

Cloud Web Security: Configure los atributos de usuario/grupo con PingFederate y ADFS mientras utiliza SAML.

Contenido

[Introducción](#)

[Requirements](#)

[Configuración](#)

[PingFed](#)

[ADFS](#)

[Verificación](#)

[Troubleshoot](#)

[Conversaciones relacionadas de la comunidad de soporte de Cisco](#)

Introducción

Este documento describe cómo configurar servidores PingFederate y ADFS (Servicios Federados de Active Directory) IDP para enviar los detalles del usuario/grupo al servicio Cloud Web Security para filtrar las políticas de forma granular.

Requirements

Cisco recomienda que tenga una comprensión básica de lo siguiente:

- Inicio de sesión administrativo/acceso al servidor PingFed/ADFS
- Conocimiento de cómo navegar por el servidor PingFed/ADFS
- Para que la granularidad funcione en el tráfico HTTPS, la inspección HTTPS se debe aplicar para todo el tráfico

Configuración

Siga los pasos siguientes para configurar los atributos de usuario/grupo con PingFederate y ADFS .

PingFed

En **orígenes de atributos** > **ficha de búsqueda de usuario**:

- Contrato de atributo: **AUTHENTICATED_GROUPS**
Fuente: **LDAP**

Valor: **miembroOf**

- Contrato de atributo: **SAML_SUBJECT**

Fuente: **LDAP**

Valor: **sAMAccountName**

ADFS

En **Relaciones de confianza** > ficha **Confiar en confianza de parte**:

- Contrato de atributo LDAP: **SAM-Account-Name**
LDAP de tipo de reclamación saliente: **ID de nombre**
- Contrato de atributo LDAP: **Grupos Token**
LDAP de tipo de reclamación saliente: **Grupo**

Verificación

Troubleshoot

No hay sección de solución de problemas para este documento.