Authentifier votre client API REST à l'aide d'OAuth

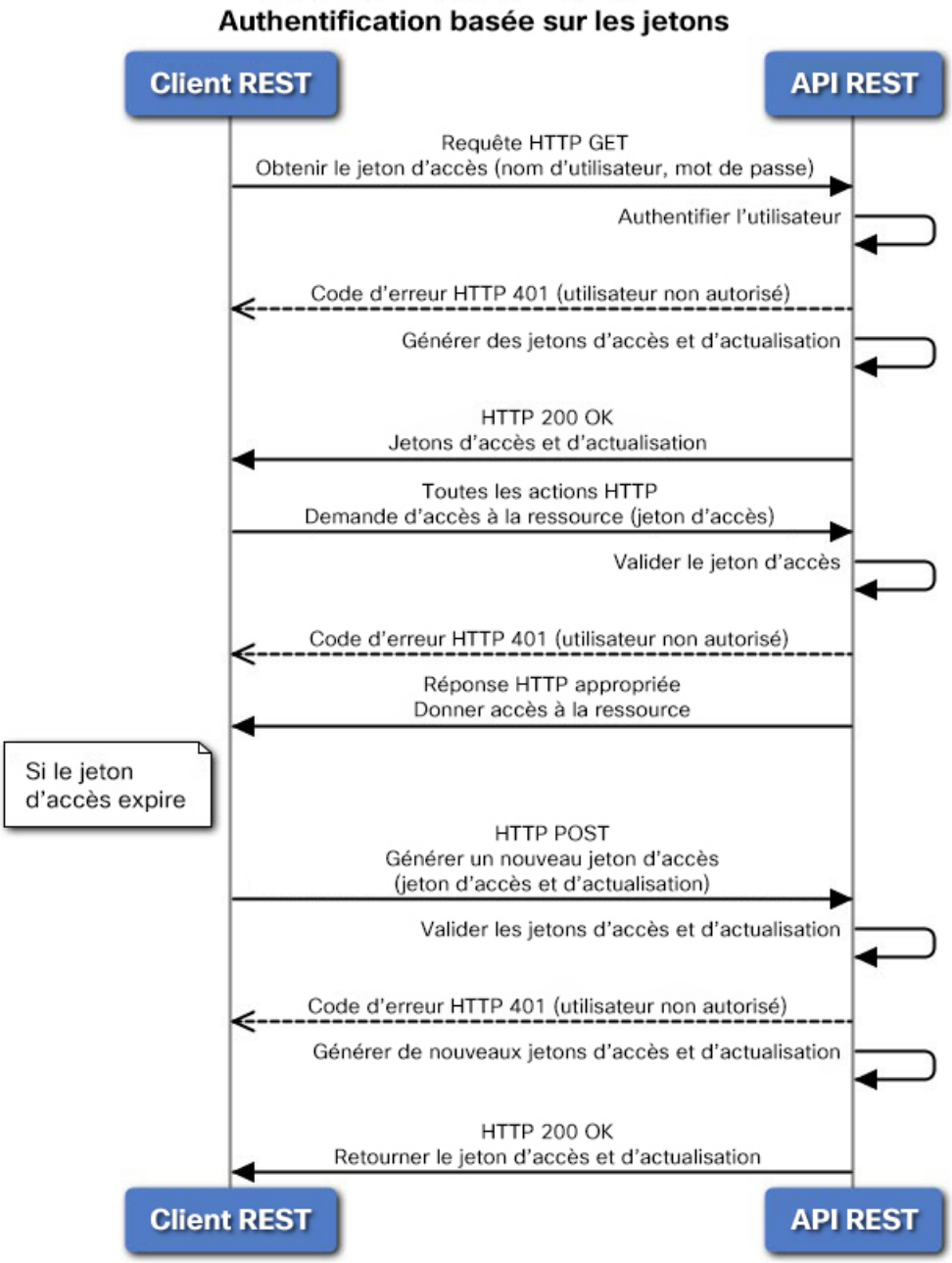
L'API REST Défense contre les menaces utilise OAuth 2.0 pour authentifier les appels provenant de clients API. OAuth est une méthode basée sur les jetons d'accès, et Défense contre les menaces utilise les jetons Web JSON comme modèle. Voici les normes pertinentes :

- RFC6749, le cadre d'autorisation OAuth 2.0, https://tools.ietf.org/html/rfc6749.
- RFC7519, jeton Web JSON (JWT), https://tools.ietf.org/html/rfc7519.

