Get Ready - MinistryPlatform New OAuth

We will be rolling out a large update to the Platform that will include many enhancements and new features. One of the largest changes is a complete replacement of the OAuth stack.

What is OAuth?

OAuth 2 is an industry standard way of implementing Authentication and Authorization. OAuth provides the security framework for users authenticating and for applications authenticating to access data anonymously or access data on a user's behalf.

Why is this Changing

There are number technical reasons why this needed to change. The first is better support. Our old OAuth stack was built on top of some technology that is no longer being iterated and improved. The new stack is under constant development and has great documentation. In addition to these behind the scenes changes, our new stack will fully support Refresh Tokens, JWT Tokens, Open ID, and several of standard features. Additionally, we have improved the login experience to offer a true SSO integration that all our applications will eventually implement.

Getting Ready for the Migration

The move to the new OAuth stack includes several breaking changes. First and foremost, the OAuth endpoints are all changing as will some of the scopes and requirements. Let's review the flows that will be supported along with required scopes / grants.

OAuth 2 Flows Support

The MinistryPlatform OAuth implementation is built from and on top of the Identity Server 3 project (https://identityserver.github.io/Documentation/docsv2/). All of the endpoint documentation should very closely match the stock configuration. To learn more about each of the following flows, considering reading the following: https://alexbilbie.com/guide-to-oauth-2-grants/

The following flows are commonly used.

Client Credentials Flow

When to Use: Server side code requesting data from MinistryPlatform as an application.
Grant Type: **client_credentials**
Scope Required: **http://www.thinkministry.com/dataplatform/scopes/all**

Implicit Flow

When to Use: Client side application that receives an access token directly from the authorization server. The user is directed to the OAuth login interface and once authenticated an access token is returned via URL parameter. This should only be used in fully authenticated applications.
Grant Type: **implicit**
Scope Required: **http://www.thinkministry.com/dataplatform/scopes/all**
Redirect_Uri: REQUIRED

Authorization Code

When to Use: Server side redirected login. This is a two-step process where first the server redirects to the authorization server. Either the user is forced to login or immediately returns a code to the calling server via Redirect_Uri. The server uses this code to obtain an access token (second step).
Grant Type: **code / authorization_code** (Two Steps)
Scope Required: **http://www.thinkministry.com/dataplatform/scopes/all, openid**
Redirect_Uri: REQUIRED

Resource Owner

When to Use: Used to authenticate an end user and obtain a user specific Access Token / Claims. Username and password are transmitted to the authorization server.
Grant Type: **password**
Scope Required: **http://www.thinkministry.com/dataplatform/scopes/all openid**

Refresh Token

When to Use: Used to refresh a previously acquired access token. You must request '**offline_access'** in your scopes to get the refresh token. Refresh Tokens are long lived and can be used to renew / refresh the access token.
Grant Type: **refresh_token**
Scope Required: **http://www.thinkministry.com/dataplatform/scopes/all openid offline_access**

Breaking Changes

In previous versions of MinistryPlatform, the OAuth server would allow the following scenarios that now no longer work:

- Non-existent Scopes – you MUST supply one or more scopes
- No redirect_Uri for Implicit / Authorization Code Flows – you MUST record the exact Redirect_Uri in API_Client or receive an invalid Redirect_Uri error message
- All endpoints have changed. We will be forwarding the old discovery endpoint to the new one, but any hardcoded endpoints will break
- Resource Owner Flow – to gain access to UserInfo you must pass both scopes or UserInfo endpoint will not return user data

Co-Existence

Below you will find our suggested course of action to fully enable co-existence (Working today and ready for the update).

