为ESA和SMA管理配置SAML SSO外部身份验证

目录

简介

本文档介绍如何为ESA和SMA系统管理配置SAML 2.0 SSO外部身份验证。

环境

- 产品：邮件安全设备(ESA)、安全管理设备(SMA)
- 适用于：ESA和SMA系统管理
- 群集行为：在机器级别配置服务提供商(SP)和IdP配置文件；在集群级别配置外部身份验证映射。

先决条件

- 对ESA/SMA Web界面的管理访问
- X.509证书和私钥以PKCS #12(PFX)或PEM格式（自签名或CA签名）提供
- 访问第三方身份提供程序(IdP)应用及其SAML元数据/SSO URL

预配置核对表

- 验证管理员用于访问设备的管理接口主机名/FQDN;确认断言消费者服务(ACS)URL与该主机名匹配。
- 如果设备在集群中，计划在启用SAML外部身份验证之前为每个成员配置计算机级别的SAML。
- 确定IdP是否要求每台设备使用单独的应用程序或领域。
- 确认所需的证书和密钥可用。
- 确认IdP发送ESA/SMA角色映射所需的组或角色属性。

警告：本文档不适用于最终用户隔离(EUQ)SAML SSO。

背景信息

- Cisco TAC不为第三方IdP配置提供技术支持。为通用IdP提供了示例配置参考。

SSO SAML IdPs

- Duo Access Gateway(DAG)增加了双因素身份验证，通过SAML 2.0联合完成常用的云服务。
- Active Directory联合身份验证服务(ADFS) — 使用ADFS 2、3、4、Azure Active Directory(Azure AD)、SecureAUTH和PingFederate进行测试
- 如果IdP在SAML 2.0单点登录框架中支持其他双因素身份验证，则可以使用其他双因素身份验证。
- Okta支持使用支持服务的IdP进行身份验证。

