How to Create a Permission Set in Salesforce

Permission sets let you grant additional object-level security to users for specific, one-off scenarios without creating a new profile. They are useful when you need to extend access to a small group of users—typically between 1 and 10—rather than modifying everyone's profile. For example, in an organization with both sales and service teams, a knowledgeable sales team member may need temporary access to help the service team with a specific case. This guide walks you through how to create a permission set in Salesforce, configure its object and field permissions, and assign it to users.

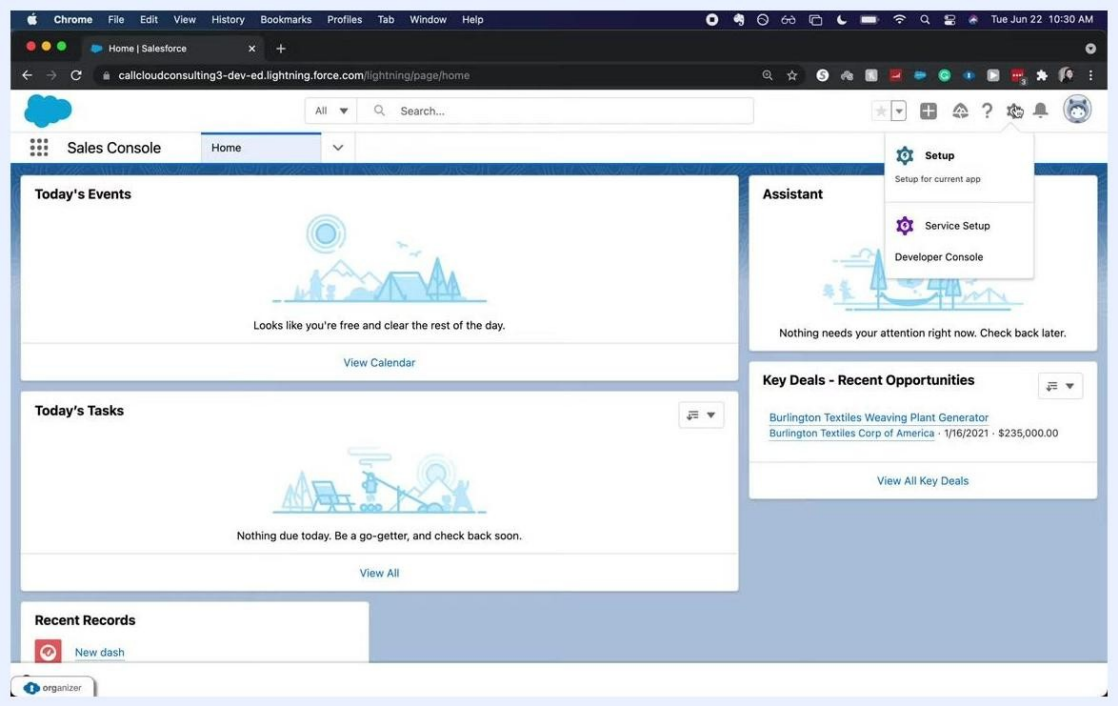
Prerequisites

Before you begin, make sure you have the following:

- An active Salesforce Lightning environment that you are logged into.
- Administrative privileges to access Setup options.
- Access to the Sales Console Home page, which displays panels such as Today's Events, Today's Tasks, Assistant, Key Deals – Recent Opportunities, and Recent Records.
- A top navigation bar showing options like All, Search, and icons for notifications, settings, and your user profile.

Step 1: Open the Salesforce Setup area

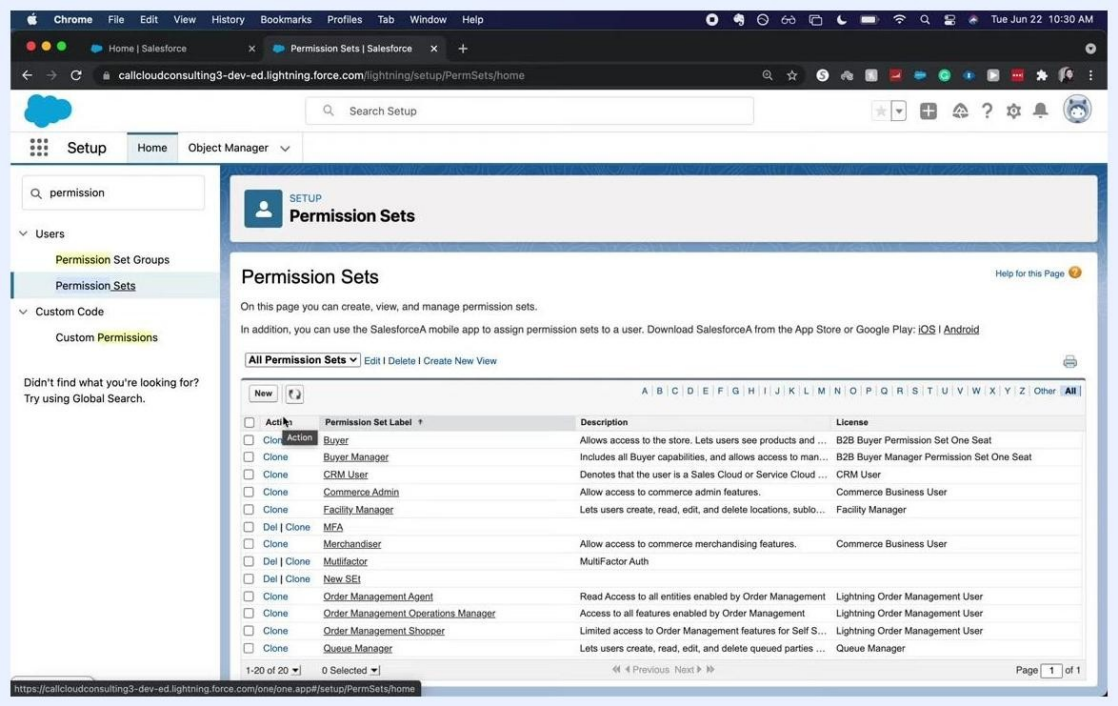
Locate the gear icon in the upper right corner of the Salesforce interface and click it to open the dropdown menu. Select Setup from the dropdown to enter the Salesforce Setup area.



Salesforce Lightning interface with the Setup menu open, showing options for Setup, Service Setup, and Developer Console, with the cursor hovering over the gear icon.

Step 2: Search for Permission Sets

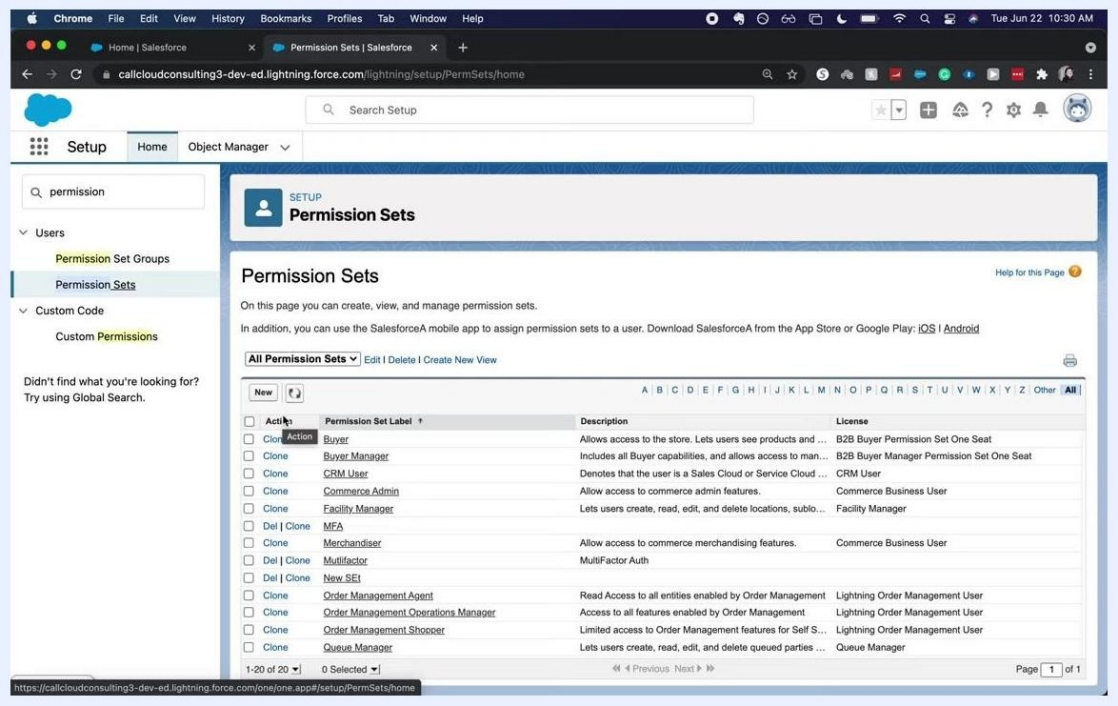
In the Salesforce Setup area, find the Quick Find/Search Setup box on the left sidebar. Type "permission" into the search box, then click Permission Sets under the Users section.



Salesforce Setup Home page with "permission" typed into the Quick Find box, highlighting Permission Sets under Users.

Step 3: Start creating a new permission set

On the Permission Sets page, click the New button at the top of the list to begin creating your permission set.



