

Cloud Web安全：配置与PingFederate和ADFS的用户/组属性，曾经SAML。

目录

[简介](#)

[要求](#)

[配置](#)

[PingFed](#)

[ADFS](#)

[验证](#)

[故障排除](#)

[相关的思科支持社区讨论](#)

[简介](#)

本文描述如何配置PingFederate和ADFS (活动目录联盟的服务) IDP服务器发送用户/组详细信息到Cloud Web安全性服务为了granularly过滤器策略。

[要求](#)

思科建议您有基本的了解以下。

- 管理登录/访问对PingFed/ADFS服务器
- 知识如何导航PingFed/ADFS服务器
- 为了granularly能工作在HTTPS流量，必须为所有流量强制执行HTTPS检查

[配置](#)

请在步骤之下请跟随配置与PingFederate和ADFS的用户/组属性。

PingFed

在**属性下来源**>**用户查找**选项卡：

- 属性合同：**AUTHENTICATED_GROUPS**
来源：**LDAP**

值：**memberOf**
- 属性合同：**SAML_SUBJECT**
来源：**LDAP**

值：**sAMAccountName**

ADFS

在信任关系下>取决于当事人信任选项卡：

- LDAP属性合同：**SAM帐户NAME**
流出的声明类型LDAP：**命名ID**
- LDAP属性合同：**标记组**
流出的声明类型LDAP：**组**

验证

故障排除

没有本文的故障排除部分。