Profile and Permission Set

Introduction

1. Data Security in Salesforce deals with providing a secure environment to share data and confidential files. Salesforce profiles and permission sets are essential for maintaining a secure and efficient organization. These features allow Salesforce administrators to manage access to various functionalities and records within the platform.

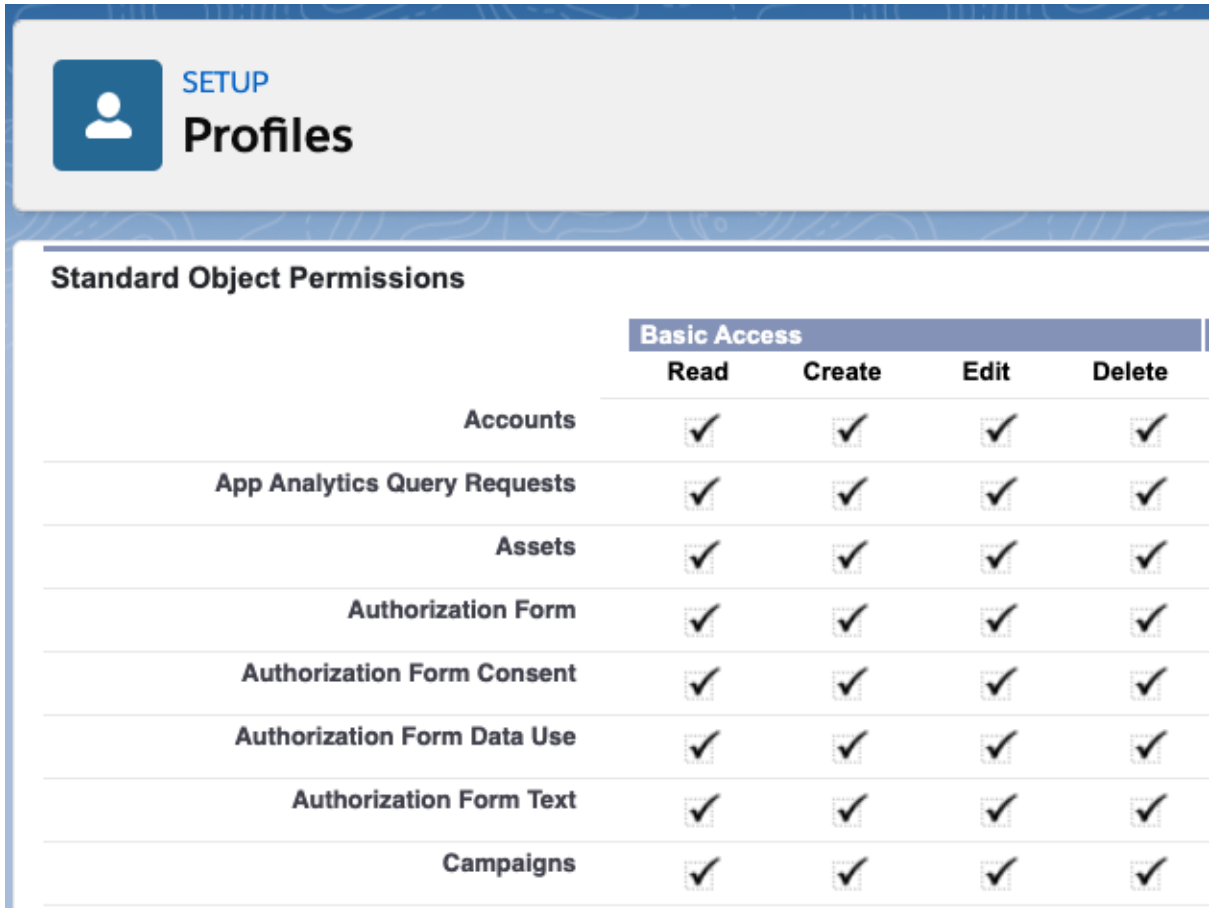
2. Profiles control what users can **do** in your Salesforce org. This can be referred to as CRED:

C = create
R = read
E = edit
D = delete

3. Profiles define how users access objects and data, and what they can do within the application. When you create users, you assign a profile to each one.

