

Data Field Access

This parameter or feature is part of our Early Adopters Program. To find out if you are eligible for participation, contact your Customer Engagement Executive by filling out a [support form](#). You can access the support page by clicking **Support** on the upper menu after logging into your [Gigya Console](#).

Description

The **Data Field Access** tab of the **Permission Groups** section of the **Admin** panel allows you to restrict access to specific fields of your schema based upon permissions of the user or group accessing them.

You can grant 5 levels of access to your schema:

- No access to any fields
- Full access to all fields
- Specific access to defined fields
 - Read-only access to specific defined fields
 - Write-only access to specific defined fields
 - Read and write access to specific defined fields

Data Field Permissions only apply to the following APIs (both REST and JS versions).

- `accounts.getAccountInfo`
- `accounts.setAccountInfo`
- `accounts.search`

Restricting Your Schema By Site

When an account contains multiple sites, the **Data Field Access** tab will display a merged view containing all fields from the schema of all sites. If you require the ability to have different access permissions for a field that uses the same name between multiple sites, be sure that you define the scope of the group in the **Scope** tab.

Permission Groups

Group: testScopedAccess2

Restricted Data Access Full Data Access

Description: restricted

Privileges **Scope** Data Field Access Members

- This group applies to all sites except those listed below
- This group applies only to the sites listed below

Update

- op-demo-gigya.herokuapp.com
- test-site-ch1
- test-site-ch2.com
- test-site-master.com

Usage

You can access the **Data Field Access** tool by logging into your [Gigya Console](#), navigating to the **Admin** tab in the header and selecting **Permission Groups** from the left-hand menu.

Admin ▾

Permission Groups

Administrators

Create Group

Applications

Permission Groups

Site Groups

Audit Log

Console SAML Login

Name	Description	Members	Settings
testScopedAccess1		0	  
testScopedAccess2	restricted	0	  
__admins		2	 

Once at the **Permission Groups** page, click the Edit



button next to the group you want to configure or create a new group by pressing **Create Group**.

All groups except **__admins** begin with having no access to any fields. To enable full access to all fields for a group, toggle the switch in the top-right of the page from **Restricted Data Access** to **Full Data Access**.

Permission Groups

Group: testScopedAccess2

Description: restricted

Restricted Data Access Full Data Access

Privileges

Scope

Data Field Access

Members

When a group has the Full Data Access toggle selected, you are not able to individually edit the permissions for any fields of your schema and you will see a notice informing you that this group has full access to all fields.

Privileges

Scope

Data Field Access

Members

Update

Field Name	Read	Write
account	<input type="checkbox"/>	<input type="checkbox"/>
committed	<input type="checkbox"/>	<input type="checkbox"/>
created	<input type="checkbox"/>	<input type="checkbox"/>
createdTimestamp	<input type="checkbox"/>	<input type="checkbox"/>
data	<input type="checkbox"/>	<input type="checkbox"/>

This group has full access to all data fields. To restrict their data access, first select "Restricted Data Access" in the top-right toggle.

Restricting Schema Fields

To restrict access to all fields in your schema and specify individually which fields this group has access to, ensure that the toggle in the top-right of the page is set to **Restricted Data Access**. This will allow you to manually set the permissions for fields that you want this group to have access to. Using the appropriate checkboxes you can set the group to have either read-only access to a field or both read and write access to the

field (image below).

For instance, if you have a Customer Service group that you want to be able to change email addresses that a user may have entered incorrectly, you can set the emails object of the schema to be read-only, which will give the group the ability to see both verified and unverified email addresses for a user. Then, to enable the group to edit an unverified email (but not existing verified addresses) you can enable write permissions for the unverified emails. Finally, be sure to press **Update** so that your changes are saved.

Permission Groups

Group: testScopedAccess2

Restricted Data Access Full Data Access

Description: restricted

Privileges

Scope

Data Field Access

Members



Update

Field Name	Read	Write
account	<input type="checkbox"/>	<input type="checkbox"/>
committed	<input type="checkbox"/>	<input type="checkbox"/>
created	<input type="checkbox"/>	<input type="checkbox"/>
createdTimestamp	<input type="checkbox"/>	<input type="checkbox"/>
data	<input type="checkbox"/>	<input type="checkbox"/>
emails	<input checked="" type="checkbox"/>	<input type="checkbox"/>
unverified	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
verified	<input checked="" type="checkbox"/>	<input type="checkbox"/>
identities	<input type="checkbox"/>	<input type="checkbox"/>
activities	<input type="checkbox"/>	<input type="checkbox"/>
address	<input type="checkbox"/>	<input type="checkbox"/>

Privileges

Depending upon what privileges you grant users under the **Privileges** tab, some fields may automatically receive **read** and/or **write** permissions to enable the users to utilize these granted privileges. You will see these fields with their necessary permissions uneditable. As an example, you grant the privilege to edit user records:

Identity Access		
<input checked="" type="checkbox"/> User records <input type="checkbox"/> Delete user records		<p>Users with permissions to Identity Access are also granted access to the data of the following fields:</p> <ul style="list-style-type: none">- UID- Created- Last Login- Last Updated- Is Registered- Is Verified- Profile<ul style="list-style-type: none">- First Name- Last Name- Nickname- Name- Email- Username- Emails<ul style="list-style-type: none">- Verified- Unverified- Login IDs<ul style="list-style-type: none">- Emails

You will see in the right-hand column, a list of fields that these users will also be automatically granted access to. When you then go and view the Data Field Access tab, these fields will be greyed out and uneditable.

