

Upcoming Changes

Chris Hutchinson, SW Engineering Manager



DEVELOP WITH
DEERE
2019

Agenda

Wednesday, December 4, 2019

- **OAuth 2.0 Migration**

- OAuth 2.0 overview
- Steps to migrate
- Migration timeline

- **Required Customer Action Event**

- What is a Required Customer Action Event?
- How to identify and handle
- Expectations for future events

OAuth 2.0 Migration

DEVELOP WITH
DEERE
2019



JOHN DEERE

NOTHING RUNS LIKE A DEERE

OAuth 2.0 – Overview

- **What is OAuth and why is it important?**
 - OAuth is a standardized authentication protocol
 - Allows a user to approve an application to act on their behalf
 - John Deere APIs leverage OAuth for authentication and access consent
- **Why is John Deere switching from OAuth 1.0a to OAuth 2.0?**
 - Well supported – predominant industry standard
 - More flexible with respect to grant types and access scopes
 - Better security with short lived tokens (leverages refresh tokens)

OAuth 2.0 – Migration Timelines

For the **MyJohnDeere API** and **JDLink Machine Data API**...

- Feb 2020 – OAuth 2.0 fully supported
- Mar 2020 – 12 month 1.0a deprecation communication
- Sep 2020 – 6 month 1.0a deprecation communication
- Dec 2020 – 3 month 1.0a deprecation communication
- Feb 2021 – 1 month 1.0a deprecation communication
- **Mar 2021 – OAuth 1.0a officially deprecated**
 - **Existing OAuth 1.0a access tokens will no longer work**
 - **OAuth 2.0 will be the only supported authentication protocol**

OAuth 2.0 – Application Requirements – What you need...

- **Client Key and Secret**

- Obtained by setting up an application in developer.deere.com

- **OAuth Access Scopes**

- An applicaiton will be required to specify what scopes of access it requires (from which the user will be asked to consent)

- **Redirect URI**

- Client application redirect landing page after user provides authentication and consent
 - The redirect URI is configured via the application developer.deere.com OAuth profile

- **John Deere's OAuth .well-known URI**

- Provides standardized meta data such as authorization URI, token URI, scopes, and more

- <https://signin.johndeere.com/oauth2/aus78tnlaysMraFhC1t7/.well-known/oauth-authorization-server>

