IBM Cloud Identity Portal

EAI 集成指南

IBM Cloud Identity Portal

EAI 集成指南

EAI 集成指南

目录

Cloud Identity Portal EAI 集成

集成 Cloud Identity Portal 与外部认证接口 (EAI) 应用程序。

外部认证接口 (EAI) 应用程序处理 Cloud Identity Portal 所保护的 Web 资源的认证和会话管理。

概述

集成 Cloud Identity Portal 与外部认证接口 (EAI) 应用程序。EAI 应用程序处理受保护 Web 资源的认证和会话管理。

API 状态

本《EAI 集成指南》中的每个 API 都有经过验证的可用状态。可用的 EAI 应用程序包括：

- 使用标准 HTTPS 进行认证
- 使用 REST 进行认证
- 检查认证状态
- WebSEAL 注销
- 通过社交媒体认证用户
- 通过社交媒体和 REST 认证用户
- 传输使用 SMS 的会话
- 创建 Web 浏览器会话
- 检索 Web 浏览器会话

相关主题包括：

- 对特定请求的响应
  - 缺省响应页面
  - 可配置响应程序

认证和授权

认证使用标准的 HTTPS 和 REST。

REST 表示具象状态传输。REST API 是按用户、组和组成员处理任何数量的授权请求的服务，例如，目的是为了获取对服务器的访问权。请求类型包括 GET、POST、PUT 和 DELETE。客户机或不同类型的管理门户网站用户通过发送请求和接收响应（请求和

响应均使用 HTTP 协议）来请求访问权。然后，REST API 服务做出响应。Cloud Identity Portal 的请求和响应格式化为 JSON 对象。

基于 REST 的服务称为 RESTful 服务。

使用标准 HTTPS 进行认证

使用标准 HTTPS 认证用户。

方法

```
POST /EAI/Login
```

尝试使用标准 POST 和响应重定向来认证用户。

cURL 请求示例

```
curl -X POST -d "username=gordita&password=IluvTr3ats!&redirect=https://
your.site.com/protected/index.html&reprompt=https://your.site.com/
index.html" https://gateway.domain.com/EAI/Login
```

请求参数

表 *1.* 请求参数

参数名称	描述
username	用户的**用户名**。
password	提供的**密码**。
redirect	成功认证后要将用户发送到的 URL。
reprompt	失败认证尝试后要将用户发送到的 URL。

返回

200：客户特定配置可能导致产生代码 200，并将 **JavaScript** 重定向到指定的位置。如果客户特定配置成功，那么会将用户发送到重定向 URL。如果客户特定配置失败，那么会将用户发送到重新提示 URL。

302：重定向，适用于所有情况。

autherror：向重新提示 URL 追加查询字符串参数。重新提示 URL 指示认证尝试期间发生的错误。如果失败，WebSEAL 将重定向到配置的错误页面。

使用 REST 进行认证

使用 REST 认证用户。

方法

```
POST /EAI/api/login
```

尝试认证用户。

cURL 请求示例

```
curl -X POST -H "Content-Type:application/x-www-form-urlencoded" -d
"username=gordita&password=IluvTr3ats!" https://gateway.domain.com/EAI/api/
login
```

请求参数

表 2. 请求参数

参数名称	描述
username	用户的**用户名**。
password	提供的**密码**。

响应示例

```
{
"status" : "Authentication successful."
}
```

返回

状态

200：正常，表示成功。

401：未经授权，针对所有其他响应。

403：被禁止，表示帐户由于任何原因被锁定。

50X：服务器上发生错误。

成功时，还会返回用户会话 Cookie。

检查认证状态

检查用户的认证状态。

方法

```
GET /EAI/api/session/isAuthenticated
```

尝试检查用户的认证状态。

cURL 请求示例

```
curl https://gateway.domain.com/EAI/api/session/isAuthenticated
```

请求参数

无。

响应示例

```
{ status: "no"}
```

返回

针对所有请求返回**200：正常**。有效内容状态属性指示用户是否已认证。

状态：

- yes：认证会话已就绪。
- no：没有就绪的认证会话。

会话终止

您可以终止使用传统 **WebSEAL** 的会话。 **WebSEAL** 是当前唯一可用的会话终止方法。

WebSEAL 的 /pkmslogout 允许删除所有 **WebSEAL** Cookie 并清空用户会话。此过程完成后，用户将被重定向到其他位置。

WebSEAL 注销

结束用户会话，清空所有 **WebSEAL** 会话 Cookie 并将用户重定向到注销登录页面。

该重定向可以在此次调用中配置，也可以通过可配置响应程序进行配置。如果您想要禁止该重定向，以便浏览器不会被重定向，但仍移除 Cookie，那么还可以从隐藏的图像标记调用此 URL。

```
<img src="/pkmslogout" style="display:none" height="1" width="1" />
```

