Extensão Single Sign-on Kerberos

Manual do utilizador

Dezembro de 2019

Índice

Introdução

Com a extensão Single Sign-on (SSO) Kerberos, é fácil utilizar o início de sessão único baseado no Kerberos nos dispositivos Apple da empresa.

Autenticação Kerberos simplificada

A extensão SSO Kerberos simplifica o processo de aquisição de um ticket de atribuição de ticket (TGT) Kerberos a partir do domínio do Active Directory da empresa, permitindo que os utilizadores efetuem facilmente a autenticação em recursos como páginas da internet, apps e servidores de ficheiros. No macOS, a extensão SSO Kerberos adquire proativamente um TGT Kerberos após as alterações ao estado da rede para garantir que o utilizador está preparado para efetuar a autenticação, quando necessário.

Gestão de contas do Active Directory

A extensão SSO Kerberos também ajuda os utilizadores a gerirem as suas contas do Active Directory. No macOS, permite que os utilizadores alterem as palavras-passe do Active Directory e notifica-os quando uma palavra-passe estiver prestes a expirar. Os utilizadores também podem alterar as palavras-passe das contas locais para que correspondam às palavras-passe do Active Directory.

Compatibilidade com o Active Directory

A extensão SSO Kerberos deve ser utilizada com um domínio do Active Directory no local. Não é possível utilizar o Azure Active Directory. Para utilizar a extensão SSO Kerberos, não é necessário que os dispositivos sejam associados a um domínio do Active Directory. Além disso, não é necessário que os utilizadores iniciem sessão nos computadores Mac com as contas móveis ou do Active Directory. Em vez disso, a Apple recomenda a utilização de contas locais.

Requisitos

- iOS 13, iPadOS ou macOS Catalina.
- Um domínio do Active Directory a executar o Windows Server 2008 ou posterior. A extensão SSO Kerberos não se destina à utilização com o Azure Active Directory. Requer um domínio do Active Directory no local tradicional.
- Acesso à rede onde o domínio do Active Directory está alojado. Este acesso à rede pode ser efetuado através de Wi-Fi, Ethernet ou VPN.
- Os dispositivos devem ser geridos com uma solução de gestão de dispositivos móveis (MDM) compatível com a carga útil de perfil de configuração Single Sign-On (SSO) extensível. Contacte o seu fornecedor de MDM para solicitar informações sobre a compatibilidade com esta carga útil de perfil de configuração.

Enterprise Connect

A extensão SSO Kerberos destina-se a substituir o Enterprise Connect. Se utiliza atualmente o Enterprise Connect e pretende efetuar a transição para a extensão SSO Kerberos, consulte a secção "Efetuar a transição a partir do Enterprise Connect" deste documento para obter mais informações.

Primeiros passos

Criar e implementar um perfil de configuração

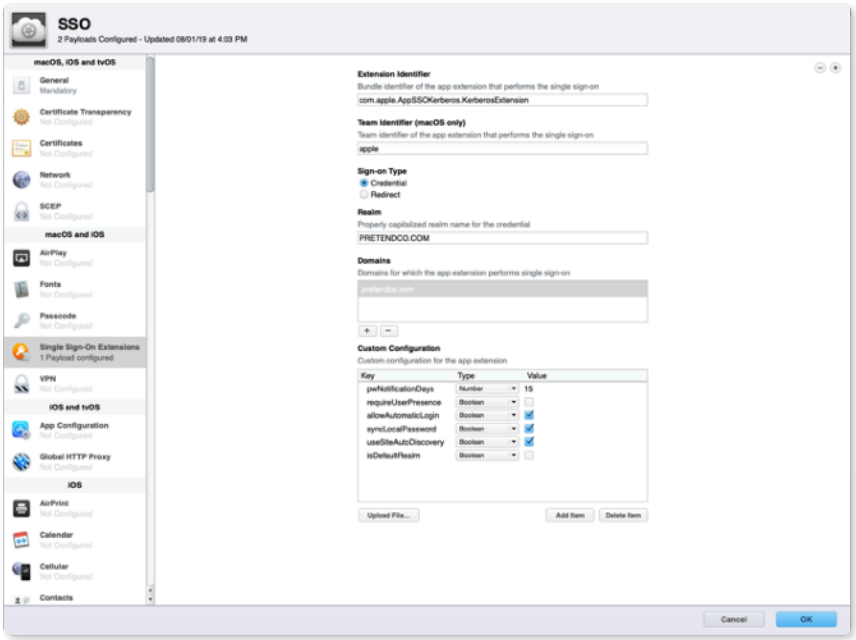
Para utilizar a extensão SSO Kerberos, deve configurá-la utilizando um perfil de configuração, enviado para o dispositivo a partir de uma solução de MDM.