Les rubriques suivantes expliquent les méthodes pour obtenir et utiliser les jetons requis.

Survol du processus d'authentification du client API

Voici la vue de bout en bout de la façon d'authentifier votre client API auprès du dispositif Défense contre les menaces.



Avant de commencer

Chaque jeton représente une session de connexion HTTPS, qui compte pour les sessions API et les sessions gestionnaire d'appareil. Il peut y avoir un maximum de cinq sessions HTTPS actives. Si vous dépassez cette limite, la session la plus ancienne, la connexion au gestionnaire d'appareil ou le jeton API, expirera pour permettre la nouvelle session. Par conséquent, il est important que vous n'obteniez que les jetons dont vous avez besoin et que vous réutilisiez chaque jeton jusqu'à son expiration, pour ensuite les renouveler. L'obtention d'un nouveau jeton pour chaque appel d'API entraînera une perte de session importante et pourrait bloquer l'accès des utilisateurs au gestionnaire d'appareil. Ces limites ne s'appliquent pas aux sessions SSH.

Procédure

Étape 1 Authentifiez l'utilisateur du client API en utilisant la méthode dont vous avez besoin.

Votre client est tenu d'authentifier les utilisateurs et de s'assurer qu'ils sont autorisés à accéder au dispositif Défense contre les menaces. Si vous souhaitez fournir des capacités différentielles en fonction des droits d'autorisation, vous devez intégrer cette fonction à votre client.

Par exemple, si vous souhaitez autoriser l'accès en lecture seule, vous devez configurer le serveur d'authentification, les comptes d'utilisateurs et autres éléments requis. Ensuite, lorsqu'un utilisateur avec des droits en lecture seule se connecte à votre client, vous devez vous assurer d'émettre uniquement des appels GET. Dans la version v1 de l'API, ce type d'accès à une variable ne peut pas être contrôlé par le dispositif Défense contre les menaces lui-même. À partir de la version v2 de l'API, si vous utilisez des utilisateurs externes et que vous ne filtrez pas les appels en fonction de l'autorisation des utilisateurs, vous obtiendrez des erreurs en cas de non-concordance entre l'autorisation d'un utilisateur et les appels que vous tentez.

Pour la version v1, lorsque vous communiquez avec le dispositif, vous devez utiliser le compte d'utilisateur **admin** sur le dispositif Défense contre les menaces. Le compte **admin** dispose d'une autorisation complète de lecture/écriture pour tous les objets configurables par l'utilisateur.

Étape 2 Demandez un jeton d'accès attribué par mot de passe en fonction du nom d'utilisateur et du mot de passe à l'aide du compte **admin**.

Consultez Demander un jeton d'accès attribué par mot de passe, à la page 3.

Étape 3 Vous pouvez également demander un jeton d'accès personnalisé pour votre client.

Avec un jeton personnalisé, vous pouvez demander explicitement une période de validité et attribuer un nom de sujet au jeton. Consultez Demander un jeton d'accès personnalisé, à la page 5.

Étape 4 Utilisez le jeton d'accès sur les appels d'API dans l'en-tête Authorization: Bearer (Autorisation : porteur).

Consultez Utiliser un jeton d'accès sur les appels d'API, à la page 7.

Étape 5 Avant que le jeton d'accès expire, actualisez le jeton.

Consultez Renouveler un jeton d'accès, à la page 8.

