Data Access Security

Veeva Professional Services

Module Objectives

- **Configure Access to Functionality and Data**
- **Describe the different mechanisms for securing access including**
  - Profiles
  - Permission Sets
  - Field Level Security
  - Record Ownership
  - Organization-Wide Defaults
  - Role Hierarchy
  - Territory Hierarchy
  - Sharing Rules
- **Create and manage user accounts**

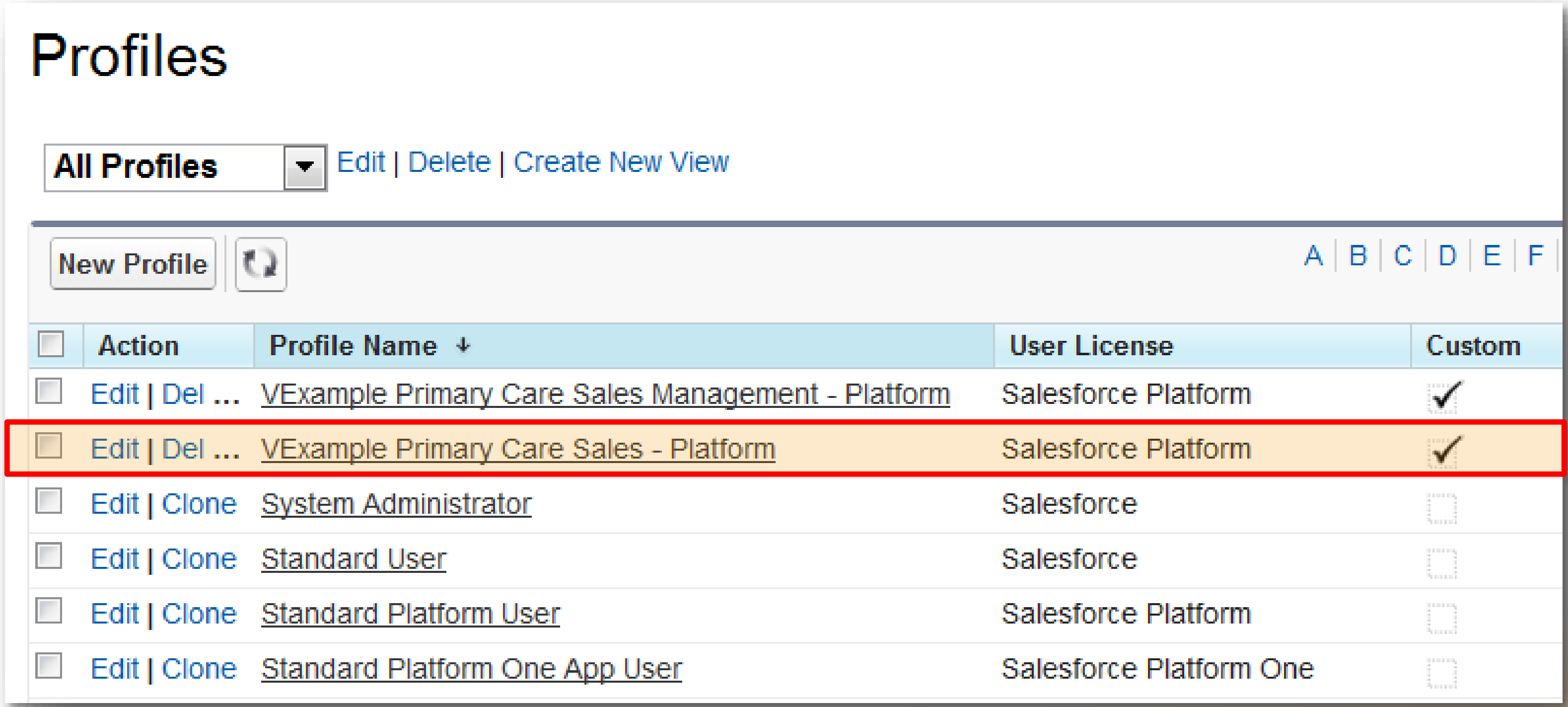
Profiles

Profile Definition

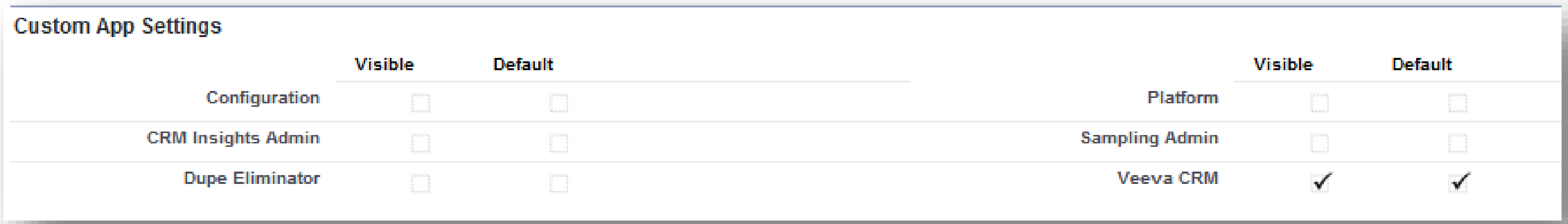
- **Profile is a collection of settings and permissions that determine**
  - What users can see in the application user interface
  - What users can do with what they see
- **Create profiles based on job functions**
  - System Administrator, Primary Care, Medical Scientific Liaison (MSL), Managed Markets, or Sales Operations
- **Users are assigned to one profile**
- **Minimize the number of profiles to have fewer profiles to configure during upgrades**

Accessing Profiles

- **To create or configure profiles go to**
  - Setup → Manage Users → Profiles
- **End-users profiles normally have the word Platform in their names**

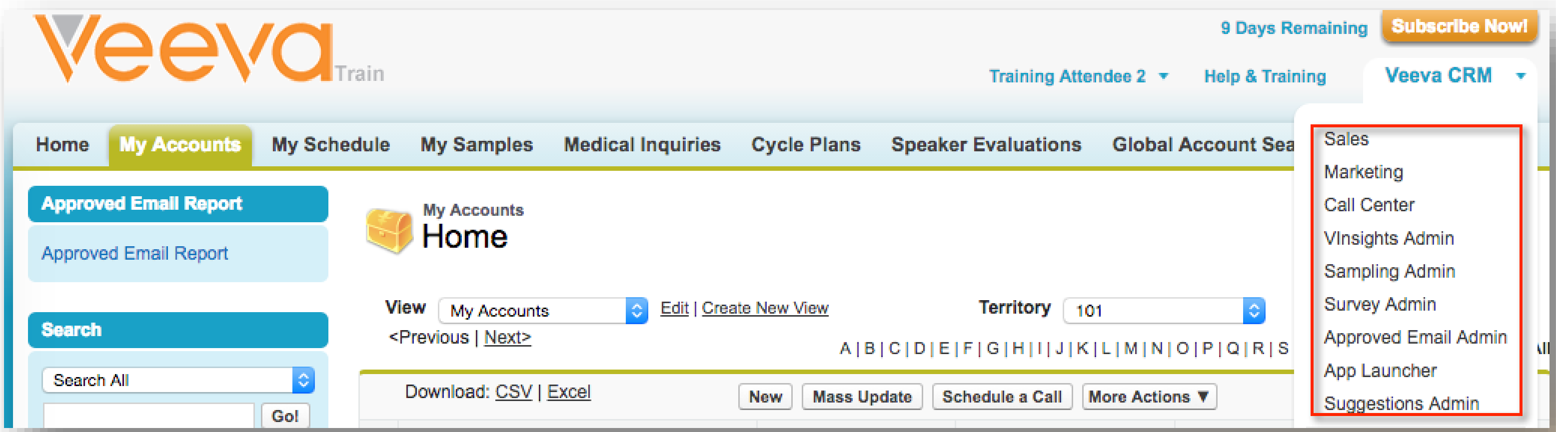


Application Access



- **An application is a collection of tabs**

- **Typically, end-users profiles will have access to the Veeva CRM application only**
  - Certain user profiles, such as a Sales Operations profile may have access to additional applications, such the Sampling Admin application