Nota: o perfil de configuração deve ser enviado para o dispositivo através da MDM. No macOS, deve tratar-se de um registo na MDM aprovado pelo utilizador e deve ser instalado no âmbito System. Não é possível adicionar o perfil manualmente.

Para configurar com um perfil de configuração, é necessário utilizar a carga útil Single Sign-on extensível apresentada no iOS 13, iPadOS e macOS 10.15. O Profile Manager, que faz parte do macOS Server, inclui compatibilidade com a carga útil Single Sign-on extensível. Se a sua solução de MDM ainda não for compatível com esta carga útil, poderá ser capaz de criar o perfil necessário no Profile Manager e, em seguida, importá-lo para a solução de MDM para efetuar a distribuição. Para mais informações, contacte o seu fornecedor de MDM.

Para criar um perfil de configuração utilizando o Profile Manager, siga estes passos:

1. Inicie sessão no Profile Manager.
2. Crie um perfil para um grupo de dispositivos ou um dispositivo específico.
3. Selecione as extensões Single Sign-On na lista Payload e, em seguida, clique no botão Add (+) para adicionar uma nova carga útil.
4. No campo Extension Identifier, introduza "com.apple.AppSSOKerberos.KerberosExtension".
5. No campo Team Identifier, introduza "apple".



6. Selecione Credential em Sign-on Type.
7. No campo Realm, introduza o nome do domínio do Active Directory onde as contas de utilizador residem, em maiúsculas. Não utilize o nome da sua floresta do Active Directory, exceto se as contas de utilizador residirem ao nível da floresta.

8. Em Domains, clique no botão Add (+) e adicione domínios para todos os recursos que utilizem o Kerberos. Por exemplo, se utilizar a autenticação Kerberos com recursos em us.pretendco.com, adicione ".us.pretendco.com". (Não se esqueça do ponto final no início.)
9. Em Custom Configuration, adicione os seguintes valores:

Key	Type	Value
pwNotificationDays	Número	15
requireUserPresence	Boolean	Não assinalado
allowAutomaticLogin	Boolean	Assinalado
syncLocalPassword	Boolean	Assinalado
useSiteAutoDiscovery	Boolean	Assinalado
isDefaultRealm	Boolean	Não assinalado

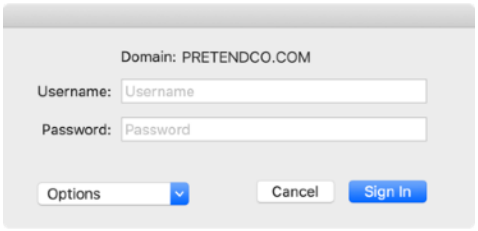
10. Clique em OK para guardar o novo perfil de configuração. Será instalado automaticamente no dispositivo ou grupo de dispositivos selecionado.

Configuração do utilizador — iOS e iPadOS

1. Ligue o dispositivo a uma rede onde o domínio do Active Directory da empresa estiver disponível.
2. Faça uma das ações seguintes:
   - Utilize o Safari para aceder a uma página da internet compatível com a autenticação Kerberos.
   - Abra uma app compatível com a autenticação Kerberos.
3. Introduza o seu nome de utilizador e a sua palavra-passe do Kerberos ou Active Directory.
4. Ser-lhe-á solicitado que indique se pretende iniciar sessão automaticamente de forma permanente. A maioria dos utilizadores deve tocar em Yes.
5. Toque em Sign In. Após uma breve pausa, a página da internet ou a app serão carregadas. Se optou por iniciar sessão na extensão SSO Kerberos automaticamente, já não terá de introduzir as credenciais até alterar a palavra-passe. Se optou por não iniciar sessão automaticamente, ser-lhe-á solicitado que introduza as credenciais apenas quando a sua credencial do Kerberos expirar (normalmente, no prazo de 10 horas).

