OKTA

* Okta :-

→ It's mainly an identity Provider (IDP)

→ Okta Connects any person with any application on any device that runs in the cloud.

* IDAAS :- (Identity as a Service)

→ IDAAS is cloud based authentication (or) identity management Service, operated by 3rd party vendor like okta, ping identity, one login.

* Identity :-

The fact of being who (or) what a person (or) thing is

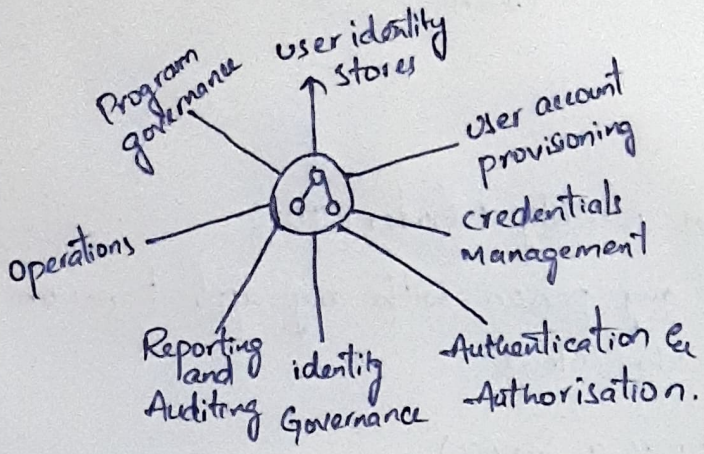
* Digital Identity :-

System to represent an external agent that agent may be a person organisational digital identity is the body of information about an individual.

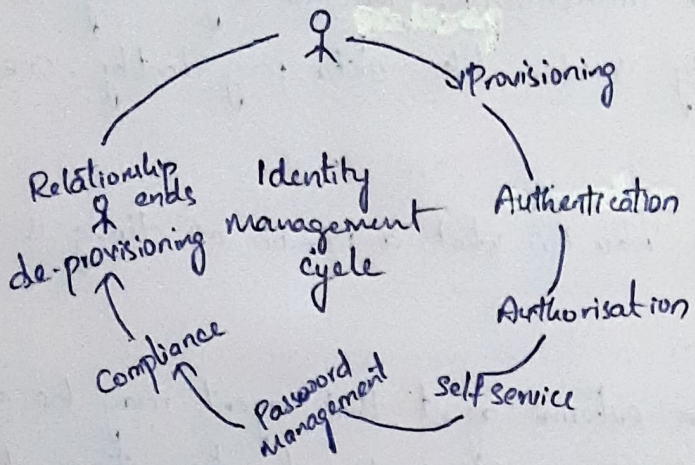
Organisation or electronic device that exists online or a digital identity is information on an identity used by computer, application, or device.

Examples of data points that can help from digital identity include

1) username & password
2) Purchasing behaviour or History
3) Date of birth
4) Social Security number
5) Online Search activities, Such as electronic transactions
6) medical history



* Relationship begins



Authentication & Authorisation :-

* Authentication :-

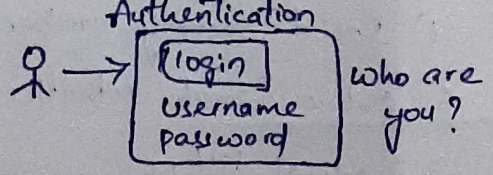
Authentication is the process of verifying "who you are". When you log on to a Pc with a username and password you are authenticating

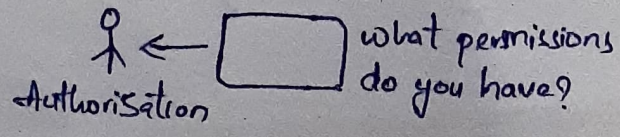
* Authorisation :-

Authorisation refers to what yo do it verifying that you have access to something

→ Authentication is the first step of authorisation so always comes first. Authorisation is done after successful

(Okta gives 10 types of authentications)





* Okta have around 1000+ SAML applications
* Okta have around 150 + mobile applications
* Okta have around 140 + provisioning of the userside.
* okta is also a tool who can directly map with the all of the softwares which are in the cloud.

IAM (identity Access management) :-

It is a system that stores, secures and manage all these identities and access privilages

→ IAM ensures that the user is granted controlled access to application or resources when any type of user logs in
  * From any location
  * On any networks
  * on any device

→ IAM most common solutions include Single sign on, multifactor authentication and Access management.

Cloud :-

Cloud refers to software (or) service that are accessed via the web instead of locally on your computer (or) on premises servers

The advantage of cloud is that you can access your information or applications on any device with an internet connection.

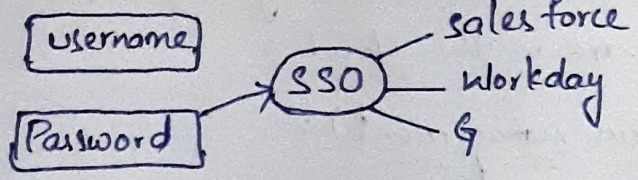
On-Premises :-

Refers to the software (or) technology hosted and run on local machines/computers on the premises of an organisation as opposed to running remotely on hosted server (or) in the cloud.

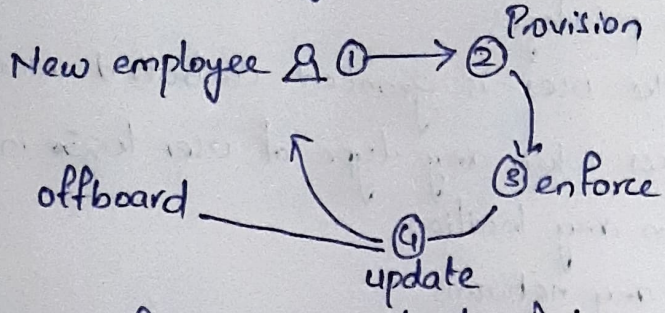
Single Sign-on (SSO) :-

It is a service that permits a user to use one set of login credentials (ex: name and password) to access multiple applications

The Service authenticates the end user for all applications the user has been given rights to and eliminates further prompts to log in when the user switches applications during the same session.



LCM (Life cycle management) :-



MFA (Multi-factor authentication) :-

Multifactor authentication allows organisations to configure login policies, which require users to enter additional credentials beyond a password, to verify their identity supported second factors include security question, soft-token, and third party hardware devices

Okta benefits :-

* Manage your users, apps, groups and policies and even external directories such as active directory.

Apps can be integrated with Okta :-

Supports specific authenication and authorisation protocols SAML 2.0 and OIDC/auth mostly.

Features of Okta :-

Active directory integration, LDAP integration, SSO to apps like office 365, Gsuite, AWS and many others, centeralised de-provisioning of users, MFA solutions, flexible policies, Mobile identity management.

Login to okta :-

Okta free trail account
↓
30 days
↓
Fill the details
↓
account will be created

Few software needed to okta :-

* Virtual box (Oracle virtual box download)
* windows 2016 server iso file
↓
Try windows server 2018 essentials on microsoft evaluation center
↓
ISO
↓
Download

* After downloading oracle virtual box
* click on new button
  - Name of the machine
  - Type (microsoft windows)
  - Version (windows 7 (64-bit))
  - Next
  - memory size
  - next
  - Create a virtual hard disk now
  - Create
  - VDI (virtual box disc image)
  - Next
  - Dynamically allocated
  - Next
  - Create
* After creating you need to setup the things
  - Settings
  - Basic
  - Name (DC)
  - Type
  - Version.

Advance

↓

Shared clipboard (bidirectional)

↓

Drag n drop (bi directional)

↓

Next part will be system part

↓

System (System part)

↓

Motherboard

↓

Increase base memory

↓

boot order (Optical - 2nd
↓ Harddisk - 1st)

Processor (2 processor)

↓

Display (part)

↓

Video memory (make it large) (54MB)

↓

Storage (storage part)

↓

Choose empty disk symbol

↓

Right side (disk symbol)

↓

Choose a disk file

↓

windows iso file

↓

Audio by default (part)

↓

Network (part)

↓

Adapter 1

↓

Attached to (bridge adapter)

Name : Intel (R) Dual Band wireless-N 7265

↓

Advance (session)

↓

Adapter Type (Intel Pro/1000 MT Desktop (82540EM)

↓

Promiscuous mode

↓

Seriport (by default) No need to change

↓

USB (by default)

↓

Shared folder (by default)

↓

user interface (by default)

↓

OK

↓

After creating

↓

Click on show (Normal start)

↓

After starting

↓

Click on input

↓

keyboard (insert ctrl + Alt + del)

↓

It's enter into Screen part

↓

username and password

↓

Next screen will be going to populated

↓

set up

↓

Server manager

↓

Add roles and features.

Role based (or) feature based installation

↓

Next

↓

Select a server from the server pool

↓

Next

↓

Choose (Active directory Domain Service, Active directory federation Service

↓

Next

↓

Next

* After installation AD if you get any errors like yellow flag will be get notifications

↓

Go to yellow flag

↓

Promote this server to a domain controller

↓

Add a new forest

↓

Root domain name (oktawin.com)

↓

Next

↓

Password

↓

Confirm password

↓

Next

↓

Next

↓

Next

↓

Next

↓

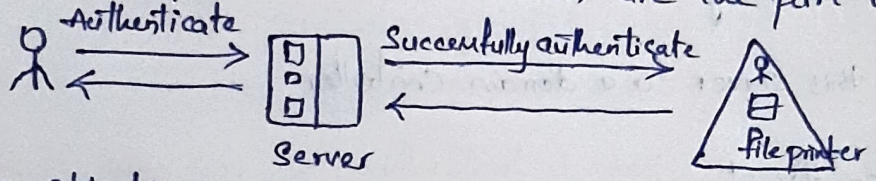
Next

↓

Install

Active directory :

* Information about all the objects - users, computers, resources like printers, shared files/folders - in an organisations network
* It is a repository where you can s. all your objects with in the organisation network
* It is similar to a telephone directory
* It is a software to arrage, store information, provides access and permission based on those information.
* Arrange all the network users, computers and other objects into logic hierarchial groupings
* Active directory information is used to authenticate / authorise the users, computers, resources which are the part of a networks



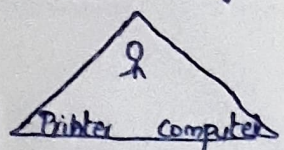
* Active objects
  - → physical entity of a network
  - → can be describe by a set of attributes

Objects :-

* Forest
* Domain
* Organisation unit
* users
* Contact
* Computer
* Shared folder
* Printer
* Site
* Subnet

Active directory objects :

* Objects are explained by their attributes like Name, location, department etc.
* Container object



When we club all the users in one manner (or) in one box we can call it as container object.

* Leaf object

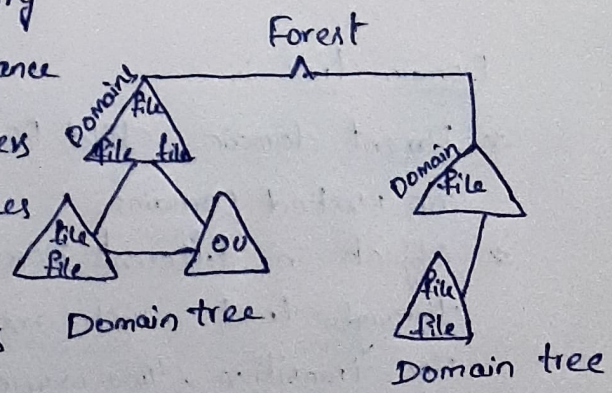
we are talking individual personality, individual effect you can call it is a leaf object.