4. A user's profile determines the objects they can access and the things they can do with any object record (such as create, read, edit, or delete). Permission sets grant additional permissions and access settings to a user.

profile’s settings looks like below



Profile Types

There are two major types of user profiles in Salesforce – standard profiles and custom profiles. While a standard profile is a profile already provided by Salesforce, a custom profile can be created by the users based on their specific requirements

1.Standard Profiles: These are pre-defined profiles provided by Salesforce, such as "System Administrator," "Sales User," and "Read-Only User." These profiles offer a quick and easy way to manage user access, but they cannot be modified.
2.Custom Profiles: For a more tailored approach, admins can create custom profiles based on their organization's unique needs. Custom profiles offer flexibility and control, allowing admins to fine-tune access levels for specific user groups.

Levels of Data Access

You can control which users have access to which data in your whole org, a specific object, a specific field, or an individual record.

Organization

For your whole org, you can maintain a list of authorized users, set password policies, and limit logins to certain hours and locations.

Objects

Access to object-level data is the simplest thing to control. By setting permissions on a particular type of object, you can prevent a group of users from creating, viewing, editing, or deleting any records of that object.

For example, you can use object permissions to ensure that interviewers can view positions and job applications but not edit or delete them. You can use profiles to manage the objects that users can access and the permissions they have for each object. You can also use permission sets and permission set groups to extend access and permissions without modifying users' profiles.

Fields

You can restrict access to certain fields, even if a user has access to the object.

For example, you can make the salary field in a position object invisible to interviewers but visible to hiring managers and recruiters.

How To Create A Profile In Salesforce?

Creating profiles in Salesforce is a simple process with no complications. Here are the steps you can follow to create a profile in Salesforce Lightning:

1. Log into your Salesforce Lightning account and go to “Setup”.
2. Click on the option of “Setup Home” and search for profiles in the Quick Find Box.
3. Once you have opened the Profiles window, click on the option of “New Profile.”
4. You will now see a drop-down menu of a list of different profiles. Choose an existing profile from the list.
5. Enter the name of the concerned profile in the space provided.
6. Once you are done, click on “Save” and your Salesforce profile is successfully created.

What can be controlled in profiles Salesforce?

Profiles and permission sets both control CRED (Create, Read, Edit, Delete) permissions on Objects, fields, user settings, tab settings, app settings, Apex class access, Visualforce page access, page layouts, record types, login hours and login IP ranges.

1. Object and Field-Level Security:

• Profiles control which objects (e.g., Accounts, Contacts, Opportunities) users can access and the level of access (Read, Create, Edit, Delete).

• Profiles also dictate field-level security, determining whether users can view, edit, or delete specific fields within an object.

2. Tab Visibility:

• Profiles control which tabs and objects are visible to users. You can customize tab visibility to limit the number of tabs users see on their Salesforce interface, reducing clutter and focusing their attention on relevant objects.

3. App Permissions:

• Profiles can grant or restrict access to custom apps and their associated tabs, ensuring that users only see the apps relevant to their roles and responsibilities.

4. System Permissions:

• Profiles include system permissions that allow or deny users the ability to perform certain system-wide actions, such as modifying all data, managing reports, or installing packages.

5. Record-Level Security:

• While not controlled directly by profiles, record-level security is often determined by a combination of profiles and other settings, such as sharing rules, criteria-based sharing, and manual sharing.

• Profiles can specify the default record access settings, but they can be overridden at the record level based on sharing settings.

6. Login IP Ranges:

• Profiles can enforce login IP ranges, which restrict where users can log in from. This adds an extra layer of security by ensuring that users can only access Salesforce from approved locations.

7. Password Policies:

• Profiles can enforce password policies, such as complexity requirements and expiration rules, to enhance user account security.

8. User Interface Settings:

•Profiles can control user interface settings, such as the ability to customize home page components, enable inline editing, and use various features and tools within Salesforce.

9. Page Layout Assignments:

•Profiles can determine which page layouts users see when viewing records. This allows for customization of the user interface based on user roles.

10. Field-Level Security:

•In addition to object-level access, profiles also specify field-level access. This means you can control which fields within an object a user can see, edit, or delete based on their profile settings.

11. Apex Class and Visualforce Page Access:

•Profiles dictate which Apex classes and Visualforce pages users can access and execute. This ensures that only authorized users can run specific code

What can be controlled in Permission Set Salesforce?

In Salesforce, a Permission Set is a flexible and customizable way to grant additional permissions and access settings to users beyond what their profile provides. Permission Sets are used to extend user access without changing their core profile settings. Here are some key points about Permission Sets in Salesforce:

1. Supplemental Permissions:

• Permission Sets grant additional permissions and access settings to users, allowing them to perform specific tasks or access certain objects, fields, or features that are not part of their primary profile.

2. Customization:

• You can create custom Permission Sets tailored to the needs of different user groups or roles within your organization. This flexibility makes Permission Sets a powerful tool for granting permissions on an as-needed basis.

