# Rozszerzenie do pojedynczego logowania Kerberos

## Podręcznik użytkownika

Grudzień 2019 r.

# Spis treści

# Wprowadzenie

Rozszerzenie do pojedynczego logowania Kerberos ułatwia korzystanie z mechanizmu pojedynczego logowania (single sign-on, SSO), bazującego na protokole Kerberos, na urządzeniach Apple używanych w organizacji.

## Uproszczone uwierzytelnianie Kerberos

Rozszerzenie do pojedynczego logowania Kerberos upraszcza proces uzyskiwania biletu uprawniającego do przyznania biletu (ticket-granting ticket, TGT) w protokole Kerberos z domeny Active Directory używanej przez organizację. W rezultacie użytkownicy mogą wygodnie i sprawnie uwierzytelniać się w takich zasobach, jak witryny internetowe, aplikacje i serwery plików. W systemie macOS rozszerzenie do pojedynczego logowania Kerberos proaktywnie uzyskuje bilet TGT po zmianach stanu sieci, aby w razie potrzeby użytkownik był gotowy do uwierzytelnienia.

## Zarządzanie kontami Active Directory

Rozszerzenie do pojedynczego logowania Kerberos pomaga także użytkownikom w zarządzaniu ich kontami Active Directory. W systemie macOS umożliwia użytkownikowi zmianę jego hasła w usłudze Active Directory i powiadamia o zbliżającym się terminie wygaśnięcia hasła. Użytkownik może również zmienić swoje hasło do konta lokalnego na identyczne z używanym w usłudze Active Directory.

## Współpraca z usługą Active Directory

Rozszerzenie do pojedynczego logowania Kerberos powinno być używane z lokalną domeną Active Directory. Usługa Azure Active Directory nie jest obsługiwana. Urządzenia nie muszą być przyłączone do domeny Active Directory, aby korzystać z rozszerzenia do pojedynczego logowania Kerberos. Ponadto użytkownicy nie muszą logować się na swoich komputerach Mac, używając kont Active Directory lub kont przenośnych; Apple zaleca, by zamiast nich używali kont lokalnych.

## Wymagania

- iOS 13, iPadOS lub macOS Catalina.
- Domena Active Directory z systemem Windows Server 2008 lub nowszym. Rozszerzenie do pojedynczego logowania Kerberos nie jest przeznaczone do użytku z usługą Azure Active Directory. Wymaga tradycyjnej lokalnej domeny Active Directory.
- Dostęp do sieci, w której utrzymywana jest domena Active Directory. Dostęp ten może odbywać się przez połączenie Wi-Fi, Ethernet lub VPN.
- Urządzenia muszą być zarządzane za pomocą rozwiązania do zarządzania urządzeniami mobilnymi (mobile device management, MDM) obsługującego pakiet danych Extensible Single Sign-on (SSO) w profilu konfiguracji. Należy dowiedzieć się u dostawcy rozwiązania MDM, czy obsługuje ono ten pakiet danych profilu konfiguracji.

## Enterprise Connect

Rozszerzenie do pojedynczego logowania Kerberos ma w zamierzeniu zastąpić aplikację Enterprise Connect. Jeśli organizacja używa obecnie aplikacji Enterprise Connect i zamierza przejść na rozszerzenie do pojedynczego logowania Kerberos, należy zapoznać się z dodatkowymi informacjami zamieszczonymi w sekcji „Przejście z aplikacji Enterprise Connect” w niniejszym dokumencie.

# Pierwsze kroki

## Tworzenie i wdrażanie profilu konfiguracji

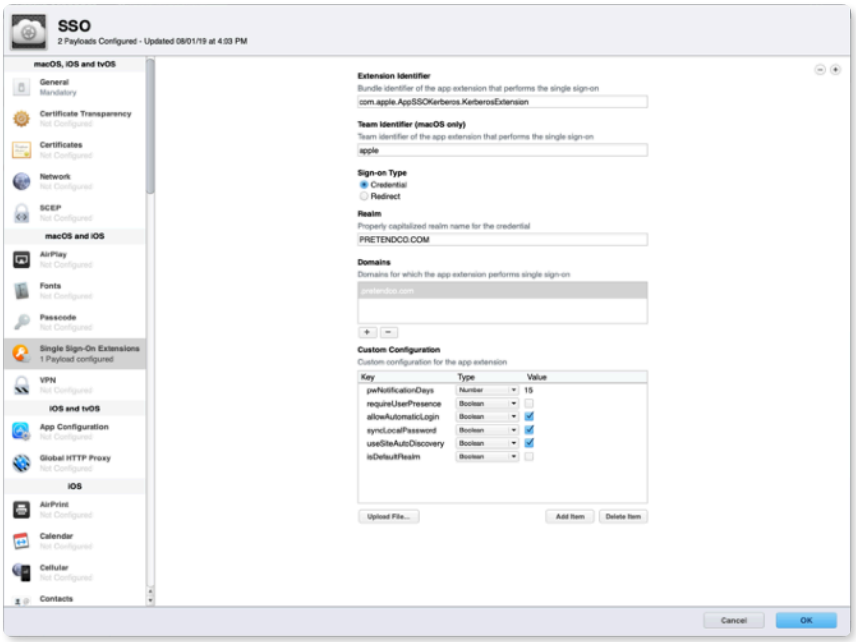
Aby używać rozszerzenia do pojedynczego logowania Kerberos, należy skonfigurować je przy użyciu profilu konfiguracji dostarczanego do urządzenia przez rozwiązanie MDM.