, computer, printer

* Security principle objects :-
  * Object that can be authenticated and assigned permissions
  * Each object has a
    GUID - 128 bit (globally unique identifier)
    SID - Security identifier for each security principal object
    SID - contains unique number

Active directory forest :-

* Highest level of security laboratory
* A complete active directory instance
* Objects like Domains, users, Computers printers and other network resources
* Information and data exchange can happen only b/w the objects inside a forest
* To communicate with objects in other forest, explicit created forest level trust are required.

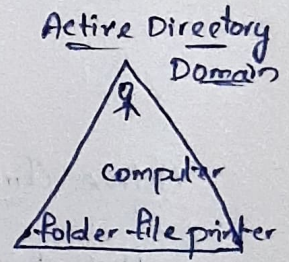


* Can Contain one (or) more domains or a combination of domain (or) domain trees.
* The Schema (or) design of an AD is consistent throughout the forest.

Active directory Domain :-

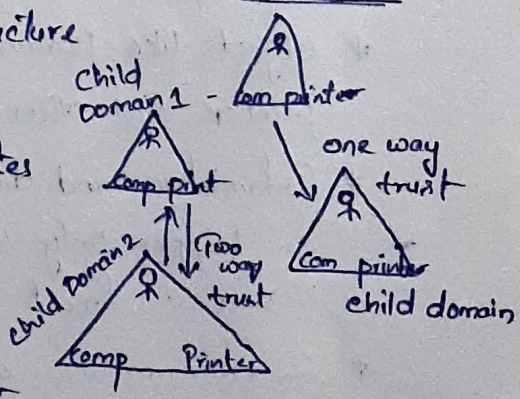
* logical grouping of objects
* Administrative boundary for objects
* No limits on the number of objects that can be contained in a domain
* Objects need not be in a same physical location.
* Domain Controller is the domains supreme authority.

* Domain Controller :-
  * DC is responsible for all the authentications, authorisations, additions, deletions, edits, modifications inside a domain.
  * If an user an access to a domain, he can log on from anywhere and any computer in a domain
  * The permissions, policies and rights can be set for all the objects at the domain level or at the individual object level as well.



Domain tree :-

* Parent domain - child Domains) tree structure (or) Nested Domains
* Objects in different Domains communicates through trust which are transitive, Non-transitive, Two way (or) one way
* By defaults, all the Domains in a forest are connected by transitive trust
* All Domains in a domain tree share a Contiguous name space.



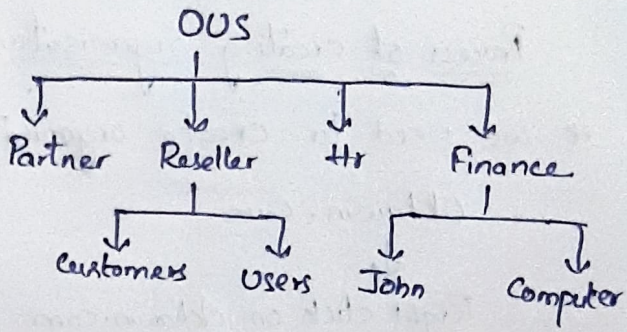
* In short domain has 4 components

1) A hierarchial structure of containers, objects
2) An unique domain name.
3) A Security mechanism to Authenticate and authorise access to Domains resources.
4) Policies that shows how functionality is allowed (or) restricted for users, computers in a domain

* Organisational Unit (OU)

→ All OU's inside a domain are connected
→ Group policies settings can be at the OU level.
→ Delegation of administrative control is possible in OU
→ Child OU(s) inherit the properities of the parent OU

Organisation Unit:-



Active directory users :-

* Part of the organisation
* Onique identity in the domain
* Access the domain resources
* Authorisation based access
* has an unique SID

Active directory computers :-

* Individual computers / workstations, Servers which are part of a network.
* Each computer has a unique computer account.
* Computer account allows each computer to be authenticated and authorised for access to the domain and domain resources
* A Server could be a domain controller (or) global catalog Server (or) a member Server.

Active directory Contact :-

* An individual who is not part of the organisation but related to the organisation
  Ex:- Customer, Supplier, Vendor etc.
* Unlike an user, a Contact cannot logon (or) access the domain (or) network.
* Cannot be assigned permissions (or) authorisations (or) restrictions
* After login to the Server.
* Go to tools
  ↓
  Active directory users and computers

[Oktawin.com → Forest
Inside forest we have
Objects]

[under domain controller
we can see our parent
machine]

Process of creating organisations unit :-

* we need to create organisation unit under Oktawin.com forest.

Oktawin.com
↓
Right click on oktawin.com
↓
New
↓
Organisational Unit
↓
Name (oktawin.com)
↓
Ok

* After creating first we need to create Domains inside the forest

Oktawin.com
↓
Rightclick on Oktawin.com
↓
New
↓
Organisational Unit
↓
Name (India)
↓
Ok

* oktawin.com (Domain)
  ↓
  Right click on oktawin.com
  ↓
  New
  ↓
  organisational unit
  ↓
  Name (US)
  ↓
  ok.

* After that we need to create two OU's under India

  India
  ↓
  Right click on India
  ↓
  New
  ↓
  Organisational unit
  ↓
  Name (Bangalore)
  ↓
  Ok

  * India
  ↓
  Right click on India
  ↓
  New
  ↓
  organisational unit
  ↓
  Name (Hyderabad)
  ↓
  Ok

  * US
  ↓
  Right click on US
  ↓
  New
  ↓
  Organisational unit
  ↓
  Name (California)
  ↓
  ok.

  * US
  ↓
  Right click on US
  ↓
  New
  ↓
  organisational unit
  ↓
  Name (New york)
  ↓
  Ok.

* After that we need to create two OU's under US

* In Hyderabad you need to create sub folder.

* Hyderabad
↓
Right click on Hyd
↓
New
↓
Organisational Unit
↓
Name (hr)
↓
ok

* Hyderabad
↓
Right click on Hyd
↓
New
↓
organisational unit
↓
Name (IT)
↓
Ok.

* Under California you need to create sub folder.

California
↓
Right click on California
↓
New
↓
Organisational Unit
↓
Name (sales)
↓
Ok.

California
↓
Right click on California
↓
New
↓
organisational Unit
↓
Name (finance & Accounts)
↓
ok.

* If you want to delete any OU (Organisational) Unit)

click on created OU (IT)
↓ click
Right on IT
↓
Properties
↓
Object
↓
uncheck (protect object from accidental deletion)
↓
Apply
↓
Ok.

Group Scope :-

Domain local group :-

To give access to resources in the same domain as the group, users can be from different domains

Global group :-

To give access to resources that are in different domains to users from a specific domain.

Universal group :-

Used to give access to resources located in different domains to a group of users from different domains

Active directory groups :-

* Contains users and computers who are called members of the group.
* All permissions, authorisations and restrictions placed on the groups apply to all the members of the group.

Two types of groups :-

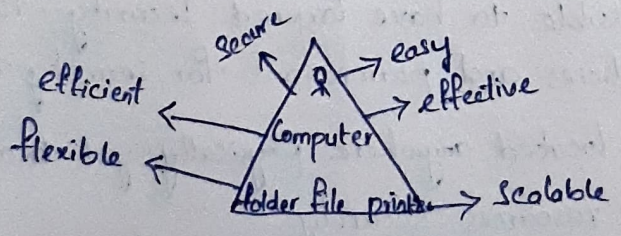
1) Security groups
2) Distribution groups

Why should we need to active directory Services :-

* Highly Secure - possible to have layered security, that is have policies and permissions for security at different levels
* Objects can be located anywhere physically yet to access the domain/network's resources Securely.
* Millions of users can be added to a single domain, easily Scalable, highly flexible, readily extensible.
* Easy, efficient search mechanism to locate an object

* Centralised storage :- for users, departments which make back up and restore - efficient, fast and easy.
* efficient and efficiency management of services because of centralised management of services
* Server as a platform for services like exchange, Sharepoint etc.,
* Enable Single Sign-on (SSO) and pre and post action scripts like logon scripts
* Individual profiles - users can have the same environmental settings immaterial of which computer or location they logon from.
* Mandatory profiles - It is also possible to restrict the environment that is make only a specific set of applications and services to a set of users (or) Computers.
* Centralised Auditing - which makes it easier to track all the operations
* Active directory uses in organisations like government, schools, Corporates, Non-government, Hospitals, Research organisations.

Active directory services - one stop solution :-



* Cost effective management and control mechanism to control all the objects, resources and information in an organisation / networks.

* creating group policy management :-

Active directory

↓

Tools

↓

Group policy management

↓

Need to create a forest

↓

After creating forest

↓

Need to create domain

↓

Right click on under domain with the name Oktawin.com

↓

Create a GPO in this domain and link it here

↓

Name (wallpaper)

↓

Ok

After creating GPO

Click on GPO

↓

Right click on wall paper1

↓

Edit

↓

Next click on user configuration.

↓

Policies

↓

Administrative templates

↓

Desktop

Desktop

↓

Desktop wallpaper (double click) on (Right click edit)

↓

enable

↓

wallpaper Name [It should be in drive] and you should give the path of the downloaded file.

↓

wallpaper style → fit (Optional available)

↓

Apply

↓

Ok

* After applying you need to restart your repository
* you can ~~apply~~ able to see wall paper on your desktop.

* Configuration of Active directory

Directory
↓
Directory integrations
↓
Add directory
↓
Add active directory
↓
Set up Active directory
↓
Download agent.

[Active directory agent :-
light weight Secure connector that allow okta to integrate with your okta active directory domain the agent enables Okta features such as users import and the deligated authentication]

* After downloading the agent
* Click on downloaded agent and agent will soon
* Next
↓
Install (agent will be installed in "C" drive)
↓
Domain (oktacoin.com)
↓
Next
↓
Use an alternate account (here we have option we can choose this one)
↓
username
Password :- we need to create a password
↓
Next (if there got errors) go for above one.
↓
Create a new okta Service account (mapping has to be established)
↓
Username
Password :- we need to create a password
↓
Next

Next
↓
Product there number of options will be available
↓
enter sub domain (okta win Sr → my subdomain of okta)
↓
Next

* If you get GOG error you need to setup the internet ~~things~~ settings
* After internet setting you will get popup like "Allow access" to active agent
* Finish
↓
Next
↓
okta username format (user principle name (UPN))
↓
Next
↓
Next
↓
Next
↓
Done

* How to create user in active directory
  * Goto Server manager
  ↓
  Tools
  ↓
  Active directory users and Computers
  ↓
  under organisation unit (OU) you need to create user
  ↓
  Right click on OU
  ↓
  New
  ↓
  First name
  ↓
  last name
  ↓
  Full name (There is no space in full name)
  ↓
  User login name → Next → Create password → Finish

* How to import the users from Active directory to okta

Directory
↓
Directory integration
↓
Active directory
↓
import
↓
Import new
↓
Incremental import (Here we have the another opinion full import (could take a while) (fastest)
↓
Import
↓
ok
↓
check the users list. click to check box all the users
↓
Confirm assignments
↓
Check the auto active user confirmation
↓
Confirm

Incremental import:
only imports Active directory users that were created (or) updated since your last import, users not present in the data will not be changed. (This is the type of import performed by automatic scheduled imports)

Full import (could take a while)
Replaces all users data with the imported user set users not present in the data will be deactivated

For example:
* Any changes made in user in active directory will go for "incremental import"
* There are to number of users are there in the Active directory we want all of the users are provision in the okta so that case we can use the "full import"

* How to create a group in okta :-

Directory
↓
Group
↓
Add Group
↓
Group name
↓
Group description
↓
Add group.

