Salesforce Admin Certification Study Guide

Configuration and Setup: 15%

■ EXTERNAL SECURITY

Password Policies

Organization-Wide Password Policies (Setup ■ Security Controls ■ Password Policies)

Key Settings:

- Password Length: Minimum 8 characters recommended
- Password Complexity: Can require alphabetical, numeric, uppercase, lowercase, special characters
- Password Expiration: Options: 30, 60, 90, 180 days, 1 year, or Never expires
- Password History: Remembers 3-24 previous passwords (default: 3) - prevents password reuse
- Lockout Effective Period: How long after failed login attempts user is locked out
- Maximum Invalid Login Attempts: Typically 3-10 attempts before lockout
- Obscure Secret Answer: Hides security question answers

Profile-Level Password Policies:

- Override organization-wide settings for specific profiles
- More restrictive than org-wide policies
- Cannot be used to make policies less strict

Exam Tips:

- Password policies can be set at BOTH organization and profile level
- Profile settings OVERRIDE organization settings
- Users with "Password Never Expires" permission are exempt
- When you expire all passwords, users must reset on next login
- Password history is NOT saved until you set a value

IP Restrictions

Two Types of IP Controls:

1. Trusted IP Ranges (Organization-Level)

- Setup ■ Network Access
- Users logging in from trusted IPs bypass identity verification
- No verification code required
- Does NOT restrict login, just removes extra authentication step
- Benefits: Allows easy login for office networks/VPN

2. Login IP Ranges (Profile-Level)

- More restrictive than Trusted IPs
- Defined on each profile
- BLOCKS login attempts from IPs outside the range
- If IP restrictions exist on profile, login from outside range is DENIED

Important Distinctions:

- Trusted IPs = Make login easier (skip verification)
- Login IP Ranges = Restrict access (block login)
- Profile-level restrictions override org-level settings

Session Settings:

- "Enforce login IP ranges on every request" - applies restrictions to all requests, not just login

Exam Scenario:

- Question: "Which feature restricts a user's ability to log into Salesforce?"
- Answer: Login Hours & Login IP Ranges (NOT Trusted IP ranges)

Network and Login Settings

Login Hours (Profile-Level)

- Setup ■ Profiles ■ Select Profile ■ Login Hours
- Restricts WHEN users can log in
- Based on Pacific Time (or org default timezone)
- If users are logged in when hours end: they can VIEW current page but CANNOT take further actions
- Used for security (e.g., support users only during business hours)

Session Settings (Setup ■ Session Settings)

- Session Timeout: 15 minutes to 24 hours of inactivity
- Can be set at Organization-level (default: 2 hours)
- Can be set at Profile-level (overrides org-level)
- Security best practice: 2 hours or less
- Force logout on session timeout: Yes/No
- Session security levels: High Assurance, Low Assurance

Exam Key Point:

- Profile session settings OVERRIDE organization session settings
- Login Hours evaluated separately from IP restrictions

■ INTERNAL SECURITY

Profiles

Mantra: "Profiles DO" (control what users can DO)

What Profiles Control:

- CRED Permissions: Create, Read, Edit, Delete on objects
- Object-level permissions: Which objects users can access
- Field-level security: Which fields are visible/editable
- Page layout assignments: Which layouts users see
- Record type assignments: Which record types are available
- Tab settings: Which tabs are visible/hidden/default
- Administrative permissions: Modify All Data, Customize Application, etc.
- General user permissions: Run Reports, Export Reports, etc.
- Login hours and Login IP ranges
- Session settings: Timeout duration
- Password policies: Can override org-wide settings

Key Facts:

- Every user MUST have exactly ONE profile
- Cannot delete standard profiles
- Can clone profiles to create custom ones

- Standard Profiles: System Administrator, Standard User, Read Only, Marketing User, Contract Manager, Solution Manager

Exam Tip:

- System Administrator profile has full access: View All, Modify All, and ultimate permissions
- Profiles define BASELINE permissions
- Profiles can ONLY RESTRICT, not expand beyond license limits

---

Permission Sets

Purpose: Add permissions BEYOND what profile provides

Key Characteristics:

- Used to extend permissions, NOT restrict them
- Users can have MULTIPLE permission sets (or none)
- Do NOT require changing the user's profile
- Great for temporary or specialized access
- Task-based and flexible

Common Use Cases:

- Few users need special permissions across different profiles
- Temporary access to specific features
- Access to managed packages (e.g., CPQ)
- Users need access to specific objects/fields not in their profile

Best Practice:

- Keep profiles simple and restrictive
- Use permission sets for nuanced access needs
- Avoids "profile chaos" (too many profiles)

