Kerberosシングルサインオン Extension

ユーザガイド

2019年12月

目次

概要

KerberosシングルサインオンExtensionを使うと、組織のAppleデバイスでKerberosベースのシングルサインオンを簡単に利用できます。

シンプルに使えるKerberos認証

Kerberos SSO Extensionを使うと、組織のActive DirectoryドメインからKerberos TGT（Ticket Granting Ticket）を取得するプロセスがシンプルになり、ウェブサイトやアプリケーション、ファイルサーバなどのリソースに対するユーザー認証がシームレスに実行されるようになります。macOSでは、ネットワークの状態が変更された時にKerberos SSO Extensionが自動的にKerberos TGTを取得するので、必要に応じてユーザー認証がすぐに行われます。

Active Directoryアカウントの管理

Kerberos SSO Extensionは、ユーザーによるActive Directoryアカウントの管理にも役立ちます。macOSでは、ユーザーはActive Directoryのパスワードを変更することができ、パスワードの有効期限が近付いた時に通知を受けることもできます。ローカルアカウントのパスワードを、Active Directoryのパスワードと同じパスワードに変更することもできます。

Active Directoryのサポート

Kerberos SSO Extensionは、オンプレミスのActive Directoryドメインで使用してください。Azure Active Directoryはサポートされていません。Kerberos SSO Extensionを使用する場合でも、デバイスをActive Directoryドメインに参加させる必要はありません。また、ユーザーはActive Directoryやモバイルアカウントを使ってMacコンピュータにログインする必要もありません。Appleはローカルアカウントの使用を推奨しています。

要件

- iOS 13、iPadOS、またはmacOS Catalina。
- Windows Server 2008以降が稼働するActive Directoryドメイン。Kerberos SSO Extensionは、Azure Active Directoryとの使用を想定したものではありません。従来のオンプレミスのActive Directoryドメインが必要です。
- Active Directoryドメインがホストされているネットワークへのアクセス。Wi-Fi、Ethernet、またはVPNによるネットワークアクセスを利用できます。
- デバイスは、拡張可能なシングルサインオン（SSO）の構成プロファイルペイロードをサポートするモバイルデバイス管理（MDM）ソリューションで管理されている必要があります。この構成プロファイルペイロードのサポート状況については、MDMベンダーにお問い合わせください。

Enterprise Connect

Kerberos SSO Extensionは、Enterprise Connectに置き換わる機能です。現在Enterprise Connectを利用中で、Kerberos SSO Extensionへの移行を検討している場合は、詳細について本書の「Enterprise Connectからの移行」セクションを参照してください。

はじめに

構成プロファイルの作成と配布

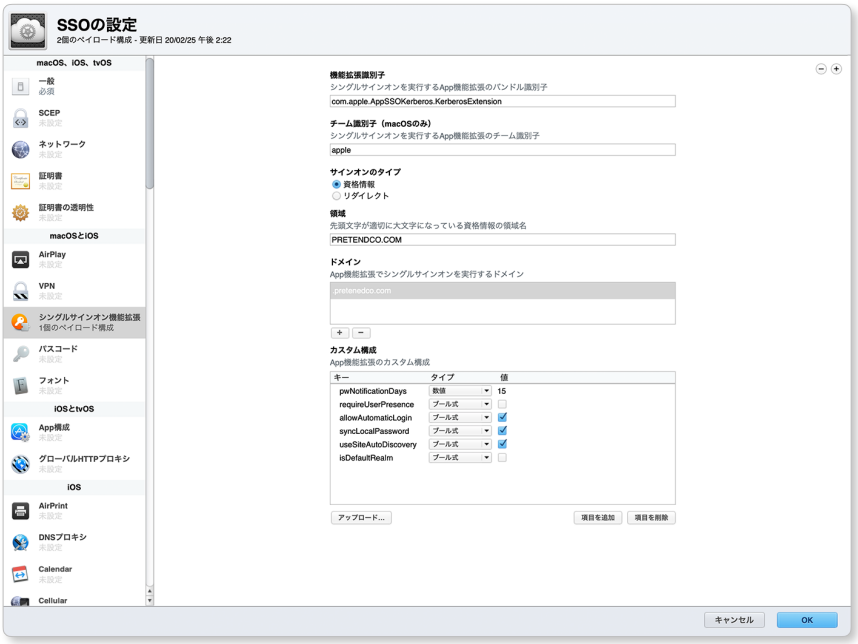
Kerberos SSO Extensionを使用するには、構成プロファイルを使って構成し、MDMソリューションからデバイスに配布する必要があります。