* How to Add users in a group :

* click on group you were created
↓
manage people
↓
list of users (you need to select the users)
↓
Save

* how to enable Control panel policy in Active directory

Server manager
↓
Tools
↓
groups and policies
↓
under forest (you need to create Control panel policy)
↓
Right click on oo
↓
create a GPO in this domain and link at here
↓
Name (Hide Control panel)
↓
ok.

*

* After creating new group policy
* Right click on Create policy (hide control panel)
  ↓
  Goto OU (oktawin)
  ↓
  Right click
  ↓
  Link with existing one
  ↓
  Choose hide control panel
  ↓
  Ok
* After that goto hide control panel policy
  ↓
  Right click on panel
  ↓
  edit
  ↓
  [redacted]
  ↓
  user configuration
  ↓
  Policies
  ↓
  Administration template
  ↓
  Control panel
  ↓
  Display
  ↓
  Disable the display control panel (double click)
  ↓
  enable
  ↓
  Apply
  ↓
  Ok

* After that go to hide Control panel
* Right click on hide control panel.
  ↓
  edit
  ↓
  user configuration
  ↓
  policies
  ↓
  Administrative templates
  ↓
  Control panel
  ↓
  prohibit access to control panel and Pc Settings (double click)
  ↓
  enable
  ↓
  Apply
  ↓
  Ok
* After that you need to restart your machine
* your cannot be seen your Control panel in your machine

* Overview of Single Sign-on in okta

→ Single Sign-on (SSO), frees people from password chains or having to remember my raid usernames and password needed to access the applications they use daily.

→ okta enables you to provide SSO access to cloud, on-premises and mobile applications with a single set of credentials once signed into okta you can launch any of your web applications without having to reenter your credentials. okta establishes a secure connections with a users browser and then authenticates the user to okta-managed apps using one of the available SSO authentication methods

* Secure web authentication (SWA) :-

→ SWA is an okta team and refers to a method developed by okta which which uses a browser plugin to securely pass credentials into web forms on behalf of the authenticated okta user.

→ SWA was created by okta to provide single sign-on for applications that don't support proprietary federated sign-on methods (or) SAML

→ The okta browser plugin is required.

End user plugins in okta :-

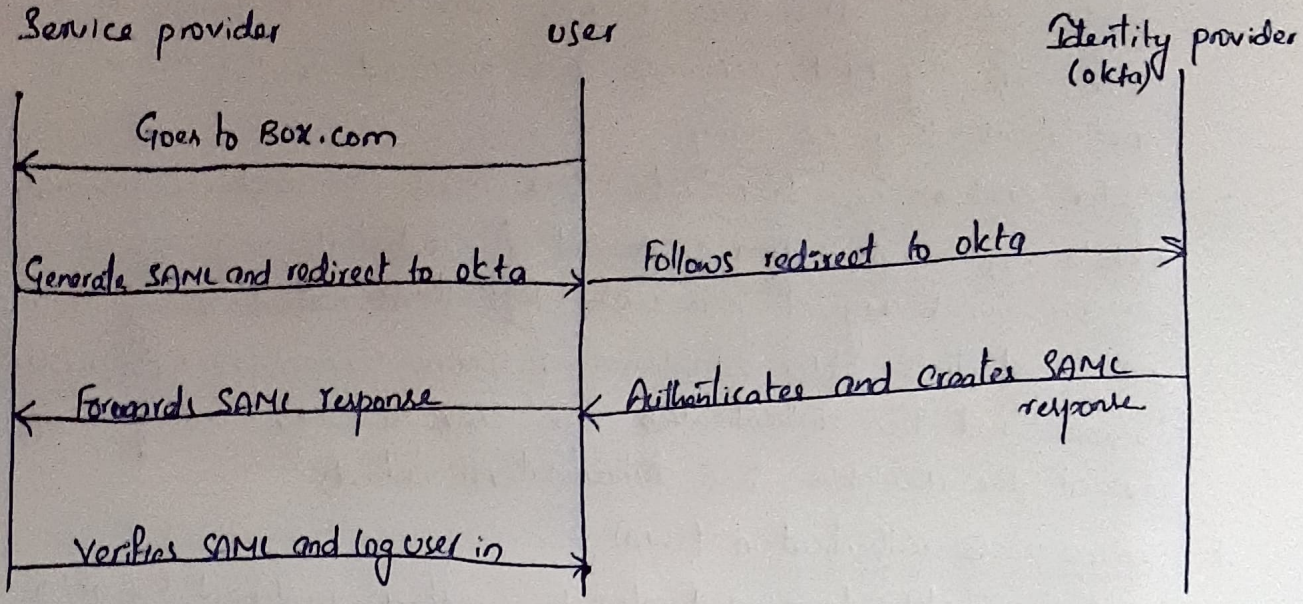
* Firefox, Internet explorer, internet explorer (windows installer), safari, Chrome, edge. (These are 3rd party notices)

Security assertion mark up language (SAML)

→ SAML is an XML based standard for exchanging authentication and authorisation data b/w an identity provider (or) IDP and a service provider (or) SP

→ SAML allows identity provider (like okta) to create a secure connection to a service provider. when using SAML, the service provider is not authenticating the user but rather trusting the secure authentication assertion from the identity provider

* okta - XML For Pat exchange (SAML) → SP (Box, Zoom, SLACK etc.)



WS-Federation:-

This authentication method is typically associated with Microsoft applications and works similarly to SAML

The okta integration Network (OIN)

The okta integration Network (or) OIN is a catalog of the industry's broadest and deepest integration with crucial enterprise applications. Customers gets simple, Secure access to thousands of apps and can even add their own applications if they do not already appear in the OIN

How to add application using SWA

Applications
↓
Application
↓
Add application
↓
Search in Search bar (linkedin)
↓
Add
↓
Next

* After you need to check the Sign on methods

↓

Administator set username password the same as users okta password.

↓

Application user name format (okta username)

↓

Update application username on (create and update)

↓

Done.

* After creating the application of linkedin
* Click on the application (linkedin)

↓

Assignments

↓

Assign

↓

Add person (Assign to people)

↓

choose user

↓

Save and go back

↓

Done

[If I change the username in okta user has to remember the both of the name like existing one and changed one]

Installation of plugin

Install plugin

↓

Add to chrome

↓

Add extension

These will install after application has been created in my app

* After assigning the application to the user
* Goto my apps
* Click on application it will redirect to the linkedin application

* How to create application using SAML

* The version of SAML 2.0

* Application
↓
Add application
↓
Drop box
↓
SAML 2.0
↓
View step instructions
↓
Start provisioning ☑
Check the box
↓
Done

Optional - whether we are going to be optional part its users choice

* After creating dropbox application you need to assign the user for the application.

Assignments
↓
Assign
↓
Assign to people
↓
choose the user
↓
Save and go backs
↓
Done.

Process of downloading drop box

Dropbox business
↓
dropbox business
↓
Get started
↓
Advanced
↓
Try for free
↓
Create your account
↓
Start free trial
↓
Continue with trial
↓
open
↓
Download dropbox
↓
Remind me later
↓
Admin Console
↓
Settings
↓
Single Sign-on (Authentication)
(Required) (many options or (optional) available)
↓
Copy the sign in URL from okta
↓
Paste the URL in dropbox SSO
↓
Download the certificate
↓
Browse the certificate and upload in dropbox
↓
Save (Sign-in off)

* Go to my app
* Click on dropbox application
  ↓
  It will redirect to the dropbox application
  ↓
  Continue
  ↓
  you will get inside the dropbox.

What is SSO?

Single sign-on is an agreement b/w three entities

1) Users
2) Identity provider
3) Service providers

Users :-

Individual people need to access different services. Users should be able to manage personal information such as their password and they should be uniquely identifiable.

Identity providers :- (Okta)

An identity provider tell us more about that user. It is the source of truth for not only who this person is, but also what roles they have. Those roles, inturn, inform other systems about what this person is allowed to do.

Service providers :- (dropbox, zoom, linkedin examples)

Service providers are traditionally applications, but they can include all sorts of products and services such as wifi access, your phone or "internet of things" devices like a smart lock (or) a refrigerator

Protocols :- (set of rules)

Basic Auth :-

A simple username and password schema on an app, by app basis

OAuth :-

API security model that relies on an outside identity provider and key-store to grant and deny access to API's

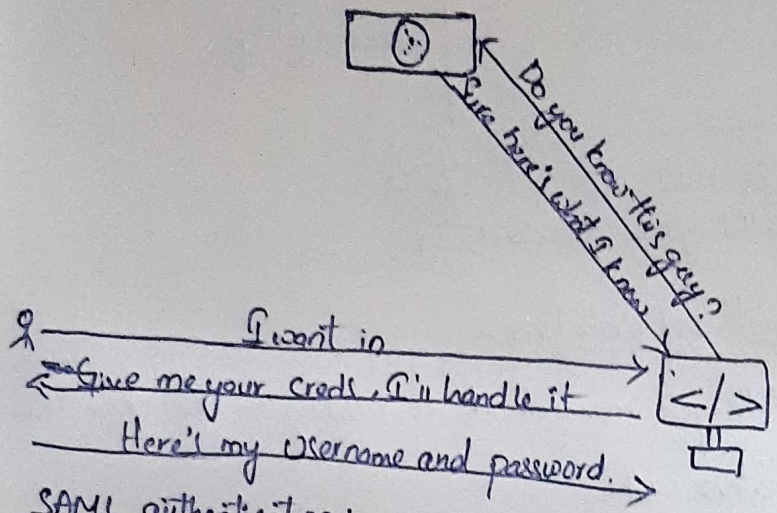
SAML :-

A web based model that allows a third party application (or) service to validate the users identity and retrieve details about that users.