Uwaga: Profil konfiguracji musi być dostarczony do urządzenia przez rozwiązanie MDM. W systemie macOS wymagana jest rejestracja w systemie MDM zatwierdzona przez użytkownika, a profil musi być zainstalowany w zasięgu systemowym. Ręczne dodawanie profilu nie jest obsługiwane.

Do przeprowadzenia konfiguracji z użyciem profilu konfiguracji zastosowany zostanie pakiet danych Extensible Single Sign-on wprowadzony w systemach iOS 13, iPadOS i macOS 10.15. Aplikacja Profile Manager — wchodząca w skład oprogramowania macOS Server — obsługuje pakiet danych Extensible Single Sign-on. Jeśli stosowane rozwiązanie MDM nie obsługuje tego pakietu danych, to być może będzie się dało utworzyć odpowiedni profil w aplikacji Profile Manager, a następnie zaimportować go do rozwiązania MDM w celu dystrybucji. Aby uzyskać więcej informacji, należy skontaktować się z dostawcą rozwiązania MDM.

Aby utworzyć profil konfiguracji w aplikacji Profile Manager, wykonaj następujące czynności:

1. Zaloguj się do aplikacji Profile Manager.
2. Utwórz profil dla grupy urządzeń lub konkretnego urządzenia.
3. Wybierz pozycję Single Sign-On Extensions na liście Payload, a następie kliknij przycisk dodawania (+), aby dodać nowy pakiet danych.
4. W polu Extension Identifier wprowadź identyfikator „com.apple.AppSSOKerberos.KerberosExtension”.
5. W polu Team Identifier wprowadź „apple”.




6. W polu Sign-on Type wybierz opcję Credential.

7. W polu Realm wprowadź nazwę domeny Active Directory, w której znajdują się konta użytkowników, zapisaną w całości wielkimi literami. Nie używaj nazwy lasu Active Directory, chyba że konta użytkowników istnieją na poziomie lasu.
8. W polu Domains kliknij przycisk dodawania (+) i dodaj domeny wszelkich zasobów, które korzystają z protokołu Kerberos. Na przykład, jeśli protokół Kerberos używany jest do uwierzytelniania w zasobach z domeny us.pretendco.com, dodaj nazwę „.us.pretendco.com". (Koniecznie z kropką na początku).
9. W obszarze Custom Configuration dodaj następujące wartości:

| Key | Type | Value |
|---|---|---|
| pwNotificationDays | Number | 15 |
| requireUserPresence | Boolean | Niezaznaczony |
| allowAutomaticLogin | Boolean | Zaznaczony |
| syncLocalPassword | Boolean | Zaznaczony |
| useSiteAutoDiscovery | Boolean | Zaznaczony |
| isDefaultRealm | Boolean | Niezaznaczony |

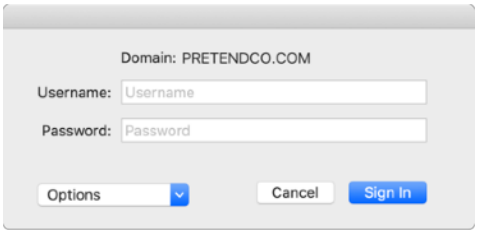
10. Kliknij przycisk OK, aby zapisać nowy profil konfiguracji. Profil zostanie automatycznie zainstalowany w wybranym urządzeniu lub w wybranej grupie urządzeń.

## Konfiguracja użytkownika — iOS i iPadOS

1. Podłącz urządzenie do sieci, w której dostępna jest domena Active Directory organizacji.
2. Wykonaj jedną z następujących czynności:
   - W Safari otwórz witrynę internetową obsługującą uwierzytelnianie Kerberos.
   - Uruchom aplikację obsługującą uwierzytelnianie Kerberos.
3. Wprowadź swoją nazwę użytkownika i hasło dla usługi Kerberos lub Active Directory.
4. Pojawi się pytanie o to, czy użytkownik ma być na stałe zalogowany automatycznie. Większość użytkowników stuka odpowiedź twierdzącą, Yes.
5. Stuknij przycisk Sign In. Po krótkiej zwłoce witryna internetowa lub aplikacja zostanie załadowana. Po wybraniu opcji automatycznego logowania w rozszerzeniu do pojedynczego logowania Kerberos pytanie o dane uwierzytelniania nie będzie się już pojawiać, dopóki nie zmienisz hasła. Jeśli opcja automatycznego logowania nie została wybrana, pytanie o dane uwierzytelniania będzie pojawiać się dopiero po wygaśnięciu danych uwierzytelniania w usłudze Kerberos — zwykle po 10 godzinach.

## Konfiguracja użytkownika — macOS

1. Wymagane jest uwierzytelnienie się w rozszerzeniu do pojedynczego logowania Kerberos. Można rozpocząć ten proces na kilka sposobów:
   - Jeśli Mac jest podłączony do sieci, w której dostępna jest domena Active Directory użytkownika, monit o uwierzytelnienie pojawi się od razu po zainstalowaniu profilu konfiguracji z pakietem danych Extensible SSO.
   - W przypadku otwarcia w przeglądarce Safari witryny internetowej akceptującej uwierzytelnianie Kerberos lub używania aplikacji, która wymaga takiego rodzaju uwierzytelniania, pojawi się monit o uwierzytelnienie.
   - Monit o uwierzytelnienie pojawi się od razu po każdym podłączeniu Maca do sieci, w której dostępna jest usługa Active Directory użytkownika.
   - Można wybrać menu dodatkowe rozszerzenia do pojedynczego logowania Kerberos, a następnie kliknąć opcję Sign In.
2. Pojawi się monit o dane uwierzytelniania w usłudze Kerberos. Wprowadź swoją nazwę użytkownika i hasło dla usługi Kerberos lub Active Directory.




