OptiID
The next best thing since sliced bread

Eric Markson | June 30, 2023
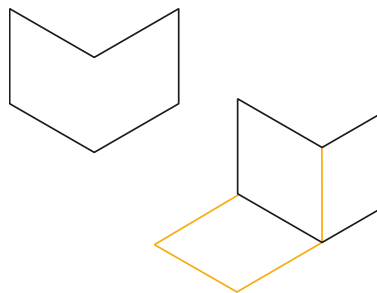
Technical Architect. Platinum OMVP. Content Cloud SME.

Eric Markson

Blog: https://www.optimizelyvisuals.dev

Email: eric@optimizelyvisuals.dev

Agenda
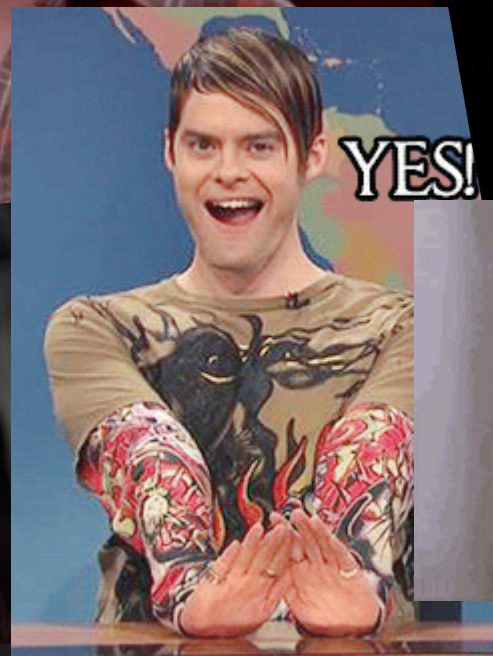
What is OptiID?

Is it necessary?

So....IS it necessary?

opti01mstr49ta7inte.dxcloud.episerver.net
opti01mstr49ta7inte-slot.dxcloud.episerver.net
opti01mstr49ta7prep.dxcloud.episerver.net
opti01mstr49ta7prep-slot.dxcloud.episerver.net
opti01mstr49ta7prod.dxcloud.episerver.net
opti01mstr49ta7prod-slot.dxcloud.episerver.net
Inte.customurl.com
Inte.customurl.com?x-ms-routing-name=slot
prep.customurl.com
prep.customurl.com?x-ms-routing-name=slot
prod.customurl.com
prod.customurl.com?x-ms-routing-name=slot
customurl.local
paasportal.episerver.net
manager.idio.co
manager.usea01.idio.episerver.net
app.zaius.com
app.optimizely.com
accounts.welcomesoftware.com

I mean...YES! Everyone agrees!

What is OptiID?

Simply said…

OptiID is the single place that will allow login and switching between the Optimizely products and respective environments.

It's the most direct visual way to show users that all these products are, in fact, part of the same suite.

It is also the portal that will allow the product administrators to give individualized permissions to each user.

Products that NOW support OptiID

- Content Marketing (Welcome)
- DXP Platform (Content Cloud)
- DXP Dev Portal (PAAS Portal)
- Admin Center (OptiID Admin)
- Data Platform (ODP)
- Customized Commerce

Products that WILL support OptiID

- Configured Commerce
- Product Recommendations
- Content Recommendations
    - Can be accessed from inside CMS

Implementation

Implementation

SSO App

The SSO platforms that are currently supported are Azure AD or Okta.

The documentation isn't perfect and took some trial and error on my part, but here is the setup:

Create SAML SSO endpoint

1. Send Optimizely the Identifier, Login URL, and Certificate
    - As of now, ignore the documentation where it says you can login at this point...it's a mistake
2. Apply the Audience and Assertion URL that Optimizely provides back
3. Login and enjoy!

The one issue in Azure AD that I ran into was being able to properly pass through the user email.