OAuth 2.0 – Scopes

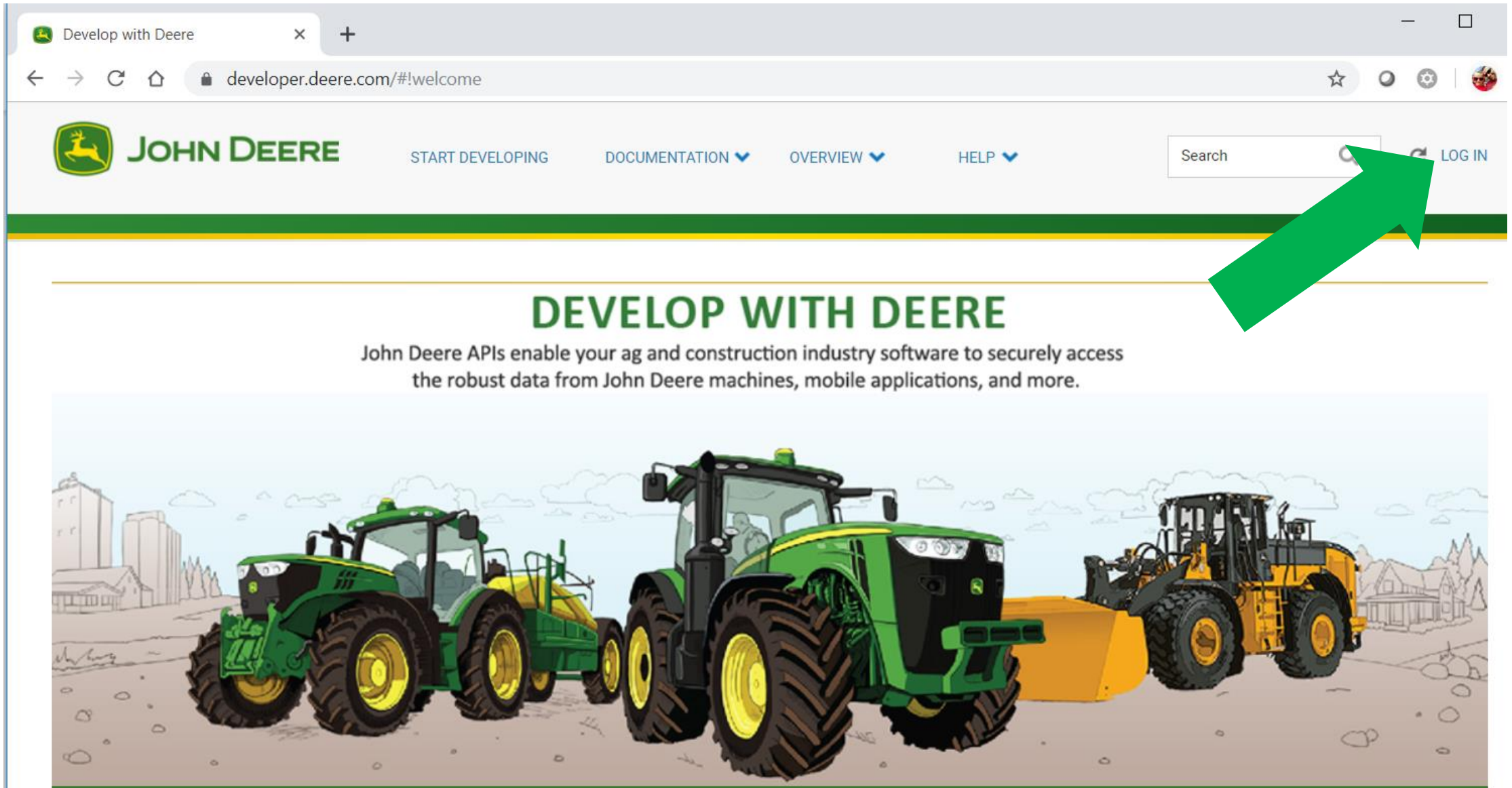
- Profile – **View** user's name and contact info
- Org 1 – **View** operators, staff, and partners
- Org 2 – **Modify** operators, staff, and partners
- Eq 1 – **View** equipment and terminals
- Eq 2 – **Modify** equipment and terminals
- Ag 1 – **View** products, fields, and boundaries
- Ag 2 – **View** agronomic time series data
- Ag 3 – **Modify** products, fields, boundaries, agronomic time series data
- Files – **Upload** and **download** files