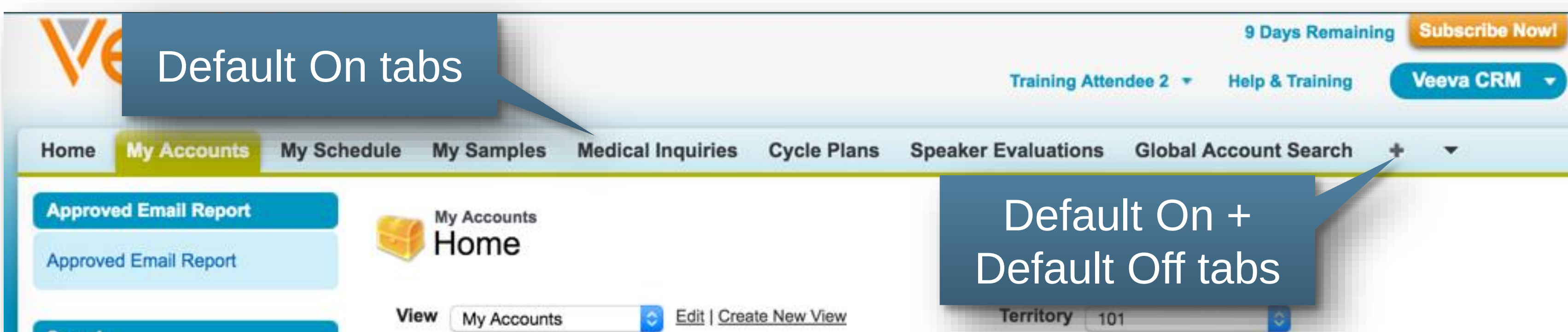
Tab Access

Tab Settings

Standard Tab Settings

Home	Default On	Dashboards	Default Off
Accounts	Default Off	Data.com	Tab Hidden
Answers	Tab Hidden	Documents	Default On
Console	Tab Hidden	Ideas	Tab Hidden
Contacts	Default Off	Reports	Default Off

- **Tabs contain data from specific objects**
    - Default On – tab will always appear on the tab bar
    - Default Off – tab is available from the "+"
    - Tab Hidden – tab is not available to the user



CRUD for Objects Access

- **Controls whether users of a profile can read, create, edit, and delete records for each standard or custom object**
  - System Administrators also have the “View All” and “Modify All” permissions on all objects

Standard Object Permissions

	Basic Access				Data Administration	
	Read	Create	Edit	Delete	View All	Modify All
Accounts	✓	☐	✓	☐	☐	☐
Contacts	✓	✓	✓	✓	☐	☐
Documents	✓	✓	✓	☐	☐	☐

	Basic Access				Data Administration	
	Read	Create	Edit	Delete	View All	Modify All
Ideas	☐	☐				
Push Topics	☐	☐	☐	☐		

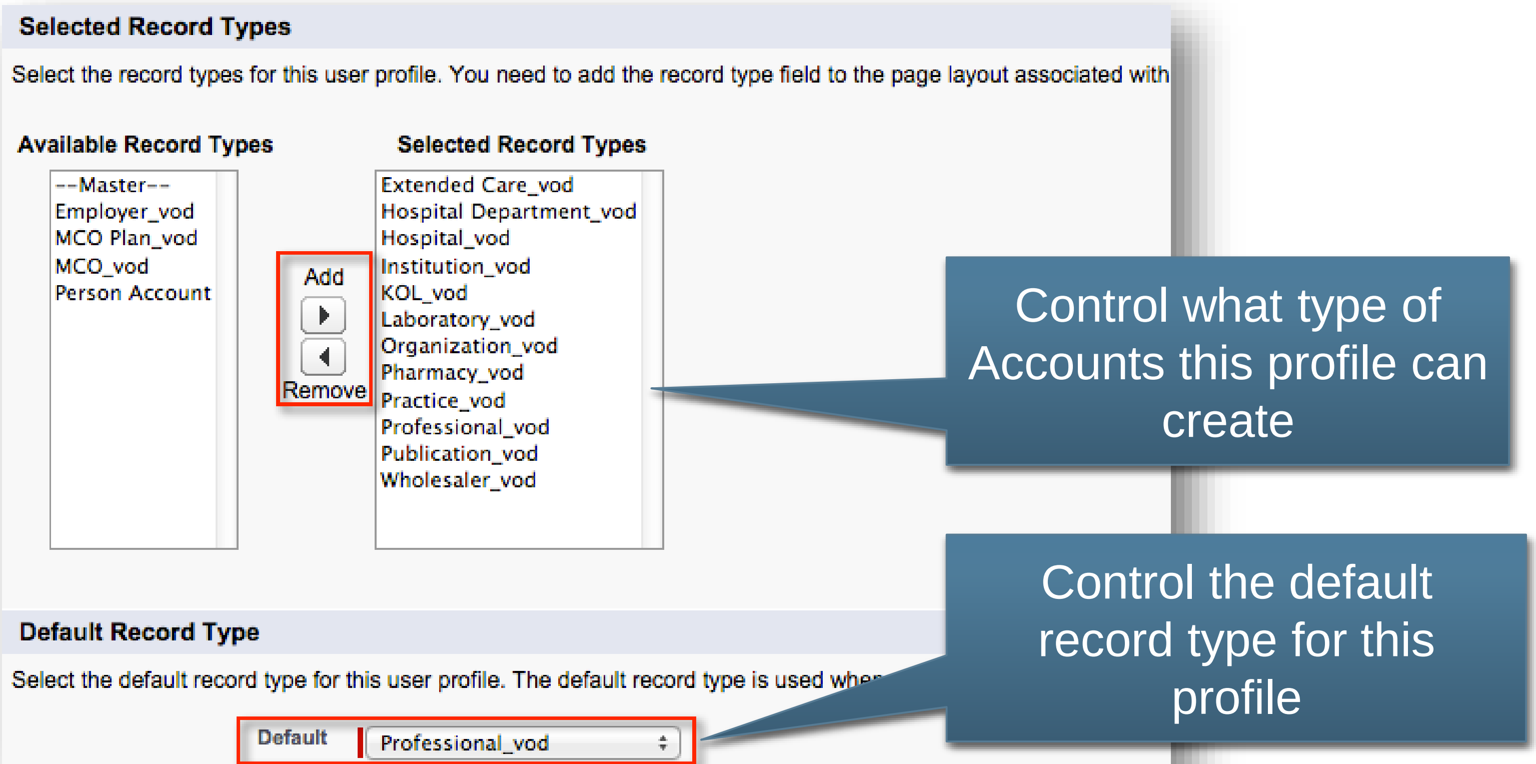
Custom Object Permissions

	Basic Access				Data Administration	
	Read	Create	Edit	Delete	View All	Modify All
Account Lists	✓	✓	✓	✓	☐	☐
Account List Items	✓	✓	✓	✓	☐	☐

