

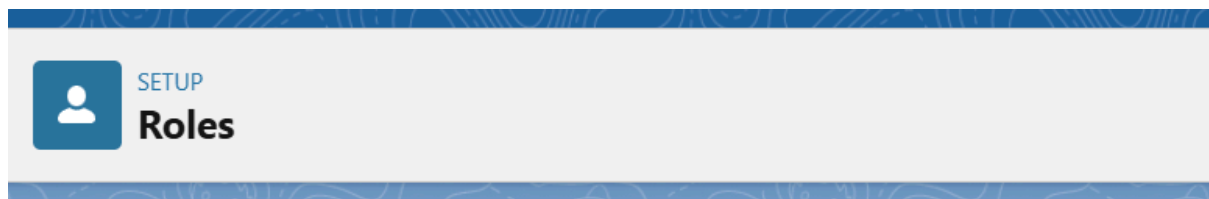
Green Energy Usage Monitor - Phase 2

Phase 2 Completion Document

Step 1: Define Clear Role Requirements

The first step was to define what each role—Manager, Technician, and Customer—should be able to do within the Salesforce system.

- The Manager has full access to manage all operations, approve user requests, and view detailed reports.
- The Technician has access specifically to maintenance-related tasks and updates on technical issues to carry out their responsibilities effectively.
- The Customer is given limited access, primarily to view their own data and submit or view service requests related to their accounts.

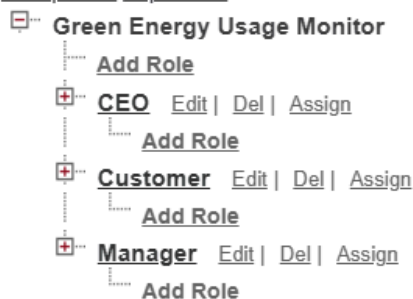


Creating the Role Hierarchy

You can build on the existing role hierarchy shown on this page. To insert a new role, click **Add Role**.

Your Organization's Role Hierarchy

[Collapse All](#) [Expand All](#)



Step 2: Create or Confirm Profiles for Each Role

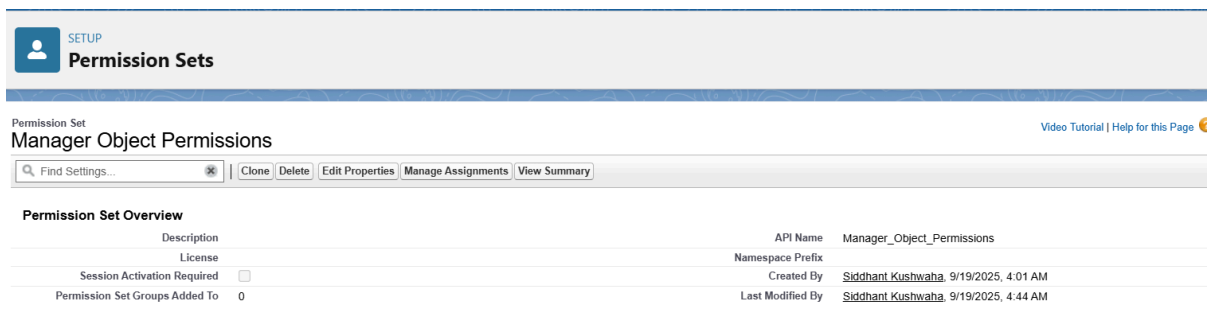
For these roles, profiles were created or confirmed in Salesforce by cloning standard profiles and customizing them:

- The Standard User profile was cloned and customized for the Manager and Technician roles to adjust access and permissions accordingly.
 - A limited profile similar to the Customer Community User was cloned or created for the Customer role to restrict access strictly to appropriate data and functionality.
- These profiles act as templates that govern user permissions and accessibility aligned with their respective roles.

Step 3: Assign Object Access Permissions for Standard Objects

Since no custom objects were created, the focus was on standard Salesforce objects.

- Managers were given full Create, Read, Update, and Delete (CRUD) permissions on Accounts, Contacts, Cases, and Tasks/Events to manage customer data and business operations fully.
- Technicians received read-only permission on Account records, limited read and edit access on related Contacts, and read/edit access for assigned Cases and Tasks to handle maintenance efficiently.
- Customers were restricted to read only their own Accounts, allowed to read and edit their own Contact records, and permitted to create and view their own Cases, with minimal or no access to Tasks.



