Section Three: Roles and Custom Reports

IdentityIQ Implementation Training for SailPoint

IdentityIQ Version 6.2

11305 Four Points Drive
Bldg 2, Suite 100
Austin, TX 78726
www.sailpoint.com

Contents

Section 3: Roles, Tasks, Rules and Custom Reports

In this section, we will be exploring Roles and ways to extend IdentityIQ.

In the previous sections we:

- loaded identities, applications, accounts and entitlements
- performed certifications on the data we loaded
- used analytics, populations and groups to help us to organize and make sense of the data
- detected policy violations
- assigned a risk model to identities

In this section we will be doing the following:

- Define a Role Model
  - Business Roles – Based on identity or account attributes
  - IT Roles – Based on account entitlements
- Learn about the SailPoint API by running an assortment of example rules
- Learn how to create and deploy a custom task
- Learn how to create a custom report

Exercise #1: Defining a Role Model

Objective:

Learn how to define roles and to assign them to Identities and detect them from account entitlements

Overview:

In our case, we are going to setup some roles to do the following:

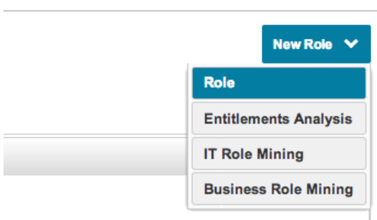
- Container Roles for all the roles we will create
- Region Roles driven off of Identity Attributes (i.e. a Role for users in Americas, Europe and Asia-Pacific).
- Application Roles (TRAKK Application) to define Roles for the TRAKK Time Sheet application
- Application Roles (PRISM Application) to define Roles for the PRISM application.

After configuring roles, we will learn how to update identities so that roles get assigned and detected and stored in the identity cubes.

Create Role Container

1. Create TRAKK Container

   a. Navigate to **Define → Roles** and select **New Role** and choose **Role**

   b. Name: **TRAKK**

   c. Display Name: **TRAKK**

   d. Type: **Organizational**

   e. Owner: **The Administrator**

   f. Click: **Submit**

2. Create Regions Container

   a. New Role and choose **Role**

b. Name: **Regions**

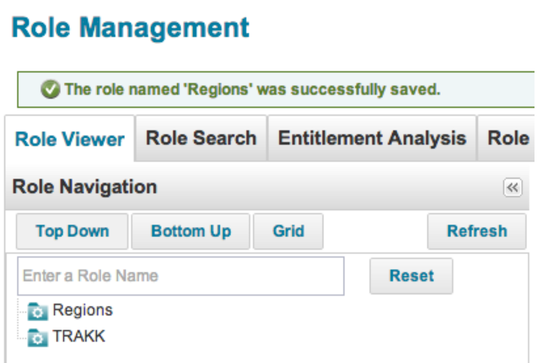
c. Display Name: **Regions**

d. Type: **Organizational**

e. Owner: **The Administrator**

f. Click: **Submit**

3. You should have two container roles defined:



Run a Business Role Mining Task to generate Region Roles

1. From the **Role Management** screen, click **New Role** and select **Business Role Mining**

2. Configure the Role Mining Task using the following settings:

   a. Name: **Business Roles - Regions**

   b. Compute Population Statistics: **Checked**

   c. Specify an Existing Root Container Role: **Regions**

   d. Ordered Identity Mining Attributes: **Region**

   e. Type of Business Roles to generate: **Business**

   f. Owner: **The Administrator**

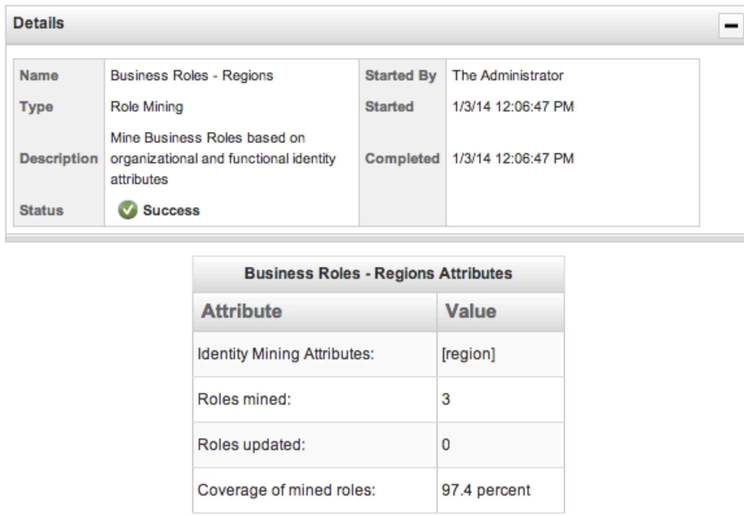
   g. Prefix to Apply to Generated Business Roles: **Region**