Étape 6 Lorsque vous avez terminé, révoquez le jeton s'il n'a pas encore expiré.

Consultez Révoquer un jeton d'accès, à la page 9.

Demander un jeton d'accès attribué par mot de passe

Chaque appel de l'API REST doit inclure un jeton d'authentification pour vérifier que l'appelant est autorisé à effectuer l'action demandée. Initialement, vous devez obtenir un jeton d'accès en fournissant le nom d'utilisateur/mot de passe **admin**. Cela s'appelle un jeton d'accès accordé par mot de passe, c'est-à-dire que grant_type = password (type_d'octroi = mot de passe).

Procédure

Étape 1 Créez l'objet JSON pour l'octroi du jeton d'accès accordé par mot de passe.

```
{
  "grant_type": "password",
  "username": "string",
  "password": "string"
}
```

Précisez le nom d'utilisateur **admin** et le bon mot de passe, par exemple :

```
{
  "grant_type": "password",
  "username": "admin",
  "password": "Admin123"
}
```

Étape 2 Utilisez POST /fdm/token pour obtenir le jeton d'accès.

Par exemple, la commande **curl** ressemblerait à ce qui suit :

```
curl -X POST --header 'Content-Type: application/json' --header
'Accept: application/json' -d '{
   "grant_type": "password",
   "username": "admin",
   "password": "Admin123"
 }' 'https://ftd.example.com/api/fdm/dernière version/fdm/token'
```

Étape 3 Récupérez les jetons d'accès et de renouvellement de la réponse.

Une bonne réponse (code d'état 200) ressemble à ce qui suit :

```
{
  "access_token": "eyJhbGciOiJIUzI1NiJ9.eyJpYXQiOjE1MDI4MzI2NjcsInN
1YiI6ImFkbWluIiwianRpIjoiMGM3ZDBmNDgtODIwMS0xMWU3LWE4MWMtMDcwZmYzOW
U3ZjQ0IiwibmJmIjoxNTAyODMyNjY3LCJleHAiOjE1MDI4MzQ0NjcsInJlZnJlc2hU
b2tlbkV4cGlyZXNBdCI6MTUwMjgzNTA2NzQxOSwidG9rZW5UeXBlIjoiSldUX0FjY2
VzcyIsIm9yaWdpbiI6InBhc3N3b3JkIn0.b2hI6fVA_GbmhCOPM-ZUx6IC8SgCk1Ak
HXI-llV0r7s",
  "expires_in": 1800,
  "token_type": "Bearer",
  "refresh_token": "eyJhbGciOiJIUzI1NiJ9.eyJpYXQiOjE1MDI4MzI2NjcsI
nN1YiI6ImFkbWluIiwia nRpIjoiMGM3ZDBmNDgtODIwMS0xMWU3LWE4MWMtMDcwZmY
zOWU3ZjQ0IiwibmJmIjoxNTAyODMyNjY3LCJleHAiOjE1MDI4MzUwNjcsImFjY2Vzc1
Rva2VuRXhwaXJlc0F0IjoxNTAyODM0NDY3NDE5LCJyZWZyZXNoQ291bnQiOi0xLCJ0b2
tlblR5cGUiOiJKV1RfUmVmcmVzaCIsIm9yaWdpbiI6InBhc3N3b3JkIn0.iLNqz1c1Xl
vcq0j9pQYW4gwYsvUCcSyaiDRXGutAz_o",
  "refresh_expires_in": 2400
}
```

Lieu :

- **access_token** est le jeton-porteur que vous devez inclure dans les appels d'API. Consultez Utiliser un jeton d'accès sur les appels d'API, à la page 7.

- **expires_in** est le nombre de secondes pendant lesquelles le jeton d'accès est valide, à partir de l'émission de ce dernier.
- **refresh_token** est le jeton que vous utiliseriez pour une demande de renouvellement. Consultez Renouveler un jeton d'accès, à la page 8.
- **refresh_expires_in** est le nombre de secondes pendant lesquelles le jeton de renouvellement est valide. Ce nombre est toujours plus élevé que le nombre de secondes de la période de validité du jeton d'accès.