Configuração do utilizador — macOS

1. Deve efetuar a autenticação na extensão SSO Kerberos. Há várias formas de iniciar este processo:
   - Se o Mac estiver ligado a uma rede onde o seu domínio do Active Directory estiver disponível, ser-lhe-á solicitado que efetue a autenticação de imediato após a instalação do perfil de configuração SSO extensível.
   - Se utilizar o Safari para aceder a uma página da internet que aceite a autenticação Kerberos, ou se utilizar uma app que requeira a autenticação Kerberos, ser-lhe-á solicitado que efetue a autenticação.
   - Ser-lhe-á imediatamente solicitado que efetue a autenticação sempre que ligar o Mac a uma rede onde o Active Directory estiver disponível.
   - Pode selecionar o menu extra da extensão SSO Kerberos e, em seguida, clicar em Sign In.
2. Ser-lhe-á solicitado que introduza as credenciais do Kerberos. Introduza o seu nome de utilizador e a sua palavra-passe do Kerberos ou Active Directory.



3. Ser-lhe-á solicitado que indique se pretende iniciar sessão automaticamente. A maioria dos utilizadores deve clicar em Yes.
4. Clique em Sign In. Após uma breve pausa, a página da internet ou a app serão carregadas. Se optou por iniciar sessão na extensão SSO Kerberos automaticamente, já não terá de introduzir as credenciais até alterar a palavra-passe. Se optou por não iniciar sessão automaticamente, ser-lhe-á solicitado que introduza as credenciais apenas quando a sua credencial do Kerberos expirar (normalmente, no prazo de 10 horas).
5. Se a sua palavra-passe estiver prestes a expirar, irá receber uma notificação a indicar quantos dias faltam para expirar. Pode clicar na notificação e alterar a palavra-passe.
6. Se ativou a funcionalidade de sincronização de palavras-passe, ser-lhe-á solicitado que introduza a palavra-passe local e a palavra-passe do Active Directory que utiliza atualmente. Introduza as duas e clique em OK para sincronizar as palavras-passe. Isto ser-lhe-á solicitado durante o início de sessão inicial, mesmo se as palavras-passe já estiverem sincronizadas.

Alterações da palavra-passe — macOS

Também pode alterar a palavra-passe do Active Directory com a extensão SSO Kerberos:

1. Certifique-se de que iniciou sessão na extensão SSO Kerberos.
2. Selecione o menu extra SSO Kerberos e escolha Change Password. Também poderá receber uma notificação a indicar que a palavra-passe está prestes a expirar.
3. Introduza a palavra-passe atual e, em seguida, a nova palavra-passe. Certifique-se de que utiliza uma nova palavra-passe que cumpra os requisitos de palavra-passe da empresa. Clique em OK.
4. Após uma breve pausa, será apresentada uma caixa de diálogo a indicar que a alteração da palavra-passe foi bem-sucedida. Se a funcionalidade de sincronização de palavras-passe estiver ativada, a palavra-passe da sua conta local será atualizada para corresponder à nova palavra-passe do Active Directory.

Utilizar o menu extra SSO Kerberos — macOS

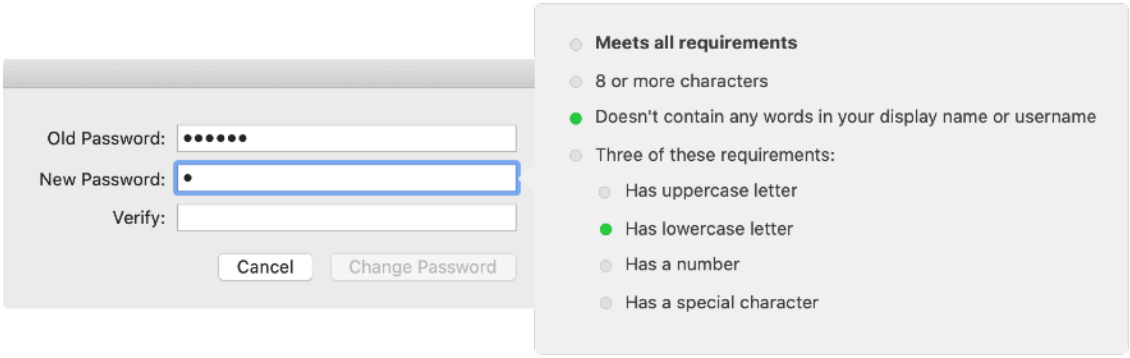
O menu extra SSO Kerberos fornece o acesso fácil a informações úteis sobre a sua conta e funções da extensão. Será apresentado como uma chave cinzenta ou preta na barra de menus no canto superior direito.

Para obter informações de estado sobre a sua conta, comece por observar a cor do ícone do menu extra SSO Kerberos. Se a chave for cinzenta, não tem sessão iniciada na extensão. Se a chave for preta, tem sessão iniciada. Após selecionar a chave, verá a conta com que iniciou sessão, bem como os dias que faltam até à palavra-passe expirar. O menu também permite iniciar sessão, terminar sessão e alterar a palavra-passe.