Permission Set Groups:

- Collections of permission sets
- Assign multiple permission sets at once
- Useful for complex role requirements

Exam Tip:

- Permission sets ONLY grant additional permissions

- They CANNOT restrict or remove permissions from profiles
- Most permissive setting always wins (profile + permission sets)

Roles and Role Hierarchy

Mantra: "Roles SEE" (control what users can SEE)

Purpose: Control record-level visibility in hierarchical structure

How It Works:

- Users higher in hierarchy can access records owned by users below them
- Follows "parallel record sharing" concept
- ONLY grants MORE access upward, never restricts
- Does NOT have to match org chart (based on data access needs)

Key Points:

- CEO can see Sales Director's records
- Sales Director can see Sales Manager's records
- Sales Manager can see Sales Rep's records
- Sales Reps CANNOT see each other's records (unless OWD allows)
- Users at SAME level cannot see each other's data through role hierarchy alone

Role vs. Position:

- Roles are about DATA ACCESS, not job titles
- One user can only have ONE role at a time
- Roles work WITH org-wide defaults (OWD) to control visibility

Grant Access Using Hierarchies:

- Setting on OWD for each object
- When enabled: role hierarchy applies
- When disabled: role hierarchy does NOT grant access

Exam Scenario:

- If OWD is Private + Role Hierarchy enabled = Managers see subordinates' records
- If OWD is Private + Role Hierarchy disabled = Only record owner sees record

---

Organization-Wide Defaults (OWD)

The FOUNDATION of Record-Level Security

Golden Rule: OWD should be set to the MOST RESTRICTIVE level

Access Levels:

1. Private: Only record owner, users above in role hierarchy, and admins
2. Public Read Only: All users can VIEW, only owner can EDIT
3. Public Read/Write: All users can VIEW and EDIT
4. Public Read/Write/Transfer: All users can VIEW, EDIT, and TRANSFER ownership (specific objects)
5. Controlled by Parent: (Master-Detail only) access determined by parent record

Critical Concepts:

- OWD sets the BASELINE (most restrictive level)
- Other sharing tools can ONLY grant MORE access, never less
- Cannot be used to restrict access beyond OWD setting
- Different OWD per object (Accounts, Contacts, Opportunities, etc.)

The Sharing Model Hierarchy (Opening Access):

1. OWD ■ Most restrictive baseline
2. Role Hierarchy ■ Opens access upward
3. Sharing Rules ■ Opens access horizontally (criteria-based or ownership-based)
4. Manual Sharing ■ Opens access on individual records
5. Teams ■ Opens access to team members (Account Teams, Opportunity Teams, Case Teams)

Exam Key Points:

- OWD + Profiles work together but are different:

- OWD = Record-level access (WHO can see WHICH records)

- Profile = Object-level permissions (WHAT actions users can perform)

- User must have object permissions (profile/permission set) PLUS record access (OWD/sharing) to see a record
- If OWD is Public Read/Write, sharing rules/role hierarchy have NO effect

---

Sharing Rules

Purpose: Open access beyond OWD without changing OWD setting

Two Types:

1. Ownership-Based Sharing Rules

- Share records owned by certain users/roles with other users/roles
- Example: Share all opportunities owned by Sales Reps with Sales Managers

2. Criteria-Based Sharing Rules

- Share records meeting certain criteria with specified users/roles
- Example: Share all accounts in California with West Region team

Key Facts:

- Can grant Read Only or Read/Write access
- CANNOT be more restrictive than OWD
- Only grant ADDITIONAL access
- Can share with: Public Groups, Roles, Roles and Subordinates

Exam Tip:

- Sharing rules work horizontally (across hierarchy)
- Cannot use sharing rules to restrict access
- If OWD is Public Read/Write, sharing rules are unnecessary

Manual Sharing

One-off record sharing

- Share specific record with specific user
- Can be done by: Record owner, users above owner in role hierarchy, System Admin
- Useful for exceptions and temporary needs
- Can grant Read Only or Read/Write access

Field-Level Security (FLS)

Controls which fields users can see and edit

Where Set:

- Profiles: Object Settings ■ Field Permissions
- Permission Sets: Field Permissions

Two Settings per Field:

- Visible: User can see the field
- Editable: User can edit the field (requires visible)

Key Points:

- FLS is UNIVERSALLY enforced (page layouts, related lists, reports, API, etc.)
- Overrides page layout settings
- Most secure way to protect sensitive data
- If FLS is hidden, field is hidden EVERYWHERE
- If FLS allows view but page layout hides field, user CANNOT see field (page layout wins for visibility)
- If FLS is read-only, field CANNOT be edited even if page layout allows

