dreamforce | GROUNDSWELL CLOUD SOLUTIONS a GyanSys company

Best Practices for Data Security in Experience Cloud

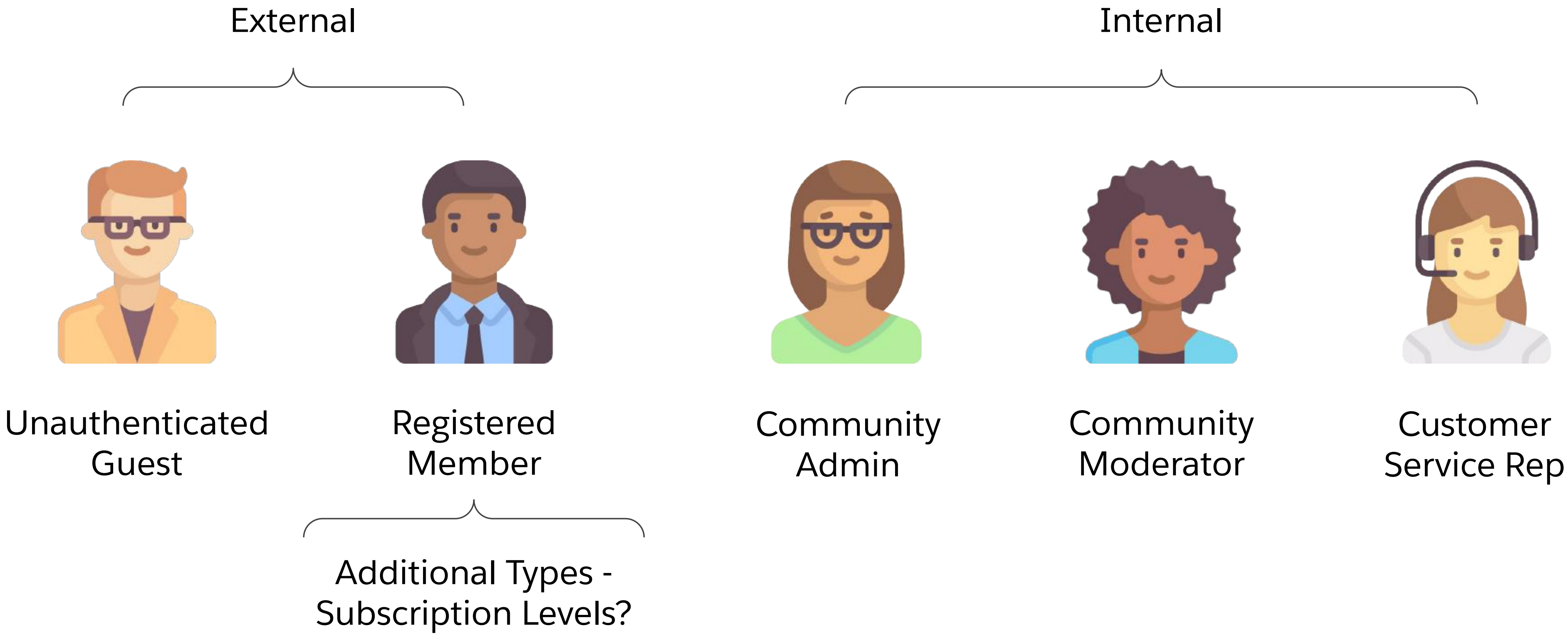
Savio Jose, Product Practice Manager
savio@gscloudsolutions.com

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	● Chatter Access ● Knowledge Article Access

Rule 2

Scrutinize Unauthenticated Guest User Access

Guest User Security Policies

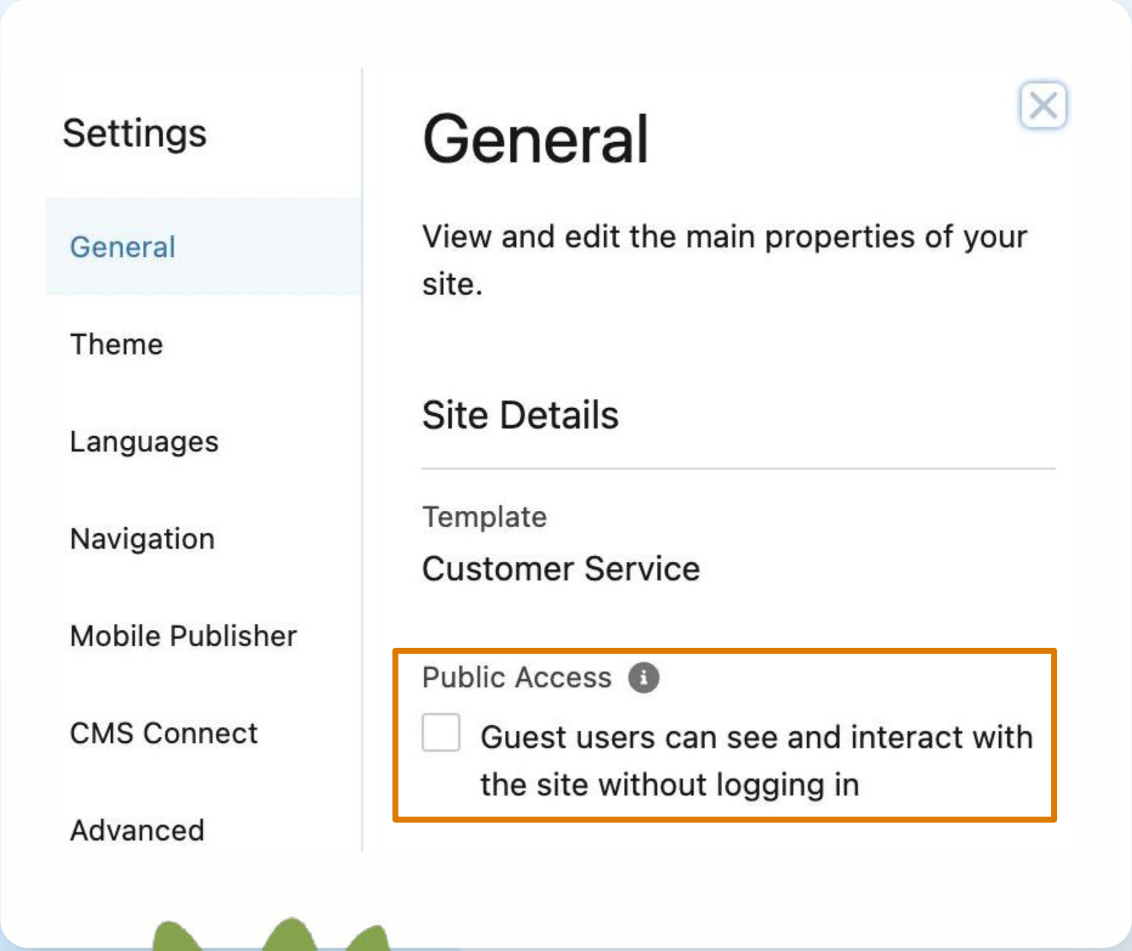
Enabled since Summer 20’ Release

- 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.