Funções avançadas

Testes imediatos da palavra-passe

Em muitas configurações do Active Directory, a extensão SSO Kerberos testa novas palavras-passe do utilizador à medida que são introduzidas e informa os utilizadores sobre os requisitos de palavra-passe que devem cumprir para alterarem as palavras-passe. Após a configuração, o utilizador terá acesso a esta vista quando introduzir a nova palavra-passe:



Para utilizar esta funcionalidade, o domínio do Active Directory deve utilizar apenas políticas de palavra-passe padrão do Active Directory. Por predefinição, o Active Directory permite que um administrador requeira que uma palavra-passe seja complexa e tenha um determinado comprimento. Para saber mais sobre o que constitui uma palavra-passe complexa, consulte technet.microsoft.com/en-us/library/cc786468(v=ws.10).aspx.

Nota: poderá não conseguir utilizar esta funcionalidade se o seu domínio utilizar ferramentas ou DLL de outras empresas para expandir a política de palavra-passe do Active Directory. Por exemplo, se não tiver permissão para utilizar determinadas palavras ou o seu nome de utilizador na palavra-passe, ou se for necessário utilizar um número específico de caracteres especiais na palavra-passe, poderá estar a utilizar extensões de política de palavra-passe de outras empresas. Se não tiver a certeza, peça mais informações ao seu administrador do Active Directory.

Se o domínio do Active Directory da empresa cumprir os requisitos, pode ativar os testes imediatos da palavra-passe. No seu perfil de configuração da extensão SSO Kerberos, defina os parâmetros seguintes:

Parâmetro	Key	Type	Value	Opcional
Requerer palavras-passe complexas	pwReqComplexity	Boolean	SIM	Não
Comprimento exigido da palavra-passe	pwReqLength	Integer	Número	Sim
Reutilizar limite da palavra-passe anterior	pwReqHistory	Integer	Número	Sim
Idade mínima da palavra-passe	pwReqMinAge	Integer	Número	Sim

Os testes imediatos da palavra-passe têm algumas limitações. Não permitem testar se uma palavra-passe já foi utilizada. Também não permitem testar se a palavra-passe contém o seu nome de apresentação do Active Directory se ainda não tiver um TGT Kerberos. Isto pode acontecer se estiver a definir a palavra-passe pela primeira vez ou se a palavra-passe tiver expirado. Todos os outros testes vão decorrer conforme esperado.

Apresentação de requisitos de palavra-passe

Se não puder utilizar os testes imediatos de palavras-passe, pode configurar a extensão SSO Kerberos para apresentar uma cadeia de texto com os requisitos de palavra-passe da empresa à medida que os utilizadores introduzem as novas palavras-passe. No perfil de configuração da extensão SSO Kerberos, defina "pwReqText" como uma cadeia que contenha o texto que pretende apresentar ao utilizador durante a alteração da palavra-passe.

Alterar ou desativar a funcionalidade de palavra-passe

Algumas empresas poderão não conseguir utilizar a funcionalidade padrão de alteração da palavra-passe da extensão SSO Kerberos, uma vez que não permitem alterações da palavra-passe com o Active Directory. No perfil de configuração da extensão SSO Kerberos, defina "allowPasswordChanges" como FALSE para desativar esta funcionalidade.

Compatibilidade com páginas de alteração da palavra-passe — macOS

A extensão SSO Kerberos pode ser configurada para abrir uma página de alteração da palavra-passe no navegador predefinido quando o utilizador selecionar "Change password" ou reconhecer um aviso de expiração da palavra-passe. A Apple recomenda a utilização desta funcionalidade apenas ao utilizar uma conta local, uma vez que não é possível utilizar contas móveis.

No perfil de configuração da extensão SSO Kerberos, defina "pwChangeURL" como o URL da sua página de alteração da palavra-passe. Assim que os utilizadores alterarem as palavras-passe, devem terminar sessão na extensão Kerberos e voltar a iniciar sessão com as palavras-passe atualizadas. Se a sincronização de palavras-passe locais estiver ativada, os utilizadores recebem instruções para voltarem a sincronizar as palavras-passe.

Sincronização de palavras-passe — macOS

A extensão SSO Kerberos permite definir a palavra-passe da conta local para corresponder à palavra-passe do Active Directory de um utilizador. Ative esta funcionalidade definindo "syncLocalPassword" como TRUE na secção Custom Configuration do perfil de configuração da extensão SSO Kerberos.