Demander un jeton d'accès personnalisé

Vous pouvez utiliser le jeton d'accès attribué par mot de passe. Cependant, vous pouvez également demander un jeton d'accès personnalisé. Avec un jeton personnalisé, vous pouvez fournir un nom de sujet pour différencier l'utilisation des jetons (pour votre référence ultérieure). Vous pouvez également demander des périodes de validité spécifiques si les valeurs par défaut renvoyées pour les jetons de mot de passe ne satisfont pas à vos exigences.

Avant de commencer

Vous devez d'abord obtenir un jeton d'accès attribué par mot de passe avant d'obtenir un jeton personnalisé. Consultez Demander un jeton d'accès attribué par mot de passe, à la page 3.

De plus :

- Vous pouvez demander un jeton personnalisé uniquement si vous êtes un utilisateur local. Les utilisateurs externes ne peuvent pas demander de jetons personnalisés.
- Vous pouvez utiliser un jeton personnalisé sur l'unité pour laquelle vous l'obtenez uniquement. Vous ne pouvez pas utiliser le jeton sur l'appareil homologue dans un groupe à haute disponibilité.

Procédure

Étape 1 Créez l'objet JSON pour l'octroi du jeton d'accès personnalisé.

```
{
  "grant_type": "custom_token",
  "access_token": "string",
  "desired_expires_in": 0,
  "desired_refresh_expires_in": 0,
  "desired_subject": "string",
  "desired_refresh_count": 0
}
```

Lieu :

- **access_token** est un jeton d'accès attribué par mot de passe valide.

- **desired_expires_in** est un entier représentant le nombre de secondes pendant lesquelles le jeton d'accès personnalisé sera valide. En comparaison, les jetons attribués par mot de passe sont valides pendant 1800 secondes.
- **desired_refresh_expires_in** est un entier représentant le nombre de secondes pendant lesquelles le jeton d'actualisation personnalisé sera valide. Si vous obtenez un jeton d'actualisation, assurez-vous que cette valeur est supérieure à la valeur **desired_expires_in**. En comparaison, les jetons d'actualisation attribués par mot de passe sont valides pendant 2400 secondes. Ce paramètre n'est pas obligatoire si vous spécifiez 0 pour **desired_refresh_count**.
- **desired_subject** est un nom que vous attribuez au jeton personnalisé.
- **desired_refresh_count** est le nombre de fois où vous souhaitez pouvoir actualiser le jeton. Précisez 0 si vous ne souhaitez pas obtenir de jeton d'actualisation. Si vous n'avez pas de jeton d'actualisation, vous devez obtenir un nouveau jeton d'accès lorsque le jeton existant expire.

Par exemple, l'option suivante demande un jeton personnalisé pour api-client qui expire après 2400 secondes, avec un jeton d'actualisation qui expire après 3000 secondes. Le jeton peut être actualisé trois fois.

```
{{
  "grant_type": "custom_token",
  "access_token": "eyJhbGciOiJIUzI1NiJ9.eyJpYXQiOjE1MDI4MzI2NjcsInN
1YiI6ImFkbWluIiwianRpIjoiMGM3ZDBmNDgtODIwMS0xMWU3LWE4MWMtMDcwZmYzOW
U3ZjQ0IiwibmJmIjoxNTAyODMyNjY3LCJleHAiOjE1MDI4MzQ0NjcsInJlZnJlc2hU
b2tlbkV4cGlyZXNBdCI6MTUwMjgzNTA2NzQxOSwidG9rZW5UeXBlIjoiSldUX0FjY2
VzcyIsIm9yaWdpbiI6InBhc3N3b3JkIn0.b2hI6fVA_GbmhCOPM-ZUx6IC8SgCk1Ak
HXI-llV0r7s",
  "desired_expires_in": 2400,
  "desired_refresh_expires_in": 3000,
  "desired_subject": "api-client",
  "desired_refresh_count": 3
}
```

Étape 2 Utilisez POST /fdm/token pour obtenir le jeton d'accès.