注意：構成プロファイルはMDMを使ってデバイスに配布する必要があります。macOSの場合は、ユーザー承認型MDM登録を使い、「System」スコープにインストールする必要があります。手動でのプロファイル追加には対応していません。

構成プロファイルを使って構成するには、iOS 13、iPadOS、およびmacOS 10.15から追加された拡張可能なシングルサインオンのペイロードを使用します。macOS Serverに搭載されているプロファイルマネージャは、拡張可能なシングルサインオンのペイロードに対応しています。MDMソリューションがまだこのペイロードに対応していない場合は、必要なプロファイルをプロファイルマネージャで作成し、それをMDMソリューションに読み込んで配布できる場合があります。詳細については、MDMベンダーにお問い合わせください。

プロファイルマネージャを使って構成プロファイルを作成するには、以下の手順に従ってください。

1. プロファイルマネージャにサインインします。
2. デバイスグループまたは特定のデバイスのプロファイルを作成します。
3. ペイロードリストで「シングルサインオン機能拡張」を選択してから、「構成」ボタンをクリックして新しいペイロードを追加します。
4. 「機能拡張識別子」フィールドに「com.apple.AppSSOKerberos.KerberosExtension」と入力します。
5. 「チーム識別子」フィールドに「apple」と入力します。



6. 「サインオンのタイプ」で「資格情報」を選択します。
7. 「領域」フィールドに、ユーザーアカウントがあるActive Directoryドメインの名前を入力します。すべて大文字で入力してください。ユーザーアカウントがフォレストレベルに存在している場合を除き、Active Directoryフォレストの名前を入力しないでください。

8. 「ドメイン」で追加ボタン(+)をクリックし、Kerberosを使用するすべてのリソースのドメインを追加します。
例えば、us.pretendco.comのリソースでKerberos認証を使用する場合は、「.us.pretendco.com」を追加します(先頭のピリオドを必ず入力してください)。

9. 「カスタム構成」には、以下のように値を追加します。

キー	型	値(例)
pwNotificationDays	数値	15
requireUserPresence	ブール式	チェック解除
allowAutomaticLogin	ブール式	チェック
syncLocalPassword	ブール式	チェック
useSiteAutoDiscovery	ブール式	チェック
isDefaultRealm	ブール式	チェック解除

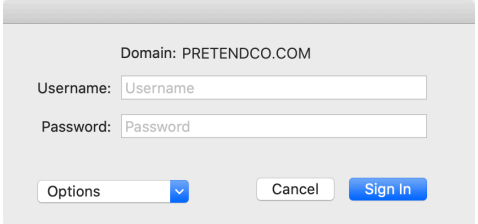
10. 「OK」をクリックして新しい構成プロファイルを保存します。選択したデバイスまたはデバイスグループに、構成プロファイルが自動的にインストールされます。

ユーザー設定 — iOSおよびiPadOS

1. 組織のActive Directoryドメインを利用できるネットワークにデバイスを接続します。
2. 以下のいずれかを実行します。
   - Safariを使って、Kerberos認証に対応しているウェブサイトにアクセスする。
   - Kerberos認証に対応しているアプリケーションを起動する。
3. Kerberos(Active Directory)のユーザ名とパスワードを入力して「サインイン」をタップします。
4. 今後も自動的にサインインするかどうか確認するメッセージが表示されます。ほとんどの場合は「はい」をタップしてください。
5. ウェブサイトまたはアプリケーションが読み込まれます。Kerberos SSO Extensionに自動的にサインインすると選択した場合は、パスワードを変更するまで資格情報を再度求められることはありません。自動的にサインインすると選択しなかった場合は、Kerberosの資格情報の有効期限(通常は10時間)が切れた後に資格情報を求められます。

