Intégration des utilisateurs à l'aide d'OAuth

Les intégrations au niveau utilisateur sont réalisées à l'aide d'OAuthgrants. Un utilisateur d'un système tiers est lié à un utilisateur Bold et demande l'autorisation d'accéder à tout ce à quoi l'utilisateur Bold peut accéder. Pour implémenter une intégration au niveau utilisateur, les éléments suivants sont nécessaires :

- un identifiant clientIDENTITÉ DU CLIENT
- un secret clientCLIENT_SECRET un
- uri de redirectionREDIRECT_URI

L'identifiant client et le secret client sont fournis par demande Boldon. L'URI de redirection fait partie du système tiers et doit être fourni en gras.

Étape 1 : Appelez BoldauthorizationURL

L'application client tierce doit appeler l'URL d'autorisation en gras. Cela garantira que l'on demande à l'utilisateur Bold si le tiers est autorisé à accéder au système Bold.

https://auth.boldsmartlock.com/?
client_id=CLIENT_ID&response_type=code&state=STATEDATA&redirect_uri=REDIRECT_URI

LeÉtatLe paramètre peut contenir n'importe quelle donnée et sera transmis ultérieurement au système tiers. Le système tiers utilise généralement ces données pour valider l'autorisation accordée et la relier à une demande spécifique.

L'appel de l'URL d'autorisation ouvrira soit un écran de connexion dans lequel l'utilisateur devra se connecter avec ses informations d'identification Bold, soit ouvrira simplement l'application Bold lorsqu'elle sera installée à l'aide de « liens profonds ».

Étape 2 : implémenter l'URI direct

Lorsque l'utilisateur a accordé l'autorisation au tiers, la plate-forme Bold appelle l'URI de redirection. Cet URI doit être implémenté par le serveur d'applications tiers ou via un « lien profond » de l'application tierce.

L'URI appelé aura deux paramètres de requête supplémentaires :

- état = DONNÉES D'ÉTAT: contenant les mêmes données d'état qui ont été transmises à l'URL d'autorisation, et
- code=CODE: contenant le code d'autorisation nécessaire à la connexion.

Dans le cas où l'utilisateur a refusé l'autorisation, l'URI de redirection est toujours appelé, sauf avec une erreur à la place du code d'autorisation.

- état = DONNÉES D'ÉTAT: contenant les mêmes données d'état qui ont été transmises à l'URL d'autorisation, et
- erreur = accès_denié: indiquant que l'autorisation a été refusée.

Étape 3 : Connectez-vous à l'utilisateur

Avec le code d'autorisationCODEqui a été fourni comme paramètre pour l'appel uri de redirection, le système tiers peut connecter l'utilisateur avec le système Bold. On peut soit utiliser l'API, soit le SDK.

Étape 3a : Connectez-vous à l'API

LeAPI OAuth audacieusefournit l'API suivante pour se connecter à l'aide d'un code d'autorisation :

```
POST https://api.boldsmartlock.com/v2/oauth/token
```

Les champs de formulaire suivants doivent être fournis, à partir de la spécification OAuth v2 :

type_de_subvention	Code d'autorisation
code	CODE
redirect_uri	REDIRECT_URI
identité du client	IDENTITÉ DU CLIENT
client_secret	CLIENT_SECRET

Les données renvoyées ressemblent à cet exemple :

```
{
   "jeton d'accès":"03c64166-2c09-456d-ad7e-c1f3a6969b0c",
   "refresh_token" :      "38a32770-a799-49a2-b631-096b7ad8ece0",
   "type_jeton" :      "Porteur",
   "expire dans":      86400
}
```

Lejeton d'accèsest utilisé pour effectuer des appels API. UTILISATION DE L'EN-TÊTE Autorisation 'Bearer $access_token' XXXXXLeexpire dansLa valeur indique combien de secondes le jeton est valide. Pour éviter l'expiration, les jetons doivent être périodiquement actualisés. Cela se fait en utilisant la même API, mais avec les paramètres de formulaire suivants :

type_de_subvention	rafraîchir_token
rafraîchir_token	REFRESH_TOKEN
identité du client	IDENTITÉ DU CLIENT
client_secret	CLIENT_SECRET

Après un rafraîchissement, les deux anciensjeton d'accèsetrafraîchir_tokenne sont plus valables.

