mitgeteilt wird, wie viele Tage bis zum Ablauf noch bleiben. Sie können auf die Benachrichtigung klicken und Ihr Passwort ändern.
6. Wenn Sie das Feature zum Synchronisieren des Passworts aktiviert haben, werden Sie nach Ihrem aktuellen Active Directory Passwort und dem aktuellen lokalen Passwort gefragt. Geben Sie beide ein und klicken Sie dann auf „OK", um Ihre Passwörter zu synchronisieren. Sie sehen diese Aufforderung auch bei der ersten Anmeldung, selbst wenn Ihre Passwörter bereits synchronisiert sind.

Passwort ändern – macOS

Sie können Ihr Active Directory Passwort auch mit der Kerberos SSO Erweiterung ändern:

1. Vergewissern Sie sich, dass Sie bei der Kerberos SSO Erweiterung angemeldet sind.
2. Wählen Sie die Kerberos SSO Menüerweiterung aus und gehen Sie auf „Change Password". Eventuell erhalten Sie auch eine Benachrichtigung, dass Ihr Passwort abläuft.
3. Geben Sie zuerst Ihr aktuelles Passwort ein und dann Ihr neues Passwort. Wählen Sie ein neues Passwort, das den Passwortanforderungen Ihrer Organisation entspricht. Klicken Sie auf „OK".
4. Nach einer kurzen Pause wird ein Dialog angezeigt, der Ihnen mitteilt, dass die Passwortänderung erfolgreich war. Wenn das Feature zum Synchronisieren des Passworts aktiviert ist, wird das Passwort Ihres lokalen Accounts aktualisiert, damit es mit Ihrem neuen Active Directory Passwort übereinstimmt.

Kerberos SSO Menüerweiterung verwenden – macOS

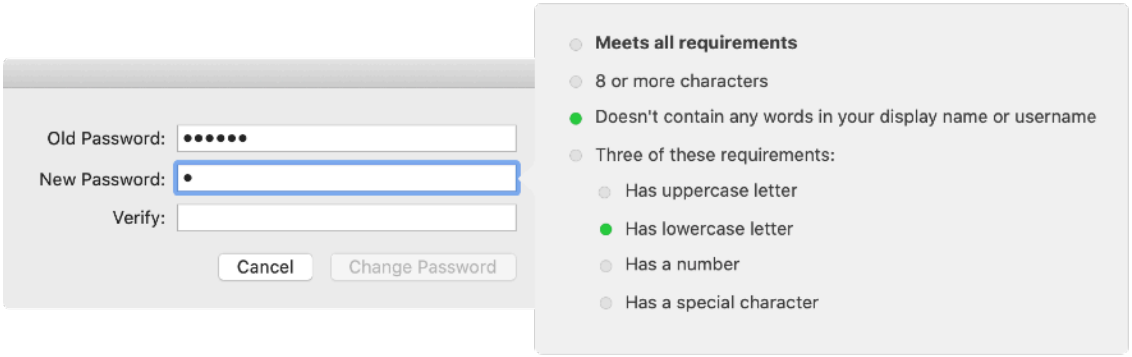
Mit der Kerberos SSO Menüerweiterung können Sie einfach hilfreiche Informationen über Ihren Account und die Funktionen der Erweiterung aufrufen. Sie wird als grauer oder schwarzer Schlüssel in der Menüleiste oben rechts angezeigt.

Die Farbe des Symbols für die Kerberos SSO Menüerweiterung zeigt Ihnen Statusinformationen zu Ihrem Account an. Wenn der Schlüssel grau ist, sind Sie nicht bei der Erweiterung angemeldet. Ein schwarzer Schlüssel zeigt, dass Sie angemeldet sind. Nachdem Sie den Schlüssel ausgewählt haben, sehen Sie, mit welchem Account Sie angemeldet sind und wie viele Tage bis zum Ablauf Ihres Passworts bleiben. Sie können sich im Menü außerdem an- und abmelden und Ihr Passwort ändern.