ユーザー設定 — macOS

1. Kerberos SSO Extensionには認証が必要です。この認証プロセスはいくつかの方法で開始できます。
   - Active Directoryドメインを利用できるネットワークに接続されているMacでは、拡張可能なSSO構成プロファイルがインストールされるとすぐに認証を求められます。
   - Safariを使ってKerberos認証に対応しているウェブサイトにアクセスしたり、Kerberos認証が必要なアプリケーションを使うと、認証を求められます。
   - Active Directoryを利用できるネットワークにMacを接続すると、すぐに認証を求められます。
   - Kerberos SSO ExtensionのMenu Extraを選択し、「サインイン」をクリックして認証に進むことができます。
2. Kerberosの資格情報が求められます。Kerberos（Active Directory）のユーザ名とパスワードを入力して「サインイン」をクリックします。



3. 自動的にサインインするかどうか確認するメッセージが表示されます。ほとんどの場合は「はい」をクリックしてください。
4. ウェブサイトまたはアプリケーションが読み込まれます。Kerberos SSO Extensionに自動的にサインインすると選択した場合は、パスワードを変更するまで資格情報を再度求められることはありません。自動的にサインインすると選択しなかった場合は、Kerberosの資格情報の有効期限（通常は10時間）が切れた後に資格情報を求められます。
5. パスワードの有効期限が近付くと、有効期限までの日数を知らせる通知が届きます。通知をクリックすると、パスワードを変更できます。
6. パスワードの同期機能を有効にした場合は、現在のActive Directoryのパスワードとローカルパスワードが求められます。両方とも入力してから「パスワードを同期」をクリックして、パスワードを同期します。このプロンプトは、パスワードがすでに同期されている場合でも、最初のサインイン時に表示されます。

パスワードの変更 — macOS

Kerberos SSO Extensionでは、Active Directoryのパスワードも変更できます。

1. Kerberos SSO Extensionにサインインしていることを確認します。
2. Kerberos SSO Menu Extraを選択し、「パスワードを変更」を選択します。パスワードの有効期限を知らせる通知が届く場合もあります。
3. 現在のパスワードを入力してから、新しいパスワードを入力します。新しいパスワードが組織のパスワード要件を満たすようにします。「パスワードを変更」をクリックします。
4. パスワードが正しく変更されたことを伝えるダイアログが表示されます。パスワードの同期機能が有効になっている場合は、ローカルアカウントのパスワードが、新しいActive Directoryのパスワードと同じパスワードにアップデートされます。

Kerberos SSO Menu Extra — macOS

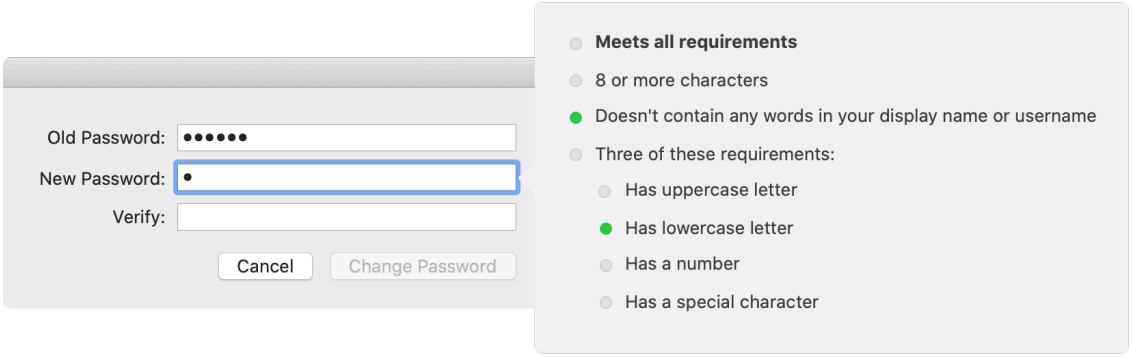
Kerberos SSO Menu Extraでは、アカウントやExtensionの機能に関する便利な情報に簡単にアクセスできます。
Menu Extraは、右上のメニューバーにグレイまたは黒の鍵アイコンとして表示されています。

アカウントの状態に関する情報を確認する場合は、まずKerberos SSO Menu Extraアイコンの色を確認します。
グレイの場合は、Extensionにサインインしていません。黒の場合は、サインインしています。鍵のアイコンを選択すると、サインインしているアカウントと、パスワードの有効期限までの日数が表示されます。このメニューでは、サインインまたはサインアウトしたり、パスワードを変更したりすることもできます。

