# Configuring OIDC as third-party IDP in Access (Auth0)

WorkspaceONE Access now supports acting as a relying party in an Open ID Connect flow of authentication. (SaaS 2012 release of Access)

In this lab we will be adding **Auth0** as our identity provider that we will integrate with WorkspaceONE Access.

Part 1: Sign up for Auth0 Trial

Part 2: Adding Auth0 as a third-party IDP in Workspace ONE

Part 3: Test authentication flow

## Part 1: Sign up for Auth0 Trial

In this part we will be signing up for a free Auth0 trial account and setting up the the Auth0 environment.

← → C â auth0.com/signup	بې بې بې بې د. بې کې کې
$\diamond$	Sign Up
Try the world's #1	Email
authentication-as-a-service	sfrank.aw@gmail.com
platform for free!	Password
Let Auth0 handle the complexities of secure authentication so you can focus on building your app!	
START FOR FREE AND SAVE TIME WITH AUTHO!	By clicking any of the Sign Up buttons, I agree to the <b>terms of service</b>
Passwordless     Lock for Web iOS & Android	SIGN UP
<ul> <li>Up to 2 social identity providers</li> </ul>	or
<ul> <li>Unlimited Serverless Rules</li> </ul>	SIGN UP WITH GITHUB
Built for developers Powered for the enterprise	
ATLASSIAN PLATAM	SIGN UP WITH MICROSOFT
SIEMENS AMD	

1. Open a new browser window and navigate to <a href="https://auth0.com/signup">https://auth0.com/signup</a>

- Type a demo email address (Do NOT use your corporate e-mail address)
- And a password
- Click SIGN UP

$\mathbf{O}$	
	simeonf 🥑 .us.auth0.com
	To help you easily explore our product, we've selected a tenant doma
	name for you. Although you can't rename a tenant, you can always ac
Welcome to Auth0	later.
Help us setup your first tenant and start	
authenticating.	REGION
STEP 1 OF 2	🚟 AU 💽 EU 💽 Japan 📑 US
	We can host all of your data in any of these regions.
	Useful if you need to comply with EU Data Protection Directive
	NEXT

2. Specify the **domain suffix** that you would like to use. Ensure it is easy to remember and that you make note of it.

- Click US for Region.
- Click **NEXT**.

<b>\$</b>	€ ~
Let's set your company up for success. step 2 OF 2	Account type Are you creating this account for yourself or on behalf of a company?

- 3. Set the Account Type option to Personal
- and click CREATE ACCOUNT



4. You should now be in the a Auth0 Admin Console.



#### 5. In the Auth0 Admin console navigate to User Management on the left and click Users.

• Now click on + CREATE USER

Create user	×
Email *	•
mark@euc-livefire.com	
Password *	
Repeat Password *	
••••••	
Connection *	
Username-Password-Authentication 🔹	
CANCEL	Ď

6. Fill in the **email** of the unique user you have been using for the labs. (example: mark@euc-livefire.com)

- Then type VMware1! as the password.
- Click **CREATE** at the bottom of the page.

## Part 2: Adding Auth0 as a third-party IDP in Workspace ONE

In this section you will configure Auth0 to as as a third-party OIDC IDP in WorkspaceONE Access.



### 1. In the **Auth0 Admin Console** navigate to **Applications > Applications** and then click **+ CREATE APPLICATION**



2. In the Create Application pop-up window type **WorkspaceONE Access** as the Name for the application.

For the Application type select Regular Web Applications

#### Then click **CREATE**



3. Click on the **Settings** tab and copy the **Client ID** and **Client Secret** to a notepad.

Hide Advanced Settings				
Advanced Settings				
Application Metadata Device S	ettings OAuth Grant Types WS-Federation	Certificates	Endpoints	
OAuth				
OAuth Authorization URL	https://sfrank.us.auth0.com/authorize	Ø		
Device Authorization URL	https://sfrank.us.auth0.com/oauth/device/code	Ø		
OAuth Token URL	https://sfrank.us.auth0.com/oauth/token	Ø		
OAuth User Info URL	https://sfrank.us.auth0.com/userinfo	Ø		
OpenID Configuration	https://sfrank.us.auth0.com/.well-known/openid-config	e		

4. Still on the **settings** tab, scroll down until you see "**Show Advanced Settings**" Click it and click on **Endpoints**. The **OAuth** URLs will be displayed. Copy the **OpenID Configuration** into your notepad.

(8) Workspac	Workspace ONE <sup>™</sup> Access     Tenant Admin ~ AW-EMUSK						-EMUSK		
Dashboard -	Users & Groups Catalog	J 🔻 Identity & A	ccess Management	Roles			Q Search users, groups or appli	cations	
Directories Identi	ty Providers Password	l Recovery Assistant	Authentication I	Methods Polici	es			Manage	Setup
	Identity Provid	lers (3)					Create SAML IDP		
	Identity Provi	Auth Methods	Directory	Network Ran	Connector(s)	Туре	Create OpenID Connect IDP		
	System Identity Provider	Password (Local Directory)	System Directory	ALL RANGES		Built-in	Create Built-in IDP		
	Bullt-in	Mobile SSO (for iOS) Certificate (cloud deployment) User Risk Score Device Compliance (with Workspace ONE UEM) Password (cloud	LivefireSync UEMLocalDirecto sfmusk	ALL RANGES	ws1- connector.euc- livefire.com	Built-in	Enabled		

