



Best Practices for Data Security in Experience Cloud

Savio Jose, Product Practice Manager
savio@gscloudsolutions.com



Experience Cloud Data Security Rule Book

Build secure sites with confidence following a consolidated list of data security rules.



Rule 1

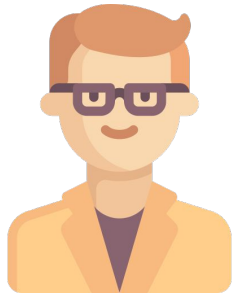
Define Personas with Granular Capabilities



Sample Personas for a Self-Service Site



External



Unauthenticated
Guest



Registered
Member



Additional Types -
Subscription Levels?

Internal



Community
Admin



Community
Moderator



Customer
Service Rep



Sample Persona & Permission Mapping Template



- Profiles are used as a shell for License & Page-Layout Assignment
- 1:1 relationship between Persona & PermissionSetGroups
 - For Internal users this is based on their job function
- Create Feature Specific Permission Sets

Persona	Profile	License	PermissionSetGroup	Feature Specific Permission Sets
Registered Member	Community Forum Member - Customer Community	Customer Community	Community Forum Member - Customer Community	<ul style="list-style-type: none">● Chatter Access● Knowledge Article Access

Rule 2

Scrutinize Unauthenticated Guest User Access



Guest User Security Policies

Enabled since Summer 20' Release

- Guest users **can't be the owner of any record** in your org.
- Guest users **can only get access to records through guest user sharing rules** & the **maximum access granted is read**.
- Guest users **can't have the update or delete permissions on objects**.
- **Run Flows for Guest Users** is no longer supported.





Enabling Public Access To Your Site

Enable public access at the page level instead of the site level.

Settings

- General
- Theme
- Languages
- Navigation
- Mobile Publisher
- CMS Connect
- Advanced

General

View and edit the main properties of your site.

Site Details

Template
Customer Service

Public Access ⓘ

Guest users can see and interact with the site without logging in

Pages

Find a page...

- Home ⓘ
- Account Management
- > Action Plan Object
- > Action Plan Template Object
- > Case Object
- Contact Support