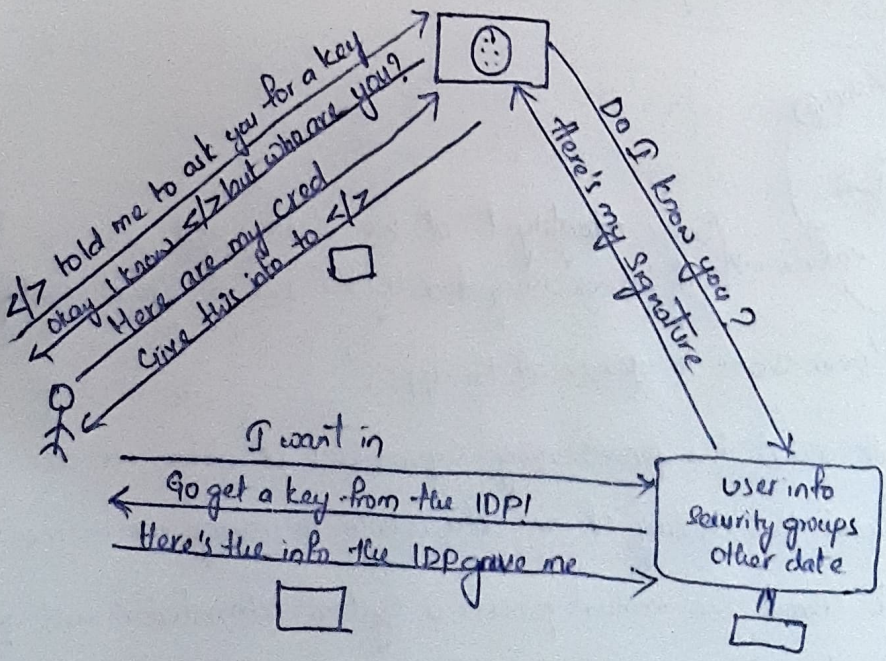
Imp-

* In the SAML basica thing is done by the Service provider its not asking for the authenticity of the user and.
* It is asking authentity from the identity provider, on the behalf of the identity provider, identity provider gives certification of the trust from the users.
* So identity in the certificate which is consumed by the service provider and. So by that way user will be authenticated.

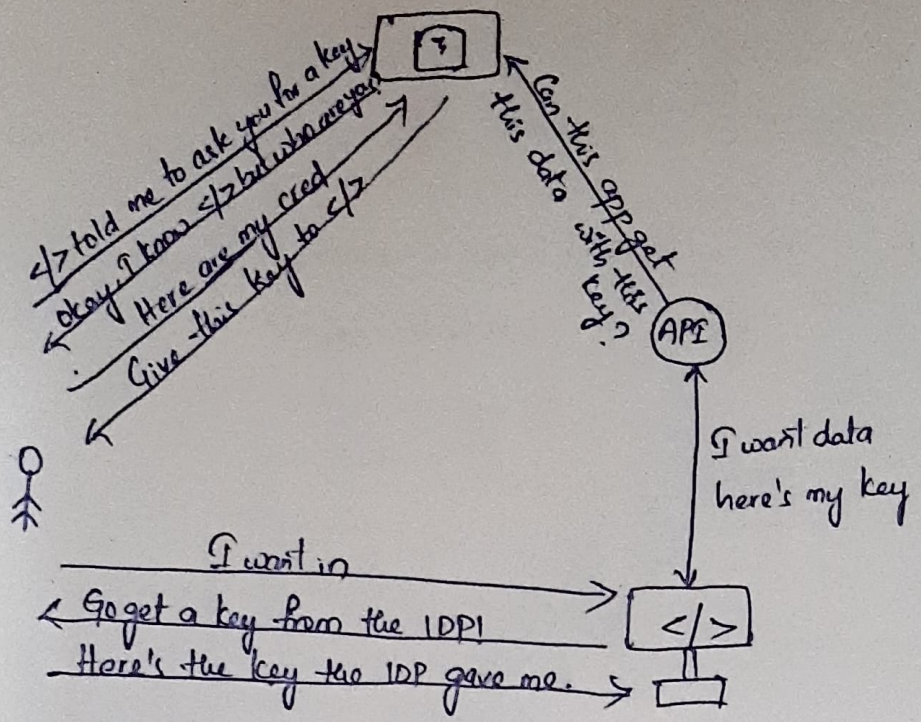
Basic authentication:-



SAML authentication:-

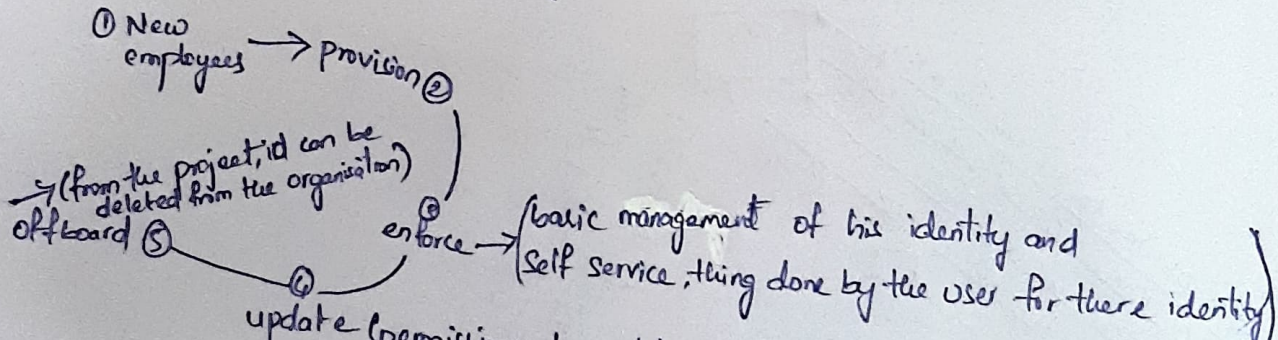


Typical authentication :-



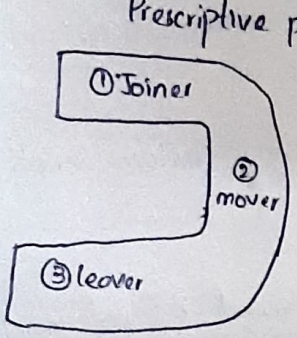
Automate lifecycle management and workflows :-

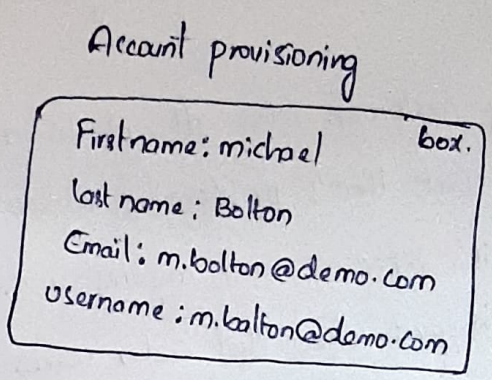
* lifecycle tells how the lifecycle management is working on the okta side
* how the flow of applications works.
* Every object has own life cycle



When we talk about the provisioning capabilities of okta, we are essentially talking about the ability of an okta admin to manage an entire user lifecycle. Think about the manual process a System administrator must go through when on boarding a new employee. They might have to first create a new account within active directory for the employee, Create a new account with in okta, and then finally Create accounts in any of the applications the employee may need to access to such as Box, workday, or Salesforce. It is a very tedious, time Consuming and manual Process.

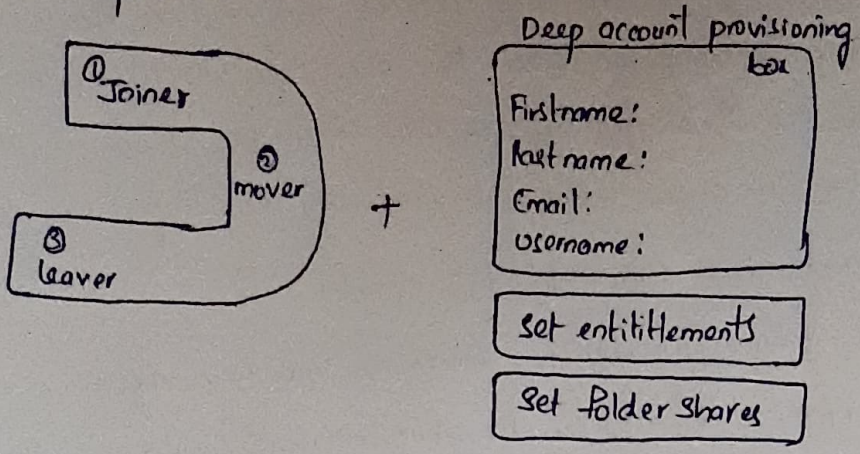
* with okta provisioning we can help automate some of these processes. when available, okta provisioning can cover the entire user life cycle from creating the new user account to updating the user attributes within the account and when the employee leaves the company or no longer requires access to the account and even deprovision the account.
* It is upto the service provider to determine via their application programming interface (or) APS as to whether (or) not provisioning capabilities will be available. when adding an application from the okta integration network or OIN should you want to focus your search to only those applications which do support provisioning. you can use the supports provisioning filter located on the left to view only applications which supports provisioning features.





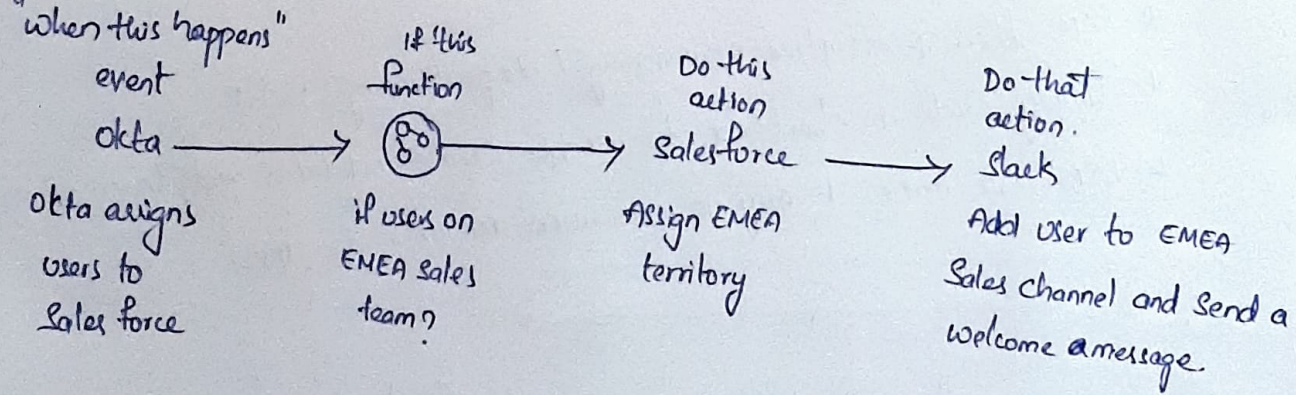
* okta's lifecycle management (LCM) helps connect users with apps, with LCM you are able to automate all lifecycles with any business process for external and internal users
* LCM offers prescriptive provisioning / deprovisioning paths
* Simply click a checkbox to enable creates, updates and deactivates
* LCM also make it easy to provision accounts to apps.

Be spoke workflows



* In some cases, Customers need to build be spoke workflows to handle unique business process. They need to add logic, timing and multiple actions to their joiner, mover and leaver processes. In other cases, Customers simply need to do more within a specific application. For example, in addition to provisioning a base account in Box, it might need to also set entitlements (or) set folder shares

* Many customers who attempt to automate are using custom scripts (or) Code. But that's problematic in two ways.
* First it's expensive and requires a ceilain skill set Second it's not maintainable what happens when that coder leaves your organisation?
* okta's workflow is the next step workflows allow you to automate identity-Specific tasks across apps without requires code



Okta workflows :-

* workflows is a interface - driven no code - required design console that facilitates the implementation of automated business processes, especially for identity related use cases. A key component of the product is integration with a wide range of third party apps and functions.

* About workflow capabilities :-

Okta workflows offers a number of powerful features towards efficient and automated account management.

with okta work flows, you can:

* Provision and deprovision app accounts.
* Sequence actions with logic and timing.
* Resolve identity creation conflicts
* Send notification for lifecycle event.
* Log and share life cycle events.