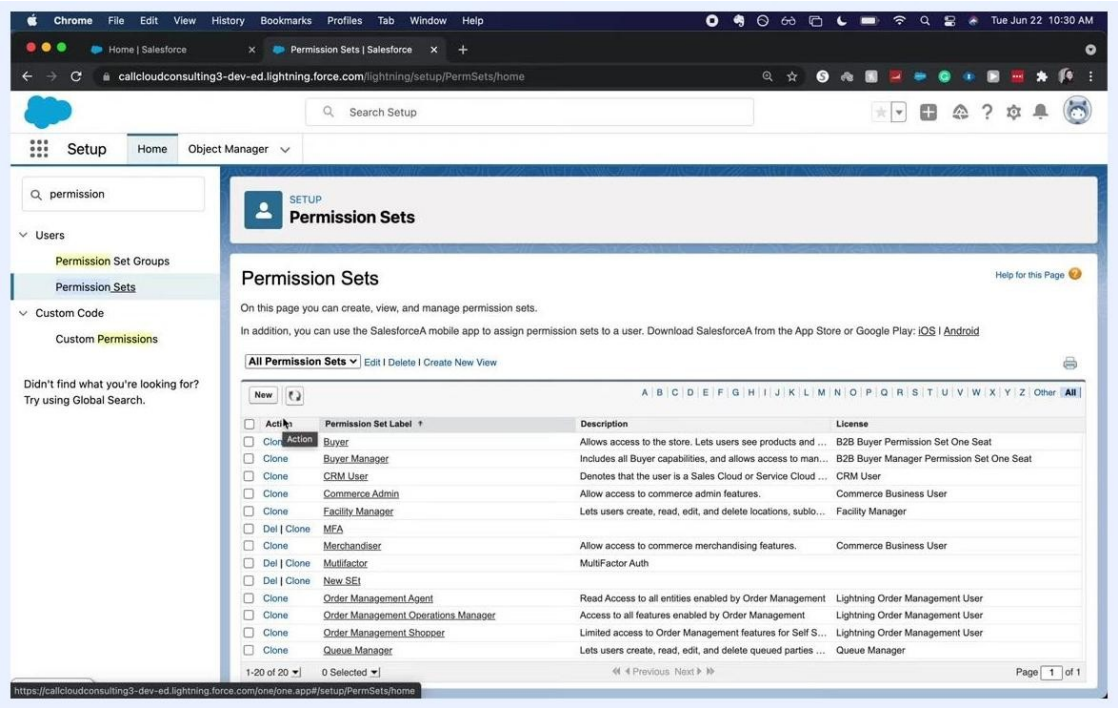
Permission Sets list page with the New button highlighted, showing existing permission sets and their descriptions.

Step 4: Enter the permission set information

Fill in the following fields:

- Label: Enter a name for your permission set (for example, "New").
- API Name: Enter the API name (for example, "New").
- Description: Optional, but recommended for clarity.
- Session Activation Required: Check this box if you want users assigned to this permission set to reactivate their session.

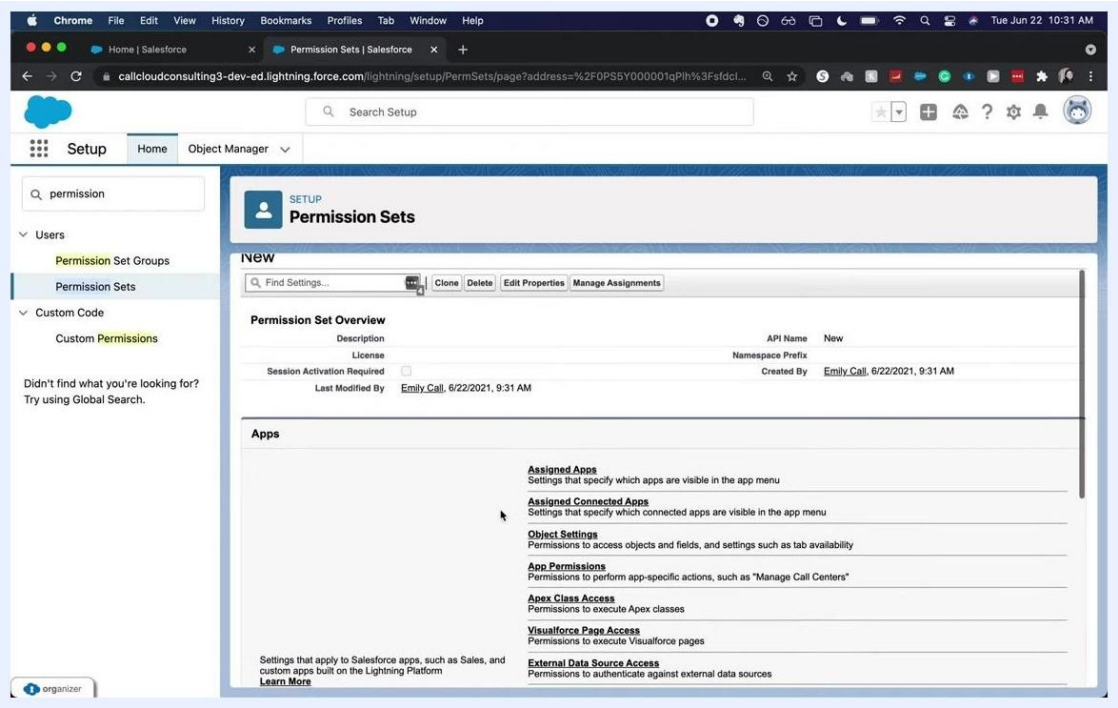
- License: Select the appropriate license for the users who will use this permission set. Leave it as --None-- unless you want to restrict it to a specific license, such as Chatter Free User, Partner User, or Sales User.



Permission Set creation screen with Label "New", API Name "New", the Session Activation Required option, and the License dropdown set to "--None--".

Step 5: Save the permission set

Click Save to create the new permission set.



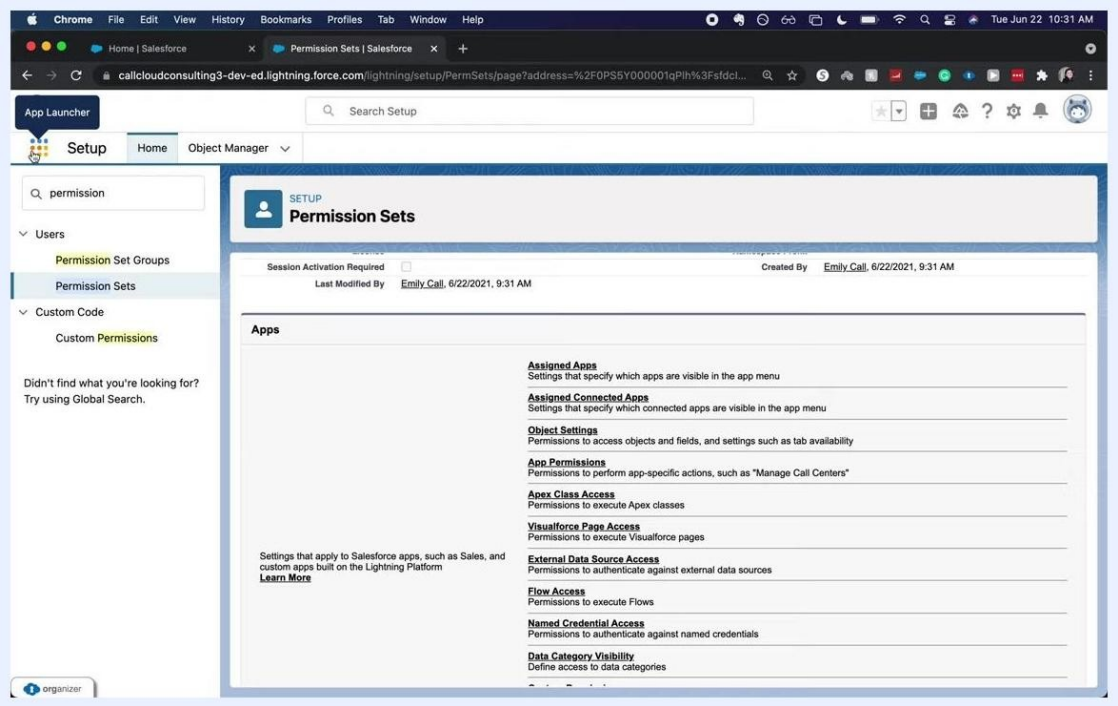
Permission Set creation screen with all fields filled in and the License dropdown visible, ready to save.

Step 6: Review the Permission Set Overview page

After saving, you land on the Permission Set Overview page. Here you can see your permission set's details, including:

- Label and API Name
- Session Activation Required status
- Created By and Last Modified By information

The main section also lists configuration categories, including Assigned Apps, Assigned Connected Apps, Object Settings, App Permissions, Apex Class Access, Visualforce Page Access, External Data Source Access, Flow Access, Named Credential Access, and Data Category Visibility.



