

“DATA SECURITY IN SALESFORCE”

*Project Report submitted in partial fulfillment of the requirements for
the Degree of*

BACHELOR OF TECHNOLOGY

IN

COMPUTER SCIENCE AND ENGINEERING

By

ANSHUL SHARMA

Enrollment No: **161303**

UNDER THE GUIDANCE

OF

Dr. Pardeep Kumar

Associate Professor - Dept. of CSE and IT



Department of Computer Science and Engineering
JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY,
WAKNAGHAT

PROJECT REPORT UNERTAKING

I Mr. **Anshul Sharma** - Roll No - **161303** Branch **CSE** is doing my internship with **COGNIZANT** from **7 Feb 2020** to **7 June 2020**

As per procedure I have to submit my project report to the university related to my work that I have done during this internship.

I have compiled my project report. But due to COVID-19 situation my project mentor in the company is not able to sign my project report.

So I hereby declare that the project report is fully designed/developed by me and no part of the work is borrowed or purchased from any agency. And I'll produce a certificate/document of my internship completion with the company to TnP Cell whenever COVID-19 situation gets normal.



Name : Anshul Sharma

Date : 20-June-2020

DECLARATION

I hereby declare that the work reported in this report “**SECURING SALESFORCE DATA**” in partial fulfillment of the requirements for the award of the degree of Bachelor of Technology in Computer Science and Engineering submitted in the department of Computer Science and Engineering, Jaypee University of Information Technology, Waknaghat, is an authentic record of my own work carried out over a period from Feb 2020 to May 2020 under the supervision of **Dr. Pardeep Kumar (Associate Professor - Dept. of CSE and IT)** and **Mr. Shibu Kalidhasan (Salesforce trainer at Cognizant Technology Solutions Ltd.)**

The matter embodied in the report has not been submitted for the award of any other degree or diploma.



Anshul Sharma

(161303)



This is to certify that the above statement made by the candidate is true to the best of my knowledge.

ACKNOWLEDGEMENT

I would like to express my special thanks of gratitude to my guide **Dr. Pardeep Kumar** (**Associate Professor - Dept. of CSE and IT**) and mentor **Mr. Shibu Kalidhasan** (**Salesforce trainer at Cognizant Technology Solutions Ltd.**) who gave me the precious opportunity to do this project on the topic '**Securing Salesforce Data**', which also helped me in doing a lot of research and I came to know about so many new things.

I am really thankful to him.

Anshul Sharma

(161303)

TABLE OF CONTENTS

CAPTION	PAGE NO.
DECLARATION	i
ACKNOWLEDGEMENT	ii
LIST OF FIGURES	iii-iv
ABSTRACT	v-vi
CHAPTER 1 – INTRODUCTION	1
1.1 Security basics	1
1.1.1 Providing security guidelines	2
1.1.2 Choosing right security settings	3
1.1.3 Using security configurations	5
CHAPTER 2 - DATA SECURITY	7
2.1 Data Security: An Overview	7
2.1.1 Levels of data access	7
2.1.2 Usage of Audit Trails	10
2.2 Data Security : Controlling Access in a Org	11
2.2.1 Creating a User	11
2.2.2 Deactivating a User	12
2.2.3 Setting password Policies	12

2.2.4 Controlling Using IP addresses and Time	13
2.2.5 Controlling Access to the Records	15
2.2.6 Creating a Role Hierarchy	20
2.2.7 Define Sharing Rules	24

CHAPTER 3 - SESSION-BASED PERMISSION SETS AND SECURITY

3.1 Session-Based Permission Sets: An Overview	25
3.1.1 Creating a Session-Based Permission Set	25
3.1.2 Activating Session-Based Permission Sets	27
3.1.3 Creating Easy access for Activation flow	29

CHAPTER 4 – IDENTITY

4.1 Salesforce Identity	31
4.2 Knowing your identity users	35
4.3 Learning the Identity's Language	37

CHAPTER 5 - USER AUTHENTICATION

Pardab Kumar

5.1 Securing User's Identity	43
5.1.1 Setting Up Two Factor Authentication	44
5.2 Setting up SSO	46

CONCLUSION

50

REFERENCES

51

LIST OF FIGURES

Fig 1.1 Security Settings	4
Fig-2.1 :Controlling Data Access(Salesforce Platform)	9
Fig 2.2.1 : Creating a user	11
Fig 2.2.3 : Password Policies	13
Fig 2.2.4 : IP ranges	14
Fig:2.2.5 a : Record level Access	16
Fig 2.2.5 b : Org-Wide Sharing	17
Fig 2.2.5 b : Org-Wide Defaults	19
Fig 2.2.6a : Creating role hierarchy	21
Fig 2.2.6b : Adding a Role	22
Fig 2.2.7 : Adding a Public Group	23
Fig:3.1 Permission Set	26
Fig 3.1.2 : Session Based Permission Sets	28
Fig 3.1.3 : Activation Flow	30
Fig 4.1a : Multiple apps	31
Fig 4.1a : Social Sign On	33
Fig 4.1b : two factor authentication	34
Fig 4.2 : Comparing Features	36
Fig 4.3a : SAML	38
Fig 4.3b OAuth 2.0.	39

Fig 4.3c: Open ID Connect	40
Fig 4.3d: SAML flow	42
Fig 5.1 : Two Factor Authentication	43
Fig 5.1.1 : Creating two factor authentication	45
Fig 5.2a : Creating ID	46
Fig 5.2b : Setting up SSO	47
Fig 5.2c : linking Salesforce and Identity	48
Fig 5.2d: XML response	49

ABSTRACT

Salesforce is comprised with the security measures for protecting your data and applications. You can also introduce your own security schemes that matches your organization's structure and needs. You and Salesforce have a shared duty to protect your data. The Salesforce security features allows you to empower your clients to do their jobs efficiently.

- **Salesforce Security Basics**

The security features of Salesforce helps you empower your users to do their jobs in a safe and effective manner. Salesforce limits data exposure to users acting upon it. Implement security checks which you think are sufficient for your data sensitivity. We will work together to protect your data against unauthorized access by your users from outside of your company and from inappropriate use.

- **Authenticate Users**

Authentication means preventing inappropriate access to the company or its data by making sure that any person who is logged in is whoever they say they are .

- **Give Users Access to Data**

One of the key decisions affecting data security is choosing the data set that each user or group of users could see. You need to find the right balance between restricting data access, thereby minimizing the risk of stolen or misused data versus the ease of accessing data for your users.

- **Monitoring Your Organization's Security**

Track the login and domain history, monitor changes to the setup, and take event-based actions.

- **Real-Time Event Monitoring**

Real-Time Event Tracking lets you track and identify typical Salesforce incidents in near to real time. The event data may be stored for audit or reporting purposes. Using Condition Builder – a point-and - click tool – or Apex code, you can create transaction security policies.

CHAPTER 1

INTRODUCTION

1.1 Security basics

Global cybercrime is on the mind of every human being , considering that in our personal lives and at work, we use technology the whole day . In 2015, The “Verizon’s Data Breach Investigation “ has a report estimating the annual cost of global cybercrime at a whopping \$100 billion.

The attacking landscape is more complex than ever, and the prevention , detection, analysis, and response to threats has never been tougher or more crucial for security teams.

By manipulating simple human behaviors, attackers have changed their methods from technical threats to direct assaults on employees. People in your company are now your biggest threat to security, because they present the easiest advantages for hackers. Every person has an effect on security more than ever .

Basic methods used by attackers :

- **Phishing and Malware**

An attempt to obtain confidential information (such as usernames, passwords and debit or credit card details) by disguising as a trusted entity . This technique is used to trick users to install and access malware aimed at damaging or manipulating a device , computer or network.

- **Social Engineering**

Social engineering is the art of tricking or manipulating people into participating or sharing sensitive information.

- **Exploiting Public Info**

Using information that is publicly accessible to help plan a social manipulation attack, hack a password login or construct a targeted phishing email.

- **Badge Surfing**

Getting into a protected area, either by following a legal badge holders in or by convincing the individual to let them in.

- **Eavesdropping**

Listening secretly in on personal discussions or private conversations .

- **Dumpster Diving**

Collecting recyclable materials or trash information which was not properly destroyed.

- **Installing Rogue Devices**

Network devices or USB thumb drives are installed where they can give a hacking group access to a secure system.

1.1.1 Providing security guidelines

Passwords are your defense's first line. A password is sometimes the only thing separating you and the tragedy.

Setting specifications for password length, history, and complexity along with many other values, and determine what to do if users ever forgets their password.

These simple success factors helps reducing in password threats, whether or not you are using additional technologies for extra protection, such as two-factor authentication and single sign-on.

- Change passwords often
- Have unique passwords
- Better having longer passwords
- Make passwords difficult to crack
- You would never share a password, right?

A key safety practice is giving users the minimum amount of access they need to do their task. This is called the 'least privilege principle' .

1.1.2 Choosing right security settings

You are automatically in your company's security group as a Salesforce administrator. Security is the basis of all of Salesforce 's service. In addition to protecting your data and software, you can also create your own security scheme customized to your organization's needs.

Many layers of protection at Salesforce work together to keep the company secure. Your data is secure from unauthorized usage from outside your business and your own users always want to protect it from improper use. You can unlock features built into the platform to make the understanding as safe for your business as possible. There is no strategy or feature for security that is bullet proof. But shoring the introduction of these capabilities will decrease the org 's probability of being compromised, and may help minimize data loss even if it is.

