IBM Cloud Identity Portal

EAI Me API 指南

IBM Cloud Identity Portal

EAI Me API 指南

EAI Me API 指南

目录

Cloud Identity Portal EAI Me 集成 . . . 1
概述 1
认证 1
向 Me API 进行认证 1
用户名和密码认证. 1
社交媒体联合 2
刷新令牌. 4
验证令牌. 5
单用户操作 5
向 Me API 进行认证 5
获取用户详细信息. 5
获取服务. 6
获取角色. 7
获取 KBA 问题 7
更改密码. 8
启动 Web 会话 9

声明 11
商标. 12

Cloud Identity Portal EAI Me 集成

将 Cloud Identity Portal 与外部认证接口 (EAI) 应用程序集成，Me API 添加一系列单用户 API 调用。

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。Me API 添加一系列单用户 API 调用，这些调用在 Cloud Identity Portal API 中有对等项。

认证

使用 **OAuth** 令牌进行认证。

向 Me API 进行认证

要为用户获取 **OAuth** 令牌，该 API 需要已知**客户机标识**的 **OAuth2** 基本授权头。当前实现支持硬编码的客户机标识 **eai-client**。下文的两个认证调用示例包含要发送的必需**基本授权**头。

用户名和密码认证

API 支持使用 **OAuth 2.0 密码**流的认证。

方法

```
POST /EAI/oauth/token
```

内容类型

```
application/x-www-form-urlencoded
```

cURL 请求示例

```
curl -X POST -H "Content-Type:application/x-www-form-urlencoded" -H
"Authorization: Basic ZWFpLWNsaWVudDo=" -d "grant_type=password
&username=gorditapassword=IluvTr3ats!" https://gateway.domain.com/EAI/oauth/
token
```

```
curl -X POST -H "Content-Type:application/json" -H "Authorization: Basic
ZWFpLWNsaWVudDo=" "https://gateway.domain.com/EAI/oauth/token?grant_type=password
&username=testuser &password=testpassword"
```

请求参数

表 *1.* 请求参数

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

响应示例

```
{
access_token: "4ed14dd2-d4f3-4089-8f06-02ae42a08420"
token_type: "bearer"
refresh_token: "c11fbcad-fb04-4444-abce-1fd3923bc611"
expires_in: 3194
scope: "read"
}
```

返回

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。

社交媒体联合

该 API 还支持联合社交媒体登录。

社交媒体数据通过 **JSON Web 令牌** (JWT) 进行传递，并符合 OAuth 2.0 JWT Assertion Profile。

方法

```
POST /EAI/oauth/token
```

内容类型

```
application/x-www-form-urlencoded
```

cURL 请求示例

```
curl -X POST -H "Content-Type:application/x-www-form-urlencoded" -H
"Authorization: Basic ZWFpLWNsaWVudDo=" -d "grant_type=
urn%3Aietf%3Aparams%3Aoauth%3Agranttype% 3Ajwtbearer&assertion=eyJhbGciOi
Jub25lIiwidHlwIjoiSdUIn0=.eyJleHAiOiIxNDE zMjcxNDU0NjI2IiwicGxhdCI6ImZhY2
Vib29rIiwic3ViIjoiMjc2ODI3ODY5MTQxODU4Iiwi dG9rZW4iOiJDQUFEN3hnTE4yMkl
CQUpnQWlsbnBzSDdRZHg4Tk9KUmxGWTY4eVh5dURoZXBRS lB1QjJKV042dVJqdXVoc1pDZ0
YwWkNmN1luU0hGbW1yN1pDU0FWSkduOURHb2ZkVndlWVBHdj d4dXl4ejhZdzhvWkF6T3U0
WkJTSHRxbUhIOEZ0NHIzQU9JWkI2VUptWDNaQXFnZ3hmRThNWWh aQkkzN0c0em94VEROMWR
PRm5PdHV1SmV5NVI3RE9Wajd0YUpiVXdieVJjMjQyM3JKRW9vc3g2 UWVUbGFCIiwibmJm
IjoiMTQxMzI2Nzg1NDYyNiIsImlzcyI6Imh0dHBzOi8vd3d3LmxpbmNvb G4uY29tLmNu
```

```
IiwianRpIjoiNzk0M2RhNGQtMTBmYy00MWUwLThjNjgtNjIzZDUyYzk0MzRhIi
widHlwIjoiaHR0cHM6Ly93d3cuaWJtLmNvbS9nYXRld2F5L3NvY2lhbCIsImlhdCI6Ij
E0MTM yNjc4NTQ2MjYifQ==. "https://gateway.domain.com/EAI/oauth/token
```