将ESA/SMA配置为服务提供商

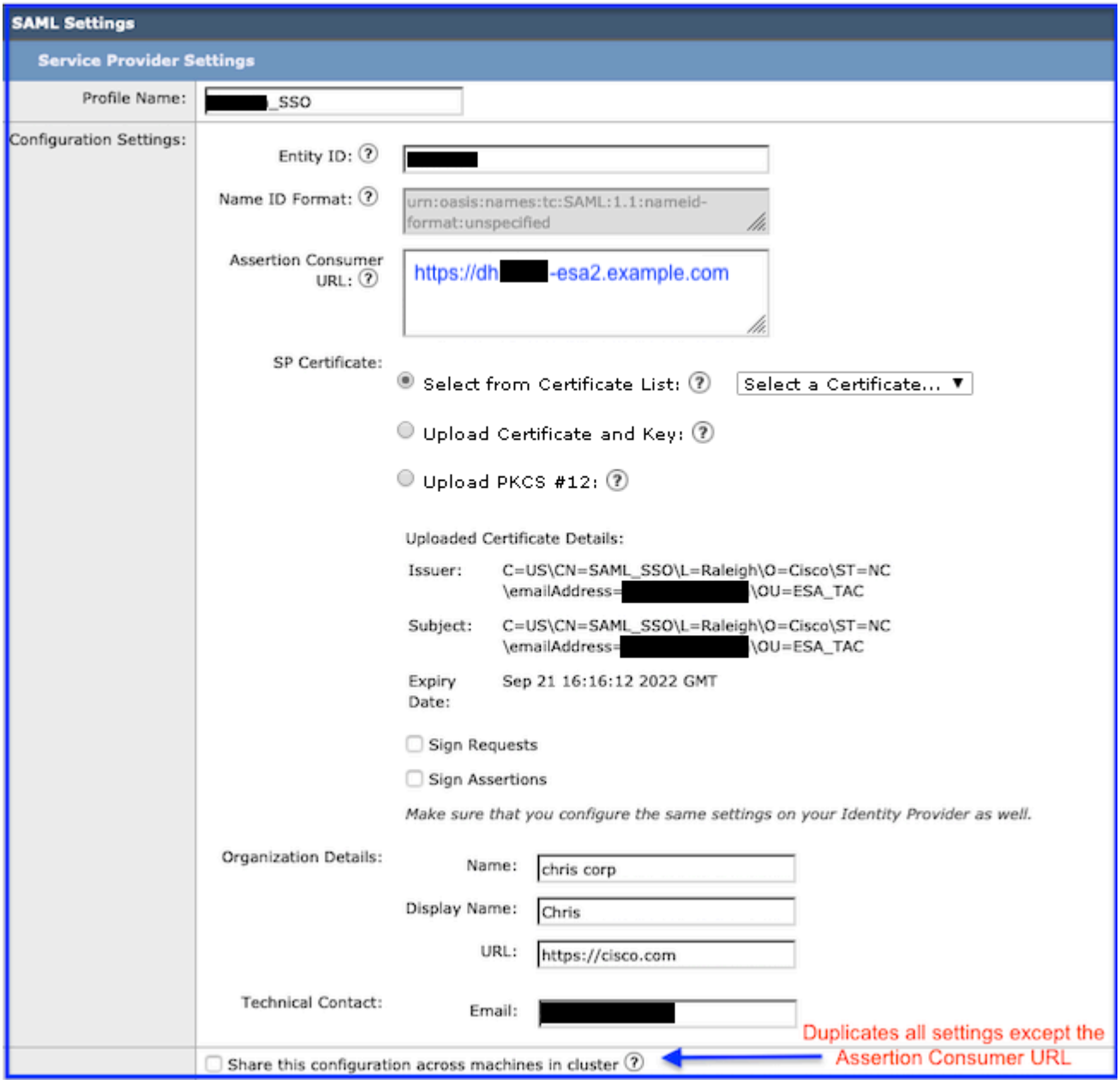
导航到系统管理> SAML >（机器级别）>添加服务提供商。

注意：在启用SAML之前，集群中的ESA需要对集群的所有成员进行计算机级配置。

- 如果选中页面底部的选项在集群中的计算机间共享此配置，则以下条件适用：
  - 除断言使用者URL外，所有字段都会复制到集群成员。
  - Assertion Consumer URL会自动填充作为ACS的管理接口的主机名。

- 使用备用主机名访问主机的环境需要手动配置每台主机，例如CES托管的设备。
- 配置文件名称:用于在ESA或SMA接口中标记SP实例的名称。
- 实体ID:IdP看到的用于SP实例的名称。此名称是IdP用于表示SP的标签。这可以是任何名称，例如ESA_SP或ESA_SSO。
- 名称ID格式:不可配置的字段。
- 断言使用者URL或断言使用者服务(ACS):IdP用于与此ESA/SMA主机通信的URL。
- SP证书:
    - Format:PFX/PKCS12或PEM格式的X.509公共/专用证书。
    - 选项 1：从证书列表中选择:从Network > Certificates内的ESA上已创建的证书中选择。
    - 选项 2：上传证书和密钥:上传PEM格式的证书和密钥。
    - 选项 3：上传PKCS #12:上传PKCS #12文件。
    - 可选：在ESA/SMA上为SAML单点登录创建自签名证书。
    - 如果需要，可对私钥进行密码保护。

注意：如果使用PEM格式的证书，请将每个证书和私钥保存在不同的文件中。



"服务提供程序设置"页

"服务提供程序设置"页

- 签名请求:用于签署发送到IdP的ESA/SMA SAML通信的选项。
- 签名断言:选项要求IdP对发送到ESA/SMA的声明进行签名。
- 组织详情:可以使用适当的公司数据填充。
- 提交并提交更改以保留设置。
- 从SAML配置页面下载SP元数据。

配置身份提供程序(IdP)以与ESA/SMA设备配合使用

注意：某些IdP要求每个ESA有单独的应用程序或领域。(例如：DUO)

