Understand Umbrella Support for Importing User and Group Identities from Azure AD and Okta

Contents

Introduction

This document describes Umbrella now supporting provisioning user and group identities from Azure Active Directory and Okta, based on the SCIM standard.

Supported Use Cases

Umbrella SWG:

- Import user and group identities from Azure AD/Okta in conjunction with setting up SAML authentication against Azure AD/Okta for end users that are connecting to SWG via an IPsec tunnel, PAC files or proxy chaining.
- Import user and group identities from Azure AD to enable user identification for the AnyConnect SWG module on devices that are authenticating against on-prem AD or Azure AD.
- Import user and group identities from Okta to enable user identification for the AnyConnect SWG module on devices that are authenticating against on-prem AD.

Umbrella DNS:

- Import user and group identities from Azure AD to enable user identification for AnyConnect DNS module/Roaming Client on devices that are authenticating against on-prem AD or Azure AD.
- Import user and group identities from Okta to enable user identification for AnyConnect DNS module/Roaming Client on devices that are authenticating against on-prem AD.

Constraints

- **Azure AD/Okta cannot provide user identity integration for Umbrella Virtual Appliances (VAs).** This is because Azure AD/Okta does not have visibility of the private IP – user mappings, which are required by the VAs. VA deployments continue to require deployment of an on-premise Umbrella AD connector to facilitate AD integration.
- Concurrent deployment of the same user/group identities from on-premise AD and Azure AD/Okta is not supported. If you have previously deployed an on-premise AD connector to provision users and groups, and are now looking to provision the same user and group identities from Azure AD/Okta, you mandatorily need to stop the AD connector before turning on the Azure AD/Okta provisioning.
- There is no limit to the number of users that can be provisioned from Azure AD/Okta. For groups, **a maximum of 200 groups** can be provisioned from Azure AD/Okta to an Umbrella org. Azure AD supports dynamic groups, so you can create an ‘All Users’ group, and provision this group along with up to 199 other groups on which they want to define Umbrella policy. Okta similarly has a built-in

Everyone group, so you can provision this group along with up to 199 other groups on which they want to define policy.
- AnyConnect SWG does not support a SAML authentication against Azure AD. It relies on the same passive authentication mechanism that is used with the on-premise AD.

Provisioning Identities

To provision identities from either of these Identity providers, you can use the instructions documented at the links below:

- Provision identities from Azure AD: https://docs.umbrella.com/umbrella-user-guide/docs/microsoft-azure-ad-integration
- Provision identities from Okta: https://docs.umbrella.com/umbrella-user-guide/docs/okta-integration