   h. Select **Save and Execute** and **OK**

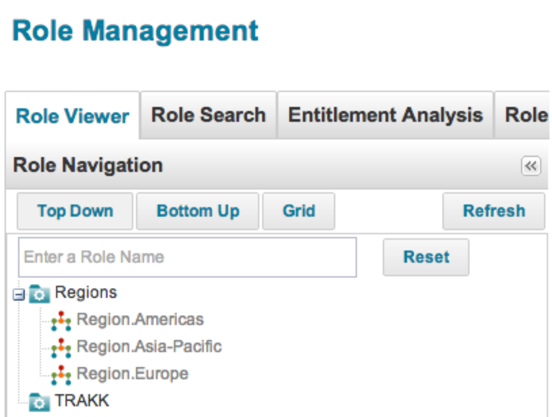
3. Observe the results of Role Mining

   a. Click the **Role Mining Results** tab

   b. Select the Role Mining results and observe:



   c. Navigate back to the **Role Viewer** tab and refresh by selecting **Refresh** and see the roles defined.



4. Enable each of the three Region roles by repeating the following steps for each role

   a. Select the role

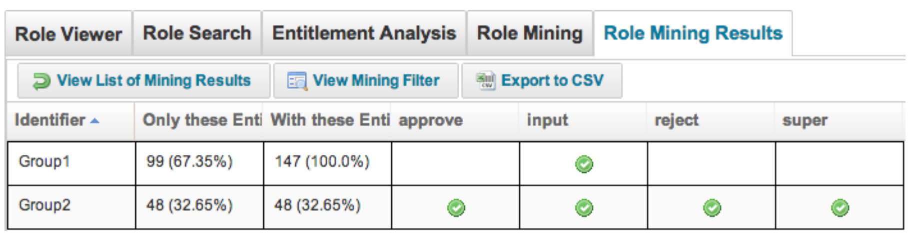
   b. In the right side of the screen select **Edit Role**

   c. Scroll down and uncheck **Disabled** to enable the role

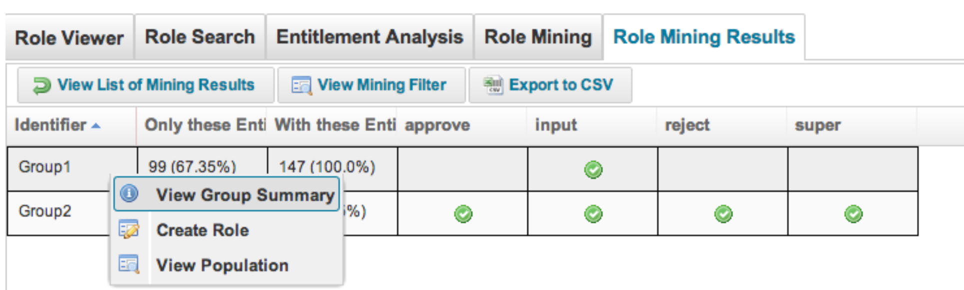
   d. Scroll down and **Submit** the changes

Run an IT Role Mining Task to create TRAKK Roles

1. Under **Role Management**, select **New Role** and choose **IT Role Mining**
2. Configure the IT Role Mining Task as shown:
    a. Name: **IT Roles – TRAKK**
    b. Owner: **The Administrator**
    c. Identities to Mine: **Search by Attributes**
    d. Inactive: **False**
    e. Applications to Mine: **TRAKK**
    f. Click **Save and Execute** and click **OK**
3. Observe the results of Role Mining
    a. Click the **Role Mining Results** tab
    b. Select the Role Mining results and select **IT Roles – TRAKK**



    c. From the results, we will create an IT-Role for all users with the Input entitlement. To do this, right click Group1 and select **Create Role**.



    d. Configure the Role:
        i. Name: **TRAKK – Basic**
        ii. Owner: **The Administrator**
        iii. Container Role: **TRAKK**

iv. Scroll down and click **Save**

4. Enable the **TRAKK – Basic** role

    a. Go to the **Role Viewer** tab, click **Refresh** and select the **TRAKK-Basic** Role

    b. Edit this role and enable it.