Full documentation will be made available on developer.deere.com by Feb 2020

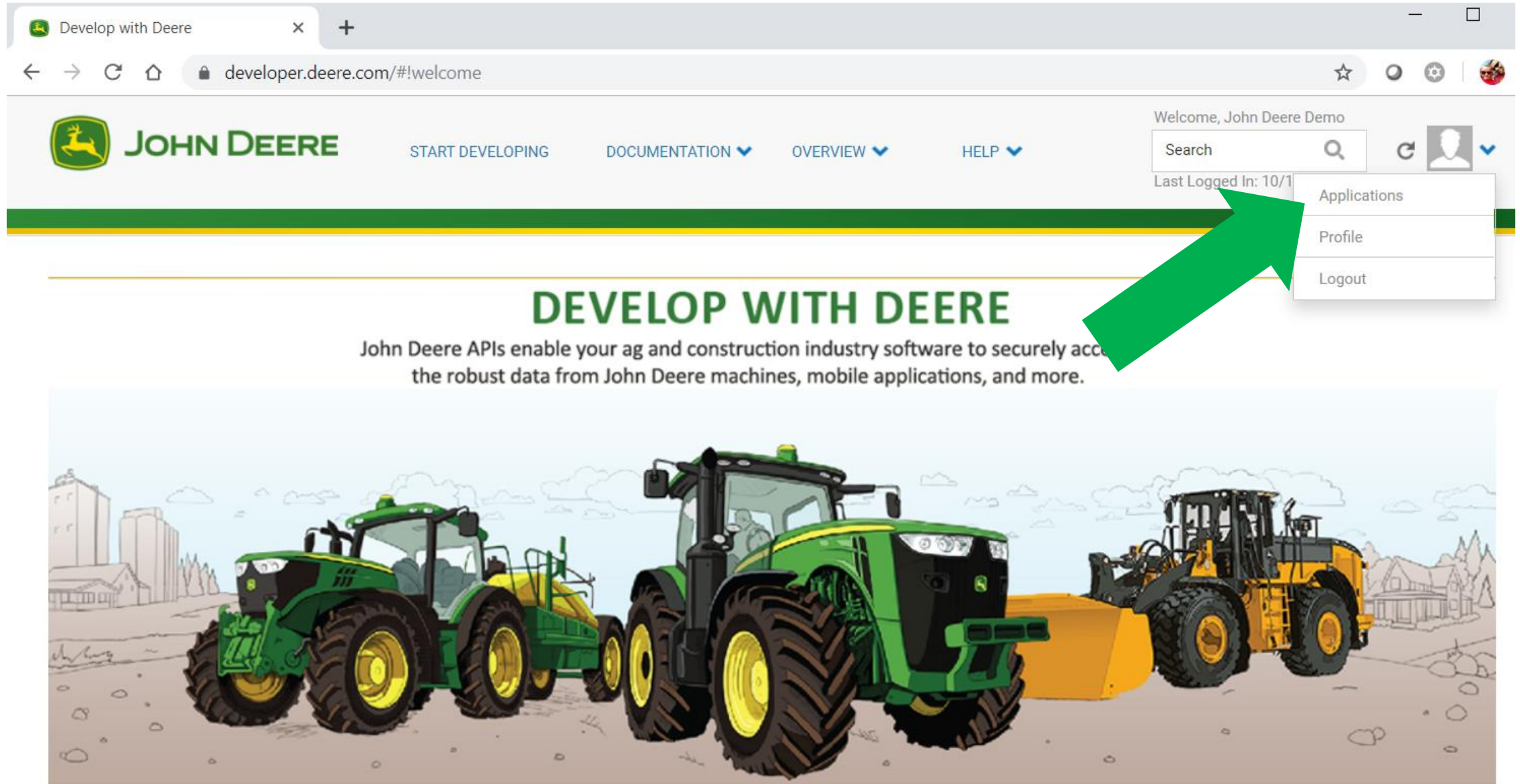
OAuth 2.0 – Migration Steps – Action Required!

1. Register client redirect URI in developer.deere.com
2. Update client authentication logic for OAuth 2.0

OAuth 2.0 – Register Client Redirect URI



OAuth 2.0 – Register Client Redirect URI



The screenshot shows the John Deere Developer Portal interface. The browser tab is titled "Develop with Deere" and the address bar shows the URL "developer.deere.com/#!welcome". The header features the John Deere logo, navigation links for "START DEVELOPING", "DOCUMENTATION", "OVERVIEW", and "HELP", and a user profile section. The user profile section displays "Welcome, John Deere Demo", a search bar, and a dropdown menu. The dropdown menu is open, showing options: "Applications", "Profile", and "Logout". A large green arrow points to the "Applications" option. Below the header, the main content area has the heading "DEVELOP WITH DEERE" and a paragraph: "John Deere APIs enable your ag and construction industry software to securely access the robust data from John Deere machines, mobile applications, and more." The background image shows three John Deere tractors in a field.