Properties

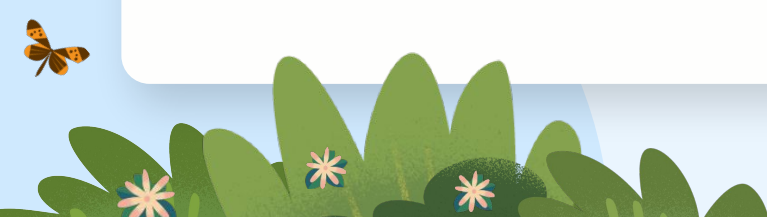
Name ⓘ
Home

URL ⓘ
/

API Name ⓘ
Home

Page Access ⓘ

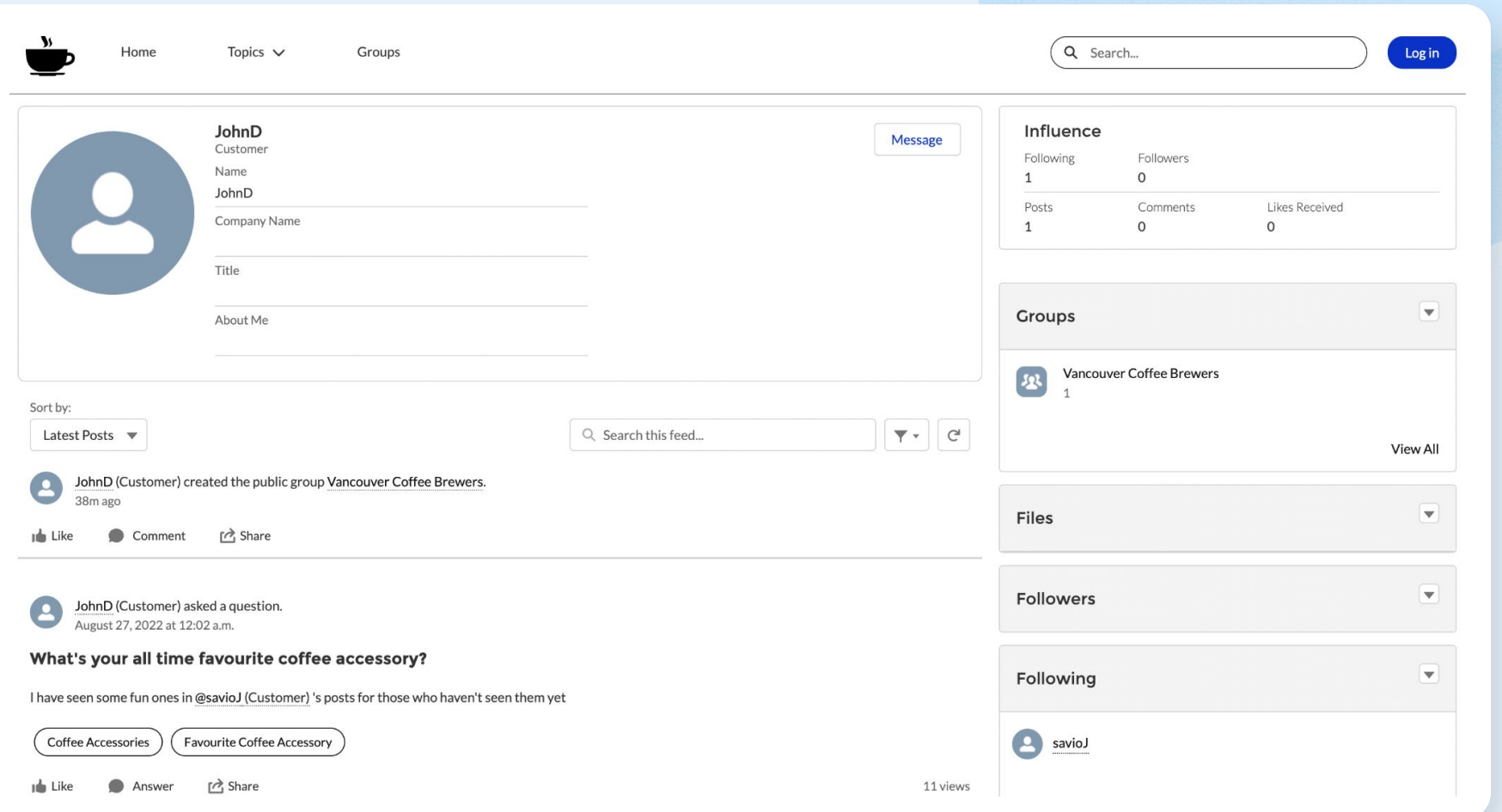
Public



Use Page/Component Audience Variations for Guest

Hide sensitive info from guest users on public pages

Does the Guest user need access to all the components in this user profiles page?



The screenshot shows a Salesforce user profile for 'JohnD' (Customer). The profile includes a profile picture, a 'Message' button, and fields for Name, Company Name, Title, and About Me. Below the profile is a feed of posts. The first post is 'JohnD (Customer) created the public group Vancouver Coffee Brewers.' with options to Like, Comment, and Share. The second post is 'JohnD (Customer) asked a question.' with the text 'What's your all time favourite coffee accessory?' and a question body 'I have seen some fun ones in @savioJ (Customer) 's posts for those who haven't seen them yet'. There are two tags: 'Coffee Accessories' and 'Favourite Coffee Accessory'. The post has options to Like, Answer, and Share, and shows '11 views'. On the right side, there is an 'Influence' section with a table showing 'Following: 1', 'Followers: 0', 'Posts: 1', 'Comments: 0', and 'Likes Received: 0'. Below that are sections for 'Groups' (Vancouver Coffee Brewers), 'Files', 'Followers', and 'Following' (savioJ).

Following	Followers
1	0

Posts	Comments	Likes Received
1	0	0

Rule 3

Define and Secure Personally Identifiable Information(PII)



Enhanced Personal Information Management



Hide PII fields from External users

- If PII fields are present on user profile pages they will display as blank for other users
 - Name fields will be replaced by Nickname

Caveats

- This setting isn't enforced in Apex
- PII fields on other objects require custom handling

The screenshot shows the Salesforce Object Manager interface for the 'User' object. The breadcrumb trail is 'SETUP > OBJECT MANAGER'. The main heading is 'User'. On the left, a navigation menu lists various configuration options: Details, Fields & Relationships, User Page Layouts, User Profile Page Layouts, Community Member Page Layouts, Lightning Record Pages, Buttons and Links, Compact Layouts, **Field Sets** (highlighted), and Object Limits. The main content area is titled 'PersonalInfo_EPIM' and contains a 'Field Set Properties' dialog. This dialog has 'Save', 'Cancel', 'Undo', and 'Redo' buttons. Below the buttons is a list of fields for the 'User' object: Account ID, Contact ID, Created By ID, Individual ID, Last Modified By ID, Manager ID, and Profile ID. To the right of this list is a 'Quick Find' search box containing 'User Name' and a table with the following content:

About Me	Alias
Account	Allow Fore
Active	Call Center
Admin Info Emails	Chatter Em

Below the field list, there is a prompt: 'Drag any of the fields above into the list below.' Underneath this is a section titled 'In the Field Set' with an information icon. This section contains a list of fields that are currently in the field set: Email Sender Name, Street, Zip/Postal Code, Email, First Name, and Fax.

Rule 4

Know & Review Your Global & Individual Site Settings



Digital Experience Settings

Global Settings for All Sites

- Recommended default state of these settings are the most secure.