A sincronização de palavras-passe abrange duas funções básicas. Em primeiro lugar, quando o utilizador usa a extensão SSO Kerberos para alterar palavras-passe, esta funcionalidade define a palavra-passe local para corresponder à palavra-passe do Active Directory. Caso a palavra-passe local e a palavra-passe do Active Directory deixem de estar sincronizadas, a extensão SSO Kerberos sincroniza-as novamente utilizando o seguinte:

- Após a ativação da sincronização de palavras-passe e após todas as tentativas subsequentes de ligação por parte da extensão SSO Kerberos, as datas em que os utilizadores alteraram a palavra-passe local e a palavra-passe do Active Directory pela última vez são comparadas com os valores em cache. Se os valores corresponderem, as palavras-passe estão sincronizadas e não é necessária nenhuma ação. Se não corresponderem, a extensão SSO Kerberos irá solicitar a palavra-passe local e a palavra-passe do Active Directory dos utilizadores. Assim que os utilizadores fornecerem as palavras-passe locais, a extensão SSO Kerberos define a palavra-passe local de forma a corresponder à palavra-passe do Active Directory.
- As alterações das palavras-passe decorrem de forma semelhante. Quando os utilizadores alterarem a palavra-passe com a extensão SSO Kerberos, as palavras-passe antigas do Active Directory serão verificadas em função das contas locais. Se uma palavra-passe antiga do Active Directory e a palavra-passe local corresponderem, a extensão SSO Kerberos altera as duas palavras-passe. Se não corresponderem, apenas a palavra-passe do Active Directory é alterada. Durante a tentativa de ligação seguinte, os utilizadores necessitam de introduzir as palavras-passe locais.

Esta funcionalidade tem os seguintes requisitos:

- Se os utilizadores tiverem sessão iniciada nos computadores Mac com contas do Active Directory (e não contas locais), a sincronização de palavras-passe é desativada. Esta funcionalidade destina-se apenas à utilização com contas locais. Se os utilizadores tiverem sessão iniciada nos computadores Mac com contas do Active Directory, esta funcionalidade não é necessária.
- Se uma política de palavra-passe for aplicada para contas locais, por exemplo, utilizando um perfil de configuração ou um comando pwpolicy, certifique-se de que a política de palavra-passe local é correspondente ou menos rígida do que a política de palavra-passe do Active Directory. Se a política de palavra-passe local for mais rígida do que a política do Active Directory, a extensão SSO Kerberos poderá aceitar uma palavra-passe que cumpra os requisitos do Active Directory mas não permita definir a palavra-passe local, uma vez que a palavra-passe não cumpre os requisitos da palavra-passe local. Se for necessário que a política de palavra-passe local seja mais rígida do que a política de palavra-passe do Active Directory, não deve utilizar esta funcionalidade.
- O nome de utilizador local é diferente do nome de utilizador do Active Directory. Apenas as palavras-passe são definidas de forma a corresponderem.

Compatibilidade com cartões inteligentes — macOS

A extensão SSO Kerberos permite a utilização de identidades com base em cartões inteligentes para a autenticação. Os cartões inteligentes devem ter um controlador CryptoTokenKit disponível. Não é possível utilizar controladores com base em tokend. O macOS 10.15 inclui compatibilidade com a norma PIV, que é muito utilizada pelo governo dos EUA.

Antes de começar, certifique-se de que o seu domínio do Active Directory está configurado para suportar a autenticação de cartões inteligentes. O processo de ativação da autenticação de cartões inteligentes no Active Directory não é abrangido por este documento. Para mais informações, consulte a documentação da Microsoft.

Para iniciar sessão na extensão SSO Kerberos com um cartão inteligente, siga estes passos:

1. Clique no menu Options e, em seguida, selecione "Use a smart card".
2. Quando vir o botão Identity, insira o cartão inteligente e clique no botão.
3. Escolha a identidade com que pretende efetuar a autenticação, clique em OK e, em seguida, clique em Sign In.
4. Quando solicitado, introduza o seu PIN.

Se a extensão SSO Kerberos necessitar de adquirir um TGT Kerberos, ser-lhe-á solicitado que insira o cartão inteligente e introduza o seu PIN. Estão disponíveis mais informações sobre a compatibilidade com cartões inteligentes no macOS através da execução de "man SmartCardServices" no Terminal.

Notificações distribuídas — macOS

A extensão SSO Kerberos publica notificações distribuídas quando ocorrem vários eventos. As apps e os serviços no macOS utilizam notificações distribuídas para informar as outras apps e serviços sobre a ocorrência de um evento. Uma app ou serviço que procure reconhecer o evento pode agir quando este ocorrer.