    c. Scroll down and select **Submit**

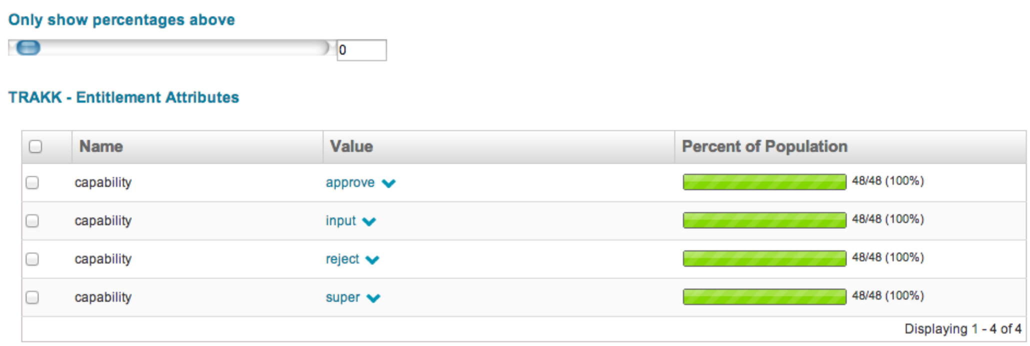
5. We will now create a child role to the **TRAKK – Basic**

    a. Select the **Entitlement Analysis** tab

    b. Select **TRAKK** as the application

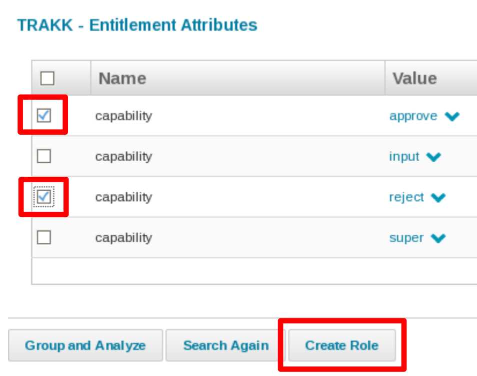
    c. Under Identity Attributes: Is Manager: **True**

    d. Select **Search**

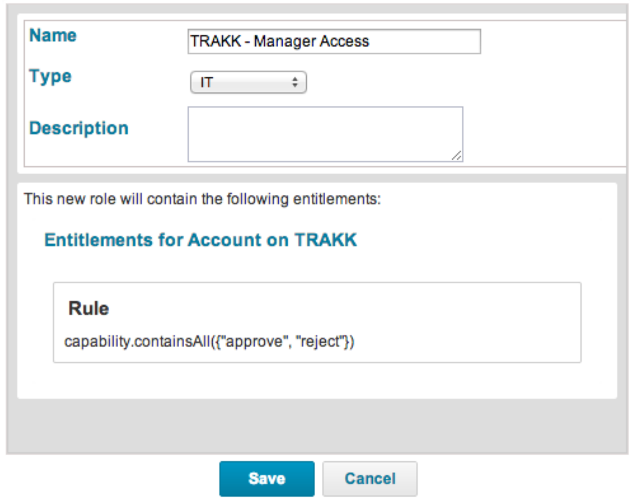


    e. From these results, we can see that all Managers that have TRAKK access have the same set of entitlements, which include the ability to approve and reject entitlements.

    f. We will create a new role from the entitlement analysis that will include these two entitlements. Select the checkboxes next to **approve** and **reject** and click **Create Role**



g. Name the Role **TRAKK – Manager Access**, and **Save**



h. Go back to the **Role Viewer** tab and **Refresh**. You should see the **TRAKK – Manager Access** role in the role hierarchy.

i. Select **TRAKK – Manager Access** and in the right side of the screen, select **Edit Role**

j. Scroll down to **Inherited Roles** and select **Modify Inheritance**

k. Enter **TRAKK** in the Search Box and select **TRAKK-Basic** and then select **Add** and **Save**

l. Scroll Down and select **Submit** to save the role.

m. Once again, go to the **Role Viewer** tab, **Refresh** and take a look at the changes to the role hierarchy.

n. Note that we have made the Manager role inherit from the Basic role. This is so that our hierarchy reflects the following:

   i. All users have Basic access to TRAKK (input)

   ii. Some users have Basic access plus additional Manager access to TRAKK (approve/reject)

   iii. A user with the Manager access to TRAKK will inherit the Basic access as well since it's defined in its inheritance path.

o. Next, we'll model super user access to TRAKK (using the capability "super".)

