Practical 9: User and Role Management

Subject: Identity and Access Management (ISIM)

This guide details the exercises for modifying user information, creating roles (static and dynamic), implementing Separation of Duty (SoD) policies, and approving policy violations.

Part 1: User Management

Prerequisites:

- You should have users like Alice Smith, Bob Smith, etc., created from Practical 8.
- **Login:** `https://isim.test:9444/itim/console/` (ISIM Admin Console)
- **User:** `itim manager` (or your admin ID created in Prac 8)
- **Password:** `P@ssword`

Exercise 1: Changing User Information

Scenario A: Changing a Name (Alice Smith -> Alice Smyth)

1. Go to **Manage Users** on the Home tab.
2. Search for "Alice Smith".
3. Click the arrow next to her name -> **Change**.
4. **Personal Information Tab:**
   - Change Last Name to `Smyth` .
   - Change Full Name to `Alice Smyth` .
   - Change Preferred User ID to `asmyth` .
5. **Contact Information Tab:**
   - Change Email to `asmyth@jke.test` .
6. Click **Submit Now**.
7. **Update Account ID:**
   - Find Alice Smyth again. Click arrow -> **Accounts**.
   - Find the `ITIM Service` account. Click arrow -> **Change**.
   - Change User ID to `asmyth` .
   - Click **Submit Now**.

Scenario B: Changing a Manager (Transferring)

1. Go to **Manage Users**.
2. Find "Alice Smyth". Click arrow -> **Change**.
3. **Business Information Tab:**

   - Find the **Manager** field. Click **Search**.
   - Search for "Sue Thomas". Select her and click **OK**.
4. Click **Submit Now**.

Exercise 2: Transferring Users (Changing Business Unit)

1. Go to **Manage Users**.
2. Find "Sue Thomas". Select the checkbox next to her name.
3. Click the **Transfer** button (top menu).
4. Search for Business Unit: `Finance`. Select it and click **OK**.
5. Click **Transfer**.
   - *Repeat for Bob Smith -> Transfer to `WW` (under Sales).*
   - *Repeat for John Davis -> Transfer to `TechSupport`.*

Part 2: Role Management

Exercise 3: Creating Organizational Roles

A. Creating Static Roles

1. Go to **Manage Roles**.
2. Click **Create**.
3. **Role Type:** Select `Static`. Business Unit: `JK Enterprises`. Click **Next**.
4. **General Info:** Name: `JKE System Admin`. Desc: `Org Role for System Admins`. Click **Next**.
5. **Access Info:** Check "Enable access for this role". Click **Next**.
6. Skip Assignment Attributes.
7. **Role Membership:** Click **Add**. Search for `Erica Carr`. Select and Click **OK**.
8. Click **Finish**.

B. Creating More Static Roles (No members yet) Repeat steps 1-5 for these roles in the `Finance` business unit:

- `Asset Handling and Disposition` (Check "Show as common access")
- `Booking and Ledgers` (Check "Show as common access")
- `Comparison and Review` (Check "Show as common access")
- `Finance Employees`

C. Creating Dynamic Roles

1. Click **Create**.
2. **Role Type:** Select `Dynamic`. Business Unit: `JK Enterprises`. Click **Next**.
3. **General Info:** Name: `Help Desk`. Click **Next**.

4. **Access Info:** Check "Enable access". Click **Next**.
5. **Definition (Rule):** Enter LDAP filter: `(title=*Manager*)` .
   - *(Note: The practical uses `cn=*` for Help Desk, but `title=*Manager*` is usually for manager roles. Follow your specific lab instruction if it differs).*
6. Click **Finish**.

Exercise 4: Creating Child Role Assignments (Role Hierarchy)

You will make specific finance roles "children" of the main "Finance Employees" role. This means if you are a "Finance Employee", you might inherit other rights, or vice versa.

