Profiles vs Permission Sets in Salesforce Data Cloud

1. Introduction

In Salesforce, **Profiles** and **Permission Sets** are the two main mechanisms for **managing user access and security**.

The same concept applies within **Salesforce Data Cloud** (Customer Data Platform): both are used to control who can **view, modify, or manage data and configurations** such as Data Streams, Data Model Objects (DMOs), Calculated Insights, Segments, and Identity Resolution rules.

Although Data Cloud extends Salesforce's capabilities, it still inherits the **core Salesforce security model**, where **Profiles define baseline access**, and **Permission Sets provide additional, flexible access**.

---

2. Overview of Profiles and Permission Sets

Feature	Profile	Permission Set
Definition	A Profile defines a user's baseline access level to objects, fields, tabs, apps, and system permissions.	A Permission Set grants *additional* access on top of the user's profile.
Purpose	Establishes what a user can do by default when their account is created.	Expands permissions without changing the assigned profile.

Feature	Profile	Permission Set
Scope	Global baseline permissions.	Granular, task-specific permissions.
Assigned To	One profile per user.	Multiple permission sets per user.
Best For	Defining standard access by role (e.g., Data Cloud Admin, Analyst).	Granting temporary or specialized access (e.g., manage segments, explore data).

---

3. Profiles in Salesforce Data Cloud

Definition

A **Profile** in Salesforce Data Cloud defines the **default access** a user has to Data Cloud features, objects, and data operations.

It acts as the **foundational layer of security**, ensuring every user only has permissions necessary for their job function.

Common Profiles in Data Cloud

1. **System Administrator** – Full access to all Data Cloud configuration and data management.
2. **Data Cloud Admin / Data Manager** – Can create Data Streams, configure Identity Resolution, and manage transformations.
3. **Data Analyst** – Can explore data, run queries, and view dashboards.
4. **Marketing User** – Can view segments and activation audiences but cannot change schema or dataflows.
5. **Viewer / Read-Only** – Can view Data Cloud objects but cannot modify them.

What Profiles Control

Category	Example Permissions
Object Access	Create, Read, Edit, Delete access to Data Streams, DMOs, CIOs, and Segments.
Field-Level Access	Control over specific fields within a Data Model Object.
Tab Access	Visibility to Data Cloud app tabs (Data Streams, Data Explorer, Profile Explorer).
Administrative Rights	Ability to manage ingestion pipelines, identity resolution rules, or calculated insights.
Login Access	Determines which users can log into the Data Cloud workspace.

Example

A user assigned the **Data Cloud Analyst** profile can view Data Model Objects and explore data, but cannot create new Data Streams or modify schema configurations.

---

4. Permission Sets in Salesforce Data Cloud

Definition

A **Permission Set** in Salesforce Data Cloud provides **additional or specialized permissions** beyond what a user's profile grants.
It offers **fine-grained control**, enabling flexible access management without changing the base profile.

Purpose

Permission Sets are often used to:

- Grant temporary elevated access.
- Allow selected users to perform specialized tasks (like managing Data Streams or activating Segments).
- Assign Data Cloud–specific roles such as *Data Explorer User* or *Segment Manager*.
- Enable access to **Einstein AI features**, **Data Cloud APIs**, or **Data Graphs**.

What Permission Sets Control

Function	**Example Permission Set**
Manage Data Streams	Grants permission to create, edit, and delete data ingestion pipelines.
View Data Explorer	Allows viewing and validating data in Data Explorer.
Manage Data Model Objects	Enables creation or modification of DMOs and schema mappings.
Access Profile Explorer	Allows viewing unified customer profiles.
Manage Segments and Activation	Permits building, editing, and publishing Segments.
Access APIs	Grants access to Data Cloud REST or Query APIs.

Example

A marketing analyst with a **Marketing User** profile can be assigned an additional **"Manage Segments"** permission set to allow segment creation and activation, without giving admin-level permissions.

---

5. How Profiles and Permission Sets Work Together

Step	Description
1	Every user must have one Profile, which sets their minimum access.
2	Permission Sets can then be assigned to extend permissions as needed.
3	Combined, they define the total level of access to Salesforce Data Cloud objects and capabilities.
4	Removing a permission set removes only the additional access, not the base permissions from the profile.

Example Scenario

- **User:** Maya (Marketing Analyst)
- **Profile:** Marketing User (view-only access to segments)
- **Added Permission Set:** Manage Segments

After assigning the permission set, Maya can now create and edit segments, but still cannot modify Data Streams or DMOs.

This approach allows security to remain **principle of least privilege** while maintaining flexibility.

---

6. Real-World Use Case: Enterprise Data Cloud Implementation

Background

An e-commerce company implements Salesforce Data Cloud for customer 360 data unification and segmentation.

The team includes administrators, data engineers, analysts, and marketers.

Access Model

Role	Profile	Permission Sets	Purpose
Data Cloud Administrator	System Administrator	None (full access)	Manages the entire platform
Data Engineer	Data Cloud Manager	Manage Data Streams, Manage Data Models	Configures ingestion and modeling
Data Analyst	Data Cloud Analyst	Access Data Explorer, Access Calculated Insights	Performs validation and builds reports
Marketing Manager	Marketing User	Manage Segments, Access Profile Explorer	Creates and activates segments for campaigns
Compliance Officer	Read-Only	View Unified Profiles	Monitors data usage and compliance

Outcome

- The admin defines broad roles using profiles.
- Fine-tuned access is managed via permission sets.
- Access remains controlled, auditable, and easily adjustable for new users.

---

7. Best Practices

1. **Use Profiles for roles and departments**

   Create profiles that reflect major functional roles, such as “Data Cloud Analyst” or “Marketing User.”

2. **Use Permission Sets for flexibility**

   Add extra permissions when users need temporary or additional access.

3. **Follow the principle of least privilege**

   Assign the minimum permissions necessary for a user to perform their job.

4. **Group Permission Sets into Permission Set Groups**

   Simplify management by bundling related permissions (for example, a “Data Cloud Operations” group).

5. **Regularly audit user access**

   Periodically review assigned profiles and permission sets to ensure they match current responsibilities.

6. **Leverage Named Credentials**

   For API or integration access, use Named Credentials rather than giving users broad administrative permissions.

---

8. Summary Comparison Table

Feature	Profiles	Permission Sets
Definition	Baseline access assigned to a user	Additional, granular access assigned optionally
Quantity per user	One	Multiple
Primary Use	Define standard roles and base permissions	Extend or customize permissions
Flexibility	Low	High
Common Use Case	Role-based access (Admin, Analyst, Marketer)	Task-based access (Manage Segments, View Profiles)
Example in Data Cloud	“Data Cloud Analyst” profile defines base access	“Access Profile Explorer” permission set grants extra feature
Change Impact	Affects all users with that profile	Affects only assigned users

---

9. Final Summary

In Salesforce Data Cloud:

- **Profiles** establish the **default access** a user has to data objects, tools, and features.
- **Permission Sets** grant **additional, optional access** for specific tasks or modules.

This combination allows organizations to maintain both **security and flexibility**, ensuring that users only access what they need while still enabling collaboration across admin, data, and marketing teams.