Erweiterte Funktionen

Live-Passwortprüfung

In vielen Active Directory Konfigurationen kann die Kerberos SSO Erweiterung neue Benutzerpasswörter bei der Eingabe überprüfen und Benutzern mitteilen, welche Passwortanforderungen sie erfüllen müssen, um ihre Passwörter zu ändern. Bei der Konfiguration sieht der Benutzer diese Ansicht, wenn er das neue Passwort eingibt:



Um diese Funktion zu nutzen, kann Ihre Active Directory Domain nur die Standard-Passwortrichtlinien von Active Directory verwenden. Standardmäßig ermöglicht Active Directory einem Administrator, ein komplexes Passwort und eine bestimmte Länge zu verlangen. Weitere Infos darüber, welche Eigenschaften ein komplexes Passwort hat, finden Sie unter technet.microsoft.com/en-us/library/cc786468(v=ws.10).aspx.

Hinweis: Sie können diese Funktion möglicherweise nicht nutzen, wenn Ihre Domain Tools oder DLLs von anderen Anbietern verwendet, um die Standard-Passwortrichtlinie von Active Directory zu erweitern. Wenn Sie z. B. bestimmte Wörter oder Ihren Benutzernamen nicht in Ihrem Passwort verwenden dürfen oder wenn Sie eine bestimmte Anzahl von Sonderzeichen in Ihrem Passwort verwenden müssen, nutzen Sie vermutlich Passwortrichtlinien-Erweiterungen von anderen Anbietern. Wenn Sie sich nicht sicher sind, fragen Sie Ihren Active Directory Administrator nach weiteren Informationen.

Wenn die Active Directory Domain Ihres Unternehmens die Anforderungen erfüllt, können Sie die Live-Passwortprüfung aktivieren. Legen Sie in Ihrem Konfigurationsprofil der Kerberos SSO Erweiterung die folgenden Parameter fest:

Parameter	Key	Type	Value	Optional
Komplexe Passwörter verlangen	pwReqComplexity	Boolean	JA	Nein
Erforderliche Passwortlänge	pwReqLength	Integer	Number	Ja
Erneute Verwendung früherer Passwörter	pwReqHistory	Integer	Number	Ja
Mindestalter für das Passwort	pwReqMinAge	Integer	Number	Ja

Die Live-Passwortprüfung hat einige Einschränkungen. Sie kann nicht überprüfen, ob ein Passwort bereits verwendet wurde. Sie kann ebenfalls nicht überprüfen, ob Ihr Passwort Ihren angezeigten Active Directory Namen enthält, wenn Sie nicht bereits ein Kerberos TGT haben. Das kann der Fall sein, wenn Sie Ihr Passwort zum ersten Mal festlegen oder wenn Ihr Passwort abgelaufen ist. Alle weiteren Prüfungen funktionieren normal.

Anzeige der Passwortanforderungen

Wenn Sie die Live-Passwortprüfung nicht verwenden können, ist es möglich, die Kerberos SSO Erweiterung so zu konfigurieren, dass ein Textstring mit den Passwortanforderungen Ihrer Organisation angezeigt wird, wenn die Benutzer ihre neuen Passwörter eingeben. Ändern Sie in Ihrem Konfigurationsprofil der Kerberos SSO Erweiterung „pwReqText" zu einem String, der den Text enthält, den Sie einem Benutzer bei Passwortänderungen anzeigen möchten.

Passwort-Funktionalität ändern oder deaktivieren

Einige Organisationen können die Standard-Funktionalität zur Passwortänderung der Kerberos SSO Erweiterung möglicherweise nicht nutzen, da sie keine Passwortänderungen für Active Directory zulassen. Definieren Sie in Ihrem Konfigurationsprofil der Kerberos SSO Erweiterung „allowPasswordChanges" mit „FALSE", um diese Funktionalität zu deaktivieren.