Develop with Deere

developer.deere.com/#!welcome

JOHN DEERE

START DEVELOPING DOCUMENTATION OVERVIEW HELP

Welcome, John Deere Demo


Search

Last Logged In: 10/1

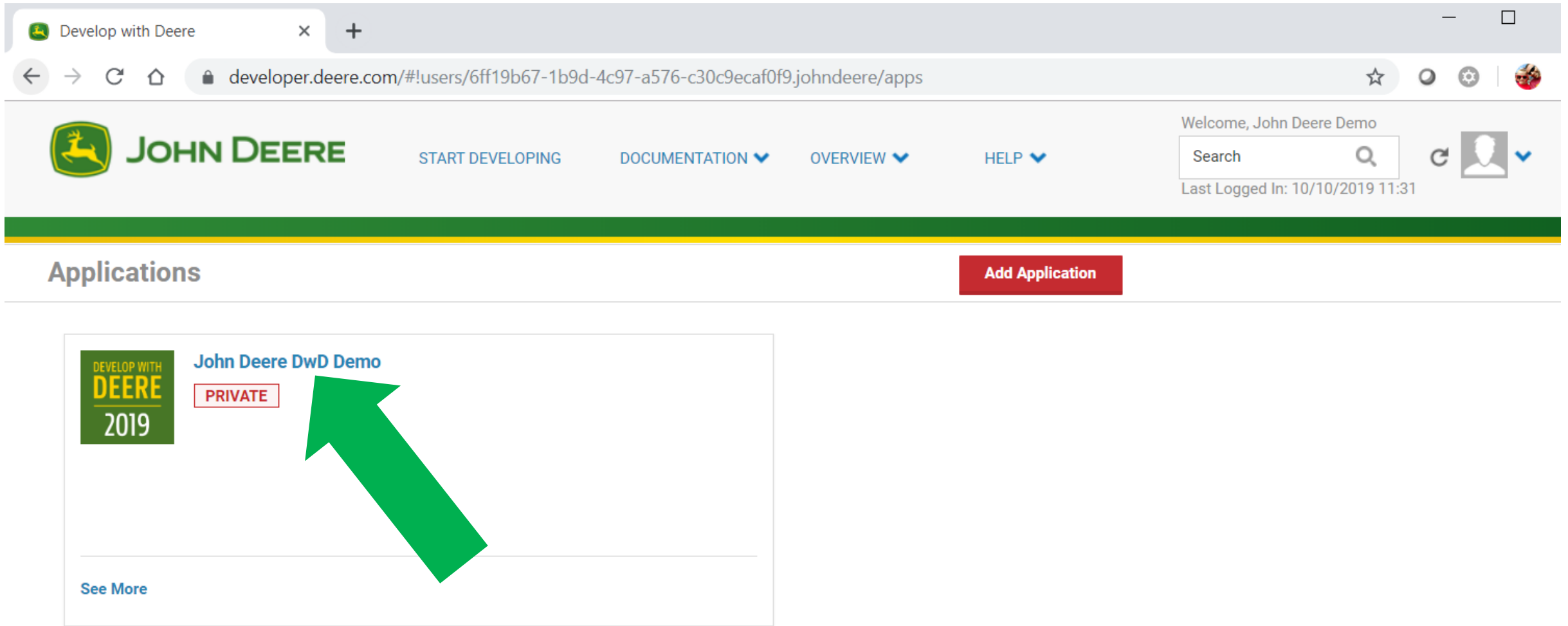
- Applications
- Profile
- Logout

DEVELOP WITH DEERE

John Deere APIs enable your ag and construction industry software to securely access the robust data from John Deere machines, mobile applications, and more.



OAuth 2.0 – Register Client Redirect URI



The screenshot shows a web browser window with the URL `developer.deere.com/#!/users/6ff19b67-1b9d-4c97-a576-c30c9ecaf0f9,johndeere/apps`. The page header includes the John Deere logo, navigation links for [START DEVELOPING](#), [DOCUMENTATION](#), [OVERVIEW](#), and [HELP](#), and a user profile section for "John Deere Demo" with a search bar and a "Last Logged In" timestamp of 10/10/2019 11:31.

