

dhushon / iamswhoiams

Private

Federate Identities from authoritative IdP (Azure AD) to Okta via intermediate SP

MIT License

0 stars0 forks

Star

Unwatch

<> Code

Issues

Pull requests

Actions

Projects

Security

Insights

main

iamswhoiams / idfed.md

dhushon

Update idfed.md ...

History

1 contributor

122 lines (72 sloc) | 7.48 KB

Federating AAD with Okta for Multi-Cloud Self-Service Project Creation

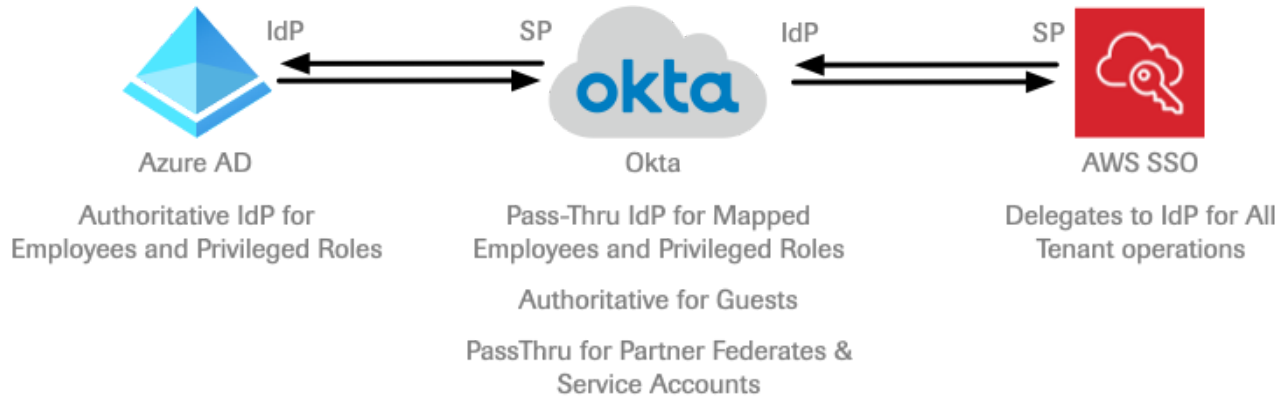
The goal of this project is to demonstrate the ability to create a non-authoritative Enterprise IdP (SP?) for use in building Advance Development Tenancies (ADT) in a variety of Public Cloud and SaaS platforms. Since the ADT's MAY use subscriptions/accounts slaved off 2, existing parent domains and maybe more provided by clients/partners, it's important that administrative access be maintained by IT, Security and Audit for the purpose of monitoring and emergency actions.

At the same time, it is likely that 3rd parties will need to be involved in the development, integration, and demonstration of these projects and as such, an easier way to grant privileged/non-privileged principal accounts as well as service accounts will be pre-requisite to success.

https://github.com/dhushon/iamswhoiams/blob/main/idfed.md

1/12

To prevent misconfiguration, privilege bleed-thru and resource visibility, as well as Commercial/GCC multi-directory challenges, using an Hybrid IdP WILL be important to the success of this project.



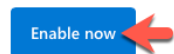
The goal being to create a **Layered** IdP/SP Domain capability for ADT in which Okta becomes the delegate AuthN/Z provider for the ADT created accounts and services. One interesting point is that Okta CAN act as an LDAPS IdP and therefore for some remaining DataCenter assets running linux with LDAP, Okta might become a more authoritative IdP for those services in it's hybrid mode.

Still, we do expect that Employees / Devices / Productivity services will remain in EAD as the primary IdP whether thru AAD or AD Connect for the hybridization or authoritative reference.