Um administrador pode utilizar esta funcionalidade para efetuar uma ação quando ocorrerem determinados eventos. Por exemplo, um administrador poderá pretender executar um script sempre que a extensão SSO Kerberos adquirir uma nova credencial do Kerberos.

A extensão SSO Kerberos publica simplesmente notificações distribuídas quando ocorrem eventos especificados. Não executa ações quando estes eventos ocorrem. O administrador deve fornecer uma ferramenta para reconhecer estas notificações e executar ações quando ocorrerem.

O anexo contém um exemplo de uma lista de propriedades script e launchd (.plist) capaz de reconhecer notificações e executar ações. Modifique este exemplo conforme necessário para a implementação.

Abaixo encontram-se notificações distribuídas publicadas pela extensão SSO Kerberos:

Nome	Publicado quando
com.apple.KerberosPlugin.ConnectionCompleted	A extensão SSO Kerberos executou o processo de ligação.
com.apple.KerberosPlugin.ADPasswordChanged	O utilizador alterou a palavra-passe do Active Directory com a extensão.
com.apple.KerberosPlugin.LocalPasswordSynced	O utilizador sincronizou a palavra-passe local e a do Active Directory.
com.apple.KerberosPlugin.InternalNetworkAvailable	O utilizador estabeleceu ligação a uma rede onde o domínio do Active Directory configurado está disponível.
com.apple.KerberosPlugin.InternalNetworkNotAvailable	O utilizador estabeleceu ligação a uma rede onde o domínio do Active Directory configurado não está disponível.
com.apple.KerberosExtension.gotNewCredential	O utilizador adquiriu um novo TGT Kerberos.
com.apple.KerberosExtension.passwordChangedWithPasswordSync	O utilizador alterou a palavra-passe do Active Directory e a palavra-passe local foi atualizada para corresponder à nova palavra-passe do Active Directory.

Compatibilidade com a linha de comandos — macOS

Os administradores podem utilizar uma ferramenta de linha de comando chamada *app-sso* para controlar a extensão SSO Kerberos e aceder a informações úteis. Por exemplo, podem utilizar a ferramenta para começar o início de sessão, as alterações da palavra-passe e o término de sessão. Também é possível imprimir informações úteis, como o utilizador com sessão iniciada atualmente, a página atual do Active Directory do computador, a partilha doméstica da rede do utilizador, a data de expiração da palavra-passe do utilizador e várias outras informações úteis no formato JSON ou de lista de propriedades. Esta informação pode ser analisada e carregada para uma solução de gestão do Mac para fins de inventário e outras finalidades.

Para mais informações sobre a utilização de app-sso, execute "app-sso -h" na app Terminal.

Contas móveis — macOS

A extensão SSO Kerberos não requer que o Mac esteja vinculado ao Active Directory ou que o utilizador tenha sessão iniciada no Mac com uma conta móvel. A Apple sugere a utilização da extensão SSO Kerberos com uma conta local. As contas locais funcionam melhor com o modelo de implementação recomendado para o macOS e são a melhor escolha para os utilizadores do Mac da atualidade, que podem estabelecer ligação à rede da empresa de forma intermitente. A extensão SSO Kerberos foi criada especificamente para melhorar a integração do Active Directory a partir de uma conta local.

No entanto, se optar por continuar a utilizar contas móveis, ainda pode utilizar a extensão SSO Kerberos. Esta funcionalidade tem os seguintes requisitos:

- A sincronização de palavras-passe não pode ser efetuada com contas móveis. Se utilizar a extensão SSO Kerberos para alterar a palavra-passe do Active Directory e tiver sessão iniciada no Mac com a mesma conta de utilizador que está a utilizar com a extensão SSO Kerberos, as alterações da palavra-passe funcionam da mesma forma como no painel de preferências Users & Groups. No entanto, se efetuar uma alteração de palavra-passe externa (isto é, se alterar a palavra-passe numa página da internet ou se o serviço de assistência a repuser), a extensão SSO Kerberos não poderá voltar a sincronizar a palavra-passe da conta móvel e a palavra-passe do Active Directory.
- Não é possível utilizar um URL de alteração da palavra-passe com a extensão Kerberos e uma conta móvel.

Mapeamento domínio-protocolo

Um administrador poderá necessitar de definir um mapeamento domínio-protocolo personalizado para o Kerberos. Por exemplo, uma empresa poderá ter um protocolo Kerberos com o nome "ad.pretendco.com" mas poderá necessitar de usar a autenticação Kerberos para recursos no domínio "fakecompany.com".