Par exemple, la commande **curl** ressemblerait à ce qui suit :

```
curl -X POST --header 'Content-Type: application/json' --header
'Accept: application/json' -d '{
   "grant_type": "custom_token",
   "access_token": "eyJhbGciOiJIUzI1NiJ9.eyJpYXQiOjE1MDI4MzU5N
jgsInN1YiI6ImFkbWluIiwianRpIjoiYmMyNjM4N2EtODIwOC0xMWU3LWE4MWM
tYzNlYTZkZjJjZThjIiwibmJmIjoxNTAyODM1OTY4LCJleHAiOjE1MDI4Mzc3N
jgsInJlZnJlc2hUb2tlbkV4cGlyZXNBdCI6MTUwMjgzODM2ODYwNiwidG9rZW5
UeXBlIjoiSldUX0FjY2VzcyIsIm9yaWdpbiI6InBhc3N3b3JkIn0.acOE_Y4SE
ds-NE4Qw99fQlUzdoSkhsjInaCh0a9WK38",
   "desired_expires_in": 2400,
   "desired_refresh_expires_in": 3000,
   "desired_subject": "api-client",
   "desired_refresh_count": 3
 }' 'https://ftd.example.com/api/fdm/dernière version/fdm/token'
```

Étape 3 Récupérez les jetons d'accès et de renouvellement de la réponse.

Une bonne réponse (code d'état 200) ressemble à ce qui suit :

```
{
```

```
  "access_token": "eyJhbGciOiJIUzI1NiJ9.eyJpYXQiOjE1MDI4MzU5O
TEsInN1YiI6ImFwaS1jbGllbnQiLCJqdGkiOiJjOWIxYzdjYi04MjA4LTExZT
ctYTgxYy02YmY0NzY3ZmRmZGUiLCJuYmYiOjE1MDI4MzU5OTEsImV4cCI6MTU
wMjgzODM5MSwicmVmcmVzaFRva2VuRXhwaXJlc0F0IjoxNTAyODM4OTkxMzMx
LCJ0b2tlblR5cGUiOiJKV1RfQWNjZXNzIiwib3JpZ2luIjoiY3VzdG9tIn0.9
IVzLjGffVQffHAWdrNkrYfvuO6TgpJ7Zi_z3RYubN8",
  "expires_in": 2400,
  "token_type": "Bearer",
  "refresh_token": "eyJhbGciOiJIUzI1NiJ9.eyJpYXQiOjE1MDI4MzU5
OTEsInN1YiI6ImFwaS1jbGllbnQiLCJqdGkiOiJjOWIxYzdjYi04MjA4LTExZ
TctYTgxYy02YmY0NzY3ZmRmZGUiLCJuYmYiOjE1MDI4MzU5OTEsImV4cCI6MT
UwMjgzODk5MSwiYWNjZXNzVG9rZW5FeHBpcmVzQXQiOjE1MDI4MzgzOTEzMzE
sInJlZnJlc2hDb3VudCI6MywidG9rZW5UeXBlIjoiSldUX1JlZnJlc2giLCJv
cmlnaW4iOiJjdXN0b20ifQ.qseqjg3Uo183YvfN_77iJZELEqwpWw5AbKAqAn
CIcSA",
  "refresh_expires_in": 3000
}
```


Lieu :

- **access_token** est le jeton-porteur que vous devez inclure dans les appels d'API. Consultez Utiliser un jeton d'accès sur les appels d'API, à la page 7.
- **expires_in** est le nombre de secondes pendant lesquelles le jeton d'accès est valide, à partir de l'émission de ce dernier.
- **refresh_token** est le jeton que vous utiliseriez pour une demande de renouvellement. Consultez Renouveler un jeton d'accès, à la page 8.
- **refresh_expires_in** est le nombre de secondes pendant lesquelles le jeton de renouvellement est valide. Ce nombre est toujours plus élevé que le nombre de secondes de la période de validité du jeton d'accès.

