IBM Cloud Identity Portal

Handbuch zur EAI Me-API

IBM Cloud Identity Portal

Handbuch zur EAI Me-API

Handbuch zur EAI Me-API

Inhaltsverzeichnis

EAI Me-Integration für Cloud Identity Portal

Integrieren Sie Cloud Identity Portal in die Anwendung "External Authentication Interface" (EAI). Die Me-API fügt eine Reihe von Einzelbenutzer-API-Aufrufen hinzu.

Die Anwendung "External Authentication Interface" (EAI) ist für das Authentifizierungs- und Sitzungsmanagement für Webressourcen verantwortlich, die durch Cloud Identity Portal geschützt werden.

Übersicht

Integrieren Sie Cloud Identity Portal in die Anwendung "External Authentication Interface" (EAI). Die Anwendung "EAI" ist für das Authentifizierungs- und Sitzungsmanagement für geschützte Webressourcen verantwortlich. Die Me-API fügt eine Reihe von Einzelbenutzer-API-Aufrufen hinzu, die Entsprechungen in der Cloud Identity Portal-API haben.

Authentifizierung

Die Authentifizierung mit **OAuth**-Token.

Authentifizierung bei der Me-API

Um ein **OAuth**-Token für einen Benutzer abzurufen, erfordert die API einen Header mit einer "**OAuth2** Basic Authorization" einer bekannten **client ID**. Die aktuelle Implementierung unterstützt eine fest codierte Client-ID (**eai-client**). Die Beispiele der zwei Authentifizierungsaufrufe, die folgen, enthalten den erforderlichen Header vom Typ **Basic Authorization**, der gesendet werden soll.

Authentifizierung über Benutzername und Kennwort

Die API unterstützt eine Authentifizierung, die den Ablauf für das **OAuth 2.0**-Kennwort (**password**) verwendet.

Methode

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

Inhaltstyp

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

cURL-Beispielanforderungen

```
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"
```

Anforderungsparameter

Tabelle 1. Anforderungsparameter

Parametername	Beschreibung
grant_type	Das **password** (Kennwort) des Benutzers.
username	Der **username** (Benutzername) des Benutzers.
password	Das angegebene **password** (Kennwort).

Beispielantwort

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

Gibt zurück

200: OK bedeutet Erfolg.

401: Nicht berechtigt für jede andere Antwort.

403: Nicht zulässig, falls der Account aus irgendeinem Grund gesperrt ist.

Social-Media-Föderation

Die API unterstützt auch die Föderation einer Social-Media-Anmeldung.

Die Social-Media-Daten werden mithilfe eines **JSON Web Token** (JWT) übergeben. Sie müssen mit dem OAuth 2.0-JWT-Zusicherungsprofil konform sein.

Methode

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

Inhaltstyp

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

cURL-Beispielanforderung

```
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
```

Anforderungsparameter

Tabelle 2. Anforderungsparameter

Parametername	Beschreibung
grant_type	Muss `urn:ietf:params:oauth:grant-type:jwt-bearer` sein. Die Zusicherung ist ein **JSON Web Token** (JWT), das die folgenden Anforderungen enthält: **exp**: Die Ablaufzeit der Anforderung. Optional. **plat**: Die Social-Media-Plattform, bei der der Benutzer authentifiziert ist. Dies kann eine der folgenden Plattformen sein: *facebook*, *google*, *qq*, *renren*, *wechat*, *weibo* und *yahoo*. **sub**: Die ID der Anwendungs-ID der Social-Media-Plattform. **token**: Das Berechtigungstoken (**token**), das empfangen wurde, als die Social-Media-Autorisierung abgeschlossen war. **iss**: Eine URL, die angibt, wer das **token** ausgestellt hat. **jti**: Eine eindeutige ID für das Token. Optional. **typ**: Der Typ des Token. Derzeit wird nur `urn:com:ibm:cloud identity:social` unterstützt. Die unterstützten JWT-Zeitmarken: exp, nbf, iat. Optional. Derzeit muss das **JSON Web Token** in einfachem Text ausgestellt werden. Dabei muss der Header dem Beispiel in der folgenden Tabelle entsprechen.

