Begrijp overkoepelende ondersteuning voor het importeren van gebruikers- en groepsidentiteiten van Azure AD en Okta

Inhoud

Inleiding

In dit document wordt beschreven dat Umbrella nu ondersteuning biedt voor de provisioning van gebruikers- en groepsidentiteiten van Azure Active Directory en Okta, op basis van de SCIM-standaard.

Ondersteunde gebruiksscenario's

Umbrella SWG:

- Importeer gebruikers- en groepsidentiteiten van Azure AD/Okta in combinatie met het instellen van SAML-verificatie tegen Azure AD/Okta voor eindgebruikers die verbinding maken met SWG via een IPsec-tunnel, PAC-bestanden of proxyketens.
- Importeer gebruikers- en groepsidentiteiten uit Azure AD om gebruikersidentificatie voor de AnyConnect SWG-module mogelijk te maken op apparaten die worden geverifieerd met AD op voorhand of Azure AD.
- Importeer gebruikers- en groepsidentiteiten uit Okta om gebruikersidentificatie voor de AnyConnect SWG-module mogelijk te maken op apparaten die worden geverifieerd met AD op voorgrond.

Paraplu-DNS:

- Gebruikers- en groepsidentiteiten importeren uit Azure AD om gebruikersidentificatie mogelijk te maken voor AnyConnect DNS-module/roamingclient op apparaten die zich verifiëren tegen AD op het premiestation of Azure AD.
- Importeer gebruikers- en groepsidentiteiten van Okta om gebruikersidentificatie voor AnyConnect DNS-module/roamingclient mogelijk te maken op apparaten die worden geverifieerd tegen AD op voorhand.

beperkingen

- Azure AD/Okta kan geen gebruikersidentiteitsintegratie bieden voor Umbrella Virtual Appliances (VA's). Dit komt omdat Azure AD / Okta geen zichtbaarheid heeft van de privé-IP - gebruikerstoewijzingen, die vereist zijn door de VA's. VA-implementaties vereisen nog steeds de implementatie van een on-premise Umbrella AD-connector om AD-integratie te vergemakkelijken.
- Gelijktijdige implementatie van dezelfde gebruikers-/groepsidentiteiten van on-premise AD en Azure AD/Okta wordt niet ondersteund. Als u eerder een on-premise AD-connector hebt geïmplementeerd om gebruikers en groepen te voorzien en nu dezelfde gebruikers- en groepsidentiteiten van Azure AD/Okta wilt aanbieden, moet u de AD-connector verplicht stoppen voordat u de Azure AD/Okta-provisioning inschakelt.
- Er is geen limiet aan het aantal gebruikers dat kan worden geleverd vanuit Azure AD/Okta. Voor groepen kunnen maximaal 200 groepen van Azure AD/Okta naar een Umbrella org worden gestuurd. Azure AD ondersteunt dynamische groepen, zodat u een groep 'Alle gebruikers' kunt maken en deze groep samen met maximaal 199 andere groepen kunt aanbieden waarop ze het overkoepelende beleid willen definiëren. Okta heeft ook een ingebouwde Iedereen groep, zodat u deze groep samen met maximaal 199 andere groepen waarop ze willen het beleid te bepalen.
- AnyConnect SWG ondersteunt geen SAML-verificatie tegen Azure AD. Het is gebaseerd op hetzelfde passieve authenticatiemechanisme dat wordt gebruikt met de on-premise AD.

Provisioning-identiteiten

Om identiteiten van een van deze Identiteitsproviders te verstrekken, kunt u de instructies gebruiken die zijn gedocumenteerd op de onderstaande links:

- Aanbiedingsidentiteiten van Azure AD: https://docs.umbrella.com/umbrella-user-guide/docs/microsoft-azure-ad-integration
- Aanbiedingsidentiteiten van Okta: https://docs.umbrella.com/umbrella-user-guide/docs/okta-integration

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.