Get Instance of Azure Active Directory (AAD)

Free trials of AAD are available from Microsoft [here](#)

Enable Azure Active Directory Premium trial



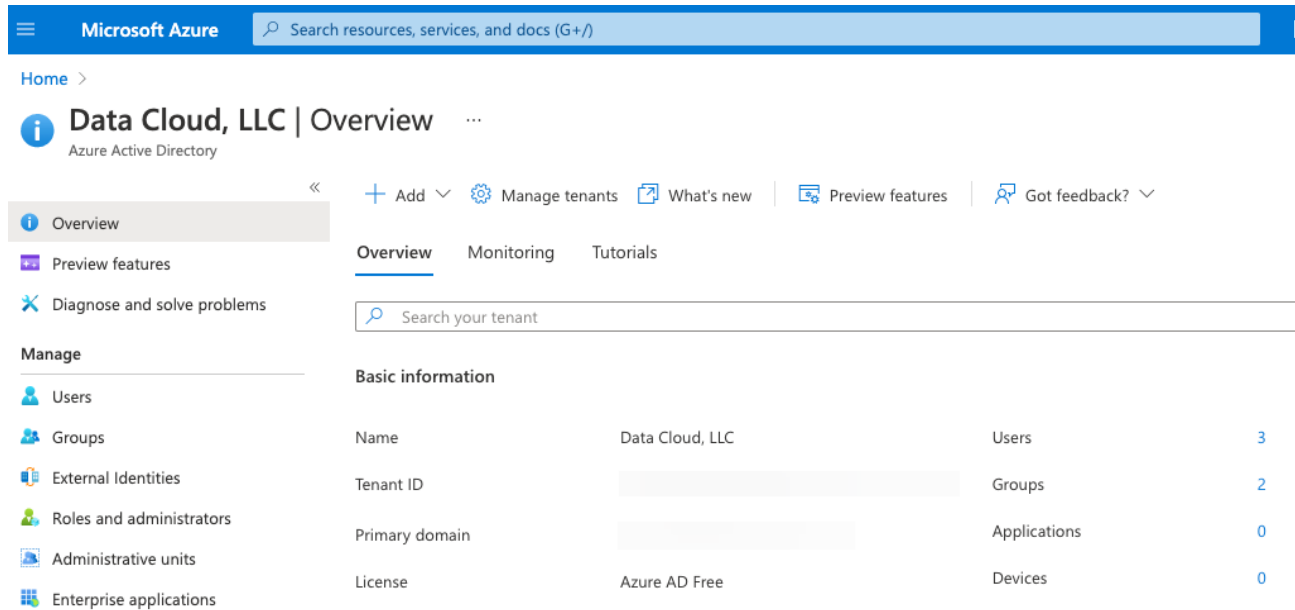
[Learn more >](#)

See how in 5 simple steps



1. [Open Active Directory](#)
2. [Pick a directory](#)
3. [Activate the trial](#)
4. [Confirm your licenses](#)
5. [Assign your licenses](#)

I used my GitHub account identity to provision my instance and was able to setup via the portal. Notice that automation of the creation of specific creation, development, promotion, deployment, and destruction inclusive of specific Service Principals and the assignment of principals to groups will likely leverage the Azure CLI or PowerShell environments for continuous changes in membership.



Microsoft Azure Search resources, services, and docs (G+/)

Home > **Data Cloud, LLC | Overview** ...

Azure Active Directory

Overview | Preview features | Diagnose and solve problems

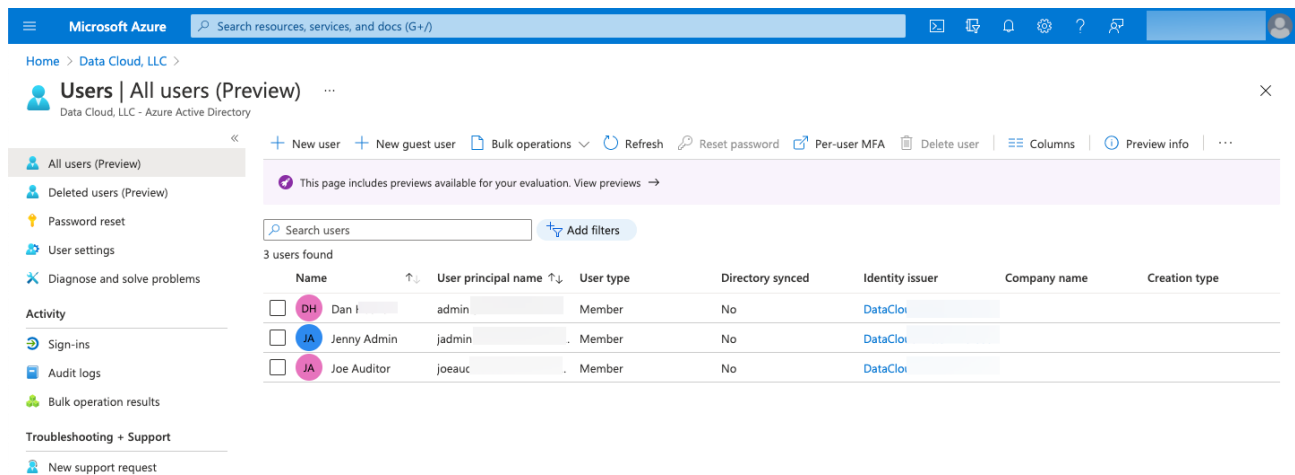
Manage: Users, Groups, External Identities, Roles and administrators, Administrative units, Enterprise applications