Wenn Sie in der oben beschriebenen **JWT**-Datenstruktur in der Anforderungsparametertabelle verschlüsseln, folgen Sie den Regeln des Standards. Die Ausgabe ähnelt dem Codeblock. Das Beispiel ist für Zeilenumbrüche formatiert. Die tatsächliche Übergabe muss in einer einzigen Zeile erfolgen:

```
// 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==.
```

Beispielantwort

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

Gibt zurück

200: OK bedeutet Erfolg.

401: Nicht berechtigt für jede andere Antwort.

403: Nicht zulässig, falls der Account aus irgendeinem Grund gesperrt ist.

Aktualisierungstoken

Wenn das Token fast abgelaufen ist, können Sie das Aktualisierungstoken verwenden, um ein neues Zugriffstoken abzurufen.

Methode

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

Inhaltstyp

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

cURL-Beispielanforderungen

```
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:
application/json" "https://gateway.domain.com/EAI/oauth/
token?grant_type=refresh_token&client_id=eai-client&refresh_token=7123fb5e-
47a8-4c63-a913-85064b29dc0c"
```

Anforderungsparameter

Tabelle 3. Anforderungsparameter

Parametername	Beschreibung
grant_type	Der erforderliche Parameter ist **refresh_token**.
client_id	Der erforderliche Parameter ist **eai-client**.
refresh_token	Stellt das **refresh_token** (Aktualisierungstoken) während der Authentifizierung bereit.

Beispielantwort

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

Gibt zurück

200: OK bedeutet Erfolg.

401: Nicht berechtigt für jede andere Antwort.

403: Nicht zulässig, falls der Account aus irgendeinem Grund gesperrt ist.

Tokens auswerten

Verwenden Sie diese API, um zu bestimmen, ob ein Oauth-Token aktuell gültig ist.

Methode

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

cURL-Beispielanforderungen

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

Anforderungsparameter

Tabelle 4. Anforderungsparameter

Parametername	Beschreibung
token	Das zu überprüfende Oauth-Token.

Beispielantwort

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

Gibt zurück

200: OK bedeutet Erfolg.

400: Fehlerhafte Anforderung, wenn das Token nicht erkannt wird.

Einzelbenutzeroperationen

Operationen, die für den Benutzer verfügbar sind.

Authentifizierung bei der Me-API

Für alle Operationen ist es erforderlich, dass das **access token** (Zugriffstoken) aus dem Authentifizierungsablauf als ein **Bearer token** (Trägertoken) dargestellt wird.

Benutzerdetails abrufen

Ruft die Benutzerdetails des authentifizierten Benutzers ab. Gibt alle verfügbaren Attribute zurück.

Methode

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

Inhaltstyp:

```
application/json
```

cURL-Beispielanforderungen

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

Anforderungsparameter

Keine.

Beispielantwort

```
{"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}
```

Gibt zurück

200: OK bedeutet Erfolg.

Services abrufen

Ruft die Services ab, zu denen der authentifizierte Benutzer gehört.

Methode

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

Inhaltstyp:

```
application/json
```

cURL-Beispielanforderungen

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

Anforderungsparameter

Keine.

Beispielantwort

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

Gibt zurück

200: OK bedeutet Erfolg.

Rollen abrufen

Ruft die Rollen ab, zu denen der authentifizierte Benutzer gehört.

Methode

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

Inhaltstyp:

```
application/json
```

cURL-Beispielanforderungen

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

Anforderungsparameter

Keine.

Beispielantwort

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

Gibt zurück

200: OK bedeutet Erfolg.

KBA-Fragen abrufen

Ruft die KBA-Fragen (Knowledge Based Authentication; wissensbasierte Authentifizierung) ab, die auch als Sicherheitsfragen bezeichnet werden, die der Benutzer definiert. Die Methode zum Abrufen der KBA-Fragen gibt nur die Fragennummern

zurück. Sie muss paarweise mit den KBA-Methoden der GmaApi verbunden werden, um den eigentlichen Fragetext in der gewünschten Sprache abzurufen.