About the elements of okta workflows :-

A workflow, or flow, is a sequence of steps that represent the events, logic and actions in a use case.

* Event :- what has to happen for your flow to begin ? The first card in any flow is an event

* Action :-

what should happen if the application event occurs ? Action cards instruct your flow to send commands to applications

* Fuctions :-

use cases aren't always linear, how should action cards account for different scenarios ? Function cards let you act on the data from a card or branch into another logical flow.

How does it work?

The triggering event and the resulting actions in your use case are linked through Connectors and mapped input and output values.

* Connector - which applications are involved in your flow?
  Connectors enable you to interact with them without setting up API's

* Connection:-
  A connection is your unique level of access to the connected app (for example, admin or end user

* Input:-
  Input fields determine how an action (or) function card proceeds.
  For example the input field of the Search for user action card above is user details

* Output:-
  output fields contain the results are generated by the event, action, or function card. In the example flow above the user unassigned from application event card produces output values like date and time, message, event ID, Event type and event time.

* mapping:-
  The movement of data b/w card is referred to as mapping. To map data b/w cards, drag and drop the opposite field of one card to the input of another card. Be sure that the format of the fields match (text, number, true/false, date & time, object or list)

* How to add Automation

Work flow
↓
Automations
↓
Add automation
↓
Name (deactivating user)
↓
Save
↓

* After creating the automation we need to follow few steps below:

Add condition (when the following conditions are true)
↓
Select condition type (user inactivity in okta)
↓
Duration (2 days)
↓
Save

* After adding the condition we need to add action.

Add action (perform the following
↓
Action type (change user lifecycle state in okta)
↓
Change use state to (Deactivated)
↓
Save.

* Okta and office 365

* At okta, office 365 is our #1 integrated application. It is important that you explore the best configuration to ensure a successful implementation of office 365 with okta

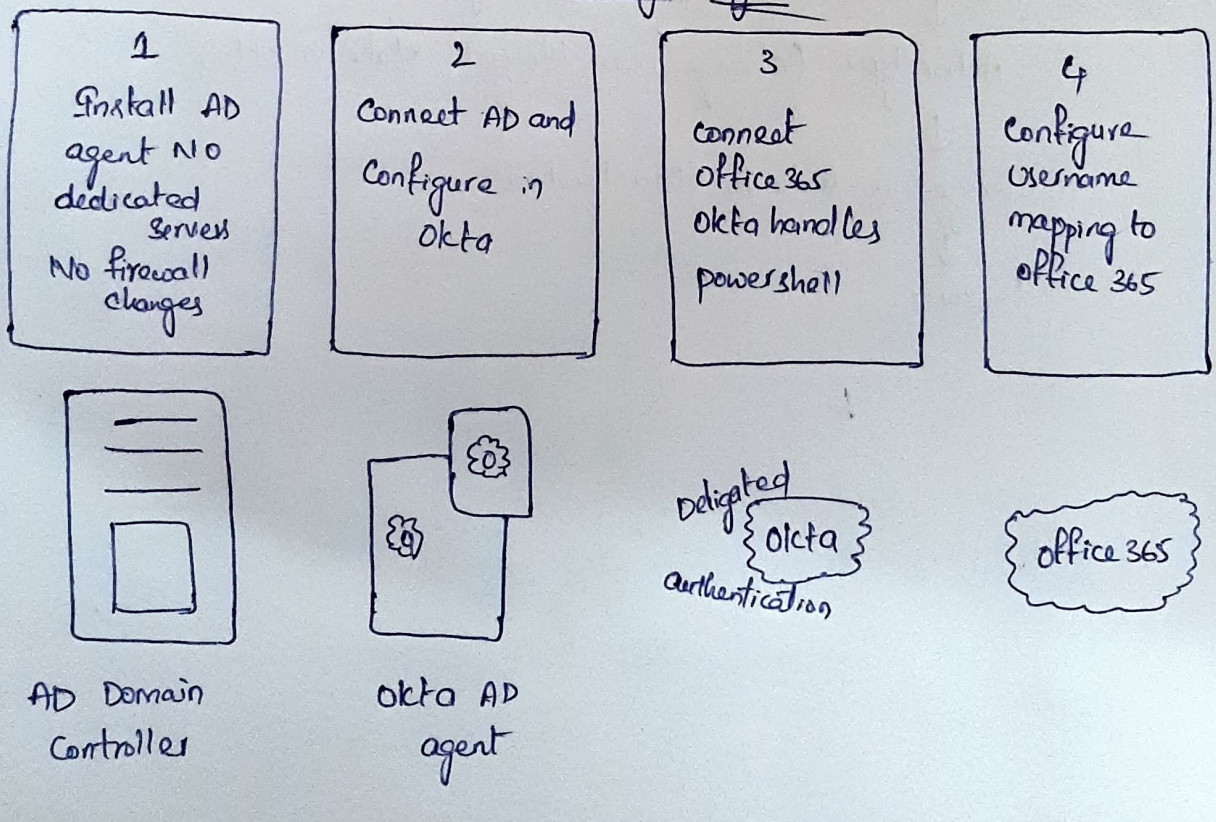
* Okta works with office 365 regardless of how your accounts are mastered, you can have active directory mastered users, LDAP mastered users, or okta mastered users

with regards to officers okta can do 2 very important things for you.

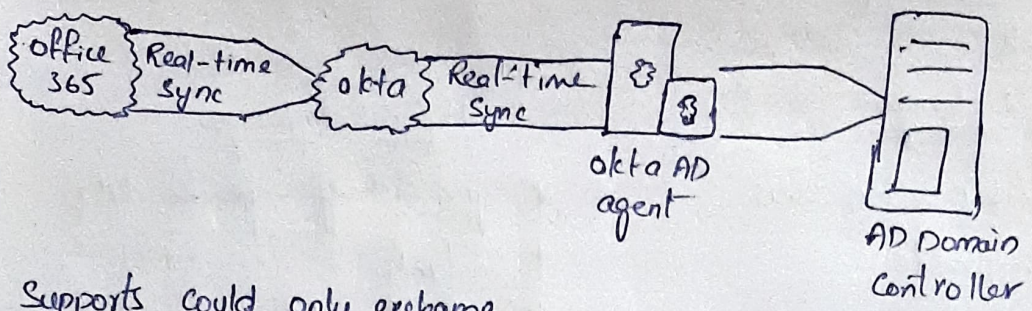
* we can federate (or SSO) using ws-federation, microsofts standard federation method which is very similar to SAML.

* okta can also provision users, a key part of the user lifecycle management flow.
with okta provisioning, we can automatically create the new accounts that users need within office 365, keep those accounts synchronised and then deprovision (or deactivate) an account when the user is deactivated in okta (or) within your external directory service such as Active directory

* use okta today for office365 Single Sign-on.



Okta office 365 provisioning



Supports could only exchange

* provision / deprovision users
* Sync rich profile
* Assign user roles
* Sync groups
* Transform attributes

Modern features

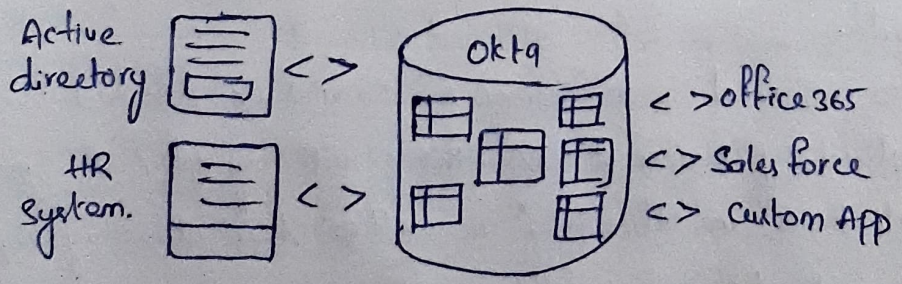
* Real-time sync
* One admin console
* Built-in high availability.
* Sophisticated multi-domain Support
* Service-level license assignment

* provisioning Types:-

→ okta provisioning has gone through several places and its important while you are scoping your implementation - that you understand what those places are and which provisioning type is right for your organisation.

* profile Sync
* user sync
* universal Sync
* licenses / Role management only.

Universal Directory - designed for integration :-



* Okta has own identity and service providers
* okta manages all the users

* office 365 provisioning

Requirements

Cloud-only exchange

* provision / deprovision users
* Sync rich profile
* Assign user roles
* Sync groups
* Transform attributes

Hybrid exchange

* sync exchange-specific data
* Contacts
* Distribution lists
* Calendar resources.
* more.

* profile Synchronisation :-

profile sync, also referred to as "version 0", synchronises only the basic profile in office 365, Consisting of "5 attributes." In order to create an okta-mastered user, you are required to provide 4 attributes. last name, first name, user name and primary email address. profile sync Synchronizes these 4 required attributes, plus the display name attribute when using profile sync, okta is leveraging the SOAP API's

* user Synchronization :-

user Synchronization, also referred to as "version 1" will synchronize a users full profile in office 365, consisting of over "20 attributes" and this is the option which is used for provisioning and cloud-mastered accounts you have when deploying user sync. okta leverages the graph API's and is also able to assign License and roles to users.

Universal Synchronization :-

universal sync, also referred to as "version 2". should be selected when you have Active directory mastered users. This provisioning option will synchronize over a "lot user" attributes" in office 365," as well as other directory objects; Such as Contact and distribution lists.

Imp

* How can you manages your DL (distribution lists)

A) It just comes the universal provisioning either we just want only of the user profile is going to be sync with okta with the help of DL. we can manages DL using universal provisioning which is created in the okta site either created in the AD site.

* Licenses / Roles management only :-

There is a fourth option as well that involves licenses (or) Role management only. This option will be used by those organisations that will be using the microsoft provisioning option. Azure Active Directory Connect (or) Azure AD connect. This will be the case for organisations which use an on-prime exchange server creating a "hybrid" (or) "write-back" scenario. It's important to note that microsoft provisioning to provision your directory-mastered users and then leverage okta's license/role management provisioning to assign office 365 licenses to users.

office365 implementation checklist :-

what do you need to do implement office 365?

microsoft has three requirements

* First you must register your companies public domain with your office365 tenant This is true for all implementations
* Next, you must check that your default domain is set correctly Again this is true for all implementations
* Finally, you need to prepare your directory. This is when you will decide if you will be using microsoft provisioning (or) okta provisioning and, if you're using okta provisioning, which okta provisioning option is best for you?
* lets examine the first two steps of our implementation checklist within our Office365 tenant.

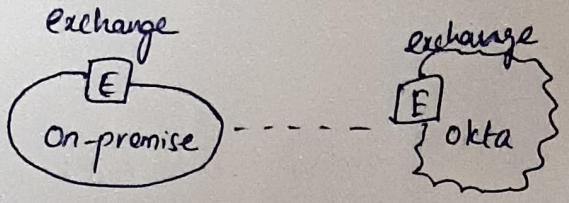
Verifying the registration of your public domain.

Imp okta provisioning universal sync

As part of our implementation checklist steps is to prepare your directory. when it comes to preparing your directory, here are some questions to ask

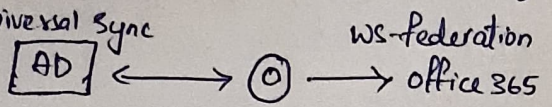
1) Does your Company have an on-prime exchange Server and one in the cloud? If so, does the exchange Server in the cloud need to write back to the server on-premise?