Website-unterstützte Passwortänderung – macOS

Die Kerberos SSO Erweiterung kann so konfiguriert werden, dass eine Website für die Passwortänderung im Standardbrowser geöffnet wird, wenn der Benutzer „Change password" auswählt oder einen Hinweis zum Ablauf des Passworts bestätigt. Apple empfiehlt, diese Funktion nur mit einem lokalen Account zu verwenden, da mobile Accounts nicht unterstützt werden.

Ändern Sie in Ihrem Konfigurationsprofil der Kerberos SSO Erweiterung „pwChangeURL" zur URL Ihrer Website für die Passwortänderung. Sobald die Benutzer ihre Passwörter geändert haben, müssen sie sich bei der Kerberos Erweiterung abmelden und sich dann mit ihren aktualisierten Passwörtern wieder anmelden. Wenn die lokale Passwortsynchronisierung aktiviert ist, werden die Benutzer durch das Synchronisieren ihrer Passwörter geführt.

Passwortsynchronisierung – macOS

Die Kerberos SSO Erweiterung kann das lokale Account-Passwort an das Active Directory Passwort eines Benutzers anpassen. Aktivieren Sie diese Funktion, indem Sie „syncLocalPassword" im Abschnitt „Custom Configuration" Ihres Konfigurationsprofils der Kerberos SSO Erweiterung auf „TRUE" setzen.

Die Passwortsynchronisierung umfasst zwei grundlegende Funktionen. Wenn der Benutzer die Kerberos SSO Erweiterung zum Ändern von Passwörtern verwendet, gleicht diese Funktion sein lokales Passwort an sein Active Directory Passwort an. Sollten das lokale und das Active Directory Passwort nicht mehr synchron sein, synchronisiert die Kerberos SSO Erweiterung diese wie folgt wieder:

- Bei der Aktivierung der Passwortsynchronisierung und bei jedem weiteren Verbindungsversuch durch die Kerberos SSO Erweiterung werden die Daten, an denen Benutzer ihre lokalen und Active Directory Passwörter zuletzt geändert haben, mit den im Cache gespeicherten Werten verglichen. Wenn die Werte übereinstimmen, sind die Passwörter synchronisiert und es ist keine Aktion erforderlich. Stimmen sie nicht überein, fordert die Kerberos SSO Erweiterung die Benutzer zur Eingabe des lokalen und des Active Directory Passworts auf. Sobald Benutzer ihre lokalen Passwörter eingegeben haben, passt die Kerberos SSO Erweiterung ihr lokales Passwort an ihr Active Directory Passwort an.
- Passwortänderungen funktionieren auf ähnliche Weise. Wenn Benutzer ein Passwort mit der Kerberos SSO Erweiterung ändern, werden ihre alten Active Directory Passwörter mit den lokalen Accounts verglichen. Wenn ein altes Active Directory Passwort und das lokale Passwort übereinstimmen, ändert die Kerberos SSO Erweiterung beide Passwörter. Wenn sie nicht übereinstimmen, wird nur das Active Directory Passwort geändert. Die Benutzer werden dann beim nächsten Verbindungsversuch aufgefordert, ihr lokales Passwort einzugeben.

Diese Funktion hat folgende Anforderungen:

- Wenn Benutzer bei ihren Mac Computern mit Active Directory Accounts und nicht mit lokalen Accounts angemeldet sind, ist die Passwortsynchronisierung deaktiviert. Diese Funktion ist nur für die Verwendung mit lokalen Accounts vorgesehen; wenn Benutzer mit Active Directory Accounts bei ihren Mac Computern angemeldet sind, ist diese Funktion nicht notwendig.
- Wenn eine Passwortrichtlinie für lokale Accounts durchgesetzt wird – wie z. B. die Verwendung eines Konfigurationsprofils oder des pwpolicy-Befehls –, vergewissern Sie sich, dass die lokale Passwortrichtlinie mit der Active Directory Passwortrichtlinie übereinstimmt oder weniger restriktiv ist. Wenn die lokalen Passwortrichtlinie restriktiver ist als die Active Directory Richtlinie, akzeptiert die Kerberos SSO Erweiterung möglicherweise ein Passwort, das die Anforderungen von Active Directory erfüllt, kann aber das lokale Passwort nicht festlegen, da das Passwort nicht den lokalen Passwortanforderungen entspricht. Wenn die lokale Passwortrichtlinie restriktiver sein muss als die Active Directory Passwortrichtlinie, sollten Sie diese Funktion nicht verwenden.
- Der lokale Benutzername unterscheidet sich von dem Active Directory Benutzernamen – nur die Passwörter werden so festgelegt, dass sie übereinstimmen.

Smart Card Unterstützung – macOS

Die Kerberos SSO Erweiterung unterstützt die Verwendung von Smart Card basierten Identitäten für die Authentifizierung. Smart Cards müssen über einen CryptoTokenKit-Treiber verfügen; TokenD-basierte Treiber werden nicht unterstützt. macOS 10.15 unterstützt den PIV-Standard, der von der amerikanischen Regierung häufig verwendet wird.

Vergewissern Sie sich vor Beginn, dass Ihre Active Directory Domain so konfiguriert ist, dass sie die Smart Card Authentifizierung unterstützt. Der Prozess zur Aktivierung der Smart Card Authentifizierung bei Active Directory sprengt den Rahmen dieses Dokuments. Weitere Einzelheiten finden Sie in der Dokumentation von Microsoft.

Für die Anmeldung bei der Kerberos SSO Erweiterung mit einer Smart Card befolgen Sie diese Schritte:

1. Klicken Sie auf das Menü „Options“ und wählen Sie dann „Use a smart card“.
2. Wenn die Taste „Identity“ angezeigt wird, setzen Sie Ihre Smart Card ein und klicken Sie auf die Taste.
3. Wählen Sie die Identität, mit der Sie sich authentifizieren möchten, klicken Sie auf „OK“ und dann auf „Sign In“.
4. Geben Sie Ihre PIN ein, wenn Sie dazu aufgefordert werden.

Wenn die Kerberos SSO Erweiterung ein Kerberos TGT anfordern muss, werden Sie aufgefordert, Ihre Smart Card einzusetzen und Ihre PIN einzugeben. Weitere Informationen über die Smart Card Unterstützung in macOS erhalten Sie, wenn Sie in Terminal „man SmartCardServices“ ausführen.

Verteilte Benachrichtigungen – macOS

Die Kerberos SSO Erweiterung postet verteilte Benachrichtigungen bei verschiedenen Ereignissen. Apps und Dienste in macOS informieren andere Apps und Dienste mit verteilten Benachrichtigungen darüber, dass ein Ereignis eingetreten ist. Eine App oder ein Dienst, die auf dieses Ereignis achten, können bestimmte Aktionen ausführen, wenn das Ereignis eintritt.

Ein Administrator kann diese Funktionalität nutzen, um bei bestimmten Ereignissen bestimmte Aktionen durchzuführen. So kann ein Administrator z. B. jedes Mal ein Skript ausführen, wenn die Kerberos SSO Erweiterung neue Kerberos Anmeldedaten anfordert.

Die Kerberos SSO Erweiterung postet einfach verteilte Benachrichtigungen bei bestimmten Ereignissen. Sie führt keine Aktionen aus, wenn diese Ereignisse eintreten. Der Administrator muss ein Tool einsetzen, mit dem diese Benachrichtigungen verfolgt und Aktionen ausgeführt werden, wenn sie eintreten.

Im Anhang finden Sie ein Beispiel für ein Skript und eine launchd-Eigenschaftsliste (.plist), die Benachrichtigungen verfolgen und Aktionen ausführen können. Modifizieren Sie dieses Beispiel nach Bedarf für Ihre Implementierung.