高度な機能

パスワードのリアルタイム検証

多くのActive Directory構成では、Kerberos SSO Extensionが入力中の新しいパスワードを検証し、パスワード変更に必要なパスワード要件をユーザーに表示することができます。これを設定すると、新しいパスワードの入力中に以下のように表示されます。



この機能を使うには、Active Directoryドメインで標準的なActive Directoryのパスワードポリシーのみを使用している必要があります。Active Directoryでは、デフォルトで管理者が特定の長さを持つ複雑なパスワードを要求することができます。複雑なパスワードの構成要素について詳しくは、technet.microsoft.com/en-us/library/cc786468(v=ws.10).aspx（英語）を参照してください。

注意：お使いのドメインで他社製ツールやDLLを使って、標準的なActive Directoryのパスワードポリシーを拡張している場合、この機能をご利用いただけない場合があります。例えば、パスワードでユーザー名以外にも特定の単語の使用が許可されていない場合や、指定した文字数の特殊文字を使用する必要がある場合、パスワードポリシーを拡張する他社製品が使用されている可能性があります。他社製品の使用状況がわからない場合は、詳細についてActive Directoryの管理者に問い合わせてください。

組織のActive Directoryドメインが要件を満たす場合は、パスワードのリアルタイム検証を有効にすることができます。Kerberos SSO Extensionの構成プロファイルで、以下のパラメータを設定します。

パラメータ	キー	型	値	必須／任意
複雑なパスワードを要求	pwReqComplexity	ブール式	YES	必須
必要なパスワードの長さ	pwReqLength	整数	数値	任意
以前のパスワードの再利用制限	pwReqHistory	整数	数値	任意
最低限必要なパスワードの有効期限	pwReqMinAge	整数	数値	任意

パスワードのリアルタイム検証にはいくつかの制限があります。過去に使用されたパスワードかどうかを検証することはできません。また、Kerberos TGTをまだ取得していない場合は、パスワードにActive Directoryの表示名が含まれているかどうかも検証できません。はじめてパスワードを設定する場合やパスワードの有効期限が切れた場合に、このような状況になる可能性があります。これ以外の検証はすべて正常に機能します。

パスワード要件の表示

パスワードのリアルタイム検証を使用できない場合は、ユーザーによる新しいパスワードの入力中に組織のパスワード要件と何らかのテキストを表示するようにKerberos SSO Extensionを構成することができます。Kerberos SSO Extensionの構成プロファイルで、パスワードの変更中にユーザーに表示するテキストを含む文字列を「pwReqText」に設定します。

パスワード機能を有効にする／無効にする

Active Directoryに対するパスワードの変更を許可しない組織もあるため、Kerberos SSO Extensionの標準のパスワード変更機能を使用できない場合もあります。Kerberos SSO Extensionの構成プロファイルで「allowPasswordChange」を「FALSE」に設定すると、この機能が無効になります。

パスワード変更用ウェブサイトのサポート — macOS

ユーザーが「パスワードを変更」を選択するか、パスワードの有効期限の通知を確認したら、デフォルトのブラウザでパスワード変更用ウェブサイトが開くように、Kerberos SSO Extensionを構成することができます。モバイルアカウントはサポートされていないので、この機能はローカルアカウントの使用時のみにお使いになることをおすすめします。

Kerberos SSO Extensionの構成プロファイルで、「pwChangeURL」をパスワード変更用ウェブサイトのURLに設定します。パスワードを変更したユーザーは、Kerberos Extensionからサインアウトし、新しいパスワードでもう一度サインインする必要があります。ローカルパスワードの同期が有効になっている場合は、パスワードを同期し直すための指示が表示されます。

パスワードの同期 — macOS

Kerberos SSO Extensionでは、ローカルアカウントのパスワードを、そのユーザーのActive Directoryのパスワードと同じパスワードにするよう設定できます。この機能を有効にするには、Kerberos SSO Extensionの構成プロファイルの「カスタム構成」セクションで、「syncLocalPassword」を「TRUE」に設定します。

パスワード同期には2つの基本機能があります。まず、ユーザーがKerberos SSO Extensionを使ってパスワードを変更すると、この機能によってローカルパスワードがActive Directoryのパスワードと同じパスワードに設定されます。ローカルパスワードとActive Directoryのパスワードの同期が切れると、Kerberos SSO Extensionは以下のように同期し直します。