#### **Configure Workspace ONE Access**

5. Open a new tab in your browser and authenticate to your Workspace ONE Access tenant. Navigate to Identity & Access Management > Identity Providers and click Add Identity Provider > Create OpenID Connect IDP

Type: Opt	anID Connect
Identity Provider Name*	Auth0
Authentication Configuration	Select Automatic Discovery to use the well-known published OpenID Connect URL to get all the OpenID Connect endpoints. Select Manual Configuration to add the OpenID Connect endpoint URLs manually, if using Auto Discovery is not possible or contains wrong information.   Automatic Discovery  Manual Configuration  Configuration
	https://sfrank.us.auth0.com/.well-known/openid-configuration
	OpenID Connect config endpoint to discover authorize, token, issuer and JWKS endpoints.
Client ID*	2wTswzDCgBj1P18aQMIiUsDFdAX00n9Q

5. Set the name of the **Identity Provider** to Auth0

Authentication Configuration: Automatic Discovery

Paste the **OpenID Configuration**URL from Auth0 into the Configuration URL

Paste the Client ID from your notepad

Paste the Client Secret from your notepad

User Lookup Attribute	Open ID User Identifier Attribute	Workspace ONE Access User Identifier Attr
	email 🗸	email ~
Just-in-Ĭime User Provisioning	Enable	
Users	Select which users can authenticate using this ld LivefireSync UEMLocalDirectory_sfmusk	IP. Choose from the available directories from the list below.
Network	Select which networks this IdP can be accessed below.	from. Choose from the available network ranges from the list
	ALL RANGES	

6. Now set the User Lookup Attribute to email for both OpenID User and Workspace ONE

#### Click LivefireSync for the Users directory

#### Click All Ranges for Network

Authentication Method Name*	Enter a name to identify the OpenID Connect authentication method. When you select this authentication method in the access policy, users are redirected to authenticate against the OpenID Connect authorization server.
	AuthO
Pass through Claims	Enable pass through claims to add non-standard OpenID Connect claims. Non-standard claims are sent by third party OpenID Connect identity provider and added to the token generated by Workspace ONE Access.
Redirect URI	Integrate with Open ID Connect Provider using Redirect URI below https://aw-emusk.vidmpreview.com/federation/auth/response/oauth2
	Add Cancel

7. Set the Authentication Method name to Auth0

**Copy** the **Redirect URI** into your notepad.

Click **Add** to save the settings.

ADD POLICY EDIT DELETE EDIT DEFAULT POLICY NETWORK RANGES
Policy Name Applies to Rule
default_access_policy_set     1 Application(s)     3 Rule(s)

## 8. Click Identity & Access Management > Policies and click EDIT DEFAULT POLICY

Edit F	Policy					×
1 Defir 2 Con	nition figuration	You can create a list of rul of devices that can access application before reauthe	es to access the applications se s the applications, the auth met enticating.	elected. For each rule, select th hods, and the maximum numb	ne IP network range, ti er of hours users can	he type use the
3 Sum	nmary	Network Range	Device Type	Authentication	Re-authenticate	
		# ALL RANGES	Web Browser	Password (cloud deplo	8 Hour(s)	×
		# ALL RANGES	Workspace ONE App	Password (cloud deplo	2160 Hour(s)	×
		# ALL RANGES	Windows 10	Certificate (cloud depl	8 Hour(s)	×
		⊕ ADD POLICY RULE				

9. In the **Edit Policy** window click **Configuration** then choose the policy with **Web Browser** Device Type and click **ALL RANGES**.

If a user's network range is	ALL RANGES ~	1
and the user accessing content from *	Web Browser V	٩
and user belongs to group(s)	Q Select Groups	٩
	Rule applies to all users if no group(s) selected.	
and user is registering FIDO2 authenticator *	No	٩
Then perform this action	Authenticate using V	٩
then the user may authenticate using *	AuthO ~	① ⊕
If the preceding method fails or is not applicable, then	Password (Local Directory) V	()
	ADD FALLBACK METHOD	
	CANCEL	SAVE

10. In the **Edit Policy Rule** pop-up change the first authentication method to **Auth0** and leave the fall back method as **Password (Local Directory)** 

Click **SAVE** at the bottom of the pop-up.