Unten finden Sie verteilte Benachrichtigungen, die von der Kerberos SSO Erweiterung gepostet wurden:

Name	Gepostet bei diesem Ereignis
com.apple.KerberosPlugin.ConnectionCompleted	Die Kerberos SSO Erweiterung hat ihren Verbindungsprozess ausgeführt.
com.apple.KerberosPlugin.ADPasswordChanged	Der Benutzer hat das Active Directory Passwort mit der Erweiterung geändert.
com.apple.KerberosPlugin.LocalPasswordSynced	Der Benutzer hat das Active Directory Passwort und das lokale Passwort synchronisiert.
com.apple.KerberosPlugin.InternalNetworkAvailable	Der Benutzer hat sich mit einem Netzwerk verbunden, in dem die konfigurierte Active Directory Domain verfügbar ist.
com.apple.KerberosPlugin.InternalNetworkNotAvailable	Der Benutzer hat sich mit einem Netzwerk verbunden, in dem die konfigurierte Active Directory Domain nicht verfügbar ist.
com.apple.KerberosExtension.gotNewCredential	Der Benutzer hat ein neues Kerberos TGT erhalten.
com.apple.KerberosExtension.passwordChangedWithPasswordSync	Der Benutzer hat das Active Directory Passwort geändert, und das lokale Passwort wurde aktualisiert, um dem neuen Active Directory Passwort zu entsprechen.

Befehlszeilen-Unterstützung – macOS

Administratoren können mit einem Befehlszeilen-Tool namens *app-sso* die Kerberos SSO Erweiterung steuern und auf nützliche Informationen zugreifen. Sie können mit dem Tool z. B. die An- und Abmeldung sowie Passwortänderungen initiieren. Es kann außerdem nützliche Informationen, wie den aktuell angemeldeten Benutzer, die aktuelle Active Directory Site des Computers, die Netzwerkfreigaben des Benutzers, wann das Passwort des Benutzers abläuft und mehr, in einer Eigenschaftsliste oder im JSON-Format ausdrucken. Diese Informationen können gegliedert und für ein Bestandsverzeichnis und andere Zwecke in eine Verwaltungslösung für Mac geladen werden.

Weitere Informationen zum Einsatz von app-sso erhalten Sie, wenn Sie „app-sso -h" in der Terminal App ausführen.

Mobile Accounts – macOS

Die Kerberos SSO Erweiterung erfordert nicht, dass Ihr Mac mit Active Directory verbunden oder der Benutzer mit einem mobilen Account beim Mac angemeldet ist. Apple empfiehlt, die Kerberos SSO Erweiterung mit einem lokalen Account zu nutzen. Lokale Accounts funktionieren am besten mit dem empfohlenen Implementierungsmodell für macOS und sind die beste Wahl für Mac Benutzer von heute, die sich vielleicht nur vorübergehend mit dem Netzwerk Ihrer Organisation verbinden. Die Kerberos SSO Erweiterung wurde speziell dafür entwickelt, die Active Directory Integration von einem lokalen Account aus zu verbessern.

Sollten Sie sich jedoch dafür entscheiden, weiterhin mobile Accounts zu verwenden, können Sie trotzdem die Kerberos SSO Erweiterung nutzen. Diese Funktion hat folgende Anforderungen:

- Die Passwortsynchronisierung funktioniert nicht mit mobilen Accounts. Wenn Sie mit der Kerberos SSO Erweiterung Ihr Active Directory Passwort ändern und mit demselben Benutzeraccount, den Sie mit der Kerberos SSO Erweiterung nutzen, bei Ihrem Mac angemeldet sind, funktionieren Passwortänderungen wie in der Systemeinstellung „Users & Groups". Wenn Sie jedoch eine externe Passwortänderung vornehmen, indem Sie Ihr Passwort auf einer Website ändern oder Ihr Help Desk es zurücksetzt, kann die Kerberos SSO Erweiterung das Passwort Ihres mobilen Accounts nicht wieder mit Ihrem Active Directory Passwort synchronisieren.
- Eine URL zur Passwortänderung mit der Kerberos Erweiterung und einem mobilen Account wird nicht unterstützt.