- パスワード同期が有効になった時、およびそれ以降にKerberos SSO Extensionによって接続が試行された時に、ユーザーによるローカルパスワードとActive Directoryパスワードの最終変更日がキャッシュ値と比較されます。値が一致すればパスワードは同期されているので、何も実行されません。一致しない場合、Kerberos SSO Extensionはローカルパスワードと Active Directoryパスワードをユーザーに求めます。ユーザーがローカルパスワードを入力したら、Kerberos SSO Extensionはローカルパスワードを、そのユーザーのActive Directoryのパスワードと同じパスワードに設定します。
- パスワードの変更も同様の仕組みで行われます。ユーザーがKerberos SSO Extensionでパスワード変更を実行すると、古いActive Directoryのパスワードがローカルアカウントのパスワードと比較されます。古いActive Directoryのパスワードとローカルパスワードが一致すると、Kerberos SSO Extensionは両方のパスワードを変更します。一致しない場合は、Active Directoryのパスワードのみが変更されます。ユーザーが次回接続する時に、ローカルパスワードが求められます。

この機能には、以下の要件があります。

- ユーザーがローカルアカウントではなく、Active DirectoryのアカウントでMacコンピュータにログインしている場合、パスワード同期は無効になります。パスワードの同期はローカルアカウントで使用する機能です。ユーザーがActive DirectoryのアカウントでMacコンピュータにログインしている場合、この機能を使う必要はありません。
- ローカルアカウントにパスワードポリシーが適用されている場合は（構成プロファイルやpwpolicyコマンドを使用している場合など）、ローカルのパスワードポリシーがActive Directoryのパスワードポリシーと同じか、それよりも厳格ではないことを確認してください。ローカルのパスワードポリシーがActive Directoryのポリシーよりも厳格な場合、Kerberos SSO Extensionが Active Directoryの要件を満たすパスワードを採用しても、ローカルパスワードの要件を満たさないため、ローカルパスワードを設定できないことがあります。ローカルのパスワードポリシーをActive Directoryのパスワードポリシーよりも厳格にする必要がある場合は、この機能を使わないでください。
- ローカルのユーザー名はActive Directoryのユーザー名と異なります。同じ値に設定されるのはパスワードのみです。

スマートカードのサポート — macOS

Kerberos SSO Extensionは、スマートカードを使ったID認証をサポートしています。スマートカードではCryptoTokenKit ドライバを利用できる必要があります。TokenDベースのドライバはサポートされていません。macOS 10.15にはPIV Standard のサポートが含まれています。これは米国政府によって広く利用されています。

始める前に、Active Directoryドメインがスマートカード認証をサポートするよう構成されていることを確認します。 Active Directoryでスマートカード認証を有効にする手順は本書では取り上げません。詳細については、Microsoftのドキュメントを参照してください。

スマートカードを使ってKerberos SSO Extensionにサインインするには、以下の手順に従います。

1. 「オプション」メニューをクリックし、「スマートカードまたはIDを使用する」を選択します。
2. 「ID」ボタンが表示されたら、スマートカードを挿入してボタンをクリックします。
3. 認証に使うIDを選択し、「選択」をクリックしてから「サインイン」をクリックします。
4. プロンプトが表示されたら、PINを入力します。

Kerberos SSO ExtensionでKerberos TGTを取得する必要がある場合は、スマートカードを挿入してPINを入力するよう求められます。macOSでのスマートカードサポートの詳細については、ターミナルで「man SmartCardServices」を実行して確認ください。

Distributed Notifications — macOS

Kerberos SSO Extensionは、様々なイベントが発生した時にDistributed Notificationsを送信します。macOSのアプリケーションとサービスは、Distributed Notificationsを使ってイベントの発生をほかのアプリケーションやサービスに伝えます。このイベントの通知をリッスンするアプリケーションまたはサービスがあれば、イベント発生時にアクションを実行することができます。

管理者はこの機能を使って、特定のイベントが発生した時に何らかのアクションを実行することができます。例えば、Kerberos SSO Extensionで新しいKerberos資格情報が取得された時にスクリプトを実行したい場合があります。

Kerberos SSO Extensionは、指定されたイベントが発生した時にDistributed Notificationsの送信だけを行います。イベントが発生しても、ほかのアクションは実行しません。管理者は、この通知をリッスンし通知を受信したらアクションを実行するツールを用意する必要があります。