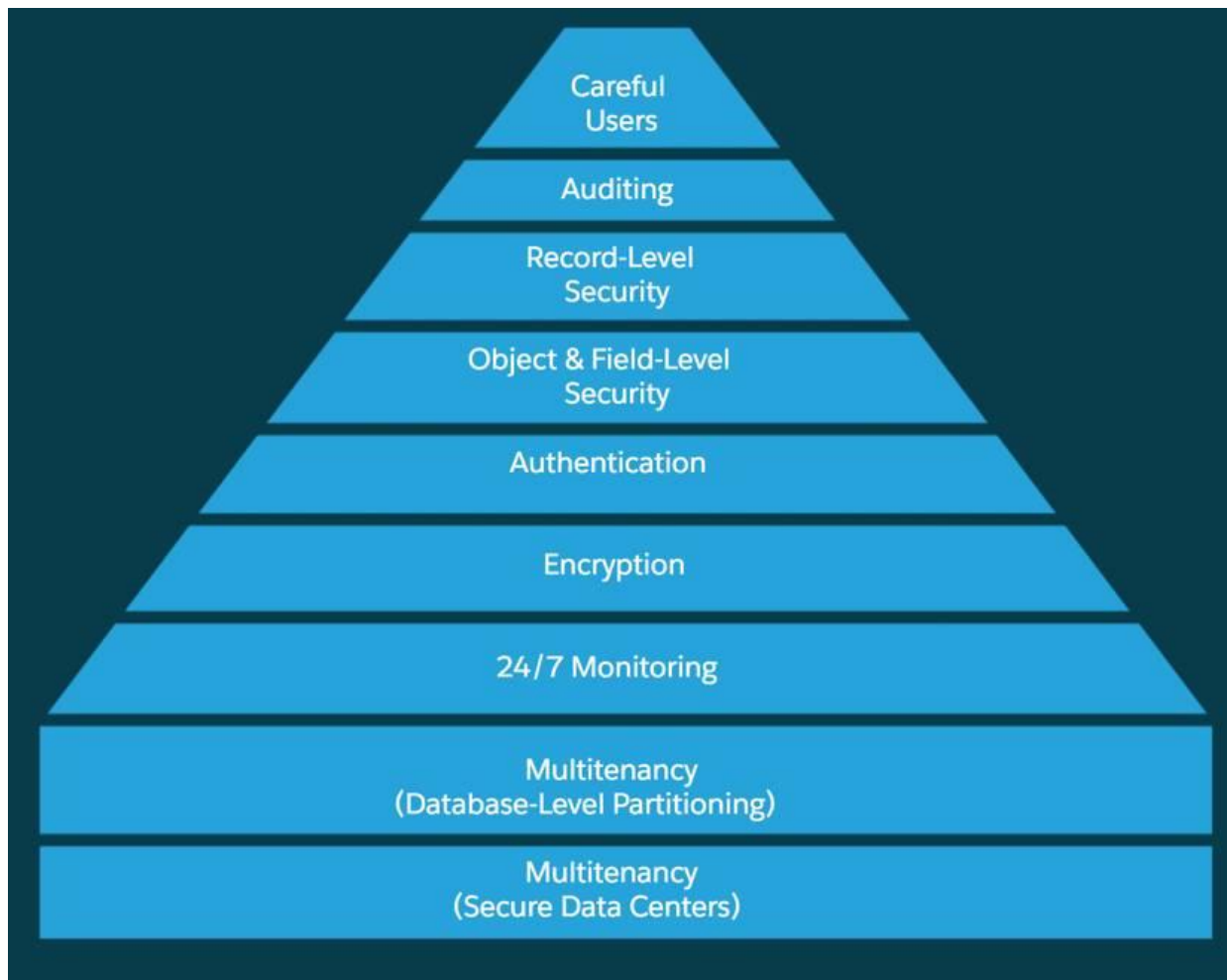


Fig. 1.1 – Security settings

- **Multitenancy**

Salesforce is a multi-tenant platform: to meet the needs of several different clients, it uses a large pool of computing resources. Salesforce protects data from all other customer orgs from your org by using a unique identifier associated with the session of each user. Using this identifier, your subsequent requests are linked to your org when you log in to your org.

- **Letting the Right Users In**

One effective way to increase the security of your Salesforce org is to allow a second authentication level when the users log in. Users can either respond to a Salesforce Authenticator Mobile App notification, or enter a code they get from their mobile device or a hardware token. In this way, even if the credentials of a user are breached, it is still possible to protect the user account.

- **Limiting What Users Can Do**

Several access and control layers determine "who sees what" in a Salesforce org, and "who can do what." If you have several Salesforce orgs, set up the controls in each and every org separately.

- **Encrypting Your Data**

Platform Encryption provides a whole new layer of protection to your information while maintaining critical application features. At rest, the selected data is encrypted by using an "advanced key derivation system". You can secure data to a more detailed level than ever before, and the business can adhere to privacy policies , legal standards and contractual commitments to treat private data with confidence.

Pardab Kumar

1.1.3 USING SECURITY CONFIGURATIONS

- **DASHBOARD as a security check**

You call it the Health check. Using Health Check to increase overall protection of your company and the ability to keep the harmful entities out. Through Health Check, you can

find and address flaws in the security settings, everything from one page. A review score indicates how well your company aligns with the suggested Salesforce norm.

If you change the settings being less restrictive, your score will typically go down. For example, suppose you reduced the minimum length of your password from eight characters (the standard value) to five, and changed other settings on Password Policies towards less strict. These updates make passwords increasingly vulnerable to guesses and other brute force attacks from your users.

- **Identifying and fixing security risks in the Org**

How do you start to fix the security risks for your org? Initially, go to your very own org Health Check

Type *Health Check* into the Quick Find box from Setup and then click on Health Check.

Every other setting mentioned as a risk has a convenient Edit link which will take you to a page where you can modify the setting to the default. In Health Check standard values are listed.

Reviewing security across multiple orgs:

You can access security settings, threats, health check ratings, and baseline settings for Salesforce by using Tooling API. For verifying that multiple Salesforce applications have the similar level of security, you may add this data to your dashboards and security monitoring system. SecurityHealthCheckRisks and SecurityHealthCheck are the tooling API objects that you use.

```
1 SELECT Score,  
2 (SELECT RiskType, Setting, SettingGroup, OrgValue, StandardValue FROM SecurityHealthCheckRisks WHERE RiskType='HIGH_RISK')  
3 FROM SecurityHealthCheck
```

Above is an SOQL query's example that gets a score of org's Health Check and high-risk settings list.

CHAPTER 2

DATA SECURITY

2.1 Data Security: An Overview

Selecting the set of data that can be seen by every user or group of users is one of the major decisions affecting the safety of your Salesforce app or org. Once your data model has been designed and implemented, give some consideration to what data they need to do and what sorts of things your users are doing. With the flexible and layered sharing model of the Salesforce platform, it's easy for assigning different sets of data to different user sets. You can maintain comfort and security, lower the risk of data being stolen or misused, and still ensure that all users can easily have the data they require. The framework makes it easy to determine which users are able to access, build, edit or remove any record or field within the application. You can handle access to your entire org, to a particular object, to a particular field or even to a single record.

2.1.1 Levels of data access

You can monitor which users have access to which information in your entire org, a specific entity, a particular area, or a single record.

- **Organization**

You can track and maintain a list of authenticated users for your entire org, establish password policies and restrict logins to certain locations and times.

- **Objects**

The easiest thing to monitor is accessing the data at object-level. By establishing multiple permissions on a specific type of object, you can prevent any record of the object from

being created, viewed, edited or deleted by a group of users. For instance, you can use object permissions for ensuring that the interviewers are able to view job applications and positions but not delete or modify them.

- **Fields**

Even when a user has an access to an object, you can limit access to some sensitive fields. For example, in a position object, you can set the income field not visible to interviewers and on the other hand visible to recruiters and hiring managers.

- **Records**

You can allow specific users to access an object, but then constrain the individual records of objects they are allowed to view. An interviewer, for an instance, can see and edit their own reviews but not other interviewer's reviews. There are four ways in which you can manage record level access.

1. **Org-Wide defaults** states the default level that users have access to the other's records. You use the org-wide sharing settings to lock your data into the most restrictive stage, and then use the other security and sharing tools at the record level to selectively give other users accesses.
2. **Role Hierarchies** gives users the hierarchy access in higher stage to all records in the hierarchy owned by users underneath them. The role hierarchies need not have to fit exactly the chart of your organization. Rather, each role in the hierarchy must reflect the level of access to data that a user or user groups needs.
3. **Sharing rules** are the automatic exceptions for specific groups of users to org-wide defaults, so they can access the records that they don't own or normally can't view. Sharing rules, such as the role hierarchies, are used to provide access to records for additional users. They can't be tighter than your default settings across your organization

4. **Manual Sharing** enables proprietors of specific records to share with the other users. While manual sharing is not automated such as role hierarchies , org-wide sharing settings, or sharing rules. it may be useful in some situations, such as when a recruiter on holiday needs to momentarily assign someone else the ownership of a job application.

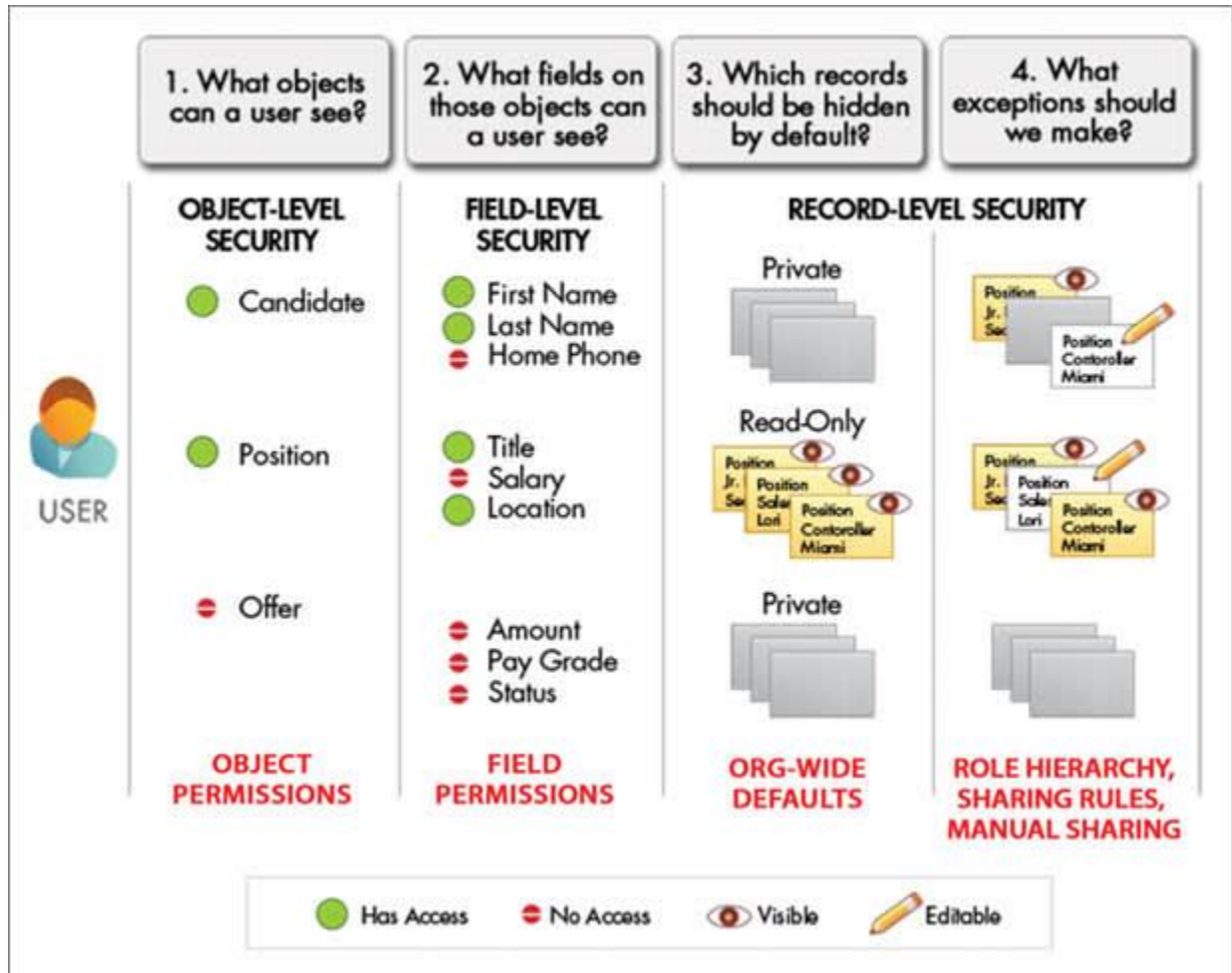


Fig-2.1 :Controlling Data Access(Salesforce Platform)

2.1.2 Usage of Audit Trails

Auditing provides valuable information to be able to diagnose potential security problems or deal with real ones. Someone within your organization should be regularly audit to detect potential misuse. Look for any unexpected shifts or usage patterns.

