Practices for Lesson 10: Access Control and Security

Practices for Lesson 10

Overview

In these practices, you will explore record and view visibility.

**Practice 10-1: Managing Access Groups, Users and Setting up User Profile**

**Overview**

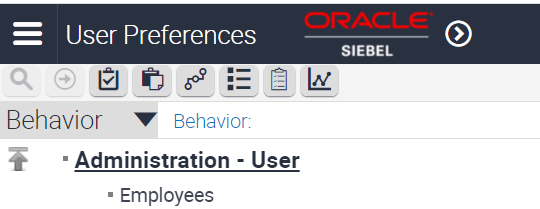
In this practice, you will explore record and view visibility.

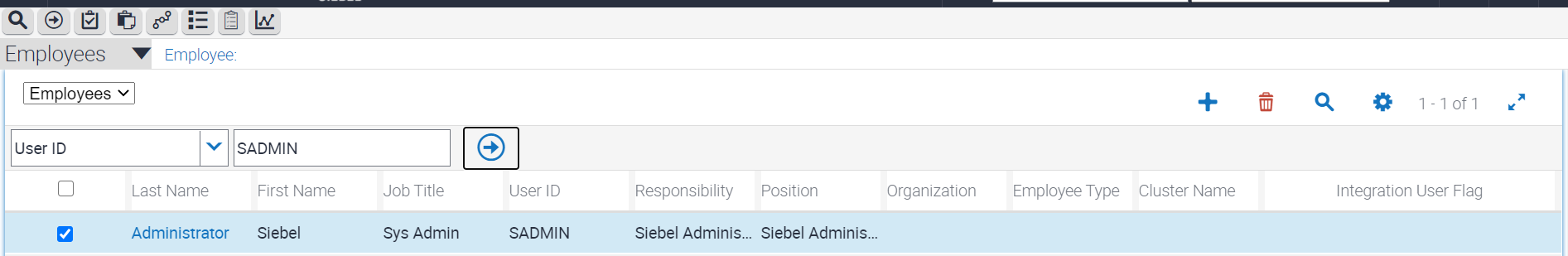
**Note:** For security reasons, you will not be able to have more than one client session logged in at a time.

Assumptions

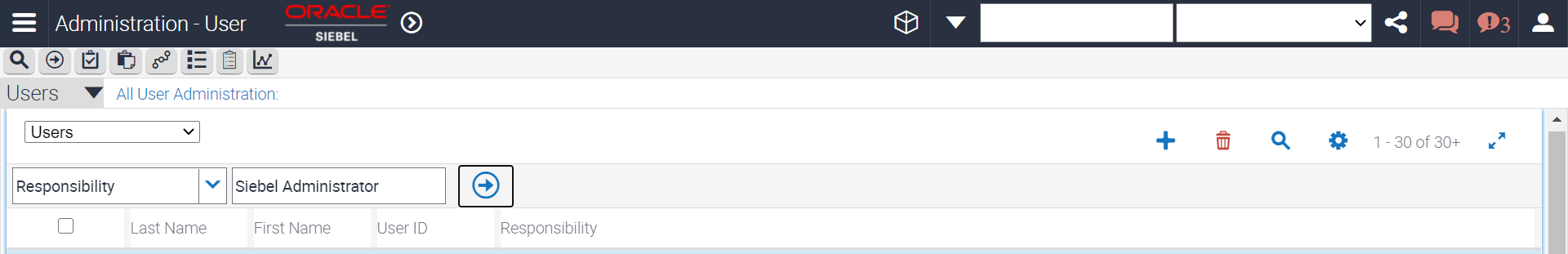
You should have completed the Practices of Lesson 9.

**Tasks**

1. Start the Siebel Web Client.
2. Open Browser and Enter the URL for Siebel Web Client
3. Enter: User ID as SADMIN
4. Click **OK**.
5. Employees are users at your company who will log into the Siebel application. Explore Employees:
6. Use the site map to navigate **to Administration - User > Employees.**
7. Query for User ID = SADMIN OR MSTERN. These are the logins you will use in the remainder of the practice.
8. Verify the SADMIN record.