	Basic Access				Data Administration	
	Read	Create	Edit	Delete	View All	Modify All
Key Messages	✓	✓	✓	✓	☐	☐
Lot Catalog	✓	☐	☐	☐	☐	☐

Object Record Type Access

- **Record Type Settings control the record types available when creating new records for an object**



Field Level Security Access

- **Field Level Security (FLS) is used to control whether users of a profile can access specific fields**
    - Example, hide the Territory field on the Professional page layout from end-users but display it to the System Administrators
- **If a user profile also has edit (CRUD) permission for an object then the visible fields are also editable**
- **If necessary fields can be made read-only via FLS or via page layouts**
    - Example, for users of a specific profile, you need to make the Specialty account field read-only on the Professional page but editable on the Hospital page

Setting FLS from a Profile

- **To set FLS on many objects and many fields for a single profile**
  - Setup → Manage Users → Profiles → [Profile] → Field-Level Security → [Field]

Affiliation Field-Level Security for profile

Help for this Page

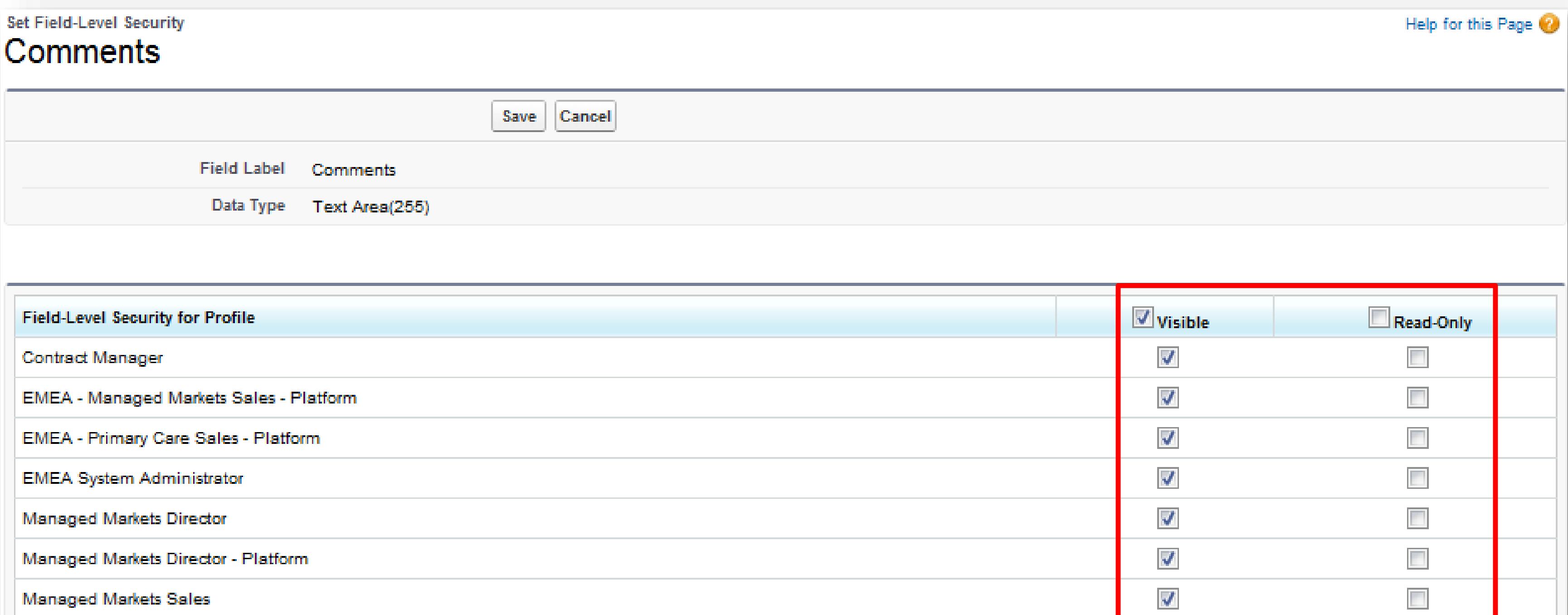
VExample Primary Care Sales - Platform

Edit | Back to Profile

Field Name	Field Type	Visible	Read-Only
AffiliationNumber	Auto Number	✓	✓
Child_Affiliation	Lookup	✓	
Comments	Text Area	✓	
Created By	Lookup	✓	✓
Destroy	Checkbox	✓	
Disable Trigger	Checkbox	✓	
External Id	Text	✓	
From Account	Lookup	✓	
From Contact	Lookup	✓	
Influence	Picklist	✓	
Key Field	Text	✓	✓
Last Modified By	Lookup	✓	✓

Setting FLS from an Object

- **To set FLS on a single field for many profiles**
  - Setup → Create → Objects → [Object] → [Field] field detail page → Set Field-Level Security button
  - Setup → Customize → Accounts → [Fields] field detail page → Set Field-Level Security button



Setting Password Policies from Profile

- **Profile Password Policies settings override the organization-wide Password Policies for that profile's users**

Password Policies

User passwords expire in	90 days
Enforce password history	3 passwords remembered
Minimum password length	8
Password complexity requirement	Must mix alpha and numeric characters
Password question requirement	Cannot contain password
Maximum invalid login attempts	10
Lockout effective period	30 minutes
Obscure secret answer for password resets	☐
Require a minimum 1 day password lifetime	☐

Edit | Clone | Delete | View Users

- **Integration user profiles should have passwords that never expire**

Additional Access

- **Profiles are also used to configure**
  - Page Layouts assignment
    - Which page layout(s) is being used for all objects per profile
  - Enable Apex Class Access
    - Which Apex Classes users of this profile have access to execute
  - Enable Visualforce Page Access
    - Which Visual Force Pages users of this profile have access to in the application