Salesforce Doc Reference for Guest User Policy Updates & Improvements

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

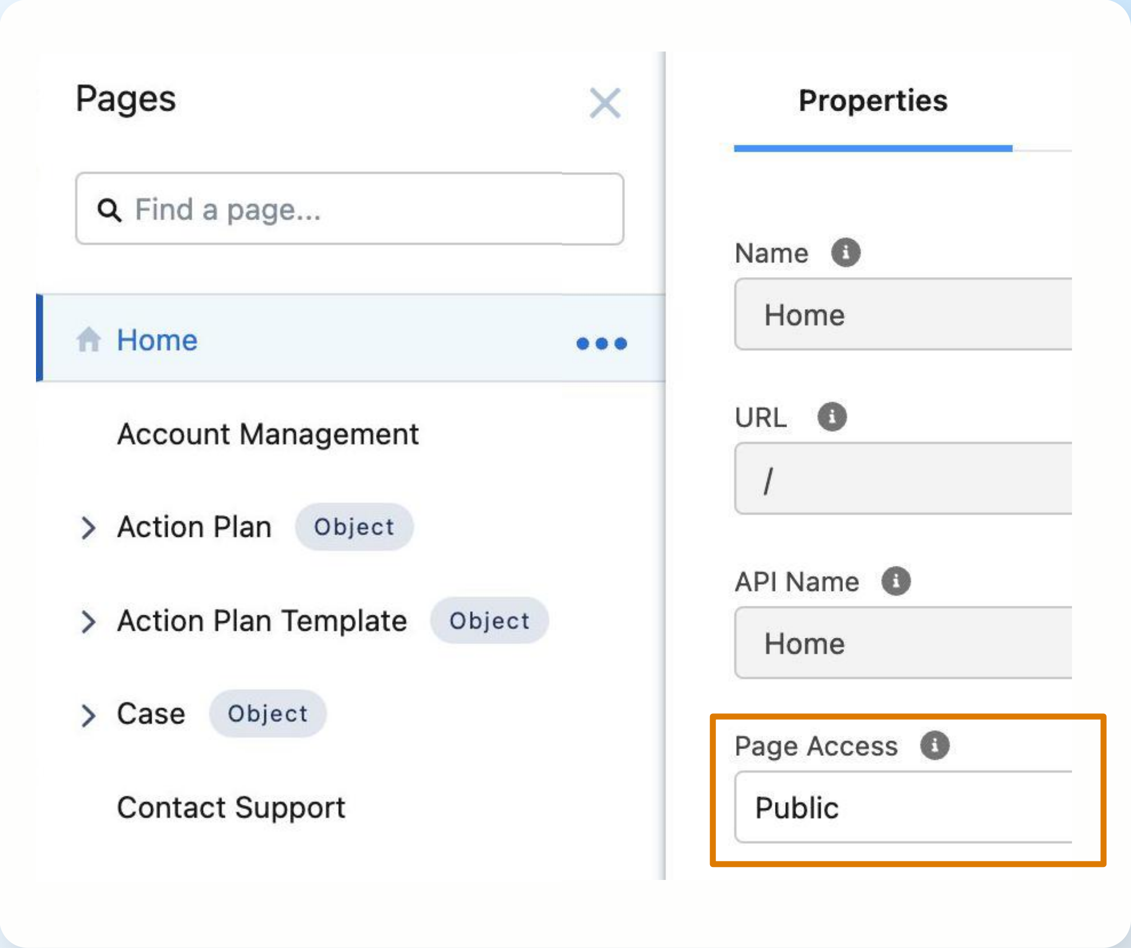
General

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: /

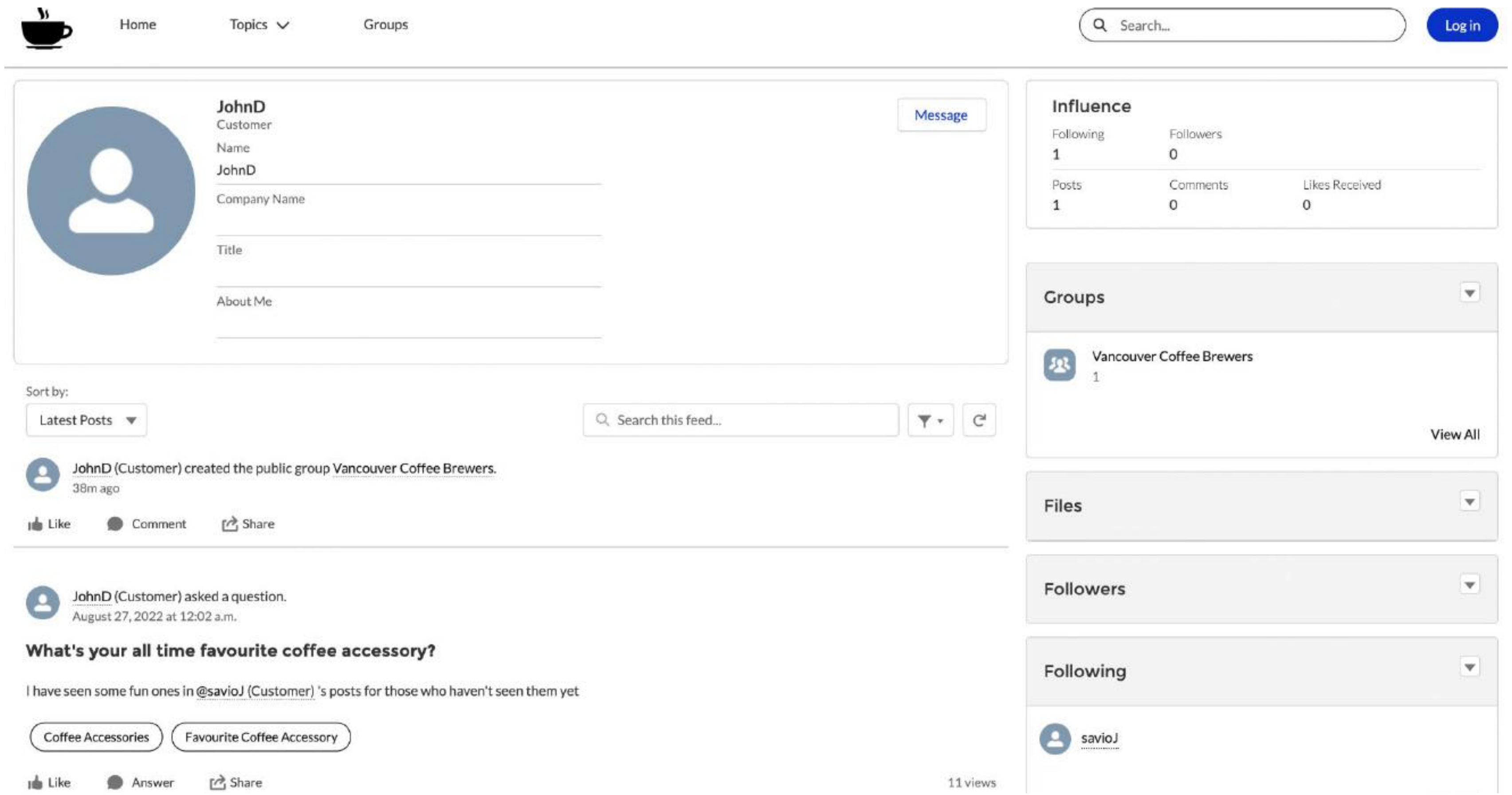
API Name: Home

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?



JohnD
Customer
Name
JohnD
Company Name
Title
About Me

Influence

Following	Followers	
1	0	
Posts	Comments	Likes Received
1	0	0

Groups

Vancouver Coffee Brewers
1

Following

savioJ

JohnD (Customer) created the public group Vancouver Coffee Brewers.
38m ago

JohnD (Customer) asked a question.
August 27, 2022 at 12:02 a.m.

What's your all time favourite coffee accessory?

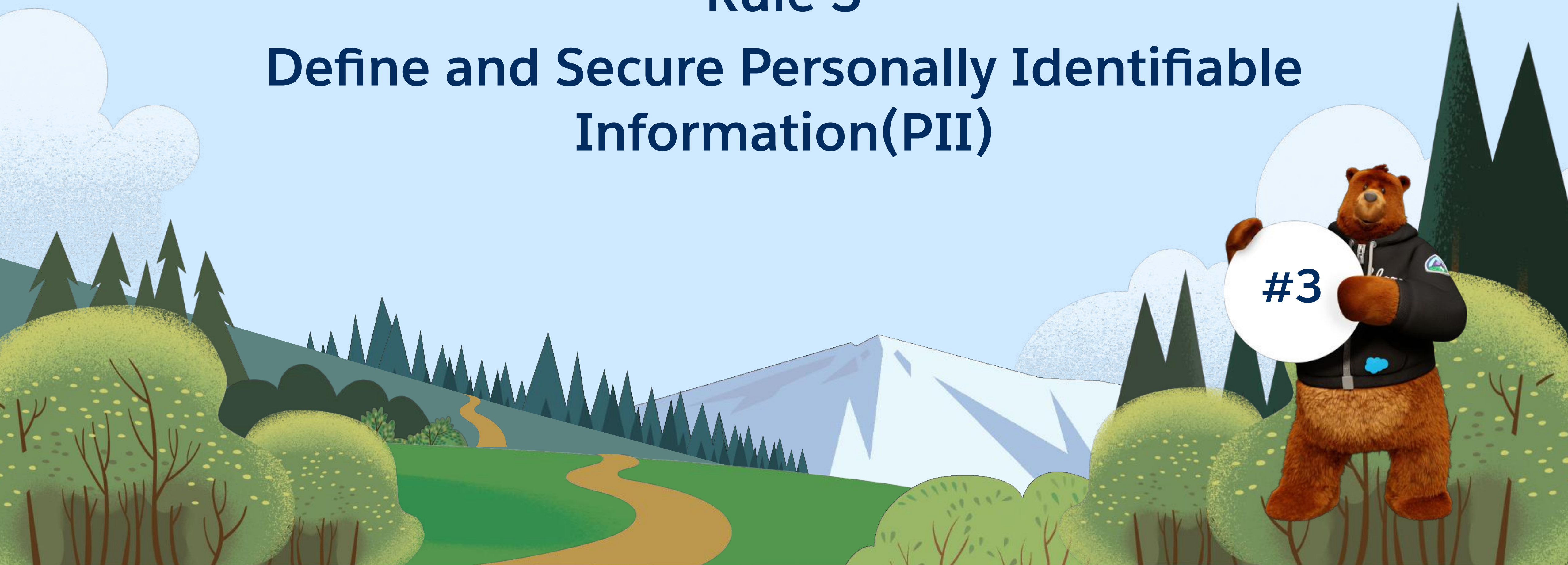
I have seen some fun ones in @savioJ (Customer) 's posts for those who haven't seen them yet

Coffee Accessories | Favourite Coffee Accessory

11 views

Rule 3

Define and Secure Personally Identifiable Information(PII)