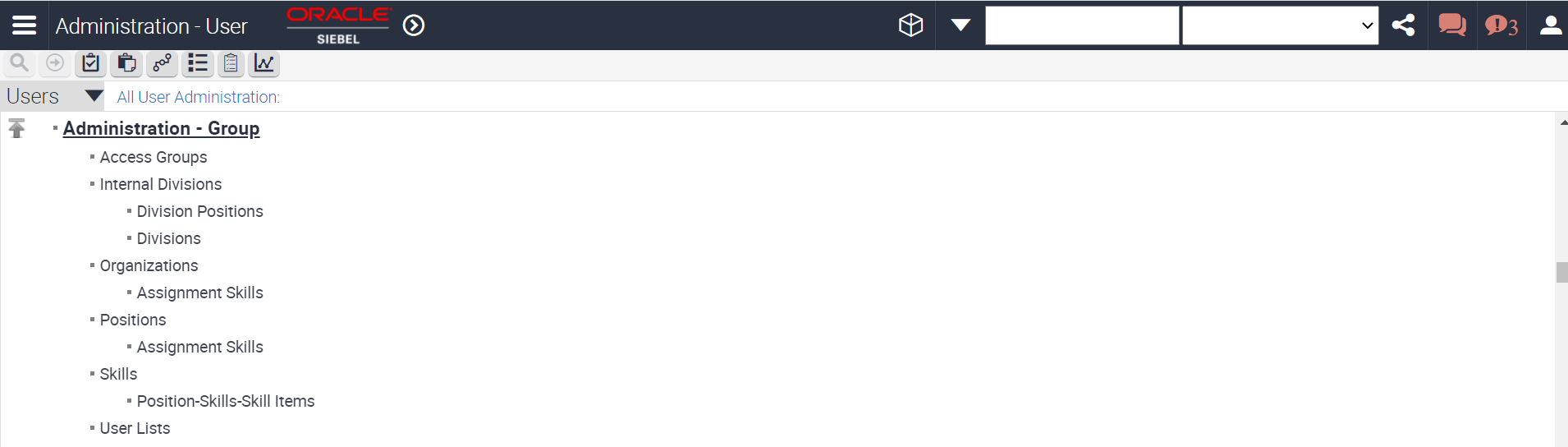
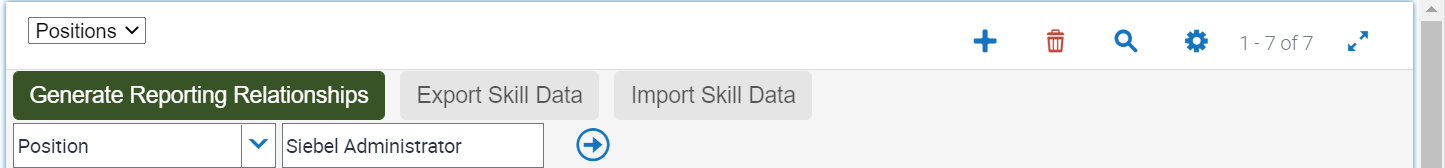
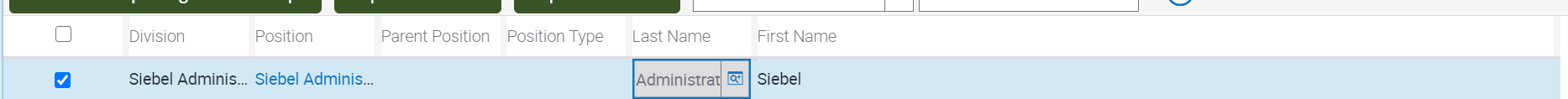


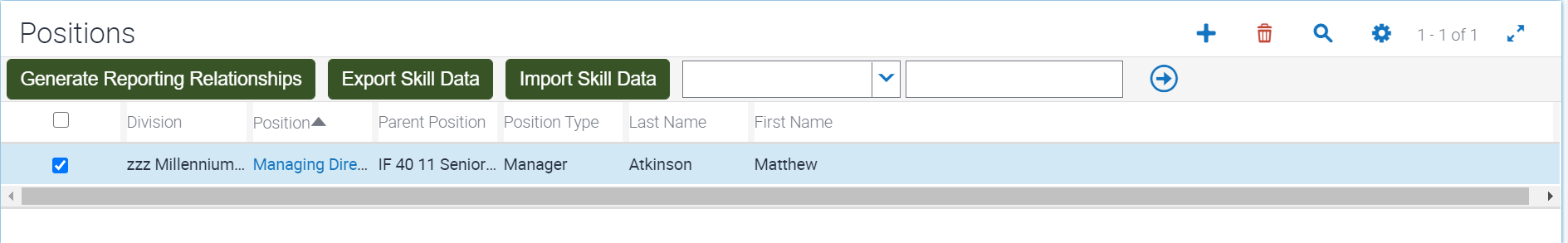
1. In the same screen, choose user type and filter for Siebel Administrator