Étape 3b : connexion en utilisant le SDK

Quand leBoldDeviceSDKest utilisé, il suffit d'appelerconnexionAvecAuthorizationCodecomme indiqué ci-dessous. En cas de réussite, un jeton d'autorisation est renvoyé et peut être utilisé pour appeler l'API Bold. Le SDK actualisera automatiquement les jetons d'accès en cas de besoin.

```
BoldDeviceSDK.loginWithAuthorizationCode (CLIENT_ID, CLIENT_SECRET, REDIRECT_URI,
CODE)
```

Intégration de l'organisation à l'aide de jetons d'accès

Avec une intégration organisationnelle, les systèmes tiers reçoivent des autorisations sur tout ce qui est géré par une organisation Bold. Le tiers doit demander une organisation Bold et un compte administrateur sur cette organisation avant l'intégration. Avec l'intégration, le tiers peut créer et gérer des utilisateurs, des groupes, des partages, etc. De plus, le système tiers peut demander une autorisation d'accès pour un utilisateur particulier. Ceci est nécessaire pour qu'une application d'utilisateur final tierce accède à l'API Bold.

Étape 1 : Créer un jeton d'accès

Un système tiers accède à l'API Bold à l'aide d'un AccessToken. Les jetons d'accès sont gérés par les administrateurs de l'organisation et ne doivent pas être confondus avec unjeton d'accèsutilisé par OAuth. Un jeton d'accès a un identifiant et un secret qui sont utilisés pour accéder à l'API. Notez que le secret n'est fourni qu'une seule fois lors de la création d'un jeton d'accès.

Étape 1a : Créer un jeton d'accès dans le portail

Connectez-vous au portail en tant qu'utilisateur de l'organisation et créez un jeton d'accès sur la page « intégrations ».*Notez que cette page n'a pas encore été mise en œuvre, veuillez donc vous référer à l'étape 1b.*.

Étape 1b : Créer un jeton d'accès à l'aide de l'API

Un jeton d'accès peut également être créé directement via l'API Bold. Pour créer un jeton d'accès, il faut disposer d'un accès OAuth valide. Voir leAPI de jeton d'accès.

```
POST /v1/accounts/ACCOUNT_ID/access-tokens
```

La réponse contient l'identifiant et le secret du jeton d'accès :

```
{
"accessTokenId" : String, UUID 4 au format (ex "a426e157-8a5c-456a-8865- bec6394867ab"),

"accessTokenSecret" : String, "clientInstanceId" : Number,
enregistrement de la clé primaire, "accountId" : Number,
enregistrement de la clé primaire, "organizationId" : Number,
enregistrement de la clé primaire, "description" : String,

"dateExpiration" : Date/heure avec un fuseau horaire (ISO 8601, par exemple "2022-06-
23T13:53:02+02:00")
}
```

Étape 2 : accéder à l'API

Avec l'identifiant et le secret du jeton d'accès, on peut accéder à l'API en utilisant l'authentification de base :

Autorisation 'Basic BASE64_OF_accessTokenId:accessTokenSecret'

Contrairement à l'accès OAuth classique, ce token reste valable indéfiniment et n'a pas besoin d'être actualisé périodiquement. Il est donc de la responsabilité de l'intégrateur de garder secrètes les informations du jeton d'accès et d'en demander un nouveau (étape 1) lorsqu'il le juge nécessaire.

Étape 3 : Créer des utilisateurs et d'autres éléments

Le système tiers peut créer des utilisateurs sur la plateforme Bold en utilisant API de gestion des utilisateurs:

```
POST /v1/utilisateurs
{
    "téléphone":  chaîne
    "e-mail":     chaîne
    "géré":           vrai
}
```

Notez que les utilisateurs doivent être marquésgéré. Cet indicateur indique que la direction est sous le contrôle d'un système tiers et permet, par exemple, que le système tiers puisse demander une autorisation d'accès pour cet utilisateur. Les informations renvoyées contiennent l'identifiant de l'utilisateur qui peut être utilisé par le système tiers pour la comptabilité :

```
{
    "ID de l'utilisateur":  nombre
}
```

Étape 4 : Demander l'accès aux utilisateurs

Afin de permettre à un utilisateur d'un système ou d'une application tiers d'accéder à notre API, par exemple à l'aide du SDK Bold Device, la plateforme tierce demande un code d'autorisation à la plateforme Bold et l'envoie à l'application utilisateur. L'application utilisateur demande un jeton d'accès OAuth à l'aide de ce code d'autorisation et actualise ce jeton quotidiennement, comme prescrit par OAuth. Le SDK Bold Device le fera pour vous.

```
POST /v2/integrations/CLIENT_ID/autorisation
Autorisation d'en-tête 'Basic BASE64_OF_accessTokenId:accessTokenSecret' {

   {
      "ID client" : CLIENT_ID,
      "responseType": "code",
      "scope": "plateforme",
      "autorisé": vrai
   }
}
```

Les informations renvoyées contiennent le code d'autorisation nécessaire pour authentifier l'utilisateur :

```
{
"code" : CODE,
"ID client" : CLIENT_ID,
"expiration": "2023-04-06T07:10:39.694749Z" }
```

Ce code peut être utilisé comme décrit à l'étape 3 de la documentation 'Intégration utilisateur'.