请求参数

表 2. 请求参数

参数名称	描述
grant_type	必须是 `urn:ietf:params:oauth:grant-type:jwt-bearer` 断言是包含以下声明的 **JSON Web 令牌** (JWT)： **exp**：声明的到期时间。可选。 **plat**：用户用来认证的社交媒体平台。值包括：*facebook*、*google*、*qq*、*renren*、*wechat*、*weibo* 和 *yahoo*。 **sub**：社交媒体平台应用程序的标识。 **token**：社交媒体授权完成时收到的授权**令牌**。 **iss**：表示发出了**令牌**的用户的 URL。 **jti**：令牌的唯一标识。可选。 **typ**：令牌类型。当前仅支持 `urn:com:ibm:cloud identity:social`。 支持的 JWT 时间戳记：exp、nbf 和 iat。可选。 当前，必须以纯文本形式并且使用该表后面的示例中所用的头，发出 **JSON Web 令牌**。

当您以"请求参数"表中的上述 **JWT** 数据结构进行编码时，即符合标准规则。输出类似于以下代码块。该示例格式设置为跨多行显示。实际提交必须为一行：

```
// header { "alg": "none", "typ": "JWT" }
// claims { "exp": "1413271454626", "plat":"Facebook",
"sub":"276827869141858", "token":"TOKEN", "nbf":"1413267854626",
"iss":"ISSUER", "jti":"ID", "typ":"urn:com:ibm:cloudidentity:
social", "iat":"1413267854626" } eyJhbGciOiJub25lIiwidHlwI
joiSldUIn0=.eyJleHAiOiIxNDEzMjcxNDU0NjI2IiwicGxhdCI6ImZhY2Vib
29rIiwic3ViIjoiMjc2ODI3ODY5MTQxODU4IiwidG9rZW4iOiJDQUFEN3hnTE
4yMklCQUpnQWlsbnBzSDdRZHg4Tk9KUmxGWTY4eVh5dURoZXBRSlB1QjJKV0
42dVJqdXVoc1pDZ0YwWkNmN1luU0hGbW1yN1pDU0FWSkduOURHb2ZkVndl
WVBHdjd4dXl4ejhZdzhvWkF6T3U0WkJTSHRxbUhIOEZ0NHIzQU9JWkI2VUpt
WDNaQXFnZ3hmRThNWWhaQkkzN0c0em94VEROMWRPRm5PdHV1SmV5NVI3RE9
Wajd0YUpiVXdieVJjMjQyM3JKRW9vc3g2UWVUbGFCIiwibmJmIjoiMTQxMz
I2Nzg1NDYyNiIsImlzcyI6Imh0dHBzOi8vd3d3LmxpbmNvbG4uY29tLmNu
IiwianRpIjoiNzk0M2RhNGQtMTBmYy00MWUwLThjNjgtNjIzZDUyYzk0Mz
RhIiwidHlwIjoiaHR0cHM6Ly93d3cuaWJtLmNvbS9nYXRld2F5L
3NvY2lhbCIsImlhdCI6IjE0MTMyNjc4NTQ2MjYifQ==.
```

响应示例

```
{
access_token: "4ed14dd2-d4f3-4089-8f06-02ae42a08420"
token_type: "bearer"
refresh_token: "c11fbcad-fb04-4444-abce-1fd3923bc611"
expires_in: 3194
scope: "read"
}
```

返回

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。

刷新令牌

令牌即将到期时，您可以使用刷新令牌来获取新访问令牌。

方法

```
POST /EAI/oauth/token
```

内容类型

```
application/x-www-form-urlencoded
```

cURL 请求示例

```
curl -X POST -H "Content-Type:application/x-www-form-urlencoded" -H
"Authorization: Basic ZWFpLWNsaWVudDo=" -d "grant_type=refresh_token
&client_id=eai-client&refresh_token=c11fbcad-fb04-4444- abce-1fd3923bc611"
https://gateway.domain.com/EAI/oauth/token
```

```
curl -X POST -H "Authorization: Basic ZWFpLWNsaWVudDo=" -H "Content-Type: appli-
cation/json" "https://gateway.domain.com/EAI/oauth/token?grant_type=refresh_token
&client_id=eai-client&refresh_token=7123fb5e-47a8-4c63-a913-85064b29dc0c"
```

请求参数

表 *3.* 请求参数

参数名称	描述
grant_type	必需参数为 **refresh_token**。
client_id	必需参数为 **eai-client**。
refresh_token	在认证期间提供 **refresh_token**。

响应示例

```
{
access_token: "4ed14dd2-d4f3-4089-8f06-02ae42a08420"
token_type: "bearer"
refresh_token: "c11fbcad-fb04-4444-abce-1fd3923bc611"
expires_in: 3194
scope: "read"
}
```

返回

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。

验证令牌

使用该 API 来确定 Oauth 令牌是否有效。

方法

```
GET /EAI/oauth/check_token
```

cURL 请求示例

```
curl https://gateway.domain.com/EAI/oauth/check_token?token=4ed14dd2-d4f3-
4089-8f06-02ae42a08420
```

请求参数

表 4. 请求参数

参数名称	描述
token	要检查的 Oauth 令牌。

响应示例

```
{
"authorities" : [ "ROLE_CLIENT" ],
"client_id" : "eai-client",
"exp" : 1418616268,
"scope" : [ "read" ],
"user_name" : "eaitest"
}
```

