

单点登录系统



实施指南

单点登录

本手册包含以下章节：

- [单点登录概述](#)
- [在 SiteCatalyst 中配置单点登录](#)
- [关于配置身份提供者](#)

单点登录概述

Omniure SiteCatalyst 可让您使用单点登录方法访问 Web 数据。这种方法使用方便，您的用户无需另外安装登录系统，即可访问 SiteCatalyst。这给您提供了以下独一无二的好处：

- 用户无需再另外记住 SiteCatalyst 应用程序的密码，省去为找回忘记的密码所耗费的时间。
- 增强了对重要业务数据的控制，且管理更加方便安全，这是因为公司的网络密码策略控制对 SiteCatalyst 的访问。

单点登录有以下两种方式：

- 在“SiteCatalyst”登录屏幕使用单点登录功能。
- 您可从公司内部网创建至 SiteCatalyst 的链接，这样，登录至该内部网的用户可以直接访问 SiteCatalyst。

单点登录包括与公司内部网络集成的身份提供者服务器。此服务器基于网络，可以验证公司网络以外的系统（如 SiteCatalyst）发出的登录请求。当 SiteCatalyst 收到单点登录访问请求时，它将访问身份提供者服务器以验证该请求。身份提供者服务器将确认此用户是否有权访问您的网络。

单点登录无需专门的密码，但这并不影响其安全性。该方法使用密钥对加密，从而确保用户访问正确的身份提供者，杜绝其它身份提供者的虚假验证。您还可以将自己的身份提供者配置为使用主体确认，以此验证请求者。

面向受众

使用此手册前，用户应先熟悉 XML。了解 SAML 和数字签名知识将有助于此操作。

在 SiteCatalyst 中配置单点登录

您可从 SiteCatalyst 中的管理控制台配置单点登录。尝试配置单点登录前，请确保您已了解以下信息：

- 身份提供者的 URL。
- 用于验证身份提供者的公钥和私钥的存储位置。（如果没有密钥对，SiteCatalyst 将为您生成密钥对。然后，您便可以从 SiteCatalyst 应用程序下载此密钥对。）

配置 SiteCatalyst 进行单点登录

1. 在 SiteCatalyst 的欢迎屏幕中，单击**管理**。
2. 单击**管理控制台 > 公司**。
3. 单击**单点登录**。

图 2.1: 单点登录配置

公司设置

主页 安全性 技术支持 公告 Web 服务 P3P 政策 **单点登录** 待定操作 联合品牌

管理单点登录服务

单点登录服务向贵公司提供如下功能：使用 SiteCatalyst 用户的 Intranet 登录验证信息，通过您自己的 Intranet 登录门户验证这些用户的身份。

下载文档

启用单点登录服务 *注意：必须先单击“保存更改”，SSO 才能充分已启用*

配置单点登录

身份验证 URL
 请提供将通过 Omniture 门户的登录尝试重定向到的 URL，以进行身份验证。

密钥生成
 您可以选择由 Omniture 生成证书公钥和私钥，也可以选择自行生成后将公钥提供给 Omniture。

注意：如果生成密钥或上载密钥，将删除以前保存的所有公钥和私钥。

由 Omniture 生成私钥和公钥对

上载我用 Base 64 编码的公钥

保存我当前的现有密钥。

4. 选中**启用单点登录服务**。
5. 在**验证 URL** 字段中键入身份提供者的 URL。
6. 选择下列选项之一：
 - a. **Omniture 生成公钥和私钥**。如果当前没有密钥对，请选择此选项创建密钥对。然后使用**下载当前公钥**和**下载当前私钥**下载密钥。在身份提供者进行验证时，SiteCatalyst 使用公钥，您本人使用私钥。
 - b. **上载我用 Base 64 编码的公钥**。如果已有所需的密钥对，您可以使用此选项。单击**浏览**从计算机中查找公钥并上载。
 - c. **保留现有的密钥**。如果不希望对 SiteCatalyst 当前使用的密钥对做任何更改，但需执行其它更改，请使用此选项。
7. 单击**保存更改**。

关于配置身份提供者

您可以从多个供应商处购买身份提供者硬件和软件，也可以从互联网下载免费软件并安装在服务器上。供应商文档将向您介绍如何正确安装与配置身份提供者。要实现单点登录，您需了解以下配置设置：

- 身份提供者必须配置为使用 SAML 2.0。
- 断言响应必须包含私钥。针对单点登录配置 SiteCatalyst 时，必须向 SiteCatalyst 提供用于验证身份提供者的公钥。
- 必须使用 SHA1 创建密钥。
- 摘要和签名必须为 64 位编码。
- 必须是 RSA 密钥。
- 断言使用的 XML 代码必须为单个字符串、64 位编码，并具有“SAMLRequest”字样。有关正确格式的 XML 代码示例，请参阅第 5 页的“代码示例”。

关于主体确认

此外，设置身份提供者时，必须配置为按主体确认，以确保请求是来自有效用户而非虚假请求。您可以在 Web 浏览器请求内使用任何设置方法来完成配置。这使您可完全自主地确定组织验证策略的安全级别。可用方法包括但不限于：