这些链接在发布时提供多个IdP的示例配置。
Cisco TAC不为第三方产品提供技术支持。这些示例作为参考提供。

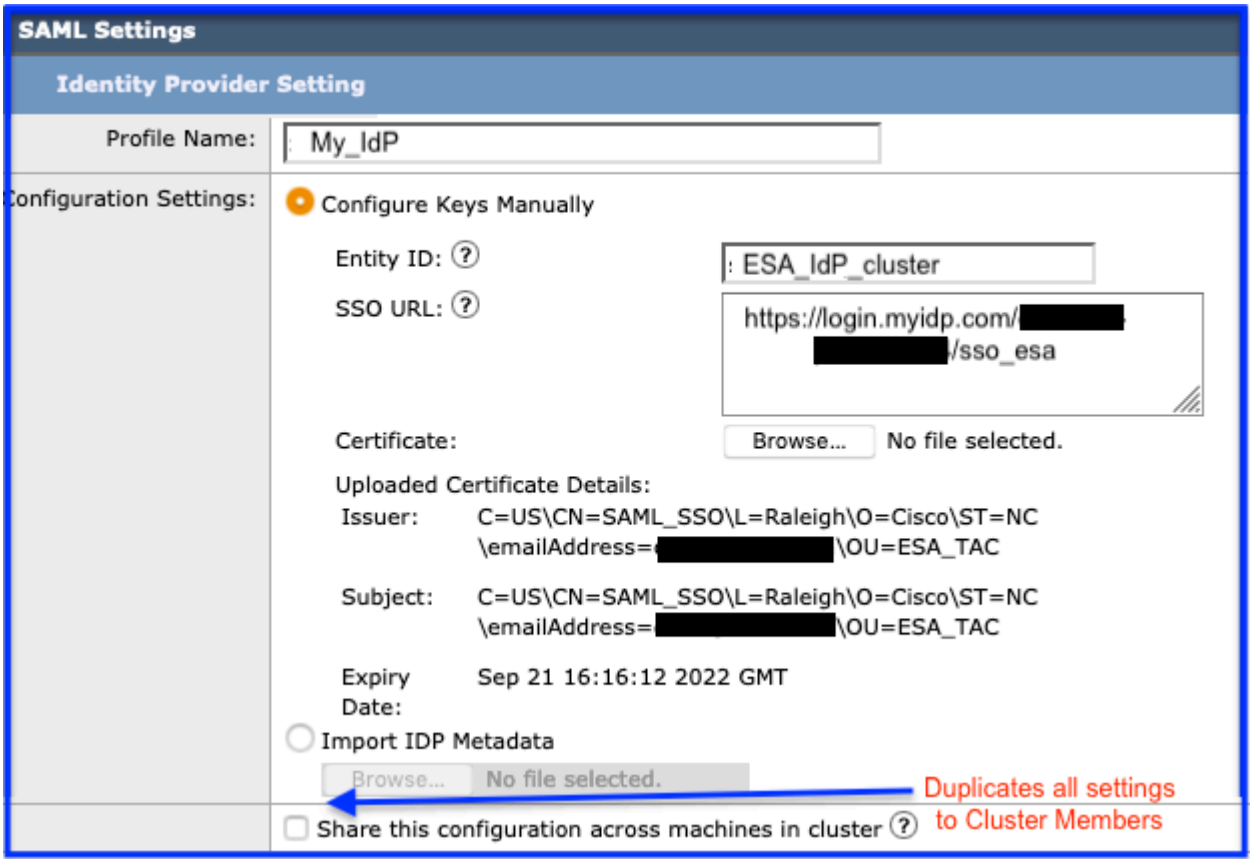
在ESA/SMA上配置IDP设置

1.定位至系统管理> SAML。

2.选择添加身份提供程序。

- 有两个可用选项：
- 导入IdP元数据
- 手动配置密钥:
  - 实体ID:可以是用于标识IdP的任何值
  - SSO URL:SP向其发送SAML身份验证请求的URL
  - 将私钥和公用证书上传到不同的文件中

