Salesforce Advanced Admin Exam Study Guide: Topic 1 - Security and Access (20%)

Salesforce Basics: For Advanced Admin Newbies

If you're stepping into the Advanced Admin world or just starting this epic journey, don't panic—here's a colossal, ultra-welcoming intro to get you hyped, cozy, and ready to roll with confidence.

- **What is Salesforce Advanced Admin?**
    - It's the ultimate level of Salesforce mastery—an online platform where you transform your org into a locked-down, enterprise-grade fortress, mastering advanced security, data, changes, analytics, custom objects, content, automation, mobile, service, deployment, and beyond, all in the cloud with no tech disasters required.
    - Picture it as your business's security superhero—like a genius gatekeeper who controls who sees what, protects data like a vault, and keeps the org running smoothly, building on your basic Admin skills to tackle enterprise complexity.
- **Why It's a Total Game-Changer**:
    - It goes way beyond basic logins—like adding a user—and dives into hardcore security: profiles, roles, sharing rules, field-level access, and more to safeguard data and customize visibility. It's like upgrading from a padlock to a high-tech security system—your team gets what they need, and nothing they don't, no leaks, no chaos.
    - As an Advanced Admin, you're the security architect—designing access like a master strategist, teaching a super-smart robot to enforce rules with precision while keeping 1,000 users in check.
- **Key Words to Start With**:
    - **Org**: Your company's Salesforce universe—like your team's high-tech castle where data lives and security rules reign.
    - **Setup**: The control hub (top-right gear icon) where you lock it down—like the security console of your Salesforce spaceship, giving you the tools to build walls and open doors.

  - **CRM**: Customer Relationship Management—the heart of Salesforce, now with advanced security to protect every customer detail like gold.

- **What This Topic Is All About**:
  - “Security and Access” is your monster deep dive into controlling who gets in, what they see, and what they can do—using profiles, roles, permissions, sharing, and more to secure data at every level (org, object, record, field). It’s like being the chief of your org’s security force, ensuring enterprise-scale protection and user efficiency.

Salesforce Advanced Administrator Certification Study Guide: Security and Access

Overview of Security and Access

The **Security and Access** section focuses on how Salesforce administrators configure and manage data security to ensure that users can only access the data they need while protecting sensitive information. It tests your ability to implement advanced security features, troubleshoot access issues, and apply best practices in real-world scenarios. This section requires a deep understanding of Salesforce’s security model, including sharing settings, profiles, permission sets, and territory management.

Key objectives include:

- Determining implications for record and field data access in various scenarios.
- Understanding the capabilities and implications of territory management.
- Differentiating between custom profiles, permission sets, and delegated administration.

Structure of the Study Guide

1. **Core Concepts** - Explanation of foundational security components.
2. **Detailed Breakdown** - In-depth exploration of each security feature.
3. **Scenario-Based Learning** - Practical examples and use cases.
4. **Summary Table** - Quick reference for key features and their purposes.
5. **Tips and Tricks** - Best practices and exam preparation advice.

6. **Key Terms Glossary** - Definitions of critical terminology.

---

1. Core Concepts

Salesforce Security Model

Salesforce uses a layered security model to control access at various levels:

- **Organization-Level Security**: Controls who can log in (e.g., IP restrictions, login hours).
- **Object-Level Security**: Defines CRUD (Create, Read, Update, Delete) permissions via profiles and permission sets.
- **Field-Level Security (FLS)**: Restricts access to specific fields within an object.
- **Record-Level Security**: Governs which records a user can view or edit (e.g., OWD, sharing rules).

Key Components

- **Profiles**: Define baseline permissions for users (object-level and system permissions).
- **Permission Sets**: Grant additional permissions without altering profiles.
- **Roles**: Control record access via the role hierarchy.
- **Sharing Rules**: Extend access beyond the role hierarchy based on criteria or ownership.
- **Organization-Wide Defaults (OWD)**: Set the default access level for an object (Private, Public Read Only, Public Read/Write).
- **Territory Management**: Manages record access based on account characteristics rather than ownership.

---

2. Detailed Breakdown

2.1 Organization-Wide Defaults (OWD)

- **Definition**: The baseline level of access for all records of an object unless overridden by other settings.

