使用 OAuth 对 REST API 客户端进行身份验证

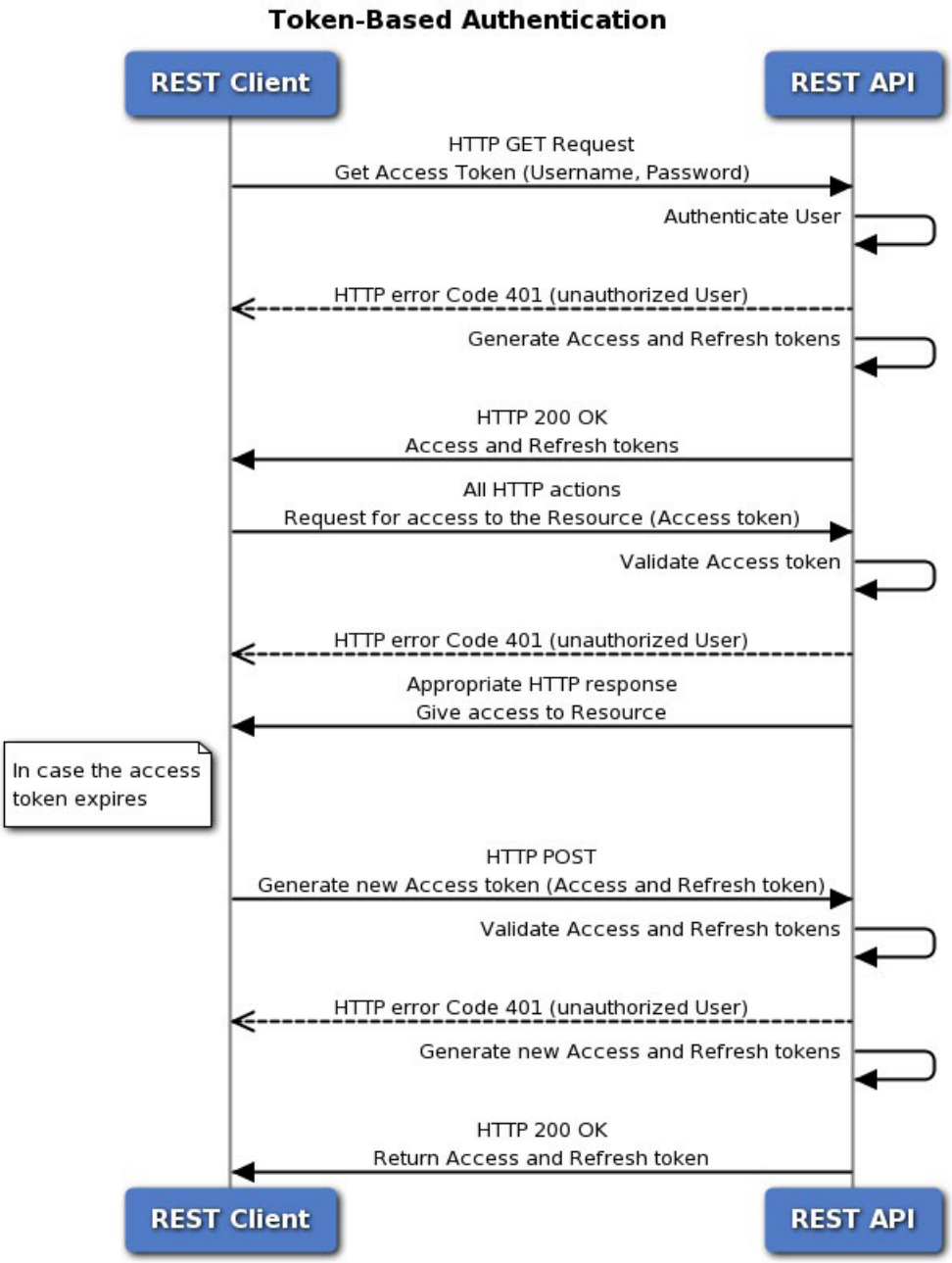
威胁防御 REST API 使用 Oauth 2.0 对来自 API 客户端的调用进行身份验证。OAuth 是一种基于访问令牌的方法，且 威胁防御 将 JSON Web 令牌用于此方案。相关标准如下：

- RFC6749，OAuth 2.0 授权框架，https://tools.ietf.org/html/rfc6749。
- RFC7519，JSON Web 令牌 (JWT)，https://tools.ietf.org/html/rfc7519。