Domain-Realm-Zuordnung

Ein Administrator muss möglicherweise eine eigene Domain-Realm-Zuordnung für Kerberos definieren. Eine Organisation kann z. B. einen Kerberos Realm namens „ad.pretendco.com" haben, muss aber möglicherweise die Kerberos Authentifizierung für Ressourcen in der Domain „fakecompany.com" verwenden.

Hinweis: Die Kerberos Implementierung auf Apple Betriebssystemen kann in fast allen Situationen automatisch die Domain-Realm-Zuordnung bestimmen. Es ist sehr selten, dass ein Administrator diese Einstellungen anpasst.

Die Domain-Realm-Zuordnung kann für die Kerberos SSO Erweiterung wie folgt konfiguriert werden:

1. Fügen Sie im Abschnitt „Custom Configuration" des erweiterbaren SSO-Profils ein Objekt namens „domainRealmMapping" hinzu. Der Objekttyp sollte „Dictionary" sein.
2. Bezeichnen Sie den Schlüssel dieses Verzeichnisses mit dem Namen Ihres Realms in Großbuchstaben.
3. Stellen Sie für den Wert dieses Verzeichnisses den Typ „Array" ein. Der erste Wert sollte der Name Ihres Kerberos Realms in Kleinbuchstaben sein, beginnend mit einem Punkt. Der zweite Wert sollte der Name der Domain sein, die sich in diesem Realm authentifizieren muss, und ebenfalls mit einem Punkt beginnen. Fügen Sie je nach Bedarf Arrays hinzu.

Weitere Informationen finden Sie in der Kerberos Dokumentation.

Der Wechsel von Enterprise Connect

Überblick

Die Kerberos SSO Erweiterung soll Enterprise Connect ersetzen, ein ähnliches Tool, das viele Organisationen bereits verwenden. Die meisten Organisationen, die von Enterprise Connect auf die Kerberos SSO Erweiterung wechseln, werden diese Schritte befolgen:

1. Erstellen Sie ein Konfigurationsprofil für die Kerberos SSO Erweiterung, das eine ähnliche Funktionalität wie Ihr aktuelles Enterprise Connect Profil hat.
2. Deinstallieren Sie Enterprise Connect.
3. Implementieren Sie das neue Konfigurationsprofil der Kerberos SSO Erweiterung.
4. Bitten Sie die Benutzer, sich bei der Kerberos SSO Erweiterung anzumelden.

Der Wechsel auf die Kerberos SSO Erweiterung ist nicht erforderlich, um die Mac Computer Ihrer Organisation auf macOS 10.15 zu aktualisieren. Enterprise Connect funktioniert wie erwartet mit macOS 10.15, aber Organisationen sollten dennoch einen möglichen Wechsel von Enterprise Connect planen.

Wer nicht wechseln sollte

Die Kerberos SSO Erweiterung wird die Anforderungen der meisten Organisationen erfüllen, die Enterprise Connect nutzen. Eine Organisation mit den folgenden Kriterien kann jedoch möglicherweise nicht oder nur teilweise von Enterprise Connect wechseln:

- Eine Organisation, die aktuell Mac Computer mit macOS 10.14 oder älter nutzt, sollte Enterprise Connect auf diesen Systemen laufen lassen und nur Mac Computer mit macOS 10.15 auf die Kerberos SSO Erweiterung umstellen. Die Kerberos SSO Erweiterung und das zugehörige Konfigurationsprofil funktionieren nur auf Mac Computern mit MacOS 10.15. Aktualisieren Sie diese Systeme auf macOS 10.15, um die Vorteile der Kerberos SSO Erweiterung zu nutzen.
- Eine Organisation, die ein Mac Verwaltungstool verwendet, das keine benutzergenehmigte MDM-Registrierung unterstützt.
- Eine Organisation, die kein Verwaltungstool verwendet.
- Eine Organisation, die eine Active Directory Funktionsebene von Windows Server 2003 oder älter verwendet.