The onboarding team helped me with this. (I do not believe this is an issue in Okta)

Caution: I am an Azure AD noobie...so do as I say, not as I do
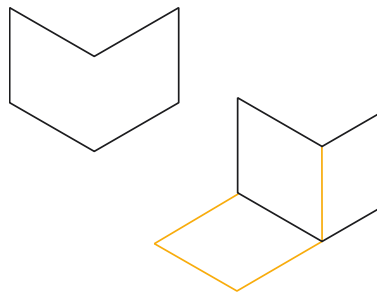
Implementation

Content Cloud + Customized Commerce

Content Cloud is (at this point) the only application that needs a developer to enable.
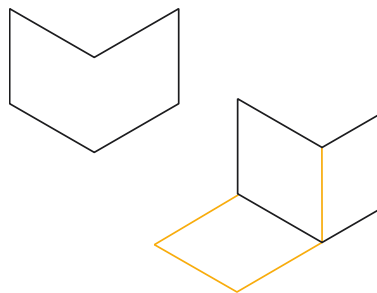
Nuget packages needed:

- EPiServer.OptimizelyIdentity (will be released on Nuget for GA)

- EPiServer.CMS.UI (>= 12.22.0)

Code needed:

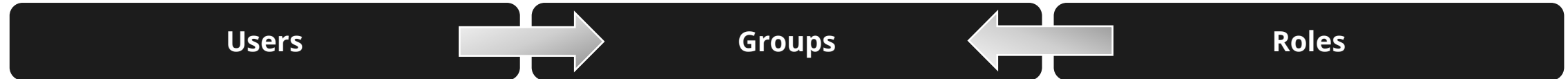Add to Startup.cs - services.AddOptimizelyIdentity(useAsDefault: true);

appsettings.json changes needed:

CMSAdmins and CMSEditors roles needs to be removed. These will be added automatically.

Users and Permissions

Users	→	Groups	←	Roles

Users

- Users can be 'Invited' (created)

- Users can be a part of the SSO environment (exist in AD) or can be local to the system
  - Local users will be prompted to create a password on first login

Groups

- Groups can contain one or more role

- Groups can also contain one or more product

- When users are assigned to a group, they are given the defined roles to the defined environments

Roles

- Roles are the named permission levels for the products

- Roles have out of the box values, but can also be manually created

- Manually created roles are assigned to a specific product + environment
  - (example, CMS is the product, and Integration is the environment)

TL;DR - All roads lead to Groups.

Groups are created to hold **Users** and **Roles**.

Roles are created to define a level of permission for a Product(s)/Environment(s)

First Thoughts

Wow....there are a lot of issues...

Firstly....THIS IS NOT A BAD THING. This is simply the price of testing cutting edge alpha/beta technology.

For a couple years, Optimizely has been trying to clean up their internal system organization. One of them being the relationship between products, users, and organizations.

This makes it very clean-cut for customers and for technical partners.

BUT where this got muddy is, since I have my own Azure AD instance and my own sandboxes, where do I live in this ecosystem to be able to have access?

Simply put...I, an OMVP with sandboxes of my own, was a corner case.

I exist in the organization of my employer, so if there are other products that are attached to other organizations in any way, I can't simply just act as the owner/administrator of them in this new system.

To fix this issue, we had to move all of my sandboxes to be under the Verndale organization.
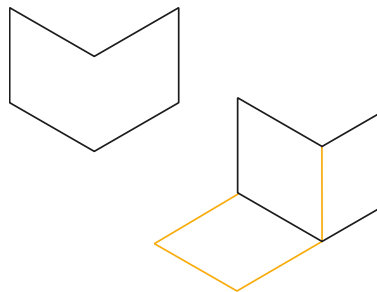
More issues?

This sandbox organization crisis led to the next big issue.

My sandboxes got mixed in with our corporate systems, owner/admin wise.

For example, we use Welcome (yes, old name, can't keep up with the rebrands) internally within our marketing team.

I was not given access because I don't need it. Since this mix-up, I am now able to completely control permissions for our Welcome platform.

This time I'm not so sure this is a corner case. This may pop up more often based on organization structure?

These instances were simply based on what our organization owns.

Where does this leave me?

I now have permissions for 13 different instances, where about half of them are not mine.

(Yes, I am working with the OptiID team to remedy this. It is more or less a training/onboarding issue and will be ironed out as time goes on)

PLEASE GIVE THE TEAM FEEDBACK!