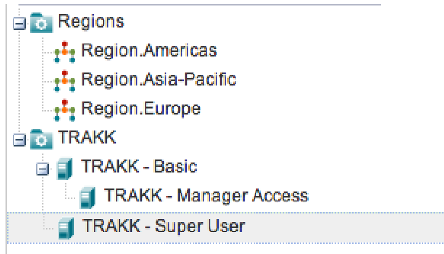
Create an IT Role with Direct Entitlements

Entitlements can be associated to a role directly or through a profile. A profile allows for more complex associations, while a direct entitlement is just that - a direct specification of the entitlements that make up a given role. Both provide the criteria that IdentityIQ uses to detect who has a given role, and specifies the entitlements to provision when assigning a role. In this exercise, we will create a role and directly define its entitlements.

1. Navigate to **Define → Roles** and make sure the **Role Viewer** tab is selected
2. Click **Add**
3. Define a new role as follows:
    a. Name: **TRAKK - Super User**
    b. Display Name: **TRAKK - Super User**
    c. Type: **IT**
    d. Owner: **The Administrator**
    e. Inherited Roles: select **Modify Inheritance**
        i. Choose **TRAKK (Organizational Role)**
        ii. **Add,** then **Save**
    f. **Entitlements:** click **Add**
        i. Application: **TRAKK**
        ii. Field: **capability**
        iii. Select Entitlement: **super**
        iv. Save

    g. Scroll down and click **Submit** to save the role.

4. Confirm that your role hierarchy looks like this:



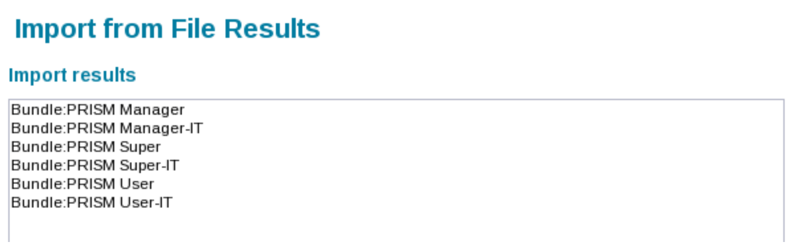
Load a Role Model for the PRISM Application

Another way to create roles is to load them via XML role definitions. Next we will load roles for the PRISM application.

1. Navigate to **System Setup → Import from File** and load the following file:

   /home/spadmin/ImplementerTraining/config/PRISM/Roles-PRISM.xml

2. Confirm that six total roles were loaded. Three IT Roles and three Business Roles



3. View the PRISM roles to complete the following chart of the PRISM role model. The PRISM Super and the PRISM Super-IT entries have been completed as examples.

Role Name	Type	Required Role	Entitlement (Profile)
PRISM Super	Business	PRISM Super-IT	Not applicable (only for IT roles)
PRISM Manager			
PRISM User			
PRISM Super-IT	IT	Not applicable (only for business roles)	Group contains “Super”
PRISM Manager-IT			
PRISM User-IT			

Exercise #2: Assign and Detect Business Roles

Objective

To learn how roles are assigned and detected as part of the identity refresh process.

Overview

In this section we will run a task that will do the following:

- Iterate over each identity
- Look at the Identity Attributes and Entitlements that are possessed by each Identity
- Determine if any Business Roles should be assigned to an Identity
- Determine if an Identity has the appropriate IT Entitlement Access to detect the appropriate IT Roles.

Assign Business Roles and Detect IT Roles

In order to assign and detect roles, we need to run a task.

1. Navigate to **Monitor → Tasks** and open the task called: **Refresh Entitlement Correlation**

    a. List the option selected for this task:

    ____

    b. Execute the task.

Refresh Entitlement Correlation Attributes

Attribute	Value
Identities examined	235
Role changes	157
Extra entitlement changes	157

