tangoe

# **Mobile Procurement REST API (MOBPROC)**:

*Access Tokens*

June 9, 2017

Tangoe, Inc.

35 Executive Blvd.

Orange, CT 06477

+1.203.859.9300

www.tangoe.com

## TABLE OF CONTENTS

**HOW TO REQUEST AN ACCESS TOKEN USING THE PASSWORD GRANT TYPE 2**

Endpoints ..... 2
Request Query Parameters ..... 3
Example ..... 4

**HOW TO REFRESH AN ACCESS TOKEN ..... 5**

Endpoints ..... 5
Request Query Parameters ..... 5
Example ..... 6

**HOW TO VALIDATE AN ACCESS TOKEN ..... 8**

Endpoints ..... 8
Request Query Parameters ..... 8
Example ..... 8

This document includes instructions for managing the access token needed in order to access the MOBPROC API using OAuth (PingFederate). Specifically:

- How to Request an Access Token using the Password grant type
- How to Refresh an Access Token
- How to Validate an Access Token

# HOW TO REQUEST AN ACCESS TOKEN USING THE PASSWORD GRANT TYPE

*NOTE: This tutorial assumes that you are using a client ID and client secret for an API client application that is configured to allow **Resource Owner Password Credentials** as one of its **Allowed Grant Types** configured in PingFederate.*

For server-to-server scenarios, it is appropriate to use the **password** grant type when getting an access token for use with Tangoe APIs. When using the **password** grant type, the following information is required:

- **client_id:** Client ID assigned to your API client application.
- **client_secret:** Client secret assigned to your API client application.
- **scope:** OAuth scope(s) required for the API you are using.
- **username:** Username for the Tangoe service account to be associated with the access token being created.
- **password:** Password for this service account.

## Endpoints

An access token is requested by making an HTTP POST to our Ping authentication endpoint. The specific endpoint used will depend upon your instance's environment type:

- For **Production**: https://oauth.tangoe.com/as/token.oauth2
- For **QA**: https://oauthqa.tangoe.com/as/token.oauth2

*NOTE: Although a unique client ID/client secret pair can be used to access multiple APIs, they are always assigned per environment. Therefore, a client ID/secret pair that is valid for one environment will not work for another environment.*

## Request Query Parameters

To get an access token, POST to the appropriate URL (above) for the type of environment your instance is using. The following query parameters need to be passed with this POST request:

| Query Parameter | Description | Example |
|---|---|---|
| grant_type | Always set to *password*. | `password` |
| client_id | Tangoe-assigned client ID for your specific API client application. | `376af94124f4400e9227c89937c12354` |
| client_secret | Tangoe-assigned client secret for your API client application. | `81f40d2777ea4a41A992535F17AC92EC` |
| scope | OAuth scope that is required for the API being called. | For the MOBPROC REST API, use `MOBPROC`. |
| username | Username for the Tangoe service account to be associated with the access token being created. This username must be formatted as follows:<br>`<source_system>://<username>`<br>The source system will be either: `command` or `rivermine`<br>If the source system is a user on the Tangoe platform, then simply enter the username without prepending `<source_system>://` | `command://myusername` |
| password | Password associated with the username above. | `mypassword` |

## Example

The following is an example of a POST request to get a token:

```
https://oauthqa.tangoe.com/as/token.oauth2?grant_type=password&client_id=376af94124f4400e9227c89937c12354&client_secret=81f40d2777ea4a41A992535F17AC92EC&scope=MOBPROC&username=command://myusername&password=mypassword
```

The following is an example of a response that might be returned:

```
{
 "token_type": "Bearer",
 "expires_in": 7199,
 "refresh_token": "a9AhNvcffquYkV4bSw0O6gt4gKZRvTUGR2lfR8nJf4",
 "access_token": "ts5grB07RB2GHAuOs67tJ4zJjV1R"
}
```

The following properties are returned in the access token response:

| Property | Description | Example |
|---|---|---|
| token_type | Our tokens will always be set to `Bearer`. | `Bearer` |
| expires_in | Number of seconds for which the access token will be valid. | `7199` |
| access_token | The actual access token to be used when making an API call. | `a9AhNvcffquYkV4bSw0O6gt4gKZRvTUGR2lfR8nJf4` |
| refresh_token | The refresh token used to refresh an existing access token. | `ts5grB07RB2GHAuOs67tJ4zJjV1R` |

# How to Refresh an Access Token

*NOTE: This tutorial assumes that you are using a client ID and client secret for an API client application that is configured to allow **Refresh Token** as one of its **Allowed Grant Types** configured in PingFederate.*

The following information is required to refresh an access token:

- **client_id:** Client ID assigned to your API client application.
- **client_secret:** Client secret assigned to your API client application.
- **scope:** OAuth scope(s) required for the API you are using.
- **refresh_token:** The refresh token that was obtained when the access token was created.