1. Don't hard code any of the OAuth endpoints. Discover them by querying the discovery endpoint. This will allow your code to "learn" about the endpoints dynamically and not be tied to specific endpoints.
    a. Current OAuth supports a discovery URL: https://dev.ministryplatform.net/ministryplatform/oauth
    b. Future OAuth supports a discovery URL: https://dev.ministryplatform.net/ministryplatformapi/oauth/.well-known/openid-configuration

2. Discover Scopes. When authenticating via client credentials only use the **http://www.thinkministry.com/dataplatform/scopes/all** scope. Otherwise use all available scopes from the discovery document. This will automatically add refresh token support in the new OAuth Stack.
3. Additional Properties moved to the top level object. Below you can compare how Additional_Properties from the old OAuth stack have been moved into the top level object. Please make adjustments accordingly.

Old UserInfo Output (JSON)


```
{
  "userid": 17,
  "sub": "d6337ca4-e1c2-4799-8910-7ec90d0c319d",
  "name": "Kehayias, Chris",
  "given_name": "Christopher",
  "family_name": "Kehayias",
  "middle_name": "Matthew",
  "nickname": "Chris",
  "email": "chris@thinkministry.com",
  "zoneinfo": "",
  "locale": "",
  "roles": [
    "Administrators"
  ],
  "additional_properties": {
    "Last_Name": "Kehayias",
    "First_Name": "Christopher",
    "Display_Name": "Kehayias, Chris",
    "Nickname": "Chris",
    "Email_Address": "chris@thinkministry.com",
    "Mobile_Phone": "321-794-1376",
    "Contact_GUID": "50f193ea-96ec-4d64-a50d-524a16eb2253",
    "Contact_ID": 13511,
    "Contact_Status": "Active",
    "Household_ID": 921838,
    "Red_Flag_Notes": null,
    "Participant_Type": "Member",
    "Home_Phone": "321-794-1376",
    "Address_Line_1": "2720 Bradfordt Dr",
    "Address_Line_2": null,
    "City": "West Melbourne",
    "State/Region": "FL",
    "Postal_Code": "32904",
    "Latitude": null,
    "Longitude": null,
    "Domain_GUID": "823a61b5-d847-4bb6-b28c-c9dbcbb6018f",
    "Congregation_Name": "Central Congregation Changed",
    "User_GUID": "d6337ca4-e1c2-4799-8910-7ec90d0c319d"
  }
}
```

New UserInfo Output (JSON)


```
{
  "userid": "53",
  "display_name": "Kehayias, Chris",
  "given_name": "Christopher",
  "family_name": "Kehayias",
  "middle_name": "Matthew",
  "nickname": "Chris",
  "email": "chris@thinkministry.com",
  "zoneinfo": "",
  "locale": "",
  "roles": [
    "Administrators",
    ""
  ],
  "ext_Last_Name": "Kehayias",
  "ext_First_Name": "Christopher",
  "ext_Display_Name": "Kehayias, Chris",
  "ext_Nickname": "Chris",
  "ext_Email_Address": "chris@thinkministry.com",
  "ext_Mobile_Phone": "321-794-1376",
  "ext_Contact_GUID": "584dec2a-4983-4421-8d3f-e6009aee5697",
  "ext_Contact_ID": "1314",
  "ext_Contact_Status": "Active",
  "ext_Household_ID": "",
  "ext_Red_Flag_Notes": "",
  "ext_Participant_Type": "Guest",
  "ext_Home_Phone": "",
  "ext_Address_Line_1": "",
  "ext_Address_Line_2": "",
  "ext_City": "",
  "ext_State/Region": "",
  "ext_Postal_Code": "",
  "ext_Latitude": "",
  "ext_Longitude": "",
  "ext_Domain_GUID": "84869469-f707-451f-b592-a5f5d8352617",
  "ext_Congregation_Name": "",
  "ext_User_GUID": "3e0e6cf6-ea43-4d6d-b06d-4fc2474a48b5",
  "sub": "3e0e6cf6-ea43-4d6d-b06d-4fc2474a48b5",
  "auth_time": "1519081234",
  "idp": "idsrv",
  "name": "chris@thinkministry.com",
  "amr": "password"
}
```


References

Identity Server 3 Documentation - https://identityserver.github.io/Documentation/docsv2/

OAuth 2 Guide - https://alexbilbie.com/guide-to-oauth-2-grants/