3. Independence from Profiles:

• Permission Sets are independent of user profiles. This means that you can assign multiple Permission Sets to a user, giving them a combination of permissions from different sources.

4. Object and Field-Level Access:

• Permission Sets can grant or revoke access to specific objects, record types, fields, and tabs within Salesforce. This allows for fine-grained control over data access.

5. Apex Class and Visualforce Page Access:

• You can use Permission Sets to grant access to specific Apex classes and Visualforce pages, allowing users to execute custom code and view custom UI elements.

6. System Permissions:

• Permission Sets include system permissions that can be enabled or disabled for users. These permissions control system-wide actions, such as modifying all data or managing reports and dashboards.

7. Application Permissions:

• Permission Sets can grant access to custom apps and their associated tabs, extending users' access to specific features or functionalities.

8. Page Layout Assignments:

• Permission Sets can determine which page layouts users see when viewing records. This allows for customization of the user interface based on their assigned Permission Sets.

9. Visual Workflow and Process Builder Access:

• Permission Sets can grant access to create, view, or edit Visual Workflows and Process Builder processes.

10. Security and Auditing:

• Permissions granted via Permission Sets are tracked in audit trails and can be used for compliance and security auditing purposes.

11. Assignment and Removal:

• You can assign Permission Sets to users individually or as part of a permission set group. Users can have multiple Permission Sets assigned to them.

• Permission Sets can be added or removed from user records at any time without affecting their profile settings.

12. License Management:

• Some features and apps in Salesforce require specific licenses. Permission Sets can be used to grant users access to these features, even if they have a different primary license.

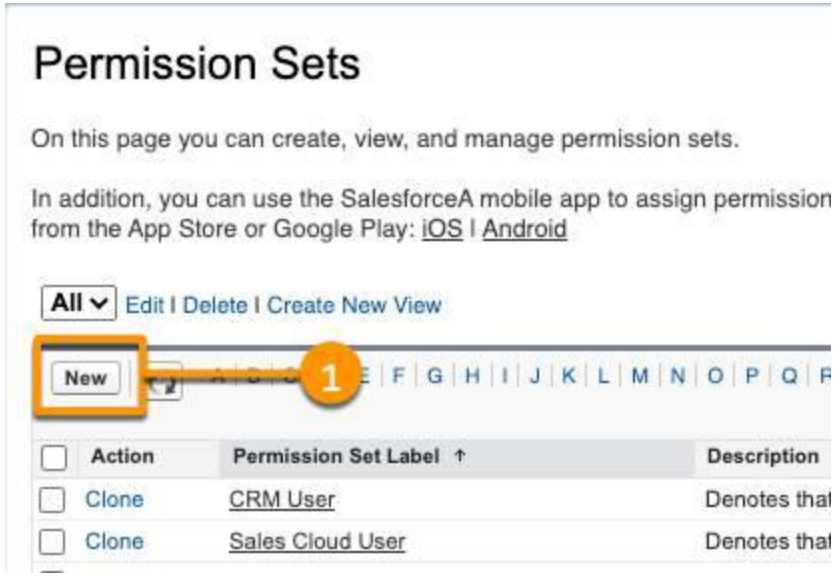
13. Testing and Deployment:

• Permission Sets are often used in testing and deployment scenarios, allowing you to assign specific permissions to users during testing phases and roll them out to production as needed.

Create a Permission Set

1. From Setup, in the Quick Find box, enter **Permission Sets**, and then select **Permission Sets**.

2. Click **Clone** next to the set you want to copy. A cloned permission set has the same user license as the original. To create a set with a different license, click **New** (1) instead.



3. Enter a label and a description. The API name is a unique name used by the API and managed packages. It automatically replicates the label, but you can modify it.

4. If this is a new permission set, select a user license option.

   - If you plan to assign this permission set to multiple users with different licenses, select --None--.
   - If only users with one type of license will use this permission set, select that user license.

5. Click **Save** to go back to the permission set overview page.

6.In the permission set toolbar, click **Manage Assignments**, then click **Add Assignments**.

7.Select the users to assign to this permission set and click **Assign**. Review the messages on the Assignment Summary page. If any users weren't assigned, the Message column tells you why.

8. Click **Done** to return to a list of the users assigned to the permission set.

Conclusion

Salesforce profiles and permission sets are indispensable tools for admins looking to create a secure and efficient environment. By mastering the use of these features, admins can effectively manage user access, cater to their organization's unique needs, and maintain a robust security model.