- **Record Modification Fields**

All objects contain fields that store the detail of the user who generated the record as well as last modified it. This provides some basic information regarding auditing.

- **Login History**

For the past six months, you can review the list of failed and successful login attempts.

- **Field History Tracking**

You can toggle on the auditing to monitor changes in the data of individual fields automatically. But since field-level auditing is accessible for all custom objects, it is only allowed by some standard objects.

- **Setup Audit Trail**

When changes to your org's configuration are made, the Setup Audit Trail is logged.

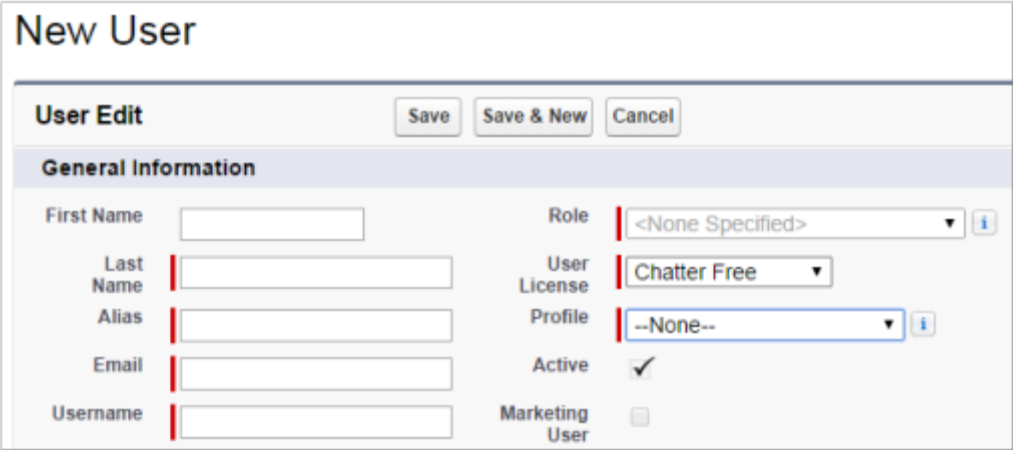
2.2 Data Security : Controlling Access in a Org

2.2.1 Creating a User

You could even create users from just a few clicks , even the multiple users. It's as easy as when you enter a alias , username and e-mail, and choosing a role, profile and license . Of course, there are many more options available but that will be all you need to get everything started.

A password is generated automatically in Salesforce, and immediately notifies the new users. After logging in users can modify or insert personal information to their own.

- Find **Users** | **Users** in **Quick Find** box present in **Setup**
- Click the option **new user** or click **multiple users**
- Enter all details and click **save** .



The screenshot shows the 'New User' form in Salesforce. The form is titled 'New User' and has a 'User Edit' header with 'Save', 'Save & New', and 'Cancel' buttons. The 'General Information' section contains the following fields:

Field	Value
First Name	
Last Name	
Alias	
Email	
Username	
Role	<None Specified>
User License	Chatter Free
Profile	--None--
Active	<input checked="" type="checkbox"/>
Marketing User	<input type="checkbox"/>

Fig 2.2.1 : Creating a user

2.2.2 Deactivating a User

You can not delete an active user, but you can only deactivate an active account so that the user is not able to sign in. The users that are deactivated loses access to all the records. (That includes individually shared records and the records that are shared with them as teams.) However, you still can transfer these data to the other users and display the names on the Users page.

- Use Quick find box to go to users present in Setup
- Click the Edit present in front of the user name
- Before clicking the save button , uncheck the active option
- For freezing , click the Freeze option

2.2.3 Setting password Policies

You can customize multiple settings to make sure that passwords are secure for your users.

1. Setting the password and login guidelines, such as defining a time limit before passwords expires for the accounts, and the complexity level needed for passwords.
2. Expire passwords with all the users in the org, except for the users that has permission for use "Password Never Expire."
3. Password reset for authorized users.
4. If by any chance a user is locked out because of too many login failed attempts, the access to the account can be unlocked by you to that user.

STEPS :

- Click **Password Policies** in Setup by searching it on **quick find** box
- Customize your settings

- Click **Save**

Password Policies

[Help for this Page](#)

Set the password restrictions and login lockout policies for all users.

Password Policies = Required Information

User passwords expire in **90 days**

Enforce password history **3 passwords remembered**

Minimum password length **8 characters**

Password complexity requirement **Must mix alpha and numeric characters**

Password question requirement **Cannot contain password**

Maximum invalid login attempts **10**

Lockout effective period **15 minutes**

Obscure secret answer for password resets

Require a minimum 1 day password lifetime

Forgot Password / Locked Account Assistance

Message

Help link

Forgot password preview If you still can't log in, try the following: Contact your company's administrator for assistance.

Locked account preview To re-enable your account, try the following: Contact your company's administrator for assistance.

API Only User Settings

Alternative Home Page

Fig 2.2.3 : Password Policies

2.2.4 Controlling Using IP addresses and Time

- **IP ranges**

The IP address is always cached in to your webbrowser the first time you log on to Salesforce. Whenever you log in from another IP address, you'll be asked to check your identity, generally by entering the verification code. This step can be bypassed for trusted IP ranges. For example , assume that your users are able to log in to accounts whenever they are in office, without entering the verification code.

- Click on **network access** in the setup using **quick find**
- Click **new**

- Enter ranges of the IP addresses
- Click **Save**
- **IP address**

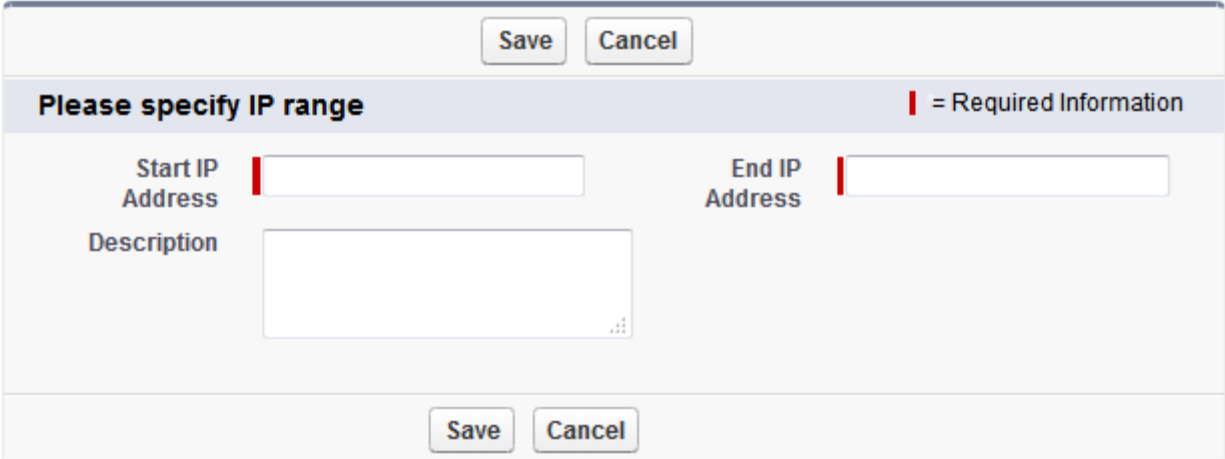
Salesforce does not by default constrain login access locations. If you're not doing anything, users can log into the org from any IP address. You can limit where users are able to log in. Suppose , for example, that some users should not be able to log in when they use the IP address outside of the office.

 - Click on **Profiles** in the setup using **quick find**
 - Click a name after selecting a profile.
 - Click **Login IP Ranges**
 - Click **new**
 - Enter ranges for starting and ending of the IP addresses
 - Click **Save**

Login IP Ranges

[Help for this Page](#) 

Enter the range of valid IP addresses from which users with this profile can log in.



The screenshot shows a configuration window for 'Login IP Ranges'. At the top, there are 'Save' and 'Cancel' buttons. Below that is a header section with the text 'Please specify IP range' and a legend ' = Required Information'. The main area contains three input fields: 'Start IP Address', 'End IP Address', and 'Description'. The 'Start IP Address' and 'End IP Address' fields have red vertical bars next to them, indicating they are required. The 'Description' field is a larger text area. At the bottom of the form are 'Save' and 'Cancel' buttons.

Fig 2.2.4 : IP ranges

- **Time**

You can describe the hours with each profile whenever the users could log in. For instance , if you decide that your organisations's employees urgently needs to look at customer information when they're taking ten to six phone calls, you can do that so they prob won't log in during weekends and evenings.

- Click on **Profiles** in the setup using **quick find**
- Click a name after selecting a profile.
- Click edit under login hours
- Set the dates and times
- Click **Save**

2.2.5 Controlling Access to the Records

a. Record-Level Security

To accurately monitor access to the data, you can allow specific users to view particular fields in a specified object, but then limiting the individual records they are authorized to see.

You regulate the record-level access in four different ways. They 're listed in the of increase in access. You will be using org-wide defaults to secure your data to its most restrictive stage and then, as needed, use other record-level security tools to provide access to specific users.

- **Org-wide defaults** : Specifies the default degree that users have access to each other's information.
- **Role hierarchies** : Ensures that the supervisors access information similar to their subordinates. Increasing role in the hierarchy reflects a level of access to data needed by a user or group of users.
- **Sharing rules** : Are the automatic exceptions to the org-wide standards for different groups of users, to allow them access to information that they do not own or usually can not see.

- **Manual Sharing** : Lets the record owners offer read and modify permissions to the users who might not otherwise have access to the data.