方法

```
GET /pkmslogout
```

cURL 请求示例

```
curl https://gateway.domain.com/pkmslogout?redirect=http://
gateway.domain.com
```

请求参数

该请求针对包含以下属性的 JSON 有效内容。

表 *3.* 请求参数

参数名称	描述
redirect	会话终止时将用户发送到的位置。

响应示例

```
HTTP/1.1 302 Moved Temporarily content-length: 1680 content-type:
text/html ... location: <logout location> ...
Set-Cookie: PD-ID=;
Max-Age=0;
Domain=.pb.com;
Path=/; Expires="Sun,
01-Jan-1995 01:00:00
GMT"; Secure
Set-Cookie: PD-ECC=;
Max-Age=0;
```

```
Domain=.pb.com;
Path=/; Expires="Sun,
01-Jan-1995 01:00:00
GMT"; Secure
```

返回

状态

200：正常，表示成功。

401：未经授权，表示因任何原因而失败。

500：服务器上发生错误。成功时，用户会话在 **WebSEAL** 上终止。

社交媒体集成

通过社交媒体认证用户。

通过社交媒体认证用户

通过调用社交媒体和使用传统 POST 尝试认证用户。

方法

```
POST /EAI/Login/social/{platform}
```

platform 对应于用于认证的社交媒体平台。由 Spring Social 提供对社交媒体的支持。

计划的**提供者**支持：*facebook*、*google*、*qq*、*renren*、*wechat*、*weibo* 和 *yahoo*。

cURL 请求示例

```
curl -X POST -H "Content-Type: application/x-www-form-urlencoded" -d
"token=123445&appId=com.your.site.app&redirect=https://your.site.com/
protected/

index.html&reprompt=https://your.site.com/index.html"https://gateway.domain.com/
EAI /Login/social/facebook
```

请求参数

包含以下参数的 JSON 有效内容。

表 *4.* 请求参数

参数名称	描述
token	用户的访问**令牌**。
appId	这是预先共享的应用程序标识，用于允许 Cloud Identity Service 确定应使用的 API 密钥。
redirect	成功认证后要将用户发送到的 URL。
reprompt	失败认证尝试后要将用户发送到的 URL。

返回

200：正常，表示成功。客户特定配置可能导致产生代码 200 和 JavaScript 重定向。

成功时，将用户发送到重定向 URL。失败时，将用户发送到重新提示 URL。查询字符串参数 **autherror** 将追加到重新提示 URL 以指示认证尝试期间发生的错误。

302：重定向，适用于所有情况。

401：未经授权，表示因任何原因而失败。错误消息可以配置为任何所需字符串，并可以基于语言环境或首选语言进行翻译（本地化）。请联系您的 IBM® 交付负责人以了解有关针对每个其他响应定制该 **401 未经授权**的详细信息。

成功时，还会返回用户会话 Cookie。

通过社交媒体和 REST 认证用户

通过调用社交媒体和 REST API 尝试认证用户。

方法

```
POST /EAI/api/login/social/{platform}
```

platform 对应于用于认证的社交媒体平台。由 Spring Social 提供对社交媒体的支持。

计划的**提供者**支持：*facebook*、*google*、*qq*、*renren*、*wechat*、*weibo* 和 *yahoo*。

cURL 请求示例

```
curl -X POST -d '{"token":"123445","appId":"com.your.site.app"}' -H "Content-Type: application/json" https://gateway.domain.com/EAI/api/login/social/facebook
```

```
curl -X POST -H "Content-Type: application/json" "https://gateway.domain.com/EAI/api/login/social/yahoo?token=12345&appId=com.your.site.app"
```

请求参数

内容类型：**application/json**。

表 *5.* 请求参数

参数名称	描述
token	用户的访问令牌。
appId	这是共享的应用程序标识，用于允许 Cloud Identity Service 确定应使用的 API 密钥。

响应示例

```
{status: success}
```

返回

200：正常，表示成功。

401：未经授权，表示因任何原因而失败。

403：被禁止，表示用户的社交媒体帐户不完整并且无法创建用户概要文件。

500：服务器上发生错误。

成功时，还会返回用户会话 Cookie。

会话管理

创建、传输和检索会话。

使用 SMS 传输会话

用户经过认证之后，在新的域名服务 (DNS) 域中创建会话。

必须存在有效会话。必须针对短消息服务 (SMS) 配置环境。

方法

```
POST /EAI/api/session/resumeSession
```

cURL 请求示例

```
curl -X POST -d "sessionID=123456&redirect=https://your.site.com/
protectedResource" https://gateway.domain.com/EAI/api/session/resumeSession
```