Allow users to see contacts that have not been enabled for partner or customer accounts

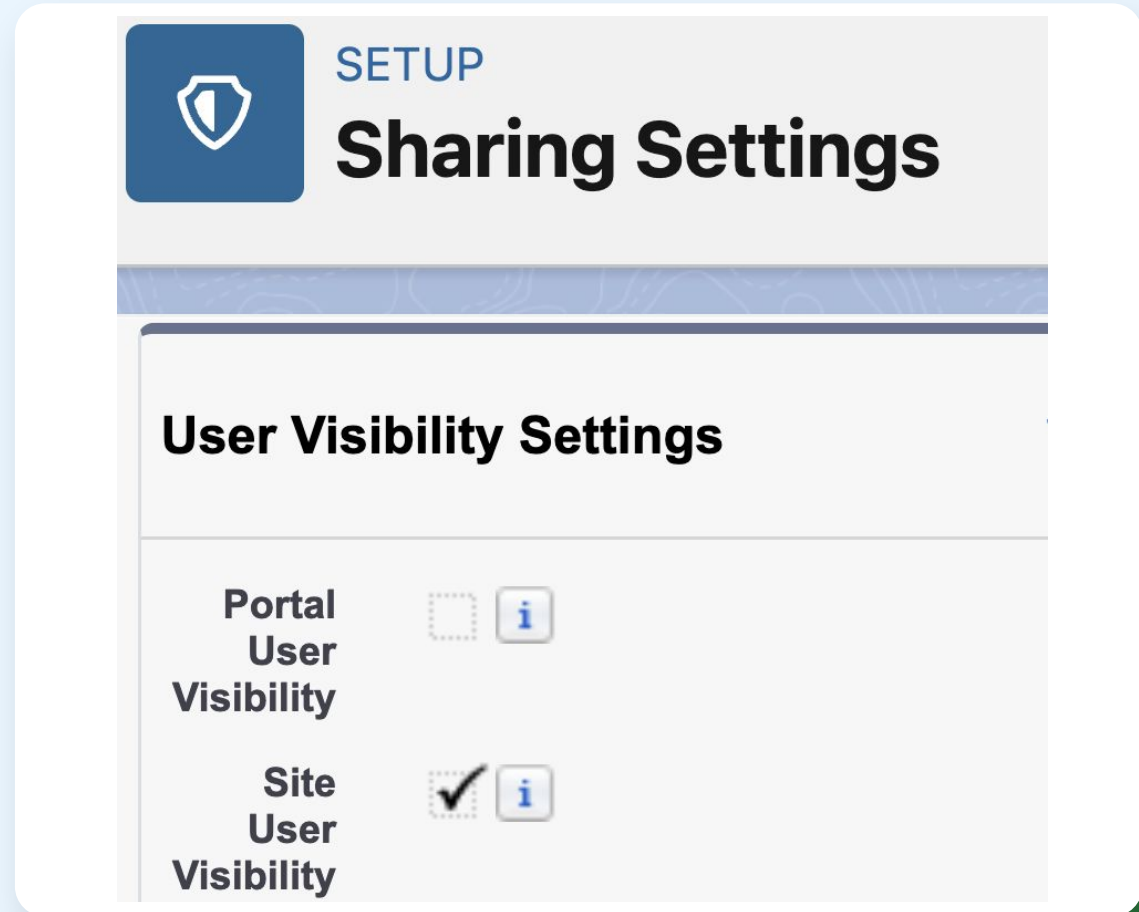
Allow using standard external profiles for self-registration, user creation, and login

Hide badges from guest users in Experience Builder sites

User Visibility Settings

Global Settings for All Sites under Sharing Settings

- Portal User Visibility
- Site User Visibility



The screenshot shows the 'Sharing Settings' page in Salesforce Setup. At the top, there is a shield icon and the text 'SETUP Sharing Settings'. Below this, the section 'User Visibility Settings' is highlighted. It contains two rows of settings:

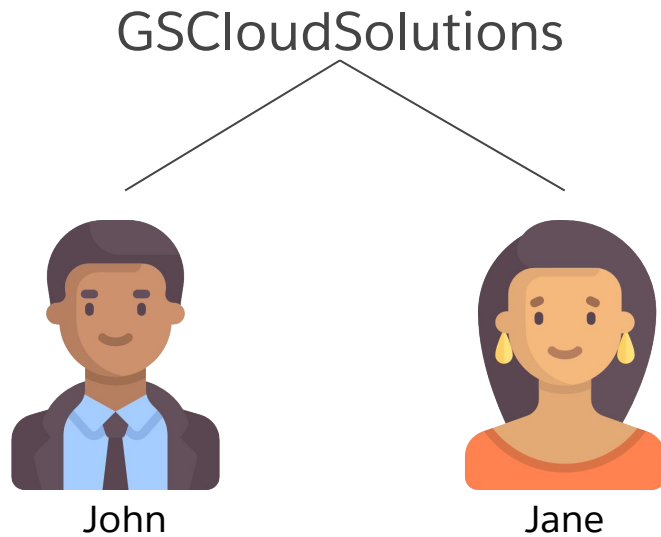
Setting	Value	Info
Portal User Visibility	<input type="checkbox"/>	i
Site User Visibility	<input checked="" type="checkbox"/>	i

Portal & Site User Visibility



Portal User Visibility - Access to Users In the Same Account

Site User Visibility - Access to All Users of the Same Site



Site Preferences

Individual Site Settings

- **Authenticated User**
 - Access to view other members of the site
 - *Requires Site User Visibility Setting Enabled
- **Guest User**
 - Access to assets likes images
 - Access to chatter feeds & discussions
 - Access to view members of the site
- **Always Use Nicknames**