The main content area is titled "Applications" and features a red "Add Application" button. Below this, a card displays the "John Deere DwD Demo" application, which is marked as "PRIVATE". A large green arrow points to the application name. A "See More" link is located at the bottom left of the application card.

OAuth 2.0 – Register Client Redirect URI

The screenshot shows the John Deere Developer Portal interface. At the top, there's a navigation bar with the John Deere logo, links for 'START DEVELOPING', 'DOCUMENTATION', 'OVERVIEW', and 'HELP', a search bar, and a user profile section with the text 'Welcome, John Deere Demo' and 'Last Logged In: 10/10/2019 11:31'. Below the navigation bar, the main content area is titled 'John Deere Dwd Demo' and includes buttons for 'Activated in Production', 'Edit', and 'Delete'. On the left side, there's a sidebar with a 'DEVELOP WITH DEERE 2019' banner and a list of menu items: 'Details', 'Overview', 'Performance', 'Logs', 'License Monitor', 'Test Client', and 'Team'. The 'Details' section is currently selected. The main content area is divided into two sections: 'DETAILS' and 'SECURITY'. The 'DETAILS' section includes fields for 'Application Description', 'Version Description', 'Parent Organization' (Tenant - JohnDeere), 'Tags' (None), 'Visibility' (Private), 'Website' (None), 'Implementation' (Sandbox), and 'Updated' (10/4/2019 14:19 [2 weeks ago]). The 'SECURITY' section includes fields for 'App ID' (johndeere-7d5qS7Wfxhq1emRPPHCQag85) and 'Shared Secret' (*****). There are 'Copy to Clipboard' buttons for both fields. A large green arrow points to the 'Shared Secret' field. At the bottom of the 'SECURITY' section, there are buttons for 'Import Credentials', 'OAuth Profile', and 'Regenerate Shared Secret'.

Develop with Deere

developer.deere.com/#!/apps/326d07bd-9d8f-4414-8ac3-f6b42dcb83fa.johndeere/versions/7d5qS7Wfxhq1emRPPHCQag85.johndeere/d...

JOHN DEERE

START DEVELOPING DOCUMENTATION OVERVIEW HELP

Welcome, John Deere Demo

Search

Last Logged In: 10/10/2019 11:31

← John Deere Dwd Demo

Activated in Production Edit Delete

DEVELOP WITH DEERE 2019

Details

Overview

Performance

Logs

License Monitor

Test Client

Team

DETAILS

Application Description

Version Description

Parent Organization

Tenant - JohnDeere

Tags : None

Visibility : Private

Website : None

Implementation : Sandbox

Updated : 10/4/2019 14:19 [2 weeks ago]

SECURITY

App ID

johndeere-7d5qS7Wfxhq1emRPPHCQag85

Copy to Clipboard

Shared Secret

Show

Copy to Clipboard

Import Credentials OAuth Profile Regenerate Shared Secret

OAuth 2.0 – Register Client Redirect URI

ACCESS TOKEN	AUTHENTICATION
Token type	Application Type
<div>Provider Default</div>	<div>Confidential</div>
ID TOKEN	Authentication Method
ID Token Signing Algorithm	<input checked="" type="radio"/> Global Setting
<div>Provider Default</div>	<input type="radio"/> Choose from authentication options below
<input type="checkbox"/> Require Authentication Time Claim	<input type="checkbox"/> Require Signed Requests
	JWKS URL
	<div>Enter a URL</div>
	<input type="checkbox"/> Restricted Common Scopes
	<input type="checkbox"/> Restricted Response Types
	Redirect URI
	<div>https://www.my.application.com/signup</div>
	<div>Add</div>

Cancel

Save

OAuth 2.0 – Migration Steps – Action Required!

