

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[流概述](#)

[此用例的预计流：](#)

[配置](#)

[步骤1.准备ISE使用一个外部SAML标识供应商](#)

[步骤2.配置访客门户使用一个外部标识供应商](#)

[步骤3.配置PingFederate作为ISE访客门户的一个标识供应商](#)

[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Cisco身份服务Engine(ISE)版本2.1到访客门户用户的provoide单个符号On(SSO)功能通过安全断言标注Language(SAML)。

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服务器作为SAML标识Provider(IdP)

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，请确保您了解应用的所有配置潜在影响。

规则

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

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(来宾用户)，标识供应商[IdP] (IPing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能包括可配置属性ISE能使用(即关联的组和电子邮件地址对AD对象)。

此用例的预计流：

1. WLC或接入交换机为一个典型的中央Web验证(CWA)流配置。

提示：请找出CWA的配置示例流在**相关信息部分**在条款的底部

2. 客户端连接，并且会话得到验证ISE。网络访问Device(NAD)运用ISE (AVPs)返回的重定向属性值对(url-redirect-acl和url重新定向)。

3. 客户端打开浏览器，生成HTTP或HTTPS流量并且重新定向对ISE ?s访客门户。

4. 一旦在门户客户端能输入以前已分配访客凭证(**赞助商创建**)，赛弗提供一个新的访客帐户或使用在功能将提供单个符号通过SAML的其AD凭证登陆(**员工洛金**)。

5. 一旦用户选择选项？员工洛金？如果有一活动断言关联对此客户端， ISE验证？s浏览器会话gainst IdP。如果没有激活的会话， IdP将强制执行用户登录。在此步骤用户在IdP门户将被提示直接地进入AD凭证。

6. IdP通过LDAP验证用户，并且创建将坚持运行在可配置时间的一新的断言。

注意：联合默认情况下的Ping将应用**会话超时**60分钟(这意味着，如果没有从ISE的SSO登录请求在60分钟之内在最初的验证以后会话删除)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。

只要断言会话是活跃的，员工将体验SSO，当usin gthe访客门户。一旦会话时间新用户验证将由IdP强制执行。

配置

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

注意：虽然多种选项和可能性存在，当您验证来宾用户，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**General**选项卡下请输入**Id运营商名称**。单击**“Save”**。配置的其余在需要从在最新步骤的IdP导入的此部分的将依靠元数据。

步骤2.配置访客门户使用外部标识供应商

1. 导航对**工作区>访客访问>配置>访客门户**

2. 创建一新门户并且选择**赛弗注册的访客门户**。

注意：这不会用户将体验的主要门户，但是将呼应以IdP验证会话状态的subportal。我将呼叫此门户SSOSubPortal。

3. 展开**门户设置**并且选择**认证方法的PingFederate**。

4. 从**标识来源顺序**以前挑选外部SAML IdP defined(PingFederate)。

5. 扩展**Acceptable Use Policy(AUP)**和**POST洛金班纳页定位**部分并且禁用两个。

门户流：

6. 保存更改。

7. 使用**赛弗注册的访客门户**选项，去上一步访客门户并且创建新的。

注意：这主要的门户可视给客户端。主要的门户将使用SSOSubportal作为ISE和IdP之间的一个接口。我们将命名此门户PrimaryPortal。

8.展开**洛金页定位**并且选择以前创建的**SSOSubPortal**下？允许将用于登录以下标识供应商访客门户？。

9. 展开**可接受的使用规定AUP**和**POST洛金班纳页定位**并且不选定他们。

这时门户流如下所示：

10. 单击**门户自定义>页>洛金**。我们应该当前有选项定制**代替洛金选项**(图标、文本等等)。

注意：注意那在右侧，在门户预览下，另外的Login选项可视。

11. 单击 **Save**。

现在两个门户应该出现在访客门户列表下。

步骤3.配置PingFederate作为ISE访客门户的标识供应商

1. 在ISE，请导航对**Administration >身份管理>外部标识来源> SAML Id供应商> PingFederate**并且单击**服务提供商资讯台**