付録には、通知をリッスンしてアクションを実行するスクリプトとlaunchdプロパティリスト(.plist)の例が掲載されています。この例を導入環境に合わせて編集してご利用ください。

Kerberos SSO Extensionが送信するDistributed Notificationsを以下に示します。

名前	送信されるタイミング
com.apple.KerberosPlugin.ConnectionCompleted	Kerberos SSO Extensionが接続プロセスを実行した。
com.apple.KerberosPlugin.ADPasswordChanged	ユーザーがこのExtensionを使ってActive Directoryのパスワードを変更した。
com.apple.KerberosPlugin.LocalPasswordSynced	ユーザーがActive Directoryのパスワードとローカルパスワードを同期した。
com.apple.KerberosPlugin.InternalNetworkAvailable	ユーザーが構成済みのActive Directoryドメインをできるネットワークに接続した。
com.apple.KerberosPlugin.InternalNetworkNotAvailable	ユーザーが構成済みのActive Directoryドメインを利用できないネットワークに接続した。
com.apple.KerberosExtension.gotNewCredential	ユーザーが新しいKerberos TGTを取得した。
com.apple.KerberosExtension.passwordChangedWithPasswordSync	ユーザーがActive Directoryのパスワードを変更し、ローカルパスワードが新しいActive Directoryのパスワードと同じパスワードにアップデートされた。

コマンドラインサポート — macOS

管理者はapp-ssoと呼ばれるコマンドラインツールを使って、Kerberos SSO Extensionを制御したり、有用な情報を取得したりできます。例えば、このツールを使ってサインインを始めたり、パスワードを変更したり、サインアウトしたりできます。さらに、現在サインインしているユーザーや、コンピュータの現在のActive Directoryサイト、ユーザーのネットワークホームの共有、ユーザーのパスワードの有効期限など、様々な有用な情報をプロパティリストまたはJSON形式で出力することもできます。この情報は、データを整形してMac上の管理ソリューションにアップロードすることで、インベントリ管理などの目的に活用することができます。

app-ssoの使い方の詳細については、ターミナルアプリケーションで「app-sso -h」を実行して確認ください。

モバイルアカウント — macOS

Kerberos SSO Extensionでは、MacをActive Directoryにバインドする必要も、ユーザーがモバイルアカウントを使ってMacにログインする必要もありません。Appleは、ローカルアカウントを使ってKerberos SSO Extensionを使用することをおすすめしています。macOSで推奨されている導入モデルにはローカルアカウントが最適です。また、組織のネットワークに常時接続しないこともある現代のMacユーザーにも最適です。Kerberos SSO Extensionは、ローカルアカウントを主体としてActive Directoryとの統合を強化するために作られています。

ただし、モバイルアカウントの使用を続けると判断した場合でも、Kerberos SSO Extensionをご利用いただけます。この機能には、以下の要件があります。

- モバイルアカウントでは、パスワード同期は利用できません。Kerberos SSO Extensionを使ってActive Directoryのパスワードを変更し、この際にKerberos SSO Extensionと同じユーザーアカウントでMacにログインしている場合、パスワードの変更は「ユーザとグループ」環境設定パネルから実行した場合と同じように機能します。一方、外部でパスワード変更を実行した場合（ウェブサイトでパスワードを変更したり、ヘルプデスクがパスワードをリセットした場合など）、Kerberos SSO ExtensionはモバイルアカウントのパスワードをActive Directoryのパスワードと同期し直すことはできません。
- Kerberos Extensionとモバイルアカウントを使ったパスワード変更URLの使用はサポートされていません。

ドメインとレルムのマッピング

Kerberosでドメインとレルムのマッピングをカスタム定義する必要がある場合があります。例えば、「ad.pretendco.com」という名前のKerberosレルムを持っている組織が、「fakecompany.com」ドメインのリソースでKerberos認証を使う必要がある場合などです。

注意：Appleのオペレーティングシステムに実装されているKerberosでは、ほぼすべての状況でドメインとレルムのマッピングを自動的に処理できます。管理者がこの設定をカスタマイズすることは、ほとんどありません。