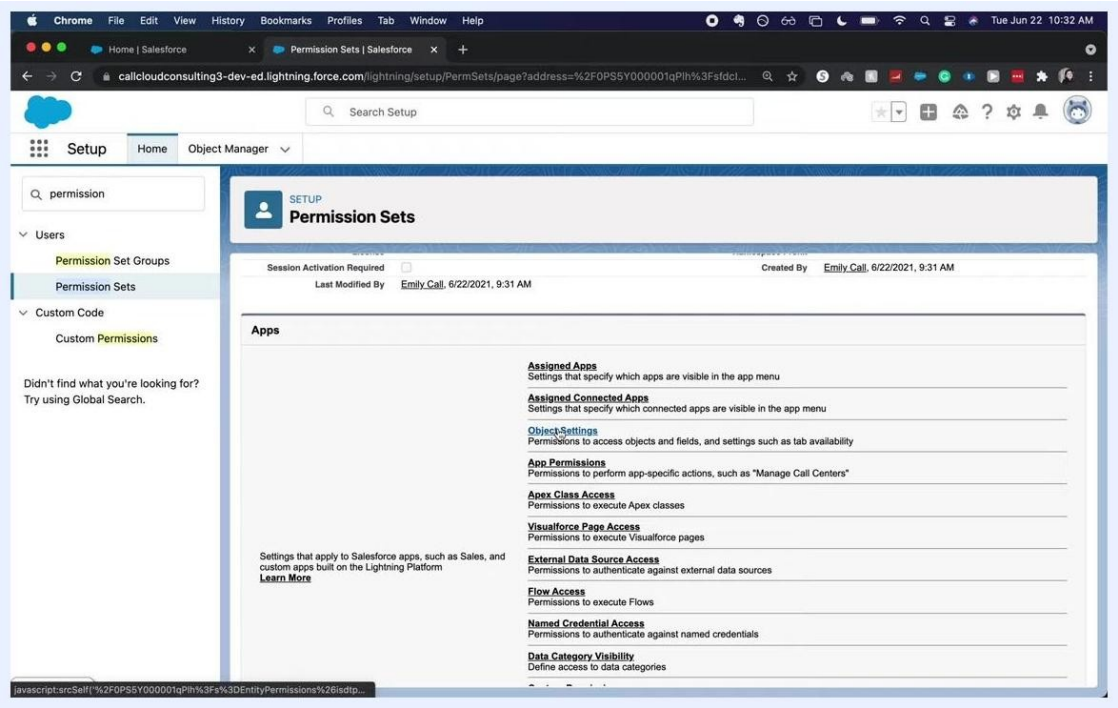
Permission Set Overview page showing the new permission set details and configuration categories.

The Assigned Apps section lets you specify which apps are visible in the app menu for users assigned this permission set. For example, you might assign the Sales Console app for sales users or the Service Console app for service users. Keep in mind that permission sets are meant for one-off scenarios that grant additional access beyond what a user's profile already provides.

The Assigned Connected Apps section works similarly, letting you specify which connected apps are visible in the app menu for users with this permission set. You can also explore additional sections such as Object Settings, App Permissions, and Apex Class Access to further customize the permission set as needed.

Step 7: Open Object Settings

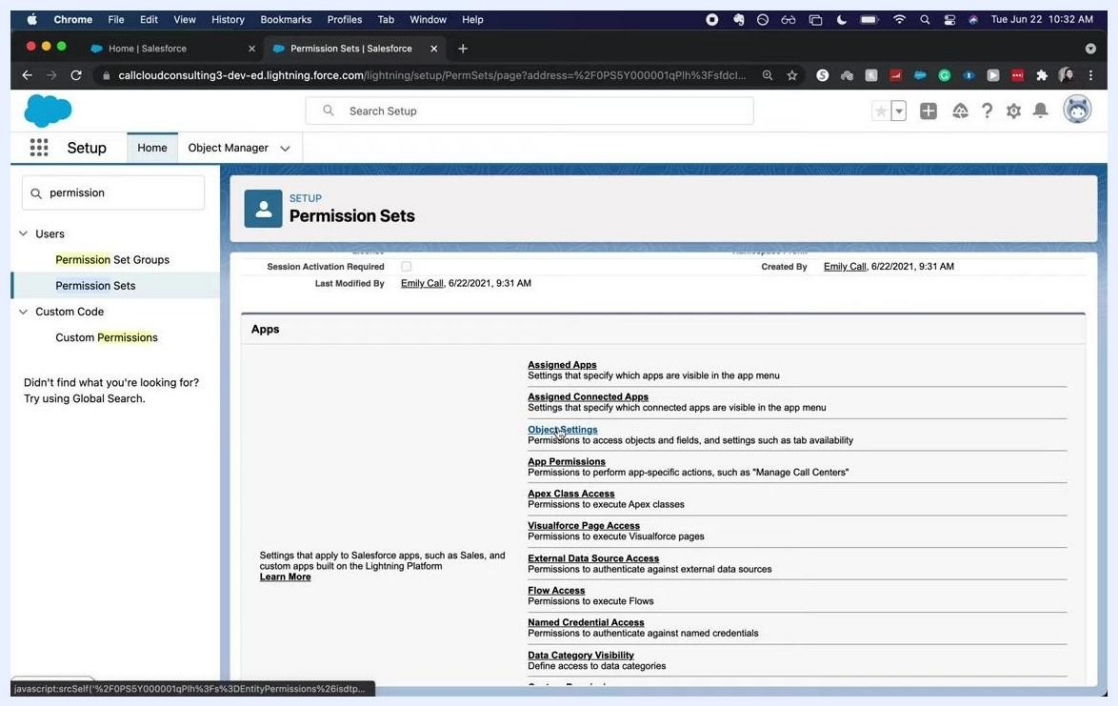
From the Permission Set Overview page, click Object Settings to manage permissions for Salesforce objects.



Permission Set Overview page with the Object Settings link highlighted under the Apps section.

Step 8: View the list of objects

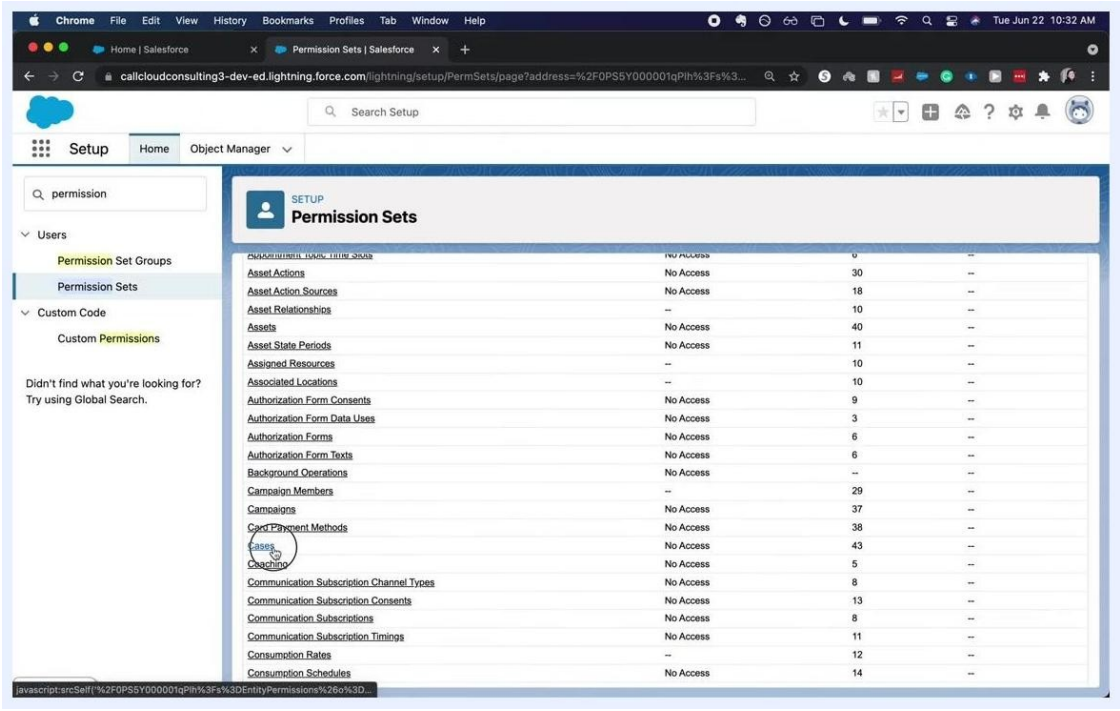
You will see a list of all objects in Salesforce, each showing its current permission status (for example, "No Access"). Scroll through the list to find the object you want to configure—in this example, Cases.



Permission Sets Object Settings page showing a list of objects and their current permissions.

