

Datto Disaster Tracking

Mock Design/Architecture Document

Masters of Disaster

Nsama Chipalo, Brandon Cole, Aaron Damrau, Jhossue Jimenez, Jacob Peterson

Last Updated

May 11th, 2015

Purpose

Due to constraints on the resources Datto currently has available, the team has decided to implement several of the systems they will provide for production as mock systems. This will allow us to be better prepared come integration time with Datto's systems. The OAuth Server, Devices API, MSP Credentials database, and Datto Devices database will all be created on our end to mimic the Datto implementations as closely as possible.

OAuth Server

The OAuth Server enables three different OAuth flows: Authorization Code, User Credentials, and Refresh Token.

Authorization Code:

This flow is used by the Disaster Tracker web application. The initial call is as follows:

```
/authorize?client_id=disaster_tracker&response_type=code&state=login&redirect_uri=http://disastertracker.tk/receive_auth
```

This renders a login page for the user. The user POSTs their information, the server verifies, and (if successful), the provided callback URL is called with an authorization code attached:

```
http://client_url/callback?code=AUTH_CODE
```

The client will then exchange the code for a token and refresh token by calling the token endpoint:

```
/token?grant_type=authorization_code&code=AUTH_CODE
```

More info: <http://bshaffer.github.io/oauth2-server-php-docs/grant-types/authorization-code/>

User Credentials:

Since the mobile app cannot ensure the safety of the token, the authorization code flow is not appropriate. In addition, for mobile usability, it is desirable for the mobile application to be able to implement a custom login screen. The User Credentials flow best meets these requirements. The initial call is as follows:

```
/token?grant_type=password&client_id=disaster_tracker_mobile&username=USER&password=PASS
```

The token and refresh tokens are directly received from this request via the registered client redirect URL. For Disaster Tracker's mobile app, this registered URL is:

```
disastertracker://receive_auth
```

More info: <http://bshaffer.github.io/oauth2-server-php-docs/grant-types/user-credentials/>

Refresh Token:

This flow is used when the access token expires. The call is simply:

```
/token?grant_type=refresh_token&refresh_token=REFRESH_TOKEN
```

New access and refresh tokens are returned, and the old tokens are invalid.

More info: <http://bshaffer.github.io/oauth2-server-php-docs/grant-types/refresh-token/>

API Specification

- **GET /devices**

- Description: Internal Use Only. Used by Disaster Tracker to get Datto's complete and current list of devices.
- Authenticated Users: Datto Intranet
- Output Format: HTTP 200 (JSON)

```
{  
    device_id: Integer,  
    msp_id: Integer,  
    latitude: Float,  
    longitude: Float,  
    city_name: String,  
    state: String  
}
```