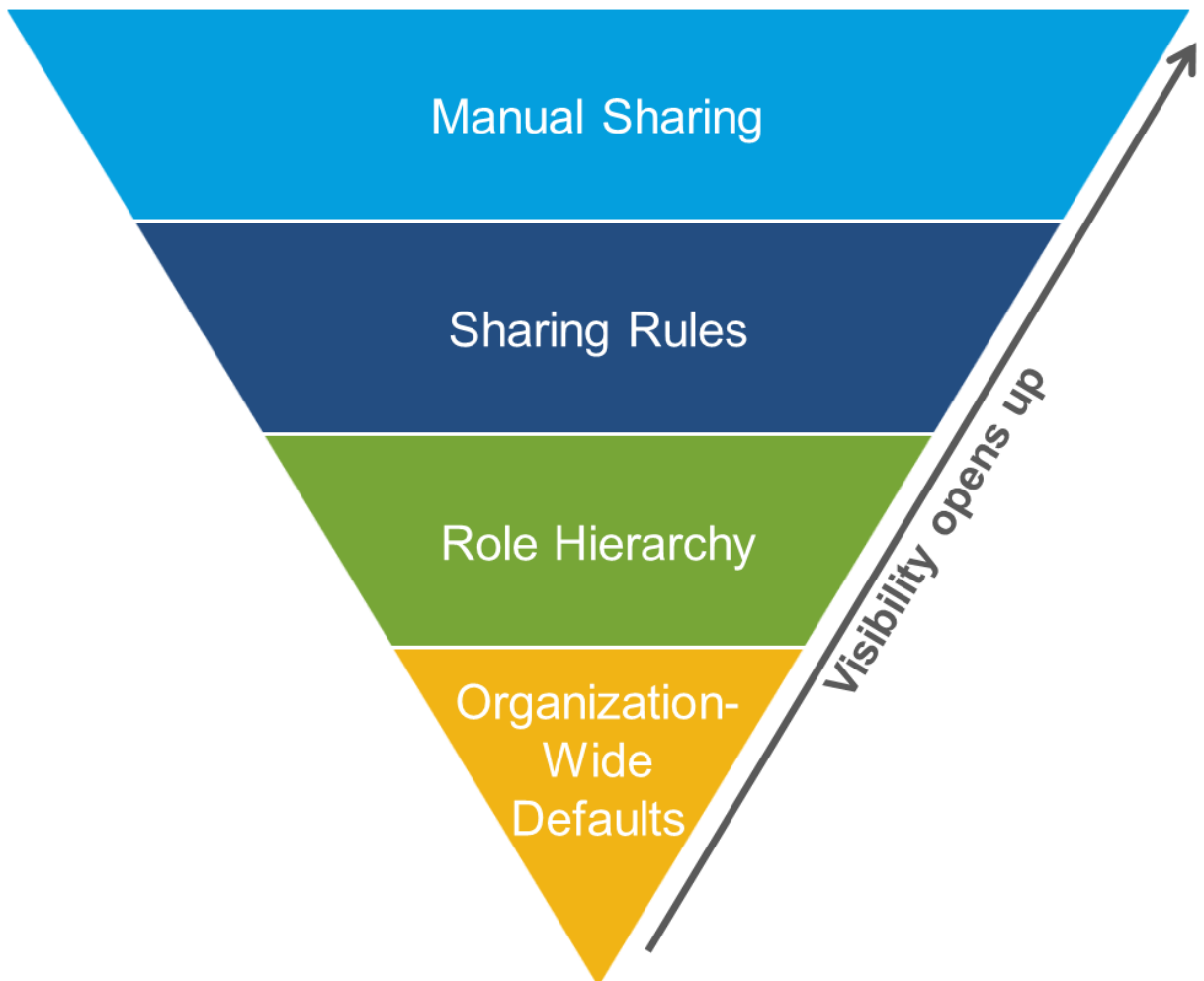


Fig: 2.2.5 a : Record level Access

b. Sharing Org-wide

Org-wide defaults defines the baseline level of access that the most limited user must have. Always use the org-wide defaults for encrypting the data, and then use the other protections and sharing resources at the record level (sharing rules, manual sharing and role hierarchies,) for

opening up the data for the users who needs it. The Object permissions specifies the default access level for all information within an entity. Org-wide defaults change certain permissions for information that a user does not own. Org-wide sharing parameters can be set individually for each and every object type. Org-wide defaults will never give users more access than what they have by their object's permission.

Consider these questions about every object to decide about the org-wide defaults you really need for your app:

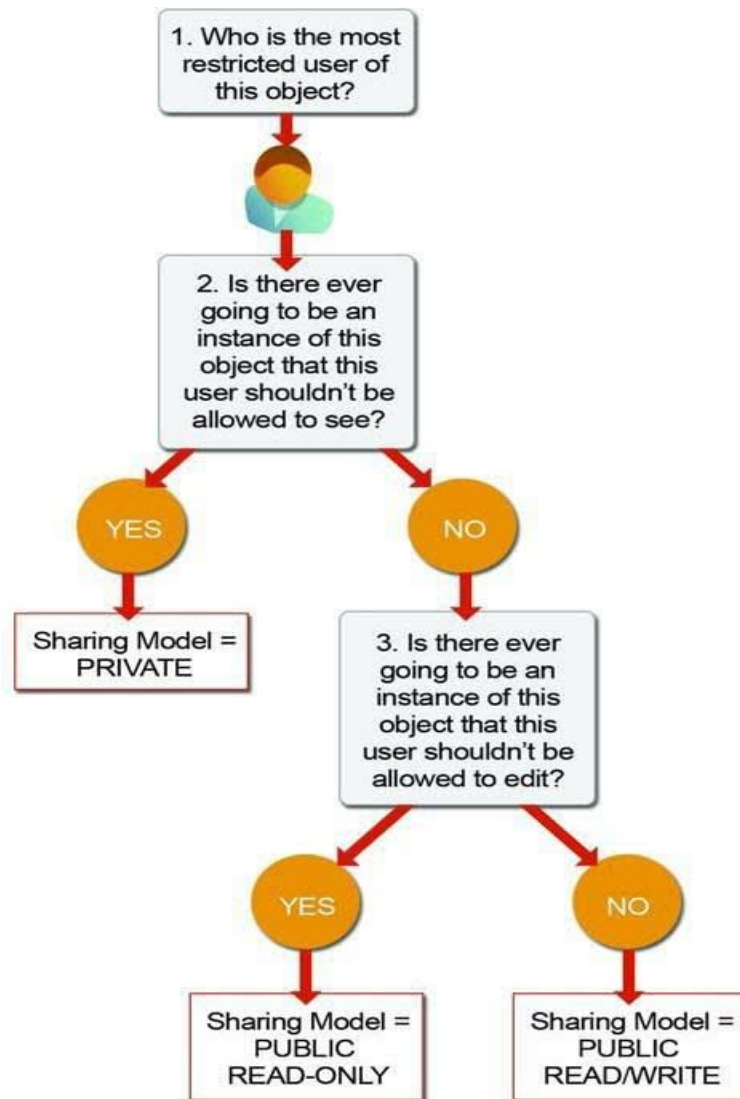


Fig 2.2.5 b : Org-Wide Sharing

- Who is that object's biggest restricted user?
- Will there ever be an instance of this object this user wouldn't be allowed to see?
- Will there ever be an example of this object that such a user shouldn't be authorized to modify?

Response on your answers, you can established one of those settings to the sharing model for that object

Private

Only owner of the record and the users in the hierarchy above are able to view, modify and report these records.

Public Read Only

Every users can access and report on the records, but only the owner can modify them, as well as users above that position in the hierarchy can.

Public Read/Write

All users are able to access, modify and report any records

Controlled by Parent

A user can access , update or remove a record if she is able to do the same thing on the record it belongs to .

c. Setting the Org-Wide Sharing to Defaults

Using org-wide defaults for specifying the level of access a most restricted user must have on the baseline level.

- Click on **Sharing settings** in the setup using **quick find**

- In **Org-wide** defaults area, click **edit**
- Select default access for each object

Organization-Wide Sharing Defaults Edit [Help for this Page](#)

Edit your organization-wide sharing defaults below. Changing these defaults will cause all sharing rules to be recalculated. This could require significant system resources and time depending on the amount of data in your organization.

Object	Default Access	Grant Access Using Hierarchies
Lead	Public Read/Write/Transfer	<input checked="" type="checkbox"/>
Account, Contract and Asset	Public Read/Write	<input checked="" type="checkbox"/>
Contact	Controlled by Parent	<input checked="" type="checkbox"/>
Opportunity	Public Read/Write	<input type="checkbox"/>
Case	Public Read/Write/Transfer	<input checked="" type="checkbox"/>
Campaign	Public Full Access	<input checked="" type="checkbox"/>
Activity	Private	<input type="checkbox"/>
Calendar	Hide Details and Add Events	<input checked="" type="checkbox"/>
Price Book	Use	
Candidate	Private	
Employment Website	Public Read Only	
Job Application	Public Read Only	
Position	Public Read/Write	<input checked="" type="checkbox"/>

Some standard objects use different org-wide default options.

Custom object org-wide default options include Private, Public Read Only, or Public Read/Write.

Fig 2.2.5 b : Org-Wide Defaults

2.2.6 Creating a Role Hierarchy

Creating and Editing Roles

The role hierarchy works in conjunction with sharing settings for determining the levels of access privileges to your Salesforce data. Users will view all the users' information in the Hierarchy level below them. Users needing to access a lot of data (like the executives, CEO) often appear close to the top of the pyramid. But role hierarchies need not fit your org's chart. Every other role in the hierarchy simply represents a level of information access needed by an user or group.

To use hierarchies for controlling sharing access for every custom object, search **Sharing Settings** in **Quick Find box** present on the left side, and then select **Sharing Settings**. Click the **Edit** button in the Org-Wide Defaults segment. Disable **Grant Access Using Hierarchies** if you wish to prevent users from automatically trying to gain access to data controlled or shared throughout the hierarchies with their underlings.

Defining a Role Hierarchy

It's easy to incorporate a role hierarchy in the project once you get an idea about what the hierarchy will look like. Beginning with the org chart of the company is easiest, and then consolidating multiple work titles into single positions whenever possible.