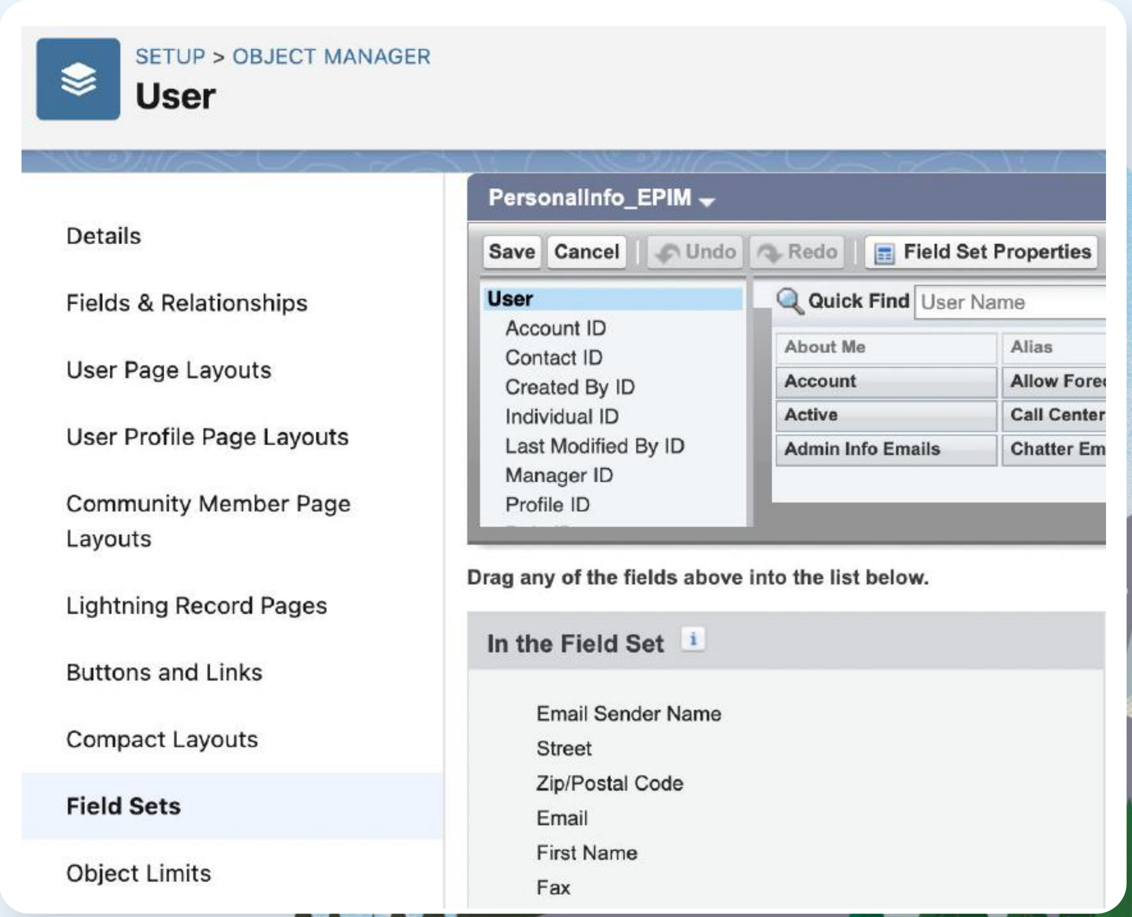
Enhanced Personal Information Management

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



SETUP > OBJECT MANAGER

User

PersonalInfo_EPIM

Drag any of the fields above into the list below.

In the Field Set

Email Sender Name
Street
Zip/Postal Code
Email
First Name
Fax

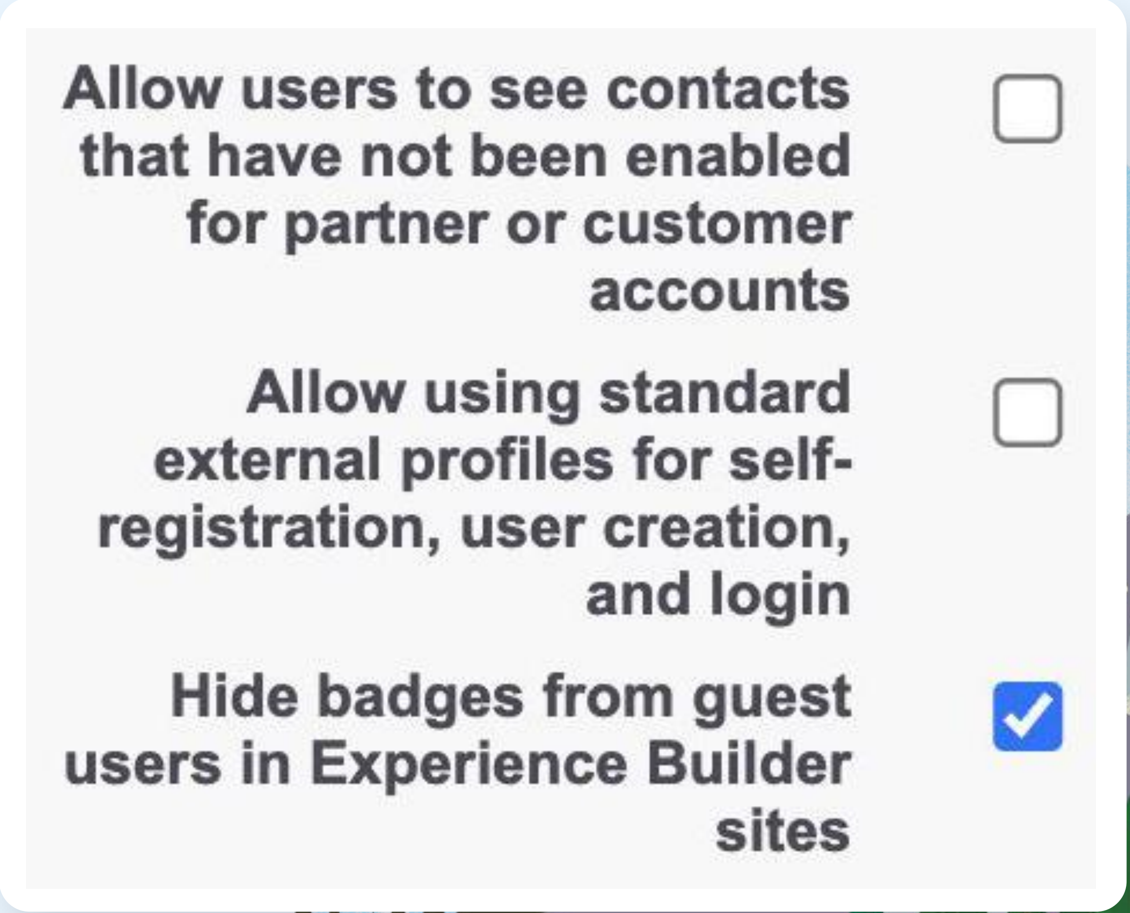
Rule 4

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 □

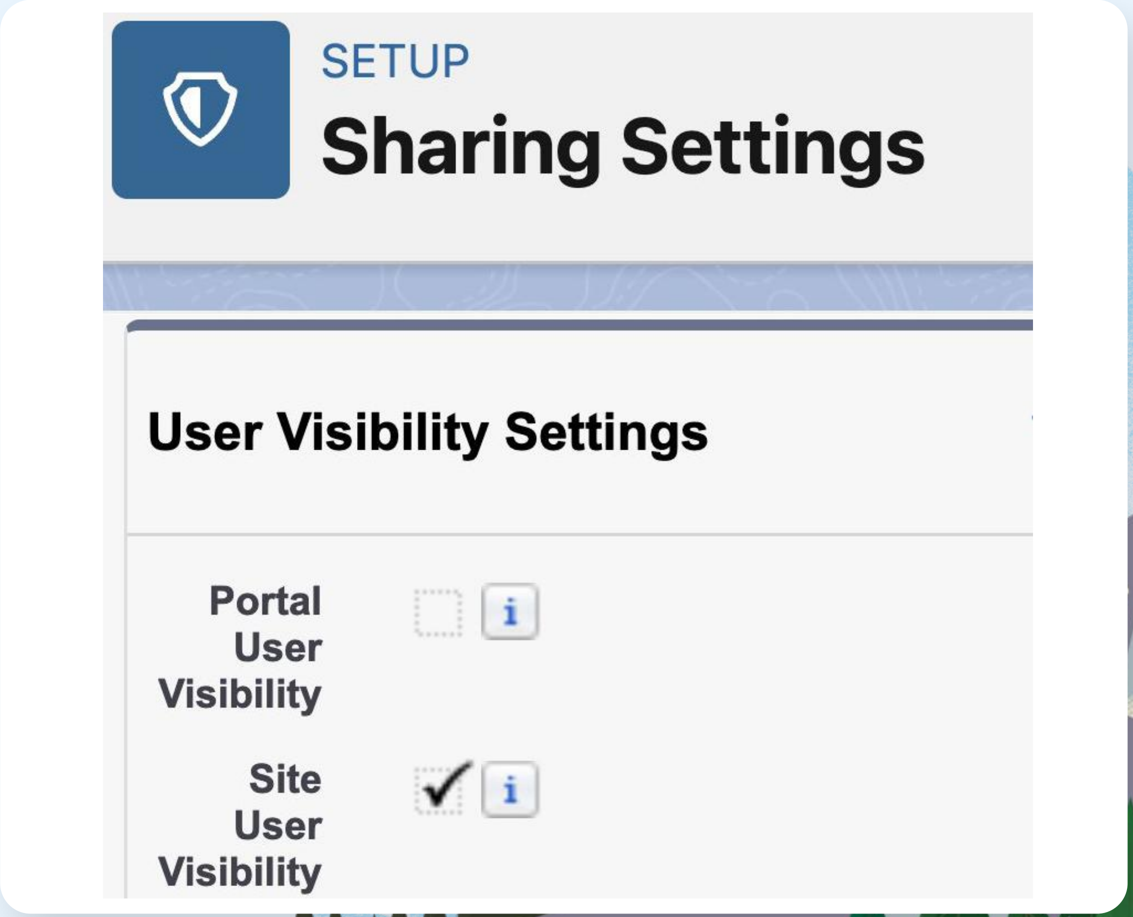
Allow using standard external profiles for self-registration, user creation, and login □