请求参数

请求包含具有以下参数的 JSON 有效内容。

表 *6.* 请求参数

参数名称	描述
sessionID	用户的 SMS 会话标识。
redirect	恢复会话后将用户发送到的 URL。

返回

200：客户特定配置可能导致产生代码 **200**，并将 **JavaScript:** 重定向到指定位置。

302：重定向。

Failure：如果失败，**WebSEAL** 将重定向到配置的错误页面。

成功时，还会返回用户会话 Cookie。

创建 Web 浏览器会话

通过会话验证令牌创建 Web 浏览器会话。

针对当前域创建 Web 会话。创建 Web 会话要求用户已通过 **GmaApi** 进行认证，并且该用户存在会话验证令牌。

方法

```
[GET | POST]

/EAI/api/session/createSessionFromToken
```

cURL 请求示例

```
curl -X POST -d "token=7470f51f-2f5f-470e-8bea-402ae678bafb&redirect=https://
your.site.com/protectedResource" https://gateway.domain.com/EAI/api/session/
createSessionFromToken
```

请求参数

包含以下参数的 JSON 有效内容。

表 7. 请求参数

参数名称	描述
token	可选。如果您要为已通过 **GmaApi** 认证的用户创建会话，那么这是该用户的 **sessionVerificationToken** 值。
redirect	可选。恢复会话后将用户发送到的 URL。

返回

200：。客户特定配置可能导致产生代码 **200** 并将 **JavaScript:** 重定向到指定位置。

302：重定向。

LSG-SESSION-ID：表示用户的 SMS 会话标识句柄的 LSG-SESSION-ID Cookie。

WebSEAL：用户的 **WebSEAL** 会话 (PD-S-SESSION-ID) 的会话 Cookie。如果失败，**WebSEAL** 将重定向到配置的错误页面。

命令序列示例

1. 通过调用 **username** 和 **password** 形式的数据来认证用户：

   ```
   curl -X POST -H "Content-Type:application/x-www-form-urlencoded" -H
   "Authorization: Basic ZWFpLWNsaWVudDo=" -d "grant_type=password
   &username=userid&password=user_password" https://gateway.domain.com/EAI/
   oauth/token
   ```

   其中，**userid** 值是用户的 **gtwyPrincipalName** 属性值，而 **user_password** 是用户的密码属性值。
2. 发起 GET 请求，并将步骤 1 中返回的 **OAuthbearer** 令牌放到**认证头**中：

   ```
   curl -H "Authorization: Bearer 56d512a9-4fa34ac6-a72a-76d66ed84d21" https://
   gateway.do main.com/EAI/api/me/startWebSession
   ```
3. 发起 GET 请求，并将返回的 **entry** 值替换到**查询字符串**中。将字段名称 **token** 用于此值：

   ```
   curl https://gateway.domain.com/EAI/api/session/createSessionFromToken?token
   =4683caf7-c937-4edc-8105-bfa075f4d6ff -v
   ```

此处的返回内容包含可以用于 **getSession** 的 **PD-S-SESSION-ID**。

注：操作系统 Windows、Linux 和 Mac 之间的语法有所不同。例如，在 Windows 中，无需使用引号。

检索 Web 浏览器会话

检索用户会话的短消息服务 (SMS) Cookie。

要求用户通过外部认证接口 (EAI) 进行认证。

方法

```
[POST] /EAI/api/session/getSession
```

cURL 请求示例

```
curl https://gateway.domain.com/EAI/api/session/getSession
```

请求参数

无。

返回

200：正常，表示成功。

LSG-SESSION-ID：表示用户的 SMS 会话标识句柄的 LSG-SESSION-ID Cookie。

对特定请求的响应

EAI 确定用于响应特定请求的正确页面。

缺省响应页面

对于一组特殊操作，EAI 具有一个名为**响应程序**的组件，用于确定要提供的正确页面。

例如，假设某用户尝试访问受保护的资源，但首先需要认证。**WebSEAL** 向**响应程序**发送了一个请求，指示该用户需要登录。然后，**响应程序**提供登录页面。这些登录页面和其他认证页面可以针对每个域进行配置，服务团队可以提供认证页面模板。

认证页面包括：

- **登录**
- **注销**
- **密码更改**（适用于到期密码）
- **成功密码更改**，仅当用户没有其他资源时显示。
- **错误**，仅适用于 **WebSEAL** 服务器错误。
- **递升式**，仅适用于递升式认证。
- **帮助**，适用于 **WebSEAL** 无法为其提供服务的操作。