- Click on **Roles** in the setup using **quick find**

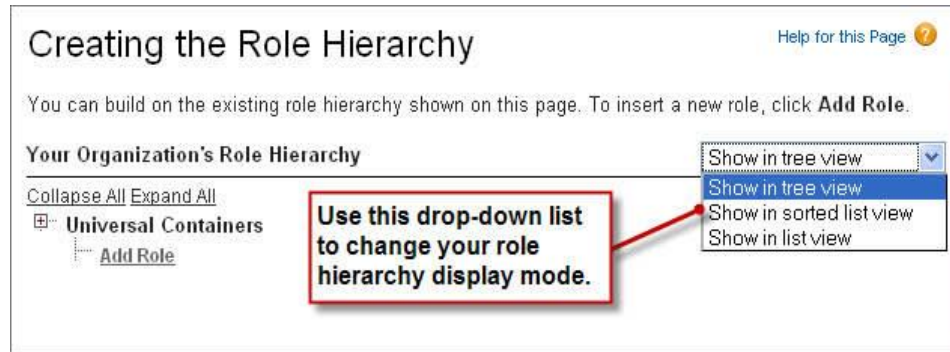


Fig 2.2.6a : Creating role hierarchy

- Click **Add Role** under the company's name
- Select default access for each object
- Enter the required details like label and enter access levels
- Now click on **Assign Users to role** and enter the role name
- Click Save

Role: **CEO** [Help for this Page](#)

Below is the list of users assigned to this role. Click Edit to modify the role name. Click Assign Users to Role to assign existing users to this role. Click New User to create a user for this role.

Hierarchy: Universal Containers » CEO
Siblings:

[Users in CEO Role \(0\)](#) | [Category Group Visibility Settings \(0\)](#)

Role Detail [Edit](#) [Delete](#)

Role Name	CEO	Role Name as displayed on reports	CEO
This role reports to	None	Sharing Groups	Role, Role and Subordinates
Modified By	Jane Smith , 8/16/2010 1:58 PM		
Customer Portal Role	<input type="checkbox"/>		

Every role can have one or more assigned users.

Users in CEO Role [Assign Users to Role](#) [New User](#) [Users in CEO Role Help](#)

No records to display

Fig 2.2.6b : Adding a Role

2.2.7 Define Sharing Rules

Defining a Public Group

It's necessary to set up the correct public group before developing a sharing rule. A public group is a group of specific users, territories or individual roles and/or roles or territories which all have a similar feature with their subordinates.

- Click on **Public groups** in the setup using **quick find**
- Click **New**
- Insert Required information regarding public group

Group Membership Help for this Page

New Group

Group Information Save Cancel

New Public Group = Required Information

Label

Group Name i

Grant Access Using Hierarchies i

Search: Roles and Subordinates for: Find

Available Members

- Role and Subordinates: Director QA
- Role and Subordinates: Director, Channel Sales
- Role and Subordinates: Director, Direct Sales
- Role and Subordinates: Eastern Sales Team
- Role and Subordinates: Installation & Repair Services
- Role and Subordinates: Marketing Team
- Role and Subordinates: Product Manager
- Role and Subordinates: QA Engineer
- Role and Subordinates: Recruiter
- Role and Subordinates: SVP, Customer Service & Support
- Role and Subordinates: SVP, Human Resources
- Role and Subordinates: SVP, Sales & Marketing
- Role and Subordinates: SW Dev Manager
- Role and Subordinates: SW Engineer

Add ▶

Remove ◀

Selected Members

- Role: SW Dev Manager
- Role: Director Product Management
- Role: Director QA
- Role and Subordinates: Recruiting Manager

Save Cancel

Fig 2.2.7 : Adding a Public Group

- Add required personal by clicking on **add**
- Click **Save**

Defining a Sharing Rule

A sharing rule may be defined for a single public role, group or territory. For a position including its subordinates or for a territory including its subordinates you may also establish a sharing rule.

There already is a public community that includes every user in your company, by design.

- Click on **Sharing Settings** in the setup using **quick find**
- From a drop down list named as **Manage sharing settings** , click job application .
- Select required access and defaults
- Click **Save**

CHAPTER 3

SESSION-BASED PERMISSION SETS AND SECURITY

3.1 Session-Based Permission Sets: An Overview

Permission sets lets you create a collection of user assignment permissions. For example, you can allocate the permissions for Managing Cases , Editing Case Comments, and Editing Activated Orders for all Supporting Managers in the org by allowing all three permissions in one set of permissions for convenient assignment.

Session-based permission sets works on the same concept, but with a session-activation feature added. When a user logs in, and starts to communicate with another user or device, a computer session begins. For instance, when you verify in your workplace computer network, you start or trigger a session that lasts until you sign off or until the session is ended for another reason.

Using session-based permission sets, one can restrict the operational access in a permission set to an enabled session for selecting permissions. When a session ends for any cause, before the user can access limited resources, a session-based permission set should be activated once again.

3.1.1 Creating a Session-Based Permission Set

It is simple to build a collection of session dependent permissions. Very smooth. The steps are in fact close to identical to any other set of permissions. The difference to this? When building your collection of permissions, you must pick Session Activation Required:

Selecting the Session Activation needed indicates to Salesforce that with only an activated session will a permission set can get enabled.

SETUP
Permission Sets

Permission Set
Create

Help for this Page ?

Save Cancel

Enter permission set information | = Required Information

Label

API Name i

Description

Session Activation Required i

Select the type of users who will use this permission set

Who will use this permission set?

- Choose '--None--' if you plan to assign this permission set to multiple users with different user and permission set licenses.
- Choose a specific user license if you want users with only one license type to use this permission set.
- Choose a specific permission set license if you want this permission set license auto-assigned with the permission set.

Not sure what a permission set license is? [Learn more here.](#)

License

Save Cancel

Fig:3.1 Permission Set

Steps for Creating Permission Sets :

- Click on **Permission Set** in the setup using **quick find**
- Click **new** and enter your **permission sets**
- Make sure to select **Session Activation Required**
- Click **Save** after checking **license requirements**

3.1.2 Activating Session-Based Permission Sets (without using code)

Since you've built your own collection of session-based permissions, let's make them available. You need to provide a way to enable a session for the collection of permissions to make it available. If you want to get your shit done with APIs, you could do that and we're not going to stop you. The **PermissionSet** object in the API contains a property called **HasActivationRequired**, a boolean indicating whether or not the set of permissions needs an active session (**true**) linked with it. Attach a record into the **SessionPermSetActivation** object with both the session ID and permission set for the trigger to be activated.

Actually this flow only works with one stage! You probably already have it figured though, that if you want to know more, Trailhead have you covered — and we encourage all to do so. Make sure you has permissions for continuing the accessing of the flow though! Let's just verify permissions rn.

1. Go to profile. Go to Users in Setup, and pick your profile. Using of the System Administrator profile is more than likely to be used by you.
2. Lookout for the option Manage Flow , and make sure that it is selected.

Now lets get back to our precious session based permission sets flow:

- Click on **Flows** in the setup using **quick find**
- Click **new Flows**
- After selecting **Screen Flow** , click on **Create**
- Drag **Actions** from elements tab from toolbox
- Search **Activate** and click on **Activate Session-based Permission Set**
- Click on **Done**

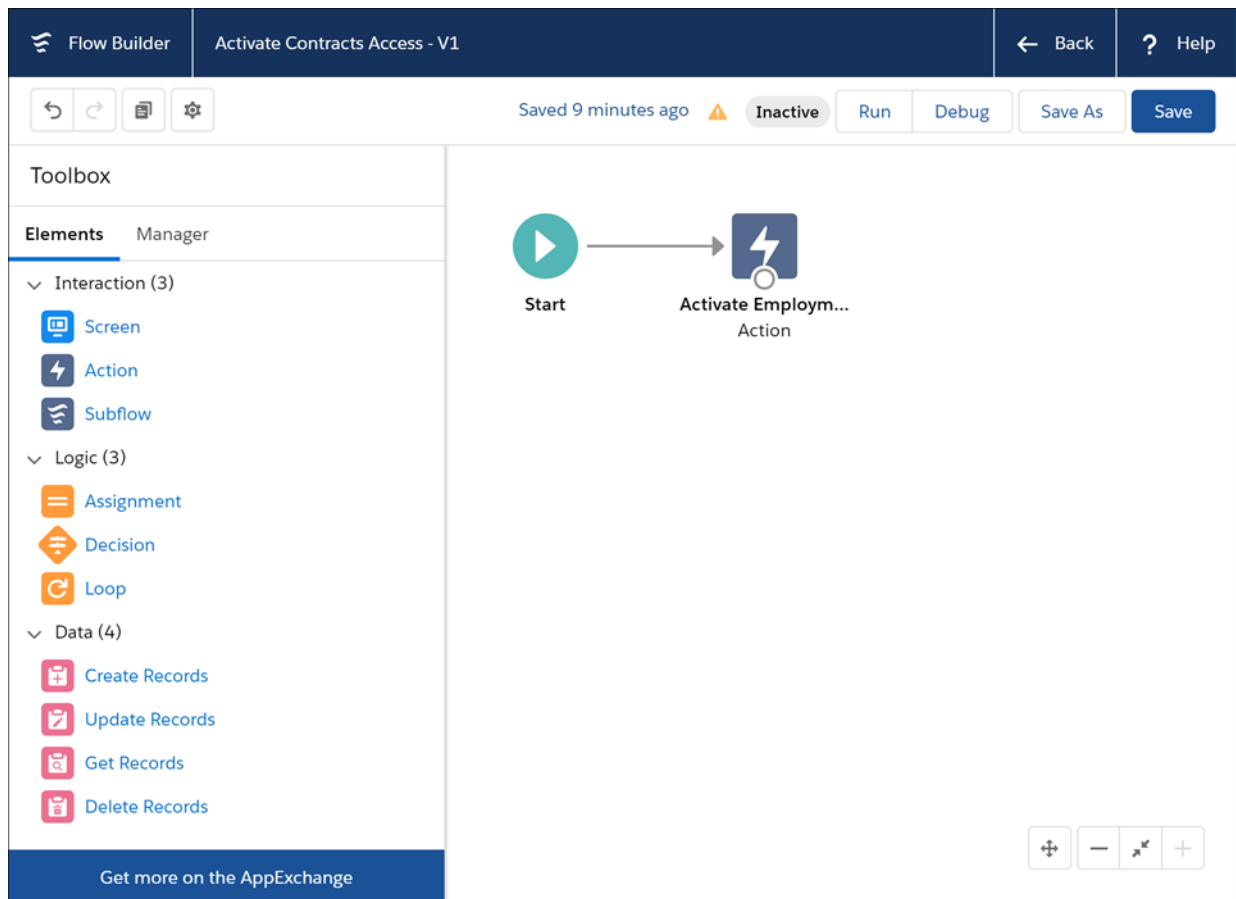


Fig 3.1.2 : Session Based Permission Sets

3.1.3 Creating Easy access for Activation flow

Using Lightning Page

We developed a session-based permission set in earlier topics and activated it by using a flow and allocated the permission set to the user. If you stop here, you might have users run their flow to enable their own permission collection. It can be awkward though, and is not very user-friendly. In our case, most hiring managers may not need to operate flows, and may not have authorities to run these.