1. Go to **Manage Roles**. Search for `Finance*` .
2. Find `Finance Employees` . Click arrow -> **Add Child Roles**.
3. Search for roles in `Finance` .
4. Select:
   - `Asset Handling and Disposition`
   - `Booking and Ledgers`
   - `Comparison and Review`
5. Click **OK** -> **Submit**.

Part 3: Policies & Violations

Exercise 5: Creating a Separation of Duty (SoD) Policy

You want to prevent one person from having too much power (e.g., handling assets AND booking ledgers).

1. Go to **Manage Policies** -> **Manage Separation of Duty Policies**.
2. Click **Create**.
3. **Name:** `ABCs of Finance` . Unit: `Finance` .
4. **Policy Rules:** Click **Create**.
   - **Name:** `Finance department ABCs` .
   - **Build List:** Search and add the 3 roles: `Asset Handling...` , `Booking...` , `Comparison...` .
   - **Allowed number of roles:** `1` (User can only have 1 of these 3).
   - Click **OK**.
5. **Policy Owners:**
   - **User Policy Owners:** Add `Sue Thomas` . (She will approve violations).
6. **Policy State:** `Enabled` .
7. Click **Submit**.

Exercise 6: Triggering and Approving a Violation

Alice needs access that violates the policy. Sue must approve it.

1. Trigger Violation (Alice):

1. **Logout** of Admin Console.
2. **Login to ISC (Identity Service Center):** `https://isim.test:9443/itim/ui/Login.jsp`
3. User: `asmyth` (Alice).
4. Click **Request Access**.
5. Select `Asset Handling and Disposition`. Click **Next**.
6. Justification: "Required for Finance". Click **Submit**.
7. Click **Request Access** again.
8. Select `Booking and Ledgers`.
9. **Warning!** You will see a yellow warning sign (SoD Violation).
10. Click **Continue My Request**. Justification: "Backup for Bob". Click **Submit**.

2. Approve Violation (Sue):

1. **Logout** Alice. **Login** as `sthomas` (Sue).
2. Go to **My Activities** (or "Manage Activities").
3. Find "Approve SoD Violation for Alice Smyth".
4. Click it. Review details.
5. **Decision:** Approve. Justification: "Temporary access granted".
6. Click **OK**.

Exam Preparation: Memory Strategy

1. User Management Flow

Think of the user profile as a folder with tabs.

- **Name change?** -> `Personal Info` tab.
- **Email change?** -> `Contact Info` tab.
- **Manager change?** -> `Business Info` tab.
- **Login ID change?** -> This is tricky. It's an **Account**, not just user info. Go to `Accounts -> ITIM Service`.

2. Role Management: Static vs. Dynamic

- **Static:** You manually add people ("Pick Erica Carr from a list").
- **Dynamic:** You write a rule ("Anyone with title 'Manager' is in").
- **Hierarchy:** Think of "Finance Employees" as the parent folder, and specific jobs (Asset, Booking) as children inside it. Use `Add Child Roles`.

3. The "SoD" Logic Chain

This is the most complex part. Memorize the **"Rule of 3"**:

1. **Create Policy:** Name it, pick the Business Unit (`Finance`).
2. **Define Rule:** Pick the conflicting roles (Asset, Booking, Comparison) and set `Max = 1` .
3. **Assign Owner:** Who says "Yes" when rules are broken? (`Sue Thomas`).

4. Violation Workflow (Two-Person Play)

- **Actor 1 (Alice):** Breaks the rule. She requests Role A (fine), then Role B (Warning!). She *must* give a reason.
- **Actor 2 (Sue):** Fixes the mess. She logs in, sees the "Activity", and clicks Approve.

5. Exam Tips

- **ISC vs. Admin Console:** Read the question carefully.
  - "Create Policy" -> **Admin Console** (Blue interface).
  - "Request Access" -> **ISC** (Modern/White interface).
- **Commit Changes:** Always click **Submit Now** or **Refresh** to verify your work.
- **Search Wildcards:** If you can't find "Finance", try searching `*Finance*` .