

# 配置ISE 2.1有PingFederate SAML SSO的赞助商门户

## 目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[流概述](#)

[配置](#)

[步骤1.准备ISE使用一个外部SAML标识供应商](#)

[步骤2.配置赞助商门户使用一个外部标识供应商](#)

[步骤3.配置PingFederate作为IdP处理ISE认证请求](#)

[步骤4.导入IdP元数据到ISE外部SAML IdP供应商配置文件](#)

[验证](#)

[故障排除](#)

[相关信息](#)

## 简介

本文描述如何配置有思科身份服务的Engine(ISE) 2.1一个PingFederate SAML服务器提供单个符号On(SSO)功能赞助用户。

## 先决条件

### 要求

Cisco 建议您了解以下主题：

- 思科身份服务引擎访客服务。
- 关于SAML SSO部署的基础知识。

### 使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科身份服务引擎版本2.1
- PingFederate从Ping标识的8.1.3.0服务器。
- Windows服务器2012与活动目录目录服务的R2。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络实际，请确保您了解所有命令潜在影响。

## 规则

参考[Cisco技术提示规则](#)关于文件规则的更多信息

## 流概述

安全断言标记语言(SAML)是交换的认证和授权数据一个基于XML的标准在安全域之间。

SAML规格定义了三个角色：首席(赞助商用户)，标识供应商(IdP) (Ping联合的服务器)和服务提供商(SP) (ISE)。在典型SAML SSO流，SP从IdP请求并且获取标识断言。凭此结果，ISE可进行政策决策，当IdP能包括在政策决策期间，ISE能使用的可配置属性。一旦最初的验证出现，不应该再提示用户输入凭证访问服务，只要断言会话是活跃的在IdP。

这是此用例的预计流：

1. 用户尝试登陆到赞助商门户通过启动已配置的赞助商门户的自定义完全合格的域名(FQDN)。
2. ISE验证，如果有一活动断言关联对此客户端浏览器会话通过发出快速重定向对IdP。如果没有激活的会话，IdP将强制执行用户登录。
3. IdP通过LDAP验证用户并且通过memberOf和电子邮件属性对ISE(SP)。
4. ISE处理IdP XML答复，并且基于memberOf属性和赞助商组配置用户将允许或拒绝(组成员匹配一已配置的赞助商组的状态检查)。
5. 会话生存时间在每解决方案将变化。在此用例，Ping Federate将配置与60分钟会话超时(如果没有从ISE的SSO登录请求在60分钟，在最初的验证，会话删除)后和480分钟会话最大值超时(即使IdP接收从ISE的不变SSO登录请求会话在8个小时将超时)的此用户的。一旦会话时间，新用户验证由IdP强制执行。
6. 当会话是活跃的时，赞助商用户应该能结束浏览器和回击到门户，无需输入凭证。

## 配置

以下部分讨论配置步骤集成与联合的Ping的ISE和如何启用赞助商门户的浏览器SSO。

**注意：**虽然多种选项和可能性存在，当您验证赞助商用户，不是所有的组合在本文描述。然而，此示例提供您必要的信息知道如何修改示例成您要达到的准确的配置。

### 步骤1.准备ISE使用外部SAML标识供应商

1. 在思科ISE，请导航对**Administration > 身份管理 > 外部标识来源 > SAML Id供应商**。
2. 单击添加
3. 在常规选项卡下，请输入Id运营商名称并且点击“**Save**”。配置的其余在需要从IdP导入的此部分的将依靠元数据。

### 步骤2.配置赞助商门户使用外部标识供应商

1. 导航对**工作区 > 访客访问 > 配置 > 赞助商门户**
2. 点击门户的**赞助商(默认)**或创建一个新的门户。
3. 在门户设置下请输入与此赞助商门户连接的自定义完全合格的域名(FQDN)。
4. 从**标识外部SAML IdP**以前定义的**来源顺序**挑选。
5. 验证流程图代表以下并且点击**保存**：