1 Definition	You can create a list of rul of devices that can access	es to access the applications se the applications, the auth met	elected. For each rule, select th hods, and the maximum numb	e IP network range, er of hours users car	the type i use the
2 Configuration	application before reauthe	inticating.			
3 Summary	Network Range	Device Type	Authentication	Re-authenticate	
	# ALL RANGES	Web Browser	AuthO+1	8 Hour(s)	×
	# ALL RANGES	Workspace ONE App	Password (cloud deplo	2160 Hour(s)	×
	# ALL RANGES	Windows 10	Certificate (cloud depl	8 Hour(s)	×
	ADD POLICY RULE				
dit Policy			CA	NCEL BACK	NEXT
dit Policy	Definition		¢3	NCEL BACK	NEXT
dit Policy 1 Definition 2 Configuration	Definition Name default_access_policy_set		c,	NCEL BACK	NEXT
dit Policy 1 Definition 2 Configuration 3 Summary	Definition Name default_access_policy_set Description		cs	NCEL BACK	NEXT
dit Policy 1 Definition 2 Configuration 3 Summary	Definition Name default_access_policy_set Description Default access policy set		cs	NCEL BACK	NEXT ×
dit Policy 1 Definition 2 Configuration 3 Summary	Definition Name default_access_policy_set Description Default_accoss_policy_set Application(s)		c2	NCEL BACK	NEXT
dit Policy 1 Definition 2 Configuration 3 Summary	Definition Name default_access_policy_set Description Default access policy set Applications 1 Applications Configuration		c2	NCEL BACK	NEXT
dit Policy 1 Definition 2 Configuration 3 Summary	Definition Name default_access_policy_set Description Default access policy set Applications 1 Applications Configuration Policy Rule 1 I a users network ranno is	ALL PANGES	c	NCEL BACK	×
dit Policy 1 Definition 2 Configuration 3 Summary	Definition Name default_access_policy_set Description Default access policy set Applications 1 Applications Configuration Policy Rule 1 Policy	ALL PANGES	c	NCEL BACK	X

11. Click **Next** on the **Configuration** page and **SAVE** on the **Summary** page of the **Edit Policy** window.

$\mathbf{Q}$	manfred Development		Q D	iscuss your needs	Docs	<b>Ú</b> ໜ
4 ~∕ ⊗	Getting Started Activity Applications	Applications Setup a mobile, web or IoT application to use A	Auth0 for Authentication. Learn more ►		+ CREATE	APPLICATION
	APIs SSO Integrations	Generic Default App	Client ID: Hh2nWECgFC93lugmSk4DDifJ3	۲. KMzkbId		
6	Authentication >					
ii	Organizations NEW	O WorkspaceONE Access Regular Web Application	Client ID: s01MkNvy5VeF5TTban6sCcUMK	Shjz1bt 🖒		•••
ĉ	User Management					
)	Branding >					
0	Security >					
ល	Actions BETA >					
X	Auth Pipeline					
o0o	Monitoring >					
85	Marketplace NEW					

12. Flip back to the **Auth0** Admin Console and click **Applications > Applications**. Click on the **WorkspaceONE Access** application.

	'Basic' (application uses HTTP Basic).
Application URIs	
Application Login URI	https://myapp.org/login
	In some scenarios, Auth0 will need to redirect to your application's login page. This URI needs to point to a route in your application that should redirect to your tenant's /authorize endpoint. Learn more
Allowed Callback URLs	https://aw- emusk.vidmpreview.com/federation/auth/response/oauth2
	After the user authenticates we will only call back to any of these URLs. You can specify multiple valid URLs by comma-separating them (typically to handle different environments like QA or testing). Make sure to specify the protocol ( https:// ) otherwise the callback may fail in some cases. With the exception of custom URI schemes for native clients, all callbacks should use protocol

13. In the **Settings** tab of the application scroll down to Application URIs and **paste** the **Redirect URI** from Access into the **Allowed Callback URLs** in Auth0.

	lifetime, after which the token can no longer be used. If rotation is enabled, an expiration lifetime must be set. Learn More	
Absolute Lifetime	31557600	
	Sets the absolute lifetime of a refresh_token (in seconds).	
Inactivity Expiration	DISABLED	
	When enabled, a <b>refresh_token</b> will expire based on a specified inactivity lifetime, after which the token can no longer be used.	
Inactivity Lifetime	2592000	
	Sets the inactivity lifetime of a refresh_token (in seconds).	
_	Show Advanced Settings	
	SAVE CHANGES	
anger Zone		
anger Zone Delete this application		
Delete this application All your apps using this client	will stop working.	DELETE
Delete this application All your apps using this client Rotate secret	will stop working.	DELETE

14. At the bottom of the page click **SAVE CHANGES**.

# Part 3: Test authentication flow

Let's now test the result of our integration with Auth0 as an OIDC IDP.



1. Open a new **Incognito window** and browse to your **Workspace ONE Access tenant**. As soon as you click **ENTER** you will be re-directed to Auth0

**Notice** the URL is your unique tenant for Auth0.

Welcome
Log in to manfred to continue to WorkspaceONE Access .
Email address
Password
Forgot password?
Continue
Don't have an account? Sign up

2. Enter the **E-mail address** of the user (**NOT** the admin account) and the password **VMware1!** Click **Continue** 



3. Now you should have been authenticated to your **Workspace**, double check your user in the top right hand corner of the Hub.

VERY IMPORTANT IF you are not planning on continuing to the bonus material please change your default access policy at this point. In order to ensure you can log back in as local administrator into Workspace ONE Access you will have to append your Access URL with /SAAS/ auth/0 (Example: aw-rfederer.vidmepreview.com/SAAS/auth/0) you will be able to log on and change the **default access policy** from Auth0 to Certificate (cloud deployment) with a fallback to Password (cloud deployment) with a fallback to Password (Local Directory).

This concludes the integration with Auth0 as a third party OIDC Identity Provider.