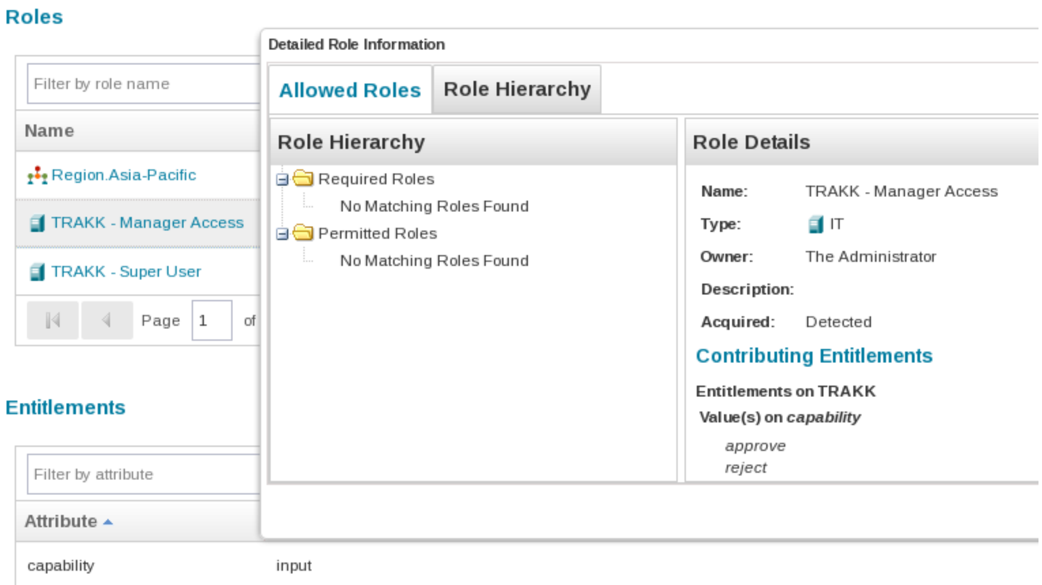
2. Navigate to **Define → Identities** and confirm that Business Roles have been assigned, and that the IT Roles have been detected.

Identities

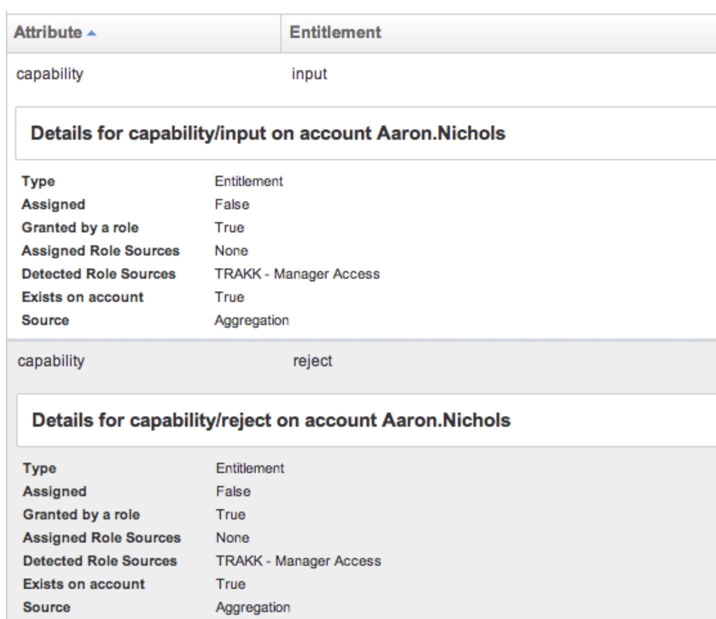
Filter by Identity Name

User Name	First Name	Last Name	Manager	Assigned Rol	Detected Role Summ	Risk Score
Aaron.Nich...	Aaron	Nichols		Region.Asi...	TRAKK - Manager A...	763
Adam.Ken...	Adam	Kennedy	Douglas.Fl...	Region.Eur...	TRAKK - Basic	500
Alan.Bradley	Alan	Bradley	Eugene.Ha...	Region.Asi...		0
Albert.Woods	Albert	Woods	Patrick.Jen...	Region.Eur...	TRAKK - Basic	500
Alice.Ford	Alice	Ford	Stephanie....	Region.Eur...	TRAKK - Basic	500

3. Click **Aaron.Nichols** and look at his **Entitlements** and notice that he now has an assigned Business Role based on his Region, and a few detected IT Roles based on his access to the TRAKK application.



4. Click a few individual entitlements to see the meta information that we are storing with regards to each entitlement. Note that these entitlements are granted by a role as the role definition includes these entitlements:



5. Click the **Show only additional entitlements** options to hide those entitlements that are included in a role.

6. Run a **Manager** certification to confirm that Roles are now part of the certification:

    a. Recipient: **Catherine.Simmons**

    b. Run Now: **checked**

    c. Confirm the following

        i. Included Access, Entitlements: **selected**

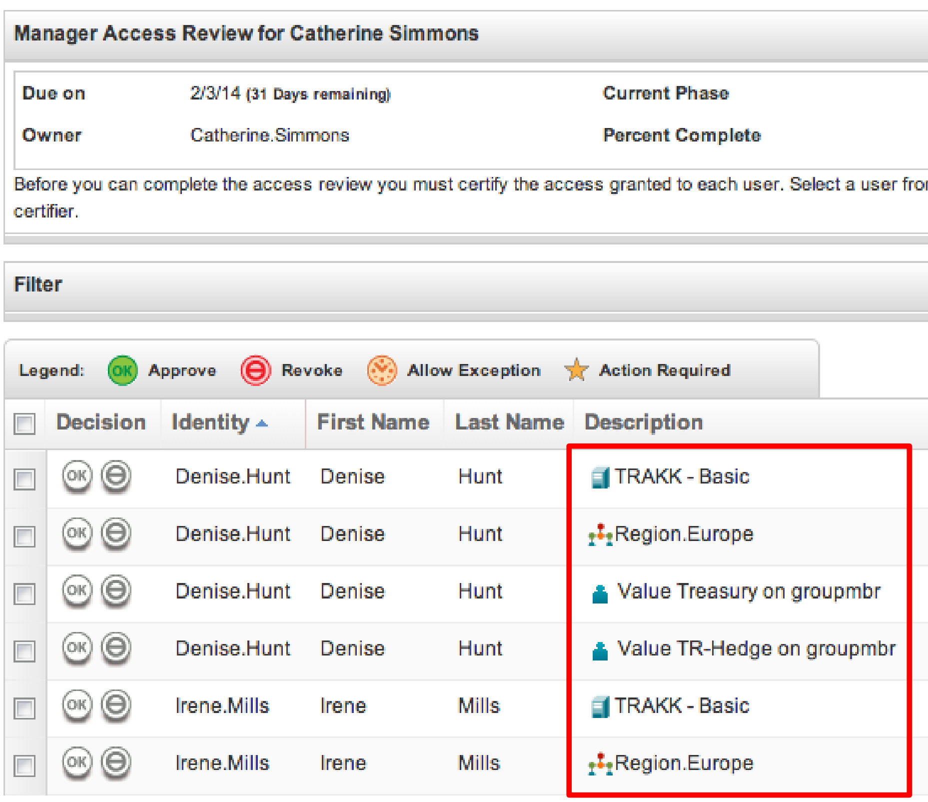
        ii. Include Additional Entitlements: **checked**

        iii. Include Roles: **checked**

        iv. Include Policy Violations: **checked**

    d. Select **Schedule Certification**

    e. Login as **Catherine.Simmons/xyzzy** and verify in the Access Review that Roles are part of the certification now.



Exercise #3: Using Roles to Provision Access to the PRISM Application

Objective

In this section we will use Role assignments to provision IT access to the PRISM application.

Overview

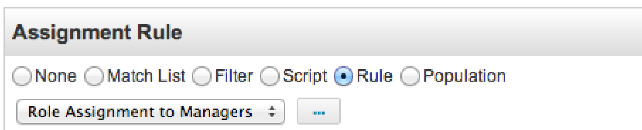
The PRISM application is a new application and only has two current user accounts on the system:

- PRISM ADMIN – An Out of the Box Account that came with the software
- Walter.Henderson – The owner of the application and the only user to create an account on the system

As part of this exercise, we will assign the “PRISM Manager” Business Role to all users that are managers at the company. We will do this by modifying the “PRISM Manager” Role to have assignment logic that defines that manager’s will be assigned to this role. We will then assign this role to everyone and this will cause provisioning to occur.

Modify Business Roles to have Assignment Logic

1. Edit the **PRISM – Manager** role
2. Scroll down to **Assignment Rule**
    a. Select **Rule**
    b. Click the … to edit the Rule
        i. Rule Name: **Role Assignment to Managers**
        ii. Script: **return identity.getManagerStatus();**
        iii. Click **Save**
    c. Choose the rule you just created:



    d. Scroll down and **Submit** to save the role changes.
3. This rule will return true if an Identity is a manager. When we refresh assigned and detected roles, this rule will assign the **PRISM – Manager** role to each identity that is a manager. In turn, this will cause the required IT Role, **PRISM – Manager-IT** to get provisioned as part of the refresh processing. This will create an account and add the user to the Manager group on the **PRISM** application.

