Comprender el soporte general para importar identidades de usuarios y grupos desde Azure AD y Okta

Contenido

Introducción

Este documento describe Umbrella, que ahora admite el aprovisionamiento de identidades de usuario y grupo desde Azure Active Directory y Okta, según el estándar SCIM.

Casos prácticos compatibles

SWG de paraguas:

- Importar identidades de usuario y grupo desde Azure AD/Okta junto con la configuración de la autenticación SAML en Azure AD/Okta para usuarios finales que se conectan a SWG a través de un túnel IPsec, archivos PAC o encadenamiento de proxy.
- Importe identidades de usuarios y grupos desde Azure AD para habilitar la identificación de usuarios para el módulo SWG de AnyConnect en dispositivos que se autentican en AD in situ o Azure AD.
- Importe identidades de usuarios y grupos desde Okta para habilitar la identificación de usuarios para el módulo SWG de AnyConnect en los dispositivos que se autentican en AD in situ.

DNS general:

- Importe identidades de usuario y grupo desde Azure AD para habilitar la identificación de usuario para el módulo DNS/cliente de roaming de AnyConnect en dispositivos que se autentican en AD in situ o Azure AD.
- Importe identidades de usuarios y grupos desde Okta para habilitar la identificación de usuarios para el módulo DNS AnyConnect/cliente de roaming en dispositivos que se autentican en AD in situ.

Restricciones

- Azure AD/Okta no puede proporcionar integración de identidad de usuario para los

dispositivos virtuales de Umbrella (VA). Esto se debe a que Azure AD/Okta no tiene visibilidad de las asignaciones de usuario de IP privada, que requieren los VA. Las implementaciones de AV siguen precisando la implementación de un conector Umbrella AD en las instalaciones para facilitar la integración de AD.

- No se admite la implementación simultánea de las mismas identidades de usuario/grupo desde AD en las instalaciones y Azure AD/Okta. Si ya ha implementado un conector de AD en las instalaciones para aprovisionar usuarios y grupos y ahora desea aprovisionar las mismas identidades de usuario y grupo desde Azure AD/Okta, debe detener obligatoriamente el conector de AD antes de activar el aprovisionamiento de Azure AD/Okta.
- No hay límite en el número de usuarios que se pueden aprovisionar desde Azure AD/Okta. Para grupos, se puede aprovisionar un máximo de 200 grupos desde Azure AD/Okta a una organización de Umbrella. Azure AD admite grupos dinámicos, por lo que puede crear un grupo "Todos los usuarios" y aprovisionar este grupo junto con hasta otros 199 grupos en los que desee definir la política de Umbrella. Okta también tiene un grupo Todos integrado, por lo que puede aprovisionar este grupo junto con hasta otros 199 grupos en los que desea definir la política.
- AnyConnect SWG no admite una autenticación SAML en Azure AD. Se basa en el mismo mecanismo de autenticación pasiva que se utiliza con el AD en las instalaciones.

Aprovisionamiento de identidades

Para aprovisionar identidades de cualquiera de estos proveedores de identidad, puede utilizar las instrucciones que se describen en los siguientes enlaces:

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

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).