The screenshot shows the Salesforce Setup interface for a Permission Set named 'Manager Object Permissions'. The page includes a search bar, action buttons (Clone, Delete, Edit Properties, Manage Assignments, View Summary), and a table with the following details:

Permission Set Overview		API Name	Manager_Object_Permissions
Description		Namespace Prefix	
License		Created By	Siddhant Kushwaha, 9/19/2025, 4:01 AM
Session Activation Required	<input type="checkbox"/>	Last Modified By	Siddhant Kushwaha, 9/19/2025, 4:44 AM
Permission Set Groups Added To	0		

Step 4: Configure Field-Level Security

Field-level security was reviewed and configured to protect sensitive data across objects such as Account, Contact, and Case. Managers were granted full visibility and edit rights on relevant fields. Technician profiles were limited to technical and relevant fields, some as read-only. Customer profiles were restricted to visibility of necessary fields related to their own data, with sensitive internal fields hidden to safeguard information security.

Fields & Relationships

9 Items, Sorted by Field Label

FIELD LABEL	FIELD NAME	DATA TYPE
Created By	CreatedById	Lookup(User)
Device ID	Device_ID__c	Text(50)
Device Type	Device_Type__c	Picklist
Energy Device Name	Name	Text(80)
Installation Date	Installation_Date__c	Date
Last Modified By	LastModifiedById	Lookup(User)
Location	Location__c	Text(100)
Owner	OwnerId	Lookup(User,Group)
Status	Status__c	Picklist

Step 5: Set Tab Visibility in Profiles

Profiles were customized to display tabs relevant only to each role’s functions. Managers were able to see all Sales and Service-related tabs, Technicians saw tabs related to Cases, Tasks, and Accounts necessary for maintenance duties, and Customers were given minimal access to tabs related to service requests or portals specific to customer use.

SETUP

Profiles

Profile

System Administrator

Help for this Page

Users with this profile have the permissions and page layouts listed below. Administrators can change a user's profile by editing that user's personal information.

If your organization uses Record Types, use the Edit links in the Record Type Settings section below to make one or more record types available to users with this profile.

Login IP Ranges [0] | Enabled Apex Class Access [2] | Enabled Visualforce Page Access [0] | Enabled External Data Source Access [0] | Enabled Named Credential Access [0] | Enabled External Credential Principal Access [0] | Enabled Custom Metadata Type Access [0] | Enabled Custom Setting Definitions Access [0] | Enabled Flow Access [0] | Enabled Service Presence Status Access [0] | Enabled Custom Permissions [0]

Profile Detail

EditCloneView Users

Name	System Administrator	Custom Profile	<input type="checkbox"/>
User License	Salesforce	Created By	salesforce.com, inc., 7/21/2025, 10:29 AM
		Modified By	Siddhant Kushwaha, 9/22/2025, 2:03 AM

Page Layouts

Standard Object Layouts	Global	Global Layout [View Assignment]	Location Group Assignment	Location Group Assignment Layout [View Assignment]
	Email Application	Not Assigned [View Assignment]	Macro	Macro Layout [View Assignment]
	Home Page Layout	Home Page Default [View Assignment]	Object Milestone	Object Milestone Layout [View Assignment]
	Account	Account Layout [View Assignment]	Operating Hours	Operating Hours Layout [View Assignment]
	Alternative Payment Method	Alternative Payment Method Layout [View Assignment]	Opportunity	Opportunity Layout [View Assignment]
	Appointment Invitation	Appointment Invitation Layout [View Assignment]	Opportunity Product	Opportunity Product Layout [View Assignment]
	Asset	Asset Layout	Order	Order Layout

Step 6: Assign Profiles to Users

Users created for the project were assigned profiles based on their defined roles. This assignment was verified to ensure that users could not escalate their permissions beyond the intended level, maintaining strict role-based access control..

All Users

Help for this Page

On this page you can create, view, and manage users.