Basic information

Property	Value	Count
Name	Data Cloud, LLC	Users: 3
Tenant ID		Groups: 2
Primary domain		Applications: 0
License	Azure AD Free	Devices: 0

Provision Users

Click on Manage->Users:



Microsoft Azure Search resources, services, and docs (G+/)

Home > Data Cloud, LLC > **Users | All users (Preview)** ...

Data Cloud, LLC - Azure Active Directory

+ New user + New guest user Bulk operations Refresh Reset password Per-user MFA Delete user Columns Preview info

This page includes previews available for your evaluation. View previews →

Search users Add filters

3 users found

	Name	User principal name	User type	Directory synced	Identity issuer	Company name	Creation type
<input type="checkbox"/>	DH Dan I.	admin	Member	No	DataCloi		
<input type="checkbox"/>	JA Jenny Admin	jadmin	Member	No	DataCloi		
<input type="checkbox"/>	JA Joe Auditor	joeauc	Member	No	DataCloi		

To create users - email, firstName, lastName, company and principalEmailAddr are all mappable fields.

Provision Groups

Click on Manage->Groups:

I had started out creating groups so I could add a group to the application vs. each user, but given my trial instance vs. previous, I could not use the group at this point.

Configure Azure AD as an Identity Provider [to a Service Provider

First go into Azure AD -> Add Application (which is a Service Provider) and it will take you to the Gallery.

1. Click on "+ Create your own application".
2. A pop-up will appear to right, name your application, I used "Okta SP"
3. Click Create

Click Setup Single Sign On

The screenshot shows the Microsoft Azure portal interface for an Okta Enterprise Application. The left sidebar contains navigation links: Overview, Deployment Plan, Manage, Properties, Owners, Roles and administrators (Preview), Users and groups, Single sign-on, Provisioning, Application proxy, Self-service, Security, Conditional Access, Permissions, Token encryption, Activity, and Sign-ins. The main content area is titled 'Okta | Overview' and includes a 'properties' section with fields for Name (Okta), Application ID (55e808d2-96e3-489b-8641-...), and Object ID (5e58daa9-5b86-479b-9d23-...). Below this is the 'Getting Started' section with five steps: 1. Assign users and groups, 2. Set up single sign on (highlighted with a red arrow), 3. Provision User Accounts, 4. Conditional Access, and 5. Self service.

Then select SAML

The screenshot shows the 'Select a single sign-on method' page in the Microsoft Azure portal. The page title is 'Okta | Single sign-on'. The main content area displays four options: Disabled, SAML (highlighted with a red arrow), Password-based, and Linked. The SAML option is described as 'Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.'

AAD will then provide a set of integration points:

SAML Signing Certificate

Edit

Status	Active
Thumbprint	9CEA37643ACE0D710AD63296857B251D1FCA5C48
Expiration	12/20/2025, 3:50:17 PM
Notification Email	
App Federation Metadata Url	https://login.microsoftonline.com/d7e35a83-2b67...
Certificate (Base64)	Download 3
Certificate (Raw)	Download
Federation Metadata XML	Download

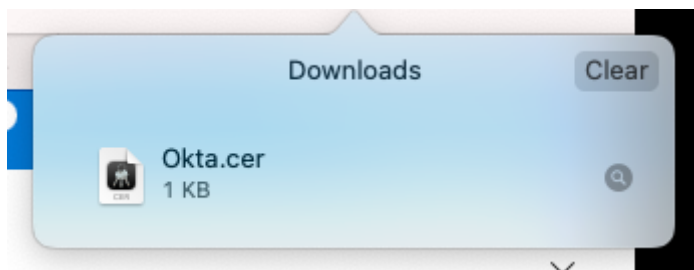
Set up Okta

You'll need to configure the application to link with Azure AD.