## **Bonus Material 1: Just-In-Time Provisioning**

In addition to the above integration Auth0 can act as a source of identity for your users and can create a user database on Access using JIT (Just-In-Time provisioning). The users get provisioned in Access as part of the initial authentication process.

8 Works	space ONE™ Acc	ess						Tena	nt Admin - AV	V-EMUSK
Dashboard	- Users & Groups	Catalog -	Identity & Acc	ess Management	Roles		Q	Search users, groups or ap	oplications	
Directories	Identity Providers	Password Reco	very Assistant	Authentication	Methods Policie	s			Manage	Setup
	Identit	ty Providers (	4)					Add Identity Provider		
	Identi	ty Provi Aut Moi (for Wo ON Ext Acc Ver (int Hut DU	h Methods bile SSO Android) rkspace E UEM ernal iess Token fy gent o) O Security	Directory	Network Ran	Connector(s)	Туре	Status		
	Works _2613	spacel Ker Pas	beros sword	LivefireSync	ALL RANGES	ws1- connector.euc- livefire.com	Workspace ONE Access	Enabled		
	Auth0	Aut	hO	LivefireSync	ALL RANGES Internal		OpenID Connect	Enabled		

In the Workspace ONE Access Admin console navigate to Identity & Access Management
 Identity Providers and click on Auth0 the Identity Provider you created above.

Provisioning		Auth0-Directory	Domains	+
	Just-III-Time Directory	Autro-Directory	Auth0	× +
	User Attribute Mappings*	Map the OpenID Connect attribut that are listed. These are required account is created.	es to the Workspace ONE Access a attributes that are added when the	ttributes user
		Open ID User Identifier A	Workspace ONE Access	+
		name	firstName 🗸	<b>×</b> +
		nickname	lastName 🗸	<b>×</b> +
		sub 🗸	ExternalID ~	<b>×</b> +
		email 🗸	distinguishedName	<b>×</b> +
		email 🗸	userName 🗸	<b>×</b> +
		email 🗸	userPrincipalName	<b>×</b> +
		email 🗸	email ~	<b>×</b> +
edirect URI	Integrate with Open ID Connec	t Provider using Redirect URI below	r	
	https://aw-emusk.vidmpre	view.com/federation/auth/resp	onse/oauth2	
	Save			

- 2. In the Auth0 IDP settings scroll down to Just-in-Time User Provisioning and click Enable.
  - Set your Directory Name to Auth0-Directory

- Domains: Auth0
- User Attribute Mappings:
- email userName
- name firstName
- nickname lastName
- email email
- email userPrincipalName
- sub ExternalID
- email distinguishedName
- Scroll down to the bottom of the page and click **Save**.

**NOTE**: Some of these values may need to be typed manually

User Attributes		
Default Attributes	Select the attributes to use when users sync to the directory or when local users are created. These attributes can be viewed from the Directory pages.	
	Required	
	disabled	
	distinguishedName	
	domain	
	email	
	employeeID	
	firstName 🗸	
	lastName 🗸	
	mfaid	
	mfaPhoneNumber	
<ul> <li>Getting Started</li> </ul>	• Back to Users	
Activity	emusk.aw@gmail.com	
Applications	user_id: auth0[602ccc9c6c534b0067e0032a	
SSO Integrations		
≪© Connections	Details Devices History Raw JSON Authorized Applications Permissions Roles	
Universal Login		
D. Users & Roles		
→ Users	1 4 2 "created_at": "2021-02-17T07:50:20.9432",	
	3 "email": "emusk.aw@gmail.com",	
OF Actions	4 'email_veriried : true, 5 'identities': [	
30 Actions	6 { 7 "connection": "Username-Password-Authentication".	
A Hooks	8 "provider": "auth@",	
M Emails	<pre>9 User_10 : 062000000000000000000000000000000000</pre>	
E Logs	11 } 12 ].	
St Marketplace NEW	13 "name": "emusk.aw@gmail.con",	
C) Extensions	<pre>14 inickname:: "emusk.aw", 15 picture": "https://s.gravatar.com/avatar/150a1e2ec5ad83d60b406fcd1f858900?s=480&amp;</pre>	
O Get Support	16 "updated_at": "2021-02-17T08:36:51.4862", 17 uper 14": auth81682cc92c65534b867c88822a"	
P. and address	18 "last_1p": "88.228.201.86",	
	19 'last_login': '2021-02-17T08:13:38.230Z",	
	21 "blocked_for": [],	
	22 "guardian authenticators": []	

**NOTE**: You must ensure here that you have all the attributes that are set to required in Workspace ONE Access mapped to an attribute otherwise the user provisioning will fail.

In order to find out which attributes you can use coming from **Auth0** click on the specific user in **Users** and click on the **Raw JSON** tab.

Here you will see the attributes listed.