3. Pojawi się pytanie o to, czy użytkownik ma być logowany automatycznie. Większość użytkowników powinna kliknąć odpowiedź twierdzącą, Yes.
4. Kliknij przycisk Sign In. Po krótkiej zwłoce witryna internetowa lub aplikacja zostanie załadowana. Po wybraniu opcji automatycznego logowania w rozszerzeniu do pojedynczego logowania Kerberos pytanie o dane uwierzytelniania nie będzie się już pojawiać, dopóki nie zmienisz hasła. Jeśli opcja automatycznego logowania nie została wybrana, pytanie o dane uwierzytelniania będzie pojawiać się dopiero po wygaśnięciu danych uwierzytelniania w usłudze Kerberos — zwykle po 10 godzinach.
5. Gdy termin wygaśnięcia hasła będzie już bliski, pojawi się powiadomienie z informacją o liczbie dni pozostałych do wygaśnięcia. Można kliknąć to powiadomienie i zmienić hasło.
6. Jeśli włączona została funkcja synchronizacji hasła, pojawi się pytanie o obecne hasło w usłudze Active Directory i hasło lokalne. Wprowadź oba hasła, a następnie kliknij przycisk OK, aby zsynchronizować hasła. Ten monit pojawi się przy pierwszym logowaniu, nawet jeśli hasła są już zsynchronizowane.

## Zmiany hasła — macOS

Za pomocą rozszerzenia do pojedynczego logowania Kerberos możesz również zmienić swoje hasło w usłudze Active Directory:

1. Upewnij się, że jesteś zalogowany(-a) do rozszerzenia do pojedynczego logowania Kerberos.
2. Wybierz menu dodatkowe pojedynczego logowania Kerberos, a następnie wybierz opcję Change Password. Może również pojawić się powiadomienie o bliskim terminie wygaśnięcia hasła.

3. Wprowadź swoje obecne hasło, a następnie nowe hasło. Nowe hasło powinno spełniać wymagania obowiązujące w organizacji w odniesieniu do haseł. Kliknij przycisk OK.
4. Po krótkiej zwłoce zostanie wyświetlone okno dialogowe z informacją o pomyślnej zmianie hasła. Jeśli włączona jest funkcja synchronizacji haseł, hasło do Twojego konta lokalnego zostanie zmienione na identyczne z nowym hasłem Active Directory.

## Korzystanie z menu dodatkowego pojedynczego logowania Kerberos — macOS

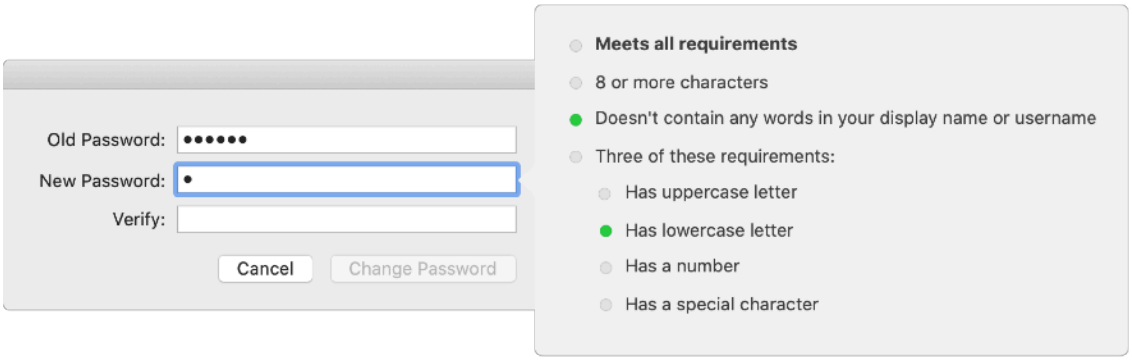
Menu dodatkowe pojedynczego logowania Kerberos zapewnia łatwy dostęp do użytecznych informacji o koncie użytkownika oraz do funkcji rozszerzenia. Menu dodatkowe będzie widoczne na pasku menu, w prawym górnym rogu, jako szary lub czarny klucz.

Aby uzyskać informacje o statusie konta, należy przede wszystkim zwrócić uwagę na kolor ikony menu dodatkowego pojedynczego logowania Kerberos. Szary kolor klucza oznacza, że użytkownik nie jest zalogowany do rozszerzenia. Czarny kolor klucza oznacza, że użytkownik jest zalogowany. Po wybraniu klucza pojawia się informacja o koncie, na którym użytkownik jest zalogowany, oraz o liczbie dni pozostałej do wygaśnięcia hasła. Menu umożliwia również zalogowanie się, wylogowanie i zmianę hasła.

# Funkcje zaawansowane

## Sprawdzanie haseł na bieżąco

W wielu konfiguracjach usługi Active Directory rozszerzenie do pojedynczego logowania Kerberos może sprawdzać nowe hasła użytkowników już na etapie ich wprowadzania i informować użytkowników, jakie wymagania musi spełniać nowe hasło. Gdy odpowiednia funkcja będzie skonfigurowana, użytkownik zobaczy następujący widok podczas wprowadzania nowego hasła:




Aby można było używać tej funkcji, w domenie Active Directory użytkownika muszą być stosowane wyłącznie standardowe zasady Active Directory dotyczące haseł. Domyślnie usługa Active Directory umożliwia administratorowi narzucenie wymogu złożoności i określonej długości hasła. Aby dowiedzieć się, jakie cechy musi mieć hasło złożone, zobacz technet.microsoft.com/en-us/library/cc786468(v=ws.10).aspx.

