Contents

Introduction

This document describes how to configure PingFederate and ADFS (Active Directory Federated Services) IDP servers to send user/group details to the Cloud Web Security service in order to granularly filter policies.

Requirements

Cisco recommends that you have a basic understanding of the following.

- Administrative login/access to the PingFed/ADFS server
- Knowledge of how to navigate the PingFed/ADFS server
- In order for granulairty to work on HTTPS traffic, HTTPS inspection must be enforced for all traffic

Configuration

Please follow below steps to Configure user/group attributes with PingFederate and ADFS .

PingFed

Under **Attribute sources > User lookup** tab:

- Attribute Contract: **AUTHENTICATED_GROUPS**
  Source:**LDAP**

  Value: **memberOf**

- Attribute Contract: **SAML_SUBJECT**
  Source: **LDAP**

  Value: **sAMAccountName**

ADFS

Under **Trust relationships > Relying party trusts** tab:

- LDAP Attribute Contract: **SAM-Account-Name**
  Outgoing Claim Type LDAP: **Name ID**
- LDAP Attribute Contract: **Token-Groups**
  Outgoing Claim Type LDAP: **Group**

Verify

Troubleshoot

There is no troubleshooting section for this document.