Step 9: Select the object to configure

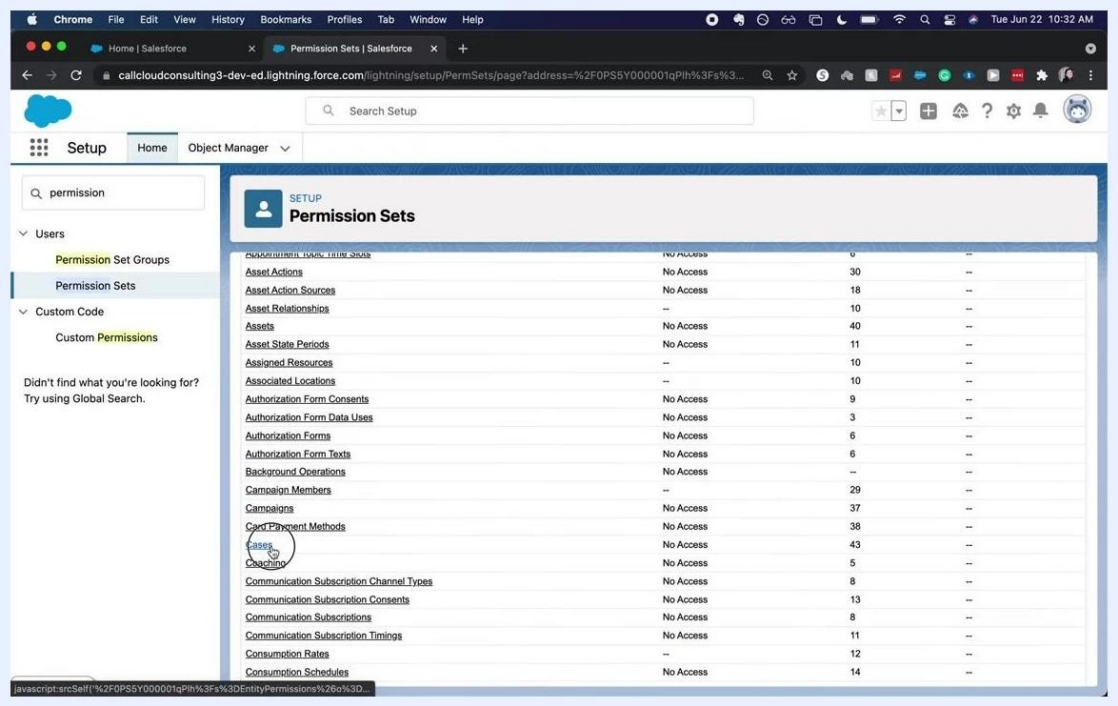
Click Cases in the object list to open its permission settings.



Permission Sets Object Settings page with the Cases object highlighted and selected.

Step 10: Set tab settings for the object

Under Tab Settings, check the Available box to make the Cases tab available to users assigned this permission set. Optionally, check the Visible box if you want the tab to be visible by default.



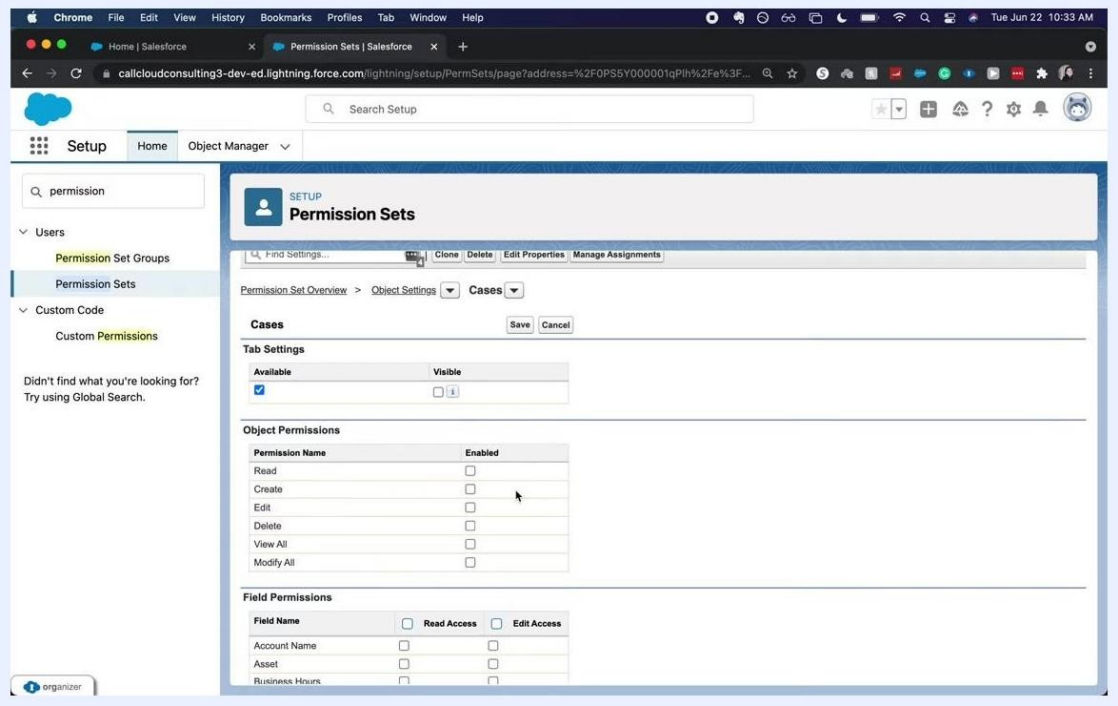
Cases object settings screen with the Available checkbox selected under Tab Settings.

Step 11: Configure object permissions

Under Object Permissions, select the permissions you want to grant:

- Check Read to allow users to view cases.
- Check Edit to allow users to modify cases.
- Leave Create and Delete unchecked if you do not want users to create or delete cases.

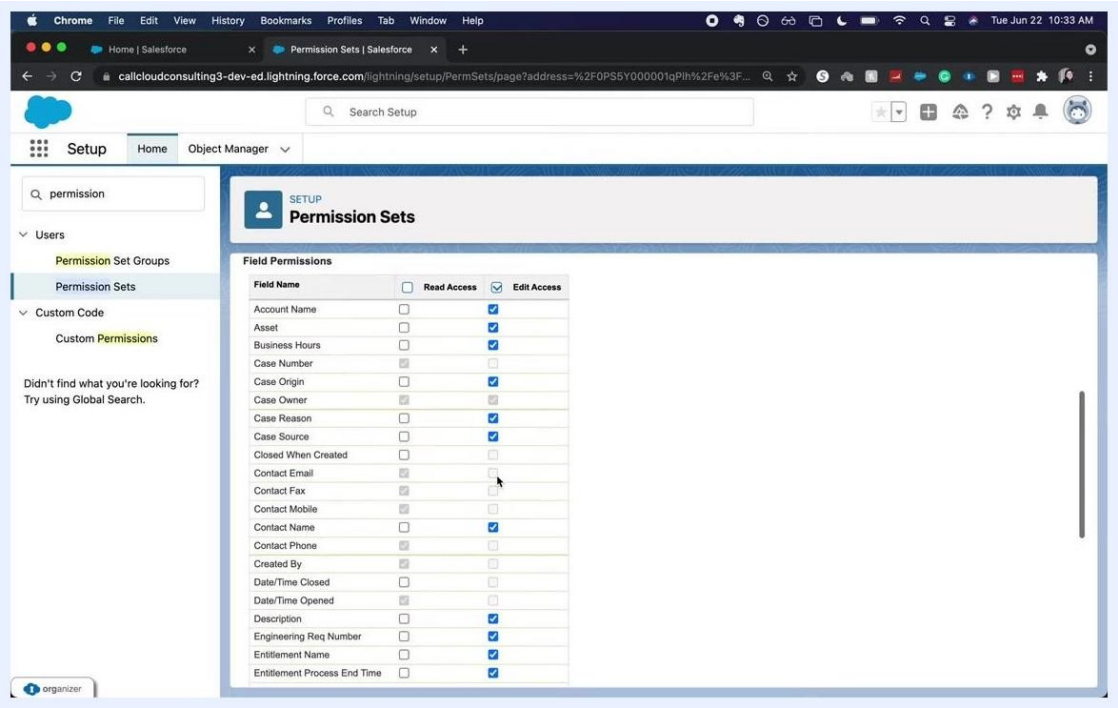
- Avoid selecting View All or Modify All unless you want users to have full access to all records of this object.



Cases object settings with Read and Edit permissions enabled, and Create and Delete unchecked.

Step 12: Set field-level permissions

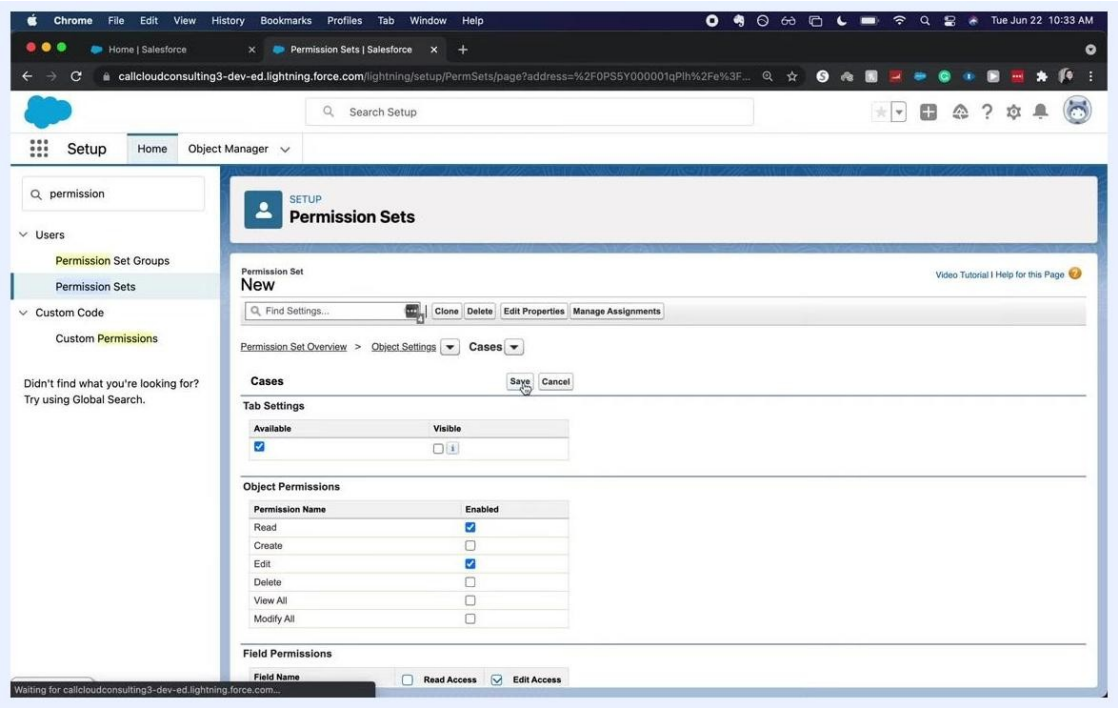
Scroll down to the Field Permissions section. For each field, check Read Access to allow users to view the field, and Edit Access to allow users to modify it. In this example, fields such as "Case Number," "Case Origin," and "Case Reason" have both Read and Edit Access enabled.