**Uwaga:** Korzystanie z tej funkcji może okazać się niemożliwe, jeśli w domenie użytkownika stosowane są narzędzia lub biblioteki DLL innych firm rozszerzające standardowe zasady usługi Active Directory dotyczące haseł. O korzystaniu z takich rozszerzeń zasad świadczy na przykład zakaz występowania w hasłach określonych wyrazów, a nie tylko nazwy użytkownika, lub wymóg określonego udziału znaków specjalnych w haśle. W razie wątpliwości należy zwrócić się do administratora usługi Active Directory o udzielenie dodatkowych informacji.

Jeśli domena Active Directory organizacji spełnia powyższe wymagania, można włączyć sprawdzanie haseł na bieżąco. W profilu konfiguracji rozszerzenia do pojedynczego logowania Kerberos ustaw następujące parametry:

| Parametr | Key | Type | Value | Opcjonalne |
|---|---|---|---|---|
| Wymaganie haseł złożonych | pwReqComplexity | Boolean | TAK | Nie |
| Wymagana długość hasła | pwReqLength | Integer | Liczba | Tak |
| Limit ponownego użycia tego samego hasła | pwReqHistory | Integer | Liczba | Tak |
| Minimalny wiek hasła | pwReqMinAge | Integer | Liczba | Tak |

Sprawdzanie haseł na bieżąco podlega pewnym ograniczeniom. Funkcja ta nie sprawdza, czy hasło było już używane. Nie jest także w stanie sprawdzić, czy hasło nie zawiera nazwy wyświetlanej Active Directory użytkownika, jeśli użytkownik nie ma jeszcze biletu TGT Kerberos. Taka sytuacja może wystąpić przy ustawianiu hasła po raz pierwszy lub po wygaśnięciu hasła. Wszystkie pozostałe wymagania są wówczas weryfikowane w zwykły sposób.

## Wyświetlanie wymagań dotyczących haseł

Jeśli nie jest możliwe skorzystanie z funkcji sprawdzania haseł na bieżąco, można skonfigurować rozszerzenie do pojedynczego logowania Kerberos w taki sposób, aby podczas wprowadzania nowych haseł przez użytkowników wyświetlane były ciągi tekstowe z wymaganiami obowiązującymi w organizacji. W profilu konfiguracji rozszerzenia do pojedynczego logowania Kerberos przypisz właściwości „pwReqText" ciąg znaków zawierający tekst informacji dla użytkowników, który powinien być wyświetlany podczas zmian haseł.

## Zmiana lub wyłączenie funkcji związanych z hasłami

W organizacjach, które nie zezwalają na zmiany haseł w katalogu Active Directory, używanie standardowej funkcji zmiany hasła w rozszerzeniu do pojedynczego logowania Kerberos nie jest możliwe. Aby wyłączyć tę funkcję, należy w profilu konfiguracji rozszerzenia do pojedynczego logowania Kerberos ustawić właściwość „allowPasswordChanges" na FALSE.

## Obsługa witryny służącej do zmiany hasła — macOS

Rozszerzenie do pojedynczego logowania Kerberos można skonfigurować w taki sposób, by po wybraniu przez użytkownika opcji „Change password" lub potwierdzeniu informacji o wygaśnięciu hasła w domyślnej przeglądarce otwierana była witryna służąca do zmiany hasła. Firma Apple zaleca używanie tej funkcji tylko w przypadku korzystania z kont lokalnych, ponieważ konta przenośne nie są obsługiwane.

W profilu konfiguracji rozszerzenia do pojedynczego logowania Kerberos należy przypisać właściwości „pwChangeURL" adres URL witryny służącej do zmiany hasła. Po zmianie hasła użytkownik musi wylogować się z rozszerzenia Kerberos, a następnie zalogować z powrotem, używając nowego hasła. Jeśli włączona jest synchronizacja haseł lokalnych, użytkownik jest prowadzony przez proces ponownej synchronizacji haseł.

## Synchronizacja haseł — macOS

Rozszerzenie do pojedynczego logowania Kerberos może ustawić hasło konta lokalnego na identyczne z hasłem do konta użytkownika w usłudze Active Directory. Funkcję tę włącza się, ustawiając na TRUE właściwość „syncLocalPassword" w sekcji konfiguracji niestandardowej profilu konfiguracji rozszerzenia do pojedynczego logowania Kerberos.

Mechanizm synchronizacji haseł spełnia zasadniczo dwie funkcje. Po pierwsze, gdy użytkownik zmienia hasło za pomocą rozszerzenia do pojedynczego logowania Kerberos, mechanizm synchronizacji ustawia hasło lokalne na identyczne z hasłem użytkownika w usłudze Active Directory. Jeśli hasło lokalne i hasło Active Directory przestaną być identyczne, rozszerzenie do pojedynczego logowania Kerberos przywraca ich synchronizację w następujący sposób:

- Bezpośrednio po włączeniu synchronizacji haseł i po każdej następnej próbie połączenia podjętej przez rozszerzenie do pojedynczego logowania Kerberos daty ostatnich zmian hasła lokalnego i hasła Active Directory są porównywane z wartościami w pamięci podręcznej. Zgodność wartości oznacza, że hasła są zsynchronizowane i nie trzeba podejmować żadnych działań. Jeśli wartości różnią się, rozszerzenie do pojedynczego logowania Kerberos wyświetli monit o podanie hasła lokalnego i hasła Active Directory. Gdy użytkownik poda hasło lokalne, rozszerzenie do pojedynczego logowania Kerberos ustawi je na identyczne z hasłem Active Directory.
- W przypadku zmiany hasła zasada działania jest podobna. Gdy użytkownik zmieni hasło w rozszerzeniu do pojedynczego logowania Kerberos, jego stare hasło Active Directory zostanie porównane z hasłem do

konta lokalnego. Jeśli stare hasło Active Directory jest identyczne z hasłem lokalnym, rozszerzenie do pojedynczego logowania Kerberos zmieni oba hasła. Jeśli hasła różnią się, zmienione zostanie tylko hasło w usłudze Active Directory. Użytkownik zostanie wówczas poproszony o podanie hasła lokalnego przy następnej próbie połączenia.