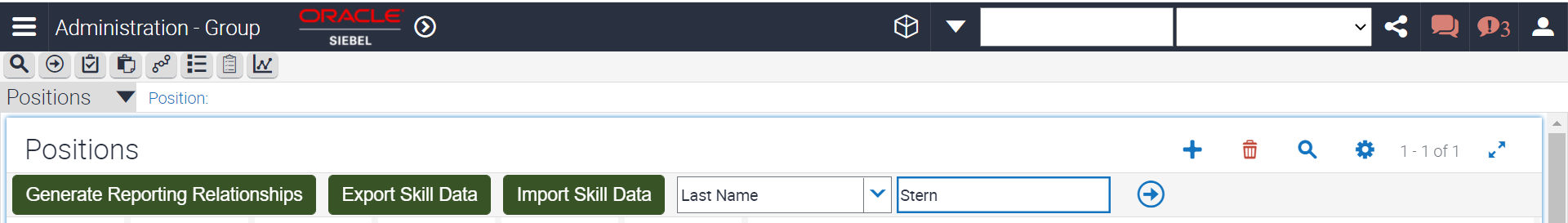
1. In the selected list, there are multiple responsibilities and the Siebel Administrator responsibility is marked as the primary.   
   A user must have at least one responsibility, but may have many. Responsibilities control the views available to the user.
2. Click **OK**.
3. Verify that many records are returned. That is because it is possible to have many employees share a single position in Siebel applications.
4. Positions control access to records in applets.

Explore Positions:

* 1. Navigate **to Sitemap 🡪 Administration - Group > Positions.**   
     
  2. Query for **Position = "Siebel Administrator".** Include the quotation marks.   
     This is the position that SADMIN is assigned to.   
     
  3. Verify that you receive many records, but they are part of different divisions.
  4. Select the record with **Division = Siebel Administration.**
  5. In Last Name, click the **Select** button.   
     
  6. Verify that in the Selected list, many employees are assigned to this position.
  7. Verify that the employee with **Last Name = Administrator** and **First Name = Siebel** is the primary position holder.
  8. In the Selected list, locate **Last Name = Atkins. SADMIN** shares this position with the other employees, such as Chris Atkins.

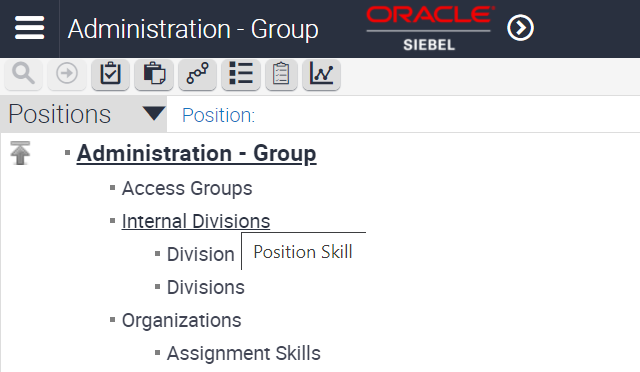


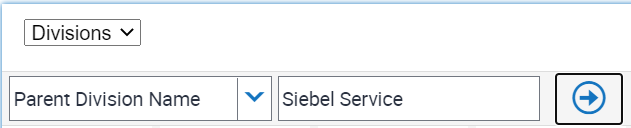
* 1. Click **OK.**
  2. Query for **Last Name = Stern** as shown below.

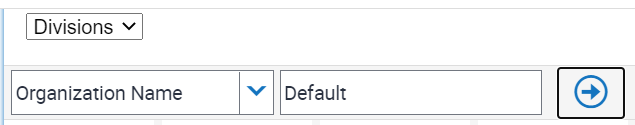


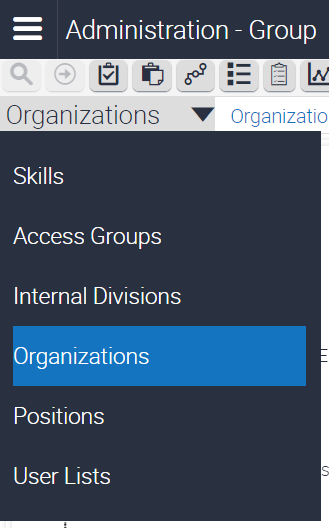
Verify that the record with First Name = Madison has Position = "HT 20 20 Sales Manager". This is the position for MSTERN.