### 步骤3.配置PingFederate作为IdP处理ISE认证请求

1. 导航对ISE Administration >身份管理>外部标识来源> SAML Id供应商> PingFederate
2. 点击**服务提供商Info**选项并且点击**出口**
3. 保存并且抽出生成的压缩文件。包含的XML文件此处将在PingFederate时将使用，当创建配置文件。
4. 打开PingFederate admin门户(典型地<https://ip:9999/pingfederate/app>)。
5. 在IDP Configuration选项> SP Connections部分下请选择**创建新**。
6. 在**连接类型**下其次请单击
7. 在**连接选项**下其次请单击
8. 在**导入元数据**下，请选择**文件**，选择文件并且选择从ISE以前导出的XML文件。
9. 在**元数据摘要**下，其次请点击。
10. 在一般信息页，在**连接名**回车下名称(IE. ISEsponsorPortal)和**其次**单击。
11. 在**浏览器SSO**下请单击**配置浏览器SSO**和在**SAML配置文件**检查下这些选项并且其次单击：
12. 在**断言寿命**其次请单击
13. 在**断言创建**请单击**配置断言创建**
14. 在**标识映射**下请选择**标准**并且**其次**单击

## SP Connection | Browser SSO | Assertion Creation

Identity Mapping

Attribute Contract

Authentication Source Mapping

Identity mapping is the process in which users authenticated by the IdP are associated with a specific local account. This process may affect the way that the SP will look up and associate the user to a specific local account.



**STANDARD:** Send the SP a known attribute value as the name identifier. The

15. 在**属性合同**>请**延伸合同**回车**属性邮件**和**memberOf**并且单击**添加**。然后，单击**下一步**。

**注意：**这是重要一步，因为ISE依靠正确赞助商组映射的这些属性并且发电子邮件为正确通知功能是必要的。

16. 在**验证来源映射**下请点击**地图新建的适配器实例**。

17. 在**适配器实例**挑选**HTML表适配器**上。单击 **Next**。
18. 在**映射方法**下请选择第二个选项并且**其次单击**
19. 在**属性来源&用户查找**单击**添加属性来源**方框。
20. 在**数据存储**回车下说明，从**活动数据**然后挑选**存储**您的LDAP连接实例并且定义了什么类型的目录服务这是。如果没有配置的数据存储，请点击**Manage数据存储**添加新的实例。
21. 在**LDAP目录搜索**下请定义LDAP用户查找的**基础DN**在域并且**其次单击**。

**注意：**在LDAP用户查找期间，因为将定义基础DN这是重要。不正确地定义的基础DN将导致错误“在LDAP模式没找到的对象”。

22. 在**LDAP过滤器**下请添加字符串**sAMAccountName=\$ {username}**并且**其次单击**。

23. 在**属性合同实现**下请选择这些选项并且**其次单击**

24. 验证配置在**Summary**部分并且**点击完成**。

25. 返回在**属性来源&用户查找**其次单击。

26. 在**故障自动保险的属性来源**下**其次请单击**。

27. 在**属性合同实现**下请选择这些选项并且**其次单击**：

27. 总之验证配置部分并且**点击完成**。

28. 返回在**验证来源映射**其次单击。

29. 一旦配置验证在**执行的Summary**部分单击下。

30. 返回在**断言创建**其次单击。

31. 在**协议设置**下请单击**配置协议设置**。

这时应该有已经填充的3个条目。单击“下一步”

32. 在**SLO服务URL**下**其次请单击**

33. 在**允许的SAML捆绑**请不选定选项**人工制品**并且**其次用肥皂擦洗**并且单击。

34. 根据**签名策略**其次单击。

35. 根据**加密策略**其次单击。

36. 查看在**汇总页**的配置并且**点击完成**。

37. 返回在**浏览器SSO >协议设置**其次单击，验证配置并且**点击完成**。这将带来上一步**浏览器SSO**选项卡。单击 **Next**。

38. 在**凭证**下请单击**配置凭证**并且选择在IdP期间将用于的签署的证书ISE通信并且检查选项**包括证书在签名**。然后，单击**下一步**。

**注意：**如果没有配置的证书，请单击**管理证书**并且按照提示符生成将使用的自签名证书签署IdP到ISE通信。

39. 验证配置在**汇总**页下并且单击**完成**。

40. 返回在**凭证**选项卡**其次**单击。

41. 在**激活&摘要**下精选在**连接状态激活**，请验证配置的其余并且单击**“Save”**。

#### 步骤4.导入IdP元数据到ISE外部SAML IdP供应商配置文件

1. 在PingFederate管理控制台下，请导航对**服务器配置>Administrative功能>元数据出口**，如果服务器为多个角色配置(IdP和SP)选择**我是标识Provider(IdP)**的选项。单击**“下一步”**