🛟 Auth(	)		Q Search	n apps, users, marketplace	Help	p & Support Docs	Discuss Your Needs	sfrank 🚺 -
4 Getting St	arted	E t	Thank you for purchasing the Free Auth0 he Free plan. Like what you're seeing? Plo	olan. You have 21 days left in your tri ease enter your billing information he	al to exp ere.	periment with feature	s that are not in	BILLING
<ul><li>Applicatio</li><li>Authentica</li></ul>	ns > ation >	Use	rs				+ CRE	ATE USER
I Organizati 은 User Mana	ons NEW	An easy to Learn mor	use UI to help administrators manage us e ►	er identities including password rese	ets, crea	ting and provisioning	g, blocking and deleting u	sers.
Roles →] Branding	,	Q Sear	ch for users			Search by User	Ŧ	X RESET
O Security	>	Name		Connection		Logins	Latest Login ↓	
아 Actions 것 Auth Pipel	BETA >	US	user32scr@sanjose32.euc-livefire.com user32scr@sanjose32.euc-livefire.com	Username-Password-/	Authenti	ic 1	an hour ago	•••
Monitoring	g → ce NEW	<b></b>	Simeon Frank sfrank.aw@gmail.com	google-oauth2		1	a day ago	
<ul><li>Extension</li><li>Settings</li></ul>	S	-						
щ.,								

3. Now flip back to the **Auth0 Admin Console** and click on **User Management** > **Users** and click + **Create User.** We will now create a user that is non-existant in the Workspace ONE directory.

	Create user	>
Email *		
emusk.aw@gmail.com	1	
Password *		
•••••		
Repeat Password *		
•••••		
Connection *		
Username-Password-A	Authentication	•
	CREATE CANCEL	

4. Create a random user that is not in the Workspace ONE Access directory. Use the password **VMware1!** Click on **CREATE** 

• • • S Log in to WorkspaceONE Acce × +	
← → C 🔒 sfrank.us.auth0.com/u/login?state=g6Fo2SBrZVVuZXBFaXIORHdsdFVyNmV0aUozZFJIRzN1NXRsY6N0aWTZIGh0X0gxdW4yMjZEMzZ	Nd2kxT 🛧 👶 Incognito 🚦
Welcome	
Log in to sfrank to continue to WorkspaceONE Access .	
Email address emusk.aw@gmail.com	
Password ®	
Forgot password?	
Continue	
Don't have an account? Sign up	
OR	
G Continue with Google	
57	

5. Open a **new incognito window**. (If a previous one was open close and re-open)

Browse to the **Workspace ONE Access URL** and you will be redirect to your **Auth0** URL. Authenticate using the **email** created for the user you created above and **VMware1!** click **Continue** 

$\leftarrow$ $\rightarrow$ C $\square$ aw	emusk.vidmprevie	w.com/catalog-	favorite	🖈 👼 Incognito		
Favor	es Apps	People	For You	Support	EE	
Favorites					EE emusk.aw@gmail.com emusk.aw	
				Looks like you just moved in. Add your favorite apps here for quicker access.	Account Sign out ⊡→	

6. You should now be authenticated using that **unique user.** 

**NOTE**: If you are seeing errors after attempting to authenticate go back to **STEP 2** in order to look at the attributes that may not be lining up correctly.

8 Works	pace ON	E™ Acces	S						Tena	nt Admin - AW-EMU	SK
Dashboard	• Users 8	k Groups	Catalog 👻	Identity & Acces	s Management Roles	]			Q Search users, groups or ap	plications	
Directories	Identity Prov	viders Pa	ssword Recover	y Assistant	Authentication Methods	Policies				Manage Setu	ip 🛛
		Directori	<b>es</b> (4)						Add Directory		
		Directo	Туре	Domains	Synced Groups	Synced Users	Last S	Alerts			
		System Directory	Local Dir ectory	1	0	1					
		LivefireS ync	Active Di rectory o ver LDA P	1	60	12	Feb 15, 2021 10:55:16 AM 🥝	8	Sync Now		
		UEMLoc alDirecto ry_sfmus k	Other Dir ectory	1	0	0					
		Auth0-Di rectory	Just-in-T ime Dire ctory	1	0	1					

7. Switch back to the Workspace ONE Access admin console and click on **Identity & Access Management > Directories** and notice you now have **Auth0-Directory** and the type is **Just-in-Time Directory**.

(8) Workspace	ONE <sup>™</sup> Access					
Dashboard 👻 Us	sers & Groups Catalog	✓ Identity & Ac	ccess Management	Roles		Q
Users Groups						
	<b>Users</b> (11)					
	User Name	User ID	Domain	Directory	VMware Verify P	Groups
	Admin,Tenant	manfred	System Domain	System Directory	N/A	ALL USERS
	L Debio, Mark	Mark	euc-livefire.com	LivefireSync	N/A	ALL USERS, M
	L Dusello,Ferna	Fernando	euc-livefire.com	LivefireSync	N/A	ALL USERS, M
	L Ikin,Kevin	Kevin	euc-livefire.com	LivefireSync	N/A	ALL USERS, DO
	L manfred, manf	manfred@euc-liv	Auth0	Auth0-Directory	N/A	ALL USERS
	Arios,Tom	Tom	euc-livefire.com	LivefireSync	N/A	ALL USERS, M
	L mark,mark@e	mark@euc-livefir	Auth0	Auth0-Directory	N/A	ALL USERS
	L Markez,Kim	kim	euc-livefire.com	LivefireSync	N/A	ALL USERS, Do

8. At the top navigation click on **Users & Groups** and click **Users**.

You should now be able to see the user that has been created as a result of JIT.