Best Practice:

- Use FLS for security (sensitive/confidential fields)
- Use Page Layouts for user experience (organizing fields)

Exam Scenario:

- Question: "How to ensure HR can edit Salary field but Sales cannot see it?"
- Answer: Set FLS on Salary field (HR: visible & editable, Sales: not visible)

■ VISIBILITY & ACCESS

Record Types

Purpose: Offer different business processes, picklist values, and page layouts

What Record Types Control:

- Page Layout Assignment: Different layouts for different processes
- Picklist Values: Different picklist options per record type
- Business Processes: Different stages/paths (e.g., Sales Process, Support Process, Lead Process)

Key Facts:

- One record type per record
- Assigned to profiles (profile determines which record types users can access)
- Each record type can have ONE sales process (or support process, lead process, etc.)

- Must create record type BEFORE assigning to profiles
- Users can have access to multiple record types
- Can set default record type per profile

Common Use Cases:

- Different sales processes for different product lines
- Different support processes for different case types
- Different lead processes for different lead sources

Exam Scenario:

- "Sales team needs 3 different processes for Opportunities based on account size, requiring different stages and different data"
- Answer: Need 3 record types (one per process) + 3 page layouts + 3 sales processes

---

Page Layouts

Purpose: Control the UI and user experience

What Page Layouts Control:

- Field placement and organization
- Section organization and labels
- Field properties: Visible, Read-Only, Required
- Related lists and their order
- Buttons (standard and custom)
- Custom links
- Quick Actions and Mobile Actions
- JavaScript buttons

Key Facts:

- One page layout per profile per record type per object
- If no record types: one page layout per profile
- Can assign same layout to multiple profiles
- Field-level security OVERRIDES page layout
- Can make fields required on page layout (but not as secure as validation rules)

Page Layout vs FLS:

- FLS: Security-focused, enforced everywhere
- Page Layout: UI-focused, only affects detail/edit pages

Exam Key Point:

- To make field required for ALL users: Validation Rule or make field required at object level
- To make field required for SOME users: Page Layout (but only enforces on UI, not API)
- For true security: Use FLS + Page Layout together

Tab and App Settings

Tabs (Profile Settings):

- Default On: Tab visible and selected by default
- Default Off: Tab visible but not selected
- Tab Hidden: Tab not visible in app

Apps:

- Collections of tabs
- Users can switch between apps
- Different apps for different functions (Sales, Service, Custom Apps)
- App Launcher: Shows all available apps

Exam Tip:

- Hiding a tab doesn't restrict object access
- To fully restrict object: Use profile object permissions

■ ORG INFORMATION & SETTINGS

Company Information

Location: Setup ■ Company Information

Key Information:

- Organization ID: Unique 15-character identifier
- Organization Name: Company name
- Default Locale: Language, timezone, currency

- Licenses: View all license types and usage

- User licenses (Salesforce, Platform, Chatter, etc.)

- Feature licenses (Marketing User, Service Cloud User, etc.)

- Permission Set Licenses

- Fiscal Year: Define fiscal year for org
- Business Hours: Default business hours
- Storage Usage: Data and File storage limits

License Types (Common):

- Salesforce License: Full CRM access (Leads, Opportunities, Accounts, etc.)
- Platform License: Custom apps, NO standard CRM objects (no Opportunities, Forecasts)
- Chatter Free: Only Chatter, no Salesforce records
- Chatter Plus: Chatter + Files, no CRM
- Community Licenses: External users (Customer Community, Partner Community)

Exam Tips:

- One user license per user
- Multiple feature licenses per user (additive)
- View license counts in Company Information
- Cannot change org ID
- Profiles are tied to license types

Business Hours

Purpose: Define when your org/support team operates

Key Uses:

- Escalation rules (cases escalate only during business hours)
- Entitlement processes (SLA countdowns run only during business hours)
- Milestones (case milestones track business hours)
- Assignment rules (can consider business hours)

Business Hours Settings:

- Time Zone: Determines daylight savings
- Hours: Start/end time for each day of week
- 24 Hours: Full day coverage option

- Active: Must be active to use
- Default: One set can be default for org

Multiple Business Hours:

- Can create multiple sets (e.g., APAC, EMEA, Americas)
- Assign different hours to different cases/entitlements
- Support global organizations

Holidays:

- Associate up to 1,000 holidays with each business hours set
- Can be recurring (every year) or one-time
- Can be all-day or specific time range
- Holidays SUSPEND business hours (escalation rules pause, milestone countdowns pause)