2. 在**元数据**模式下请选择**"Select Information to Include In Metadata Manually"**。单击 **Next**。

3. 在**协议**下**其次**请单击。

4. 在**属性合同**下**其次**请单击。

5. 在**签署的密钥**下请选择在连接配置文件以前配置的证书。单击 **Next**。

6. 在**元数据签字**下请选择签署的证书，并且检查在**关键信息元素**包括此证书的**公共密钥**。单击 **Next**。

7. 在**XML加密证明**下**其次**请单击。选项强制执行此处加密是至网络Admin。

8. 在**Summary**部分下请点击出口**“Save”**生成的元数据文件然后单击**完成**。

9. 在ISE下，请导航对**Administration >身份管理>外部标识来源> SAML Id供应商> PingFederate**。

10. 点击**标识供应商>Click浏览的设置**并且继续导入从Pingfederate元数据出口操作保存的元数据。

11. 选择**组**选项卡，并且在**组成员属性**下请添加**memberOf**然后单击**添加**

12. 以在**断言名义**请添加IdP应该返回上一步的**辨别名称**，当**memberOf**属性是获取的表LDAP认证时。此组与赞助商组将连接。

一旦添加DN，并且**“请命名在ISE”**说明点击**OK**键。

13. 选择**Attributes**选项并且单击**添加**。在此步骤我们将添加属性**“邮件”**。这在SAML验证包含;从IdP通过的结果(根据该用户对象的电子邮件属性在活动目录)。

**注意：**此步骤是重要，虽然ISE应该能处理与赞助商的会话连接的电子邮件能映射在待定状态的所有帐户从赛弗注册的流。否则，因为是**“人被访问的”**电子邮件不会被映射给一有效赞助商会话，帐户将留在一柔软状态。对电子邮件通知是重要也报价。

14. 在**高级**选项卡。下请选择以下设置：

**注意：**此部分在注销请求将指示ISE包括电子邮件属性到LDAP服务器。当赞助商从门户时，用户手册注销这是重要。

15. 单击 **Save**。

16. 在此步骤管理员将映射IdP检索的活动目录组对赞助商组。导航对**工作区>访客访问>配置>赞助商Groups> ALL\_ACCOUNTS** (或请选择适合的组)。 单击**成员**并且选择**PingFederate** : **分组**我们映射在上一个步骤并且添加它到所选的用户用户组列。然后单击 **OK**。

17. 当赛弗注册流配置，帐户将是等待批准。在这种情况下，因为验证对象电子邮件地址的简单的方法是AD和转接对在ISE的赞助商标识通过IdP服务器使用**邮件属性**，请选择"Approve and view requests from self-registered guests"并且选择"Only pending accounts assigned to this sponsor"。

18. 单击 **Save**。这停止在ISE的配置。

## 验证

1. 使用已配置的自定义FQDN，启动赞助商门户。ISE应该重定向用户到PingFederate用户认证门户。

2. 回车活动目录凭证和点击的符号。IdP登录屏幕将重定向用户对在艾斯的赞助商门户的初始AUP。

这时赞助商用户应该有对门户的完全权限。

3. 验证单个符号。当使用时“**门户测验URL**”功能ISE应该每次请求赞助商凭证，如果SSO没有配置。

启动有门户测验URL链路的赞助商门户。ISE赞助商URL将迅速换成IdP URL验证会话状态，并且，一旦会话标记被确认客户端重定向回到赞助商门户，不用输入凭证需要。

4. 验证电子邮件属性从活动目录对象正确地通过到IdP对ISE。测试的简便的方法是通过创建在门户的赞助商的一新帐户和选择**通知**选项。如果电子邮件正确地获取将看起来在赞助商的**电子邮件地址**字段下。

5. 验证**注销**功能。这是关键在集成验证赞助商注销触发在标识服务器端将终止的令牌的会话。从门户的赞助商签字并且确保，当下次用户设法访问赞助商门户，将重定向回到IdP验证屏幕。

## 故障排除

所有SAML验证处理将是登陆的ISE侧在**ise-psc.log**下。有一个专用的组件(SAML)在**Administration >记录日志>调试日志Configuration**>下选择节点有问题的>集SAML组件对**调试级别**。