Field Permissions section for the Cases object, showing various fields with Read and Edit Access selected.

Step 13: Save object and field permissions

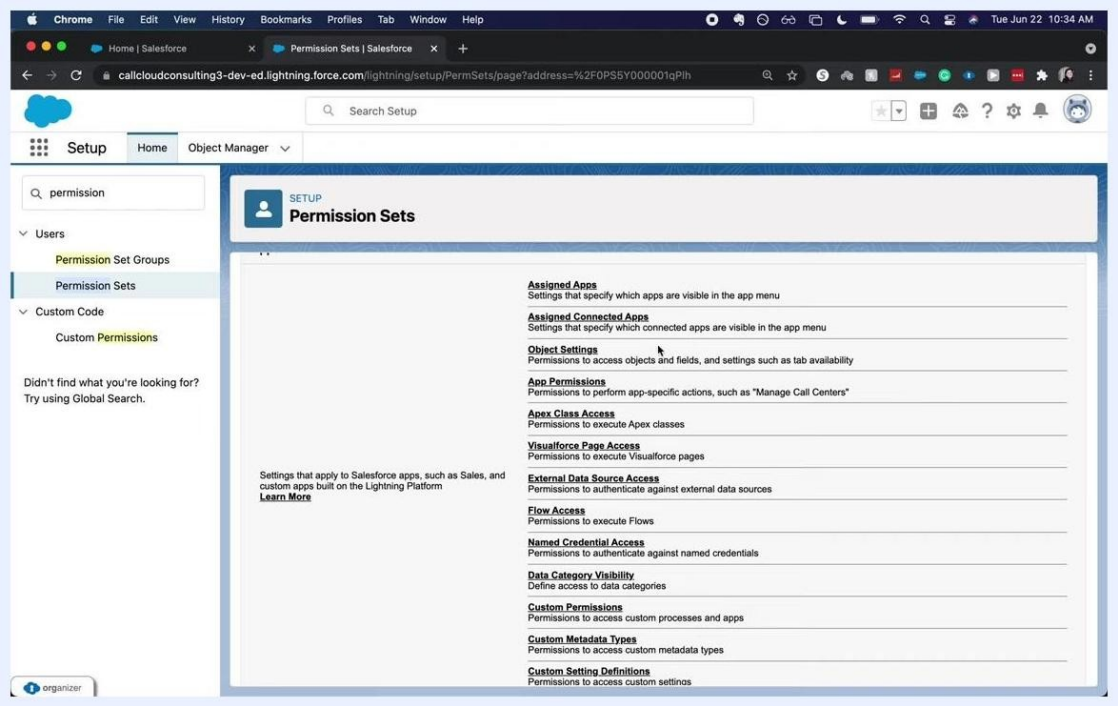
After configuring the desired permissions, click Save at the top or bottom of the page to apply your changes.



Cases object settings with Read and Edit permissions enabled and the Save button highlighted.

Step 14: Review the permission set's app-level details

Navigate back to the Permission Sets page and select your permission set from the left sidebar under Users. The overview displays fields such as Description, License, API Name, Namespace Prefix, Session Activation Required, Last Modified By, and Created By. The Apps section lists categories including Assigned Apps, Assigned Connected Apps, Object Settings, App Permissions, Apex Class Access, Visualforce Page Access, and External Data Source Access.



Salesforce Permission Sets overview listing app permissions, Apex class access, Visualforce page access, and external data source access.

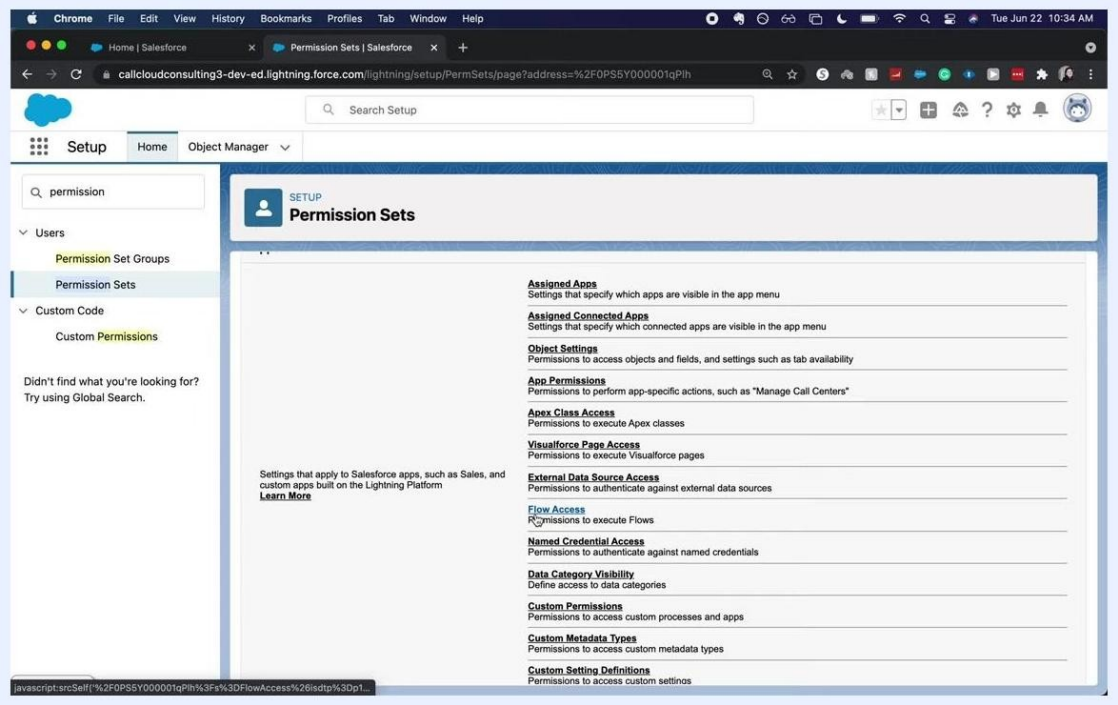
Step 15: Review the available permission categories

Each category in the permission set serves a specific purpose:

- Assigned Apps: Specifies which apps are visible in the app menu.
- Assigned Connected Apps: Specifies which connected apps are visible in the app menu.
- Object Settings: Controls access to objects and fields, and settings such as tab availability.
- App Permissions: Grants permission to perform app-specific actions, such as "Manage Call Centers."
- Apex Class Access: Grants permission to execute Apex classes.

- Visualforce Page Access: Grants permission to execute Visualforce pages.
- External Data Source Access: Grants permission to authenticate against external data sources.
- Flow Access: Grants permission to execute Flows.
- Named Credential Access: Grants permission to authenticate against named credentials.
- Data Category Visibility: Defines access to data categories.
- Custom Permissions: Grants access to custom processes and apps.
- Custom Metadata Types: Grants access to custom metadata types.
- Custom Setting Definitions: Grants access to custom settings.

If your organization has a highly customized setup, use custom permissions to grant access to specific features or processes that standard permissions do not cover.



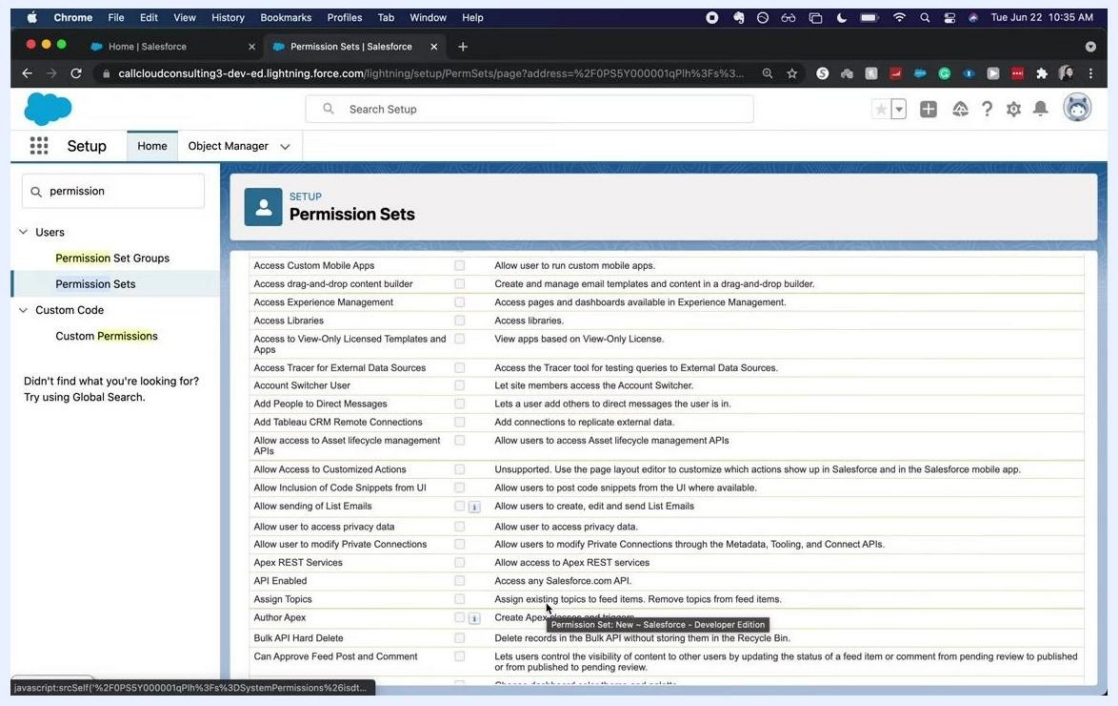
Permission Sets page showing a detailed list of permission categories and their descriptions.