- **Options**:
    - **Private**: Only the record owner and users above them in the role hierarchy can access.
    - **Public Read Only**: All users can view but not edit.
    - **Public Read/Write**: All users can view and edit.
- **Use Case**: For sensitive objects like "Patient Records," set OWD to Private to restrict access to authorized personnel only.
- **Key Consideration**: OWD is the most restrictive layer; other tools (e.g., sharing rules) can only expand access.

2.2 Role Hierarchy

- **Definition**: A tree-like structure where users higher in the hierarchy inherit access to records owned by users below them.
- **Behavior**:
    - Works with Private or Public Read Only OWD.
    - Does not apply if OWD is Public Read/Write (everyone already has access).
- **Grant Access Using Hierarchies**: Can be disabled for custom objects to prevent automatic sharing up the hierarchy.
- **Use Case**: A Regional Manager should see all records owned by Sales Reps in their region.

2.3 Sharing Rules

- **Definition**: Rules that extend record access beyond OWD and role hierarchy based on ownership or criteria.
- **Types**:
    - **Ownership-Based**: Share records owned by one group/role with another (e.g., share all records owned by “East Coast Sales” with “West Coast Sales”).
    - **Criteria-Based**: Share records meeting specific conditions (e.g., share all Opportunities where Amount > $1M with Executives).
- **Access Levels**: Read Only or Read/Write.

- **Use Case**: Share all “High Priority” Cases with a support team, regardless of ownership.

2.4 Manual Sharing

- **Definition**: Allows record owners (or users with “Modify All” permission) to manually share individual records.
- **Use Case**: A Sales Rep shares a specific Opportunity with a colleague for collaboration.
- **Limitation**: Temporary and user-driven; not scalable for large datasets.

2.5 Profiles

- **Definition**: Mandatory settings that define a user’s baseline permissions (e.g., object access, app visibility, system permissions).
- **Key Features**:
    - Assigned to every user (one profile per user).
    - Controls access to objects (CRUD) and fields (via FLS).
- **Use Case**: A “Marketing User” profile grants access to Campaigns but not Opportunities.

2.6 Permission Sets

- **Definition**: Supplemental permissions that extend a user’s access without changing their profile.
- **Key Features**:
    - Can be assigned to multiple users.
    - Ideal for granting temporary or role-specific access (e.g., “Run Reports” for a specific project).
- **Use Case**: Grant “Delete Leads” permission to a small group of users without modifying their “Standard User” profile.

2.7 Field-Level Security (FLS)

- **Definition**: Restricts access to individual fields within an object (e.g., hide “SSN” field from most users).
- **Settings**: Visible, Read-Only, or Hidden.

- **Applied Via**: Profiles or permission sets.
- **Use Case**: Ensure only HR users can see the “Salary” field on the Employee object.

2.8 Territory Management

- **Definition**: An alternative to role-based sharing, organizing record access by account attributes (e.g., geography, industry).
- **Key Features**:
  - Requires enabling in Setup (not available by default).
  - Users are assigned to territories, which grant access to associated accounts and related records (e.g., Opportunities).
- **Implications**:
  - Overrides OWD and role hierarchy for territory-assigned records.
  - Supports forecasting and reporting by territory.
- **Use Case**: A company with sales teams divided by state (e.g., “California Territory”) uses territory management to assign account access.

2.9 Delegated Administration

- **Definition**: Allows specific users to perform admin tasks (e.g., manage users, assign permissions) without full admin access.
- **Key Features**:
  - Configurable per object or feature (e.g., delegate user management for “Sales” app).
  - Reduces admin workload while maintaining control.
- **Use Case**: A team lead manages user accounts for their department without accessing system-wide settings.

2.10 Record Types

- **Definition**: Variations of an object that dictate available fields, layouts, and picklist values.
- **Security Relevance**: Indirectly affects access by controlling what users see/edit, though not a direct security tool.

- **Use Case**: “Internal” vs. “External” Case record types limit field visibility for different user groups.

