Day -11 All Star Ranger

Here is the same blog in clean plain text format for easy copy-paste:

Understanding Salesforce Security: A Complete Guide to Access Control

Security in Salesforce is built on a layered model. Instead of relying on one single setting, Salesforce combines multiple mechanisms to control who can see what and do what inside the system.

This guide explains the key pillars of Salesforce access control:

Control Access to Org

Control Access to Objects

Control Access to Fields

Org-Wide Defaults (OWD), Sharing Rules, Manual Sharing

Permission Sets and Permission Set Groups

Muted Permission Sets

Let's break them down.

Control Access to the Org (Authentication Level)

This is the first layer of security - controlling who can log in and when.

Key Components:

Profiles

Profiles define:

Login hours

Login IP ranges

App access

System permissions

Every user must have one profile.

Login IP Ranges

Restrict users so they can only log in from approved IP addresses.

Example: Office network only or VPN-based access.

Login Hours

Define specific hours during which users can log in.

Example: Support team can log in only from 8 AM - 6 PM.

Multi-Factor Authentication (MFA)

Adds extra security by requiring an authenticator app, SMS verification, or security key.

Org access answers this question: Can the user enter Salesforce?

Control Access to Objects (Object-Level Security)

Once inside Salesforce, users need permission to access objects like Accounts, Contacts, Opportunities, or Custom Objects.

Controlled Through:

Profiles

Profiles define Create, Read, Edit, Delete (CRED) permissions and also View All and Modify All.

Permission Sets

Used to grant additional object access without changing the profile.

Example: A Sales Rep profile allows Read and Edit on Opportunities, but one user needs Delete access. Instead of modifying the profile, assign a permission set.

Object access answers this question: Can the user see or modify this object?

Control Access to Fields (Field-Level Security)

Even if users can access an object, they might not be allowed to see certain fields.

Example:

Salary field on Employee object

Commission field on Opportunity

Social Security Number

Controlled Through:

Profiles

Permission Sets

You can:

Make a field visible

Make it read-only

Hide it completely

If a field is hidden at field-level security, it will not appear in page layouts, reports, list views, or the API.

Field access answers this question: Can the user see or edit this specific field?

Record-Level Security

Even if a user has object access, they may not see every record. This is controlled through:

Org-Wide Defaults (OWD)

Role Hierarchy

Sharing Rules

Manual Sharing

Org-Wide Defaults (OWD)

OWD sets the baseline level of access for records. Options include:

Private

Public Read Only

Public Read/Write

Controlled by Parent

Example:

If Opportunity OWD is set to Private, users can only see records they own.

Think of OWD as the most restrictive default access.

Role Hierarchy

Users higher in the role hierarchy automatically get access to records owned by users below them.

Example:

Sales Rep → Manager → Director

The Manager can see Sales Rep's records.

Role hierarchy grants record visibility upward.

Sharing Rules

Used to automatically extend access beyond OWD.

Two types:

Owner-Based Sharing Rules

Criteria-Based Sharing Rules

Example:

Share all Accounts owned by West Region with Marketing Team.

Share all Opportunities where Amount > 100,000 with Finance.

Sharing rules open access horizontally.

Manual Sharing

Allows record owners (or users with permission) to manually share a specific record with another user or group.

Example:

A sales rep shares one Opportunity with the Legal team.

Manual sharing is record-by-record sharing.

Permission Sets and Permission Set Groups

Permission Sets

Permission Sets give additional permissions to users without changing their profile.

Use cases:

Temporary access

Special project access

Extra object permissions

System permissions such as Export Reports

Think of a profile as base access.

Think of a permission set as extra access.

Permission Set Groups

Permission Set Groups bundle multiple permission sets together.

Instead of assigning five permission sets individually, you assign one permission set group.

Example:

A Sales User Group may include:

Opportunity Access

Lead Access

Campaign Member Access

Report Export Access

This makes access management easier and more scalable.

Muted Permission Sets

Muted Permission Sets are used inside Permission Set Groups.

They allow you to remove specific permissions from a permission set group.

Example:

A permission set group gives Delete access to Opportunities.

However, a subgroup of users should not delete Opportunities.

Instead of creating a new group, you add a Muted Permission Set and mute the Delete permission.

This helps:

Avoid duplication

Maintain cleaner architecture

Improve scalability

How Everything Works Together (Layered Security Model)

Salesforce security works in layers:

Org Access - Can the user log in?

Object Access - Can the user access the object?

Field Access - Can the user see or edit specific fields?

Record Access - Can the user see specific records?

Additional Access - Permission Sets and Groups

All layers must allow access. If one layer blocks it, access is denied.

Real-World Example

User: Sales Rep

Profile: Sales User

OWD: Opportunity = Private

Role: Sales Rep under Sales Manager

Permission Set: Discount Approval Access

Result:

Can log in

Can access Opportunities

Can edit allowed fields

Can see own records

Manager can see their records

Gets extra approval permissions from permission set

Everything works together.

Best Practices

Keep OWD as restrictive as possible (Private when possible)

Use Permission Sets instead of cloning profiles

Minimize the number of profiles

Use Permission Set Groups for scalability

Document your security model

Test access using the Login As feature

Conclusion

Salesforce security is powerful because it is layered:

Authentication (Org Access)

Authorization (Object and Field Access)

Record Visibility (OWD and Sharing)

Flexible Extensions (Permission Sets and Groups)

When designed properly, it ensures data protection, regulatory compliance, operational efficiency, and scalable user management.