A) If the answer is "yes", then you will need to use microsoft provisioning.



* Exchange things mainly do mailing things like outlook mail.

* If the answer is "No", then you use okta provisioning, when talking about okta provisioning options. so the next question you need to ask yourself is: Do you have Active Directory mastered users that will need to be provisioned into office 365? If your answer is "yes" then you will be using universal sync.

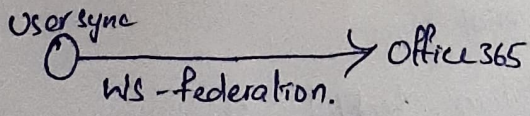


* You will need to Configure to office 365 app in your Okta org and select Universal Sync as the okta provisioning option.

* Next, you will transform data within okta to meet office365 requirements - such as username and email address - and verify that your company domain name is correct. finally, (sso) at which point all users will be required to authenticate through okta to access office 365.

Imp Okta provisioning user sync :-

* If you do not have Active directory mastered users that you would like to provision to office365 then you have Cloud base users which means you will be using the user sync provisioning option.



* The first step is to configure the office 365 application in okta and select the okta provisioning option of user sync.

This option will import the okta users full profile, consisting of " of attributes" depending on whether you have added any custom attributes, into office 365.

Transform the data Email address:-

* once you have saved your provisioning choices, you need to ensure that your username, and user email address match that of the public routable domain you registered within your microsoft office 365 tenant.
* If you need to change the format of the usernames and/or email address to meet the microsoft requirements, you can do so by transforming the data as it is passed from okta into office 365 via the profile mapping feature of universal directory within okta.

Transforming the data: Application username

Test the provisioning

* now that we have our okta provisioning set up and done our data transformation of the Application username format and email address, it is now time to test our provisioning.
* It is important to make sure provisioning is working and that user accounts have been created inside of officers before we federate.

Setting up ws-federation:-

you can configure ws-federation yourself using powershell (or) let okta configure ws-federation automatically.

Imp

* how you can set up office 365 through which method with the okta
A) ws-federation.

* There are four types of methods in the okta to integrate applications

1) SWA
2) SAML 2.0
3) Open ID
4) ws-federation

* Any microsoft application we can configure with the help of ws-federation

Best of practice :-

* A default cannot be federated.
* Create an In-cloud administrator account in office365 so that you can always have a side door into your tenant.
* Create an okta - mastered super administrator in okta to setup the microsoft office365 integration.
* Very that your okta provisioning is working before you federate. to ensure that you have your accounts setup properly inside office 365
* Never delete the office365 app in okta once federated.

* First you need to Create account in office 365

microsoft office 365 free trial
↓
Free trial - try microsoft for a month - microsoft store
↓
Try for 1 Month
↓
Sign in with credentials

* After Sign in to the office 365

My account
↓
Admin
↓
Show all
↓
Set up
↓
domain (you can see the domains)

How to Add users in office 365

My apps
↓
admin
↓
users
↓
Active users
↓
Add users

* To change user firstname, last name and password you can need to click on one of the user in office 365.

Ankit kumar (user)
↓
Reset password, Block Sign in, Delete user
↓
you can also edit the users in office 365

* Add office 365 in the okta.

* How to add office365 application in okta

Application
↓
Applications
↓
Add applications
↓
office 365
↓
Add
↓
Microsoft tenant Name (okktawin)
↓
If you want all application you can check all the boxes (or) if you want only few can uncheck the box.
↓
Automatically logon
↓
Next
↓
WS federation
↓
WS federation Configuration (Automatic)
↓
office365 Admin username (Chelkaran@okktawin.onmicrosoft.com)
↓
Password (Ckaran@123)
↓
office 365 Domain Fresh (okktawin.com)
↓
Select
↓
Application format (okta username)
↓
update application (create and update)

Allowed API Access ☑

↓

Authenticate

↓

Provide credentials in office365

↓

Next

↓

Password

↓

Sign in

↓

Accept

↓

Done.

* After creating office365 application in okta you need to assign the people the people to that application

Assignments

↓

Assign

↓

Add a person

↓

user

↓

Assign

↓

Save and Back

↓

Done

Before going to assign user go to provisioning

↓

Configure API

↓

Enable

↓

Test API

↓

Save after date provisioning

↓

edit

↓

Create user (enable)

↓

Update user attribute (enable)

↓

Deactive user (enable)

↓

Sync password (enable)

↓

Sign okta password (save)

* After assigning people goto my app

Click office 365

↓

It is redirected to the office 365

* If it is not works. Go to application

  * Application

↓

office 365

↓

import

↓

import new

↓

It will import the users from office 365 to okta

↓

Ok.

* How to deactivate the user from okta

work-flow
↓
Automation
↓
Add automation
↓
Automation Name (Oktawin)
↓
Save
↓
Add condition
↓
condition type (User in activity in okta)
↓
Duration (1 day)
↓
Save
↓
Add action
↓
Action type (Change user lifecycle state in okta)
↓
Change user state to (deactivated)
↓
Save

In the top right corner the state should be active (It shows inactive state) you need to click on active. So that user will be deactivated for 1 day in okta.

* OAuth 2.0 and OpenID Connect

OAUTH 2.0

The OAUTH 2.0 authorisation framework enables a third-party application to obtain limited access to an HTTP services either on behalf of a resource owner by orchestrating an approval interaction b/w the resource owner by and HTTP service, or by allowing the third party application to obtain access on its own behalf.

For example:-

An end user (resource owner) can grant a printing service (client) access to her protected photos stored at a photo-sharing service (resource server; without sharing her username and password with the printing service. Instead, she authenticates directly with a server trusted by the photo sharing service (authorisation server), which issues the printing service delegation-specific credentials access token)

Roles:-

OAUTH defines four roles

Resource owner

An entity capable of granting access to a ~~network~~ protected resource when the resource owner is a person, it is referred to as as end-user

Resource Server:-

The server hosting the protected resource, capable of accepting and responding to protected resource request using access tokens

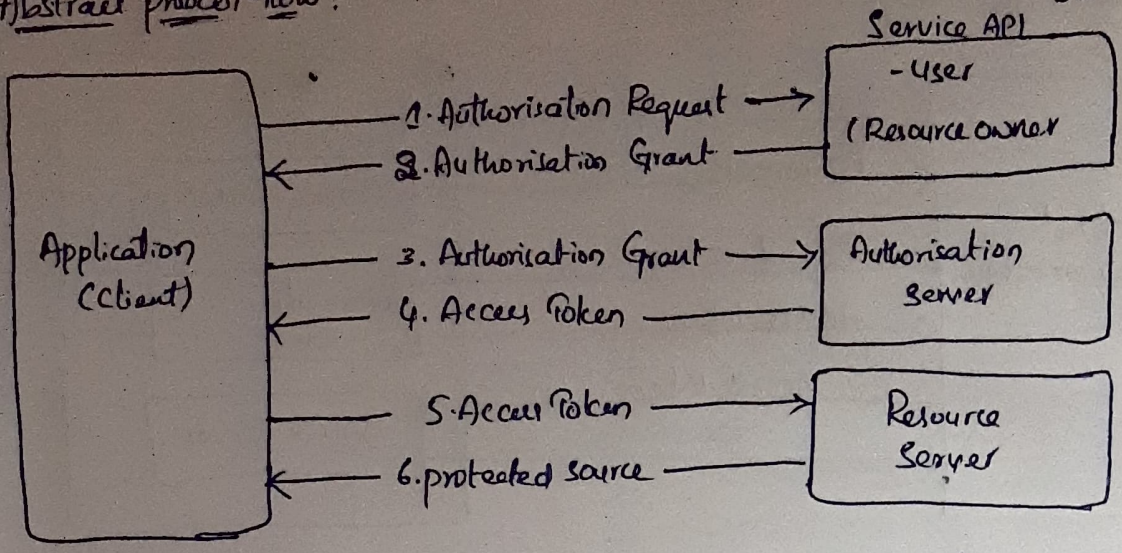
Client:-

An application making protected resource request on behalf of the resource owner and with its authorisation. The term "client" does not imply any particular implementation characteristics (eg, whether the application executes on a server, a desktop or other devices.

Authorisation Server:-

The server issuing access token to the client after successfully authenticating the resource owner and obtaining authorisation.

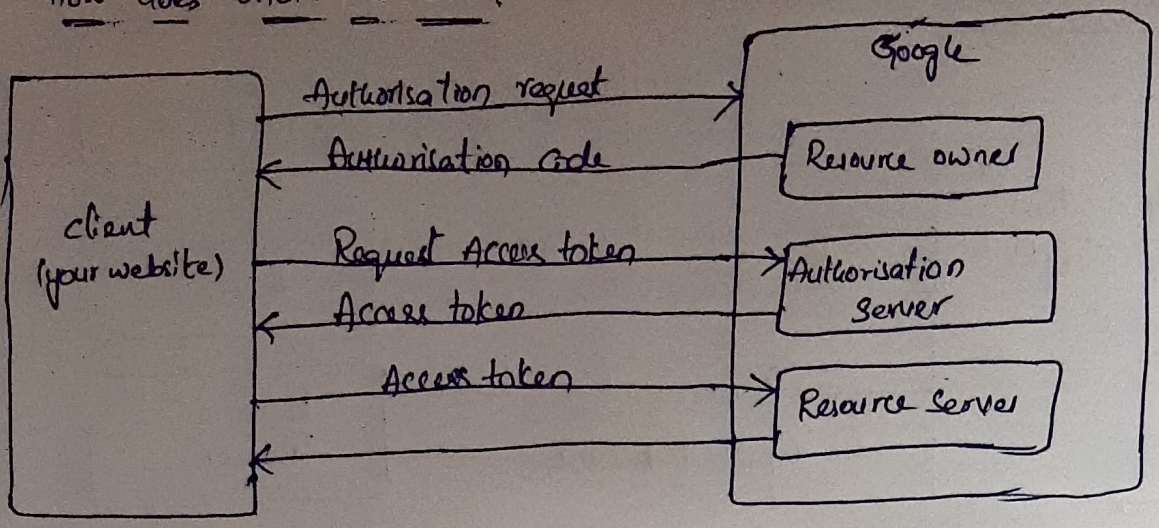
Abstract protocol flow:



Here is a more detailed explanation of the steps in the diagram

* The application request authorisation to access service resources from the user
* If the user authorised the request, the application receives an authorisation grant.
* The application request an access token from the authorisation Server(API) by presenting authentication of its own identity, and the authorisation grant
* If the application identity is authenticated and the authorisation grant is valid, the authorisation Server (API) issues an access token to the application. Authorisation is Complete.
* The application request the resource from the resource Server (API) and presents the access token for authentication.
* If the access token is valid, the resource Server (API) Servers the resource for application.

How does OAuth 2.0 work?



V. Imp

Authorisation Grant type :-

In the abstract protocol flow above, the first four steps cover obtaining an authorisation grant and access token. "The authorisation grant type depends on the method used by the application to request authorisation and the grant type supported by the API." OAuth 2.0 defines four grant types each of which is useful in different cases.

* Authorisation code :-

Used with server-side applications.

