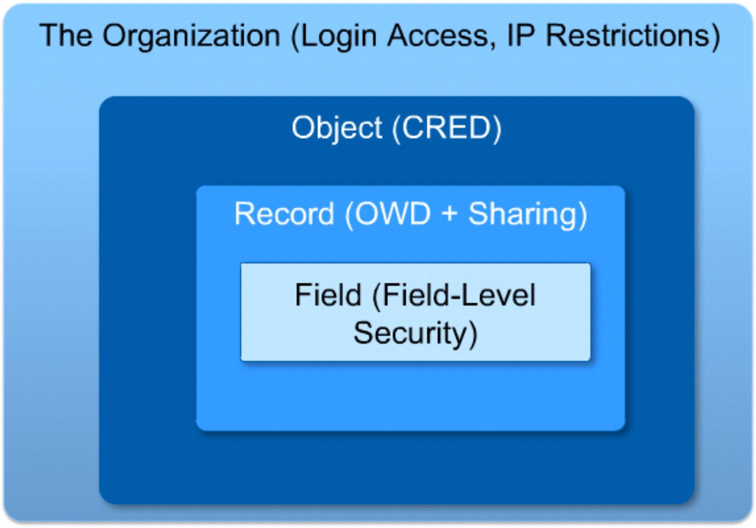
# Troubleshoot Record Access and Field Visibility

Thursday, September 17, 2015 5:44 PM

## Security Access Levels




When opening up access using the role hierarchy, sharing rules, teams, and manual sharing, the most permissive sharing access wins.

When object permissions provide a different level of access than the sharing model, the more restrictive access wins.

## Record Access: Transfers

**Sharing Rules:** All ownership-based sharing rules for the records are recalculated based on Matt's role.

**Teams:** When the record owner is changed through the UI, there is a choice to keep the associated teams. When the record owner is changed through Data Loader, teams remain on the records.

**Manual Sharing:** All manual sharing is removed from the records that were transferred to Matt.

## Record Access: Role Change

**Sharing Rules:** All ownership-based sharing rules for Karl's records are recalculated based on his new role.

**Teams:** No impact

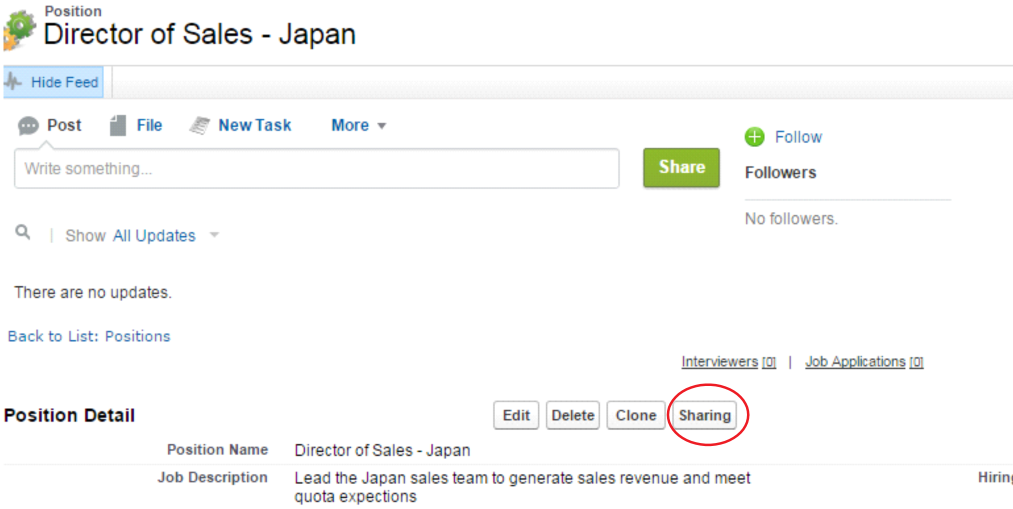
**Manual Sharing:** No impact

The Record owner did not change, so teams and manual sharing weren't impacted.

**Controlled by Parent**
When the Organization-Wide Default Settings are set to: Controlled By Parent, all access is determined by the user's access to the parent account.
Sharing Rules no longer have any impact.

**Best Practices:**
1. Use multiple permission sets to handle one-off permissions, and reduce the need for more custom profiles.
2. Define a hierarchy of roles to control access to information entered by users in lower-level roles.
3. Always assign a user to a role in the role hierarchy.
4. Use public groups to reduce the number of sharing rules.