Kerberos SSO Extensionでドメインとレルムのマッピングを構成するには、以下の手順に従います。

1. 拡張可能なSSOプロファイルの「カスタム構成」セクションで、domainRealmMappingというオブジェクトを追加します。オブジェクトタイプは「Dictionary」にします。
2. この辞書オブジェクトのキーはレルムの名前（大文字）に設定します。
3. この辞書オブジェクトの値は配列型で設定します。1つ目の値は、Kerberosレルムの名前（小文字）にし、先頭にピリオドを付けます。2つ目の値は、このレルムに対して認証が必要なドメイン名にし、こちらも先頭にピリオドを付けます。必要に応じて配列を追加します。

詳細については、Kerberosのドキュメント（英語）を参照してください。

Enterprise Connectからの移行

概要

Kerberos SSO Extensionは、同様の機能を持ち、多くの組織で使用されているEnterprise Connectに置き換わるツールです。Enterprise ConnectからKerberos SSO Extensionに移行するほとんどの組織では、以下の手順で移行することができます。

1. 現在のEnterprise Connectのプロファイルと同様の機能を提供する、Kerberos SSO Extensionの構成プロファイルを作成します。
2. Enterprise Connectをアンインストールします。
3. 新しいKerberos SSO Extensionの構成プロファイルを導入します。
4. ユーザーにKerberos SSO Extensionにサインインしてもらいます。

組織のMacコンピュータをmacOS 10.15にアップグレードすること自体でKerberos SSO Extensionへの移行が必要になるわけではなく、Enterprise ConnectはmacOS 10.15でも正常に機能します。ただし、最終的にはEnterprise Connectから移行することを計画しておいてください。

移行が適切ではない場合

Kerberos SSO Extensionは、Enterprise Connectをご利用中の大多数の組織のニーズを満たすものですが、以下の条件に該当する組織では、Enterprise Connectから移行できない、または部分的にしか移行できない場合があります。

- 現在組織内にmacOS 10.14以前を搭載したMacコンピュータが存在する場合、これらのシステムではEnterprise Connectを残し、macOS 10.15を搭載したMacコンピュータのみをKerberos SSO Extensionに移行してください。Kerberos SSO Extensionおよび関連する構成プロファイルは、macOS 10.15を搭載したMacコンピュータのみで機能します。Kerberos SSO Extensionを使用するには、macOS 10.15にアップグレードしてください。
- ユーザー承認型MDM登録をサポートしていないMac管理ツールを使用している組織。
- 管理ツールを使用していない組織。
- Windows Server 2003以前の機能レベルでActive Directoryを使用している組織。

Kerberos SSO Extensionの構成プロファイルを作成する

Kerberos SSO Extensionでは、Enterprise Connectの構成プロファイルと同様の構成プロファイルを作成する必要があります。現在お使いのEnterprise Connectの構成プロファイルにある多くの環境設定キーと同等のものが、Kerberos SSO Extensionのプロファイルにも用意されています。まずは、以下のKerberos SSO ExtensionとEnterprise Connectの環境設定キーの対応表を確認してください。

Enterprise Connect	Kerberos SSO Extension	メモ
adRealm	Realm	レルムはすべて大文字にします。
自動ログイン（デフォルトで有効）	allowAutomaticLogin	「カスタム構成」セクションに追加します。自動ログインを有効にするには「True」に設定する必要があります。
disablePasswordFunctions	allowPasswordChange	「カスタム構成」セクションに追加します。パスワード変更を無効にするには「False」に設定します。
passwordChangeURL	pwChangeURL	「カスタム構成」セクションに追加します。
passwordExpireOverride	pwExpireOverride	「カスタム構成」セクションに追加します。
passwordNotificationDays	pwNotificationDays	「カスタム構成」セクションに追加します。
prepopulatedUsername	principalName	「カスタム構成」セクションに追加します。
pwReqComplexity	pwReqComplexity	「カスタム構成」セクションに追加します。
pwReqHistory	pwReqHistory	「カスタム構成」セクションに追加します。
pwReqLength	pwReqLength	「カスタム構成」セクションに追加します。
pwReqMinimumPasswordAge	pwReqMinAge	「カスタム構成」セクションに追加します。
pwReqText	pwReqText	「カスタム構成」セクションに追加します。RTFファイルへのパスの代わりに、表示するテキスト文字列を指定します。
syncLocalPassword	syncLocalPassword	「カスタム構成」セクションに追加します。