Preferences

General

- Show nicknames [i](#)
- Optimize images for mobile devices [i](#)
- Give guest users access to public Chatter API requests [i](#)
- Let guest users view asset files and CMS content available to the
- Enable direct messages [i](#)
- Allow discussion threads [i](#)
- See other members of this site [i](#)
- Ask your Salesforce admin to enable Site User Visibility in your or
- Let guest users see other members of this site [i](#)

Rule 5

Check for Object CRUD Access & FLS in your Apex UI Controller Methods



#5

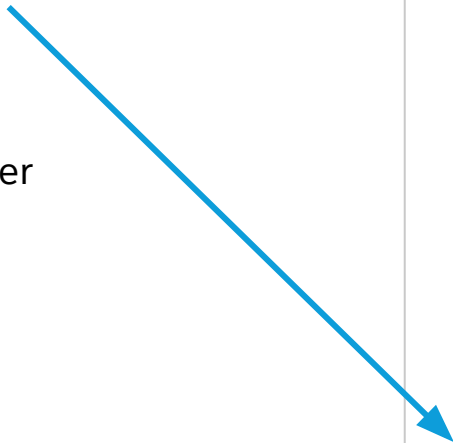
Object CRUD & FLS Check Example



Partner Member



Partner Admin



Edit User

* Name

First Name

* Last Name

* Email

Access Level

Standard

Partner Standard Access
Gives you access to all the knowledge articles and setup guides

Partner Deal Management Access
Gives you access to submit new deals, contact your Partner Admin to enable this feature.

[Request Access](#)

[Cancel](#) [Save](#)

Object CRUD & FLS Check Example



Partner Member



Partner Admin



Edit User

* Name

First Name

* Last Name

* Email

Access Level

Partner Standard Access
Gives you access to all the knowledge articles and setup guides

Partner Deal Management Access
Gives you access to submit new deals, contact your Partner Admin to enable this feature.

User Edit UI Controller

Apex Method

salesforce

@AuraEnabled

```
public static Boolean updateSiteUser(String userId, String fname,
String lname, String email, String accessLevel) {
    User u = [SELECT FirstName, LastName, Email, Access_Level__c FROM
User WHERE Id= :userId];
    u.Access_Level__c = accessLevel; //update access level
    ---update other user fields---
    update u;
}
```

Dev Tools to Inspect Network Tab for Server Calls



Network calls for @AuraEnabled methods

The screenshot shows the Chrome DevTools Network tab with the following network requests:

- data:application/x-...
- data:application/x-...
- data:application/x-...
- data:application/x-...
- data:application/x-...
- app.css?2=&aura.attributes=%7B%22authenticat...
- aura?r=0&ui-comm-runtime-components-aura-co...
- aura?r=1&aura.Component.getComponentDef=1
- hotcoffeeroundedcuponaplatefromside?v=1
- aura?r=2&aura.Component.getComponent=1&ui-...
- favicon.ico
- aura?r=3&other.User.updateSiteUser=1**
- CometdWorkerJs.js
- T
- aura?r=4&ui-instrumentation-components-beaco...

The selected request details are as follows:

Name	Headers	Payload	Preview	Response	Initiator	Timing	Cookies
		▼ Query String Parameters view source view URL-encoded r: 3 other.User.updateSiteUser: 1					
		▼ Form Data view source view URL-encoded					

The Form Data details are as follows:

- message:** {"actions": [{"id": "150;a", "descriptor": "apex://UserController/ACTION\$updateSiteUser", "callingDescriptor": "markup://c:UpdateSiteUser", "params": {"userId": "0054x000002XLS", "fname": "john", "lname": "doe", "company": "Groundswell Cloud Solutions inc.", "accessLevel": "Standard"}}]}
- aura.context:** {"mode": "PROD", "fwuid": "QPQI8lbYE8YujG6og6Dqgw", "app": "siteforce:communityApp", "loaded": {"APPLICATION@markup://siteforce:communityApp": "Zj1VcUXqZfCDWZ-Q5LxXcA"}, "dn": [], "globals": {}, "uad": false}}
- aura.pageURI:** /s/userprofile
- aura.token:** eyJub25jZSI6ImJxUXhMwMjpdmoz0EVnTDgxVUMwb1Z6TUVLREx50HBq0xDei1kMmtcdTAwM2QwLmVlcXZfCDWZ-Q5LxXcA