* Implicit :-

Used with mobile Apps (or) web applications (applications that run on the user's device)

* Resource owner password credentials :-

Used with trusted applications; such as those owned by the service itself.

* Client credentials :-

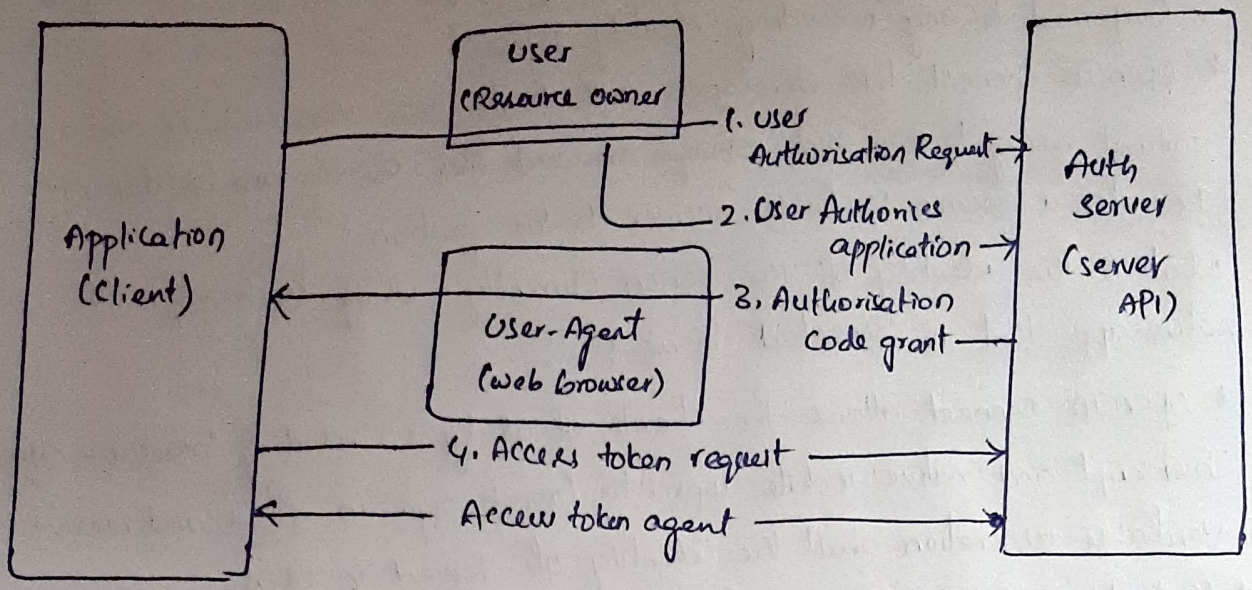
Used with applications' API access

Imp
What is the authorisation grant and how many types

* Tell me about how the Oauth is going to be work

A) Resources Server, Authorisation Server, Access token

Authorisation code flow :-



Access token :-

Access token are credentials used to access protected resources. An access token is a string representing an authorisation issued to the client. The string is usually opaque to the client. Tokens represent specific scopes and durations of access, granted by the resource owner, and enforced by the resources server and authorisation server.

Refresh Token :-

Refresh token are credentials used to obtain access tokens. Refresh tokens are issued to the client by the authorisation server and are used to obtain a new access token when the current access token becomes invalid (or) expires, or to obtain additional access tokens with identical (or) narrower scope (access tokens may have a shorter lifetime and fewer permissions than authorised by the resource owner). Issuing a refresh token is optional at the direction of the authorisation server issues a refresh token, it is included when issuing an access token.

* what is open id Connect ? How does it work?
* "OpenID Connect" is an interoperable authentication protocol based on the OAuth 2.0 family of specifications. It uses straight forward Rest/JSON message flows with a design goal of "making simple things simple and Complicated things possible". Its uniquely easy for developers to integrate, Compared to any preceding identity protocol
* OpenID Connect lets developers authenticate their users website and apps without having to own and, manage password files. For the app builder, it provides a secure verifiable, answer to the question what is the identity of the person Currently - using the browser to native app that is connected to me?"
* openID connect allows for clients of all types, including browser - based Javascript and native mobile apps, to launch sign-in flows and receive verifiable assertion about the identity of signed in users.
* (Identity, Authentication) + OAuth 2.0 = OpenID connect.
* How is openID Connect different from openID 2.0 and how does it overcome the problems experienced with OpenID 2.0?

A) * openID Connect has many architectural similarities to openID 2.0 and infact the protocols solve a very similar set of problems. However, OpenID 2.0 used XML and a Custom message signature scheme that in practice sometimes proved difficult for developers to get right, with the effect that openID 2.0 implementations would sometimes mysteriously refuse to interoperate OAuth 2.0, the substrate for openID connect, outsources the necessary encryption to the web's built in TLS (also called HTTPS or SSL) infra-structure, which is universally implemented on both client and server platforms. openID connect uses standard JSON web Token (JWT) data structures. When signatures are required. This makes openID Connect dramatically easier for developers to implement, and in practice has resulted in much better interoperability.

* The OpenID connect interoperability story has been proven it practice during an extended series of interoperability trials conducted by members of the OpenID connect working group and the developers behind numerous OpenID Connect implementations.

* How to create openID connect

Application (custom application)
↓
Applications
↓
Add applications
↓
Create new app
↓
OpenID Connect
↓
Create
↓
Application Name (my openID App)
↓
Login URL (https://localhost 8080)
↓
Save
↓
Assignments
↓
Assign
↓
Assign to people
↓
Choose a user
↓
Save and Back
↓
Done.

platforms

Web
Native app
Single page App
OAuth Service

Okta API Scope

what are the API's that are provided in Okta for this application.

Scope:-

what is the parameter and boundaries to use that thing.
Every identity, every application comes with the scope and limit to use that thing

How to Add authorisation Server

Security
↓
API
↓
Add authorisation server
↓
Name (my demo authorisation server)
↓
Audience (everyone)
↓
Description (demo with server used for demo practice)
↓
Save

* How to create New claim

claim
↓
Add claim
↓
Name
↓
Access Token
↓
Value Type
↓
few more options need to fill
↓
Create.

Automation:-

okta automations enable you to quickly prepare and respond to situations that occur during the lifecycle of 'end' users who are assigned to an okta group. This helps improve efficiency and satisfaction among employees, partners, and contingent workforce. for example Automation can help for inactivity lockouts if a user has been inactive for a set number of days and is on the verge of being locked out, you can use an automation to alert the inactive user in advance.

You set of an automation by defining the following items:

Conditions:-

The criteria that trigger okta to perform action upon a group of end users. For each automation, you can choose one condition to apply to one or more groups. Conditions can be scheduled to run once (or) to recur daily

There following conditions are currently available.

* user inactivity in okta
* user password expiration in okta.

These conditions are triggered according to a Schedule and can be applied to one (or) more groups conditions are mandatory for automations on recuring Schedules

Actions:-

The actions that you want okta to perform when the scheduled conditions are true. The following actions are currently available.

* Send email to the user
* Change user life cycle state in okta.

In line hooks:-

* In line hooks are outbound calls from okta to your own custom code, triggered at specific points in okta process flows. They allow you to integrate custom functionality into those flows.

* you implement your custom code as a web service with an internet accessible end point. It's your responsibility to arrange hosting of your code on a system eternal to okta. okta defines the rest API contract for the request it sends to your custom code as well as for the responses your custom code can send back.
* The outbound call from okta is called a hook. your code which receives the call, is referred to as your external service.
* In line hook user synchronous calls, which means that the okta process that triggered the hooks is paused until a response from your service is received

How to create an inline hook :-

Workflow
↓
Inline hook
↓
Add Inline hook (SAML, Token, password input)
↓
Choose any option
↓
fill details
↓
Save.

Event hooks:-

* Event hooks are outbound calls from okta that trigger process flows within your own software systems. They are sent when specific event occurs in your org and they deliver information about the event unlike inline hooks, event hooks are a synchronous and do not offer a way to execute the okta process flow. After sending the call, the okta process flow continues without waiting for a response from the called services.
* To set up an event hook you need to implement a web service with an internet accessible end point. It's your responsibility to arrange hosting of your code on a system external to okta. okta defines the rest API contract for the request it sends to your custom code, as well as for the responses your custom code can send back.

* How to create password policy:-

Security
↓
Authentication
↓
Add new password policy
↓
policy name (group password policy)
↓
policy description (It is used for the group password)
↓
Add group (Every group)
↓
Authentication providers
↓
Applies to (okta)
↓
password setting
↓
minimum length [8] Characters
↓
Create password policy.

After creating policy you need to add rule to that policy.

Add Rule
↓
Rule name (group rule)
↓
exclude user (Choose user)
↓
User's IP is (Anywhere)
↓
User can (change password)
↓
perform self service password reset
↓
Create rule.

* How to create Sign-on policy:

Security
↓
Authentication
↓
Sign-on
↓
Add new okta sign-on policy
↓
policy name (Sign on policy demo)
↓
policy description (It is a demo sign-on policy)
↓
Assign to groups (everyone) or choose your group name)
↓
Create policy and Add Rule.

After creating sign-on policy you need to add rule.

Add Rule
↓
Rule name (demo rule)
↓
exclude user (choose the user)
↓
users IP (Anywhere)
↓
Authentication (Any)
↓
Access is (allowed) and also session can be create.
↓
Create rule

(Radius - is integration purpose)

Networking :-

OSI (Open System Interconnection) :-

Inter connecting devices and how the information is shared has 7 layers

Application ↔ HTTP, FTP, Telnet etc.,
presentation → JPG, HTML, ZIP, MPS. so on.
Session ↔ Net Bios, PPTP (point to point Tunneling protcol)
Transport ↔ TCP, TCPS (3-lay hand shake, UDP)
Network ↔ Routing protocols (IPV4, IPV6)
data link ↔ MAC address
physical ↔ 0 and 1 bits, Copper, fiber, wireless etc.,

TCP, TCPS - If packets are missing, they will be re-transmitted
UPP - If packets are dropped, they are lost (does not re-transmit packets)
MAC address - If config, physical address in hexa-decimal
FCS (frame cheque sequence) - ensuring data is transmitted into corrupted.

TCP/IP

Application
Transport
Internet
Network Access.

Hybrid

Application
Transport
Network
data link
physical

Port for Admin

22 - SSH
23 - TELNET
69 - TFTP
80 - HTTP
443 HTTPS
636 - LDAPS
389 - LDAP

Range of IP's - 0 - 255

192:168:1-1-IP

* 8 cables per group
  electricity flowing - value '1'
  electricity not flowing - value '0'
  256th possibility the value of '0'

  $2^0+2^1+2^2+2^3+2^4+2^5+2^6+2^7 = 255 = 11111111$
  (line decimal)

00000000
↓ 2^8 = 256 possibility
11111111

Power of 2	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Binary								
Decimal	128	64	32	16	8	4	2	1

IPV4.

* Connection less protocol
* Packets are treated independently
* Packets may take different routes
* Load balancers

Address classes

A, B, C → Unicast Traffic - sending IP packets to single recipient

D → Multicast traffic - Sending IP packets to multiple host

E → Experimental purposes.