Ein Konfigurationsprofil für die Kerberos SSO Erweiterung erstellen

Sie müssen ein Konfigurationsprofil für die Kerberos SSO Erweiterung erstellen, das Ihrem Enterprise Connect Konfigurationsprofil ähnelt. Viele Preference Keys in Ihrem aktuellen Enterprise Connect Konfigurationsprofil haben Entsprechungen in einem Kerberos SSO Erweiterungsprofil. Sehen Sie sich zunächst die nachfolgende Tabelle an, die eine Übersicht der den Enterprise Connect Preference Keys entsprechenden Kerberos SSO Erweiterungen enthält:

Enterprise Connect	Kerberos SSO Erweiterung	Notizen
adRealm	Realm	Realm muss in Großbuchstaben geschrieben werden.
Automatic login (enabled by default)	allowAutomaticLogin	Zum Abschnitt „Custom Configuration“ hinzufügen. Muss auf „True“ gesetzt werden, damit die automatische Anmeldung funktioniert.
disablePasswordFunctions	allowPasswordChange	Zum Abschnitt „Custom Configuration“ hinzufügen. Auf „False“ setzen, um Passwortänderungen zu deaktivieren.
passwordChangeURL	pwChangeURL	Zum Abschnitt „Custom Configuration“ hinzufügen.
passwordExpireOverride	pwExpireOverride	Zum Abschnitt „Custom Configuration“ hinzufügen.
passwordNotificationDays	pwNotificationDays	Zum Abschnitt „Custom Configuration“ hinzufügen.
prepopulatedUsername	principalName	Zum Abschnitt „Custom Configuration“ hinzufügen.
pwReqComplexity	pwReqComplexity	Zum Abschnitt „Custom Configuration“ hinzufügen.
pwReqHistory	pwReqHistory	Zum Abschnitt „Custom Configuration“ hinzufügen.
pwReqLength	pwReqLength	Zum Abschnitt „Custom Configuration“ hinzufügen.
pwReqMinimumPasswordAge	pwReqMinAge	Zum Abschnitt „Custom Configuration“ hinzufügen.
pwReqText	pwReqText	Zum Abschnitt „Custom Configuration“ hinzufügen. Einen Textstring zum Anzeigen statt eines Pfades zu einer RTF-Datei eingeben.
syncLocalPassword	syncLocalPassword	Zum Abschnitt „Custom Configuration“ hinzufügen.

Hinweis: Einige Preference Keys in Ihrem Enterprise Connect Konfigurationsprofil sind hier möglicherweise nicht aufgelistet. Dabei könnte es sich um Funktionen handeln, die in der Kerberos SSO Erweiterung nicht mehr benötigt werden oder die nicht mehr unterstützt werden.

Enterprise Connect deinstallieren

Die gleichzeitige Ausführung der Kerberos SSO Erweiterung und von Enterprise Connect auf demselben Computer wird nicht unterstützt. Deinstallieren Sie Enterprise Connect nach dem Wechsel auf die Kerberos SSO Erweiterung. Sie brauchen Administratorrechte, um die Deinstallation durchzuführen. Führen Sie die folgenden Schritte aus, um Enterprise Connect zu deinstallieren:

Enterprise Connect 2.0 und neuer

1. Entfernen Sie den Enterprise Connect Agent, indem Sie die Terminal App starten und„launchctl unload /Library/LaunchAgents/com.apple.ecAgent" als aktuell angemeldeter Benutzer ausführen.
2. Beenden Sie die Enterprise Connect Menüerweiterung, indem Sie die Terminal App starten und „killall Enterprise\ Connect\ Menu" ausführen.
3. Löschen Sie die Enterprise Connect App aus dem Ordner „Applications".
4. Löschen Sie die Enterprise Connect launchd .plist unter „/Library/LaunchAgents/com.apple.ecAgent.plist".