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



SETUP

Sharing Settings

User Visibility Settings

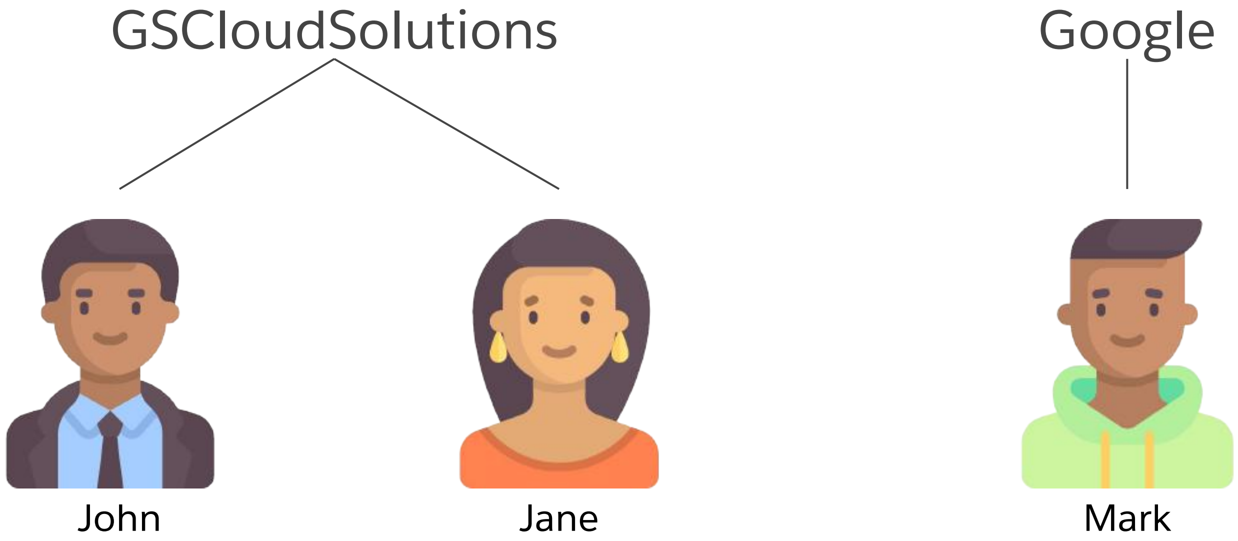
Portal User Visibility □

Site User Visibility ☑

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



GSCloudSolutions

John

Jane

Google

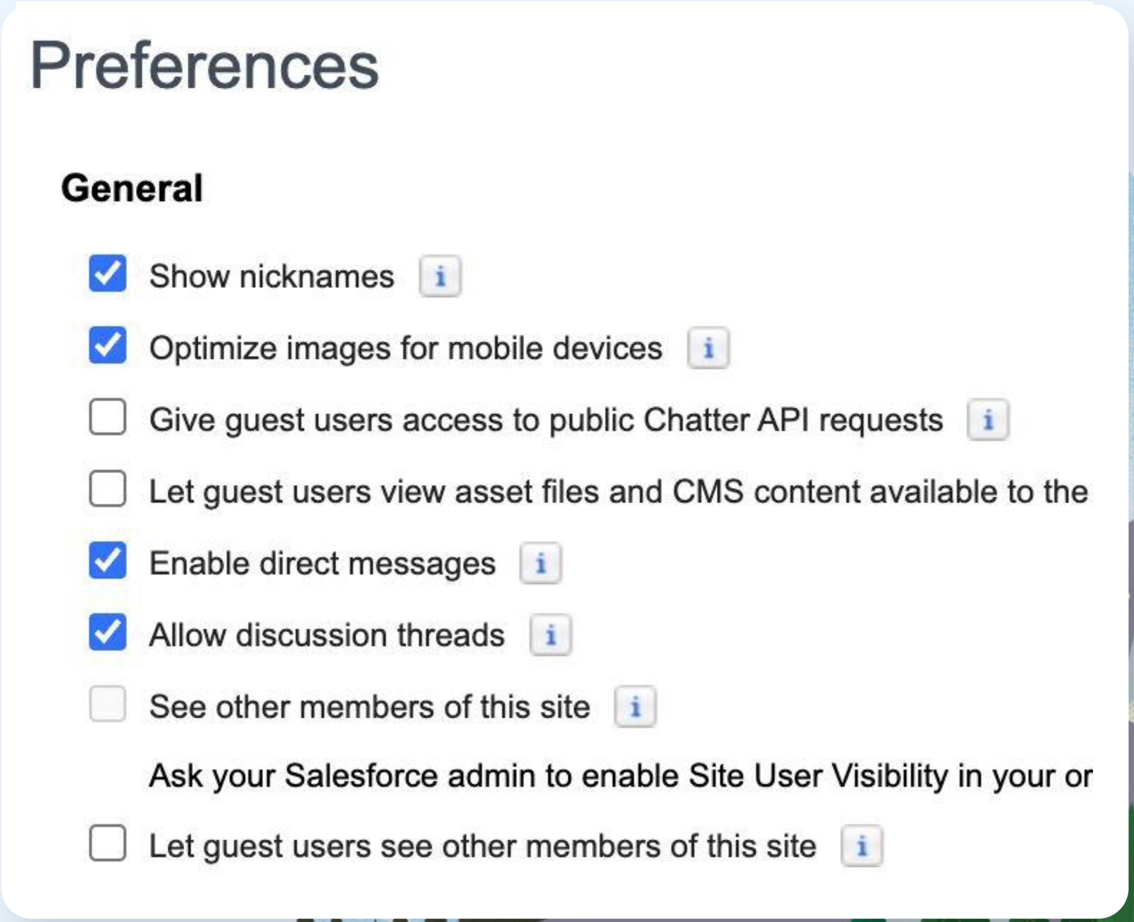
Mark

Salesforce Doc Reference

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

☑ Optimize images for mobile devices

□ Give guest users access to public Chatter API requests

□ Let guest users view asset files and CMS content available to the

☑ Enable direct messages

☑ Allow discussion threads

□ See other members of this site

Ask your Salesforce admin to enable Site User Visibility in your or

□ Let guest users see other members of this site

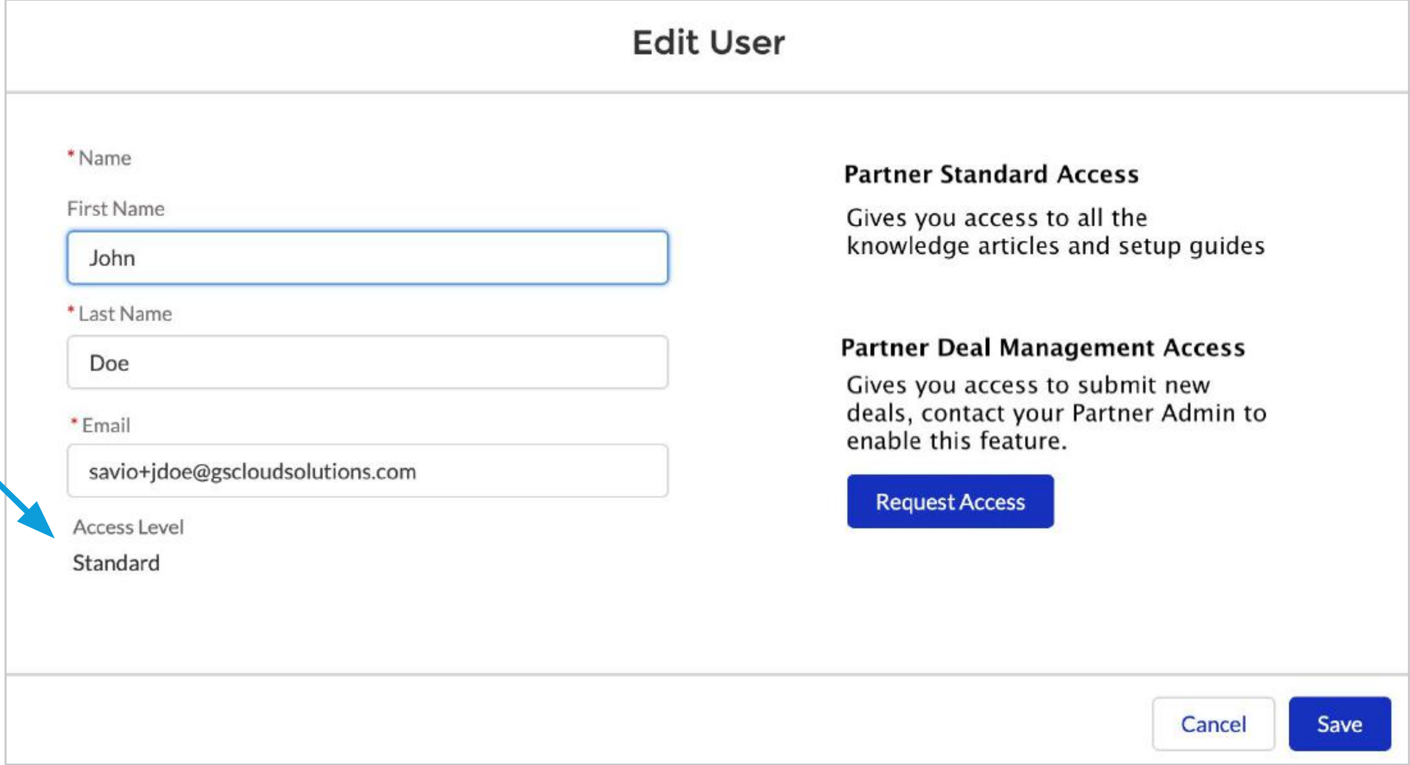
Rule 5

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

Object CRUD & FLS Check Example

Partner Member

Partner Admin



Edit User

* Name

First Name

John

* Last Name

Doe

* Email