API Payload Exposes your Method Signature

UpdateSiteUser Apex Method

```
message: {"actions": [{"id": "165;a", "descriptor": "apex://UserController/ACTION$updateSiteUser", "callingDescriptor": "UNKNOWN", "params": {"userId": "0054x000002XLSD", "fname": "john", "lname": "doe", "email": "john.doe@gsccloudsolutions.com", "accessLevel": "Standard"}}]}
```

```
aura.context: {"mode": "PROD", "fwuid": "QPQi8lbYE8YujG6og6Dqgw", "app": "siteforce:communityApp", "loaded": {"APPLICATION@markup://siteforce:communityApp": "Zj1VcUXqZfCDWZ-Q5LxXcA", "COMPONENT@markup://instrumentation:o11yCoreCollector": "8089lZkrpgraL8-V8KZXNw"}, "dn": [], "globals": {}, "uad": false}
```

aura.pageURI: /s/userprofile

```
aura.token: eyJub25jZSI6ImxUHBMEk1WVlXSGZDdFZDZVDJyUGFwdEpUQjZlZSVo2ZXl3R2N2aUt1S1VcdTAwM2QiLCJ0eXAI0iJKV1QiLCJhbGciOiJIUzI1NiIsImtpZCI6IntcInRcIjpcIjAwRDR4MDAwMDAwR3lYWVwiLFw
```

Manipulating Payload to Gain Elevated Access

Http POST Request with Postman



POST https://df22-demo.my.site.com/s/sfsites/aura Send

Params Authorization Headers (10) Body Pre-request Script Tests Cookies Code

none form-data x-www-form-urlencoded raw binary GraphQL BETA

	KEY	VALUE	DESCRIPTION
<input checked="" type="checkbox"/>	message	{"actions":[{"id":"150;a","descriptor":"apex://UserController/A...	
<input checked="" type="checkbox"/>	aura.context	{"mode":"PROD","fwuid":"QPQi8IbYE8YujG6og6Dqgw","app":"...	
<input checked="" type="checkbox"/>	aura.pageURI	/s/userprofile	
<input checked="" type="checkbox"/>	aura.token	eyJub25jZSI6ImJxUXhMWMmJpdmozOEVnTDgxVUMwb1Z6TUVL...	
	Key	Value	Description

Body Cookies (7) Headers (17) Test Results Status: 200 OK Time: 422 ms Size: 1.57 KB Save

Pretty Raw Preview JSON ≡

```
1 {
2   "actions": [
3     {
4       "id": "150;a",
5       "state": "SUCCESS",
6       "returnValue": true,
```

Enforcing Object and Field Permissions



- Filter SOQL Queries Using WITH SECURITY_ENFORCED
- Security.stripInaccessible() Method
- Enforce User Mode for Database Operations (Beta)

```
1 Account acc = new Account(Name='test');  
2 insert as user acc;
```

- Schema.DescribeSObjectResult isAccessible, isCreateable, or isUpdateable Methods