2.11 Communities/Experience Cloud Security

- **Definition**: Security settings for external users (e.g., partners, customers) in Experience Cloud sites.
- **Key Features**:
  - Sharing sets: Grant access based on role or profile.
  - External OWD: Separate defaults for external users.
- **Use Case**: Partners see only their own Accounts via a sharing set.

---

3. Scenario-Based Learning

Scenario 1: Restricting Access to Sensitive Data

- **Problem**: A company wants only HR users to view employee salary data.
- **Solution**:
  1. Set Employee object OWD to Private.
  2. Use role hierarchy to grant HR managers access to subordinates’ records.
  3. Apply FLS via profiles to hide the “Salary” field from non-HR users.
  4. Use a permission set to grant “View All” on Employee object to HR admins.

Scenario 2: Sharing Across Teams

- **Problem**: Sales Team A needs Read access to Sales Team B’s Opportunities for collaboration.
- **Solution**:
  1. Set Opportunity OWD to Private.
  2. Create an ownership-based sharing rule: Share Opportunities owned by Team A with Team B (Read Only).

Scenario 3: Territory-Based Access

- **Problem**: A company assigns accounts by region and wants sales reps to access only their region's records.
- **Solution**:
    1. Enable Territory Management.
    2. Create territories (e.g., "East Coast," "West Coast").
    3. Assign users to territories and link accounts based on a "Region" field.

---

4. Summary Table

Feature	Purpose	Access Level	Applied Via	Key Considerations
OWD	Sets default object access	Private, Public RO, RW	Object Settings	Most restrictive; can only be expanded
Role Hierarchy	Grants access up the chain	Record-level	Roles	Disabled with "Grant Access Using Hierarchies"
Sharing Rules	Extends access based on criteria/ownership	Read Only, Read/Write	Sharing Settings	Supplements OWD and hierarchy
Manual Sharing	User-driven record sharing	Read Only, Read/Write	Record Action	Not scalable; temporary
Profiles	Baseline object and system permissions	CRUD, FLS	User Assignment	Mandatory for all users
Permission Sets	Supplemental permissions	CRUD, FLS, System	User Assignment	Flexible, reusable
FLS	Restricts field visibility	Visible, Read-Only, Hidden	Profile/Permission Set	Overrides object-level access
Territory	Access by account	Record-level	Territory	Alternative to role-

Feature	Purpose	Access Level	Applied Via	Key Considerations
Management	attributes		Assignment	based sharing
Delegated Administration	Limited admin rights for specific users	Varies	Delegated Admin Groups	Reduces admin burden

---

5. Tips and Tricks

Exam Preparation Tips

- **Understand Scenarios**: The exam will present complex scenarios (e.g., “Given X, Y, Z, what’s the best solution?”). Practice identifying the most efficient tool (e.g., sharing rule vs. permission set).
- **Know the Order of Operations**: Security settings are applied in this order: OWD → Role Hierarchy → Sharing Rules → Manual Sharing.
- **Focus on Territory Management**: It’s a unique feature; know when it’s better than role-based sharing.
- **Practice Hands-On**: Use a Salesforce Developer Edition org to configure OWD, sharing rules, and territories.

Best Practices

- **Least Privilege Principle**: Grant the minimum access necessary for users to perform their jobs.
- **Audit Regularly**: Use tools like Setup Audit Trail and Health Check to monitor security settings.
- **Profiles vs. Permission Sets**: Use profiles for broad roles, permission sets for exceptions or temporary access.

---

6. Key Terms Glossary

- **OWD**: Organization-Wide Defaults - The default access level for an object.
- **FLS**: Field-Level Security - Controls access to specific fields.
- **CRUD**: Create, Read, Update, Delete - Object-level permissions.

- **Sharing Model**: The combination of OWD, roles, and sharing rules that dictates record access.
- **Territory**: A grouping of accounts and users for access management.

Final Notes

The Security and Access section is foundational to the Advanced Administrator certification. Mastering it requires both theoretical knowledge and practical application. Use Trailhead modules (e.g., “Data Security,” “Territory Management Basics”) and hands-on practice to solidify your understanding. For the exam, expect 10-12 questions on this topic, often involving multi-step solutions or troubleshooting access issues.

Good luck, Trailblazer! You’ve got this!