# **Bonus Material 2: Auth0 and Social Integrations**

One of the benefits of using Auth0 is that it allows for integrations with Social platforms such as Google & Facebook. In this exercise you will create the Google and & Facebook connection with Auth0 and authenticate to Workspace ONE Access using one of these social connections as your source of identity.



1. In the **Auth0 admin console** navigate to **Authentication** > **Social** and click **CREATE CONNECTION**.



2. If its not already added add **Google / Gmail** and **Facebook**. (In my case Google has already been added automatically)

• Notice the other available connections on this page - Dropbox, Paypal, Microsoft etc...

Faceboo	ok Social Connection by Auth0
Facebook w	ill need access to:
Redirect	users to login at Facebook
Receive a	nd store user identities from Facebook
Update u	ser root profiles with data from Facebook
	CANCEL
By continui	ng, you grant the integration access to the permissions listed above and consent to the integrati

3. Proceed with adding **Facebook** as a social connection and click **Continue** to grant access to the information listed above.

New Fa	acebook Social	Connection	E SETUP GUIDE
Name	facebook		
	If you are triggering a login manually, th use on the connection parameter.	is is the identifier you would	
App ID	Leave blank to use Auth0 dev keys		
	How to obtain a App ID?		
App Secret	Leave blank to use Auth0 dev keys		
	For security purposes, we don't show yo	our existing App Secret.	
User Data	Public Profile () public_profile	Ernail () email	
	Group Access Member Info () groups_access_member_info	Publish to Groups publish_to_groups	
	Age Range ⑦ user_age_range	Birthday ⑦ user_birthday	
	Events () user_events	Friends () user_friends	
	Gender (?)	Hometown ③	
Deprecated Permissions	manage_notifications ③	publish_actions () publish_actions	
	read_stream () read_stream	read_mailbox ⑦ read_mailbox	
	user_groups () user_groups	user_managed_groups () user_managed_groups	
	user_status ()		
	These permissions are only available for API version v2.3 or older.	applications using Graph	
Advanced			
Sync user profile attributes at each looin	ENABLED		

4.You will be presented with options for linking Facebook. This could either be a private facebook for enterprise or you can use the public Facebook accounts. For our example we will use the public Facebook Accounts.

- In the User Data section you can select which attributes you would like to sync across to Auth0. Enable **Email** .
- At the bottom of the page click **CREATE**.

()	FACEBOOK Identifier con_FnWer@wVbY03meYj	▷ TRY CONNECTION	围 SETUP GUIDE
ettings	Applications		
oplications	s using this connection.		
G	Default App GENERIC		
	Test App REGULAR WEB APPLICATION		0

5. Now give the **Default App** and **WorkspaceONE Access** applications the permission to use this connection.

	New Tab × +
$\leftrightarrow \rightarrow c$	🔁 🔕 aw-emusk.vidmpreview.com
VMWiDP	🗘 Intelligent Hub - aw-emusk.vidmpreview.com
$\leftarrow \rightarrow c$	■ sfrank.us.auth0.com/u/login?state=g6Fo2SBPSE9vVTQ1TDFkV1NpeGRJaTNkQ3hiOWhqUFNNSXU1X6N0aWTZIF9sNzFxQ24xMWwwZHptVW9
<ul><li>← → α</li></ul>	International and the second provide the second provided and provid
	Continue with Google Continue with Facebook

6. Now open an incognito window. (Make sure previous incognito windows have been closed). Browse to you **Workspace ONE Access tenant URL**.

- You will be redirected to your unique instance of **Auth0**.
- Now you will see **Continue with Google** and **Continue with Facebook** as available options here on the authentication page.
- Click Continue with Facebook

facebook	Create New Account	
	Log in to Facebook	
	empowerlisbon@gmail.com	
	•••••	
	Log In	
	Forgotten account? · Sign up for Facebook Not now	

7. Log into **Facebook** (preferably a test facebook account)

Click Log In

Edd Connection will receive: your name and profile picture and email address. If the descrit let the app post to Facebook Continue as Empower
Cancel
By continuing, IAM Connection will receive ongoing access to the information that you share and Facebook will record when IAM Connection accesses it. Learn more about this sharing and the settings that you have.
IAM Connection's Privacy Policy
Back Info that you provide
ino init jou provido
Name and profile picture REQUIRED
Name and profile picture PEQUEED Email address empowerisbon@gmail.com
Name and profile picture Recursion Email address empowerlisbon@gmail.com
Name and profile picture         RECURED           Email address empowerfisbon@gmail.com         Image: Compare the second s
Name and profile picture  Record  Record Record  Record  Record  Record  Record  Record  Record  Record  Record  Record  Record  Record  Record  Record Record  Record  Record  Record
Name and profile picture     RECURPT       Email address empowerlisbon@gmail.com     Image: Continue as Empowerlisbon@gmail.com
Name and profile picture         RECORD           Empowerlishon@gmall.com         Image: Continue as Empowerlishon@gmall.com           This doesn't let the app post to Facebook         Continue as Empowerlishon@gmall.com           By continuing, IAM Connection will receive engoing access to the information that you have and facebook will receive when IAM Connection exits in Learn more about this sharing and the settings that you have.