Step 16: Explore system permissions and service providers

In addition to the categories above, you can configure:

- System Permissions: Permissions that apply across all apps, such as "Modify All Data."

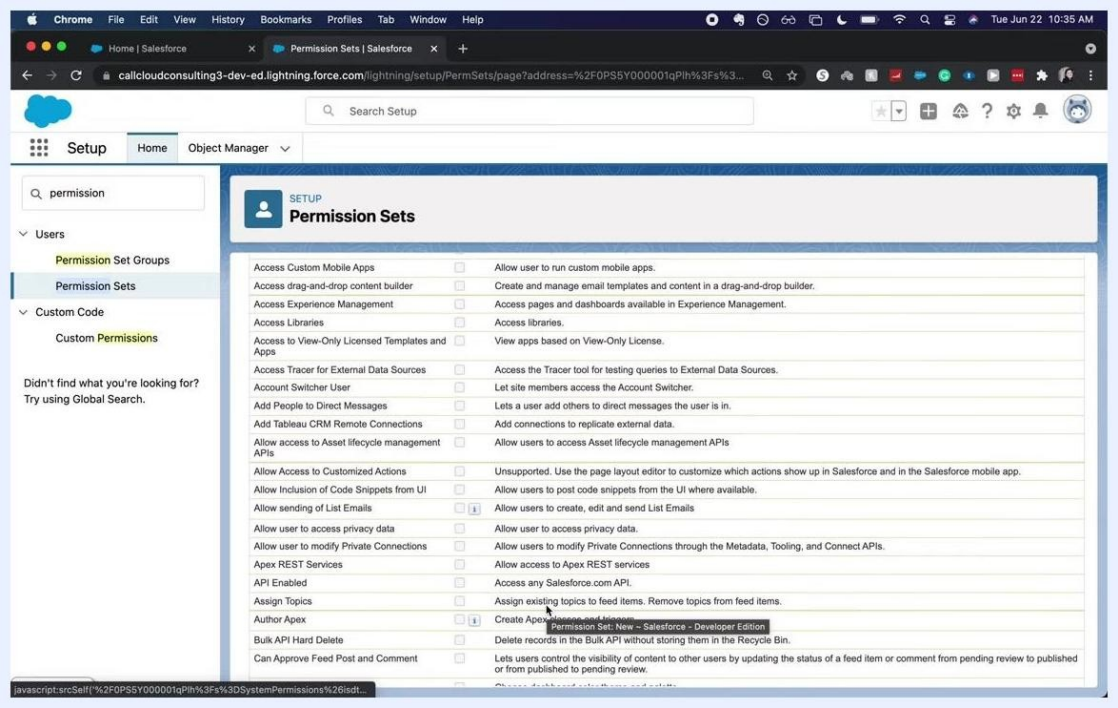
- Service Providers: Permissions that let users switch to other websites using single sign-on.



Permission Sets page with the system permissions and service providers section visible.

Step 17: Review the system permissions list

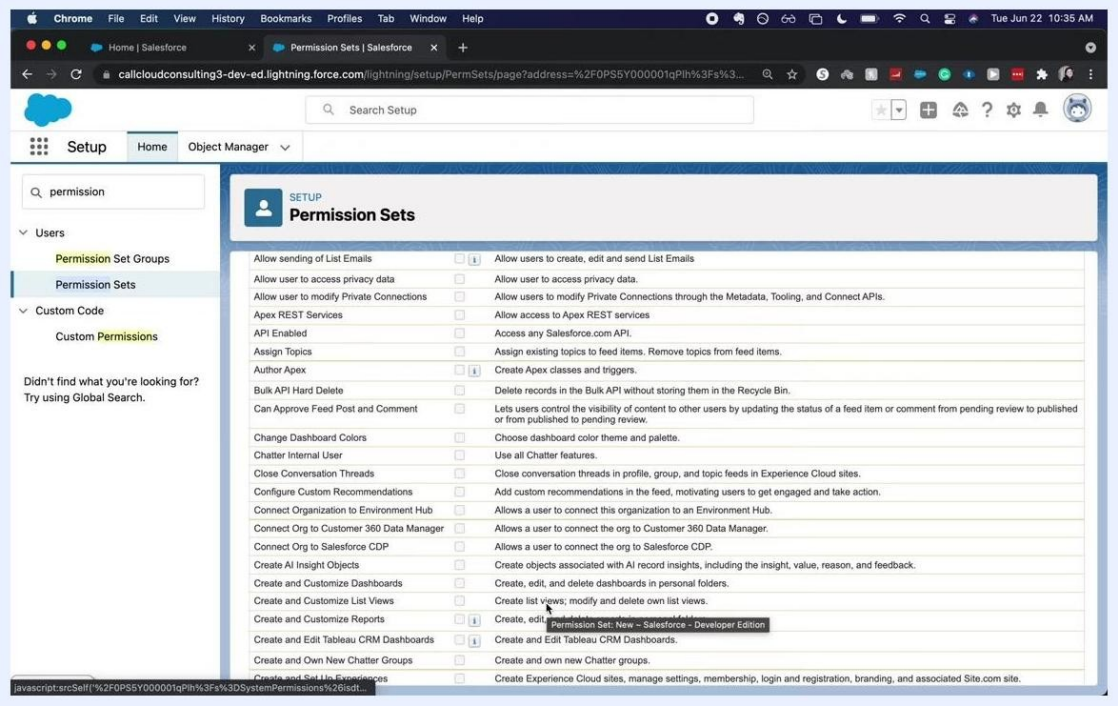
The system permissions list includes a checkbox for each permission, letting you enable or disable it for the permission set. Examples visible in this list include Access Custom Mobile Apps, Access Drag-and-Drop Content Builder, Access Experience Management, Access Libraries, Access to View-Only Licensed Templates and Apps, Access Tracer for External Data Sources, Account Switcher User, Add People to Direct Messages, Add Tableau CRM Remote Connections, Allow Access to Asset Lifecycle Management APIs, Allow Access to Customized Actions, Allow Inclusion of Code Snippets from UI, Allow Sending of List Emails, Allow User to Access Privacy Data, Allow User to Modify Private Connections, Apex REST Services, API Enabled, Assign Topics, Author Apex, Bulk API Hard Delete, and Can Approve Feed Post and Comment.



System permissions list with checkboxes for each permission, including API access, Apex REST Services, and more.

Step 18: Scroll through the extended system permissions

As you continue scrolling, you will find additional permissions such as Change Dashboard Colors, Chatter Internal User, Close Conversation Threads, Configure Custom Recommendations, Connect Organization to Environment Hub, Connect Org to Customer 360 Data Manager, Connect Org to Salesforce CDP, Create and Customize Dashboards, Create and Customize List Views, Create and Customize Reports, Create and Edit Tableau CRM Dashboards, Create and Own New Chatter Groups, and Create and Set Up Experiences.



Extended system permissions list with options for dashboards, reports, Chatter, and more.

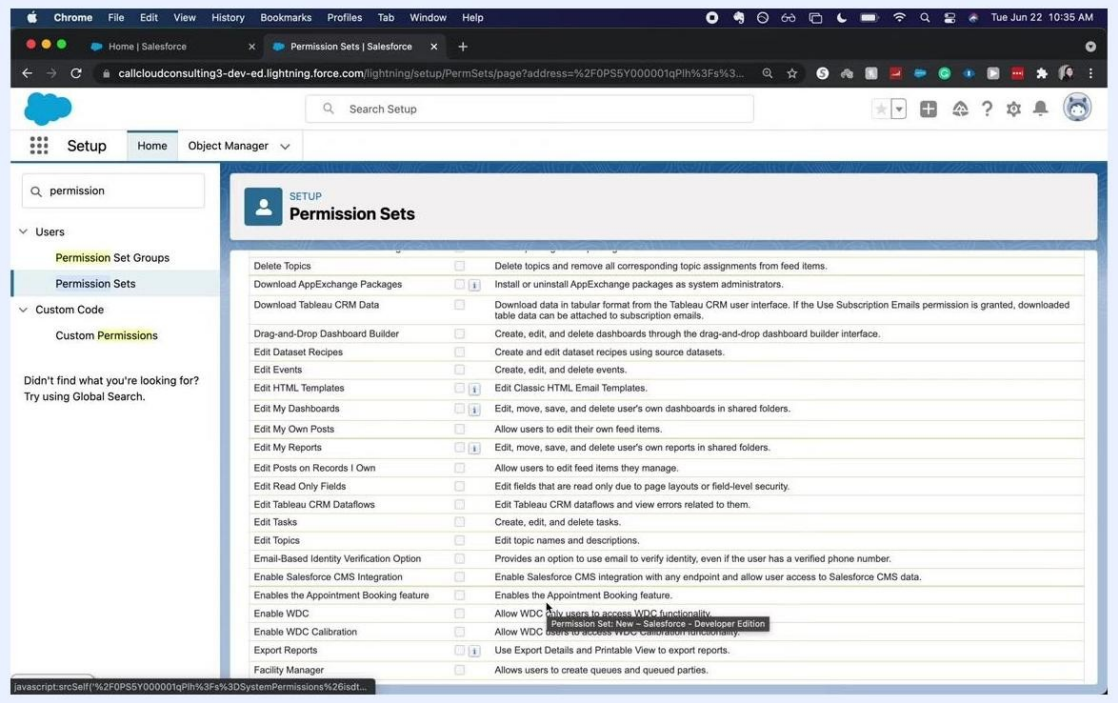
Step 19: Continue reviewing and enabling system permissions

The system permissions list is scrollable, with each permission accompanied by a checkbox and description. Notable examples include:

- Delete Topics: Delete topics and remove all corresponding topic assignments from feed items.
- Download AppExchange Packages: Install or uninstall AppExchange packages as system administrators.
- Download Tableau CRM Data: Download data in tabular format from the Tableau CRM user interface.