savio+jdoe@gscloudsolutions.com

Access Level

Standard

Partner Standard Access

Gives you access to all the knowledge articles and setup guides

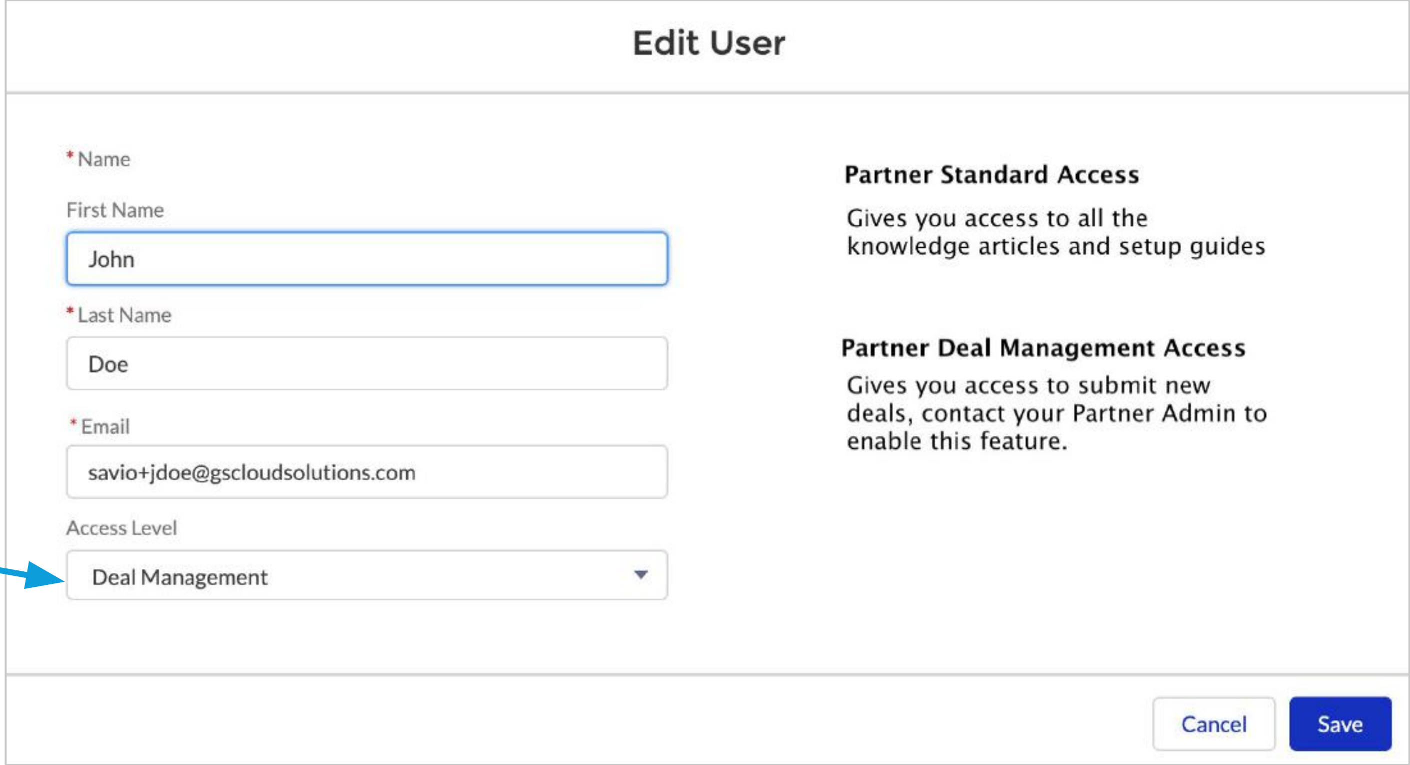
Partner Deal Management Access

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

Object CRUD & FLS Check Example

Partner Member

Partner Admin



Edit User

* Name

First Name

John

* Last Name

Doe

* Email

savio+jdoe@gscloudsolutions.com

Access Level

Deal Management

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.

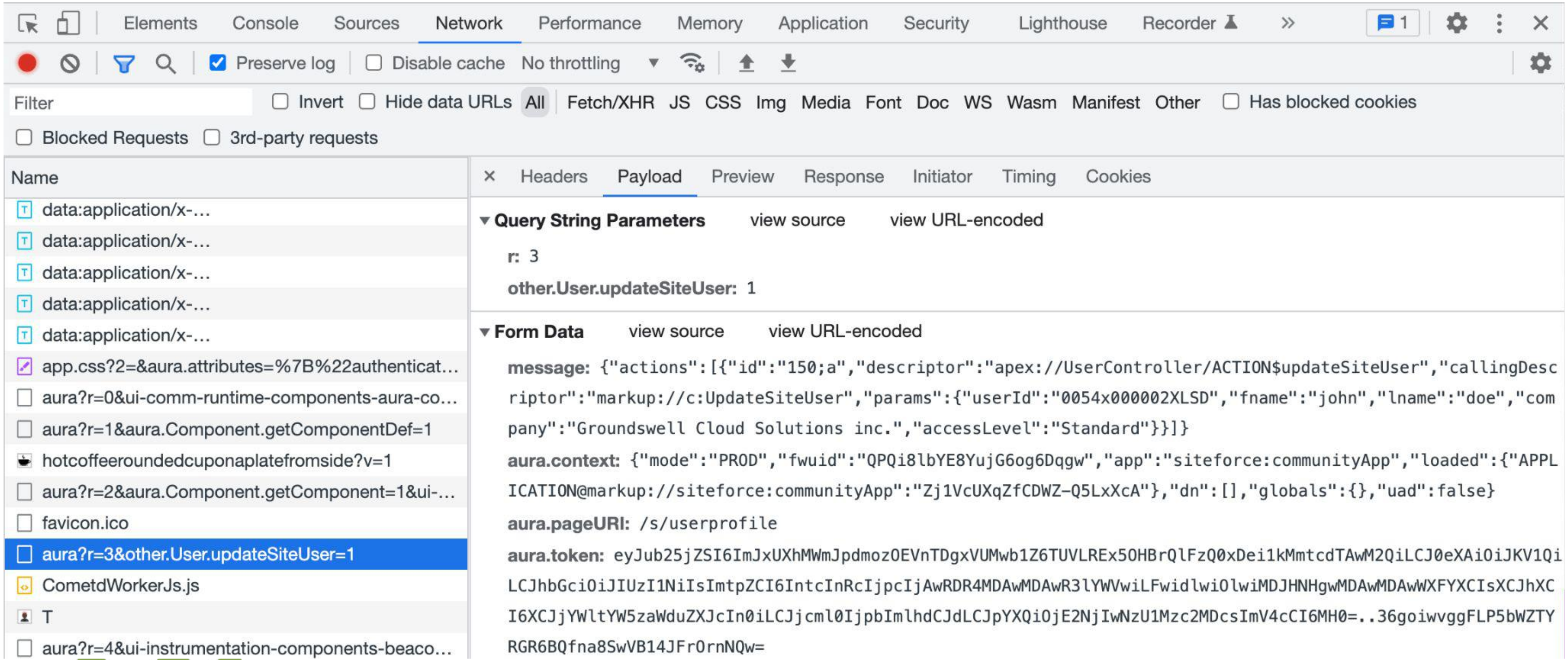
User Edit UI Controller

Apex Method

```
@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



☑ Preserve log □ Disable cache

□ Invert □ Hide data URLs All Fetch/XHR JS CSS Img Media Font Doc WS Wasm Manifest Other □ Has blocked cookies

□ Blocked Requests □ 3rd-party requests

Name

- 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…

Query String Parameters

r: 3

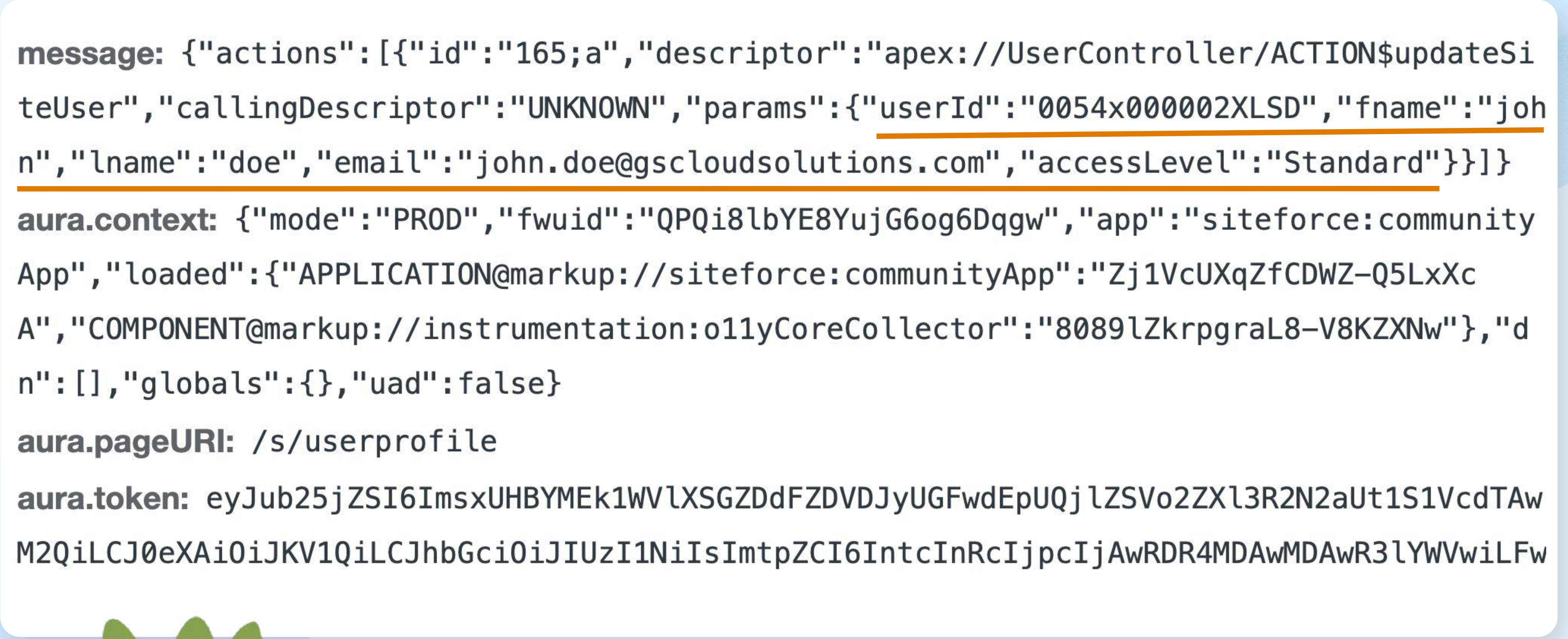
other.User.updateSiteUser: 1

Form Data