1. Register client redirect URI in developer.deere.com
2. Update client authentication logic for OAuth 2.0

OAuth 2.0 – Authorization Code Flow

1. Obtain authorization and token URI from .well-known URI

- <https://signin.johndeere.com/oauth2/aus78tnlaysMraFhC1t7/.well-known/oauth-authorization-server>

2. Acquire authorization code

- Requires user to authenticate and consent to access

3. Acquire *access* token

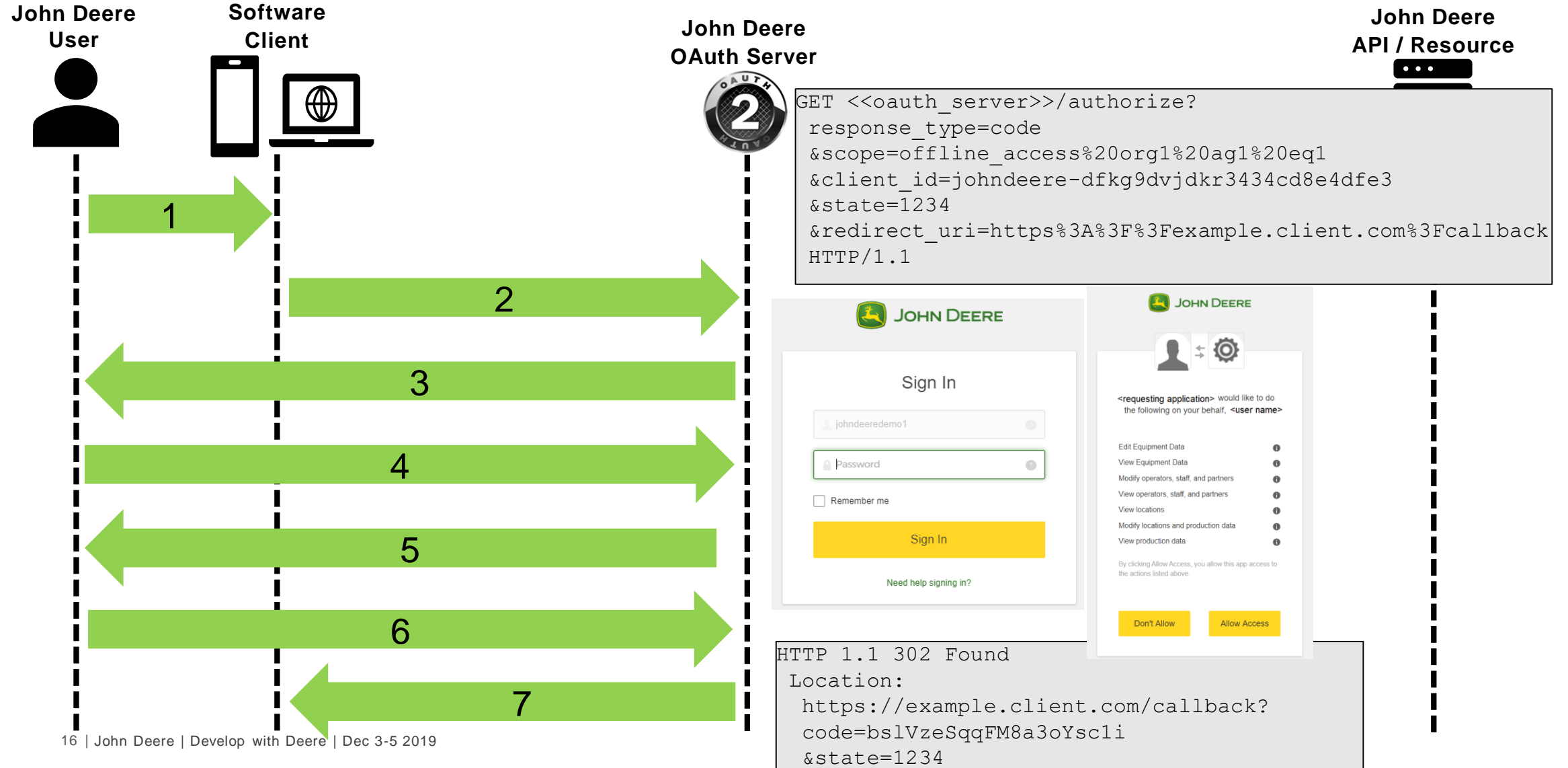
- Authorization code required to mint access token