Create a new Refresh Task that will Provision Access

1. Navigate to **Monitor → Tasks** and create a new task of type **Identity Refresh**
    a. Name: **Refresh and Provision Roles**
    b. Select both options on the task:
        i. Refresh assigned, detected roles and promote additional entitlements
        ii. Provision assignments
    c. Click **Save and Execute**
    d. Wait until the task finishes, as it will take awhile since it will look at all 200+ identities. While the task is running you can observe the progress, by clicking on the **Pending…** task in the **Task Results** window and watching the progress as it runs.
    e. Once the task is finished successfully, go to a terminal window, and login to MySQL:

```
[spadmin@training ~]$ mysql -u root -p
Enter password: root
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 64
Server version: 5.1.58-community MySQL Community Server (GPL)

Copyright (c) 2000, 2010, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> use prism
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> select * from users;
```

In your results, you should see that several managers were provisioned with access to the PRISM application:

…

```
| A      | N      | NULL       |
| Sara.Berry        | NULL        | Sara      | Berry      | Manager
| A      | N      | NULL       |
| Stephanie.Coleman | NULL        | Stephanie | Coleman    | Manager
| A      | N      | NULL       |
| Susan.Martin      | NULL        | Susan     | Martin     | Manager
| A      | N      | NULL       |
| Victor.Pierce     | NULL        | Victor    | Pierce     | Manager
| A      | N      | NULL       |
| whenderson        | NULL        | Walter    | Henderson  | User, Manager, Super
| A      | Y      | 2012-01-01 |
| William.Moore     | NULL        | William   | Moore      | Manager
| A      | N      | NULL       |
+-------------------+-------------+-----------+------------+----------------------
+--------+--------+------------+
49 rows in set (0.00 sec)
```

Exercise #6: Creating and Extending a Custom Report

Objective

To understand the steps involved in extending, creating, and customizing IdentityIQ reports.

Overview

For this exercise, we will load a custom report and observe how it functions within IdentityIQ. We will configure the report using the GUI. Then we will investigate the report XML using debug. Next we will extend the report by adding more columns. This section ends with three optional extensions.

Load and Investigate the Custom Report Definition XML File

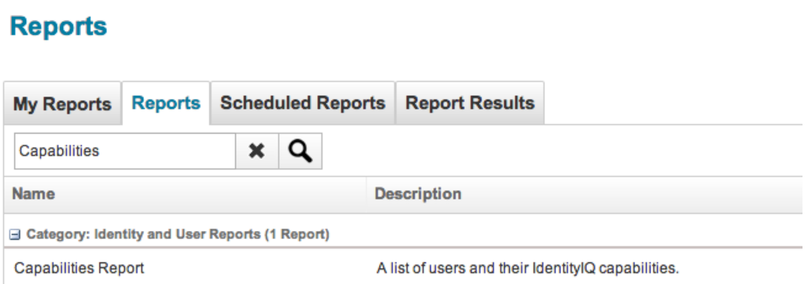
1. Navigate to **System Setup → Import from File** and load the file:

   /home/spadmin/ImplementerTraining/config/Report-CustomCapabilities.xml

2. Navigate to **Analyze → Reports** and click the **Reports** tab

   a. Filter the list of reports, filter on **Capabilities**

   b. Click **Capabilities Report**

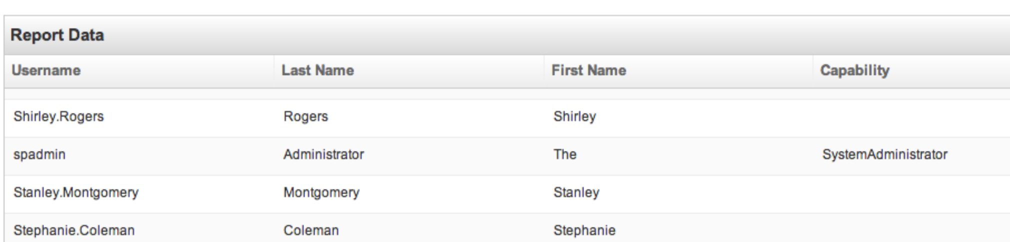


   c. Configure the report as follows:

      i. Name: **My Capabilities Report**

   d. Click **Save and Preview** to preview the report.

   e. Page through the report and check to see that the user **spadmin** has the **SystemAdministrator** capability.



Report Data

Username	Last Name	First Name	Capability
Shirley.Rogers	Rogers	Shirley	
spadmin	Administrator	The	SystemAdministrator
Stanley.Montgomery	Montgomery	Stanley	
Stephanie.Coleman	Coleman	Stephanie	

3. Click Refine Report (top, right) and click the Report Layout Section.

    a. Reorder the columns so that the Capability column is displayed first.

    b. Preview the report.