8. You will now see the permission window. **Click on Edit** this and you will see that **name and profile picture** and **e-mail address** are the only attributes being sent as configured above.

#### Click Continue as Empower.

0	Favorites	Apps	People	For You	Support		EE	
Favo	rites					EE	Empower Lisbon empowerlisbon	
					Looks like you just moved in.	Account		
					Add your favorite apps here for quicker access.	Sign out	$\rightarrow$	

9. You should now be authenticated to the Workspace ONE Hub with the facebook user. At authentication the user get created in Auth0 then through JIT gets created in Workspace ONE Access.

		00010						+ CREA	
Activity									
Applications	>	Learn more >	p administrators ma	nage user identities	nciuding password re	sets, creating an	a provisioning, c	liocking and deleting us	ers.
Authentication	n >								
Organizations	NEW	Q Search for users				Sea	rch by User	•	× R
Users	nent 🗸								
Roles		Name			Connection		Logins	Latest Login $\downarrow$	
Branding	>	Empower Li	sbon		facebook		2	3 minutes ago	
Security	>	empowerlist	oon@gmail.com						
Actions	BETA >	emusk.aw@	)gmail.com		Username-Passwor	d-Authentic	3	a day ago	
Auth Pipeline	>	emusk.aw@	Igmail.com				-	,-a-	
Monitoring	>	user32scr@	)sanjose32.euc+live	fire.com	Licoroome Decemer	d Authontia	1	a day aga	
Marketplace	NEW	user32scr@	isanjose32.euc-livef	ire.com	Osemanie-Passwor	a-Authentic	1	a uay ago	
Extensions		Simeon Fra	nk						
Settings		sfrank.aw@	gmail.com		google-oauth2		1	2 days ago	
3) Workspac	e ONE" Acce	ss				Q Search	Te	nant Admin - AW-EMU	JSK
Workspac	Ce ONE™ Acce Users & Groups	SS Catalog v Identif	ty & Access Managerr	Roles		Q Search	Te users, groups or	nant Admin - AW-EMU applications	JSK
Workspace Asshboard - ers Groups	ce ONE™ Acce Users & Groups Users (16)	SS Catalog • Identif	ty & Access Managerr	ent Roles	_	Q, Search	Te users, groups or Add U	nant Admin - AW-EML applications People Settia Iser	JSK 198
Workspace	ce ONE™ Acce Users & Groups Users (16) User Name	SS Catalog + Identif	ty & Access Managerr	Directory	VMware Verify P	Q, Search Groups	Te Lusers, groups or Add U Status	nant Admin ~ AW-EMU applications People Settia Iser	JSK <sup>198</sup>
Workspace	ce ONE" Acce Users & Groups Users (16) User Name L Admin,Tena	SS Catalog v Identif User ID nt emusk	y & Access Managerr Domain System Domain	Directory System Directory	VMware Verify P	Q Search Groups ALL USERS	Te users, groups or Add U Status Enabled	nant Admin - AW-EMU applications People Settia	JSK
Workspace	users & Groups Users & Groups Users (16) User Name Admin,Tena Admin,Tena	SS Catalog + Identif User ID Int emusk	y & Access Managerr Domain System Domain euc-livefire.com	Directory System Directory LivefireSync	VMware Verify P N/A N/A	Q Search Groups ALL USERS Enterprise Admi	Te users, groups or Add U Status Enabled Enabled	nant Admin ~ AW-EML applications People Settin	JSK <sup>198</sup>
Workspace	Users & Groups Users & Groups Users (16) User Name & Admin, Tena & admin, admi	SS Catalog + Identif User ID Int emusk in Administrator b empowerlisbon	y & Access Manager Domain System Domain euc-livefire.com Auth0	Directory System Directory LivefireSync Auth0-Directory	VMware Verify P N/A N/A N/A	Q Search Groups ALL USERS Enterprise Admi ALL USERS	Te users, groups or Add U Status Enabled Enabled	nant Admin - AW-EML applications People Settin	JSK
Bathbard - arr Groups	users (16) Users (16) User Name Admin, Tena Admin, admi	SS Catalog • Identit User ID int emusk in Administrator b empower(isbon im emusk zwo@mail.	y & Access Manager Domain System Domain euc-livefire.com Auth0	Directory System Directory LivefireSync Auth0-Directory	VMware Verify P N/A N/A N/A	Q Search Groups ALL USERS Enterprise Admi ALL USERS ALL USERS	Te USERS, groups or Add D Status Enabled Enabled	nant Admin - AW-EMU applications People Settin	JSK
Workspac	User & Groups Users (16) User Name Admin,Tenn Admin,Tenn Admin,Tenn Admin,Tenn Admin,Tenn	SS Catalog • Identif User ID Identif Marken Monorfisban m emusk.aw@gmail emusk.	bemain System Domain euc-livefire.com Auth0 . Auth0	Directory System Directory LivefireSync Autho-Directory Autho-Directory	VMware Verify P N/A N/A N/A N/A	Q Search Groups ALL USERS Enterprise Admi ALL USERS ALL USERS NewHire@euc-il	Add D	nant Admin - AW-EML applications People Settle	JSK
Workspac	Users (16) Users (16) User & Groups Users (16) User Name & Admin,Tena & admin,Tena & admin,Tena & admin,Tena & admin,Tena & admin,Tena & admin,Tena & admin,Tena & admin,Tena	SS Catalog • Identif User ID Identif Administrator B., empowerfsbon, emusk.aw@gmail emusk.aw@gmail emusk.aw@gmail	Domain Domain System Domain euc-Ivefire.com AuthO euc-Ivefire.com euc-Ivefire.com	Directory System Directory LivefreSync Autho-Directory Autho-Directory LivefreSync	VMware Varity P N/A N/A N/A N/A N/A N/A	Q Search Groups ALL USERS Enterprise Admin ALL USERS ALL USERS NewHire@euc-ii	Te Users, groupe or Add U Enabled Enabled Enabled Enabled Enabled Enabled	nant Admin - AW-EML applications People Settle	JSK
Workspac	Users & Groups Users & Groups Users (16) User Name Admin.ten Admin.ten Groupsweis Amak.auyo Musk.Ebn PD1.Userd	SS Gatalog  Value ID User ID Administrator Du, emusk.awGgmal emusk UserS	Domain Domain System Domain euc-lvefre.com AuthO euc-lvefre.com euc-lvefre.com	Directory System Directory LivefreSync Autho-Directory LivefreSync LivefreSync	VMware Venty P           N/A           N/A           N/A           N/A           N/A           N/A           N/A	Q. Search Groups ALL USERS Enterprise Admin ALL USERS ALL USERS NewHire@euc-iit ALL USERS MerkHire@euc-iit ALL USERS	Te USERS groupe or Add D Enabled Enabled Enabled Enabled Enabled Enabled	nant Admin - AW-EML applications set	JSK
Workspac	Users & Groups Users & Groups Users (16) User Name Admin, Tana Admin, Tana Adm	SS Catalog	Domain Domain System Domain euc-lvefre.com euc-lvefre.com euc-lvefre.com euc-lvefre.com	Roles           Directory           System Directory           LivefreSync           Autho-Directory           LivefreSync           LivefreSync           LivefreSync	Иймине Varity Р N/A N/A N/A N/A N/A N/A N/A	Q. Search Groups All USERS Enterprise Admi All USERS NewHim@euc-II All USERS, Me IT Support@euc All USERS, Me	Te Users, groups or Add U Enabled Enabled Enabled Enabled Inabled Inabled Inabled	applications  People Settin	JSK
Workspace      Workspace      wr     Groups	Leo ONE" Acce Users & Groups Users (16) User Name & Admin, Tens & ammonetal admin, admi & ampoweria & admin, admi & ampoweria & admin, admi & ampoweria & admin, admi & admin, admin & admin, admi & admin, admi	SS Catalog • Identify	Demain Demain System Domain euc-Ivefre.com euc-Ivefre.com euc-Ivefre.com euc-Ivefre.com euc-Ivefre.com	Bleectery           Difference           System Directory           LevetPresynce           LevetPresynce           LevetPresynce           LevetPresynce           LevetPresynce           LevetPresynce	Имините Venity Р           N/A           N/A	Q Beard Groups ALL USERS Enterprise Admit ALL USERS ALL USERS MwrHine@euc-ii ALL USERS, Me IT Support@euc ALL USERS, He	Te susers, groups or Add U Enabled Enabled Enabled Enabled In Enabled In Enabled In Enabled In Enabled In Enabled	nant Admin - AW-EMU applications People Settle	JSK