Obowiązują wówczas następujące wymagania:

- Gdy użytkownik jest zalogowany na komputerze Mac przy użyciu hasła Active Directory, a nie hasła lokalnego, synchronizacja haseł jest wyłączona. Funkcja synchronizacji haseł jest przeznaczona do stosowania tylko z hasłami lokalnymi; jeśli użytkownicy logują się na komputerach Mac przy użyciu kont Active Directory, funkcja ta jest niepotrzebna.
- Jeśli na kontach lokalnych egzekwowane są zasady dotyczące haseł — na przykład za pomocą profilu konfiguracji lub polecenia pwpolicy — to lokalne zasady muszą być identyczne z zasadami obowiązującymi w usłudze Active Directory lub mniej od nich rygorystyczne. Jeśli lokalne zasady dotyczące haseł będą bardziej rygorystyczne niż zasady w usłudze Active Directory, rozszerzenie do pojedynczego logowania Kerberos może zaakceptować hasło spełniające wymagania Active Directory, ale nie uda się zmienić hasła lokalnego, ponieważ nowe hasło nie będzie spełniało wymagań lokalnych. Jeśli lokalne zasady dotyczące haseł muszą być bardziej rygorystyczne od zasad obowiązujących w usłudze Active Directory, nie należy używać tej funkcji.
- Nazwa użytkownika lokalnego różni się od nazwy użytkownika w usłudze Active Directory — tylko hasła są zmieniane na identyczne.

## Obsługa kart inteligentnych — macOS

Rozszerzenie do pojedynczego logowania Kerberos umożliwia uwierzytelnianie na podstawie tożsamości przypisanych do kart inteligentnych. Karta inteligentna musi działać ze sterownikiem CryptoTokenKit; sterowniki oparte na modułach tokend nie są obsługiwane. macOS 10.15 obsługuje standard PIV, który jest szeroko stosowany przez instytucje rządowe USA.

Przed rozpoczęciem należy upewnić się, że konfiguracja domeny Active Directory uwzględnia uwierzytelnianie za pomocą kart inteligentnych. Proces włączania uwierzytelniania w usłudze Active Directory za pomocą kart inteligentnych nie mieści się w tematyce niniejszego dokumentu. Dodatkowe informacje można znaleźć w dokumentacji udostępnianej przez firmę Microsoft.

Aby zalogować się do rozszerzenia do pojedynczego logowania Kerberos za pomocą karty inteligentnej, wykonaj następujące czynności:

1. Kliknij menu Options, a następnie wybierz opcję „Use a smart card”.
2. Gdy pojawi się przycisk Identity, użyj karty inteligentnej i kliknij ten przycisk.
3. Wybierz tożsamość, której chcesz użyć do uwierzytelnienia, kliknij przycisk OK, a następnie przycisk Sign In.
4. W odpowiedzi na monit wprowadź swój kod PIN.

Gdy rozszerzenie do pojedynczego logowania Kerberos musi uzyskać bilet TGT usługi Kerberos, pojawi się prośba o użycie karty inteligentnej i wprowadzenie kodu PIN. Więcej informacji o obsłudze kart inteligentnych w systemie macOS można uzyskać, wpisując w Terminalu polecenie „man SmartCardServices”.

## Powiadomienia rozproszone — macOS

Rozszerzenie do pojedynczego logowania Kerberos publikuje powiadomienia rozproszone, gdy zachodzą różne zdarzenia. Aplikacje i usługi w systemie macOS za pośrednictwem powiadomień rozproszonych informują inne aplikacje i usługi o wystąpieniu zdarzenia. Aplikacja lub usługa nasłuchująca w oczekiwaniu na to zdarzenie może podjąć odpowiednie działanie, gdy ono wystąpi.

Administrator może wykorzystać tę funkcję do wykonywania działań w reakcji na określone zdarzenia. Na przykład za każdym razem, gdy rozszerzenie do pojedynczego logowania Kerberos uzyska nowe dane uwierzytelniania w usłudze Kerberos, może być uruchamiany odpowiedni skrypt.

Rozszerzenie do pojedynczego logowania Kerberos jedynie publikuje powiadomienia rozproszone, gdy zachodzą określone zdarzenia. Nie wykonuje żadnych działań w odpowiedzi na te zdarzenia. Administrator musi zapewnić narzędzie do nasłuchiwania tych powiadomień i inicjowania działań, gdy się pojawią.

W Dodatku zamieszczono przykładowy skrypt i listę właściwości dla Launchpada (.plist). Skrypt ten nasłuchuje powiadomień i inicjuje działania. Można zmodyfikować ten przykład, aby dostosować go do konkretnego wdrożenia.