Utiliser un jeton d'accès sur les appels d'API

Après avoir obtenu un jeton d'accès personnalisé ou par mot de passe, vous devez l'inclure sur chaque appel d'API dans l'en-tête **Authorization: Bearer** (Autorisation : porteur) de la demande HTTPS.

Par exemple, une commande **curl** pour lancer une méthode GET /object/networks pourrait ressembler à ce qui suit :


```
curl -k -X GET -H 'Accept: application/json'
-H 'Authorization: Bearer eyJhbGciOiJIUzI1NiJ9.yJp
YXQiOjE1MDI4MzU5OTEsInN1YiI6ImFwaS1jbGllbnQiLCJqdG
kiOiJjOWIxYzdjYi04MjA4LTExZTctYTgxYy02YmY0NzY3ZmRm
ZGUiLCJuYmYiOjE1MDI4MzU5OTEsImV4cCI6MTUwMjgzODM5MS
wicmVmcmVzaFRva2VuRXhwaXJlc0F0IjoxNTAyODM4OTkxMzMx
LCJ0b2tlblR5cGUiOiJKV1RfQWNjZXNzIiwib3JpZ2luIjoiY3
VzdG9tIn0.9IVzLjGffVQffHAWdrNkrYfvuO6TgpJ7Zi_z3RYu
bN8'
'https://ftd.example.com/api/fdm/dernière version/object/networks'
```

Remarque Lorsque vous utilisez l'explorateur d'interface de protocole d'application pour essayer des méthodes et des ressources, la commande **curl** affichée n'inclut pas l'en-tête **Authorization: Bearer** (Autorisation : porteur). Cependant, vous devez ajouter cet en-tête lorsque vous passez des appels à partir de votre client API.

Renouveler un jeton d'accès

Après l'expiration d'un jeton d'accès, vous devez le renouveler à l'aide du jeton de renouvellement qui a été fourni lors de l'octroi d'origine. Le jeton d'accès renouvelé est en fait différent du jeton d'accès d'origine. Lors du renouvellement, une nouvelle paire de jetons d'accès et de jetons de renouvellement est fournie. Ce processus ne fait pas que prolonger tout simplement la durée de vie de l'ancien jeton d'accès.

Procédure

Étape 1 Créez l'objet JSON pour l'octroi de jeton de renouvellement.

```
{
  "grant_type": "refresh_token",
  "refresh_token": "string"
}
```

Le **refresh_token** peut provenir d'un octroi par mot de passe ou par jeton d'accès.

Par exemple :

```
{
  "grant_type": "refresh_token",
  "refresh_token": "eyJhbGciOiJIUzI1NiJ9.eyJpYXQ
iOjE1MDI4MzU5OTEsInN1YiI6ImFwaS1jbGllbnQiLCJqdGk
iOiJjOWIxYzdjYi04MjA4LTExZTctYTgxYy02YmY0NzY3ZmR
mZGUiLCJuYmYiOjE1MDI4MzU5OTEsImV4cCI6MTUwMjgzODk
5MSwiYWNjZXNzVG9rZW5FeHBpcmVzQXQiOjE1MDI4MzgzOTE
zMzEsInJlZnJlc2hDb3VudCI6MywidG9rZW5UeXBlIjoiSld
UX1JlZnJlc2giLCJvcmlnaW4iOiJjdXN0b20ifQ.qseqjg3U
o183YvfN_77iJZELEqwpWw5AbKAqAnCIcSA"
}
```

Étape 2 Utilisez POST /fdm/token pour obtenir le jeton d'accès renouvelé.