Permission Sets

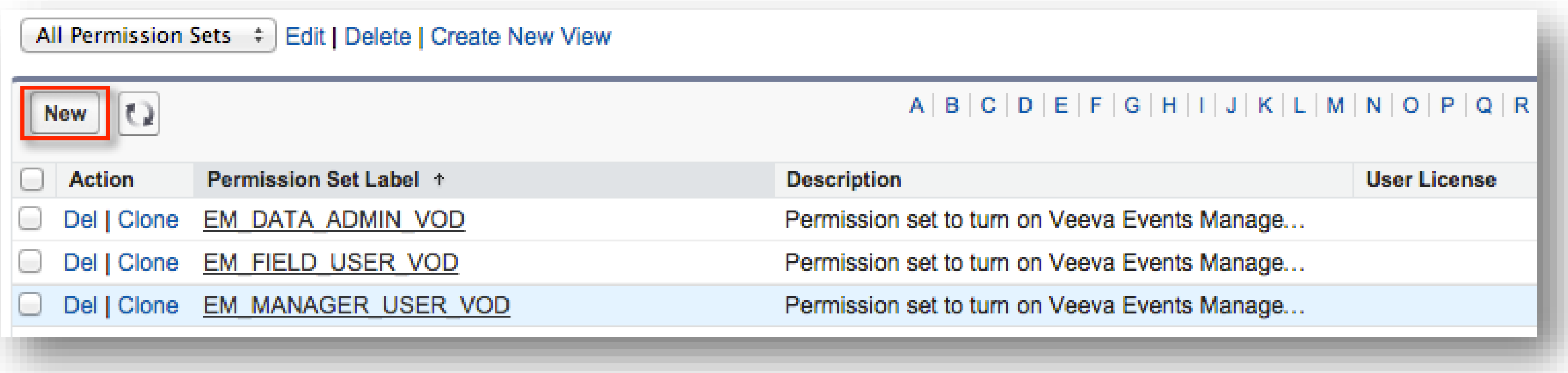
Permission Sets

- **Grants permissions at the user level without having to modify or clone profiles**
- **Define profiles with minimum permissions and then give additional permissions to specific users via permission sets**
  - Helps reduce the number of profiles in the org
- **Enable the PermissionSet Support Veeva Setting so permission sets are enforced offline on the iPad and Windows devices**

- **Veeva provides several standard permission sets**

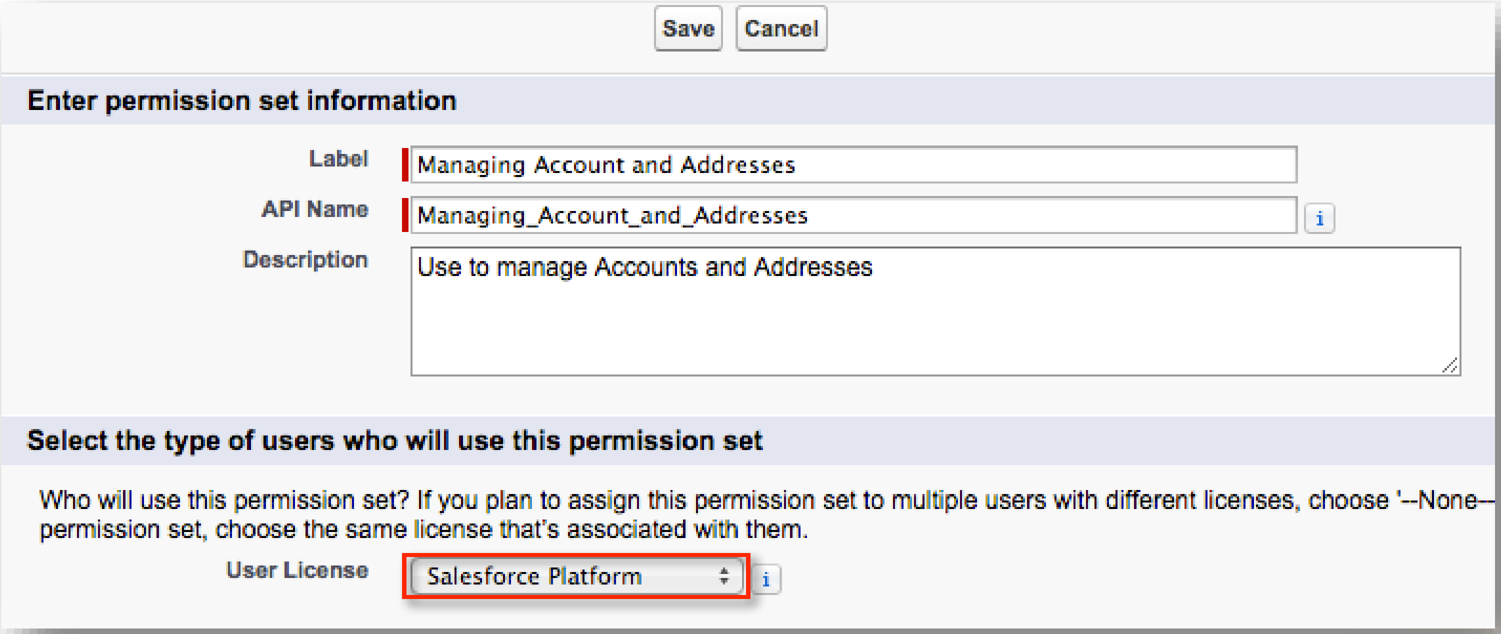
Defining Permission Sets - New

- **To create Permission Sets**
  - Setup → Manage Users → Permission Sets
- **Click the New button to create a permission set**