Nota: a implementação do Kerberos nos sistemas operativos da Apple pode determinar automaticamente o mapeamento domínio-protocolo em quase todas as situações. É muito raro um administrador personalizar estas definições.

O mapeamento domínio-protocolo pode ser configurado para a extensão SSO Kerberos através dos passos seguintes:

1. Na secção Custom Configuration do perfil SSO extensível, adicione um objeto com o nome domainRealmMapping. O tipo do objeto deve ser Dictionary.
2. Defina a chave deste dicionário como o nome do seu protocolo em maiúsculas.
3. Defina o valor deste dicionário para ser do tipo Array. O primeiro valor deve ser o nome do seu protocolo Kerberos em minúsculas, começando por um ponto final. O segundo valor deve ser o nome do domínio que necessita de efetuar a autenticação em função deste protocolo, que deve também começar por um ponto final. Adicione sistemas conforme necessário.

Para mais informações, consulte a documentação do Kerberos.

Efetuar a transição a partir do Enterprise Connect

Descrição geral

A extensão SSO Kerberos destina-se a substituir o Enterprise Connect, uma ferramenta semelhante que muitas empresas já utilizam. A maioria das empresas que efetuarem a transição do Enterprise Connect para a extensão SSO Kerberos vai seguir estes passos:

1. Crie um perfil de configuração para a extensão SSO Kerberos que forneça uma funcionalidade semelhante ao seu perfil atual do Enterprise Connect.
2. Desinstale o Enterprise Connect.
3. Implemente o novo perfil de configuração da extensão SSO Kerberos.
4. Solicite aos utilizadores que iniciem sessão na extensão SSO Kerberos.

Não é necessário efetuar a transição para a extensão SSO Kerberos para atualizar os computadores Mac da empresa para o macOS 10.15. O Enterprise Connect funciona conforme esperado com o macOS 10.15, mas as empresas devem planear uma eventual transição a partir do Enterprise Connect.

Quem não deve efetuar a transição

A extensão SSO Kerberos irá satisfazer as necessidades da vasta maioria das empresas que utilizam o Enterprise Connect. No entanto, uma empresa que cumpra os seguintes critérios poderá não conseguir efetuar a transição a partir do Enterprise Connect ou poderá conseguir apenas efetuar uma transição parcial:

- Uma empresa que utilize atualmente computadores Mac com o macOS 10.14 ou anterior deve continuar a executar o Enterprise Connect nestes sistemas e efetuar a transição para a extensão SSO Kerberos apenas em computadores Mac com o macOS 10.15. A extensão SSO Kerberos e o perfil de configuração associado apenas funcionam em computadores Mac com o macOS 10.15. Atualize estes sistemas para o macOS 10.15 para tirar partido da extensão SSO Kerberos.
- Uma empresa que utilize uma ferramenta de gestão do Mac que não seja compatível com o registo na MDM aprovado pelo utilizador.
- Uma empresa que não esteja a utilizar uma ferramenta de gestão.
- Uma empresa que utilize um nível funcional do Active Directory do Windows Server 2003 ou anterior.

Criar um perfil de configuração da extensão SSO Kerberos

Terá de criar um perfil de configuração para a extensão SSO Kerberos semelhante ao perfil de configuração do Enterprise Connect. Muitas Preference Keys no seu perfil de configuração atual do Enterprise Connect têm equivalentes num perfil da extensão SSO Kerberos. Comece por consultar a tabela abaixo, que contém um mapa dos equivalentes da extensão SSO Kerberos às Preference Keys do Enterprise Connect:

Enterprise Connect	Extensão SSO Kerberos	Notas
adRealm	Realm	O protocolo deve estar em maiúsculas.
Automatic login (enabled by default)	allowAutomaticLogin	Adicionar à secção Custom Configuration. Deve ser definido como True para permitir o início de sessão automático.
disablePasswordFunctions	allowPasswordChange	Adicionar à secção Custom Configuration. Definir como False para desativar a alteração da palavra-passe.
passwordChangeURL	pwChangeURL	Adicionar à secção Custom Configuration.
passwordExpireOverride	pwExpireOverride	Adicionar à secção Custom Configuration.
passwordNotificationDays	pwNotificationDays	Adicionar à secção Custom Configuration.
prepopulatedUsername	principalName	Adicionar à secção Custom Configuration.
pwReqComplexity	pwReqComplexity	Adicionar à secção Custom Configuration.
pwReqHistory	pwReqHistory	Adicionar à secção Custom Configuration.
pwReqLength	pwReqLength	Adicionar à secção Custom Configuration.
pwReqMinimumPasswordAge	pwReqMinAge	Adicionar à secção Custom Configuration.
pwReqText	pwReqText	Adicionar à secção Custom Configuration. Fornecer uma cadeia de texto a apresentar em vez de um caminho para um ficheiro RTF.
syncLocalPassword	syncLocalPassword	Adicionar à secção Custom Configuration.