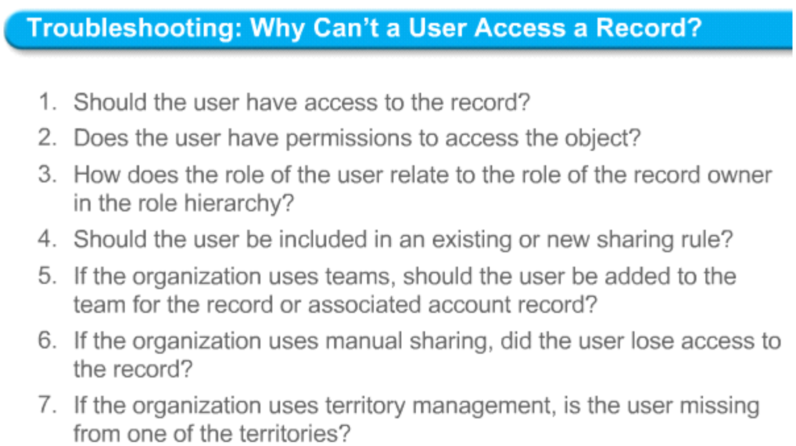
**To view Sharing details, click the "Sharing" button.**

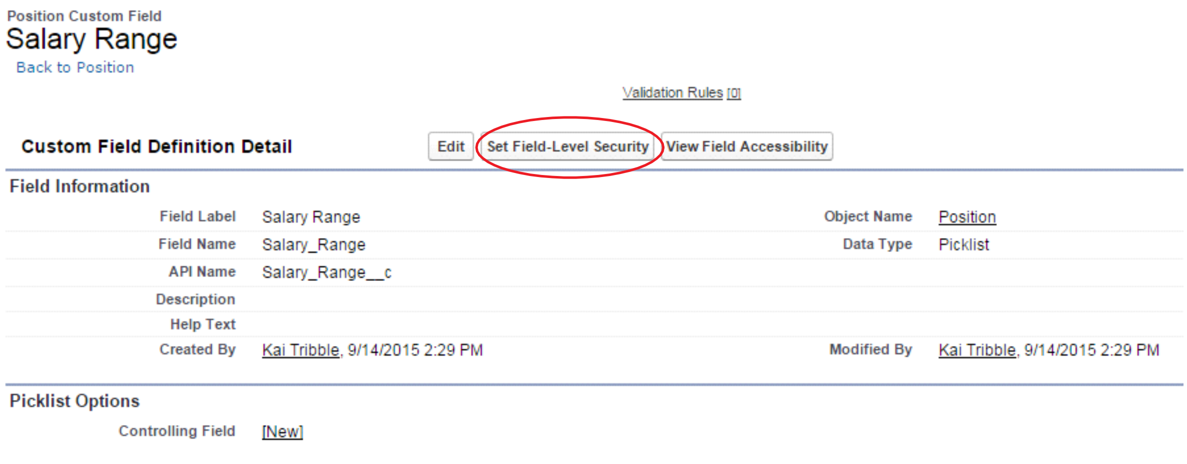



Click "Expand List" in the next page to see who has access to what and why.

**Modify Access to Position Records**
This can be done by creating new "Roles" and assigning these roles to users not based on position in Org Chart, but by access needs. Reset Sharing Rules to regain access rights: **Setup -> Security Controls -> Sharing Settings**

**Restrict Access to the Salary Range Field**
Set Field-Level Security: **Setup -> Objects -> [Object_name] -> Custom Fields and Relationships: [Field_Name] -> Set Field-Level Security**




Note: When using Global Search for troubleshooting for users, click the Search Feeds button to get all recent Chatter Feeds about that user.

**It is more scalable to grant one user access to the Account team rather than give an entire Role access to an Account.**

D. Should the user be included in an existing or new sharing rule?

i. Click **Setup | Security Controls | Sharing Settings.**
ii. Scroll down to the Account Sharing Rules section, and verify that there is not any account sharing rules.
iii. Consider the pros and cons of creating the following criteria-based sharing rule:

```
Account: Account.TextName CONTAINS American Bank shared with
Role: Sales Engineers with Read/Write access to opportunities
```

| Pros | Cons |
|---|---|
| None | All users in the Sales Engineers role would have access to the American Bank account.<br>The solution is not scalable.<br>The sharing rule depends on the value in a text field. |

E. If the organization uses teams, should the user be added to the team for the record or associated account record?

i. Click the Accounts tab.
ii. Click the **American Bank** account.
iii. Click the **Account Team** related list hover link.
iv. Click **Display Access.**
v. Consider the pros and cons of giving Amy Daniels access to all opportunities for the American Bank account by adding her to the account team.

| Pros | Cons |
|---|---|
| It gives her access to all opportunities related to American Bank.<br>If the account owner changes, the account team can be kept on the record. | None |

This is better than giving the User Sharing Settings using the Sharing button at the top of the Opportunity for a particular account because permissions are removed once the Account Owner changes.