3.在集群中的计算机之间共享此配置，以在集群中的所有ESA之间复制配置：

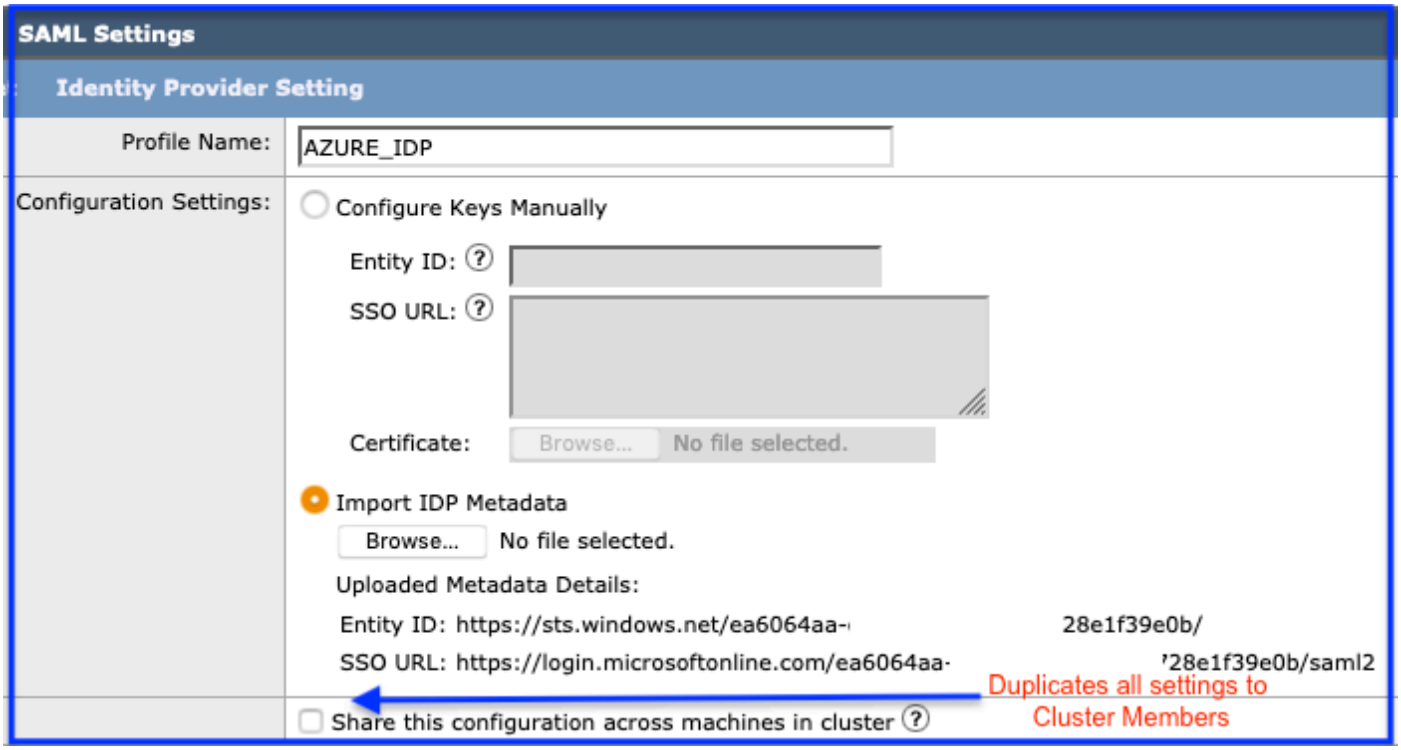


手动输入IdP内容

手动输入IdP内容

4.从IdP上传元数据

- 选择导入IdP元数据。
- 浏览到从IdP保存的元数据文件并保存配置。
- 如果应用于部署，则可使用在群集中计算机间共享此配置的选项。



从Idp上传元数据

从Idp上传元数据

在ESA/SMA上使用SAML启用外部身份验证

与LDAP外部身份验证类似，SAML单点登录需要映射将组分配到管理角色。

1.依次导航到系统管理(System Administration)>用户（集群级别）>外部身份验证(External Authentication)>启用(Enable)。