Rule 6

Data Accessible via the User Interface & API should be Consistent



Data Access via UI & API Example

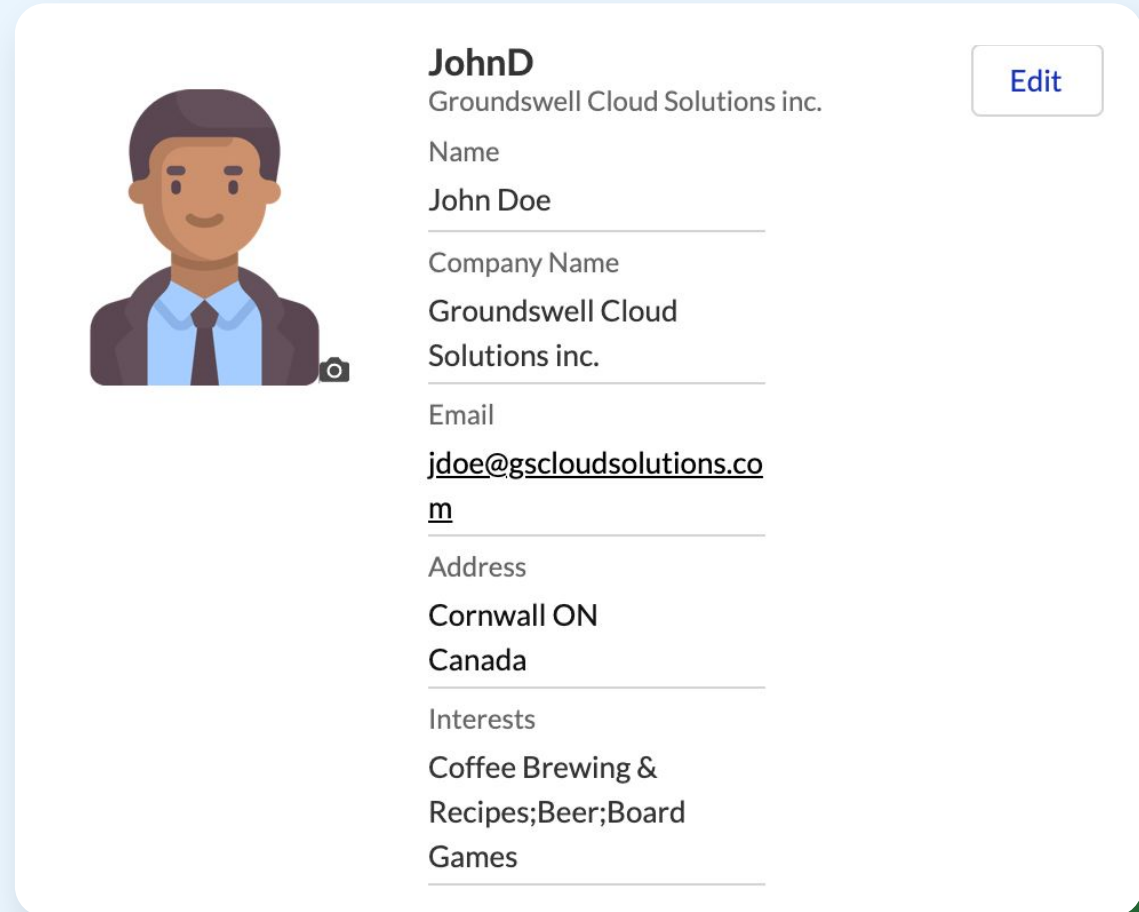


Requirement


Integration with Marketing Cloud

Implementation

- Added PII User Fields to the EPIM fieldset
- Provided Edit Access to the Contact Fields
- Enforced CRUD & FLS Checks in the Apex User Trigger
- No Site Page Exposes the Contact Record.



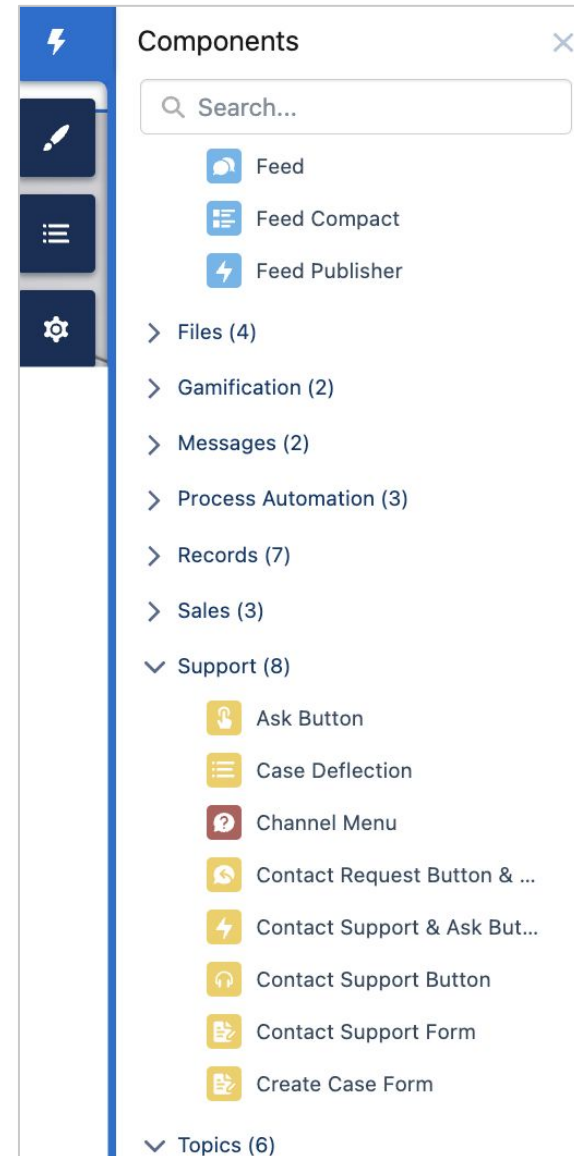
The image shows a user profile card for John Doe. On the left is a placeholder icon of a man in a suit. To the right, the name 'JohnD' is displayed in bold, followed by the company name 'Groundswell Cloud Solutions inc.' and an 'Edit' button. Below this, several fields are listed with their values: Name (John Doe), Company Name (Groundswell Cloud Solutions inc.), Email (jdoe@gscloudsolutions.com), Address (Cornwall ON, Canada), and Interests (Coffee Brewing & Recipes; Beer; Board Games).

	JohnD Groundswell Cloud Solutions inc. Edit
	Name John Doe
	Company Name Groundswell Cloud Solutions inc.
	Email jdoe@gscloudsolutions.com
	Address Cornwall ON Canada
	Interests Coffee Brewing & Recipes; Beer; Board Games

What Could Go Wrong?

- OOB Lightning Components use native Salesforce APIs such as the UI API to fetch data.
- They strictly comply with Object CRUD, FLS & Record Visibility granted to the Running User