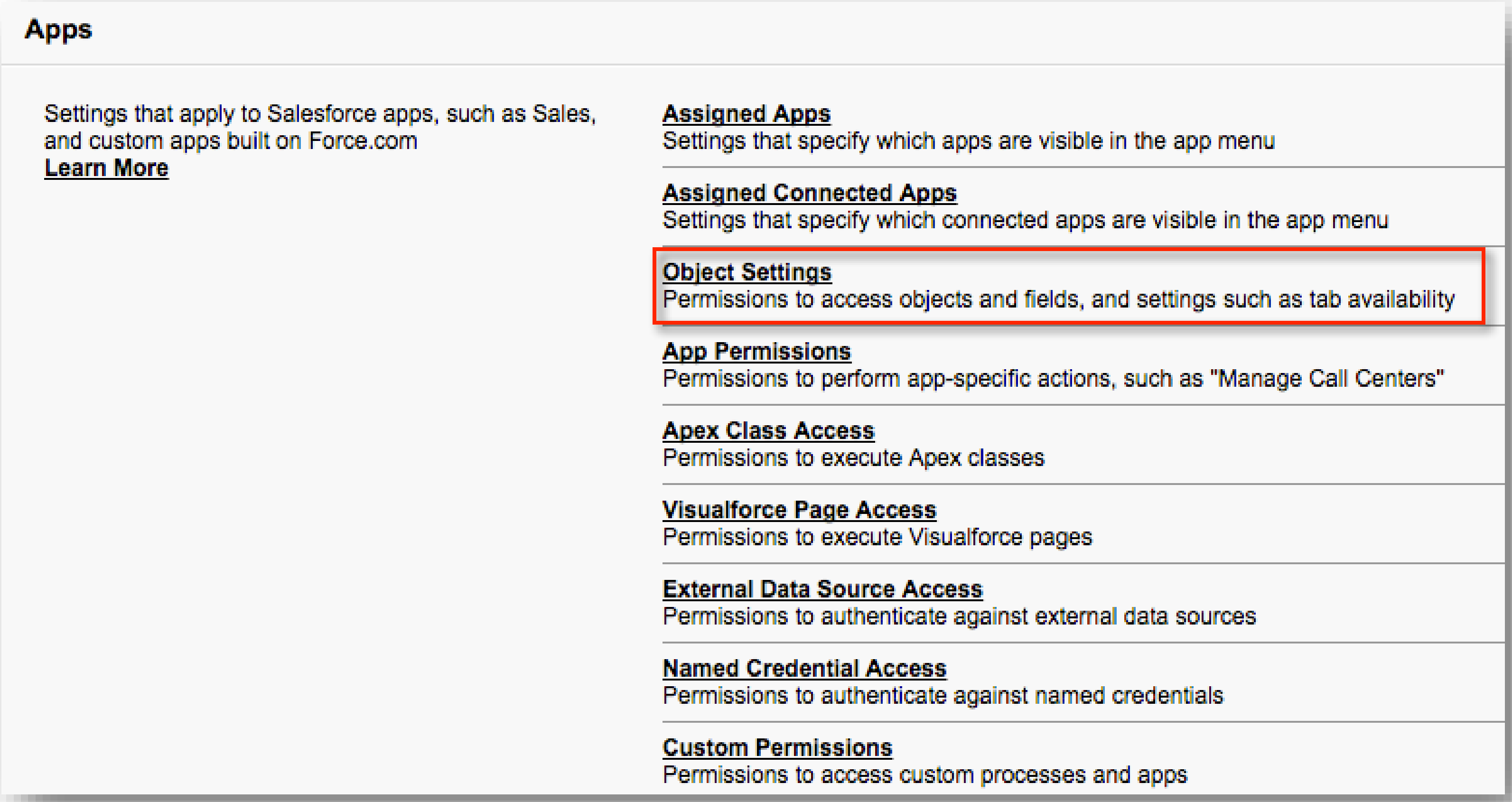
Defining Permission Sets - Information

- Enter the Label, API Name, and Description for the new permission set
- Select Salesforce Platform for the User License



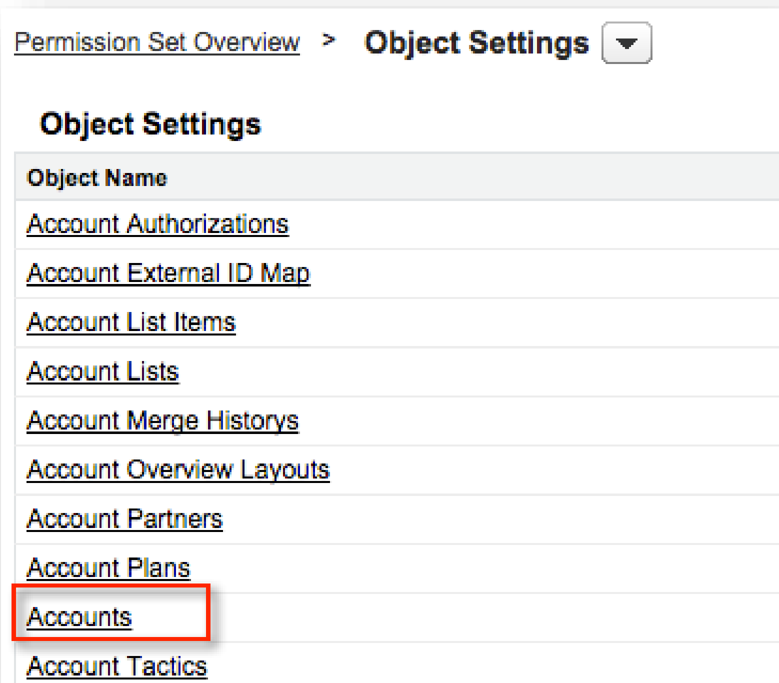
Defining Permission Sets - Apps

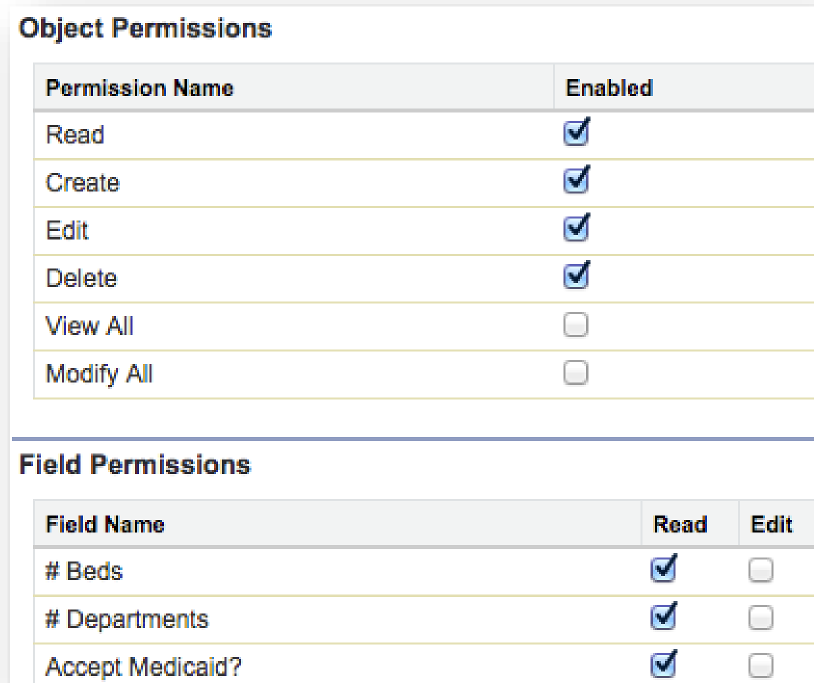
- **Select the desired Apps section**
  - Commonly select Object Settings



Defining Permission Sets - Permissions

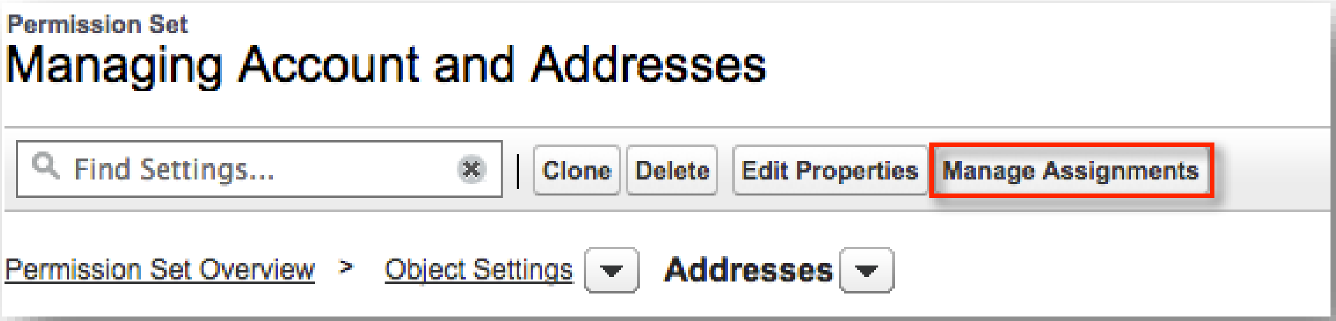
- **Select the desired Object**
  - Set the permissions for the object
  - Select a second object and set the permissions for it