4. Setup periodic *refresh* token logic to acquire new *access* token

- *Refresh* token should be used to acquire new *access* token (valid for only 12hrs)

5. Use *access* token to call API resource – Hooray!

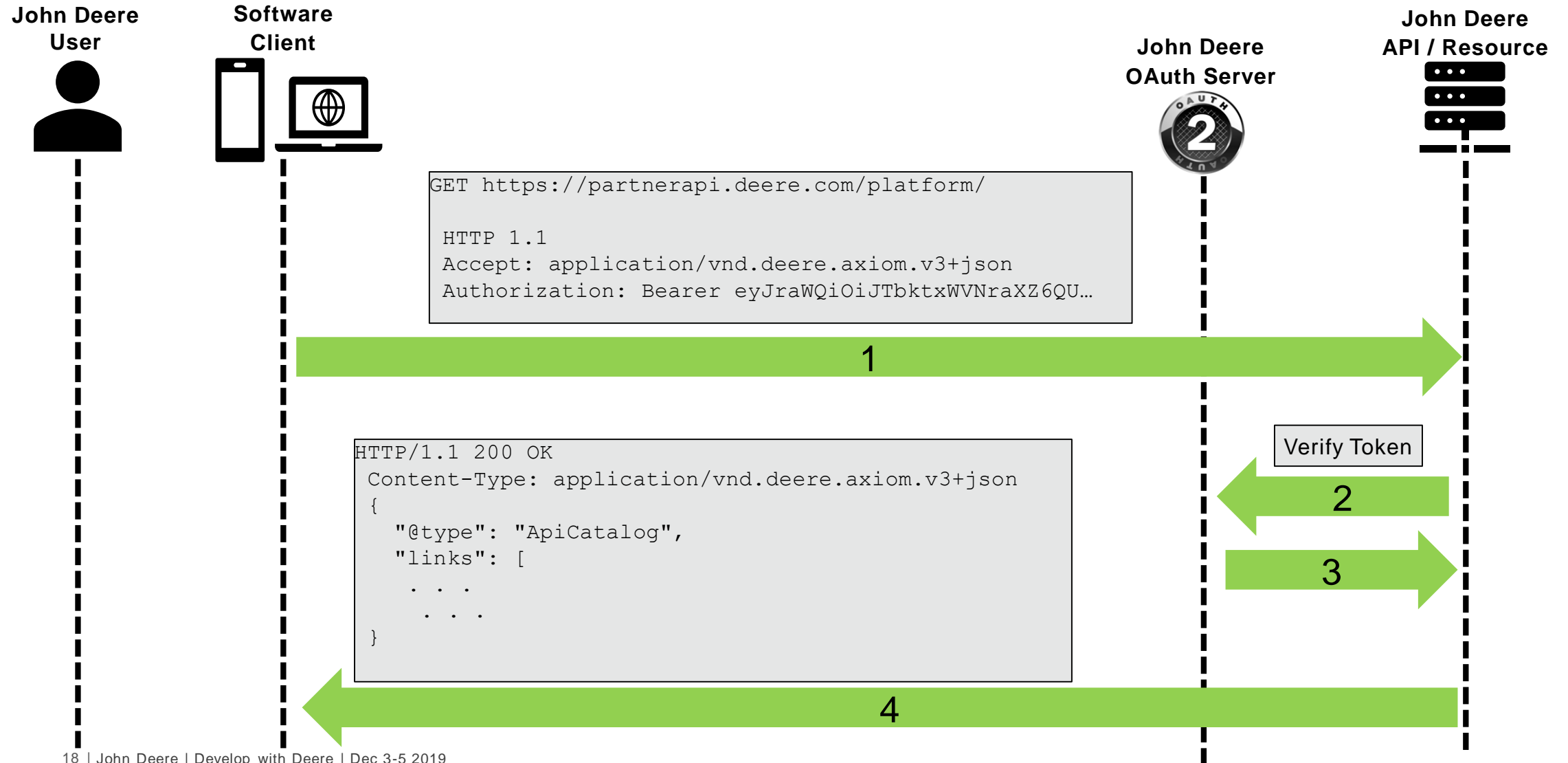
OAuth 2.0 – Auth Code Flow – Request Auth Code