# Wow...Eric, you're really selling this...

In the grand scheme of things, I am chalking all these issues up to this being a new and extremely complex system. Training is being done with all of the support and onboarding teams.

Think of this achievement.

At Opticon 2022, I harassed the Opti team enough for them to give me a sneak peek at the early wireframes for this system. (This is while the organizations were being cleaned up, before any engineering work was started)

Every single product team independently implemented this SSO system, before Opticon 2023, to FINALLY bring them into one big cohesive suite.

This is LITERALLY the thing that we've wanted from all these acquisitions.
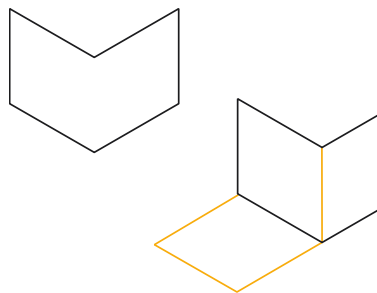
MOMENT OF SILENCE...PLEASE!

Optimizely has taken this opportunity to put the beloved login url "/episerver/cms" to rest. 💀

The new login URL is going to be:

"https://<sitename>/ui/cms"

Going to the new login URL will bring you to the login screen that will either allow you to login with SSO or with a local account. (Yes, a local account can still be created)
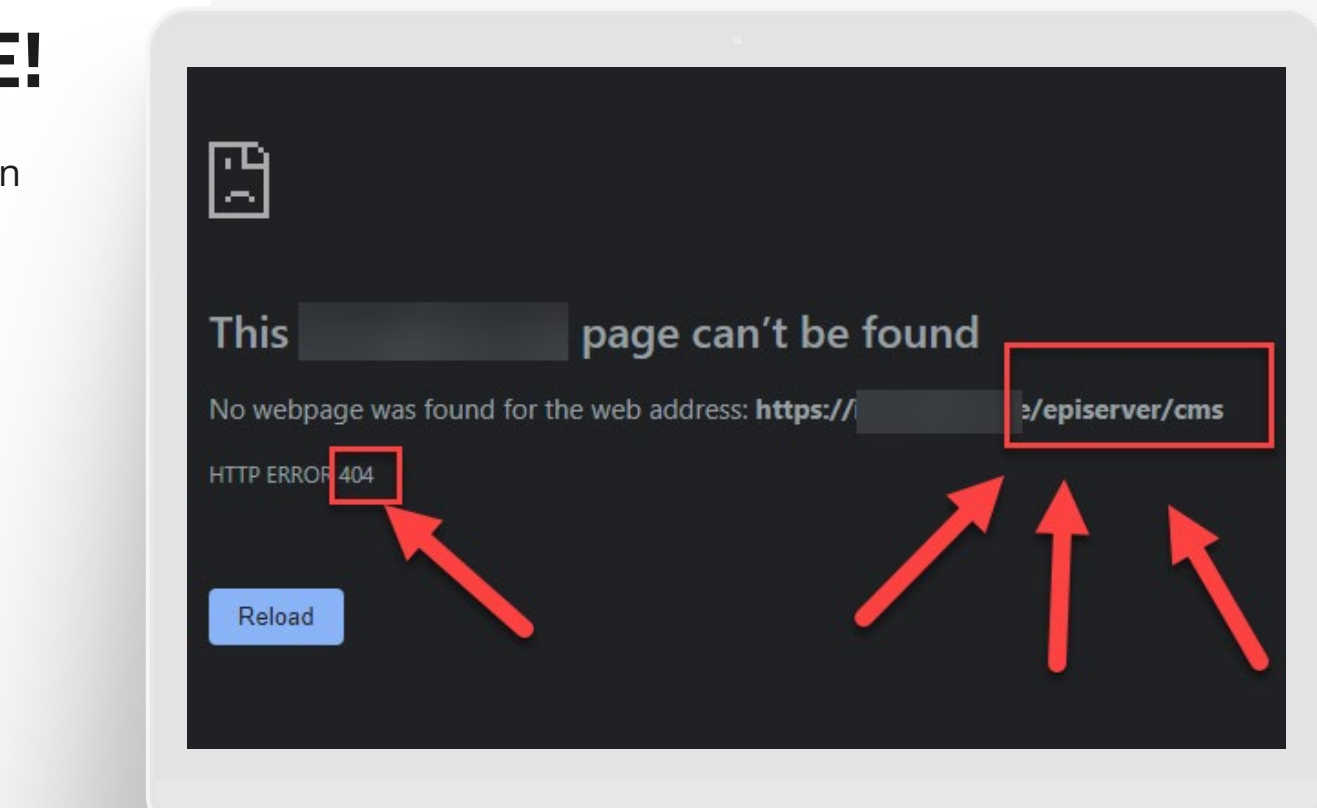
# New UI & SSO Login URL