## Endpoints

An access token is refreshed by making an HTTP POST to our Ping authentication endpoint. The specific endpoint used will depend upon your instance's environment type:

- For **Production**: https://oauth.tangoe.com/as/token.oauth2
- For **QA**: https://oauthqa.tangoe.com/as/token.oauth2

*NOTE: Although a unique client ID/client secret pair can be used to access multiple APIs, they are always assigned per environment. Therefore, a client ID/secret pair that is valid for one environment will not work for another environment.*

## Request Query Parameters

To refresh an access token, the following query parameters must be passed with this POST request:

| Query Parameter | Description | Example |
|---|---|---|
| grant_type | Always set to *refresh_token*. | `refresh_token` |
| client_id | Tangoe-assigned client ID for your specific API client application. | `376af94124f4400e9227c89937c12354` |

| Query Parameter | Description | Example |
|---|---|---|
| client_secret | Tangoe-assigned client secret for your API client application. | `81f40d2777ea4a41A992535F17AC92EC` |
| scope | OAuth scope that is required for the API being called. | For the MOBPROC REST API, use `MOBPROC`. |
| refresh_token | The refresh token that was associated with the access token that was previously created. | `a9AhNvcffquYkV4bSw0O6gt4gKZRvTUGR2lfR8nJf4` |

## Example

The following is an example of a POST request to get a token:

```
https://oauthqa.tangoe.com/as/token.oauth2?grant_type=refresh_token&client_id=376af94124f4400e9227c89937c12354&client_secret=81f40d2777ea4a41A992535F17AC92EC&scope=MOBPROC&refresh_token=a9AhNvcffquYkV4bSw0O6gt4gKZRvTUGR2lfR8nJf4
```

The following is an example of a response that might be returned:

```
{
  "token_type": "Bearer",
  "expires_in": 7200,
  "refresh_token": "wBzXpMnRjAyiLMDrn0vmhnO89pMbm22WJVXuf0RazH",
  "access_token": "Ql0mwXlo8lWHmczeiopaDt5rLMTO"
}
```

The following four properties are returned in the newly-refreshed access token response:

| Property | Description | Example |
|---|---|---|
| token_type | Our tokens will always be set to `Bearer`. | `Bearer` |
| expires_in | Number of seconds for which the access token will be valid. | `7200` |
| access_token | The actual access token to be used when making an API call. | `wBzXpMnRjAyiLMDrn0vmhnO89pMbm22WJVXuf0RazH` |
| refresh_token | The refresh token used to refresh an existing access token. | `Ql0mwXlo8lWHmczeiopaDt5rLMTO` |

# How to Validate an Access Token

The following information is required to validate an access token:

- **access_token:** The access token to be validated.

## Endpoints

An access token is validated by making an HTTP GET to our validation endpoint. The specific endpoint used will depend upon your instance's environment type:

- For **Production**: http://tngo-prod-oauth-ping-validator.cloudhub.io
- For **QA**: http://tngo-qa-oauth-ping-validator.cloudhub.io

## Request Query Parameters

To validate an access token, the following query parameters must be passed with this GET request:

| Query Parameter | Description | Example |
|---|---|---|
| access_token | The access token to be validated. | `jf8ANPs5ETFT1RPnfJnZpbcWjz2f` |

## Example

The following is an example of a GET request to validate a token:

```
https://oauthqa.tangoe.com/as/token.oauth2?grant_type=refresh_token&client_id=376af94124f4400e9227c89937c12354&client_secret=81f40d2777ea4a41A992535F17AC92EC&scope=MOBPROC&refresh_token=a9AhNvcffquYkV4bSw0O6gt4gKZRvTUGR2lfR8nJf4
```

The following is an example of a response that might be returned:


```
{
  "expires_in": 7188,
  "scope": "MOBPROC",
  "client_id": "a98b70cddd5f1432221360bd732f5ec1",
  "username": "sn2.admin.xx1",
  "platform": "command",
  "identityProvider": "pcv_edge"
}
```


The following properties are returned in the token validation response:

| Property | Description | Example |
|---|---|---|
| expires_in | Number of seconds that the access token will be valid. | `7188` |
| scope | OAuth scopes that are associated with the access token being validated. | `MOBPROC` |
| client_id | Tangoe-assigned client ID for the API client application that requested the access token being validated. | `a98b70cddd5f1432221360bd732f5ec1` |
| username | Username that is associated with the access token. | `sn2.admin.xx1` |
| platform | Source system that is associated with the access token. | `command` |
| identityProvider | Identifies the authenticating entity. | `pcv_edge` |