10. You will note in the Auth0 Admin Console in the **User Management > Users** that the new **user** from Facebook has been created.

• Additionally on the Workspace ONE Access side you will see the user has been created.

아 C 습 C https://aw-emusk.vidmpreview.co	m/SAAS/auth/0	
Workspace ONE"		
Username		
Password		
System Domain		
Sign in		
Forgot Password?		
Change to a different domain		
vmware		
CONFIGURATION	Edit Policy Rule	_
If a user's network range is	ALL RANGES	~ • •
and the user accessing content from	Web Browser	~ @
and user belongs to group(s)	Q Select Groups	•
	Rule applies to all users if no group(s) selected.	- 11
and user is registering FIDO2 authenticator	No No	٥
Then perform this action	Authenticate using	<u> </u>
then the user may authenticate using *	Certificate (cloud deployment)	<u> </u>
If the preceding method fails or is not applicable, then	Password (cloud deployment)	<u> </u>
in the precessing method falls of is not applicable, then		• • • • ×
	CAN ADD FALLBACK METHOD	CEL SAVE
	CAN	JAVE JAVE

11. **VERY IMPORTANT** In order to ensure you can log back in as local administrator into Workspace ONE Access you will have to append your Access URL with **/SAAS/auth/0** you will be able to log on and change the **default access policy** from Auth0 to Certificate (**cloud deployment**) with a fallback to **Password (cloud deployment)** with a fallback to **Password (cloud deployment)** with a fallback to **Password (cloud deployment)** with a fallback to **Password** (**Local Directory**).

In this lab you saw the power of leveraging existing identity databases (both corporate and personal) in order to provide central authentication and single-sign-on to various corporate applications using Workspace ONE Access.

This concludes the Bonus Material for the Auth0 integration as Third-party OIDC Identity Provider.

Author: Simeon Frank