Exam Key Point:

- Business hours on cases follow hierarchy:

1. Milestone business hours (if set)
2. Entitlement process business hours (if milestone not set)
3. Case business hours (if neither above set)
4. Org default business hours (if none above set)

Locale Settings

User Personal Settings:

- Language: Interface language
- Timezone: User's timezone (affects date/time display)
- Locale: Date format, number format, currency display
- Email Encoding: Character set for emails

Organization Default Settings:

- Sets default for all new users
- Individual users can override in personal settings

Fully Supported Languages:

- Translation for all UI elements, help docs
- Examples: English, French, German, Spanish, Japanese

End User Languages:

- Partial translation (less than full support)
- Core features translated

■■ END-USER CHANGES

What Users Can Change (Personal Settings)

Users can self-service update:

- Name (first, last)
- Email address
- Phone number
- Timezone
- Locale (date/number format)
- Language
- Password (reset own password)
- Security question
- Email notifications preferences
- Mobile device activation

What Users CANNOT Change:

- Username
- Profile
- Role
- License
- Permission sets

Exam Tip:

- Users can reset their OWN password if "Password Never Expires" permission is not set
- Admin can reset any user's password
- Users can update personal info but NOT security settings (profile, role)

App Navigation Customization

Users Can:

- Reorder tabs in personal settings
- Choose which app appears on login
- Customize list views (create personal views)
- Set up personal calendar settings

Admins Control:

- Available tabs per profile
- Available apps per profile
- Default app assignment

■ TROUBLESHOOTING & AUDITING

Setup Audit Trail

Purpose: Track configuration changes in Setup

What It Tracks:

- User creation/changes (profiles, permission sets, roles)
- Field-level security changes
- Object and field creation/deletion
- Validation rule changes
- Workflow and Flow changes
- Sharing rule changes
- OWD changes
- Apex class/trigger changes
- Login-As activity (tracks delegate user)
- Mass transfers
- Data imports

Key Details:

- Shows last 20 entries in UI
- Can download last 6 MONTHS (180 days) as CSV
- Location: Setup ■ Security Controls ■ View Setup Audit Trail
- Fields tracked: Date, User, Action, Section, Delegate User (if Login-As used)

- ONLY tracks metadata changes, NOT record data changes (except some specific data operations)

What It Doesn't Track:

- Specific code changes within Apex (just that class was changed)
- Specific field values in records (use Field History Tracking for that)
- Some custom development details

Exam Scenario:

- Question: "Admin needs to see who changed a profile's field-level security last week"
- Answer: Setup Audit Trail
- Question: "View last 8 months of setup changes"
- Answer: Can only download 6 months (180 days)

Login History

Purpose: Track user login activity

What's Tracked:

- User login times
- IP address of login
- Login type (Salesforce UI, API, etc.)
- Browser/device
- Success or failure
- Source (organization, community, etc.)

Location: Setup ■ Login History

- View recent logins
- Download up to 6 months of data

Use Cases:

- Security auditing
- Unusual login activity detection
- Compliance reporting
- IP address verification

Session Settings

Key Security Settings:

Session Timeout:

- Org-level: Setup ■ Session Settings
- Profile-level: Profile ■ Session Settings
- Automatically logs out inactive users
- Best practice: 2 hours or less
- Profile setting overrides org setting

Force Relogin After Timeout:

- Requires users to re-enter password
- Not just "are you still there?" prompt

Lock Sessions to IP:

- Session tied to specific IP address
- Prevents session hijacking
- Can cause issues with VPN/proxy

Enforce Login IP Ranges:

- "Enforce login IP ranges on every request"
- Applies profile IP restrictions to every API call and page request
- More secure but can impact integrations

Require Secure Connections (HTTPS):

- All connections must use HTTPS
- Industry standard, should always be enabled

Exam Key Point:

- Session timeout can be set at org and profile level
- Profile session timeout OVERRIDES org timeout
- For maximum security: Short timeout + force relogin + IP locking

---

■ EXAM STRATEGY & KEY CONCEPTS

Critical Distinctions

1. Profiles vs. Permission Sets

- Profiles: ONE per user, baseline permissions, includes login restrictions
- Permission Sets: Multiple per user, additive only, no login restrictions

2. Roles vs. Profiles

- Roles: Data VISIBILITY (what records users can SEE)
- Profiles: Data PERMISSIONS (what users can DO)

3. Trusted IPs vs. Login IP Ranges

- Trusted IPs: Skip verification code (convenience)
- Login IP Ranges: Block logins (security)