You could use a simple Visualforce markup for creating a custom tab that will run your flow. In reality, in the past you might be using Visualforce already. But if you'd like to make things much easier on your own, it is recommend to use a page with the Lightning app.

- Click on **Lightning builder app** in the setup using **quick find** after searching **Builder**
- Click **new** and before clicking **Next** , Select **App page**
- After entering the name **Name** , click on **Next**
- Click **Finish** after selecting **One Region**
- Drag into the components of **Flow** and enable **activate contracts access**
- **Activate** and click **Save**
- Select the **Lightning Experience** on the activation page
- Click on **Save** and return back

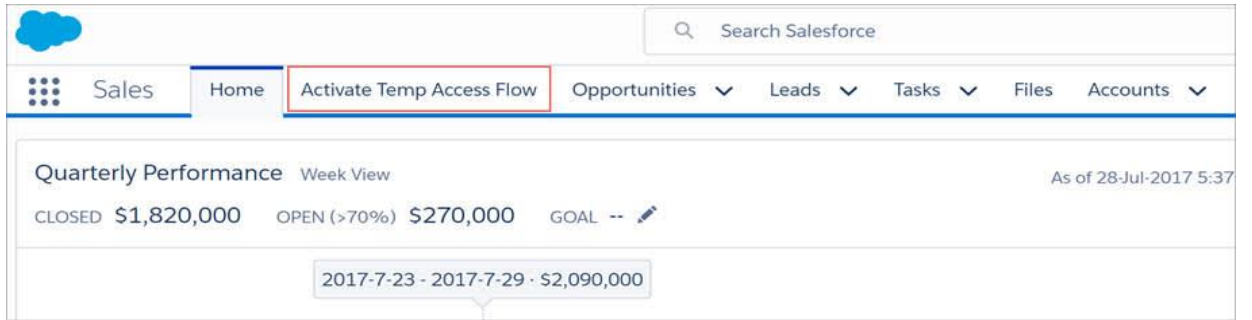


Fig 3.1.3 : Activation Flow

CHAPTER 4

IDENTITY

4.1 Salesforce Identity

Salesforce Identity lets you, at the right moment, give the right people access to appropriate resources. .You control and decides who can access your orgs, and who would use apps that run on Salesforce Platform, on-site, in other smart phones, and on clouds

With the Salesforce Identity, you log in just once to gain the access to multiple connected apps.



Fig 4.1a : Multiple apps

Meaning Of Identity

Identity is a powerful phrase in the tech industry and has various significances depending on the context. Yet identity has usually come to mean providers of identification ensuring people are who they think they are.

while in Salesforce we talk about digital context of user information, like who the user is and what the one could do in a specific context. It also might include selected features, such as names(first and last names) , contact's information , or even a work title.

Features of Salesforce Identity

Identity management is an immense logistical environment and Salesforce Identity provides tools that tackle certain aspects of this. A well-designed implementation of Salesforce Identity starts with both the determination and prioritization of the features are appropriate for the department. Start with introducing a functionality or two. Then, in time, add more functionality.

List of key Salesforce Identity features are :

SSO(Single Sign on) : Single sign-on allows users to access all approved services without signing in to each one individually — even without creating (and remembering) specific login credentials for each program. You could connect the clients to many other Salesforce orgs and other clouds functioning accounts and apps. For eg, a Salesforce Identity help desk rep can click a connection and sign in to other apps, such as Google Apps, Playgames , Xbox instantly.

Social Sign On: Users can log in to a Salesforce orgs with their login credentials from an external authentication service, such as Google or Facebook etc , using social sign-on. With some clicks, you can configure any of those providers. You can establish other

services with a little bit of more effort, including Amazon or many other similar services. Whenever you want clients to be able to connect in to a network without creating (and remembering) a new login credentials, social sign-on is incredibly beneficial. Clients can use the Facebook or Google account to log in to a Salesforce Group.



Fig 4.1a : Social Sign On

Connected Apps : Connected applications tie together the Salesforce orgs, third party softwares, and other utilities. When a connected application is created without trying to implement SSO, it will act as a bookmark. Users can access the app from its drop down menu or launcher for apps but often they have to log in and use this again. So customize them with SSO and get the most of it out like linked phones. Administrators can establish security policies via SSO, and have a clear control of the ones who uses what software. You could also use linked apps to handle mobile device security and policy.

Two Factors Authentication: In allowing two-factor authentication, clients, in relation to their login credentials, must have a secondary "factor," or proof of the identity. The other key factor can be an authentication code from a phone authenticator app such as Salesforce Authenticator which the customer gets. Or clients could have a phone message or e-mail passcode sent to them. For the latest model of the Salesforce Authenticator application , the second element could be a reply to an user 's smartphone push notification. Two-factor authentication ensures that the intruder can't sign in and do damage even though an intruder acquires an username password.



Fig 4.1b : two factor authentication

4.2 Knowing your identity users (in Salesforce)

Employee: You and your colleagues have unique access into the Salesforce orgs as well as some other online resources in your business. Your firm understands you all just well and fine. It trusts you with useful services and information so you can create and offer its solutions to the company's goods. To protect this confidence, you as a Salesforce administrator need to make sure how all employees are given special access. So to keep the company going smoothly you need to remove obstacles that make it difficult for workers to do their work.

Customers and Partners: Some people also need access to the Salesforce orgs or groups in the company. Most of these of them are clients, or prospective clients. Others may be collaborators who collaborate with both companies for the good of your client.

Your firm knows these guys not as good as the employees. You wouldn't want to offer the very same special access that the employees get to clients and stakeholders, but you still like to make it simple for them to achieve their goals by visiting your firm online.

The Salesforce Identity is easy and safe way. Salesforce Identity includes removing obstacles that hold back employees when retaining the robust security controls. Some key advantages of Identity are:

Convenience : Employees may sign it into a workspace without signing in once again, and login to the Salesforce org. We will only have a single username, which functions with both of their site and smartphone devices. You can allow them access to the third party collaboration apps and resources, such as gmail or outlook or MSoffice, by one-clicking.

Control : Managers and overseers may have more influence over their workers. If you want to have fine-grained much control over who uses how much, you can involve a supervisor or a manager to authorize requests from employees to connect to an app or product. And you could do that also, when you decide to revoke connections to an device.

Security : The beauty of Salesforce Identity would be that improved security leads to more functionality plus greater power. Single identity origin for login details through company networks and the internet makes tracking and control of usage easy for both you and other Salesforce administrators. High redundant profiles and high malicious activities risk.

Comparing Features :

Almost everybody benefits from most apps. Many apps help workers or associates and consumers alike. Many apps are to the advantage of staff or clients and partners in particular. Go back to the first section, "Getting to Know the Salesforce Identity," for just a

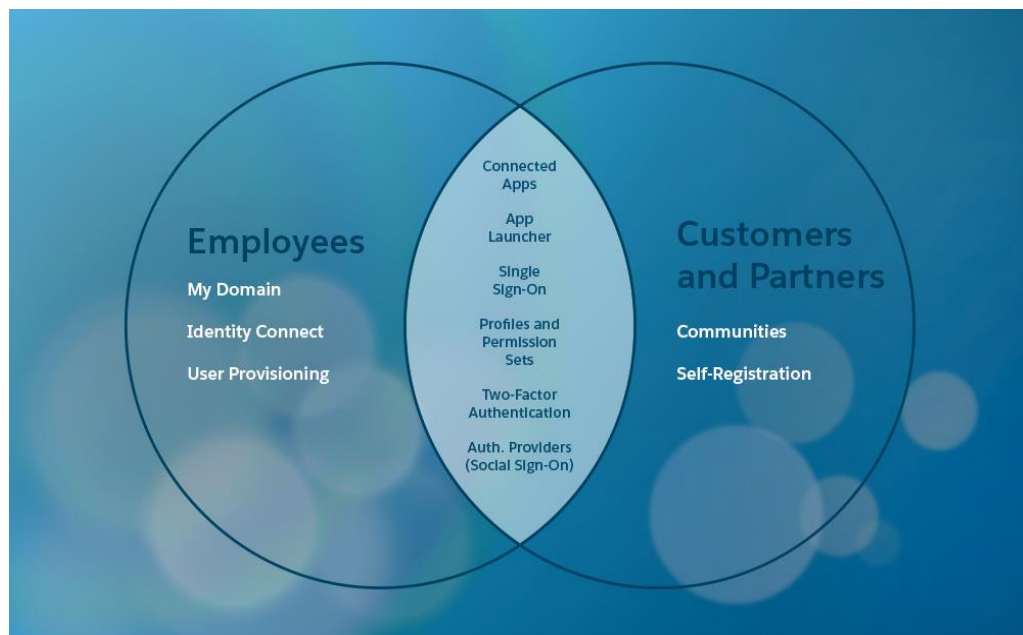


Fig 4.2 : Comparing Features

reality check on all of the features which makes up Salesforce Identity.

4.3 Learning the Identity's Language

Identity Protocols :

- SAML
- OAuth 2.0
- OpenID Connect

Protocol SAML :

You sets up single sign-on (SSO) if you want users to switch effortlessly among Salesforce orgs as well as apps without having to signing in frequently. Security Assertion Markup Language (SAML) is the protocol which allows for this.

Watch SAML in working :

- It is SAML in practice while you are logging into Salesforce and afterwards press the App Launcher to just get straight to your inbox.
- When people already sign in to other apps will access the Salesforce org by not signing in again, that's SAML in practice too.

XML and SAML

SAML protocol is based on XML , meaning that only the data packets being shared are described in XML. XML should be (nearly) human-understandable , and you'll get some insight into what's happening on. That's great news once you're struggling to figure out why things function efficiently. The following chart displays a section of an statement by SAML. Does this sound nonsense? Look again and you'll see it's not all that bad looking. This includes the username information, contact number, and name details.