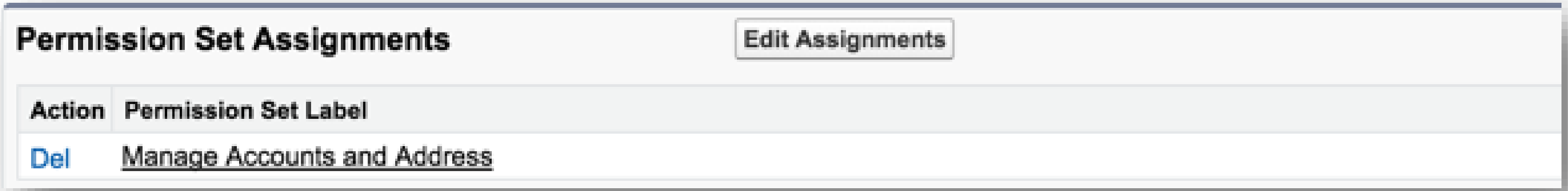


Defining Permission Sets - Assignment

- **Once defined, assign Permission Sets to uses**
  - Click the **Manage Assignments** button
    - Assign a Permission Set to up to 1000 users at a time



  - Can also assign Permission Sets from the user accounts



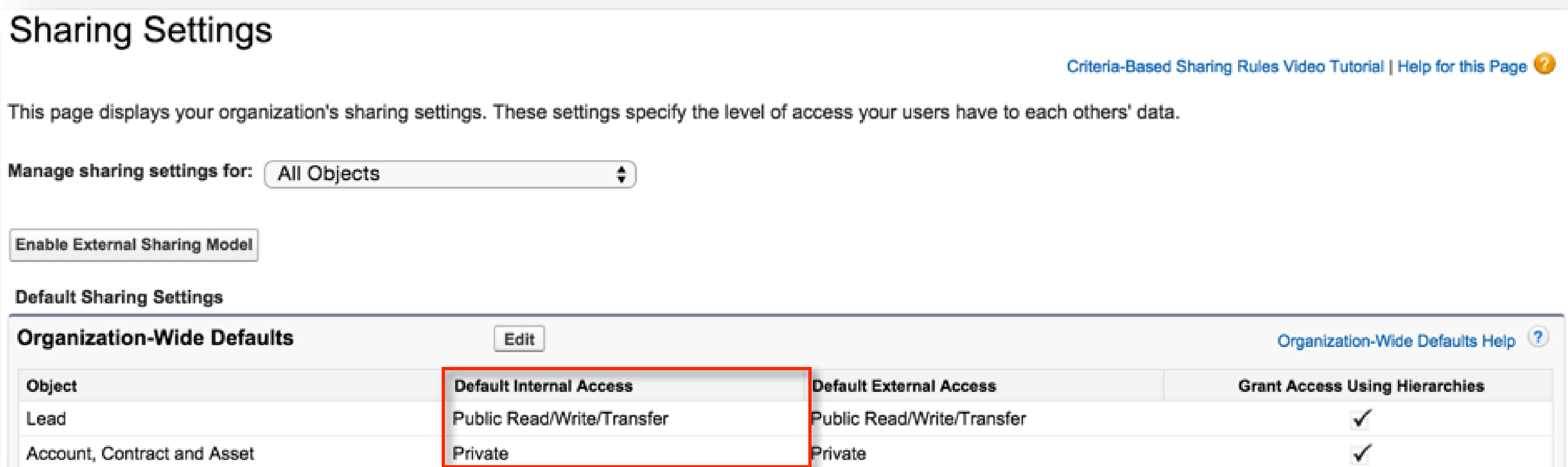
Record Access

Record Ownership

- **Fundamental element that controls how data is shared**
- **All records in the system must have an Owner**
  - By default, the owner of a record is the creator
- **The owner of a record has the following default rights to the record**
  - View
  - Edit
  - Delete
  - Transfer Ownership
  - Sharing

Sharing Settings - OWD

- **The Organization-Wide Defaults (OWD) sharing settings control visibility to the data contained in each object (database table)**
- **To access and setup OWD go to**
  - Setup → Security Controls → Sharing Settings
  - Veeva uses only the Default Internal Access



Organization-Wide Defaults

- **Organization-Wide Default (OWD) has 4 settings:**

Private	Public Read	Public Read/Write	Controlled by Parent
• Allows only the record owner to view and edit the record	• Allows all users to view records of an object regardless of record ownership	• Allows all users to view and edit records of an object regardless of record ownership; this is rare	• Takes the OWD setting at the parent object, i.e., Address takes Account’s OWD setting

Private OWD - Data Sharing

- **Private data can be shared in two ways**
  - Vertically– Managers automatically see the private data owned by their direct or indirect reports via the Territory and Role hierarchies
  - Horizontally – Create sharing rules to share private data between end-users
- **Define public groups to use in sharing rules**
  - Go to **Setup → Manage Users → Public Groups**

Action	Label ↑	Group Name
Edit | Del	EU Users	EU_Users
Edit | Del	US Users	US_Users

- **Add territories (or roles) to public groups instead of end-users**

OWD – Public Read – Sharing Rules

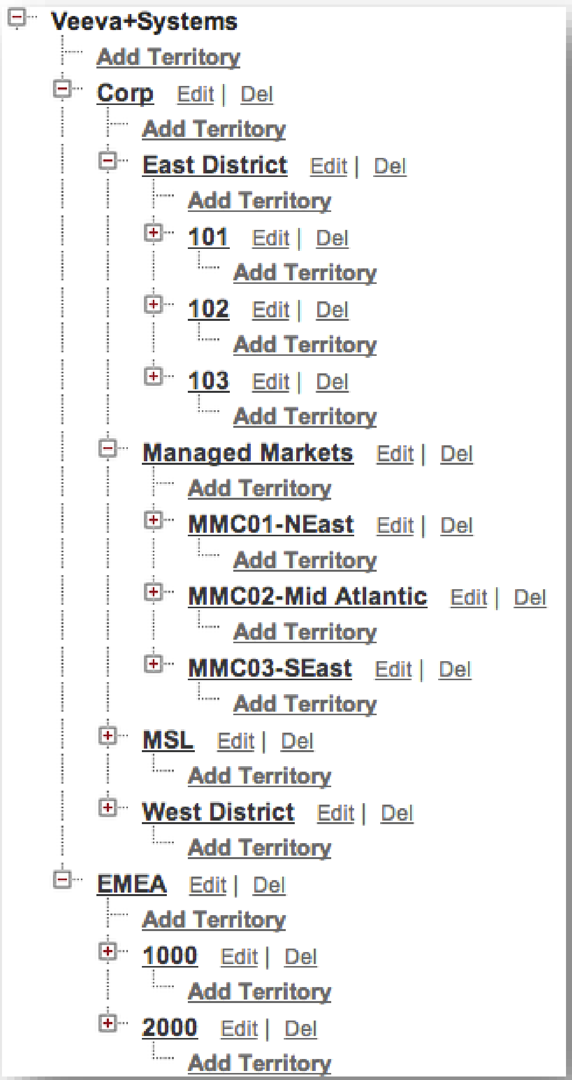
- **Lock down data to the most restrictive level, and then use sharing rules to selectively give users the ability to edit the data**
  - Example: If all users need to read Medical Events but some users need to edit them, then set the OWD to Public Read Only and grant certain user groups Read/Write permission to the Medical Event object via sharing rules

Medical Event Sharing Rules New Recalculate Medical Event Sharing Rules Help

Action	Criteria	Shared With	Access Level
Edit | Del	Owner in Entire Organization	Group: Medical Events Editors	Read/Write