Global Components + CMS Edit View

Most of the horizontal menus now become vertical with the top blue bar becoming the protected location for the product switcher.

Global Product Switcher Components

1. Instance Name (Client Name)
2. Product + Environment name
3. Environment settings

CMS Edit View

4. Dashboard
5. Edit
6. Reports
7. Audiences (Visitor Groups)
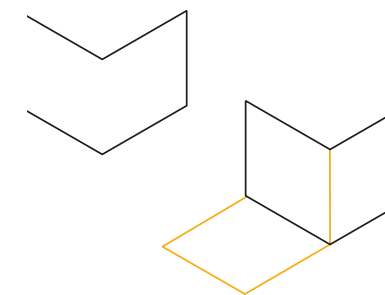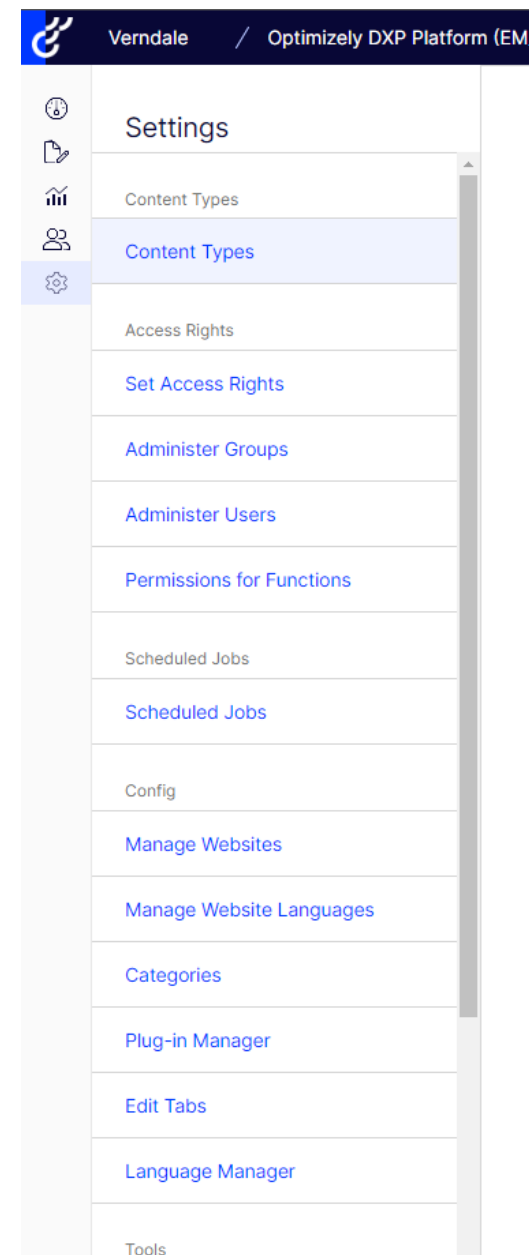8. Settings (Admin)
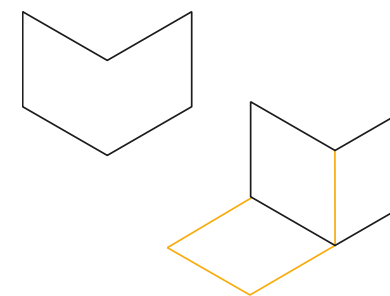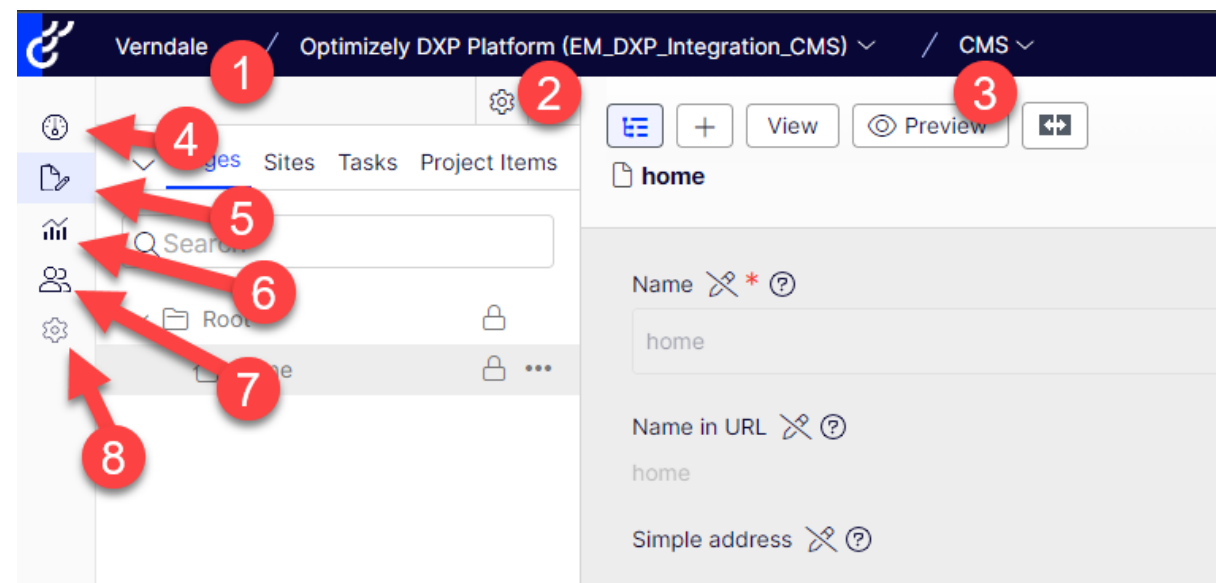
CMS Settings View (Admin)