Par exemple, la commande **curl** ressemblerait à ce qui suit :

```
curl -X POST --header 'Content-Type: application/json' --header
'Accept: application/json' -d '{
   "grant_type": "refresh_token",
   "refresh_token": "eyJhbGciOiJIUzI1NiJ9.eyJpYXQiOjE1M
DI4MzU5OTEsInN1YiI6ImFwaS1jbGllbnQiLCJqdGkiOiJjOWIxYzdj
Yi04MjA4LTExZTctYTgxYy02YmY0NzY3ZmRmZGUiLCJuYmYiOjE1MDI
4MzU5OTEsImV4cCI6MTUwMjgzODk5MSwiYWNjZXNzVG9rZW5FeHBpcm
VzQXQiOjE1MDI4MzgzOTEzMzEsInJlZnJlc2hDb3VudCI6MywidG9rZ
W5UeXBlIjoiSldUX1JlZnJlc2giLCJvcmlnaW4iOiJjdXN0b20ifQ.q
```

```
seqjg3Uo183YvfN_77iJZELEqwpWw5AbKAqAnCIcSA"
 }' 'https://ftd.example.com/api/fdm/dernière version/fdm/token'
```

Étape 3 Récupérez les jetons d'accès et de renouvellement de la réponse.

Une bonne réponse (code d'état 200) ressemble à ce qui suit. Dans cet exemple, le jeton de renouvellement était pour un jeton personnalisé. Les périodes d'expiration sont basées sur les valeurs de la demande de jeton d'accès personnalisé initiale.

```
{
  "access_token": "eyJhbGciOiJIUzI1NiJ9.eyJpYXQ
iOjE1MDI4Mzc1MTAsInN1YiI6ImFwaS1jbGllbnQiLCJqdG
kiOiJjOWIxYzdjYi04MjA4LTExZTctYTgxYy02YmY0NzY3Z
mRmZGUiLCJuYmYiOjE1MDI4Mzc1MTAsImV4cCI6MTUwMjgz
OTkxMSwicmVmcmVzaFRva2VuRXhwaXJlc0F0IjoxNTAyODQ
wNTEwNzQxLCJ0b2tlblR5cGUiOiJKV1RfQWNjZXNzIiwib3
JpZ2luIjoiY3VzdG9tIn0.fAAreX0DdnuqnM0Bs0NXYnI-9
jkpyW1pWDMwgwO_h7A",
  "expires_in": 2400,
  "token_type": "Bearer",
  "refresh_token": "eyJhbGciOiJIUzI1NiJ9.eyJpYX
QiOjE1MDI4Mzc1MTAsInN1YiI6ImFwaS1jbGllbnQiLCJqd
GkiOiJjOWIxYzdjYi04MjA4LTExZTctYTgxYy02YmY0NzY3
ZmRmZGUiLCJuYmYiOjE1MDI4Mzc1MTAsImV4cCI6MTUwMjg
0MDUxMCwiYWNjZXNzVG9rZW5FeHBpcmVzQXQiOjE1MDI4Mz
k5MTEwNzIsInJlZnJlc2hDb3VudCI6MiwidG9rZW5UeXBlI
joiSldUX1JlZnJlc2giLCJvcmlnaW4iOiJjdXN0b20ifQ.p
Adc2N0oun7Yyw872qK12pFlix4arAwyMETD1ErKu5c",
  "refresh_expires_in": 3000
}
```

Lieu :

- **access_token** est le jeton-porteur que vous devez inclure dans les appels d'API. Consultez Utiliser un jeton d'accès sur les appels d'API, à la page 7.
- **expires_in** est le nombre de secondes pendant lesquelles le jeton d'accès est valide, à partir de l'émission de ce dernier.
- **refresh_token** est le jeton que vous utiliseriez pour une demande de renouvellement.
- **refresh_expires_in** est le nombre de secondes pendant lesquelles le jeton de renouvellement est valide. Ce nombre est toujours plus élevé que le nombre de secondes de la période de validité du jeton d'accès.