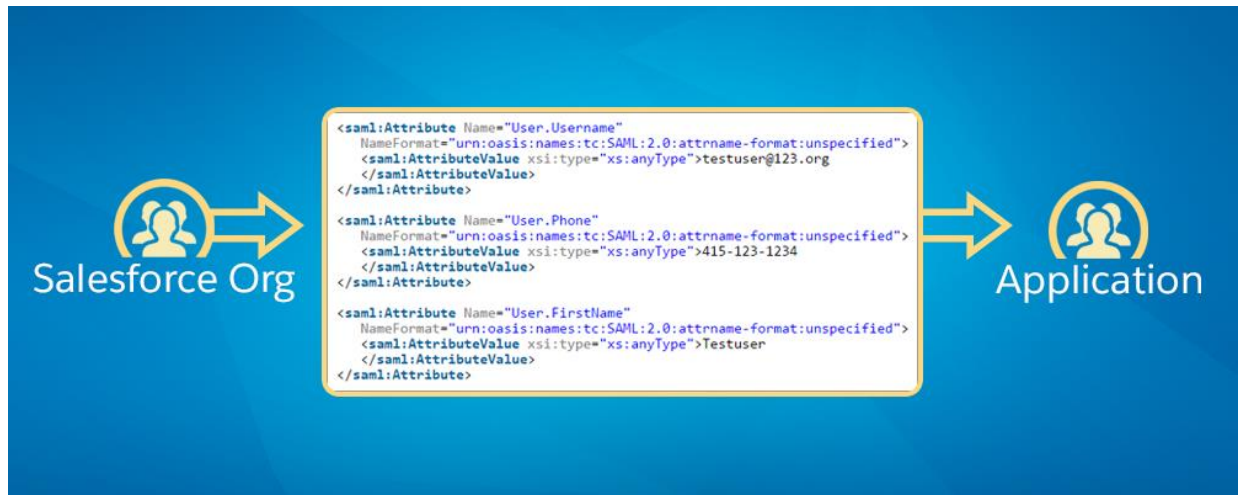


Fig 4.3a : SAML

Protocol OAuth 2.0 :

OAuth 2.0 is just an open protocol that is used for the safe sharing of data among apps. For one device the user functions but views the information from the other. You're signed in to the Salesforce app, for eg, and see your Salesforce org's data info.

For example :

- A smartphone device that uses OAuth to pull the contacts from the Salesforce org.
- A Salesforce org even requires OAuth to get contacts from some other company.

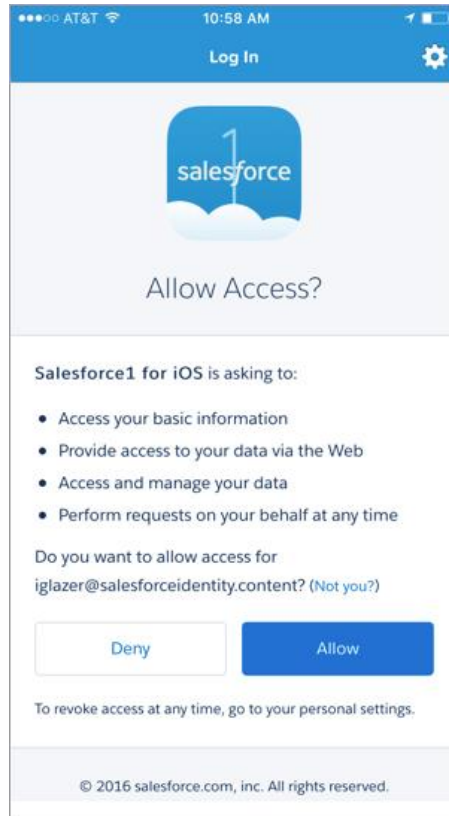


Fig 4.3b : Example of an app requesting approval for the person to view information via OAuth 2.0.

Protocol OpenID Connect :

As with SAML, OpenID Connect is also an OAuth 2.0 oriented protocol that transfers identification information through one provider to the other. Unlike SAML, OpenID Connect is planned for modern social networking environment.

The developer of the application was using the OpenID Connect protocol to allow for social sign-on.



Fig 4.3c: Open ID Connect

The advantages for users of a OpenID Connect protocol is that they have been able to reduce the nos of different accounts, login credentials. On the contrary, developers have no need to own and handle password documents to authenticate one’s users along all sites and blogs. The method makes it incredibly difficult for hackers to access logins.

Identity and Service Providers

SAML shares identity information between both the identification holder, named an identity provider (IdP), and the desired service, called a service provider, in the course of verifying the users.

Service Provider : Authorized user can circulate into Salesforce with an external identifier provider. Salesforce is indeed a service provider throughout this case users would like to have

access to this service, and one's Identity Provider enables them to do just that. This setup of Salesforce is popular as the organization also already uses an Identity Provider.

The identity provider would be one of many on the marketplace, Users sign in with an ID and then are routed to Salesforce (service provider). In another section, you can set up SSO as just a service provider within Salesforce, and also as an independent identity provider with such a third party client.

Identity provider : Authorized customers can also migrate from Salesforce to many other platforms and applications. In this scenario, Salesforce serves as an Identity Provider and offers SSO to better connect to various service providers.

SSO (SAML flow)

SSO processing all occurs with breakneck speed, but requires a few steps.

- The customer tries to connect to Salesforce.
- Salesforce accepts the SSO request and then creates a SAML submission.
- Salesforce connects the order for SAML back to app.
- The client connects the SAML request to the provider with an external name.
- The identity provider validates the identity of a user and bundles the statement of SAML that includes the authentication services.
- The SAML statement is sent to the user by the Identity provider.
- The client then redirects the argument to Salesforce.
- Salesforce is checking the assertion.
- Now, the user is logged in and can navigate Salesforce.

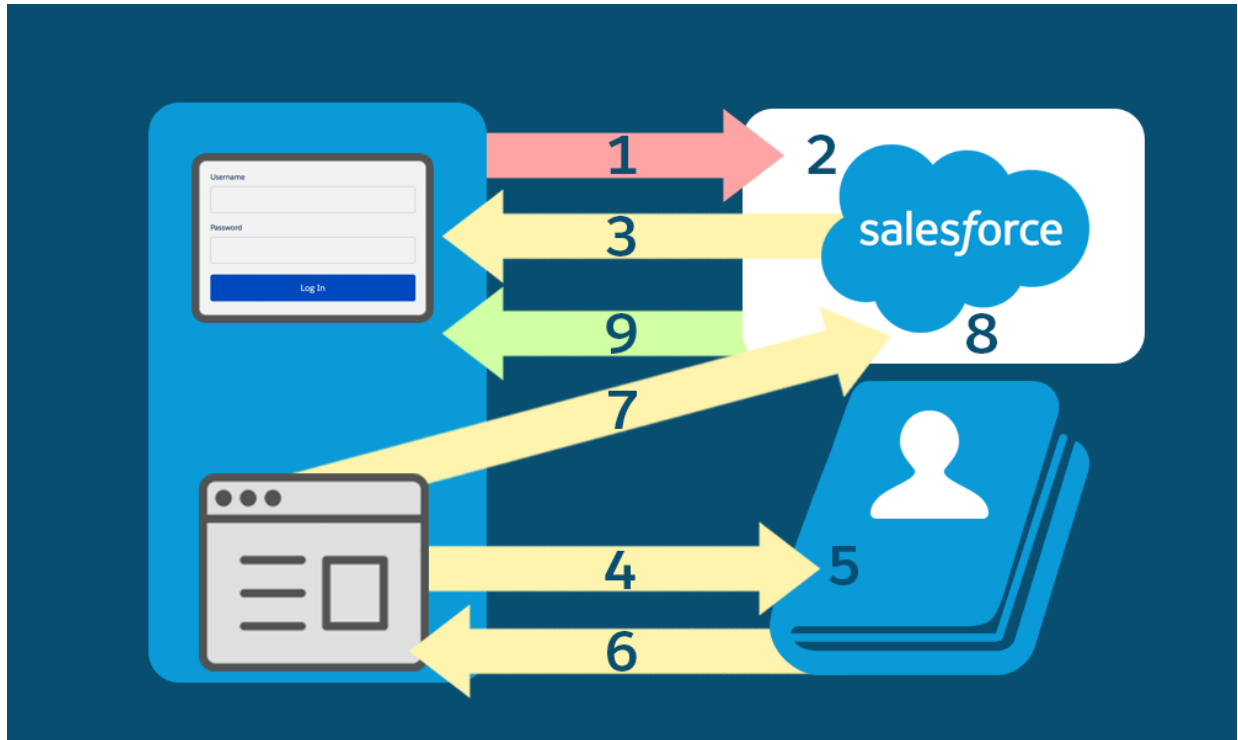


Fig 4.3d: SAML flow

CHEAT SHEET FOR IDENTITY (Fig 4.3e)

One Term	That's Easily Confused with This Term
Authentication means who a person is. These days, authentication is often used as shorthand for authorization and authentication.	Authorization means what a person can do.
Protocol specifies the set of rules that enable systems to exchange information. Generally, the term protocol and standard are used interchangeably.	Standard is a specification, a set of industry practices that vendors agree to support. Often, a standard contains a protocol to specify how the companies implement the standard.
Username and password are what the user supplies to log in to a system.	Credentials are basically the same thing.
Single sign-on (SSO) enables a person to log in once and access other apps and services without logging in again.	Social sign-on enables a person to log in to an app using the credentials established with a social account like Google. That app accepts the Google credentials, and the user doesn't have to create another account and password.
Identity provider is a trusted service that enables users to access other websites and services without logging in again.	Service provider is a website or service that hosts apps and accepts identity from an identity provider.

CHAPTER 5

USER AUTHENTICATION

5.1 Securing User's Identity

Using two factor authentication

It depends on two factors

- Some users know stuff, like their password
- Several users have downloaded something, such as a smart phone with an authenticator app

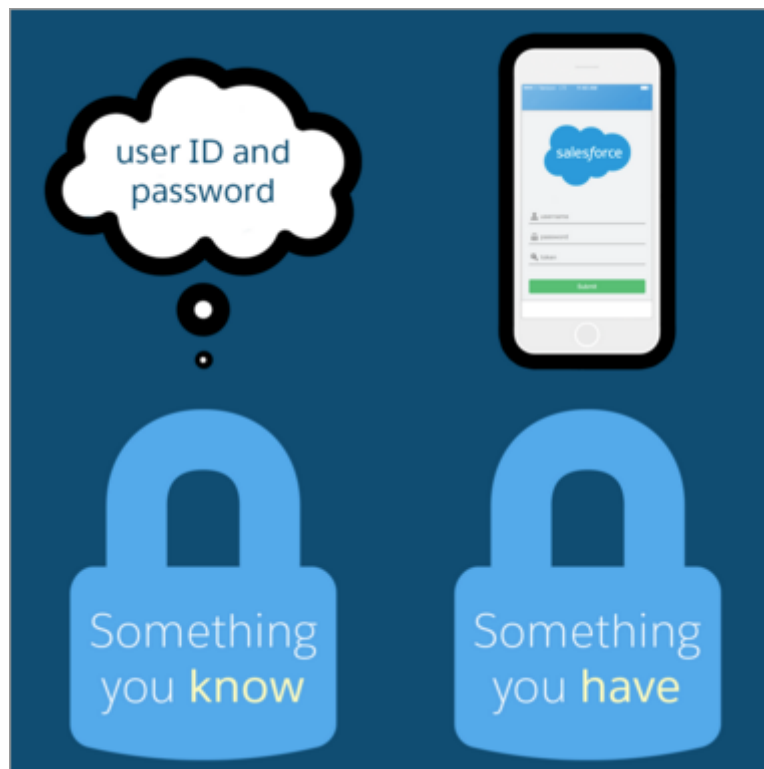


Fig 5.1 : Two Factor Authentication

The second authentication element provides an additional security layer for the org. As an administrator, you will request it any time your users sign in. Or you can only allow this under such cases, such as when users sign in from an unrecognized system or attempt to access a highly risked program. Once users check their identity correctly using both authentication methods, they can enter Salesforce and begin to work.