To get more licenses, use the Your Account app. [Let's Go](#)

View: All Users

EditCreate New User

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z Other All

New UserReset Password(s)Add Multiple Users

Action	Full Name	Alias	Username	Role	Active	Profile
<input type="checkbox"/> Edit	Chatter Expert	Chatter	chatty.00d9k000007m3vpuai.fmvuynr125c@chatter.salesforce.com		<input type="checkbox"/>	Chatter Free User
<input type="checkbox"/> Edit Login	EPIC_OrgFarm	OEPIC	epic.79b09b1a7017@orgfarm.salesforce.com		<input checked="" type="checkbox"/>	System Administrator
<input type="checkbox"/> Edit	Kushwaha_Siddhant	cse	cse22_siddhantkushwaha491@agentforce.com		<input checked="" type="checkbox"/>	System Administrator
<input type="checkbox"/> Edit Login	Man_Customer1	cust	customer123@example.com	Customer	<input checked="" type="checkbox"/>	Standard Platform User
<input type="checkbox"/> Edit Login	Manager_Hiring1	hman	hiring123@test.com	Manager	<input checked="" type="checkbox"/>	System Administrator
<input type="checkbox"/> Edit Login	Staff_Technician	tsarf	tech123@example.com	Technician	<input checked="" type="checkbox"/>	Green_Technician_Profile
<input type="checkbox"/> Edit	User_Integration	integ	integration@00d9k000007m3vpuai.com		<input checked="" type="checkbox"/>	Analytics Cloud Integration User
<input type="checkbox"/> Edit	User_Security	sec	insightssecurity@00d9k000007m3vpuai.com		<input checked="" type="checkbox"/>	Analytics Cloud Security User

New UserReset Password(s)Add Multiple Users

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z Other All

Step 7: Configure Business Hours and Holidays

Business hours and holiday schedules were verified and configured to control the timing of workflow processes and approval requests accurately. Public holidays were added to prevent automated actions from triggering on non-working days, ensuring the system aligns with operational calendars.

Business Hours (1)

Business Hours Detail

Edit

Business Hours Name	Standard Business Hours	Time Zone
Business Hours	<div> <div>Sunday</div> <div>Monday</div> <div>Tuesday</div> <div>Wednesday</div> <div>Thursday</div> <div>Friday</div> <div>Saturday</div> </div> <div> <div>24 Hours</div> <div>9:00 AM to 6:00 PM</div> <div>9:00 AM to 6:00 PM</div> <div>9:00 AM to 6:00 PM</div> <div>9:00 AM to 6:00 PM</div> <div>9:00 AM to 6:00 PM</div> <div>24 Hours</div> </div>	<div>(GMT+05:30) India Standard Time (Asia/Kolkata)</div> <div>Default Business Hours</div> <div><input type="checkbox"/></div>

Active

☒

Created By

Siddhant Kushwaha

9/19/2025, 2:59 AM

Last Modified By

Siddhant Kushwaha

9/23/2025, 10:29 AM

Edit

Step 8: Setup Sharing Rules

The organization-wide defaults were set to restrict data visibility, predominantly selecting "Private" access to minimize exposure by default. Sharing rules were then established to extend access according to role requirements: Customers can see only their own records, Technicians see records related to their assigned cases or accounts, and Managers have broader visibility across all related data.

<div> <div>SETUP</div> <div>Sharing Settings</div> </div>			
Shipment	Private	Private	✓
Shipping Carrier	Public Read Only	Private	✓
Shipping Carrier Method	Public Read Only	Private	✓
Shipping Configuration Set	Public Read Only	Private	✓
Streaming Channel	Public Read/Write	Private	✓
Tableau Host Mapping	Public Read Only	Private	✓
User Presence	Public Read Only	Private	✓
User Provisioning Request	Private	Private	✓
Waitlist	Private	Private	✓
Web Cart Document	Private	Private	✓
Work Order	Private	Private	✓
Work Plan	Private	Private	✓
Work Plan Template	Private	Private	✓
Work Step Template	Private	Private	✓
Work Type	Private	Private	✓
Work Type Group	Public Read/Write	Private	✓
Device Assignment	Controlled by Parent	Controlled by Parent	
Energy Device	Public Read/Write	Private	✓
Energy Usage Record	Controlled by Parent	Controlled by Parent	
Mentor	Public Read/Write	Private	✓
Personnel	Public Read/Write	Private	✓
Student	Public Read/Write	Private	✓

Step 9: Test User Access

Testing of user access was conducted using the "Login As" feature to simulate login as different role users—Manager, Technician, and Customer. This testing confirmed users could only view and modify data permitted by their profiles and associated sharing rules. Tab visibility and field-level restrictions were also verified to be in effect as configured.