Login URL	https://login.microsoftonline.com/d7e35a83-2b67... 2
Azure AD Identifier	https://sts.windows.net/d7e35a83-2b67-4131-9f1... 1
Logout URL	https://login.microsoftonline.com/d7e35a83-2b67...

[View step-by-step instructions](#)

Click "Download" where you see the "3" to download the Base64 Certificate



Setup Okta with Azure AD as Identity Provider (IdP)

In a new window or tab (recognizing that you will be cutting and pasting between the okta and azure ad management consoles...

1. Log into your Okta tenant / or secure a trial tenant and configure

35 days left in your trial. [Contact Sales](#)

See Okta's Business Continuity plan for COVID-19 here: [Our Commitment to Customer Success: People, Business, and Service Preparedness](#)

okta Search...

Dashboard
Directory
Applications
Security
General
HealthInsight
Authentication
Multifactor
Identity Providers
Delegated Authentication
Networks

Identity Providers

Identity Providers Routing Rules

[+ Add Identity Provider](#) [Settings](#) Search...

Name	Type	Account Mode	Profile Source
01101110 01101111 01100100 01100100 01101001 01101110 01100111 Nothing to show Try searching or filtering			

2.

Navigate to 'Admin' → 'Security' → 'Identity Providers'

Identity Providers

Identity Providers Routing Rules

[+ Add Identity Provider](#) [Settings](#)

[Add Facebook](#)

[Add Google](#)

[Add LinkedIn](#)

[Add Microsoft](#)

[Add Apple](#)

[Add OpenID Connect IdP](#)

[Add SAML 2.0 IdP](#)

3.

Click on 'Add Identity Provider'

4. Click on 'Add SAML 2.0 IdP'

5. **Add Identity Provider**

General Settings

Name: **Azure AD IdP**

Protocol: SAML2

Authentication Settings

IdP Username: Enter expression or pick from list... [Expression Language Reference](#)

Filter: ☐ Only allow usernames that match defined RegEx Pattern

Match against: Okta Username
Choose the user attribute to match against the IdP username.

Account Link Policy: Automatic

Auto-Link Restrictions: None

Now Name the IdP something reasonable

6. Enter the following information (choose a name of your choice)

Enabling JIT is a choice. You can choose not to enable JIT if you don't want Okta to auto-create users when they login for the first time using Azure AD account. Given the "provision thru" model of our user-story and automation, it is an important facet of the layered provisioning and routing.

If no match is found ?

☒ Create new user (JIT)
 ☐ Redirect to Okta sign-in page

JIT Settings

Profile Source ?

☒ Update attributes for existing users

Reactivation Settings ?

☐ Reactivate users who are deactivated in Okta
☐ Unsuspend users who are suspended in Okta

Group Assignments ?

Assign to specific groups ▼

Specific Groups

companyName

Select groups that the IDP users should be always be added to.

7. Copy & paste SAML protocol settings from Azure AD to Okta paying special attention to the fact that from the Azure Setup/Signing Certificate and Okta the field order shifts.

SAML Signing Certificate

Status: Active

Thumbprint: BC734E4122942455C30751DE62E8097688A1F903

Expiration: 8/10/2023, 6:54:07 PM

Notification Email: rajprince.tenant@technobran.onmicrosoft.com

App Federation Metadata Url: <https://login.microsoftonline.com/414092c5-59a7-4dad-b123-591d917225a7/>

Certificate (Base64): [Download](#)

Certificate (Raw): [Download](#)

Federation Metadata XML: [Download](#)

Set up Okta SP

You'll need to configure the application to link with Azure AD.