- Drag-and-Drop Dashboard Builder: Create, edit, and delete dashboards through the drag-and-drop dashboard builder interface.
- Edit Dataset Recipes: Create and edit dataset recipes using source datasets.
- Edit Events: Create, edit, and delete events.
- Edit HTML Templates: Edit Classic HTML Email Templates.
- Edit My Dashboards: Edit, move, save, and delete your own dashboards in shared folders.
- Edit My Own Posts: Edit your own feed items.
- Edit My Reports: Edit, move, save, and delete your own reports in shared folders.
- Edit Posts on Records I Own: Edit feed items you manage.
- Edit Read Only Fields: Edit fields that are read-only due to page layouts or field-level security.
- Edit Tableau CRM Dataflows: Edit Tableau CRM dataflows and view related errors.
- Edit Tasks: Create, edit, and delete tasks.
- Edit Topics: Edit topic names and descriptions.
- Email-Based Identity Verification Option: Use email to verify identity, even with a verified phone number on file.
- Enable Salesforce CMS Integration: Enable Salesforce CMS integration with any endpoint and allow user access to Salesforce CMS data.
- Enables the Appointment Booking Feature: Enables the Appointment Booking feature.
- Enable WDC: Allow WDC-only users to access WDC functionality.
- Enable WDC Calibration: Allow WDC-only users to access WDC Calibration functionality.
- Export Reports: Use Export Details and Printable View to export reports.
- Facility Manager: Allows users to create queues and queued parties.
- Files Connect Cloud: Access cloud-based external content sources, such as SharePoint Online.
- Files Connect On-Premises: Access on-premises external content sources, such as SharePoint.
- Give Recognition Badges in Experience Builder Sites: Let members give recognition badges to other members.
- Hide Option to Switch to Salesforce Classic: Always use Lightning Experience by removing the switcher.
- Hide the Seen By List: Increase privacy in a private group by hiding the count and names of those who view its posts.

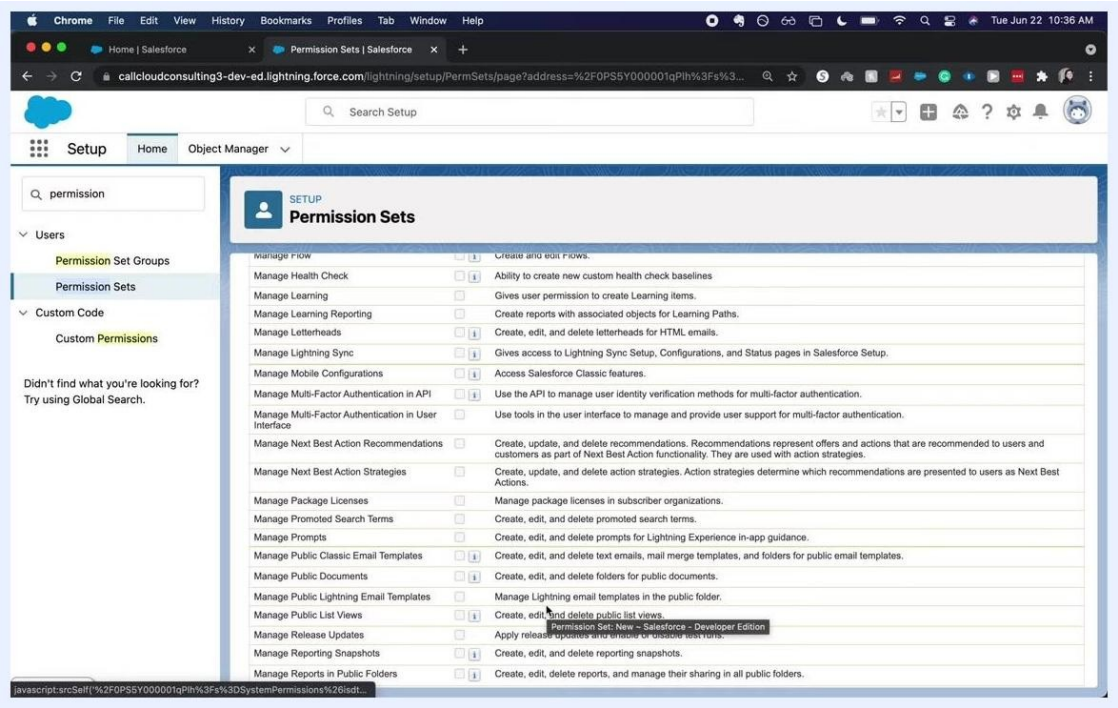
- Import Custom Objects: Allow non-admin users to import custom objects using Data Import Wizard.
- Insert System Field Values for Chatter Feeds: Set the author or creation date for a Chatter post or comment.
- Invite Customers to Chatter: Invite customers to Chatter.
- Let a User Be Included in Appointments in Salesforce Scheduler: Include a user in appointments in Salesforce Scheduler.
- Lightning Console User: Gives the user access to Lightning console apps.
- Lightning Experience User: Access Lightning Experience and switch between Lightning Experience and Salesforce Classic.
- Manage All Private Reports and Dashboards: Create and edit private reports and dashboards in all other users' private folders (API only).



Salesforce Permission Sets page showing a scrollable list of system permissions with checkboxes and descriptions for each permission.

Step 20: Review remaining system permissions

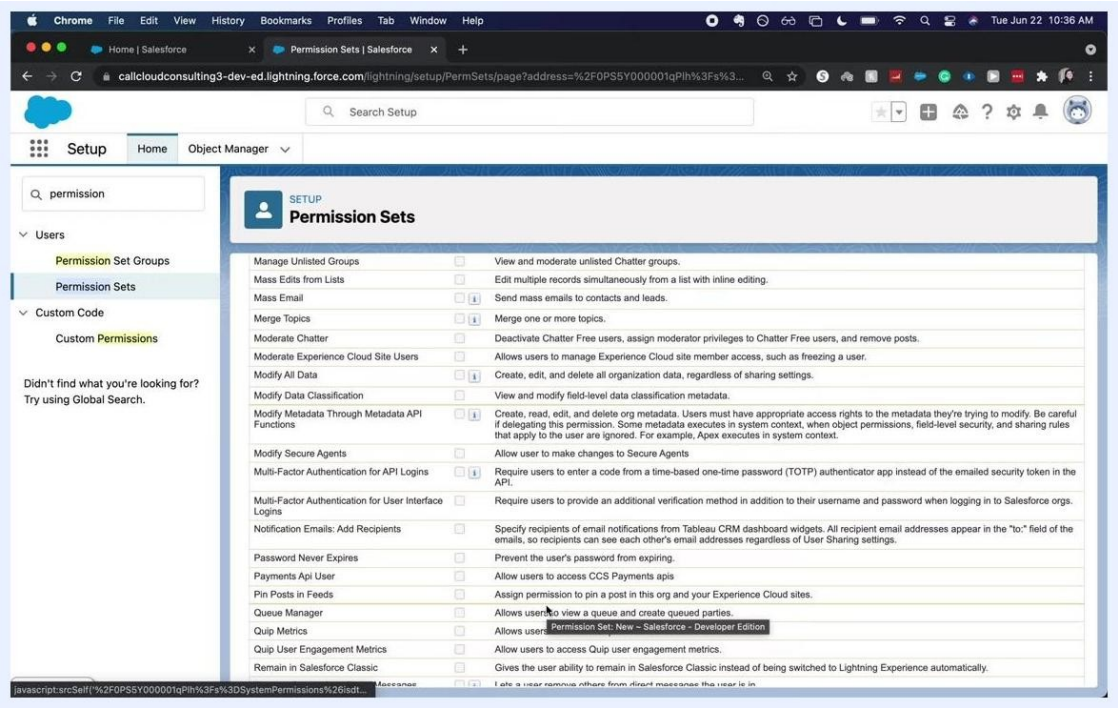
System permissions make up a significant portion of Salesforce administration knowledge. Continue reviewing the available permissions, which include options for managing flows, health checks, learning, Lightning Sync, and multi-factor authentication, to familiarize yourself with what each one controls.