我们能通过CLI访问ISE，并且发出“show logging应用程序ise-psc.log尾标”和监控SAML事件请居住，或者我们能下载进一步分析的**ise-psc.log**在**操作下>排除故障>下载日志>选择ISE节点>调试日志选项卡>点击ise-psc.log**下载日志。

典型地最初的验证日志如下所示：

```
2016-06-13 10:18:58,560 DEBUG [http-bio-14.36.157.210-8443-exec-7][[]
```

```
cpm.saml.framework.impl.SAMLFacadeImpl -::::- SAML request -  
spUrlToReturnTo:https://torsponsor21.rtpaaa.net:8443/sponsorportal/SSOLoginResponse.action
```

```
2016-06-13 08:39:36,925 DEBUG [http-bio-14.36.157.210-8443-exec-7][]  
cpm.saml.framework.impl.SAMLFacadeImpl -::::- SAML Response:  
statusCode:urn:oasis:names:tc:SAML:2.0:status:Success
```

```
2016-06-13 08:39:36,925 DEBUG [http-bio-14.36.157.210-8443-exec-7][]  
cpm.saml.framework.impl.SAMLAttributesParser -::::- [parseAttributes] Found attribute name :  
mail
```

```
2016-06-13 08:39:36,925 DEBUG [http-bio-14.36.157.210-8443-exec-7][]  
cpm.saml.framework.impl.SAMLAttributesParser -::::- [parseAttributes] Delimiter not configured,  
Attribute=<mail> add value=<antontor@rtpaaa.net>
```

```
2016-06-13 08:39:36,925 DEBUG [http-bio-14.36.157.210-8443-exec-7][]  
cpm.saml.framework.impl.SAMLAttributesParser -::::- [parseAttributes] Found attribute name :  
memberOf
```

```
2016-06-13 08:39:36,925 DEBUG [http-bio-14.36.157.210-8443-exec-7][]  
cpm.saml.framework.impl.SAMLAttributesParser -::::- [parseAttributes] Delimiter not configured,  
Attribute=<memberOf> add value=<CN=TOR,DC=rtpaaa,DC=net>
```

在首次登录事件以后，每次用户访问赞助商门户将看到ISE获取断言信息的我们验证标记是活跃的。  
结果如下所示：

```
2016-06-13 10:18:58,560 DEBUG [http-bio-14.36.157.210-8443-exec-7][]  
cpm.saml.framework.impl.SAMLFacadeImpl -::::- SAML request -  
spUrlToReturnTo:https://torsponsor21.rtpaaa.net:8443/sponsorportal/SSOLoginResponse.action
```

```
2016-06-13 08:39:36,925 DEBUG [http-bio-14.36.157.210-8443-exec-7][]  
cpm.saml.framework.impl.SAMLFacadeImpl -::::- SAML Response:  
statusCode:urn:oasis:names:tc:SAML:2.0:status:Success
```

```
2016-06-13 08:39:36,925 DEBUG [http-bio-14.36.157.210-8443-exec-7][]  
cpm.saml.framework.impl.SAMLAttributesParser -::::- [parseAttributes] Found attribute name :  
mail
```

```
2016-06-13 08:39:36,925 DEBUG [http-bio-14.36.157.210-8443-exec-7][]  
cpm.saml.framework.impl.SAMLAttributesParser -::::- [parseAttributes] Delimiter not configured,  
Attribute=<mail> add value=<antontor@rtpaaa.net>
```

```
2016-06-13 08:39:36,925 DEBUG [http-bio-14.36.157.210-8443-exec-7][]  
cpm.saml.framework.impl.SAMLAttributesParser -::::- [parseAttributes] Found attribute name :  
memberOf
```

```
2016-06-13 08:39:36,925 DEBUG [http-bio-14.36.157.210-8443-exec-7][]  
cpm.saml.framework.impl.SAMLAttributesParser -::::- [parseAttributes] Delimiter not configured,  
Attribute=<memberOf> add value=<CN=TOR,DC=rtpaaa,DC=net>
```

## 相关信息

[思科身份服务引擎的版本注释，版本2.1](#)

[思科身份服务引擎管理员指南，版本2.1](#)