Poniżej wymieniono powiadomienia rozproszone, które publikuje rozszerzenie do pojedynczego logowania Kerberos:

| Nazwa | Kiedy jest publikowane |
|---|---|
| com.apple.KerberosPlugin.ConnectionCompleted | Rozszerzenie do pojedynczego logowania Kerberos wykonało proces nawiązywania połączenia. |
| com.apple.KerberosPlugin.ADPasswordChanged | Użytkownik zmienił hasło w usłudze Active Directory za pomocą rozszerzenia. |
| com.apple.KerberosPlugin.LocalPasswordSynced | Użytkownik zsynchronizował hasło Active Directory z hasłem lokalnym. |
| com.apple.KerberosPlugin.InternalNetworkAvailable | Użytkownik nawiązał połączenie z siecią, w której dostępna jest skonfigurowana domena Active Directory. |
| com.apple.KerberosPlugin.InternalNetworkNotAvailable | Użytkownik nawiązał połączenie z siecią, w której nie jest dostępna skonfigurowana domena Active Directory. |
| com.apple.KerberosExtension.gotNewCredential | Użytkownik uzyskał nowy bilet TGT usługi Kerberos. |
| com.apple.KerberosExtension.passwordChangedWithPasswordSync | Użytkownik zmienił hasło Active Directory, a hasło lokalne zostało zmienione na identyczne z nowym hasłem Active Directory. |

## Obsługa z wiersza poleceń — macOS

Administratorzy mogą używać narzędzia *app-sso* w wierszu poleceń, aby sterować rozszerzeniem do pojedynczego logowania Kerberos i uzyskiwać dostęp do przydatnych informacji. Za pomocą tego narzędzia można na przykład zainicjować logowanie, zmianę hasła lub wylogowanie. Narzędzie może również zwrócić — w postaci listy właściwości lub w formacie JSON — przydatne informacje, takie jak nazwa obecnie zalogowanego użytkownika, bieżącą lokalizację usługi Active Directory, katalog domowy użytkownika w sieci, termin wygaśnięcia hasła użytkownika i szereg innych użytecznych informacji. Informacje te mogą być analizowane i przekazywane do rozwiązania zarządzającego komputerami Mac — w celach inwentaryzacyjnych i innych.

Aby uzyskać więcej informacji o korzystaniu z narzędzia app-sso, należy wprowadzić polecenie „app-sso -h" w aplikacji Terminal.

## Konta przenośne — macOS

Rozszerzenie do pojedynczego logowania Kerberos nie wymaga, aby Mac był powiązany z usługą Active Directory ani aby użytkownik był zalogowany na Macu przy użyciu konta przenośnego. Apple sugeruje używanie rozszerzenia do pojedynczego logowania Kerberos z kontem lokalnym. Konta lokalne sprawdzają się najlepiej w ramach rekomendowanego modelu wdrożenia systemu macOS i są najlepszym wyborem dla współczesnych użytkowników komputerów Mac, którzy nie są stale połączeni z siecią firmową. Rozszerzenie do pojedynczego logowania Kerberos zostało opracowane specjalnie z myślą o zapewnieniu lepszej integracji z usługą Active Directory użytkownikom kont lokalnych.

Można jednak używać rozszerzenia do pojedynczego logowania Kerberos, nadal korzystając z kont przenośnych. Obowiązują wówczas następujące wymagania:

- Synchronizacja haseł nie działa w przypadku kont przenośnych. Jeśli użytkownik użyje rozszerzenia do pojedynczego logowania Kerberos w celu zmiany swojego hasła w usłudze Active Directory, będąc zalgowanym na Macu przy użyciu tego samego konta, co konto użyte do logowania w rozszerzeniu, zmiany haseł odbywają się tak, jak gdyby były dokonywane na panelu preferencji Użytkownicy i grupy. Jeśli jednak dokona zewnętrznej zmiany hasła — to znaczy zmieni hasło w przeznaczonej do tego witrynie lub poprosi dział IT o zresetowanie hasła — rozszerzenie do pojedynczego logowania Kerberos nie będzie w stanie przywrócić synchronizacji hasła do konta przenośnego z hasłem Active Directory.
- Użycie adresu URL do zmiany hasła razem z rozszerzeniem do pojedynczego logowania Kerberos i kontem przenośnym nie jest możliwe.

## Odwzorowanie domena-dziedzina

W niektórych sytuacjach administrator musi zdefiniować niestandardowe odwzorowanie domena-dziedzina dla usługi Kerberos. Na przykład w organizacji używającej dziedziny Kerberos o nazwie „ad.pretendco.com" może występować konieczność uwierzytelniania Kerberos w zasobach znajdujących się w domenie „fakecompany.com".

**Uwaga:** Implementacja protokołu Kerberos stosowana w systemach operacyjnych Apple niemal we wszystkich sytuacjach jest w stanie automatycznie określić odwzorowanie domena-dziedzina. Administratorzy bardzo rzadko modyfikują te ustawienia.

Odwzorowanie domena-dziedzina dla rozszerzenia do pojedynczego logowania Kerberos można skonfigurować, wykonując następujące czynności:

1. W sekcji konfiguracji niestandardowej profilu Extensible SSO dodaj obiekt o nazwie domainRealmMapping. Powinien to być obiekt typu Dictionary, czyli słownik.
2. Jako klucz tego słownika podaj nazwę dziedziny zapisaną w całości wielkimi literami.
3. Jako typ wartości tego słownika ustaw Array. Pierwszą wartością powinna być nazwa dziedziny Kerberos zapisana małymi literami i poprzedzona kropką. Drugą wartością powinna być nazwa domeny, która wymaga uwierzytelnienia w tej dziedzinie, również poprzedzona kropką. Dodaj tyle tablic, ile potrzeba.

Więcej informacji można znaleźć w dokumentacji protokołu Kerberos.