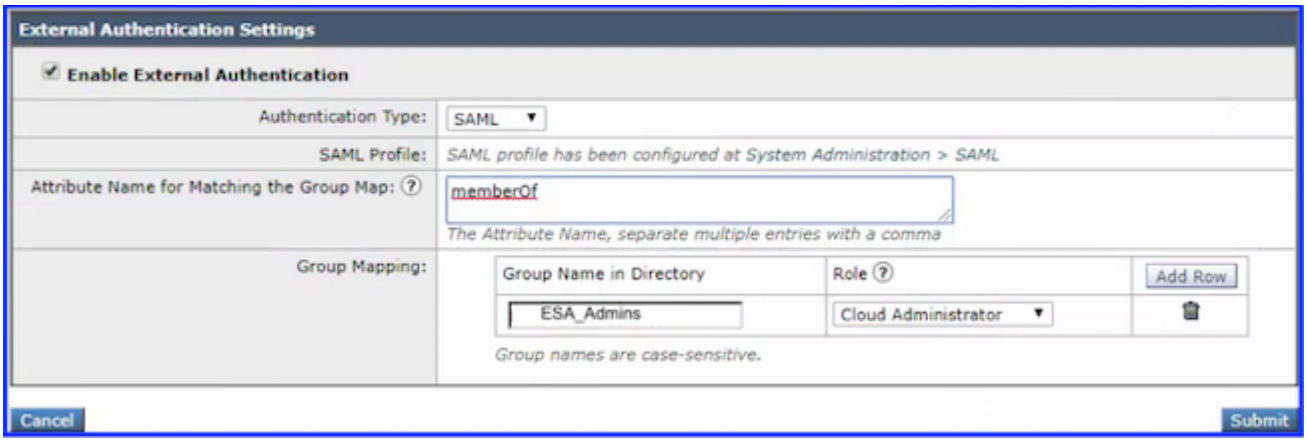
2.选择Authentication Type:SAML。

3.匹配名称映射的属性名称（可选）:输入属性名称以从组映射中搜索。

注意：属性名称取决于为SAML响应中中继的身份提供程序配置的属性。设备根据Group Mapping字段中配置的属性在SAML响应中搜索指定属性名称的匹配条目。如果未配置此字段，设备会根据已配置的Group Mapping字段搜索SAML响应中存在的所有属性。

4.根据预定义或自定义用户角色，输入在SAML目录中定义的组名属性。

- 组映射字段必须包含组属性。可以添加Unspecified Groups属性对SAML断言或响应进行身份验证。



外部身份验证设置

外部身份验证设置

5.提交并确认更改。

配置成功后，登录页面底部会显示一个新链接。ESA/SMA登录页面显示使用单点登录链接，该链接将管理员重定向到公司身份提供程序(IdP)。

选择后，管理员将重定向到公司SAML登录页面。

使用单点登录链接将重定向到SAML

使用单点登录链接重定向到SAML

故障排除

使用这些指示符可确定问题是否与设备配置或IdP配置相关。

登录页面上未显示SSO重定向链接（“使用单一登录”）

确认已配置System Administration > Users > External Authentication > SAML。

重定向返回带有“单点登录身份验证失败！”的ESA/SMA登录页面请联系您的管理员。”

Error:“单点登录身份验证失败！请联系您的管理员。”

- 身份验证在IdP处失败。
  - 这表示该配置的工作状态已达到Single Sign-On authentication页面和提交凭据的程度。
  - 此故障通常是由于IdP配置，并且需要额外的IdP设置验证。

重定向返回带有“授权失败！”的ESA/SMA登录页面请联系您的管理员。”

Error:“授权失败！请联系您的管理员。”

- 身份验证通过，但在ESA/SMA上授权失败。
  - 重点介绍Users > External Authentication > SAML中的设置。
    - Attribute Name、Group Name和Group Mapping。

相关信息

- 思科邮件安全设备 — 用户指南
- 思科内容安全管理设备 — 用户指南
- 思科网络安全 — 用户指南

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。