

# 了解Umbrella支持从Azure AD和Okta导入用户和组身份

## 目录

---

[简介](#)

[支持的使用案例](#)

[限制](#)

[调配标识](#)

---

## 简介

本文档介绍目前支持基于SCIM标准从Azure Active Directory和Okta设置用户和组身份的Umbrella。

## 支持的使用案例

雨伞交换机：

- 从Azure AD/Okta导入用户和组身份，同时为通过IPsec隧道、PAC文件或代理链接连接到SWG的最终用户设置针对Azure AD/Okta的SAML身份验证。
- 从Azure AD导入用户和组身份，以便在针对本地AD或Azure AD进行身份验证的设备上启用AnyConnect SWG模块的用户标识。
- 从Okta导入用户和组身份，以启用针对本地AD进行身份验证的设备上AnyConnect SWG模块的用户身份。

Umbrella DNS:

- 从Azure AD导入用户和组身份，以便在针对本地AD或Azure AD进行身份验证的设备上启用AnyConnect DNS模块/漫游客户端的用户标识。
- 从Okta导入用户和组身份，以启用针对本地AD进行身份验证的设备上的AnyConnect DNS模块/漫游客户端的用户身份。

## 限制

- Azure AD/Okta无法为Umbrella虚拟设备(VA)提供用户身份集成。这是因为Azure AD/Okta没有私有IP — 用户映射的可视性，这是虚拟助理所必需的。VA部署仍需要部署内部Umbrella AD连接器，以促进AD集成。
- 不支持从本地AD和Azure AD/Okta并行部署相同的用户/组身份。如果您以前部署了内部AD连接器来调配用户和组，并且现在希望从Azure AD/Okta调配相同的用户和组身份，则您必须在打开Azure AD/Okta调配之前停止AD连接器。
- 对于可以从Azure AD/Okta调配的用户数没有限制。对于组，最多可以将200个组从Azure AD/Okta调配到Umbrella组织。Azure AD支持动态组，因此您可以创建“所有用户”组，并设置此组以及他们想要在其上定义Umbrella策略的最多199个其他组。同样，Okta有一个内置的

Everyone组，因此您可以设置该组以及他们想要在其上定义策略的最多199个其他组。

- AnyConnect SWG不支持针对Azure AD的SAML身份验证。它依赖于与本地AD相同的被动身份验证机制。

## 调配标识

要从这些身份提供者调配身份，您可以使用以下链接中记录的说明：

- 从Azure AD设置标识：<https://docs.umbrella.com/umbrella-user-guide/docs/microsoft-azure-ad-integration>
- 从Okta调配身份：<https://docs.umbrella.com/umbrella-user-guide/docs/okta-integration>

## 关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。