Methode

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

Inhaltstyp:

```
application/json
```

cURL-Beispielanforderungen

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

Anforderungsparameter

Tabelle 5. Anforderungsparameter

Parametername	Beschreibung
showAnswers	Optional. Boolescher Wert: Ob Antworten bereitgestellt werden sollen. Wenn `true` festgelegt ist, werden Antworten bereitgestellt. Wenn `false` festgelegt ist, werden die Antworten ausgeblendet. Der Standardwert ist `false`.

Beispielantwort

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

Gibt zurück

200: OK bedeutet Erfolg.

Kennwort ändern

Ermöglicht es dem Benutzer, sein Kennwort zu ändern. Das aktuelle Kennwort muss verfügbar sein.

Methode

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

Inhaltstyp:

```
application/json
```

cURL-Beispielanforderungen

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

Anforderungsparameter

Tabelle 6. Anforderungsparameter

Parametername	Beschreibung
currentPassword	Erforderlich: Das aktuelle Kennwort (**current password**) des Benutzers. Das **current password** des Benutzers wird ausgewertet, bevor Sie das Kennwort ändern können.
newPassword	Erforderlich. Das gewünschte neue Kennwort (**new password**) des Benutzers. Alle anwendbaren Kennwortrichtlinien werden auf den Kennwortänderungsversuch angewendet. Clients führen eine clientseitige Überprüfung des Kennworts durch, um sicherzustellen, dass es die Kennwortkomplexitätsregeln erfüllt, bevor eine Anforderung übergeben wird.

Beispielantwort

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

Gibt zurück

200: OK bedeutet Erfolg.

401: Nicht berechtigt, falls die Überprüfung des aktuellen Kennworts fehlschlägt.

403: Nicht zulässig, falls die Überprüfung des neuen Kennworts fehlschlägt.

412: Vorbedingung für ein Fehlschlagen, wenn das neue Kennwort im Verlauf gefunden wurde.

Websitzung starten

Legt ein **sessionVerificationToken** fest, das es dem Benutzer ermöglicht, eine Websitzung in einer anderen Position als die zu erstellen, die von der /api/session/createSessionFromToken-API der EAI verwendet wird.

Methode

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

Inhaltstyp:

```
application/json
```

cURL-Beispielanforderungen

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

Anforderungsparameter

Tabelle 7. Anforderungsparameter

Parametername	Beschreibung
tokenId	Die ID des Token, das in einer Websitzungsumgebung festgelegt werden soll. Die **tokenId** ist der Wert der "user_session_id", die von **WebSEAL** an eine geschützte Ressource gesendet wurde. Andernfalls kann **tokenId** ein beliebiger Wert sein.

Beispielantwort

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

Gibt zurück

200: OK bedeutet Erfolg.

Bemerkungen

Die vorliegenden Informationen wurden für Produkte und Services entwickelt, die auf dem deutschen Markt angeboten werden.

Möglicherweise bietet IBM die in dieser Dokumentation beschriebenen Produkte, Services oder Funktionen in anderen Ländern nicht an. Informationen über die gegenwärtig im jeweiligen Land verfügbaren Produkte und Services sind beim zuständigen IBM Ansprechpartner erhältlich. Hinweise auf IBM Lizenzprogramme oder andere IBM Produkte bedeuten nicht, dass nur Programme, Produkte oder Services von IBM verwendet werden können. Anstelle der IBM Produkte, Programme oder Services können auch andere, ihnen äquivalente Produkte, Programme oder Services verwendet werden, solange diese keine gewerblichen oder anderen Schutzrechte von IBM verletzen. Die Verantwortung für den Betrieb von Produkten, Programmen und Services anderer Anbieter liegt beim Kunden.