Field Name	Read	Write
industry	<input type="checkbox"/>	<input type="checkbox"/>
interestedIn	<input type="checkbox"/>	<input type="checkbox"/>
interests	<input type="checkbox"/>	<input type="checkbox"/>
languages	<input type="checkbox"/>	<input type="checkbox"/>
> lastLoginLocation	<input type="checkbox"/>	<input type="checkbox"/>
lastName	<input checked="" type="checkbox"/>	<input type="checkbox"/>
> likes	<input type="checkbox"/>	<input type="checkbox"/>
locale	<input type="checkbox"/>	<input type="checkbox"/>
name	<input checked="" type="checkbox"/>	<input type="checkbox"/>
nickname	<input checked="" type="checkbox"/>	<input type="checkbox"/>
> oidcData	<input type="checkbox"/>	<input type="checkbox"/>
> patents	<input type="checkbox"/>	<input type="checkbox"/>
> phones	<input type="checkbox"/>	<input type="checkbox"/>
photoURL	<input type="checkbox"/>	<input type="checkbox"/>
politicalView	<input type="checkbox"/>	<input type="checkbox"/>
professionalHeadline	<input type="checkbox"/>	<input type="checkbox"/>
profileURL	<input type="checkbox"/>	<input type="checkbox"/>
proxyemail	<input type="checkbox"/>	<input type="checkbox"/>
< subscriptions	<input type="checkbox"/>	<input type="checkbox"/>

Editing a Site Identity

When a group is granted the **Identity Access > User records** privilege, if you want the users to have the ability to view and/or edit a person's Site identity you need to grant additional permissions from the **Data Field Access** tab.



Larry Tester

[Back to list](#)

ID: [dd69c7f86450465799...](#)

Email: [\[redacted\]](#)



User Details

★ Game Mechanics Achievements

Show data from:

Site

[Edit Data](#)



Personal Information

First Name:	Larry	Email:	[redacted]
Last Name:	Tester	Gender:	
Username:		Age:	

Viewing Site Identities

To view Site identities you must grant the group **read** permissions to any relevant fields of the **identities** object, i.e., identities.firstName, identities.lastName, etc.

<input checked="" type="checkbox"/> identities	<input type="checkbox"/>	<input type="checkbox"/>
activities	<input type="checkbox"/>	<input type="checkbox"/>
address	<input type="checkbox"/>	<input type="checkbox"/>
age	<input type="checkbox"/>	<input type="checkbox"/>
allowsLogin	<input type="checkbox"/>	<input type="checkbox"/>
bio	<input type="checkbox"/>	<input type="checkbox"/>
birthDay	<input type="checkbox"/>	<input type="checkbox"/>
birthMonth	<input type="checkbox"/>	<input type="checkbox"/>
birthYear	<input type="checkbox"/>	<input type="checkbox"/>
> certifications	<input type="checkbox"/>	<input type="checkbox"/>
city	<input type="checkbox"/>	<input type="checkbox"/>
country	<input type="checkbox"/>	<input type="checkbox"/>
> education	<input type="checkbox"/>	<input type="checkbox"/>
educationLevel	<input type="checkbox"/>	<input type="checkbox"/>
email	<input type="checkbox"/>	<input type="checkbox"/>
> favorites	<input type="checkbox"/>	<input type="checkbox"/>
firstName	<input checked="" type="checkbox"/>	<input type="checkbox"/>
followersCount	<input type="checkbox"/>	<input type="checkbox"/>

If you want users to be able to also **write** to the persons Site identity, you need to also grant **write** permissions to the *corresponding field of the Profile object*.

profile		
activities	<input type="checkbox"/>	<input type="checkbox"/>
address	<input type="checkbox"/>	<input type="checkbox"/>
age	<input type="checkbox"/>	<input type="checkbox"/>
bio	<input type="checkbox"/>	<input type="checkbox"/>
birthDay	<input type="checkbox"/>	<input type="checkbox"/>
birthMonth	<input type="checkbox"/>	<input type="checkbox"/>
birthYear	<input type="checkbox"/>	<input type="checkbox"/>
certifications	<input type="checkbox"/>	<input type="checkbox"/>
city	<input type="checkbox"/>	<input type="checkbox"/>
country	<input type="checkbox"/>	<input type="checkbox"/>
education	<input type="checkbox"/>	<input type="checkbox"/>
educationLevel	<input type="checkbox"/>	<input type="checkbox"/>
email	<input checked="" type="checkbox"/>	<input type="checkbox"/>
favorites	<input type="checkbox"/>	<input type="checkbox"/>
firstName	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Important
For Console users to edit data for a person's Site identity, their group must be granted **READ** permissions to the appropriate field in the **IDENTITY** object and **WRITE** permissions to the corresponding field of the **PROFILE** object.

Additional Information

- Console Administration
- Identity Access
- Accounts Data Object
- Accounts Profile Object
- Accounts Identity Object