```
message: {"actions":[{"id":"150;a","descriptor":"apex://UserController/ACTION$updateSiteUser","callingDescriptor":"markup://c:UpdateSiteUser","params":{"userId":"0054x000002XLSD","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: eyJub25jZSI6ImJxUXhMWmJpdmozOEVnTDgxVUMwb1Z6TUVLREx5OHBrQlFzQ0xDei1kMmtcdTAwM2QiLCJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiIsImtpZCI6IntcInRcIjpcIjAwRDR4MDAwMDAwR3lYWVwiLFwidlwiOlwiMDJHNHgwMDAwMDAwWXFYXCIsXCJhXCI6XCJjYWltYW5zaWduZXJcIn0iLCJjcml0IjpbImlhdCJdLCJpYXQiOjE2NjIwNzU1Mzc2MDcsImV4cCI6MH0=..36goiwvggFLP5bWZTYRGR6BQfna8SwVB14JFrOrnNQw=
```

API Payload Exposes your Method Signature

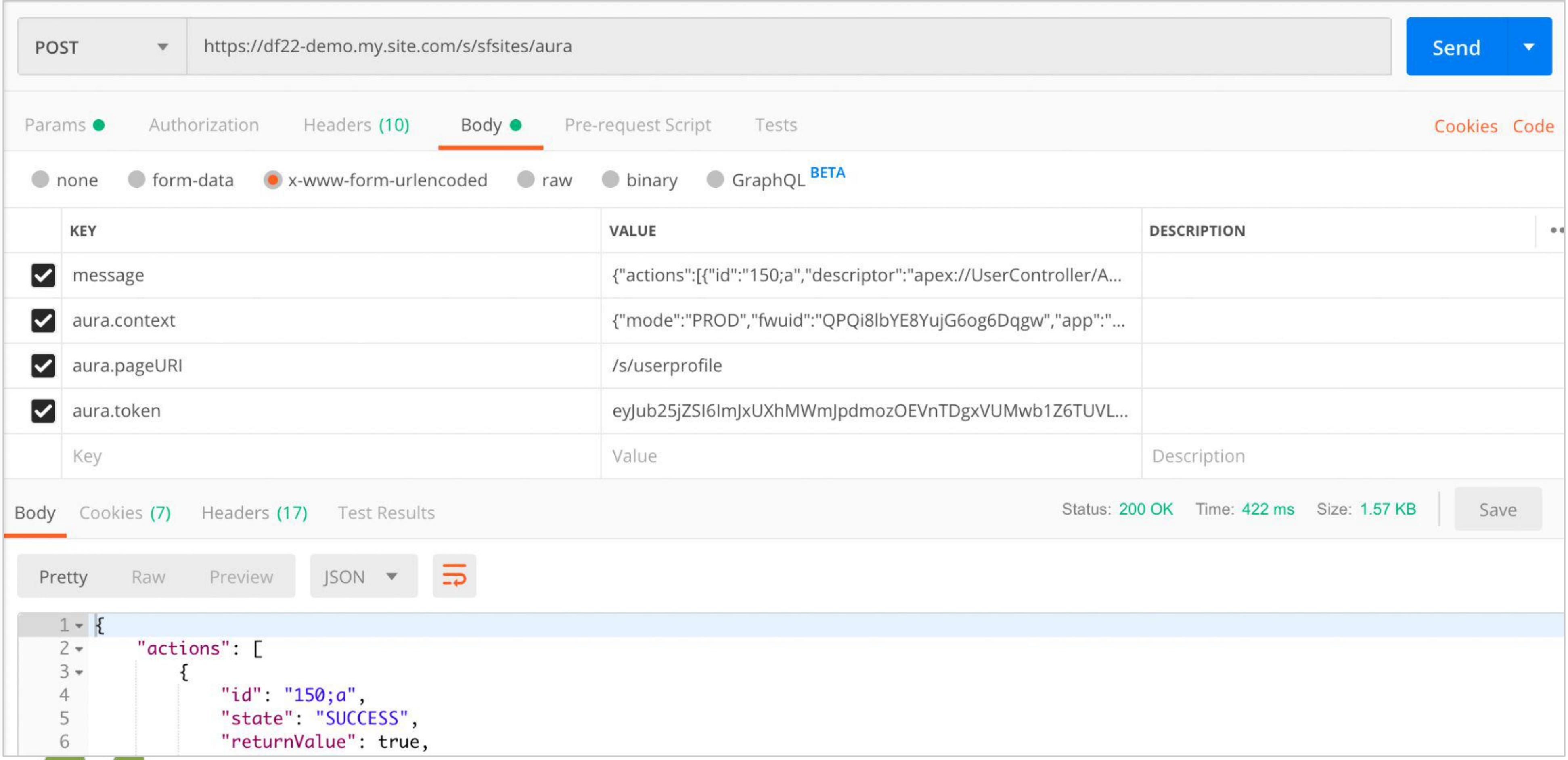
UpdateSiteUser Apex Method



```
message: {"actions":[{"id":"165;a","descriptor":"apex://UserController/ACTION$updateSi
teUser","callingDescriptor":"UNKNOWN","params":{"userId":"0054x000002XLSD","fname":"joh
n","lname":"doe","email":"john.doe@gscloudsolutions.com","accessLevel":"Standard"}}]}
aura.context: {"mode":"PROD","fwuid":"QPQi8lbYE8YujG6og6Dqgw","app":"siteforce:community
App","loaded":{"APPLICATION@markup://siteforce:communityApp":"Zj1VcUXqZfCDWZ-Q5LxXc
A","COMPONENT@markup://instrumentation:o11yCoreCollector":"8089lZkrpgraL8-V8KZXNw"},"d
n":[],"globals":{},"uad":false}
aura.pageURI: /s/userprofile
aura.token: eyJub25jZSI6ImsxUHBYMEk1WVlXSGZDdFZDVDJyUGFwdEpUQjlZSVo2ZXl3R2N2aUt1S1VcdTAw
M2QiLCJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiIsImtpZCI6IntcInRcIjpcIjAwRDR4MDAwMDAwR3lYWVwiLFw
```

Manipulating Payload to Gain Elevated Access

Http POST Request with Postman



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

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

	KEY	VALUE	DESCRIPTION
☑	message	{"actions":[{"id":"150;a","descriptor":"apex://UserController/A...	
☑	aura.context	{"mode":"PROD","fwuid":"QPQi8lbYE8YujG6og6Dqgw","app":"...	
☑	aura.pageURI	/s/userprofile	
☑	aura.token	eyJub25jZSI6ImJxUXhMWmJpdmozOEVnTDgxVUMwb1Z6TUVL...	
	Key	Value	Description

Body

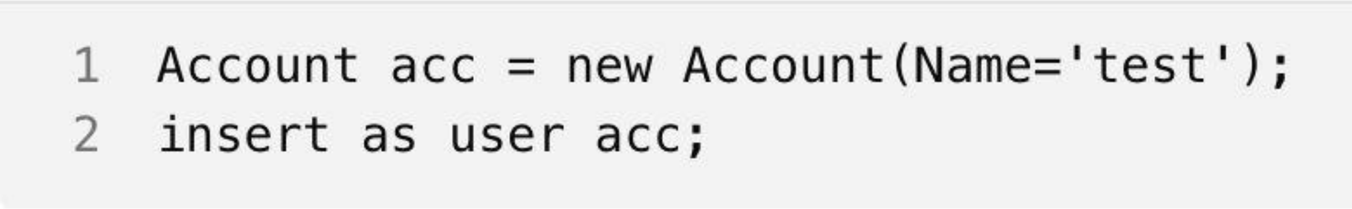
Status: 200 OK Time: 422 ms Size: 1.57 KB

JSON