# Przejście z aplikacji Enterprise Connect

## Omówienie

Rozszerzenie do pojedynczego logowania Kerberos ma w zamierzeniu zastąpić aplikację Enterprise Connect — podobne narzędzie używane już w wielu organizacjach. W większości organizacji przejście z aplikacji Enterprise Connect na rozszerzenie do pojedynczego logowania Kerberos odbywać się będzie według następującej procedury:

1. Utworzenie dla rozszerzenia profilu konfiguracji, który będzie zapewniał podobne funkcje, jak dotychczasowy profil Enterprise Connect używany w organizacji.
2. Odinstalowanie aplikacji Enterprise Connect.
3. Wdrożenie nowego profilu konfiguracji dla rozszerzenia do pojedynczego logowania Kerberos.
4. Zalogowanie się użytkowników do rozszerzenia do pojedynczego logowania Kerberos.

Przejście na rozszerzenie do pojedynczego logowania Kerberos nie jest wymagane do uaktualnienia systemów na komputerach Mac w organizacji do wersji macOS 10.15. W systemie macOS 10.15 aplikacja Enterprise Connect działa zgodnie z oczekiwaniami, jednak organizacje powinny zaplanować docelowo rezygnację z Enterprise Connect.

## Kto nie powinien dokonywać tego przejścia

Rozszerzenie do pojedynczego logowania Kerberos zaspokoi potrzeby zdecydowanej większości organizacji, które używają obecnie aplikacji Enterprise Connect. Jednak w organizacji, która spełnia poniższe kryteria, przejście z aplikacji Enterprise Connect może okazać się niemożliwe do zrealizowania lub będzie je można zrealizować tylko częściowo:

- Organizacja, która obecnie używa Maców z systemem macOS 10.14 lub wcześniejszymi powinna pozostawić działającą aplikację Enterprise Connect na tych systemach, a przejście na rozszerzenie do pojedynczego logowania Kerberos zrealizować wyłącznie na Macach z systemem macOS 10.15. Rozszerzenie do pojedynczego logowania Kerberos i powiązany z nim profil konfiguracji będzie działać tylko na komputerach Mac z systemem macOS 10.15. Aby korzystać z rozszerzenia, należy uaktualnić starsze systemy do wersji macOS 10.15.
- Organizacja korzystająca z narzędzia do zarządzania komputerami Mac, które nie obsługuje rejestracji w rozwiązaniu MDM zatwierdzanej przez użytkownika.

- Organizacja, która nie używa żadnego narzędzia do zarządzania.
- Organizacja, która korzysta z poziomu funkcjonalności Active Directory odpowiadającemu wersji Windows Server 2003 lub wcześniejszej.

## Tworzenie profilu konfiguracji dla rozszerzenia do pojedynczego logowania Kerberos

Dla rozszerzenia do pojedynczego logowania Kerberos należało będzie utworzyć profil konfiguracji podobny do profilu konfiguracji aplikacji Enterprise Connect. Wiele spośród kluczy Preference Keys obecnych w profilu konfiguracji Enterprise Connect ma odpowiedniki w profilu rozszerzenia do pojedynczego logowania Kerberos. Tworzenie profilu należy rozpocząć od zapoznania się z poniższą tabelą, która zawiera odwzorowanie między odpowiednikami w profilu rozszerzenia a kluczami Preference Keys w profilu aplikacji Enterprise Connect:

| Enterprise Connect | Rozszerzenie do pojedynczego logowania Kerberos | Uwagi |
|---|---|---|
| adRealm | Realm | Dziedzina powinna być w całości zapisana wielkimi literami. |
| Automatic login (enabled by default) | allowAutomaticLogin | Należy dodać do sekcji konfiguracji niestandardowej. Aby automatyczne logowanie działało, musi mieć wartość True. |
| disablePasswordFunctions | allowPasswordChange | Należy dodać do sekcji konfiguracji niestandardowej. Ustawienie False uniemożliwia zmiany haseł. |
| passwordChangeURL | pwChangeURL | Należy dodać do sekcji konfiguracji niestandardowej. |
| passwordExpireOverride | pwExpireOverride | Należy dodać do sekcji konfiguracji niestandardowej. |
| passwordNotificationDays | pwNotificationDays | Należy dodać do sekcji konfiguracji niestandardowej. |
| prepopulatedUsername | principalName | Należy dodać do sekcji konfiguracji niestandardowej. |
| pwReqComplexity | pwReqComplexity | Należy dodać do sekcji konfiguracji niestandardowej. |
| pwReqHistory | pwReqHistory | Należy dodać do sekcji konfiguracji niestandardowej. |
| pwReqLength | pwReqLength | Należy dodać do sekcji konfiguracji niestandardowej. |
| pwReqMinimumPasswordAge | pwReqMinAge | Należy dodać do sekcji konfiguracji niestandardowej. |
| pwReqText | pwReqText | Należy dodać do sekcji konfiguracji niestandardowej. Zamiast ścieżki do pliku RTF należy podać ciąg znaków do wyświetlenia. |
| syncLocalPassword | syncLocalPassword | Należy dodać do sekcji konfiguracji niestandardowej. |

**Uwaga:** Niektóre klucze Preference Keys obecne w profilu konfiguracji Enterprise Connect mogą nie być tutaj wymienione. Mogą one dotyczyć funkcji, które nie są już potrzebne w rozszerzeniu do pojedynczego logowania Kerberos lub nie są już obsługiwane.