可配置响应程序

作为使用缺省页面的替代方法，也可以将**响应程序**配置为重定向到客户选择的位置。

对于支持的每个操作，可以将**响应程序**配置为分析传入的引用 URL，确定该 URL 是否与特定模式匹配，然后将浏览器重定向到配置的位置。

请参阅以下"操作目标"表：

表 *8.* 操作目标

操作	访问来源	目标
登录	https://*.foo.com	https://www.foo.com/login
注销	https://*.foo.com	https://www.foo.com/logout
密码	https://*.foo.com	https://www.foo.com/selfservice
登录后	https://*.foo.com	https://www.foo.com/postlogin

如上表所述，**访问来源 URL** 可以基于正则表达式使用通配符。如果启用了该通配符功能，并且特定**操作**和**访问来源**与目标匹配，那么会将浏览器发送到目标 URL。该目标 URL 包含**访问来源 URL** 作为**查询字符串**参数。

声明

本信息是为在美国国内供应的产品和服务而编写的。

IBM 可能在其他国家或地区不提供本文档中讨论的产品、服务或功能特性。 有关您所在区域当前可获得的产品和服务的信息，请向您当地的 IBM 代表咨询。 任何对 IBM 产品、程序或服务的引用并非意在明示或暗示只能使用 IBM 的产品、程序或服务。 只要不侵犯 IBM 的知识产权，任何同等功能的产品、程序或服务，都可以代替 IBM 产品、程序或服务。但是，评估和验证任何非 IBM 产品、程序或服务的操作，由用户自行负责。

IBM 可能已拥有或正在申请与本文档内容有关的各项专利。 提供本文档并不意味着授予用户使用这些专利的任何许可。 您可以用书面形式将许可查询寄往：

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

有关双字节字符集 (DBCS) 信息的许可查询，请与您所在国家或地区的 IBM 知识产权部门联系，或用书面方式将查询寄往：

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

以下段落对于英国和与当地法律有不同规定的其他国家或地区均不适用：INTERNATIONAL BUSINESS MACHINES CORPORATION"按现状"提供本出版物，不附有任何种类的（无论是明示的还是暗含的）保证，包括但不限于暗含的有关非侵权、适销和适用于某特定用途的保证。某些国家或地区在某些交易中不允许免除明示或暗含的保证。因此本条款可能不适用于您。

本信息可能包含技术方面不够准确的地方或印刷错误。 本信息将定期更改；这些更改将编入本信息的新版本中。 IBM 可以随时对本出版物中描述的产品和/或程序进行改进和/或更改，而不另行通知。

本信息中对任何非 IBM Web 站点的引用都只是为了方便起见才提供的，不以任何方式充当对那些 Web 站点的保证。 那些 Web 站点中的资料不是 IBM 产品资料的一部分，使用那些 Web 站点带来的风险将由您自行承担。

IBM 可以按它认为适当的任何方式使用或分发您所提供的任何信息而无须对您承担任何责任。

本程序的被许可方如果要了解有关程序的信息以达到如下目的：(i) 使其能够在独立创建的程序和其它程序（包括本程序）之间进行信息交换，以及 (ii) 使其能够对已经交换的信息进行相互使用，请与下列地址联系：

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 79758 U.S.A

只要遵守适当的条件和条款，包括某些情形下的一定数量的付费，都可获得这方面的信息。

本资料中描述的许可程序及其所有可用的许可资料均由 IBM 依据 IBM 客户协议、IBM 国际程序许可协议或任何同等协议中的条款提供。

涉及非 IBM 产品的信息可从这些产品的供应商、其出版说明或其他可公开获得的 资料中获取。 IBM 没有对这些产品进行测试，也无法确认其性能的精确性、兼容性或任何其他关于非 IBM 产品的声明。 有关非 IBM 产品性能的问 题应当向这些产品的供应商提出。

所有关于 IBM 未来方向或意向的声明都可随时更改或收回，而不另行通知，它们仅仅表示了目标和意愿而已。

本信息包含在日常业务操作中使用的数据和报告的示例。为了尽可能完整地说明这些示例，示例中可能会包括个人、公司、品牌和产品的名称。所有这些名字都是虚构的，若现实生活中实际业务企业使用的名字和地址与此相似，纯属巧合。

商标

IBM、IBM 徽标和 ibm.com 是 International Business Machines Corp., 在全球许多管辖区域的商标或注册商标。 其他产品和服务名称可能是 IBM 或其他公司的商标。 当前的 IBM 商标列表，可从 Web 站点 www.ibm.com/legal/copytrade.shtml 上『版权和商标信息』部分获取。

Java™ 和所有基于 Java 的商标和徽标是 Oracle 和/或其子公司的商标或注册商标。

Linux 是 Linus Torvalds 在美国和/或其他国家或地区的商标。

Microsoft、Windows、Windows NT 和 Windows 徽标是 Microsoft Corporation 在美国和/或其他国家或地区的商标。

Printed in China