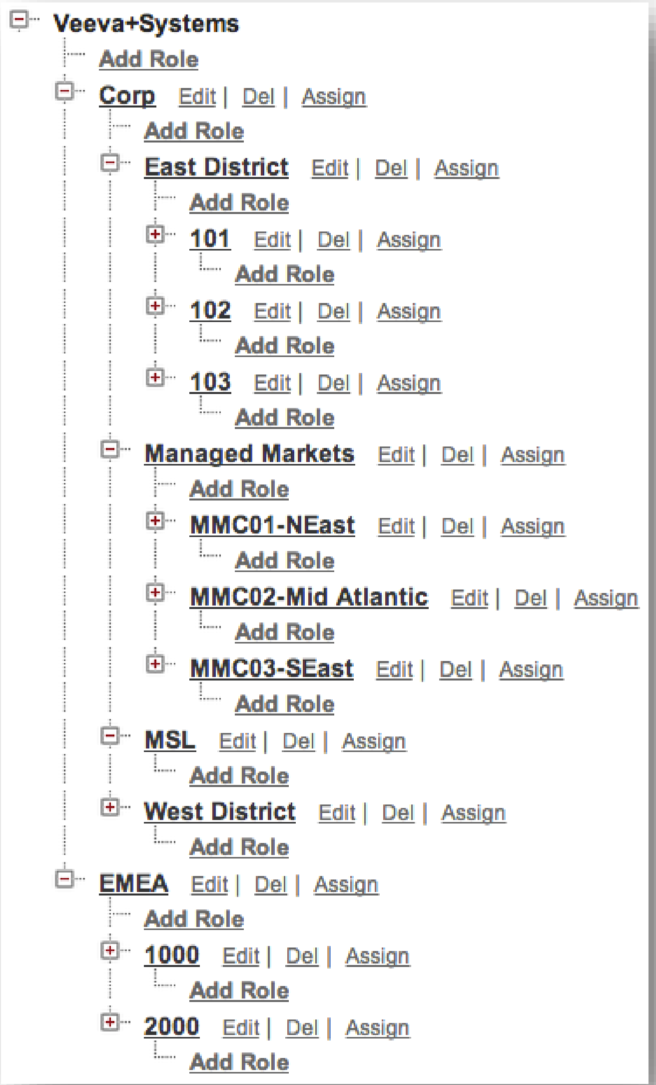
Accounts Visibility - Territory Hierarchy

- **Give users access to Accounts through territories**
  - Accounts are aligned to one or more territories
  - Users are assigned to one territory (in some cases temporarily to more than one)
  - Visibility to accounts is shared up the territory hierarchy
- **To access and setup the Territory Hierarchy go to**
  - Setup → Manage Territories → Territory Hierarchy
  - Add territories as well as edit, delete, and assign users to territories



Private Data Visibility - Role Hierarchy

- **The Role Hierarchy gives managers visibility to the data with private OWD (excluding Accounts) owned by their direct reports**
- **To access and setup the Role Hierarchy go to:**
  - Setup → Manage Users → Roles → Set Up Roles button
  - Add roles as well as edit, delete, and assign roles to users

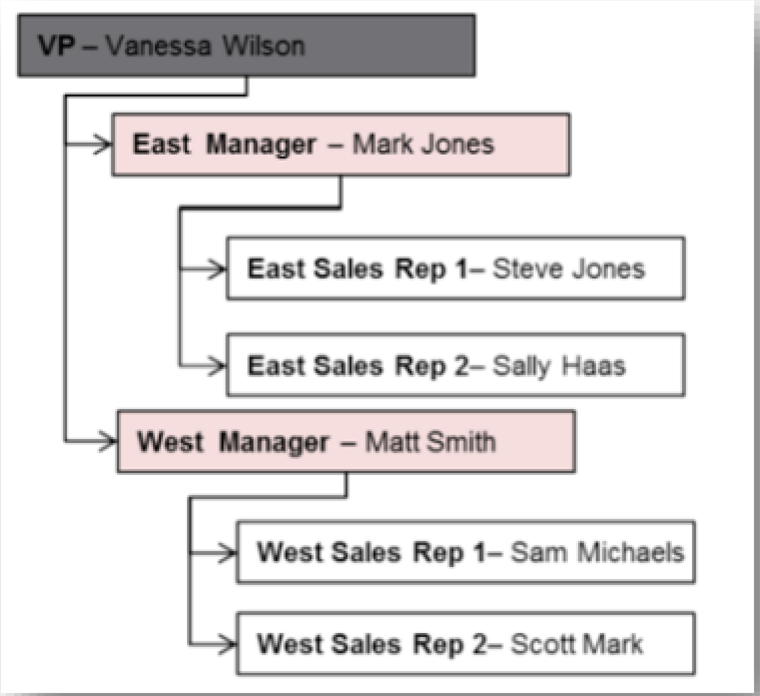


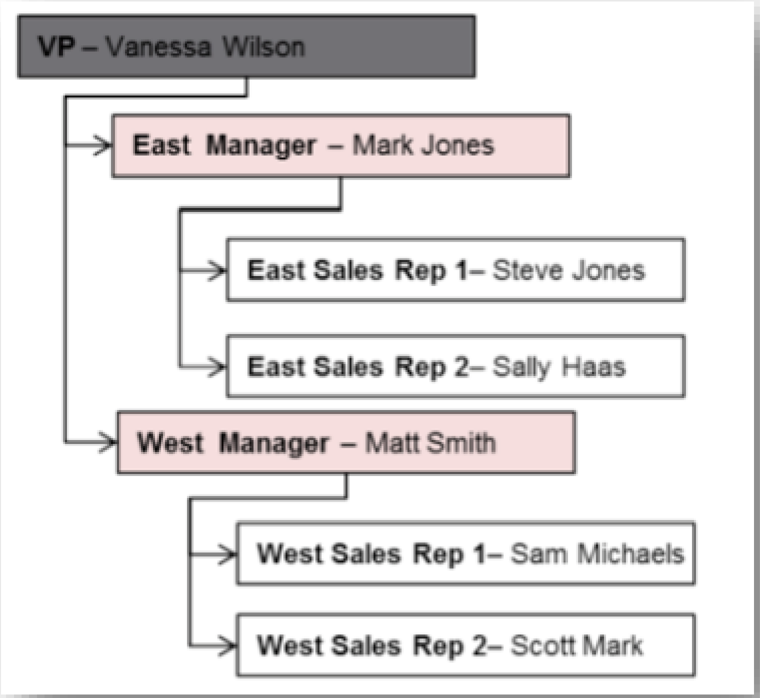
Territories vs. Roles Best Practice

- **In Veeva implementations the Territory and Role hierarchies should be identical**

- **Focus on creating the Territory hierarchy and then make the Role hierarchy exactly the same**