## Odinstalowanie aplikacji Enterprise Connect.

Jednoczesne działanie rozszerzenia do pojedynczego logowania Kerberos i aplikacji Enterprise Connect nie jest obsługiwane. Po przejściu na rozszerzenie do pojedynczego logowania Kerberos należy odinstalować aplikację Enterprise Connect. Do przeprowadzenia deinstalacji wymagane będą uprawnienia administratora. Aby odinstalować aplikację Enterprise Connect, należy wykonać poniższe czynności:

**Enterprise Connect 2.0 i nowsze wersje**

1. Usuń z pamięci agenta Enterprise Connect. W tym celu uruchom aplikację Terminal i wprowadź polecenie „launchctl unload /Library/LaunchAgents/com.apple.ecAgent", działając na koncie obecnie zalogowanego użytkownika.
2. Zakończ działanie menu dodatkowego aplikacji Enterprise Connect. W tym celu uruchom aplikację Terminal i wprowadź w niej polecenie „killall Enterprise\ Connect\ Menu".
3. Usuń aplikację Enterprise Connect z folderu Aplikacje.
4. Usuń plik .plist Launchpada dla aplikacji Enterprise Connect: /Library/LaunchAgents/com.apple.ecAgent.plist.

**Enterprise Connect 1.9.5 i starsze wersje**

1. Zakończ działanie aplikacji Enterprise Connect, wprowadzając polecenie „killall Enterprise\ Connect" w aplikacji Terminal.
2. Usuń aplikację Enterprise Connect z folderu Aplikacje.

W Dodatku zamieszczono przykładowy skrypt, który usuwa dowolną wersję aplikacji Enterprise Connect.

## Wyzwalacze skryptów w aplikacji Enterprise Connect

Aplikacja Enterprise Connect może uruchamiać skrypty w reakcji na określone zdarzenia. Enterprise Connect może na przykład uruchomić skrypt po zakończeniu nawiązywania połączenia lub po zmianie hasła przez użytkownika. Rozszerzenie do pojedynczego logowania Kerberos obsługuje skrypty inaczej niż aplikacja Enterprise Connect. Nie uruchamia skryptów bezpośrednio, lecz w reakcji na zdarzenie publikuje powiadomienie rozproszone, którego inny proces może nasłuchiwać, by uruchomić skrypt, gdy się ono pojawi. Szczegółowe informacje zawiera sekcja „Funkcje zaawansowane" w niniejszym dokumencie.

Poniżej znajduje się wykaz wyzwalaczy skryptów stosowanych w aplikacji Enterprise Connect oraz odpowiadających im powiadomień rozproszonych w rozszerzeniu do pojedynczego logowania Kerberos:

| Enterprise Connect | Rozszerzenie do pojedynczego logowania Kerberos |
|---|---|
| auditScriptPath | com.apple.KerberosPlugin.InternalNetworkAvailable |
| connectionCompletedScriptPath | com.apple.KerberosPlugin.ConnectionCompleted |
| passwordChangeScriptPath | com.apple.KerberosPlugin.ADPasswordChanged |

## Udziały sieciowe

Rozszerzenie do pojedynczego logowania Kerberos nie wykonuje żadnych operacji na udziałach sieciowych, takich jak katalog domowy użytkownika w sieci. Wiele spośród tych operacji można zastąpić skryptami.

# Dodatek

**Profil zarządzania urządzeniami: ExtensibleSingleSignOnKerberos**

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

**Dokumentacja protokołu zarządzania urządzeniami mobilnymi**

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

**Profil zarządzania urządzeniami: ExtensibleSingleSignOnKerberos.ExtensionData**

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

## Przykładowy skrypt — obsługa powiadomień rozproszonych

Rozszerzenie do pojedynczego logowania Kerberos publikuje różne powiadomienia rozproszone w odpowiedzi na różne zdarzenia, np. zmianę hasła przez użytkownika lub nawiązanie połączenia z siecią firmową. Administrator może użyć skryptu lub aplikacji do nasłuchiwania w oczekiwaniu na te powiadomienia, a w odpowiedzi na nie inicjować działania, np. uruchomić skrypt lub polecenie powłoki.

Poniżej zamieszczono przykładowy skrypt, który może uruchamiać inne skrypty lub polecenia w odpowiedzi na powiadomienia. Skrypt ten powinien być uruchamiany jako LaunchAgent, by działał na koncie zalogowanego użytkownika, albo jako LaunchDaemon, aby działał na koncie użytkownika root. Skrypt ma dwa wymagane parametry:

- **-notification** to nazwa powiadomienia rozproszonego, którego skrypt ma nasłuchiwać. Przykłady zamieszczono na stronie 11.
- **-action** to działanie, które ma zostać wykonane po opublikowaniu powiadomienia rozproszonego. Na przykład „sh /path/to/script.sh”.

Aby móc uruchomić skrypt, należy zainstalować narzędzia wiersza poleceń dla deweloperów. Pakiet instalacyjny tych narzędzi jest dostępny w witrynie Apple Developer.

```
#!/usr/bin/swift

import Foundation

class NotifyHandler {

    // Action we want to run, like a shell command or a script
    public var action = String()

    // Runs every time we receive the specified distributed
    // notification
    @objc func gotNotification(notification: NSNotification){
        let task = Process()
        task.launchPath = "/bin/zsh"
        task.arguments = ["-c", action]
        task.launch()
    }
}

// MAIN

let scriptPath: String = CommandLine.arguments.first!

// -notification is the name of the notification you are listening for
guard let notification = UserDefaults.standard.string(forKey: "notification") else {
    print("\(scriptPath): No notification passed, exiting…")
    exit(1)
}
```

```
// -action is the action you want to run. Może to być

// 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()
```

## Przykładowy skrypt — deinstalowanie Enterprise Connect

Ten przykładowy skrypt usuwa dowolną wersję aplikacji Enterprise Connect. Można uruchamiać go z rozwiązania do zarządzania komputerami Mac albo ręcznie. Skrypt musi działać z uprawnieniami użytkownika root.

```
#!/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
```