4. OWD vs. Sharing Rules

- OWD: Baseline (most restrictive)
- Sharing Rules: Open access beyond OWD

5. Page Layout vs. FLS

- Page Layout: UI/UX (field placement, required on form)
- FLS: Security (enforced everywhere)

6. Record Types vs. Page Layouts

- Record Types: Different processes + picklists + page layouts
- Page Layouts: Just UI organization

Common Exam Scenarios

Scenario 1: "Support users should only login during business hours"

- Answer: Set Login Hours on Support Profile

Scenario 2: "Sales users need to see different fields than Service users"

- Answer: Create different page layouts, assign to profiles (or use record types)

Scenario 3: "Manager should see all records of their team"

- Answer: Use Role Hierarchy (manager role above team role) + OWD set to Private with "Grant Access Using Hierarchies" enabled

Scenario 4: "3 users need temporary access to a custom app"

- Answer: Create Permission Set with app access, assign to those 3 users

Scenario 5: "HR needs to edit salary field, Sales cannot see it"

- Answer: Field-level security (HR: visible & editable, Sales: not visible)

Scenario 6: "Track who changed the profile settings last week"

- Answer: Setup Audit Trail

Scenario 7: "User can login from office but not home"

- Answer: Login IP Ranges on profile (restrict to office IPs)

Scenario 8: "All users should have strong passwords"

- Answer: Organization-wide password policies

Quick Reference: Where to Find Things

- Password Policies: Setup ■ Security Controls ■ Password Policies
- IP Settings:

- Trusted IPs: Setup ■ Network Access

- Login IPs: Setup ■ Profiles ■ [Profile] ■ Login IP Ranges

- Login Hours: Setup ■ Profiles ■ [Profile] ■ Login Hours
- Session Settings: Setup ■ Session Settings (or Profile)
- Profiles: Setup ■ Users ■ Profiles
- Permission Sets: Setup ■ Permission Sets
- Roles: Setup ■ Roles
- OWD: Setup ■ Security Controls ■ Sharing Settings
- Sharing Rules: Setup ■ Sharing Settings ■ [Object] Sharing Rules
- FLS: Setup ■ Object Manager ■ [Object] ■ Fields ■ [Field] ■ Set Field-Level Security
- Business Hours: Setup ■ Business Hours
- Holidays: Setup ■ Holidays
- Company Info: Setup ■ Company Information
- Setup Audit Trail: Setup ■ Security Controls ■ View Setup Audit Trail
- Login History: Setup ■ Login History

Final Exam Tips

■ Understand the security layers:

- Organization level ■ Profile level ■ User level
- Most restrictive to least restrictive
- Each layer can only restrict further or maintain, not open access (except permission sets)

■ Remember override rules:

- Profile password policy > Org password policy
- Profile session timeout > Org session timeout
- Login IP Ranges BLOCK (Trusted IPs don't block)
- FLS > Page Layout

■ Sharing model hierarchy:

- OWD (baseline) ■ Role Hierarchy ■ Sharing Rules ■ Manual Sharing ■ Teams
- Each step opens MORE access, never restricts

■ One user, one profile, one role, one license:

- But multiple permission sets allowed

■ Record Types = Processes:

- Different processes require record types
- Record types control page layouts and picklists

■ Know time limits:

- Setup Audit Trail: 6 months (180 days)
- Login History: 6 months
- Field History Tracking: 18 months (standard), 24 months (with Field Audit Trail)

■ Security best practices:

- OWD: Most restrictive
- Profiles: Simple and restrictive, use permission sets for exceptions
- Session timeout: 2 hours or less
- Password complexity: Length + variety
- Always use HTTPS

■ Summary Checklist

Before the exam, make sure you can answer:

- [ ] What's the difference between Trusted IPs and Login IP Ranges?
- [ ] How do profiles and permission sets differ?
- [ ] What's the role hierarchy and how does it grant access?
- [ ] What is OWD and why should it be restrictive?
- [ ] Can sharing rules restrict access? (No, only grant)
- [ ] Where is Setup Audit Trail located and what does it track?
- [ ] How long can you download Setup Audit Trail data? (6 months)
- [ ] Can a user have multiple profiles? (No, only one)
- [ ] Can a user have multiple permission sets? (Yes)
- [ ] What happens when a user's login hours end while they're logged in?
- [ ] What's the difference between Field-Level Security and Page Layouts?
- [ ] How do record types and page layouts work together?
- [ ] Where do you view available licenses? (Company Information)
- [ ] What's the purpose of business hours in Salesforce?
- [ ] Can profile password policies be less restrictive than org-wide? (No)

Good luck on your exam! ■