以下主题介绍获取和使用所需令牌的方法。

API 客户端身份验证过程概述

以下是如何使用威胁防御设备对 API 客户端进行身份验证的全方位解析。



开始之前

每个令牌代表一个 HTTPS 登录会话，该会话计入 API 会话和 设备管理器 会话。最多可以有 5 个活动 HTTPS 会话。如果超过此限制，则最早的会话（设备管理器 登录或 API 令牌）将过期以允许建立新会话。因此，重要的是，您只能获取所需的令牌，并重复使用每个令牌直到其到期，然后续约。为每个 API 调用获取新令牌将导致严重的会话中断，并可能使用户无法访问 设备管理器。这些限制不适用于 SSH 会话。

过程

步骤 1 使用所需的方法对 API 客户端用户进行身份验证。

您的客户端有义务对用户进行身份验证，并确保其有权访问和修改威胁防御 设备。如果希望根据授权权限提供不同的功能，则需要将其构建到客户端中。

例如，如果希望允许只读访问，则必须设置所需的身份验证服务器、用户账户等。然后，当拥有只读权限的用户登录客户端时，必须确保只发出 GET 调用。在 API v1 中，这种类型的变量访问不能由 威胁防御 设备自身控制。自 API v2 起，如果您使用外部用户且未根据用户授权修整调用，那么如果用户授权和尝试的调用之间不匹配，系统会出错。

在 v1 中，与设备通信时，必须在 威胁防御 设备上使用 **admin** 用户账户。**管理员**账户对所有用户可配置的对象拥有完全的读/写授权权限。

步骤 2 使用**管理员**账户，根据用户名/密码请求密码授予的访问令牌。

请参阅请求密码授予的访问令牌，第 3 页。

步骤 3 或者，为客户端请求自定义访问令牌。

使用自定义令牌，可以明确为该令牌请求一个有效期并分配一个使用者名称。请参阅请求自定义访问令牌，第 5 页。

步骤 4 在“授权：无记名”报头中使用 API 调用的访问令牌。

请参阅在 API 调用中使用访问令牌，第 7 页。

步骤 5 在访问令牌到期之前，刷新该令牌。

请参阅刷新访问令牌，第 7 页。

步骤 6 完成后，如果令牌尚未过期，系统将撤销该令牌。

请参阅撤销访问令牌，第 9 页。

请求密码授予的访问令牌

每个 REST API 调用都必须包括一个身份验证令牌，以验证调用方是否被授权执行请求的操作。最初，需要通过提供**管理员**用户名/密码获取访问令牌。这被称为密码授予的访问令牌，即 grant_type = 密码。

过程

步骤 1 为密码授予的访问令牌授权创建 JSON 对象。

```
{
```

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

指定**管理员**用户名和正确的密码，例如:

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

步骤 2 使用 POST /fdm/token 获取访问令牌。

例如，**curl** 命令将如下所示：

```
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/最新/fdm/token'
```

步骤 3 从响应中检索访问令牌和刷新令牌。

良好响应（状态代码 200）如下所示：

```
{
  "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
}
```

其中：

- **access_token** 是需要包含在 API 调用中的不记名令牌。请参阅在 API 调用中使用访问令牌，第 7 页。
- **expires_in** 是访问令牌自颁发时起的有效时间（单位：秒）。
- **refresh_token** 是用于刷新请求的令牌。请参阅刷新访问令牌，第 7 页。

- **refresh_expires**_in 是刷新令牌的有效时间（单位：秒）。此时间总是比访问令牌有效时间长。

请求自定义访问令牌

可以使用密码授予的访问令牌。但是，也可请求自定义访问令牌。使用自定义令牌，可以提供一个使用者名称，以帮助区分令牌用途（用于您的自身目的）。如果密码令牌返回的默认值不满足要求，也可请求特定的有效期。

开始之前

在获取自定义令牌之前，必须先获取密码授予的访问令牌。请参阅请求密码授予的访问令牌，第 3 页。

此外：

- 仅当您是本地用户时，您才可以请求自定义令牌。外部用户无法请求自定义令牌。
- 您仅可在为其获取令牌的设备上使用此自定义令牌。您不能在高可用性组中的对等设备上使用此令牌。

