

# Entender o Suporte do Umbrella para Importar Identidades de Usuário e Grupo do Azure AD e Okta

## Contents

---

[Introdução](#)

[Casos de uso suportados](#)

[Restrições](#)

[Identidades de provisionamento](#)

---

## Introdução

Este documento descreve o Umbrella que agora oferece suporte ao provisionamento de identidades de usuário e grupo do Azure Active Directory e do Okta, com base no padrão SCIM.

## Casos de uso suportados

SWG Umbrella:

- Importe identidades de usuário e grupo do Azure AD/Okta junto com a configuração da autenticação SAML no Azure AD/Okta para usuários finais que estão se conectando ao SWG por meio de um túnel IPsec, arquivos PAC ou encadeamento de proxy.
- Importe identidades de usuário e grupo do Azure AD para habilitar a identificação de usuário para o módulo AnyConnect SWG em dispositivos que estão autenticando no AD local ou no Azure AD.
- Importe as identidades de usuário e grupo do Okta para permitir a identificação de usuário para o módulo AnyConnect SWG em dispositivos que estão se autenticando no AD local.

DNS de guarda-chuva:

- Importe identidades de usuário e grupo do Azure AD para habilitar a identificação de usuário para o módulo DNS/cliente de roaming do AnyConnect em dispositivos que estão autenticando no AD local ou no Azure AD.
- Importe identidades de usuário e grupo do Okta para habilitar a identificação de usuário para o módulo DNS/cliente de roaming do AnyConnect em dispositivos que estão se autenticando em relação ao AD local.

## Restrições

- O Azure AD/Okta não pode fornecer integração de identidade de usuário para Umbrella Virtual Appliances (VAs). Isso ocorre porque o Azure AD/Okta não tem visibilidade do IP

privado - mapeamentos de usuário, que são exigidos pelos VAs. As implantações de VA continuam a exigir a implantação de um conector AD Umbrella local para facilitar a integração do AD.

- Não há suporte para a implantação simultânea das mesmas identidades de usuário/grupo do AD local e do Azure AD/Okta. Se você implantou anteriormente um conector AD local para provisionar usuários e grupos e agora está procurando provisionar as mesmas identidades de usuário e grupo do Azure AD/Okta, será necessário interromper o conector AD obrigatoriamente antes de ativar o provisionamento do Azure AD/Okta.
- Não há limite para o número de usuários que podem ser provisionados do Azure AD/Okta. Para grupos, um máximo de 200 grupos podem ser provisionados do Azure AD/Okta para uma organização Umbrella. O Azure AD dá suporte a grupos dinâmicos, portanto, você pode criar um grupo "Todos os Usuários" e provisionar esse grupo junto com até 199 outros grupos nos quais eles desejam definir a política do Umbrella. O Okta também tem um grupo Todos incorporado, de modo que você pode provisionar este grupo junto com até 199 outros grupos nos quais eles desejam definir a política.
- O AnyConnect SWG não oferece suporte a uma autenticação SAML no Azure AD. Ele se baseia no mesmo mecanismo de autenticação passiva usado com o AD local.

## Identities de provisionamento

Para provisionar identidades de qualquer um desses provedores de identidade, você pode usar as instruções documentadas nos links abaixo:

- Provisione identidades do Azure AD: <https://docs.umbrella.com/umbrella-user-guide/docs/microsoft-azure-ad-integration>
- Provisione identidades de Okta: <https://docs.umbrella.com/umbrella-user-guide/docs/okta-integration>

## Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.