IPV6:-

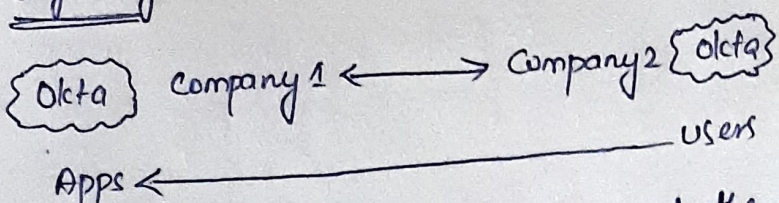
* Does not use classes

A - 1-126 H.H.H 2^4-2

B - 128-191 N.H.H $2^{16}-2$

C - 192-223 N.N.H $2^8-2=254$

Org 2 org



Both companies are using okta you need the users from the company you just bought to access the application from the parent company

Security
↓
identity providers
↓
Add identity providers
↓
Add SAML 2.0 IDP
↓
NAME (dev - and your code of dev code in okta)
↓
IDP username (IDP User Subject Name id)
↓
Match against (okta username)
↓
If no match is found (create the new user (JIT))
or
(Redirect to okta sign-on page)
↓
IDP issuer URL (IDP URL copy)
↓
IDP signature certificate (download)
↓
Add identity provider

To get URL you need to create application of org2org

Application

↓

Add application

↓

org2org

↓

Okta

↓

Base UI (URL copy from window) (remove admin part)

↓

Done

↓

Sign-on

↓

SAML 2.0 (URL)

↓

Aub Acs URL (Copy from IDP provider org2org)

↓

Audience URL (Copy from IDP)

↓

Save

Group :

* Group rules cannot be used to assign users to admin groups.
  (yes, you can assign admin role to user (or) a group)
* you can have upto max of 2k rules per org.
* you can only assign string type of attributes in group rule's conditions.
* A group already the target of a group rule cannot be granted admin privileges
* only Super admins and org admins can edits rules.
* only group admins managing all groups can search and view rules.
  Individual group admins cannot do this

IWA (or) DSSO (Desktop Single Sign-on)

Settings
↓
Downloads
↓
SSO IWA web App
↓
Download
↓
Need to configure steps

* Delegated authentication is enable for IWA

* enable (or) disable an app (or) org unassignment import safeguard :-

Application
↓
Click on application
↓
provisioning Tab
↓
Setting link
↓
Import safeguard
↓
Click edit
↓
App unassignment safeguard
↓
Disable (or) enable
↓
org. wide unassignment safeguard
↓
Disable (or) enable
↓
Save

* when JIT is enable, user do not receive activation emails

Add and update user with JIT provisioning :-

Directory
↓
Directory Integration
↓
Select an AD instance
↓
provisioning (okta in the setting list)
↓
edit
↓
general section
↓
Create and update user on login (JIT provisioning)
↓
save.

View the import monitoring dashboard

Report
↓
import monitoring
↓
Show All
↓
Status, completed, in progress (or) failed imports.

(okta sign in widget version 2.9)

Increase (or) decrease the app (or) org unassignment import safeguard

Application
↓
Applications
↓
office365 (Select the particular app)
↓
provisioning
↓
Setting (to okta)
↓
import safeguard (edit)
↓
App unassignment safeguard (increase or decrease)
↓
org-wide assignment safeguard (increase or decrease)
↓
Save

* unblock an individual user account :-

Directory
↓
people
↓
left menu select locked out
↓
click person and username
↓
more actions
↓
unlock Account.

* configure voice call for self-service password resets

Security
↓
Authentication
↓
Edit
↓
Account recovery
↓
voice call
↓
update policy

enable Active directory delegated authentication :-

Directory
↓
Directory integration
↓
Active directory (select directory)
↓
Integration (setting list)
↓
enable delegated authentication to Active directory
↓
save

* Expire all user password :-
* The password for users managed through Active directory and LDAP delegated authentication are not expired.
* Active directory and LDAP agent will configure to work even if the service account managed by okta has an expired password.

Directory
↓
people
↓ more actions
expire passwords
↓
expire passwords
↓
Confirm expiration of All okta mastered passwords

Revoke a users Certificate from the okta certificate Authority :-

Managed windows Computer :-

Directory
↓
People
↓
person & a username
↓
more actions
↓
Revoke Trust certificate
↓
To rename the device trust Certificate

User account states :-

Staged
Pending user action
Active
password reset
locked out
Suspended
Deactivated

* LDAP (light weight Diretory Access protocol)
* version 5.7.2
* Ridus agent, version 2.15.1
* Okta Sign.in widget, version 5.4.0
* universal security groups do not support cross-forest memberships
* It supports if there is a two way trust establish b/w the groups
* Okta does not support domain local groups containing members from multiple domains

Enable group import from provisioning-enabled apps :-

Application
↓
Applications
↓
choose applications (particularly)
↓
Settings
↓
integration
↓
edit
↓
import group (enable)
↓
Save

Review group imports :-

Directory
↓
groups

Remove groups imported from provisioning-enabled apps :-

Applications
↓
Applications
↓
Choose applicant (particular one)
↓
provisioning
↓
Settings
↓

integration edit
↓
import group
↓
continue (disable import group)
↓
Save.

Assign multiple apps to group :-

Directory
↓
Group
↓
Select particular group
↓
Manage apps
↓
Assign application (multiple)
↓
Save and go back
↓
Assign
↓
Done

prioritize application groups:-

Application
↓
Applications
↓
Search (choose particular app)
↓
Setting (or) filter
↓
group
↓
Drag group to a new location to change its priority

Assign attribute group priority :-

Directory
↓
profile editor
↓
Okta, Apps, Directories
↓
profile (for app)
↓
Add attribute
↓
Select one option
↓
Click save for a new attribute
↓
Save attribute.

* Group rules :-

Group rules are applied to your entire org and they can be triggered whenever you change a users profile, group membership (or) lifecycle state

Enable Group push :-

Application
↓
Applications
↓
Choose particular application
↓
push group
↓
Find by group name (or) Find groups by rule.
↓
To deactivate group push, unlink pushed groups, or push group memberships immediately
↓
click Active/inactive for a group select on. of these options
↓
Option click information

* you cannot push group with a name that already exists within the target app.
* when a group already exists in an application pushing by rule fails because the creation of a duplicate groups is not supported
* okta has 31 default base attributes for all users in an org.
* only app integration wizard and templates ws-federation can send UD (universal directory) data.

View the okta default user profile :-

Directory
↓
profile editor
↓
okta
↓
profile in the action column

Make the user profile -first and last name optional :-

Directory
↓
profile editor
↓
okta (filters)
↓
Profile (Action column)
↓
Base (filters)
↓
First name (click on (i) symbol that means information)
↓
Clear attribute required check box
↓
Save attribute
↓
last name
↓
Click information
↓
Save attribute.

Create a custom character restriction for the okta username :-

Directory
↓
profile editor
↓
okta
↓
profile (Action Column)
↓
username Click information
↓
Format restriction (select option) email support
↓ ↓
Save attribute custom character restriction
↓
None

* Remove custom attributes from a user profile:

Directory
↓
profile editor
↓
okta (filter list)
↓
profile (action column)
↓
Attributes, custom in the filter list
↓
Click x
↓
Delete attribute
↓
Repeat 5 and 6 steps to remove multiple custom attributes.

* Hide Sensitive attributes:

Directory
↓
profile editors
↓
okta (filter list)
↓
profile for okta user (default)
↓
attribute list (click information)
↓
click on (user permission - hide)
↓
save attribute

View existing application attribute mapping:-

Application
↓
Applications
↓
provisioning
↓
Attribute mappings
↓
Show unmapped attributes

Create custom user type :-

Directory
↓
profile editor
↓
Create okta user type
↓
display name
↓
Variable name
↓
Save

Delete a user type :-

Directory
↓
profile editor
↓
Click profile (you want to delete)
↓
Click delete
↓
Delete Confirm

Priortize profile source :-

Directory
↓
profile source
↓
priority

Active directory integration pre-requesition :-

* Que Server should have atleast 2 CPU's and a minimum of 8 GB RAM
* Okta recommeds installing windows Server 2012 R_2, windows Server 2016, or windows Server 2019
* System must have 80MB
* .NET 4.52

* Make active directory the profile source :-

Directory
↓
Directory integration
↓
Active directory
↓
Provisioning
↓
To okta
↓
profile & Lifecycle Source and click edit
↓
Allow active directory to source data
↓
When a user is deactivated in the app (Nothing, Deactivate, Suspend)
↓
Choose the options
↓
Save.

Schedule Active directory user imports :-

Directory
↓
Directory integrations
↓
Active directory
↓
Settings (To okta)
↓
general
↓
edit
↓
Schedule import (options)
↓
Save.

Add and update users with JIT provisioning :

Directory
↓
Directory integration
↓
Active directory
↓
Settings (okta)
↓
General (edit)
↓
Create and update users on logon (JIT provisioning)
↓
Save.

Make first and last name optional in Active directory :

Directory
↓
profile editor
↓
Directories (filter list)
↓
Active directory (profile), Action Columns
↓
Click information (first name)
↓
Attribute required
↓
Save attribute

Import groups from Active directory

Directory
↓
Directory integrations
↓
Active Directory, provisioning
↓
integration (setting list)
↓
Group OU's Connected to okta
↓
Save.

enable universal security group support :-

Directory
↓
Directory integration
↓
Active directory
↓
provisioning
↓
Settings (okta)
↓
General
↓
Universal Security group support
↓
Save

* Enable federation Broker mode :-

Application
↓
Applications
↓
Choose application
↓
Sign-on
↓
Enable federation broker mode
↓
Enable federation broker mode

Network :-

* Network zones are defined and maintained by admins.
* Network zones consist of IP zones and Dynamic zones
* IP zones and Dynamic zones have the following limitations.
  * upto 100 zones configured per org.
  * upto 150 Gateway IP's and 150 proxy IP's
* IP blocked zones may contain upto 1000 gateways per zone and upto a total 25000 per org.
* IP zones both gateway IP's and proxy IP's added by admin.
* Dynamic zones enable admins to define network promoters around location, IP type and Autonomous System number.

Block list a Network zone :-

Security
↓
Networks
↓
edit
↓
Block access from IP's matching conditions listed in this zones
↓
Save

Generate a proxy IP report :-

Reports
↓
Reports
↓
Proxies
↓
Proxy IP usage (Generate Report)
↓
Generate report.

Configure Risk Scoring in okta on policies :-

Security
↓
Authentication
↓
Sign on
↓
Add rule
↓
Risk level (under the condition name)
↓
Any
↓
Save.

* Get the report by email:-

Reports
↓
okta usage, okta password health, current Assignments (or) MFA usage.
↓
Run report

* The download link for the report is only valid for seven days. you have to request the report again after the link expires
* The system logs displays all events for the last seven days with default filters
* Profile source:-
* Profile source is an application that acts as a source of truth for user profile attribute. A user can only be sourced by a single application (or) directory at a time

What effect does priority have on a profile source?

A) The priority determines which applications (or) directory is considered the profile source applications (or) directories

What are org-managed apps?

A) user can request apps that your org has added and enable for self service

What are personal apps?

A) They can also add any apps from the okta app catalog that your org has not added and that only require a username and password for account creation.

How is device trust used?

A) Device trust is a condition that can be applied in Application sign-on policy to ensure that only trusted devices are access to an application.