- 使用 Cookie
- 验证 Windows 域
- 强制网络登录
- 通过 MAC 或 IP 地址过滤

代码示例

如上文所述，断言使用的 XML 代码必须为单个字符串、64 位编码，并具有“SAMLRequest”字样。以下是单个字符串的 XML 格式。您可以将此代码复制为自己的 XML 代码模板。斜体文本的具体内容取决于您所在的环境。

```
<Assertion ID="e228a15f04aa175d8d8c0cad9e0e820d4951bb1cfb" IssueInstant="2007-03-20T20:36:11Z" Version="2.0"
xmlns="urn:oasis:names:tc:SAML:2.0:assertion"><Issuer>ACME, Inc</
Issuer><ds:Signature xmlns:ds="http://www.w3.org/2000/09/
xmldsig#"><ds:SignedInfo><ds:SignatureMethod Algorithm="http://www.w3.org/2000/
09/xmldsig#rsa-sha1"/><ds:Reference
URI="#e228a15f04aa175d8d8c0cad9e0e820d4951bb1cfb "><ds:Transforms><ds:Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/></
ds:Transforms><ds:DigestMethod Algorithm="http://www.w3.org/2000/09/
xmldsig#sha1"/
><ds:DigestValue>ZWJmMTkyNWQ5ZDRjMjg2MjIwODc2M2ZkMzM3ZjkwZDA0Yjc1M2UxOQ==</
ds:DigestValue></ds:Reference></ds:SignedInfo>
<ds:SignatureValue>2vzXbYrt dm2s0y8JIBnRJYpPbQvMouEmYRGj8MxVrBYtY7P9kAYlSyucV/
lj8BOgAkWLACjK+p57/N6LOaXFZj/mQW3Qt8ClaLmNQTCPFxVR+WHPU+juSaludosPm5JRXe+/
OmoHNxQnTAmvr/JlzVPhdcm7N9aiiY5c24Zh1Q8=</ds:SignatureValue></
ds:Signature><Subject><NameID>john_doe</NameID><SubjectConfirmation
Method="urn:oasis:names:tc:SAML:2.0:cm:sender-vouches"/></Subject><Conditions
NotBefore="2007-03-20T20:36:11Z" NotOnOrAfter="2007-03-
20T20:41:11Z"><AudienceRestriction><Audience>https://www2.dev.omniture.com/
```

```
login.html?pid=sc</Audience></AudienceRestriction></Conditions><AttributeStatement><Attribute Name="login_version"><AttributeValue xsi:type="xs:string">sc13_5</AttributeValue></Attribute></AttributeStatement></Assertion>
```

以下为标准格式的代码，以供参考：

```
<Assertion ID="e228a15f04aa175d8d8c0cad9e0e820d4951bb1cfb"
IssueInstant="2007-03-20T20:36:11Z" Version="2.0"
xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
<Issuer>ACME, Inc.</Issuer>
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:SignedInfo>
<ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
<ds:Reference URI="#e228a15f04aa175d8d8c0cad9e0e820d4951bb1cfb">
<ds:Transforms>
<ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"/>
</ds:Transforms>
<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<ds:DigestValue>
ZWJmMTkyNWQ5ZDRjMjg2MjIwODc2M2ZkMzM3ZjkwZDA0Yjc1M2UxOQ==
</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue>
2vzXbYrtdm2s0y8JIBnRJYpPbQvMouEmYRGj8MxVrBYtY7P9kAYlSyucV/lj8BOgAkWLaCjK+p57/
N6LOaXFZj/mQW3Qt8ClaLmNQTCPFxVR+WHPU+juSaludosPm5JRXe+/OmoHNxQnTAMvr/
JlzVPhdcm7N9aiiY5c24Zh1Q8=
</ds:SignatureValue>
</ds:Signature>
<Subject>
<NameID>john_doe</NameID>
<SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:sender-vouches"/>
</Subject>
<Conditions NotBefore="2007-03-20T20:36:11Z" NotOnOrAfter="2007-03-20T20:41:11Z">
<AudienceRestriction>
<Audience>
https://sitecatalyst.omniture.com/login.html
</Audience>
</AudienceRestriction>
</Conditions>
<AttributeStatement>
<Attribute Name="login_version">
<AttributeValue xsi:type="xs:string">
sc13_5
</AttributeValue>
</Attribute>
</AttributeStatement>
</Assertion>
```

如上文所述，XML 标记中许多数据的具体内容取决于您所在的环境。表 x 列出具有变量信息的标记，并描述标记中所包含的数据。

表 2.1: XML 数据变量

标记	描述
Assertion ID	此 ID 是客户端生成的每个断言的唯一 ID。每个 ID 只能使用一次，并且只能被接受一次。这样可以避免重播攻击。
IssueInstant	生成断言的时间。使用 UTC。
Issuer	用于登录至 SiteCatalyst 的公司名称。
Reference URI	与断言 ID 相同。
Digest Value	所有 base64_encode 的值 (sha1 (convert_to_single_line (all the XML minus the signature)))
Signature	摘要值的 64 位编码签名。
NameID	当前登录主体的用户名。
NotBefore	此时间前断言无效 (+/- 5 分钟) UTC。
NotAfter	此时间后断言无效 (+/- 5 分钟) UTC。
Audience	张贴断言的位置。如果公司收到 AuthNRequest 信息，这表明该值已提供给他们。
AttributeStatement	(可选) 在公司希望用户登录至特定版本的 SiteCatalyst 时，可使用此属性语句。如未提供此版本，用户将登录至允许的最新版本。

下例说明用于创建 ID 的 PHP 函数：

```
function createAssertionId($length=42) {
    $sid = "";

    for ( $i=0; $i < $length; $i++ ) {
        $sid .= dechex( rand(0,15) );
    }

    return $sid;
}
```