The previous horizontal menu for admin has now become a big vertical menu with some better category organization.

(Yes, it looks like previous custom menu links have been migrated to this new structure. The items will be placed ABOVE the "Content Types" menu group)

User Manager

Products and Instances

Verndale / Optimizely Admin Center (Admin Center) ⌄

Products & Instances

- Products & Instances
- User Manager
- SSO Settings

Account Executive

Name	Instances
Optimizely DXP Developer Portal	1
Optimizely Content Recommendations	2
Optimizely DXP Platform	3
Optimizely Admin Center	1
Optimizely Data Platform	3
Optimizely Configured Commerce	1
Optimizely Content Marketing Platform	2

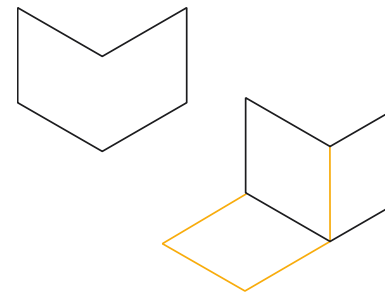## Optimizely DXP Developer Portal Instances

🔍 Filter by instance...

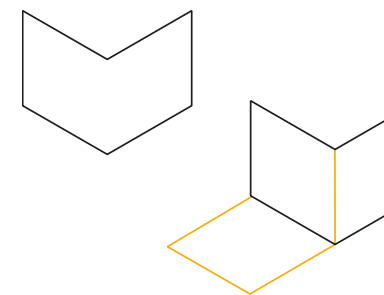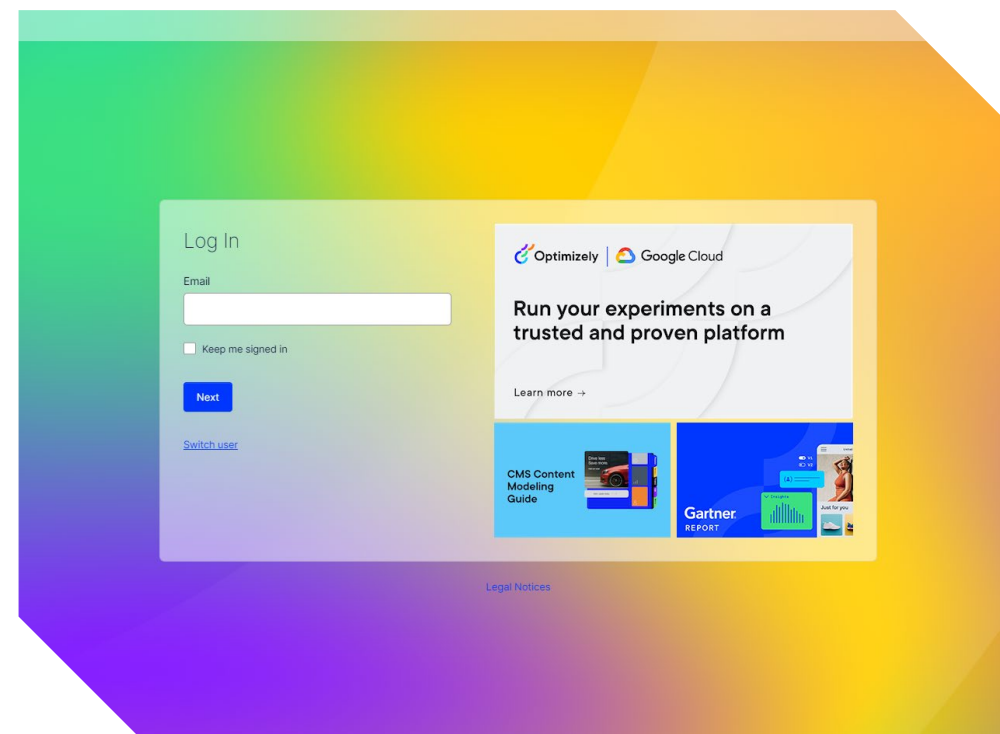| Instances	Region	Technical Contact
EM_DXP_CMS	East US	

Instance Details

Display Name
EM_DXP_CMS

Name
01mstr

Technical Contact
🔍 Search for users...

Let's Login! ☺

https://login.optimizely.com/

What's Next?

Remaining questions