Permission Sets page with system permissions, including options for managing flows, health checks, learning, Lightning Sync, multi-factor authentication, and more.

Step 21: Assign the permission set to users

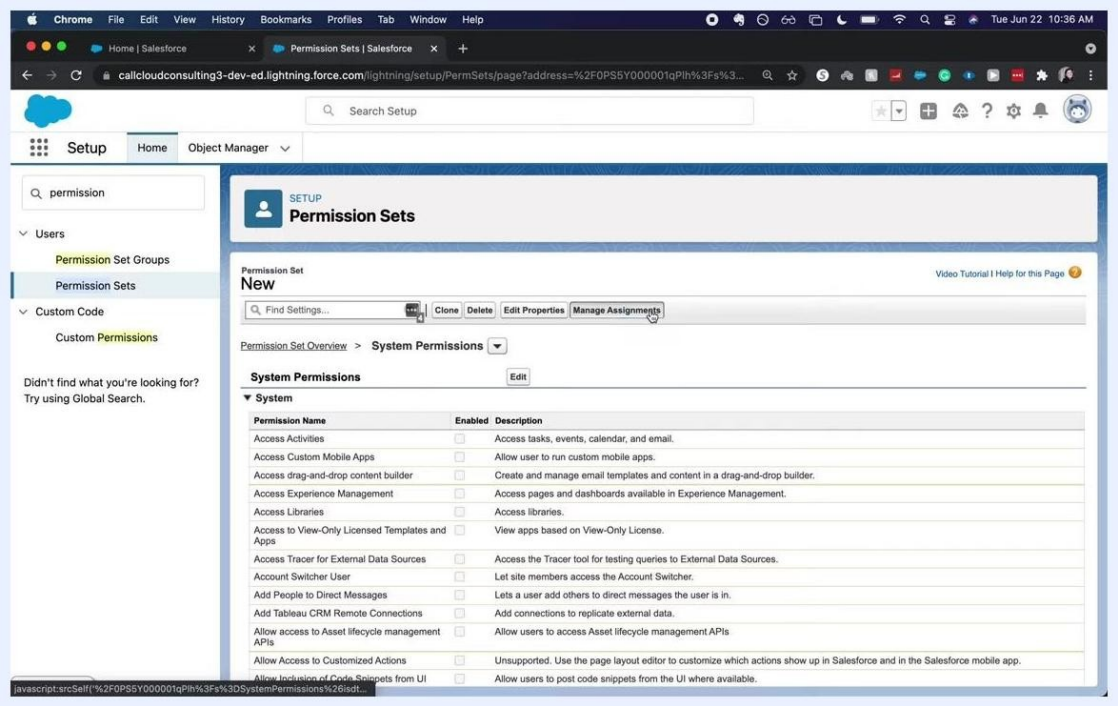
Click Manage Assignments at the top of the permission set page. On the Assign Users screen, select the checkbox next to the user or users you want to assign the permission set to, then click Assign. Note that only users with the appropriate Salesforce license will appear as assignable.



Permission Sets assignment screen showing a list of users with checkboxes, including full name, alias, username, last login, role, active status, and profile.

Step 22: Review assigned users

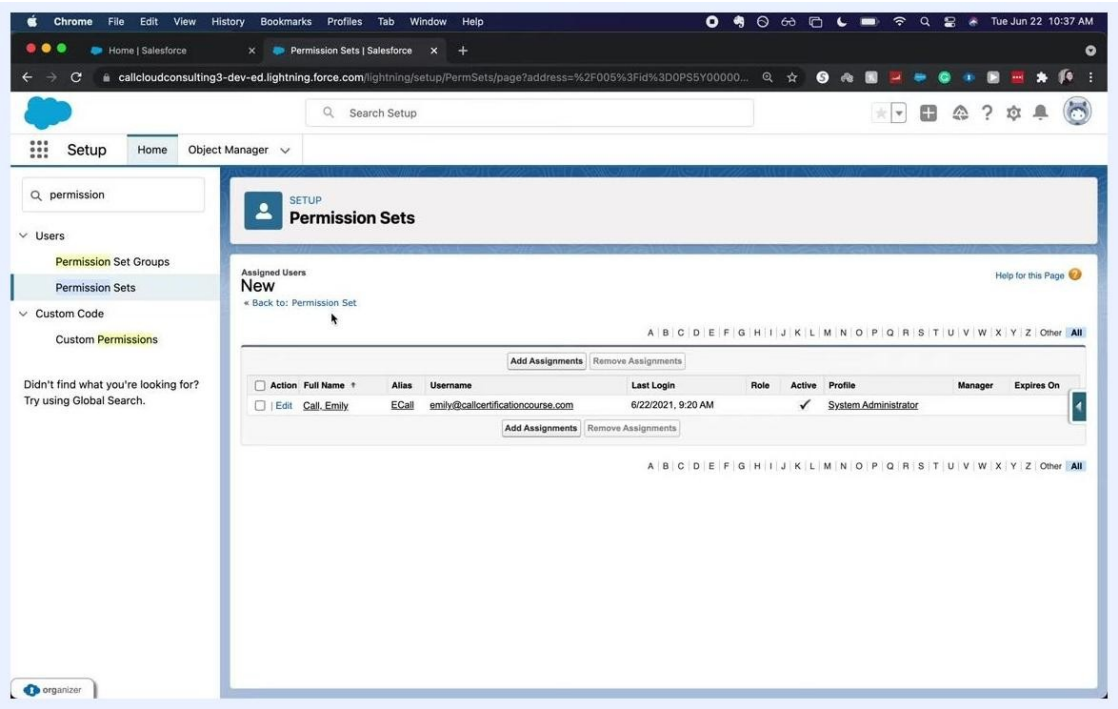
After assignment, the Assigned Users screen displays the users who now have the permission set. You can add or remove assignments from this screen at any time.



Assigned Users screen for a permission set, showing the assigned user, their alias, username, last login, role, active status, and profile.

Step 23: Verify assigned user details

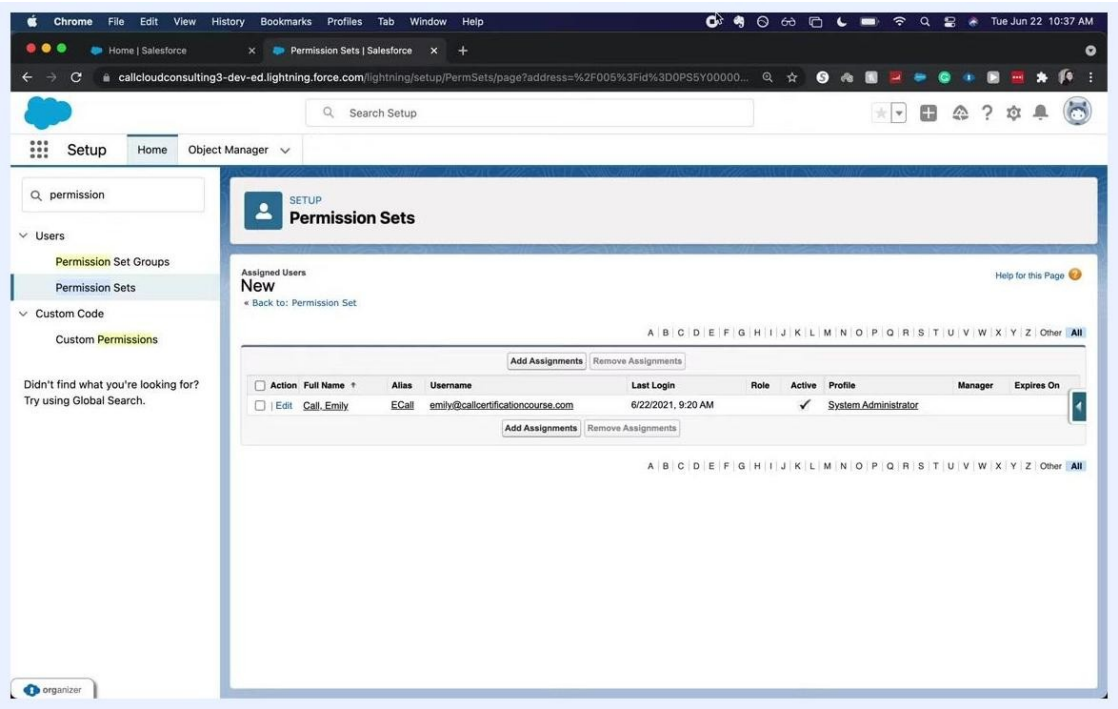
On the Permission Sets page, under Assigned Users, confirm that the intended users are listed along with their alias, username, last login date, active status, and profile. Use Add Assignments and Remove Assignments to manage user assignments, or click Edit next to a user's name to modify their assignment details.



Salesforce Permission Sets page showing the assigned user's details, including alias, username, last login, active status, and profile.

Step 24: Confirm the assignment is complete

Make sure all intended users appear under Assigned Users for the permission set. If you need to add more users, use Add Assignments. To remove a user, select the checkbox next to their name and click Remove Assignments. Use the alphabetical navigation at the top and bottom of the user list to quickly find users by their first letter.



Permission Sets page with assigned user details and assignment management options, confirming the process is complete.

Summary

You have now learned how to create a permission set in Salesforce, configure its object and field-level permissions, review its available permission categories, and assign it to specific users. Regularly review and update permission set assignments as your team's needs and your Salesforce organization evolve to ensure users retain the correct level of access for their roles.