salesforce



Accessing Data via Native Salesforce APIs



POST ▼ https://df22-demo.my.site.com/s/sfsites/aura Send ▼

KEY	VALUE	DESCRIPTION
<input checked="" type="checkbox"/> message	{ "actions":	
<input checked="" type="checkbox"/> aura.context	[{"id": "5007;a", "descriptor": "serviceComponent:	
<input checked="" type="checkbox"/> aura.pageURI	//ui.search.components.forcesearch.scopedres	
<input checked="" type="checkbox"/> aura.token	ultsdataprotider.ScopedResultsDataProviderCo	
	ntroller/ACTION\$getLookuptems", "callingDescr	
	iptor": "UNKNOWN", "params":	
	"scope": "Contact", "term": "*doe" "pageSize": 20,	
Key	"currentPage": 1, "sortBy": "", "enableRowActions":	Description
	false, "source": "", "field": "", "recordId": "", "additionalFields": ["Interests__c", "Groups__c",	
Body	Last_Website_Activity__c"], "dependentFieldBindi	ms Size: 2.17 KB Save
Cookies (7)	ngs": {}, "useADS": false}]}	
Headers (17)		
Test Results		
Pretty		
Raw		
Preview		
JSON		

```
21 "Email": "savio@gscloudsolutions.com",
22 "FirstName": "John",
23 "Last_Website_Activity__c": "Created Private Group - Vancouver Coffee Bre
24 "Name": "John Doe",
25 "SystemModstamp": "2022-09-02T23:11:59.000Z",
26 "OwnerId": "0054x000002WS0SAAW",
27 "Groups__c": "Coffee Accessories;Vancouver Coffee Brewers",
28 "CreatedDate": "2022-08-26T19:34:26.000Z",
29 "LastName": "Doe",
30 "Id": "0034x00001DRqMLAAL",
31 "LastModifiedById": "0054x000002WS0SAAW",
32 "Interests__c": "Coffee Brewing & Recipes;Beer;Board Games",
33 "subjectType": "Contact"
```



Rule 7

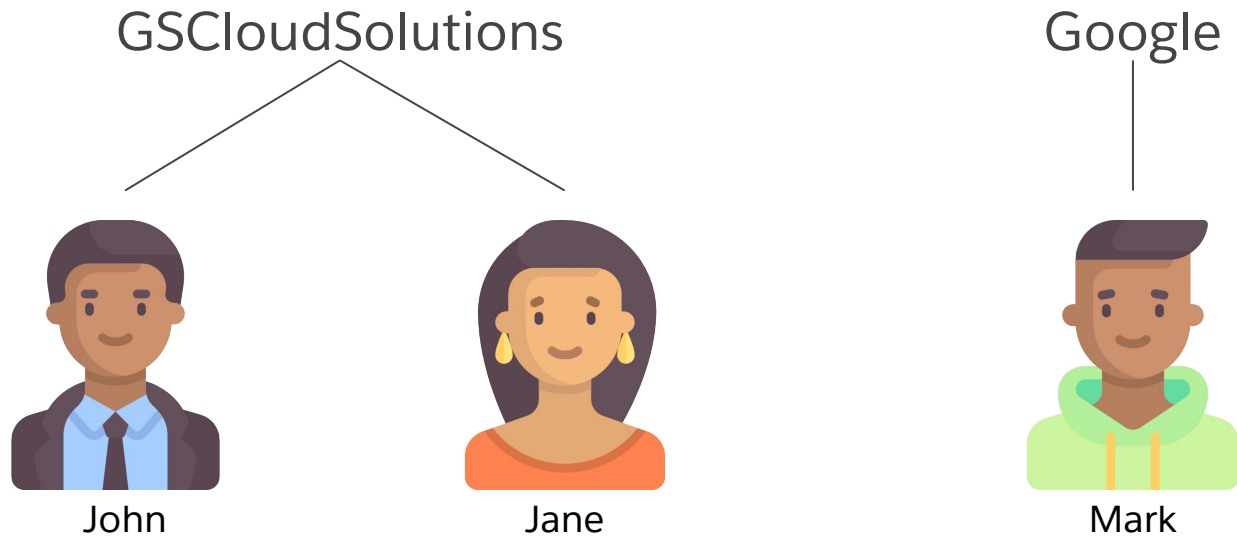
Review the Impact of Implicit Sharing



Site or Portal Implicit Sharing

Provides access to a site or portal account and all associated contacts for all site or portal users under that account.

**Shared to the lowest role under the site or portal account*



Data Access via Implicit Sharing



POST https://df22-demo.my.site.com/s/sfsites/aura Send

none form-data x-www-form-urlencoded raw binary GraphQL BETA

KEY	VALUE	DESCRIPTION
<input checked="" type="checkbox"/> message	<pre>{ "actions": [{ "id": "5007;a", "descriptor": "serviceComponent://ui.search.components.forcesearch.scopedresultsdataprovider.ScopedResultsDataProviderController/ACTIION\$getLookuptems", "callingDescriptor": "UNKNOWN", "params": { "scope": "Contact", "term": "*doe", "pageSize": 20, "currentPage": 1, "sortBy": "", "enableRowActions": false, "source": "", "field": "", "recordId": "", "additionalFields": [], "dependentFieldBindings": {}, "useADS": false } }] }</pre>	
<input checked="" type="checkbox"/> aura.context		
<input checked="" type="checkbox"/> aura.pageURI		
<input checked="" type="checkbox"/> aura.token		
Key		Description

Body Cookies (6) Headers (17) Test Results Status: 200 OK Time: 1879 ms Size: 2.35 KB Save