过程

步骤 1 为自定义访问令牌授权创建 JSON 对象。

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

其中：

- **access_token** 是有效的密码授予的访问令牌。
- **desired_expires_in** 是一个整数，表示自定义访问令牌的有效秒数。相比之下，密码授予的令牌有效期为 1800 秒。
- **desired_refresh_expires_in** 是一个整数，表示自定义刷新令牌的有效秒数。如果获得刷新令牌，请确保此值大于 **desired_expires_in** 值。相比之下，密码授予的刷新令牌有效期为 2400 秒。如果为 **desired_refresh_count** 指定 0，则不需要此参数。
- **desired_subject** 是为自定义令牌提供的名称。

- **desired_refresh_count** 是希望可以刷新令牌的次数。如果不希望获得刷新令牌，请指定 0。如果没有刷新令牌，则当现有访问令牌过期时，必须获取新的访问令牌。

例如，以下命令用于请求 API 客户端的自定义令牌（在 2400 秒后过期）和刷新令牌（在 3000 秒后过期）。该令牌可以刷新 3 次。

```
{{
  "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
}
```

步骤 2 使用 POST /fdm/token 获取访问令牌。

例如，**curl** 命令将如下所示：

```
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/最新/fdm/token'
```

步骤 3 从响应中检索访问令牌和刷新令牌。

良好响应（状态代码 200）如下所示：

```
{
  "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
}
```

其中：

- **access_token** 是需要包含在 API 调用中的不记名令牌。请参阅在 API 调用中使用访问令牌，第 7 页。
- **expires_in** 是访问令牌自颁发时起的有效时间（单位：秒）。
- **refresh_token** 是用于刷新请求的令牌。请参阅刷新访问令牌，第 7 页。
- **refresh_expires**_in 是刷新令牌的有效时间（单位：秒）。此时间总是比访问令牌有效时间长。

在 API 调用中使用访问令牌

获得密码授予的或自定义访问令牌后，必须在各 API 调用上将其纳入 HTTPS 请求的**授权：不记名**报头中。

例如，执行 GET /object/networks 的 **curl** 命令可能如下所示：

```
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/最新/object/networks'
```

注释 使用 API Explorer 尝试方法和资源时，所示的 **curl** 命令不包括**授权：不记名**报头。但是，从 API 客户端进行调用时，必须添加此报头。

刷新访问令牌

访问令牌到期后，需要使用原始授权中提供的刷新令牌来进行刷新。刷新后的访问令牌实际上与原始访问令牌有所不同。“刷新”实际上提供了一对新的访问令牌和刷新令牌，不仅仅是延长了旧访问令牌的使用时间。

过程

步骤 1 为刷新令牌授权创建 JSON 对象。

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

refresh_token 可能来自密码授予的访问令牌或自定义访问令牌授权。

例如：

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

步骤 2 使用 POST /fdm/token 获取刷新后的访问令牌。

例如，**curl** 命令将如下所示：

```
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/最新/fdm/token'
```

步骤 3 从响应中检索访问令牌和刷新令牌。

良好响应（状态代码 200）如下所示。在此示例中，刷新令牌用于自定义令牌。过期期限基于原始自定义访问令牌请求的值。

```
{
  "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
}
```


其中：

- **access_token** 是需要包含在 API 调用中的不记名令牌。请参阅在 API 调用中使用访问令牌，第 7 页。
- **expires_in** 是访问令牌自颁发时起的有效时间（单位：秒）。
- **refresh_token** 是用于刷新请求的令牌。
- **refresh_expires**_in 是刷新令牌的有效时间（单位：秒）。此时间总是比访问令牌有效时间长。

撤销访问令牌

由于访问令牌在特定时间段内有效，因此在用户注销 API 客户端时，应通过撤销令牌来进行清理。这样可以确保没有后门通向 威胁防御 设备。

过程

步骤 1 为撤销令牌授权创建 JSON 对象。

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

其中：

- **access_token** 必须为密码授予的访问令牌。不能使用自定义访问令牌撤销令牌。
- 必须指定以下内容中的一个，且只可指定一个：
  - **token_to_revoke** 是要撤销的密码授予的令牌或自定义令牌。这可以与 **access_token** 的令牌相同，因此可以使用密码授予的令牌来自行撤销。

- (不使用。)**custom_token_id_to_revoke** 通过内部唯一 ID 标识自定义访问令牌。但是，无法直接获取该值。请使用其他选项。
- **custom_token_subject_to_revoke** 是要撤销的自定义访问令牌的 **desired_subject** 值。

例如：

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

步骤 2 使用 POST /fdm/token 撤销访问令牌。

例如，**curl** 命令将如下所示：

```
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/最新/fdm/token'
```

步骤 3 评估响应以验证令牌是否已撤销。

良好响应（状态代码 200）如下所示。

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

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。