Für in diesem Handbuch beschriebene Erzeugnisse und Verfahren kann es IBM Patente oder Patentanmeldungen geben. Mit der Auslieferung dieses Handbuchs ist keine Lizenzierung dieser Patente verbunden. Lizenzanforderungen sind schriftlich an folgende Adresse zu richten (Anfragen an diese Adresse müssen auf Englisch formuliert werden):

IBM Director of Licensing
IBM Europe, Middle East & Africa
Tour Descartes
2, avenue Gambetta
92066 Paris La Defense
France

Trotz sorgfältiger Bearbeitung können technische Ungenauigkeiten oder Druckfehler in dieser Veröffentlichung nicht ausgeschlossen werden. Die hier enthaltenen Informationen werden in regelmäßigen Zeitabständen aktualisiert und als Neuausgabe veröffentlicht. IBM kann ohne weitere Mitteilung jederzeit Verbesserungen und/oder Änderungen an den in dieser Veröffentlichung beschriebenen Produkten und/oder Programmen vornehmen.

Verweise in diesen Informationen auf Websites anderer Anbieter werden lediglich als Service für den Kunden bereitgestellt und stellen keinerlei Billigung des Inhalts dieser Websites dar. Das über diese Websites verfügbare Material ist nicht Bestandteil des Materials für dieses IBM Produkt. Die Verwendung dieser Websites geschieht auf eigene Verantwortung.

Werden an IBM Informationen eingesandt, können diese beliebig verwendet werden, ohne dass eine Verpflichtung gegenüber dem Einsender entsteht.

Lizenznehmer des Programms, die Informationen zu diesem Produkt wünschen mit der Zielsetzung: (i) den Austausch von Informationen zwischen unabhängig voneinander erstellten Programmen und anderen Programmen (einschließlich des vorliegenden Programms) sowie (ii) die gemeinsame Nutzung der ausgetauschten Informationen zu ermöglichen, wenden sich an folgende Adresse:

IBM Corporation
2Z4A/101

11400 Burnet Road
Austin, TX 79758
U.S.A

Die Bereitstellung dieser Informationen kann unter Umständen von bestimmten Bedingungen - in einigen Fällen auch von der Zahlung einer Gebühr - abhängig sein.

Die Lieferung des in diesen Informationen beschriebenen Lizenzprogramms sowie des zugehörigen Lizenzmaterials erfolgt auf der Basis der IBM Rahmenvereinbarung bzw. der Allgemeinen Geschäftsbedingungen von IBM, der IBM Internationalen Nutzungsbedingungen für Programmpakete oder einer äquivalenten Vereinbarung.

Alle Informationen zu Produkten anderer Anbieter stammen von den Anbietern der aufgeführten Produkte, deren veröffentlichten Ankündigungen oder anderen allgemein verfügbaren Quellen. IBM hat diese Produkte nicht getestet und kann daher keine Aussagen zu Leistung, Kompatibilität oder anderen Merkmalen machen. Fragen zu den Leistungsmerkmalen von Produkten anderer Anbieter sind an den jeweiligen Anbieter zu richten.

Aussagen über Pläne und Absichten von IBM unterliegen Änderungen oder können zurückgenommen werden und repräsentieren nur die Ziele von IBM.

Diese Veröffentlichung enthält Beispiele für Daten und Berichte des alltäglichen Geschäftsablaufs. Sie sollen nur die Funktionen des Lizenzprogramms illustrieren und können Namen von Personen, Firmen, Marken oder Produkten enthalten. Alle diese Namen sind frei erfunden; Ähnlichkeiten mit tatsächlichen Namen und Adressen sind rein zufällig.

Marken

IBM, das IBM Logo und ibm.com sind Marken oder eingetragene Marken der International Business Machines Corporation in den USA und/oder anderen Ländern. Weitere Produkt- und Servicenamen können Marken von IBM oder anderen Unternehmen sein. Eine aktuelle Liste der IBM® Marken finden Sie auf der Webseite „Copyright and trademark information" unter www.ibm.com/legal/copytrade.shtml.

Gedruckt in Deutschland