注意：ここに掲載されていないEnterprise Connect構成プロファイルの環境設定キーもあります。掲載されていないものには、Kerberos SSO Extensionでは必要なくなった機能や、今後はサポートされない機能があります。

Enterprise Connectをアンインストールする

1台のコンピュータでKerberos SSO ExtensionとEnterprise Connectを同時に実行することはできません。Kerberos SSO Extensionに移行したら、Enterprise Connectをアンインストールしてください。アンインストールを実行するには、管理者権限が必要です。Enterprise Connectをアンインストールするには、以下の手順に従います。

Enterprise Connect 2.0以降

1. ターミナルアプリケーションを起動し、現在ログインしているユーザーで「launchctl unload /Library/LaunchAgents/com.apple.ecAgent」と実行して、Enterprise Connectエージェントをアンロードします。
2. ターミナルアプリケーションを起動し、「killall Enterprise\ Connect\ Menu」と入力して、Enterprise Connect Menu Extraを終了します。
3. 「アプリケーション」フォルダからEnterprise Connectアプリケーションを削除します。
4. Enterprise Connectのlaunchd .plist（/Library/LaunchAgents/com.apple.ecAgent.plist）を削除します。

Enterprise Connect 1.9.5以前

1. ターミナルアプリケーションで「killall Enterprise\ Connect」と入力して、Enterprise Connectを終了します。
2. 「アプリケーション」フォルダからEnterprise Connectアプリケーションを削除します。

付録には、どのバージョンのEnterprise Connectも削除できるサンプルスクリプトが掲載されています。

Enterprise Connectのスクリプトトリガ

Enterprise Connectでは、特定のイベントが発生した時にスクリプトを実行できます。例えば、Enterprise Connectが接続プロセスを完了した時や、ユーザーがパスワード変更を実行した時に、スクリプトを実行できます。Kerberos SSO Extensionでは、Enterprise Connectとは違う方法でスクリプトを処理し、スクリプトを直接実行することはありません。代わりに、イベント発生時にDistributed Notificationを送信します。別のプロセスを用意することで、この通知をリッスンして、通知が送信されたらスクリプトを実行するようにできます。詳細については、本書の「高度な機能」セクションを参照してください。

以下は、Enterprise Connectのスクリプトトリガと、Kerberos SSO Extensionで同等の機能を持つDistributed Notificationsの対応表です。

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

ネットワーク共有

Kerberos SSO Extensionは、ネットワーク共有（ユーザーのネットワークホームディレクトリなど）の処理をサポートしていません。こうした機能のほとんどは、スクリプトで実現できます。

付録

デバイス管理プロファイル：ExtensibleSingleSignOnKerberos（英語）

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

モバイルデバイス管理プロトコルリファレンス（英語）

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

デバイス管理プロファイル：ExtensibleSingleSignOnKerberos.ExtensionData（英語）

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

サンプルスクリプト — Distributed Notificationsの処理

Kerberos SSO Extensionでは、ユーザーがパスワードを変更した時や、企業ネットワークがオンラインになった時など、様々なイベントが発生した時にDistributed Notificationsを送信できます。管理者はスクリプトやアプリケーションを使ってこれらの通知をリッスンし、通知が送信されたらスクリプトやシェルコマンドなどのアクションを実行できます。

以下は、通知が送信された時にスクリプトまたはコマンドを実行できるサンプルスクリプトです。LaunchAgentでログインユーザーとして実行するか、LaunchDaemonでrootとして実行してください。このスクリプトは2つのパラメータを指定する必要があります。

- **-notification**は、リッスンするDistributed Notificationの名前です。13ページで例を確認してください。
- **-action**は、Distributed Notificationが送信された時に実行するアクションです。例えば「sh /path/to/script.sh」とします。

スクリプトを実行するには、デベロッパ用のコマンドラインツールをインストールする必要があります。ツールのインストーラパッケージはApple Developerサイトから入手できます。

```
#!/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()
```

サンプルスクリプト — Enterprise Connectのアンインストール

このサンプルスクリプトは、どのバージョンのEnterprise Connectでもアンインストールできます。Mac管理ソリューションから実行するか、手動で実行してください。このスクリプトはroot権限で実行する必要があります。

```
#!/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
```