1. How to specifically deal with non-SSO users in CMS (Local Accounts) alongside of SSO users

   - At the time of writing this, this functionality has not been pushed to the beta, but does exist and will be released

   - Word on the street is that there will be an 'invitation' process, which will allow the user to set their password once they accept the invite.

2. Learning how a Technical Implementation Partner can co-exist in a client-environment

   - Specifically, to be able to allow clients to manage users during and/or after go-live

3. What is the onboarding process for new clients? What about for partners?

   - Is this going to be granted with the PAAS Portal access form? (if OptiID SSO exists for the domain)
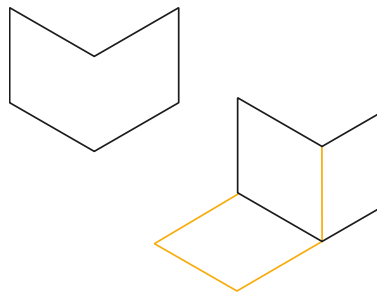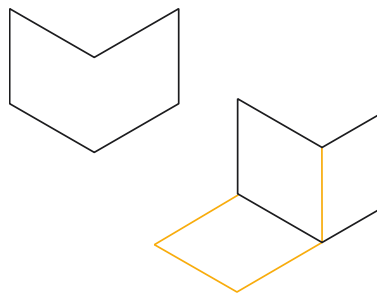
Well...let's party?

If you haven't heard...

As of today (6/30), this is officially out of beta, and is now considered GA.

Drinks are on Opti! (Disclaimer: Probably not ☹ #thankspatrick)

https://docs.developers.optimizely.com/content-management-system/docs/install-opti-id-for-cms

Thank You

VERNDALE