```
{
    "actions": [
        {
            "id": "150;a",
            "state": "SUCCESS",
            "returnValue": true,
```

Enforcing Object and Field Permissions

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



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

- Schema.DescribeSObjectResult isAccessible, isCreateable, or isUpdateable Methods

Salesforce Doc Reference

Rule 6

Data Accessible via the User Interface & API should be Consistent

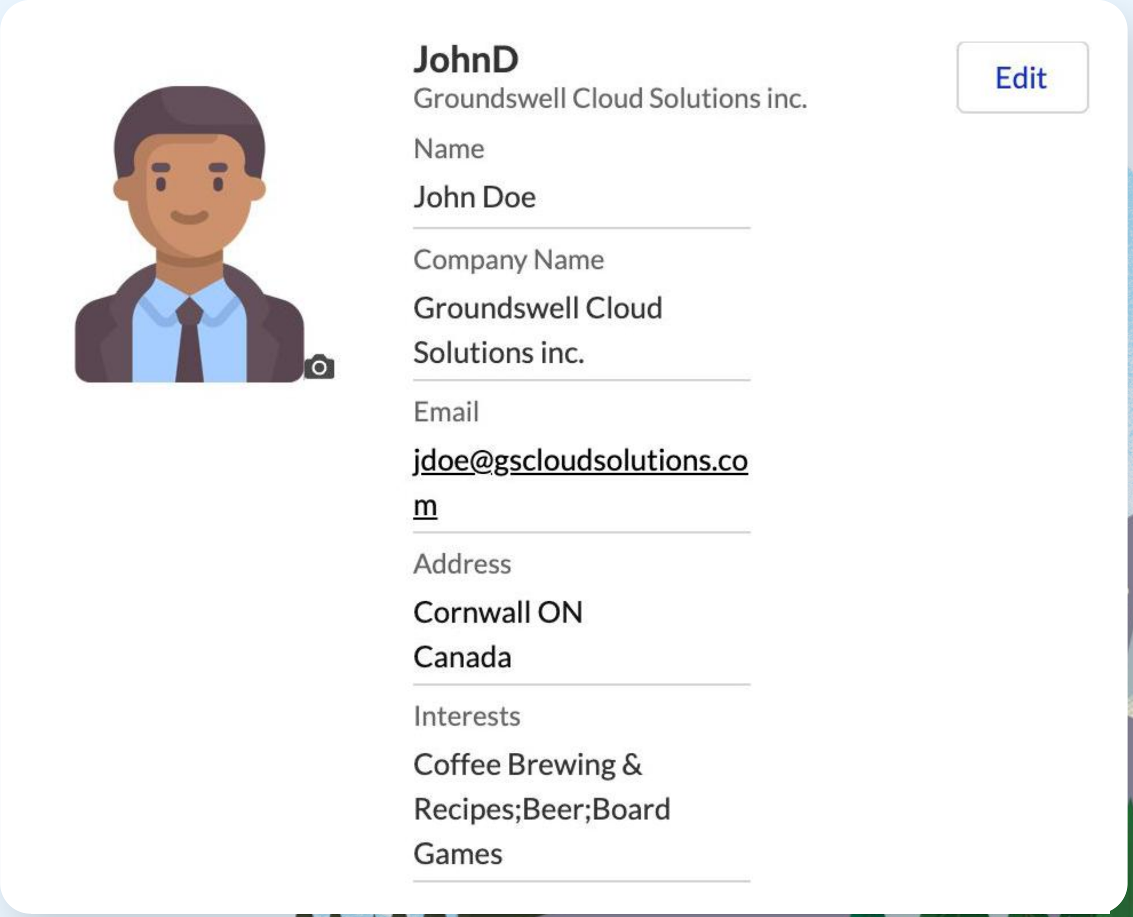
Data Access via UI & API Example

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.



JohnD
Groundswell Cloud Solutions inc.

Name
John Doe

Company Name
Groundswell Cloud Solutions inc.

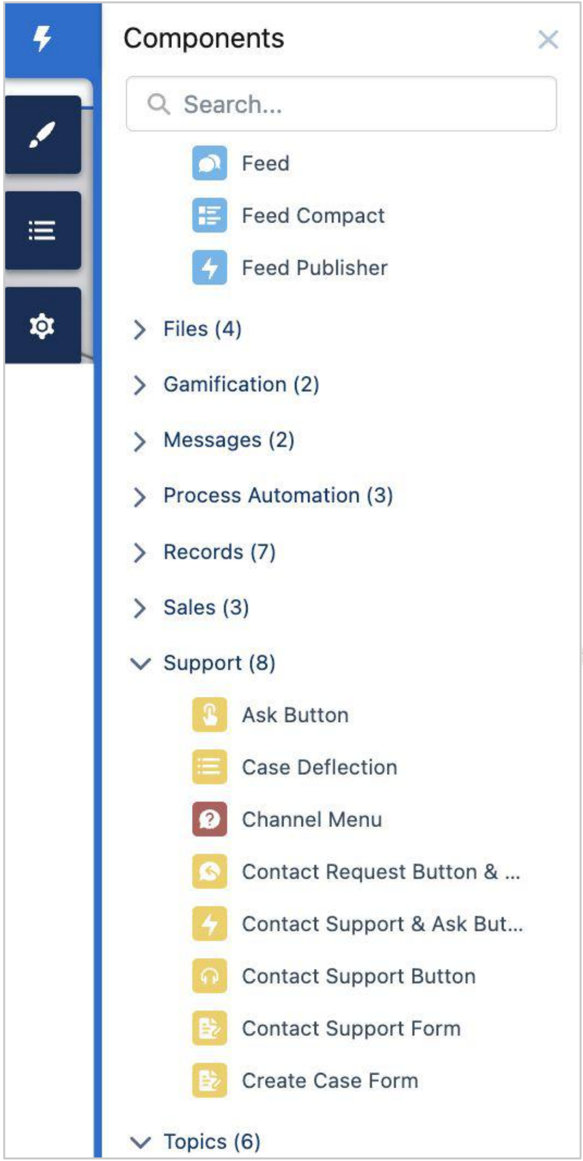
Email
jdoe@gscloudsolutions.com

Address
Cornwall ON
Canada

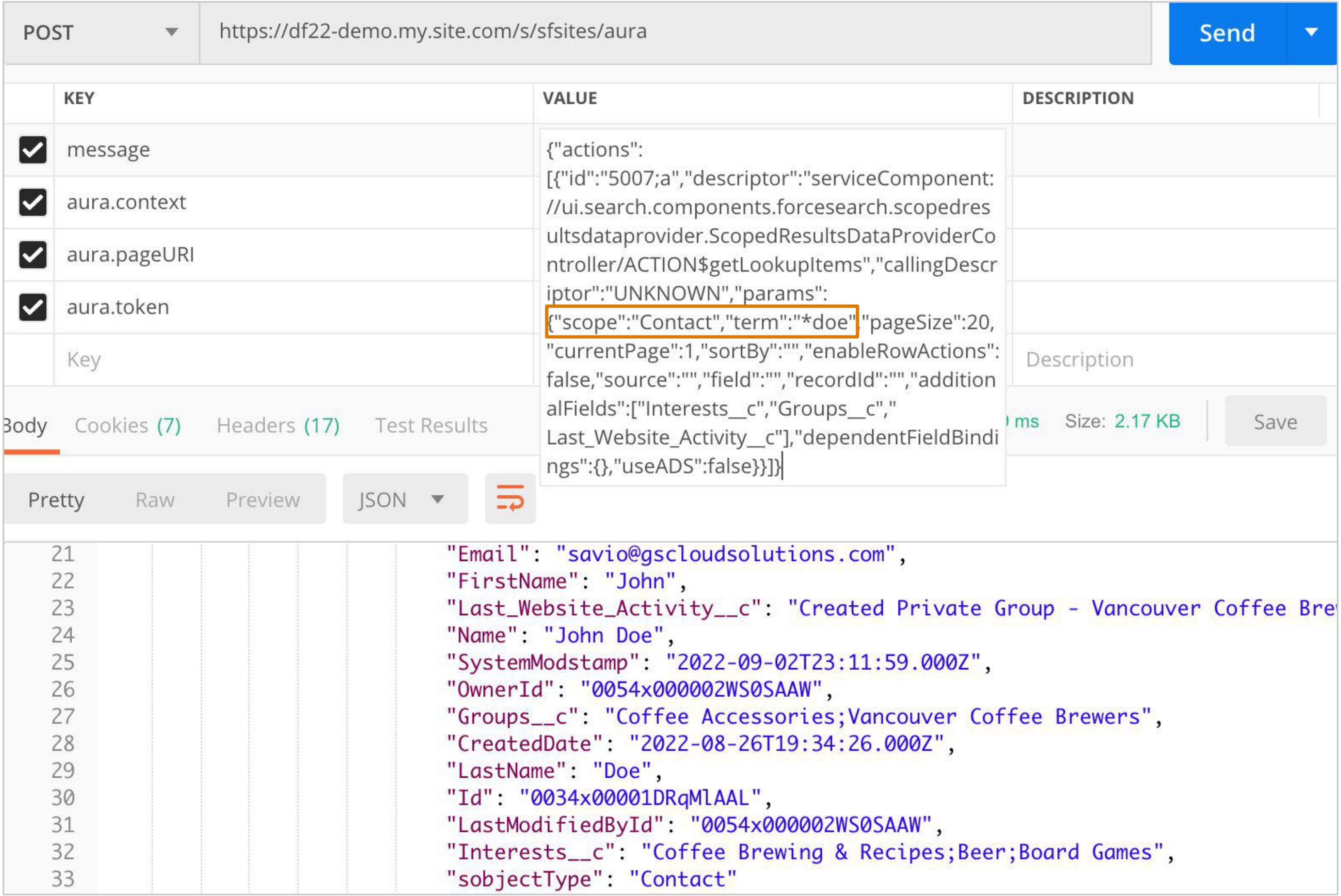
Interests
Coffee Brewing & Recipes;Beer;Board Games

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



Accessing Data via Native Salesforce APIs



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

	KEY	VALUE	DESCRIPTION
☑	message	{"actions":[{"id":"5007;a","descriptor":"serviceComponent://ui.search.components.forcesearch.scopedresultsdataprovider.ScopedResultsDataProviderController/ACTION$getLookupItems","callingDescriptor":"UNKNOWN","params":{"scope":"Contact","term":"*doe","pageSize":20,"currentPage":1,"sortBy":"","enableRowActions":false,"source":"","field":"","recordId":"","additionalFields":["Interests__c","Groups__c","Last_Website_Activity__c"],"dependentFieldBindings":{},"useADS":false}}]}	
☑	aura.context		
☑	aura.pageURI		
☑	aura.token		
	Key		Description

Body Cookies (7) Headers (17) Test Results ms Size: 2.17 KB Save

Pretty Raw Preview JSON ▾