An organization may also use Territory Management. Territory Management is an account sharing system that lets users access accounts based on the characteristics of the accounts, such as geography, product line, or business unit. You can assign these Territory Management automatically using **Account Assignment Rules.** When using Territory Management, the territory management hierarchy must also be defined. If a User and an Account have only one Territory in common, the Account is automatically assigned to that territory. Territory access is independent of Account Owner permissions.

| Role Hierarchy | Territory Hierarchy |
|---|---|
| A user has a single role. | A user can be part of many territories. |
| An account is owned by a single user. | An account can belong to multiple territories. |
| Account owners and users above them in the role hierarchy, and those who have access to a child object can access the account. | In addition to users listed in the left column, an account is accessible by all users in territories to which it is assigned, as well as those above them in the territory hierarchy. |
| A user has a single forecast based on role. | A user has a forecast for each territory in which they work with active opportunities. |

- Territory management works in parallel with other sharing functionality.
- Both role and territory hierarchy must be managed simultaneously.
- Forecasts are derived from territory hierarchy, not role hierarchy.
  - Customizable forecasting must be enabled.
  - Forecast data is derived from the opportunities associated with a user's territory.
  - Users will have a different forecast for each territory to which they are assigned.

**Accounts -> [Account_Name] -> Account Team**

**Account Team** Add | Add Default Team | Display Access | Delete All

Account team members may have greater access than defined by their account team membership.

| Action | Team Member | Account Access | Contact Access | Opportunity Access |
|---|---|---|---|---|
| Edit \| Del | Tim Howe | Read Only | Read Only | Private |
| Edit \| Del | Yuko Ishikawa | Full Access | Read/Write | Read/Write |

**Encrypt the Values of a Custom Field**
Create an encrypted custom field for opportunities and add it to the B2C Opportunity Layout:
**Setup -> Customize -> Opportunities -> Fields**
**Custom Fields and Relationships: Text (Encrypted) -> Next**

Field Label: Encrypted Credit Card Numb

Please enter the maximum length for a text field below.

Length: 16

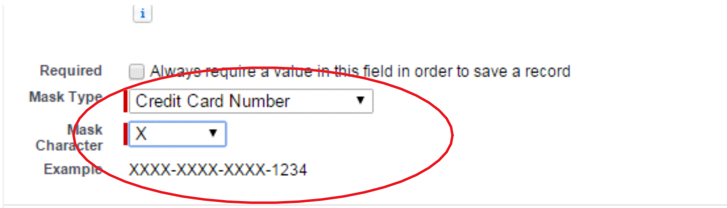
Field Name: Encrypted_Credit_Card_Num

Description: Encrypted Credit Card Number

Help Text:

Required: Always require a value in this field in order to save a record

Mask Type: Credit Card Number

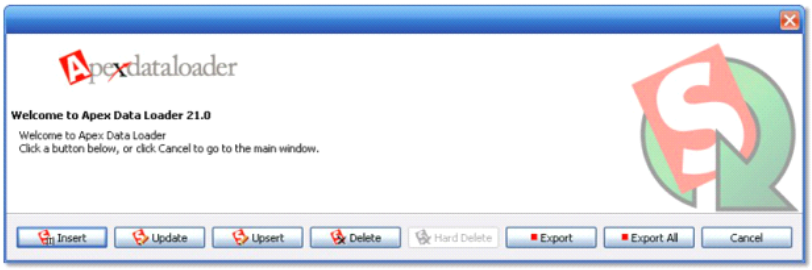



**In order for a Profile to view encrypted data, they must have the System Permission to "View Encrypted Data"**

**Steps to Import Encrypted Data:**

## Export Existing Data

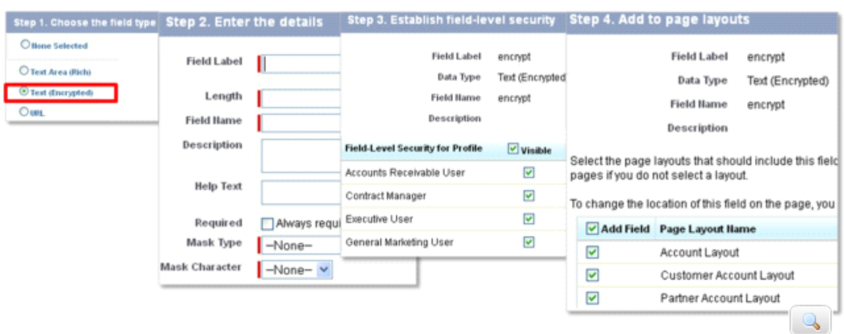
- Record ID
- Field to be encrypted




## Create Encrypted Field

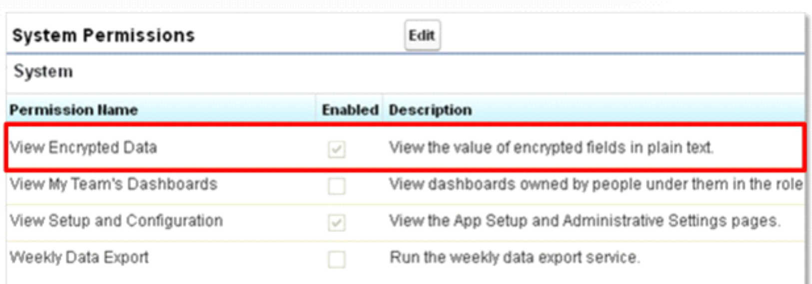
- Select Text (Encrypted) data type
- Set label, length, mask type, and mask character
- Set field-level security
- Add to page layout

**Note: Text length maximum is at 175 characters.**




## Set Profile Permissions

Set the "View Encrypted Data" permission



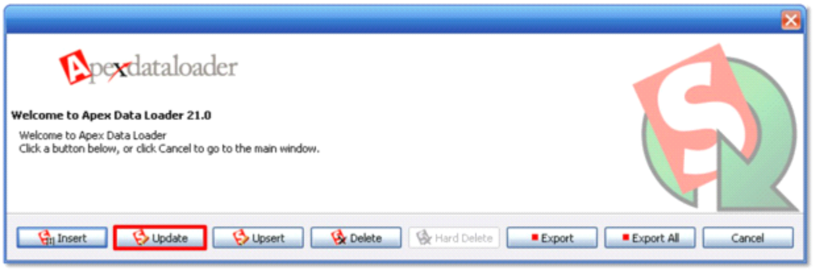
**System Permissions** Edit

**System**

| Permission Name | Enabled | Description |
|---|---|---|
| View Encrypted Data | ✓ | View the value of encrypted fields in plain text. |
| View My Team's Dashboards | | View dashboards owned by people under them in the role |
| View Setup and Configuration | ✓ | View the App Setup and Administrative Settings pages. |
| Weekly Data Export | | Run the weekly data export service. |

## Import Data into Encrypted Field

- Record ID
- Encrypted Field




**Use DataLoader to update multiple fields at once.**

### Module 2 Review

1. Suri only has the "read" permission for the case object on her profile. A criteria-based sharing rule gives her read/write access to product support cases. Will Suri be able to edit product support cases?

   Suri will not be able to edit product support cases, because object permissions give her only read permission. When working with object access, the most restrictive wins.

2. Both a sharing rule and an account team give Jose access to the Dixon Chemical account. The sharing rule gives him read access, and the account team gives him read/write access. Will Jose be able to edit the Dixon Chemical account?

   Jose will be able to edit the Dixon Chemical account, because the account team gives him read/write access. When working with record access, the most permissive wins.

3. When territory management is enabled, what determines record access to accounts and associated contacts, cases, and opportunities?

   When territory management is enabled, record access to accounts and associated contacts, cases, and opportunities is simultaneously controlled by record ownership, organization-wide defaults, role hierarchy, sharing rules, teams, manual sharing, and territory hierarchy.

4. Tom's account page layout makes the Rating field required, but his field-level security settings make the field read-only. Will Tom be able to edit the Rating field?

   Tom will not be able to edit the Rating field, because field-level security settings make the field read-only. When working with field access, the most restrictive wins.