Nota: algumas Preference Keys no perfil de configuração do Enterprise Connect podem não estar indicadas aqui. Podem referir-se a uma funcionalidade que já não é necessária na extensão SSO Kerberos ou que já não é compatível.

Desinstalar o Enterprise Connect

Não é possível executar a extensão SSO Kerberos e o Enterprise Connect em simultâneo no mesmo computador. Após efetuar a transição para a extensão SSO Kerberos, desinstale o Enterprise Connect. É necessário possuir direitos administrativos para desinstalar. Para desinstalar o Enterprise Connect, siga os passos abaixo:

Enterprise Connect 2.0 e posterior

1. Descarregue o agente do Enterprise Connect abrindo a app Terminal e executando "launchctl unload /Library/LaunchAgents/com.apple.ecAgent" como o utilizador com sessão iniciada.
2. Saia do menu extra Enterprise Connect abrindo a app Terminal e introduzindo "killall Enterprise\ Connect\ Menu" na app Terminal.
3. Apague a app Enterprise Connect da pasta Applications.
4. Apague a .plist launchd do Enterprise Connect em /Library/LaunchAgents/com.apple.ecAgent.plist.

Enterprise Connect 1.9.5 e anterior

1. Saia do Enterprise Connect introduzindo “killall Enterprise\ Connect” na app Terminal.
2. Apague a app Enterprise Connect da pasta Applications.

O anexo fornece uma amostra de script que remove qualquer versão do Enterprise Connect.

Acionadores de script do Enterprise Connect

O Enterprise Connect pode executar scripts quando ocorrem determinados eventos. Por exemplo, o Enterprise Connect pode executar um script quando concluir o processo de ligação ou quando o utilizador alterar a palavra-passe. A extensão SSO Kerberos gere os scripts de forma diferente do Enterprise Connect. Não executa os scripts diretamente. Em vez disso, publica uma notificação distribuída quando ocorre um evento, que outro processo pode reconhecer, e executa um script. Para mais informações, consulte a secção "Funções avançadas" deste documento.

Abaixo, poderá encontrar as referências dos acionadores de scripts do Enterprise Connect e as notificações distribuídas equivalentes na extensão SSO Kerberos:

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

Partilhas de rede

A extensão SSO Kerberos não suporta a gestão de partilhas de rede, como o diretório doméstico da rede do utilizador. Pode substituir uma grande parte desta funcionalidade por scripts.

Anexo

Perfil de gestão de dispositivos: ExtensibleSingleSignOnKerberos

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

Referência do protocolo para gestão de dispositivos móveis

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

Perfil da gestão de dispositivos: ExtensibleSingleSignOnKerberos.ExtensionData

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

Amostra de script — Processar notificações distribuídas

A extensão SSO Kerberos publica várias notificações distribuídas quando ocorrem eventos diferentes, por exemplo, quando o utilizador altera uma palavra-passe ou a rede empresarial fica online. Como administrador, pode utilizar um script ou uma app para reconhecer estas notificações e agir quando são publicadas, como executar um script ou comando shell.

Abaixo, poderá encontrar uma amostra de script que permite executar scripts ou comandos quando são publicadas notificações. Deve ser executada como LaunchAgent a executar como utilizador com sessão iniciada ou LaunchDaemon a executar como raiz. O script utiliza dois parâmetros necessários:

- **-notification** é o nome da notificação distribuída que deve procurar reconhecer. Para ver exemplos, consulte a página 11.
- **-action** é a ação que pretende executar quando a notificação distribuída é publicada. Um exemplo é "sh /path/to/script.sh".

Para executar o script, deve instalar as ferramentas de linha de comando para programadores. Está disponível um pacote de instalação para estas ferramentas na página para programadores da Apple.

```
#!/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()
```

Amostra de script — Desinstalar o Enterprise Connect

Esta amostra de script remove qualquer versão do Enterprise Connect. Execute-a a partir de uma solução de gestão do Mac ou manualmente. O script deve ser executado com privilégios de raiz.

```
#!/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
```