OAuth 2.0 – Auth Code Flow – Request Access Token



OAuth 2.0 – Auth Code Flow – Resource Access



Oauth 2.0 – Auth Code Flow – Refresh Access Token



OAuth 2.0 – Postman and Python Demo

- Postman Demo
- [Sample Python Code Jupyter Notebook](#)

OAuth 2.0 – Refresh Token Best Practice

- Dynamically refresh your **access** token once it expires (valid for 12 hours)
 - There is no need to ask for a new **access** token sooner than it expires
- Remember to keep your **refresh** token “hot”
 - The **refresh** token will expire in 1 year since last used
 - If the **refresh** token expires, the user will be required to re-authenticate to get a new **access** token

OAuth 2.0 – Migration Timelines

For the **MyJohnDeere API** and **JDLink Machine Data API**...

- Feb 2020 – OAuth 2.0 fully supported
- Mar 2020 – 12 month 1.0a deprecation communication
- Sep 2020 – 6 month 1.0a deprecation communication
- Dec 2020 – 3 month 1.0a deprecation communication
- Feb 2021 – 1 month 1.0a deprecation communication
- **Mar 2021 – OAuth 1.0a officially deprecated**
 - **Existing OAuth 1.0a access tokens will no longer work**
 - **OAuth 2.0 will be the only supported authentication protocol**

OAuth Resources

- developer.deere.com
 - OAuth 2.0 documentation to be added by Feb 2020
- [My John Deere API Onboarding Jupyter Notebook](#)
 - Sample/executable OAuth 2.0 Python code to be added by Feb 2020
- API Dev Support – Got questions or need additional help?
 - Email api-support@johndeere.com
- OAuth 2.0 Info - <https://oauth.net/2/>

Required Customer Action (RCA) Events

DEVELOP WITH
DEERE
2019



JOHN DEERE

NOTHING RUNS LIKE A DEERE

Required Customer Action (RCA) Event

– What is it?

- An event that requires the user to take action before further account activity is allowed
 - This includes API calls upon the user's behalf
- Examples – user must accept new terms and conditions, verify account information

– What does an RCA event look like?

- Client API calls will result in a 403 response
 - X-Deere-Terms-Location header will include a redirect URL where the user can take action
 - Response payload will indicate a short description of required user action

Required Customer Action (RCA) Event

- **API Response Status**

- 403 Forbidden

- **Response Headers**

- X-Deere-Warning - partnerapi.deere.com "Requested Org is in a restricted state."
 - X-Deere-Terms-Location - https://teammanager.deere.com/organizations/{{ORG_ID}}/terms

- **Body**

```
{
  "@type": "Errors",
  "errors": [
    {
      "@type": "Error",
      "guid": "19f7b283-d383-4990-9e14-1b3ee0f7b63d",
      "message": "Requested Org is in a restricted state."
    }
  ],
  "otherAttributes": {}
}
```

Required Customer Action (RCA) Event

– How to handle an RCA event – 2 alternatives...

1. If possible, navigate the user to the URL supplied in the 403 response X-Deere-Terms-Location header
2. Implement a way to notify the customer that action is required
 - Supply 403 response message and X-Deere-Terms-Location URL as instructions to resolve

– Timelines and expectations

- Future RCA events will be communicated in advance – none currently planned
- Consider RCA event handling as a best practice moving forward

Q&A / Feedback

DEVELOP WITH
DEERE
2019



JOHN DEERE

NOTHING RUNS LIKE A DEERE



JOHN DEERE