```
"Email": "savio@gscloudsolutions.com",
"FirstName": "John",
"Last_Website_Activity__c": "Created Private Group - Vancouver Coffee Bre
"Name": "John Doe",
"SystemModstamp": "2022-09-02T23:11:59.000Z",
"OwnerId": "0054x000002WS0SAAW",
"Groups__c": "Coffee Accessories;Vancouver Coffee Brewers",
"CreatedDate": "2022-08-26T19:34:26.000Z",
"LastName": "Doe",
"Id": "0034x00001DRqMlAAL",
"LastModifiedById": "0054x000002WS0SAAW",
"Interests__c": "Coffee Brewing & Recipes;Beer;Board Games",
"sobjectType": "Contact"
```

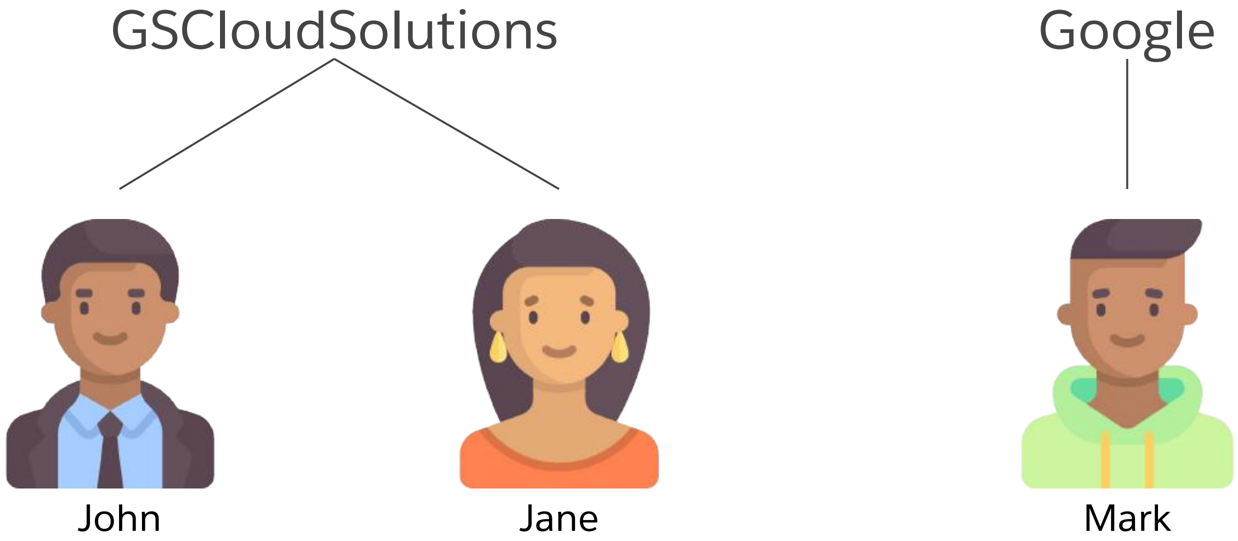
Rule 7

Review the Impact of Implicit Sharing

Site or Portal Implicit Sharing

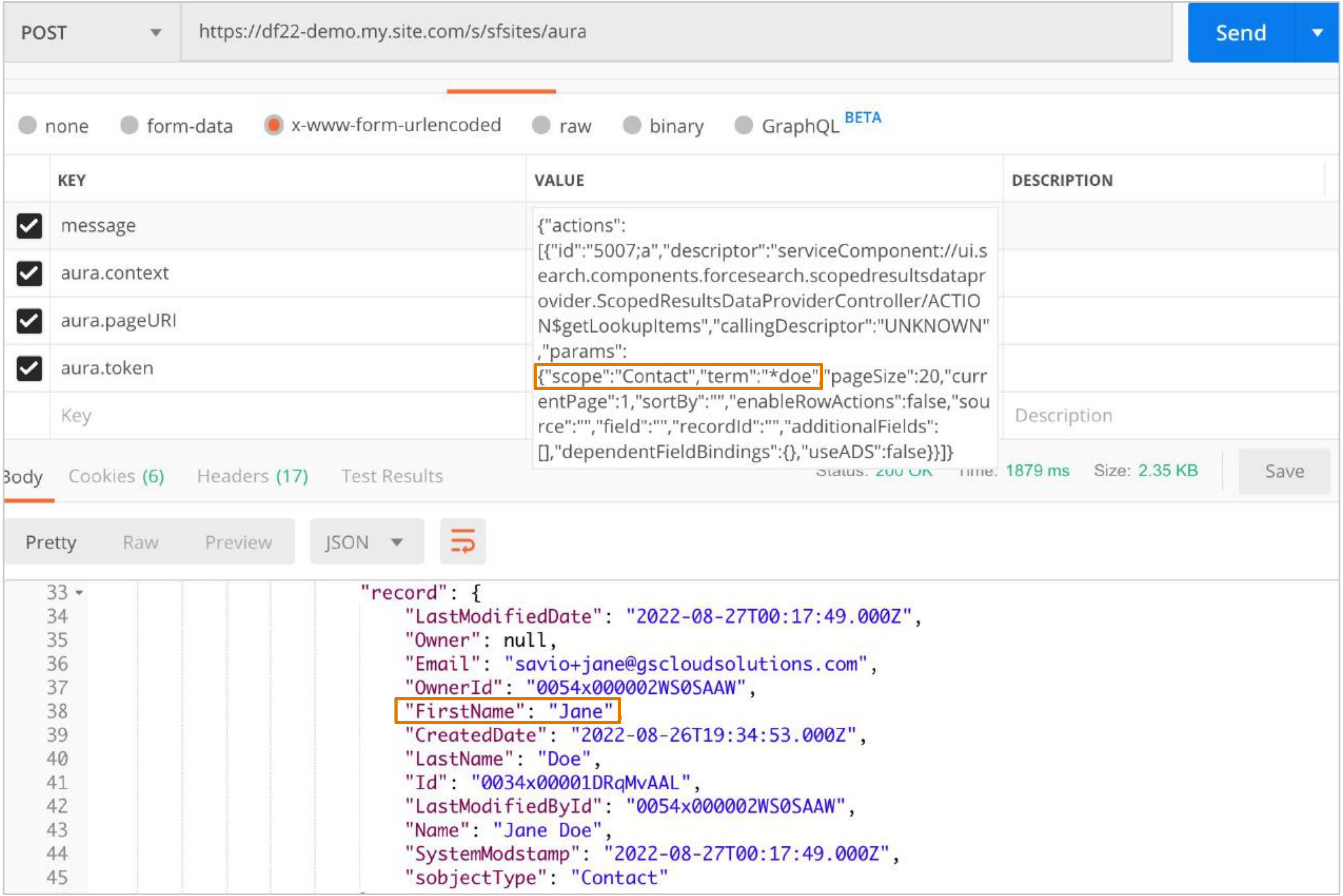
Provides access to a site or portal account and all associated contacts for all site or portal users under that account.

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



[Salesforce Doc Reference - Implicit Sharing]()

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
☑	message	{"actions":[{"id":"5007;a","descriptor":"serviceComponent://ui.search.components.forcesearch.scopedresultsdataprovider.ScopedResultsDataProviderController/ACTION$getLookupItems","callingDescriptor":"UNKNOWN","params":{"scope":"Contact","term":"*doe""pageSize":20,"currentPage":1,"sortBy":"","enableRowActions":false,"source":"","field":"","recordId":"","additionalFields":[],"dependentFieldBindings":{},"useADS":false}}]}	
☑	aura.context		
☑	aura.pageURI		
☑	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

```
                "record": {
                    "LastModifiedDate": "2022-08-27T00:17:49.000Z",
                    "Owner": null,
                    "Email": "savio+jane@gscloudsolutions.com",
                    "OwnerId": "0054x000002WS0SAAW",
                    "FirstName": "Jane"
                    "CreatedDate": "2022-08-26T19:34:53.000Z",
                    "LastName": "Doe",
                    "Id": "0034x00001DRqMvAAL",
                    "LastModifiedById": "0054x000002WS0SAAW",
                    "Name": "Jane Doe",
                    "SystemModstamp": "2022-08-27T00:17:49.000Z",
                    "sobjectType": "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

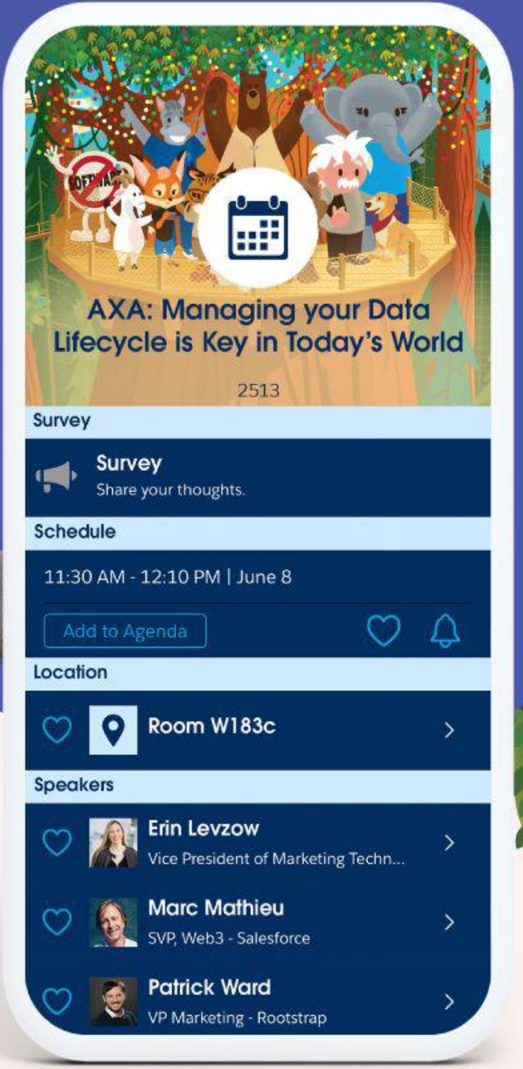
salesforce

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

dreamforce 20 Years

Share your feedback.

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



AXA: Managing your Data Lifecycle is Key in Today's World

2513

Survey

Survey
Share your thoughts.

Schedule

11:30 AM - 12:10 PM | June 8

Add to Agenda

Location

Room W183c

Speakers

Erin Levzow
Vice President of Marketing Techn...

Marc Mathieu
SVP, Web3 - Salesforce

Patrick Ward
VP Marketing - Rootstrap

#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

dreamforce

Thank you