Login URL: <https://login.microsoftonline.com/414092c5-59a7-4dad-b123-591d917225a7/>

Azure AD Identifier: <https://sts.windows.net/414092c5-59a7-4dad-b123-591d917225a7/>

Logout URL: <https://login.microsoftonline.com/common/wsfed...>

SAML PROTOCOL SETTINGS

IdP Issuer URI: <https://sts.windows.net/414092c5-59a7-4dad-b123-591d917225a7/>

IdP Single Sign-On URL: <https://login.microsoftonline.com/414092c5-59a7-4dad-b123-591d917225a7/>

IdP Signature Certificate: [CN=Microsoft Azure Federated SSO Certificate](#)
Certificate expires in 1094 days

[Show Advanced Settings](#)

8. Now Click 'Add Identity Provider'

SAML Protocol Settings

IdP Issuer URI ?

https://sts.windows.net/d7e35a83-2b67-4131-9f1e-41c3

1

IdP Single Sign-On URL ?

https://login.microsoftonline.com/d7e35a83-2b67-4131

2

IdP Signature Certificate ?

CN=accounts.accesscontrol.windows.net
Certificate expires in 1607 days

3

Show Advanced Settings

Add Identity Provider

Cancel

9. Now go back and expand the Identity provider

Okta Identity Providers configuration interface. The left sidebar shows the navigation menu with "Identity Providers" selected. The main content area displays the "Identity Providers" tab, showing a table of configured providers. The "Azure AD IdP" provider is listed with the following details:

Name	Type	Account Mode	Profile Source
Azure AD IdP	Saml2	JIT	✓
IdP ID	Ooas46	i95	
SAML metadata	Download metadata		
Assertion Consumer Service URL	https://vdatacloud.okta.com/sso/sai	pwRIL	1
Audience URI	https://www.okta.com/saml2/service-	umjqmr	2

10. And COPY the two SAML protocol settings from Okta to Azure AD (note a reversed field / text entry box order again)

Home > Data > Enterprise applications > Okta > SAML-based Sign-on

Okta | SAML-based Sign-on

Enterprise Application

Overview
Deployment Plan
Manage
Properties
Owners
Roles and administrators (Preview)
Users and groups
Single sign-on
Provisioning
Application proxy
Self-service
Security

Set up Single Sign-On with SAML

Read the [configuration guide](#) for help integrating

1 Basic SAML Configuration

Identifier (Entity ID)
Reply URL (Assertion Consumer Service URL)
Sign on URL
Relay State
Logout URL

2 User Attributes & Claims

givenname
surname
emailaddress

Basic SAML Configuration

Save

Identifier (Entity ID) *

The default identifier will be the audience of the SAML response for IDP-initiated SSO

Default

http://adapplicationregistry.onmicrosoft.com/customappssso/primary

https://www.okta.com/saml2/service-provider/spalq

Reply URL (Assertion Consumer Service URL) *

The default reply URL will be the destination in the SAML response for IDP-initiated SSO

Default

https://vdatacloud.okta.com/sso/saml2/Ooas4

Inbound Federation is now complete!

Mapping the "Claims"

The IdP responds to authentication requests with a token that include meta data that is useful for establishing identity, groups, roles and other potential decisioning within the upstream Provider. In our case we are including companyName / organization and can map this to employees to facilitate Okta JIT adds to employee groups.

Home > Data > Enterprise applications > Okta > SAML-based Sign-on

User Attributes & Claims

+ Add new claim + Add a group claim Columns

Required claim

Claim name	Value
Unique User Identifier (Name ID)	user.userprincipalname [nameid-for... ***

Additional claims

Claim name	Value
email	user.mail ***
firstName	user.givenname ***
lastName	user.surname ***

11. Click on 'Edit' to update the claims. Importantly the Claim Name must match the field names in Okta directly. As such nomenclature such as namespace definitions must be removed, and the keys matched.

Testing the SP->IdP Inbound Federation

Now you can test the log thru semantics in Azure AD.

12. My configuration required one last setting, the assignment of IdP users/groups to the Application "Okta SP" as individuals need to be permissioned for the service. This might be an interesting place to ensure that employees are trained before allowing their credentials to be authorized for use in the ATD environment.

Federating Okta as an IdP to AWS as an SP

Step 2: [here](#)

Automation Development

Okta API's are available [here](#)