5.1.1 Setting Up Two Factor Authentication

Step 1: Search Session Settings in the quick find box and open it . make highly sure that two factor authentication is highly assured.

Step 2: Creating a user :

- Select **Users** from quick box after searching
- Select **new user**
- Enter user credentials
- Click **save**
- Login as created user and reset password

Step 3: Creating two factor authentication

- As you are logged in as Sia , now signin as Admin
- Select **Permission Sets** after searching in quickfind box
- Enter all details and enable two factor authentication
- Select **Save**

Permission Set Video Tutorial | Help for this Page ?

Two-Factor Authentication for Logins

Find Settings... | [Clone](#) [Delete](#) [Edit Properties](#) [Manage Assignments](#)

Permission Set Overview

Description	API Name	Two_Factor_Authentication_for_Logins
User License	Namespace Prefix	
Created By Ruth Cloud , 2/18/2016 10:11 AM	Last Modified By	Ruth Cloud , 2/18/2016 10:11 AM

Apps

Settings that apply to Salesforce apps, such as Sales, and custom apps built on Force.com
[Learn More](#)

- Assigned Apps**
Settings that specify which apps are visible in the app menu

- Assigned Connected Apps**
Settings that specify which connected apps are visible in the app menu

- Object Settings**
Permissions to access objects and fields, and settings such as tab availability

- App Permissions**
Permissions to perform app-specific actions, such as "Manage Call Centers"

- Apex Class Access**
Permissions to execute Apex classes

- Visualforce Page Access**
Permissions to execute Visualforce pages

- External Data Source Access**
Permissions to authenticate against external data sources

- Named Credential Access**
Permissions to authenticate against named credentials

- Custom Permissions**
Permissions to access custom processes and apps

System

Settings that apply across all apps, such as record and user management
[Learn More](#)

- System Permissions**
Permissions to perform actions that apply across apps, such as "Modify All Data"

Fig 5.1.1 : Creating two factor authentication

Step 4: Assigning permission set

- Select **Manage Assignments** in the detail page of permission set
- Add assignments and select **assign**

5.2 Setting up SSO

SSO has many factors such as

- You spend a little less time administering the passcodes.
- Your workforce save resources when they're not forced to sign in to Salesforce directly. Have you known users would take 5–20 secs to sign in to an online process? Those moments are adding up.
- Many people are using Salesforce. Users can submit links to documents and information from Salesforce, and their receivers can access them with just a single button.
- You could even manage the access through one place to confidential material.

Step 1: Create an ID

- Click **Users** from quick find box after searching **Users**

The screenshot shows the 'Single Sign On Information' configuration page in Salesforce. The 'Federation ID' field is highlighted with a red oval and contains the value 'sia@jedeye-tech.com'. Below it are sections for 'Locale Settings' (Time Zone, Locale, Language) and 'Approver Settings' (Delegated Approver, Manager, Receive Approval Request Emails). At the bottom are 'Save', 'Save & New', and 'Cancel' buttons.

Fig 5.2a : Creating ID

- Click **Edit** to the name of which you wanna create SSO for
- Click **Save**

Step 2: Set up SSO

- In a new tab goto **axiomssso.herokuapp.com**
- Select “ **SAML Identity Provider and Tester** “
- Select **Single Signon Settings** from Quickfind Box
- And Fill all the necessary Settings
- And then Select **Save**

Fig 5.2b : Setting up SSO

Step 3: Linking Salesforce and identity Provider

- Return to **axiomssso.herokuapp.com**
- Select “ **SAML Identity Provider and Tester** “
- Select “ **Generate SAML response**”
- Then insert following values

SAML Single Sign-On Settings Printable View | Help for this Page ?

[Back to Single Sign-On Settings](#)

Edit Delete Clone Download Metadata SAML Assertion Validator

Name	Axiom Test App	API Name	Axiom_Test_App
SAML Version	2.0		
Issuer	http://axiomssso.herokuapp.com		
Identity Provider Certificate	CN=Axiom Demo Certificate, OU=FOR DEMONSTRATION PURPOSES ONLY. DO NOT USE FOR PRODUCTION ENVIRONMENTS., O=Axiom SSO, L=San Francisco, ST=CA, C=US Expiration: 5 Nov 2041 04:30:27 GMT		
Request Signing Certificate	Default Certificate		
Request Signature Method	RSA-SHA1		
Assertion Decryption Certificate	Assertion not encrypted		
SAML Identity Type	Federation ID		
SAML Identity Location	Subject		
Service Provider Initiated Request Binding	HTTP Redirect		
Identity Provider Login URL			
Identity Provider Logout URL			
Custom Error URL			

Just-in-time User Provisioning

User Provisioning Enabled

Endpoints

Login URL	https://jedeye-tech-dev-ed.my.salesforce.com?so=00D36000000Y40p
OAuth 2.0 Token Endpoint	https://jedeye-tech-dev-ed.my.salesforce.com/services/oauth2/token?so=00D36000000Y40p

Edit Delete Clone Download Metadata SAML Assertion Validator

Fig 5.2c : linking Salesforce and Identity

Step 4: A final check

- Select “**request SAML response**” in the settings of Axiom.
- It generates a XML response like as figure 5.2d
- Click **Login**

Use this form to encode and submit a SAMLResponse and TARGET with an HTTP POST binding to Salesforce. Start by pasting a plain-text SAML Response in XML format or [generate a new one](#). Optionally include plain-text URLs for configuring the startPage, startURL, and logoutURL. All input in the Automatic POST Builder is automatically encoded, but if necessary, make any other changes in the Manual POST Override section, and click Login.

Plain Text SAML Response:

```
<xsi:type="xs:string">http://axiomsso.herokuapp.com/RequestSamlResponse.action
</saml2:AttributeValue></saml2:Attribute><saml2:Attribute Name="logoutURL"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
<saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string"/></saml2:Attribute></saml2:AttributeStatement>
</saml2:Assertion></saml2p:Response>
```

Fig 5.2d: XML response

CONCLUSION

1. We created an efficient process for Security Measures
2. After security measures we were able to get a proper role hierarchy for security measures such as managers and employees as what data to be shared and not to be shared.
3. We discussed the ways of implementing those proper security measures as by various methods
4. We compared many security measures and a PaaS and SaaS
5. We discussed the difference between employees and customer partners as the identity measures in between
6. As we study forward there are many other forms of protecting Salesforce data, in this we only include important and basic ones
7. We did a thorough study on Single Signon and Two factor authentication as these are mainly in high demand
8. We studied a way of connecting various platforms with one another in sharing efficient data in between each other using a secure and efficient transmission.

REFERENCES

- <https://developer.salesforce.com/docs/atlas.en-us.224.0.securityImplGuide.meta/securityImplGuide/>
- https://trailhead.salesforce.com/content/learn/modules/identity_login/identity_login_sso?trail_id=security
- <https://salesforce.vidyard.com/watch/1adyGmUFX9JTrvBQYhdxVQ>
- https://trailhead.salesforce.com/en/content/learn/modules/identity_basics?trail_id=security
- https://trailhead.salesforce.com/content/learn/modules/identity_connect
- <https://trailhead.salesforce.com/en/content/learn/trails/security>
- <https://www.salesforce.com/products/platform/products/identity/>

PLAGRISM REPORT

AS			
ORIGINALITY REPORT			
8%	2%	2%	7%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS
PRIMARY SOURCES			
1	Submitted to Ave Maria University Student Paper		2%
2	Submitted to Campbellsville University Student Paper		2%
3	louisdl.louislibraries.org Internet Source		1%
4	Krutarth Soni, Brijesh Vala. "Roadmap to salesforce security governance & salesforce access management", 2017 Second International Conference on Electrical, Computer and Communication Technologies (ICECCT), 2017 Publication		1%
5	Submitted to CSU, San Jose State University Student Paper		<1%
6	Submitted to National College of Ireland Student Paper		<1%
7	Submitted to Tulane University Student Paper		<1%

8	www.ijstm.com Internet Source	<1%
9	www.e-zest.net Internet Source	<1%
10	Submitted to AUT University Student Paper	<1%
11	Submitted to Colorado Technical University Online Student Paper	<1%
12	Submitted to University of Adelaide Student Paper	<1%
13	Rakesh Gupta. "Chapter 3 Platform Security", Springer Science and Business Media LLC, 2020 Publication	<1%

Pardub K...

JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT

PLAGIARISM VERIFICATION REPORT

Date: 15-June-2020

Type of Document (Tick): PhD Thesis M.Tech Dissertation/ Report B.Tech Project Report Paper

Name: Anshul Sharma Department: CSE Enrolment No : 161303

Contact No. : +919418543297 E-mail. : sharmanshul.1998@gmail.com

Name of the Supervisor : Dr. Pardeep Kumar

Title of the Thesis/Dissertation/Project Report/Paper (In Capital letters): " DATA SECURITY IN SALESFORCE"

UNDERTAKING

I undertake that I am aware of the plagiarism related norms/ regulations, if I found guilty of any plagiarism and copyright violations in the above thesis/report even after award of degree, the University reserves the rights to withdraw/ revoke my degree/report. Kindly allow me to avail Plagiarism verification report for the document mentioned above.

Complete Thesis/Report Pages Detail:

- Total No. of Pages = 62
- Total No. of Preliminary pages = 8
- Total No. of pages accommodate bibliography/references = 1



(Signature of Student)

FOR DEPARTMENT USE

We have checked the thesis/report as per norms and found **Similarity Index** at 8 (%). Therefore, we are forwarding the complete thesis/report for final plagiarism check. The plagiarism verification report may be handed over to the candidate.



(Signature of Guide/Supervisor)

Signature of HOD

FOR LRC USE

The above document was scanned for plagiarism check. The outcome of the same is reported below:

Copy Received on	Excluded	Similarity Index (%)	Generated Plagiarism Report Details (Title, Abstract & Chapters)	
	<ul style="list-style-type: none">• All Preliminary Pages• Bibliography/Images/Quotes• 14 Words String		Word Counts	
Report Generated on			Character Counts	
		Submission ID	Total Pages Scanned	
			File Size	

Checked by
Name & Signature

Librarian

Please send your complete thesis/report in (PDF) with Title Page, Abstract and Chapters in (Word File) through the supervisor at plagcheck.juit@gmail.com