Enterprise Connect 1.9.5 und älter

1. Schließen Sie Enterprise Connect, indem Sie die Terminal App starten und „killall Enterprise\ Connect" ausführen.
2. Löschen Sie die Enterprise Connect App aus dem Ordner „Applications".

Im Anhang finden Sie ein Beispiel für ein Skript, mit dem jede Enterprise Connect Version gelöscht werden kann.

Enterprise Connect Skript-Auslöser (Trigger)

Enterprise Connect kann Skripte ausführen, wenn bestimmte Ereignisse eintreten. Enterprise Connect kann z. B. ein Skript ausführen, wenn der Verbindungsaufbau abgeschlossen ist oder wenn der Benutzer das Passwort ändert. Die Kerberos SSO Erweiterung behandelt Skripte anders als Enterprise Connect. Sie führt Skripte nicht direkt aus. Stattdessen postet sie eine verteilte Benachrichtigung, wenn ein Ereignis eintritt, auf das ein anderer Prozess achten und dann ein Skript ausführen kann. Einzelheiten hierzu finden Sie im Abschnitt „Erweiterte Funktionen" in diesem Dokument.

Nachfolgend finden Sie Verweise auf die Skript-Auslöser von Enterprise Connect und ihre entsprechenden verteilten Benachrichtigungen in der Kerberos SSO Erweiterung:

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

Netzwerkfreigaben

Die Kerberos SSO Erweiterung unterstützt nicht den Umgang mit Netzwerkfreigaben, wie z. B. den Netzwerk-Benutzerordner des Benutzers. Sie können einen Großteil dieser Funktionalität durch Skripte ersetzen.

Anhang

Geräteverwaltungsprofil: ExtensibleSingleSignOnKerberos

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

Referenzinformationen zum MDM-Protokoll

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

Geräteverwaltungsprofil: ExtensibleSingleSignOnKerberos.ExtensionData

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

Beispielskript – Verteilte Benachrichtigungen verarbeiten

Die Kerberos SSO Erweiterung postet eine Reihe von verteilten Benachrichtigungen, wenn verschiedene Ereignisse eintreten, z. B. wenn der Benutzer ein Passwort ändert oder das Unternehmensnetzwerk online geht. Als Administrator können Sie mit einem Skript oder einer App auf diese Benachrichtigungen achten und Aktionen – z. B. die Ausführung eines Skripts oder eines Shell-Befehls – durchführen, wenn sie gepostet werden.

Unten finden Sie ein Beispielskript, das Skripte oder Befehle ausführen kann, wenn Benachrichtigungen gepostet werden. Es sollte als LaunchAgent ausgeführt werden, um als angemeldeter Benutzer zu laufen, oder als LaunchDaemon, um als Root zu laufen. Das Skript benötigt zwei erforderliche Parameter:

- **-notification** ist der Name der verteilten Benachrichtigung, auf die Sie achten wollen. Siehe Seite 11 für Beispiele.
- **-action** ist die Aktion, die Sie ausführen möchten, wenn die verteilte Benachrichtigung gepostet wird. Ein Beispiel ist „sh /path/to/script.sh“.

Um das Skript auszuführen, müssen Sie die Befehlszeilen-Tools für Entwickler installieren. Ein Installationspaket für diese Tools finden Sie auf der Apple Developer Website.

```
#!/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()
```

Beispielskript – Enterprise Connect deinstallieren

Dieses Beispielskript löscht jede Enterprise Connect Version. Führen Sie es über eine Mac Verwaltungslösung oder manuell aus. Das Skript muss mit Root-Rechten ausgeführt werden.

```
#!/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
```