2. 在**出口服务提供商资讯台**下请点击**出口**

3. 保存并且抽出生成的压缩文件。包含的XML文件此处在下步骤时的PingFederate将使用，当创建配置文件。

注意：从这时起，我们将报道PingFederate配置。此配置将是相同的为多种解决方案类似赞助商门户、MyDevices和BYOD门户。(那些解决方案在此条款没有报道)

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. Under元数据摘要，其次点击。

10. On一般信息页，在连接名回车下名称(IE。ISEGuestWebAuth)和其次单击。

11. 在浏览器SSO下请单击配置浏览器SSO和在SAML配置文件检查下以下选项并且其次单击：

12. On断言寿命其次单击

13. On断言创建单击配置断言创建

14. Under标识映射选择标准并且其次单击

15. 在属性合同>延伸合同请输入属性邮件，并且memberOfand单击添加。然后其次请单击

配置此选项将允许标识供应商通过MemberOf和给活动目录提供的属性发电子邮件给ISE，在政策决策期间，ISE能使用以后作为情况。

16. Under验证来源映射点击地图新建的适配器实例。

17. On适配器实例挑选HTML表适配器。单击“下一步”

18. 在映射下方法选择第二个选项下来并且其次单击：

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，请单击管理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将导致在LDAP模式没找到的对象。

22. Under LDAP过滤器添加字符串sAMAccountName=\$ {username}并且其次单击。

23. 在**属性合同实现**下请选择以下选项并且**其次单击**。
24. 验证配置在Summary部分并且**单击完成**。
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**：
28. 总之验证配置部分并且**单击完成**。
29. 返回在**验证来源映射**其次单击。
30. 一旦配置验证在**汇总页**下**请点击完成**。
31. 返回在**断言创建**其次单击。
32. 在**协议设置clickNext**下请**配置协议设置**。这时应该有已经填充的2个条目。单击 **Next**。
33. 在SLO服务下URL**其次单击**
34. 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**。
35. 根据签名策略**其次请单击**。
36. 根据加密策略**其次请单击**。
37. 查看在**汇总页**的配置并且**单击完成**。
38. 返回在**浏览器SSO >协议设置**其次单击，**验证配置并且单击完成**。
39. 这将带来我们回到**浏览器SSO选项卡**。**其次单击**。
40. 在**凭证**下**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**。

41. 验证配置在**汇总页**下并且**单击完成**。
42. 返回在**凭证选项卡**其次单击。
43. 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**单击完成**。

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)请选择**我是标识Provider(IdP)**的选项。单击“**下一步**”
2. 在**精选元数据**的模式下？**选择信息手工包括在元数据？**。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**下选择签署的证书，并且检查**包括此证书？在关键信息元素的s公共密钥**。单击 **Next**。
7. 在**XML加密证明**下**其次**请单击。

注意：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**。保存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**标识供应商设置 > 浏览**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，在**组成员属性**下请添加**memberOf**然后单击**添加**

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LADP验证时。在这种情况下组配置与突岩的赞助商组连接，并且此组的DN如下：

一旦添加DN和？在ISE的名称？说明点击**OK**键。

12. 选择**Attributes**选项并且单击**添加**。

在此步骤我们将添加属性？**邮件**？那在从根据Ping的IdP通过的SAML标记包含？在LDAP的s查询，它应该包含该对象的电子邮件属性。

注意：步骤11和12保证ISE将收到AD对象电子邮件，并且MemberOf属性通过IdP登陆操作。

验证

1. 启动访客门户使用门户测验URL或通过跟随CWA请流。用户将有选项输入访客凭证，创建他们自己的帐户和员工洛金。
2. 点击**员工洛金**。因为没有激活的会话用户将重定向到IdP登录门户。
3. 回车AD凭证和点击**符号**。
4. IdP登录屏幕将重定向用户对访客门户成功页。
5. 这时，在用户来上一步到访客门户并且选择时候？**员工洛金**？只要会话是活跃的在IdP，他们在网络将允许。

故障排除

SAMLise-psc.log(SAML)**Administration >>Configuration>>SAML**

CLIISEshow loggingise-psc.logSAMLise-psc.log>>>**ISE>>ise-psc.log**

相关信息

- [与思科WLC和ISE配置示例的中央Web验证。](#)
- [与交换机和身份服务引擎配置示例的中央Web验证。](#)
- [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](#)