- **Territory Hierarchy** **Role Hierarchy**





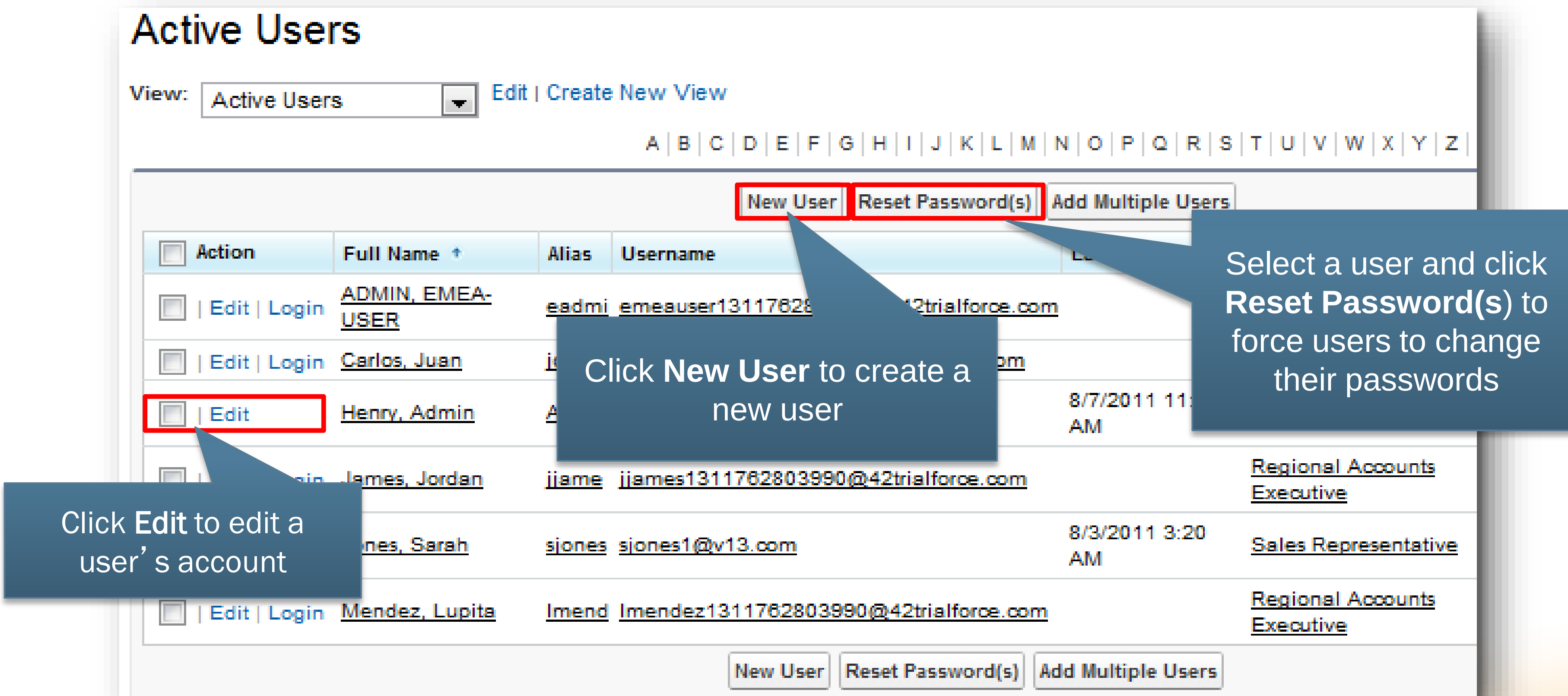
Change Account Owner Workflow

- **The Veeva My Accounts tab displays an Account if**
  - The Account belongs to the user's territory
  - The user created and therefore owns the Account
- **If the Accounts are realigned to different territories**
  - User still sees Accounts he/she owns even though the account is no longer in the user's territory
- **In Veeva implementations which users are allowed to create Accounts**
  - Create a workflow that updates the Account Owner field and sets it to a designated Administrator user

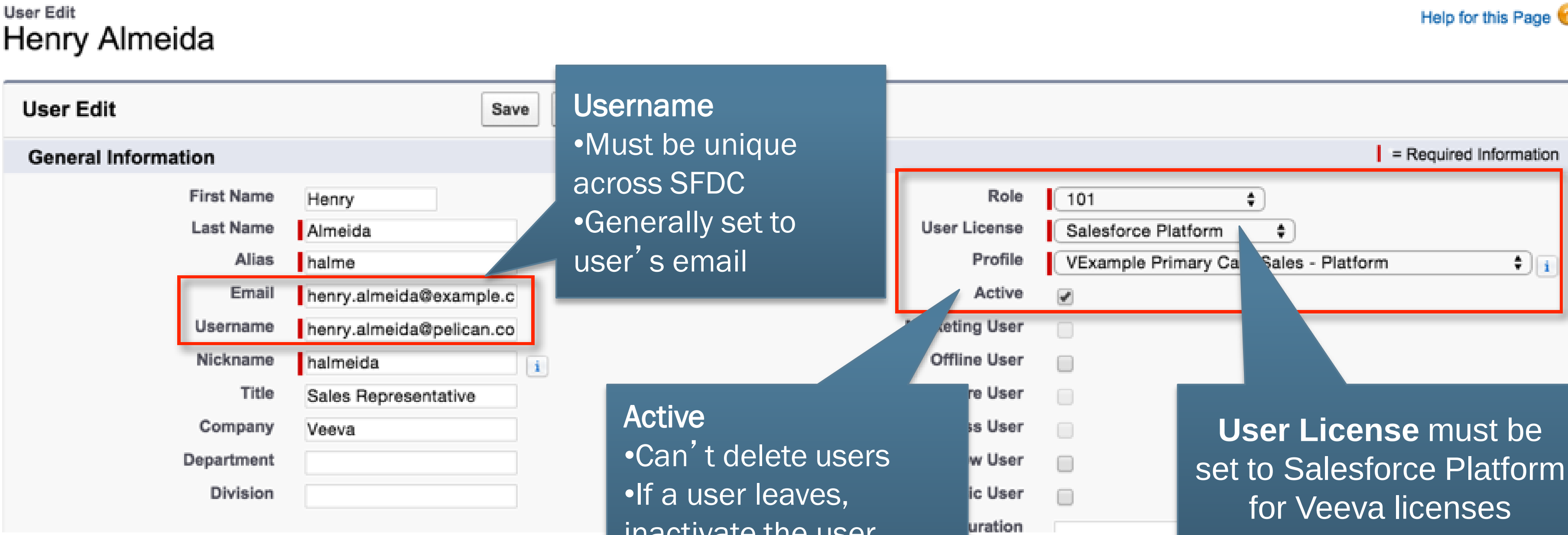
User Management

Accessing User Management

- **To setup and manage user accounts go to**
  - Setup → Manage Users → Users



Creating a New User



Username
- Must be unique across SFDC
- Generally set to user's email

Active
- Can't delete users
- If a user leaves, inactivate the user account

User License must be set to Salesforce Platform for Veeva licenses

Add User to a Territory

- **To access and setup territory hierarchy go to**
  - Setup → Manage Territories → Territory Hierarchy
- **Click the Add Territory link to add a territory to the hierarchy**
- **Click the Territory name and then click the Add Users button to assign a user to a territory**

Module Summary

- **Configured Access to Functionality and Data**
- **Described the different mechanisms for securing access including**
  - Profiles
  - Field Level Security
  - Record Ownership
  - Organization-Wide Defaults
  - Role Hierarchy
  - Territory Hierarchy
  - Sharing Rules
- **Discussed how to manage and create user accounts**

Labs

- Create a role
- Create a user profile
- Access and create territories
- Review OWD