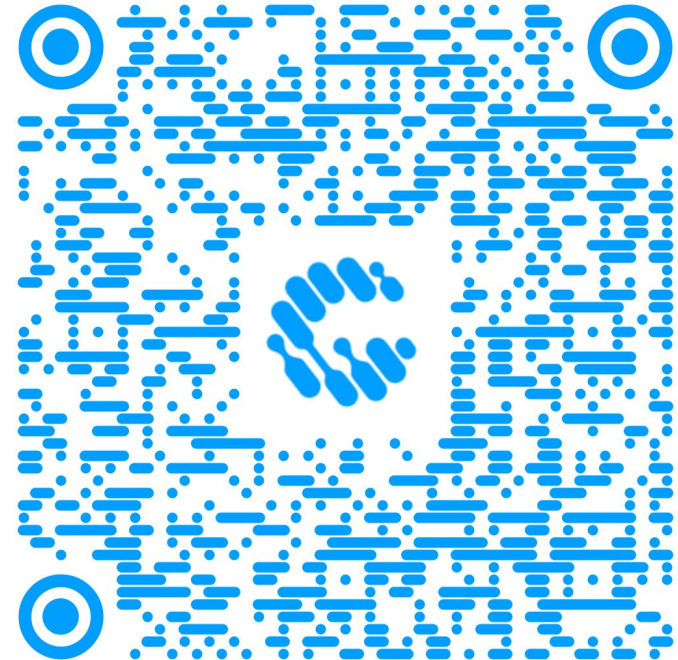
Pretty Raw Preview JSON ≡

```
33  "record": {
34    "LastModifiedDate": "2022-08-27T00:17:49.000Z",
35    "Owner": null,
36    "Email": "savio+jane@gsccloudsolutions.com",
37    "OwnerId": "0054x000002WS0SAAW",
38    "FirstName": "Jane",
39    "CreatedDate": "2022-08-26T19:34:53.000Z",
40    "LastName": "Doe",
41    "Id": "0034x00001DRqMvAAL",
42    "LastModifiedById": "0054x000002WS0SAAW",
43    "Name": "Jane Doe",
44    "SystemModstamp": "2022-08-27T00:17:49.000Z",
45    "subjectType": "Contact"
```



Where Do You Go From Here?

- Access to Experience Cloud Data Security Rule book
 - Additional rules on Clickjack Protection & CSP Level for Sites, External Sharing, etc.
 - Use this as a frame of reference to validate the security posture of your site
- Trailhead Modules for Web Application Security
 - [Learn Secure Development Best Practices](#)
 - [Develop Secure Web Apps](#)
- Follow the latest security risks & trends
 - [OWASP Top Ten](#)



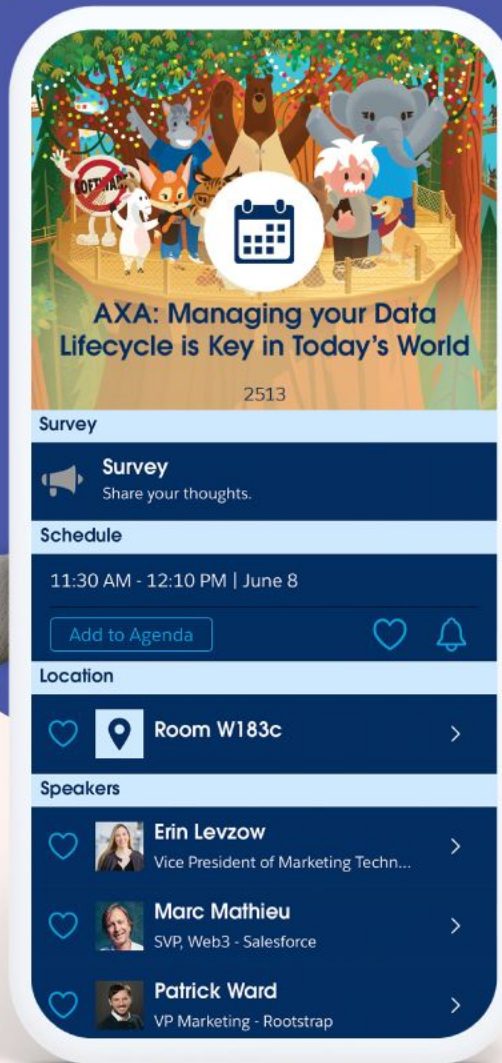
Keeping your data secure
is a joint effort between
You and Salesforce!





Share your feedback.

Provide your feedback on this session in the Salesforce Events mobile app and help make our content even better.



#DF22

Groundsweller's at Dreamforce



We're all wearing "G" pins so come say hello!



Leonardo Berardino
Principal Developer

*Presenting: Open-Source
Mocking Framework
Based on Apex Stub API
12 pm today!*



Cameron Reid
Emerging Technologies
Lead

*Presented: Diagramming
for the Admin*



Pei Huang
CTO

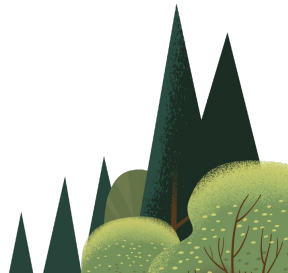
*Presenting: Named
Credentials: Securing &
Simplifying API Callouts
3 pm today!*



Gerauld Rivera
Marketing Cloud
Product Lead



Colin Hamilton
Field Service
Product Lead



Thank you