返回

200：正常，表示成功。

400：错误请求，表示令牌未被识别。

单用户操作

用户可用的操作。

向 Me API 进行认证

所有操作都要求来自认证流的**访问令牌**表示为**不记名令牌**。

获取用户详细信息

检索已认证用户的用户详细信息。返回所有可用属性。

方法

```
GET /EAI/api/me
```

内容类型：

```
application/json
```

cURL 请求示例

curl -H "Authorization: Bearer *access_token*" https://gateway.domain.com/EAI/api/me

请求参数

无。

响应示例

```
{"status" : "success",
"entry" : {
"status" : null,
"gtwayUUID" : "323966f1-0780-4fb4-928b-8fe3d4f19b94",
"uid" : "test",
"gma_isAccount" : true,
"uid" : "test",
"mail" : "test@us.ibm.com",
"gtwayPrincipalName" : "test",
"sn" : "testing",
"gtwayPrefLanguage" : "en-us",
"c" : "usa",
"cn" : "test testing",
"gtwayIsManager" : "true",
"gtwayUUID" : "323966f1-0780-4fb4-928b-8fe3d4f19b94",
"givenName" : "Test",
"employeeNumber" : "1234567890"
},
"totalCount" : 1}
```

返回

200：正常，表示成功。

获取服务

检索已认证用户所属的服务。

方法

GET /EAI/api/me/services

内容类型：

application/json

cURL 请求示例

curl -H "Authorization: Bearer *access_token*" https://gateway.domain.com/EAI/api/me/services

请求参数

无。

响应示例

```
{
"status" : "success",
"entry" : [ "svc_GatewayWAMService", "svc_test service" ],
"totalCount" : 2
}
```

返回

200：正常，表示成功。

获取角色

检索已认证用户所属的角色。

方法

```
GET /EAI/api/me/roles
```

内容类型：

```
application/json
```

cURL 请求示例

```
curl -H "Authorization: Bearer access_token" https://gateway.domain.com/EAI/
api/me/roles
```

请求参数

无。

响应示例

```
{
"status" : "success",
"entry" : [ "Help Desk", "Manager", "Default" ],
"totalCount" : 3
}
```

返回

200：正常，表示成功。

获取 KBA 问题

检索用户定义的知识型认证 (KBA) 问题，也称为安全问题。"获取 KBA 问题"方法仅返回问题编号，必须与 GmaApi 的 KBA 方法配对使用以检索所需语言的实际问题文本。

方法

```
GET /EAI/api/me/kba
```

内容类型：

```
application/json
```

cURL 请求示例

```
curl -H "Authorization: Bearer access_token" https://gateway.domain.com/EAI/api/me/kba?showAnswers=true
```

请求参数

表 5. 请求参数

参数名称	描述
showAnswers	可选。布尔值：是否提供答案。设置为 true 时，提供答案。设置为 false 时，隐藏答案。缺省值为 false。

响应示例

```
{
"status" : "success",
"entry" : [ {
"questionNumber" : 1,
"answer" : "1952"
}, {
"questionNumber" : 2,
"answer" : "1950"
}, {
"questionNumber" : 5,
"answer" : "smith"
} ],
"totalCount" : 3
}
```

返回

200：正常，表示成功。

更改密码

允许用户更改其密码。当前密码必须可用。

方法

```
POST /EAI/api/me/changePassword
```

内容类型：

```
application/json
```

cURL 请求示例

```
curl -H "Authorization: Bearer access_token" -d "currentPassword=Passw0rd!&newPassword=MyNewPassw0rd!" https://gateway.domain.com/EAI/api/me/changePassword
```

请求参数

表 *6.* 请求参数

参数名称	描述
currentPassword	必需：用户的**当前密码**。在更改密码之前验证用户的**当前密码**。
newPassword	必需。用户所需的**新密码**。所有适用密码策略都将应用于密码更改尝试。客户机执行客户端密码验证以确保符合密码复杂度规则，然后再提交请求。

响应示例

```
{
"status" : "success",
}
```

返回

200：正常，表示成功。

401：未经授权，表示当前密码验证失败。

403：被禁止，表示新密码验证失败。

412：未通过前提条件，表示在历史记录中发现该新密码。

启动 Web 会话

设置 **sessionVerificationToken** 以允许用户在使用 EAI /api/session/createSessionFromToken API 的其他位置创建 Web 会话。

方法

```
[POST|GET] /EAI/api/me/startWebSession
```

内容类型：

```
application/json
```

cURL 请求示例

```
curl -H "Authorization: Bearer access_token" -d "tokenId=1234-abcd" https://
gateway.domain.com/EAI/api/me/startWebSession
```

请求参数

表 *7.* 请求参数

参数名称	描述
tokenId	要在 Web 会话环境中设置的令牌的标识。**tokenId** 是将发送给 **WebSEAL** 保护的资源的 user_session_id 值。否则，**tokenId** 可以是任意值。

响应示例

```
{
"status":"success",
"entry" : "74018cff-724d-4c37-b0a5-1aff422afb4f",
"totalCount" : 1
}
```

返回

200：正常，表示成功。

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。

Printed in China