Révoquer un jeton d'accès

Comme les jetons d'accès sont valides pour une durée donnée, vous devez nettoyer votre système en révoquant un jeton lorsque l'utilisateur se déconnecte de votre client API. Ainsi, vous vous assurez qu'aucune porte d'entrée vulnérable n'est laissée ouverte pour le dispositif Défense contre les menaces.

Procédure

Étape 1 Créez l'objet JSON pour l'octroi de jeton de révocation.

```
{
  "grant_type": "revoke_token",
  "access_token": "string",
  "token_to_revoke": "string",
  "custom_token_id_to_revoke": "string",
  "custom_token_subject_to_revoke": "string"
}
```

Lieu :

- **access_token** doit être un jeton d'accès attribué par mot de passe. Vous ne pouvez pas révoquer un jeton en utilisant un jeton d'accès personnalisé.
- Vous devez spécifier une et une seule des options suivantes :
  - **token_to_revoke** est un jeton attribué par mot de passe ou un jeton personnalisé que vous souhaitez révoquer. Il peut s'agir du même jeton que **access_token**, vous pouvez donc utiliser un jeton attribué par mot de passe pour le révoquer.
  - (Ne pas utiliser.) **custom_token_id_to_revoke** identifie le jeton d'accès personnalisé par son identifiant unique interne. Cependant, il n'y a aucun moyen direct par lequel vous pouvez obtenir cette valeur. Utilisez plutôt les autres options.
  - **custom_token_subject_to_revoke** est la valeur **desired_subject** du jeton d'accès personnalisé que vous souhaitez révoquer.

Par exemple :

```
{
  "grant_type": "revoke_token",
  "access_token": "eyJhbGciOiJIUzI1NiJ9.eyJpYXQ
iOjE1MDI5MDQzMjQsInN1YiI6ImFkbWluIiwianRpIjoiZT
MzNGIxOWYtODJhNy0xMWU3LWE4MWMtNGQ3NzY2ZTExMzVkI
iwibmJmIjoxNTAyOTA0MzI0LCJleHAiOjE1MDI5MDYxMjQs
InJlZnJlc2hUb2tlbkV4cGlyZXNBdCI6MTUwMjkwNjcyNDE
xMiwidG9rZW5UeXBlIjoiSldUX0FjY2VzcyIsIm9yaWdpbi
I6InBhc3N3b3JkIn0.OVZBT9yVZc4zxZfZiiLH4SZcFclaH
yCPbZJC_Gyd5FE",
  "custom_token_subject_to_revoke": "api-client"
}
```

Étape 2 Utilisez POST /fdm/token pour révoquer le jeton d'accès.

Par exemple, la commande **curl** ressemblerait à ce qui suit :

```
curl -X POST --header 'Content-Type: application/json'
--header 'Accept: application/json' -d '{
   "grant_type": "revoke_token",
   "access_token": "eyJhbGciOiJIUzI1NiJ9.eyJpYXQ
iOjE1MDI5MDQzMjQsInN1YiI6ImFkbWluIiwianRpIjoiZTM
```

```
zNGIxOWYtODJhNy0xMWU3LWE4MWMtNGQ3NzY2ZTExMzVkIiw
ibmJmIjoxNTAyOTA0MzI0LCJleHAiOjE1MDI5MDYxMjQsInJ
lZnJlc2hUb2tlbkV4cGlyZXNBdCI6MTUwMjkwNjcyNDExMiw
idG9rZW5UeXBlIjoiSldUX0FjY2VzcyIsIm9yaWdpbiI6InB
hc3N3b3JkIn0.OVZBT9yVZc4zxZfZiiLH4SZcFclaHyCPbZJ
C_Gyd5FE",
   "custom_token_subject_to_revoke": "api-client"
 }' 'https://ftd.example.com/api/fdm/dernière version/fdm/token'
```

Étape 3 Évaluez la réponse pour vérifier que le jeton a été révoqué.

Une bonne réponse (code d'état 200) ressemble à ce qui suit.

```
{
  "message": "OK",
  "status_code": 200
}
```

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.