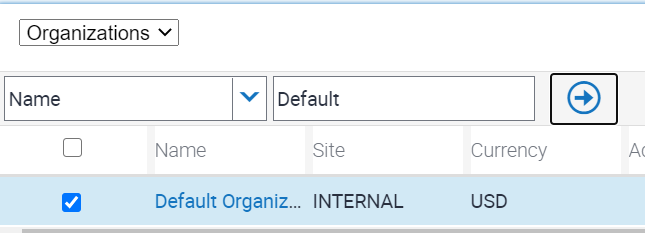
* 1. In the left hand explorer pane, notice that "HT 20 20 Sales Manager" is followed by "(Madison Stern)". This shows the employee associated with the position. In this case Madison Stern (MSTERN).
  2. In the left pane, **expand "HT 20 20 Sales Manager**".
  3. You will see several positions are displayed. This means that these positions report to Madison Stern.
  4. Verify that one of positions displays "(Terry Smythe)". This means that Terry Smythe reports to Madison Stern. You will be inspecting MSTERN's Team view further practices.

1. Divisions represent the structure of your company, but are not used for record access. **Explore Divisions:**
   1. Navigation to **Administration - Group > Internal Divisions**.   
      
   2. Query for **Division Name = "Siebel Service".** Include the quotation marks.



* 1. You will see some records.
  2. Select the record with **Organization Name = Default Organization**.   
     
  3. In the bottom applet, verify that the Organization Flag is not checked. This means, this is a division not an organization.
  4. In the top applet, select the other record.
  5. In the bottom applet, verify that it is marked as an organization.

1. Organizations are used to control access to records in applets.   
   **Explore Organizations:** 
   1. Navigate to **Administration - Group > Organizations.**
   2. Query for Name = Default.

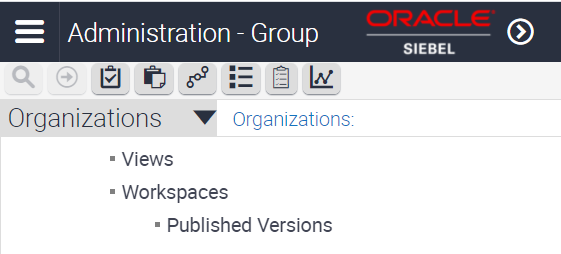


* 1. In the left pane, expand **Default Organization.**
  2. Several organizations are displayed under the Default Organization. These are child organizations.
  3. Verify that "**Siebel Administration**" does not appear in the list because it is a division, not an organization.

1. Responsibilities control access to views. Explore Responsibilities:
   1. Navigate to **Administration - Application > Responsibilities.**
   2. In the top applet**, query for Responsibility = "Siebel Administrator**". Include the quotation marks. This is the responsibility assigned to SADMIN.
   3. In the bottom left applet, verify that many views are assigned to this responsibility and Add and Delete buttons are inactive.   
      **Note:** The Siebel Administrator responsibility is part of the seed data that is added as part of installation. The views that are part of seed responsibilities cannot be edited. You can copy, rename, and edit copies of seed responsibilities if you need to for your business purposes.
   4. In the bottom left applet, query for View Name = Home Page.
   5. Verify that Home Page View (WCC) is among the list. This is the home page view for the Call Center application. You could have determined this using About View.
   6. In the bottom right applet, check that many users are assigned to this responsibility.
   7. In the bottom right applet, query for User ID = SADMIN. This confirms that SADMIN has this responsibility. Note: You can add users to seed responsibilities.
2. Views provide access to applets and data.

Explore Views:

1. Navigate to **Administration - Application > Views.**



1. Query **for View Name = Home Page.**
2. Select the "Home Page View (WCC)" record.
3. Verify in the bottom applet that this view is part of many responsibilities.
4. In the bottom applet, **query for Responsibility = "Siebel Administrator".** Include the quotation marks.
5. You will notice that a record is returned.
6. This confirms that this view is part of a responsibility that is assigned to SADMIN.
7. Close the browser