Report Data

Capability	Username	Last Name	First Name
	Aaron.Nichols	Nichols	Aaron
	Adam.Kennedy	Kennedy	Adam
	Alan.Bradley	Bradley	Alan
	Albert.Woods	Woods	Albert

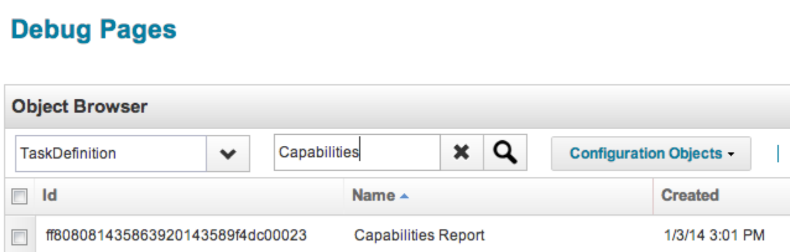
4. Change the report so that Username is displayed first, followed by Capability and omit First Name and Last Name from this report.

Report Data

Username	Capability
Aaron.Nichols	
Adam.Kennedy	
Alan.Bradley	

5. Save and Preview the report.

6. Navigate to the **Debug Page** and search for **TaskDefinition** objects and look for the **Capabilities Report** that we just loaded. Click the **Capabilities Report** and view the report XML.



7. Observe the XML to see what is causing the report to generate the information in the report.

    a. Notice that the DataSource defines the base object (in our case Identity) and the default sort order.

```
<DataSource defaultSort="name" objectType="Identity" type="Filter">
```

b. Notice that the ReportColumnConfigs drives the columns shown in the report.

```
<Columns>
  <ReportColumnConfig field="identity" header="rept_user_details_col_identity"
property="name" sortable="true" width="110"/>
  <ReportColumnConfig field="lastName" header="rept_user_details_col_lastname"
property="lastname" sortable="true" width="110"/>
  <ReportColumnConfig field="firstName" header="rept_user_details_col_firstname"
property="firstname" sortable="true" width="110"/>
  <ReportColumnConfig field="capability" header="Capability"
property="capabilities.name" sortable="true" width="110"/>
</Columns>
```

c. Effectively, this report grabs all the identities in the system and lists the four columns (name, lastname, firstname, capabilities.name) defined.

d. Close the Capabilities XML.

8. Still on the **Debug Page**, search again for **TaskDefinition** objects and this time look for the **My Capabilities Report** that we just created and view the report XML.

   a. Observe that this definition includes the specific configuration for **My Capabilities Report**.

      i. Notice the entry key for reportColumnOrder. Why are only two columns listed?

      ____

      ____

   b. Observe that the **My Capabilities Report** XML references the report template from which it was configured.

```
<Reference class="sailpoint.object.TaskDefinition"
id="ff80808140569e2201407d0889211672" name="Capabilities Report"/>
```

   c. Close the **My Capabilities Report** XML.

Extend the Report

1. Continuing to work on the **Debug Page**, redisplay the **Capabilities** XML.

2. Extend the Columns in the Capabilities Report to add the user's region and location. Add the following ReportColumnConfigs to the existing Columns.

```
<ReportColumnConfig field="region" header="Region" property="region" sortable="true"
width="110"/>
<ReportColumnConfig field="location" header="Location" property="location"
sortable="true" width="110"/>
```

3. Navigate to **Analyze → Reports** and click the **Reports** tab.

4. Configure a new Capabilities Report.

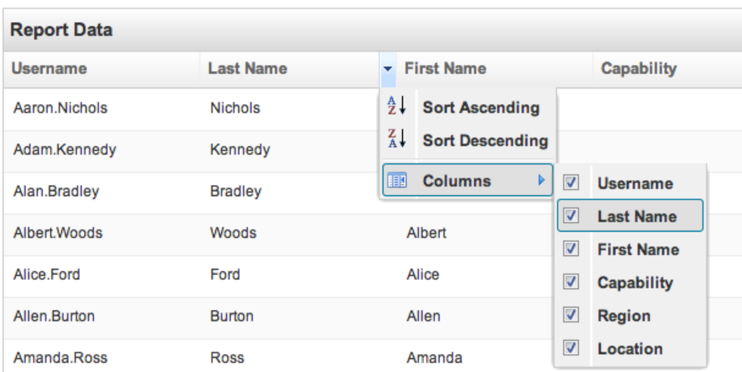
   a. Name: **My Capabilities Report 2**

5. Click Save and Preview and confirm that the Region and Location columns are now displayed.

Report Data

Username	Last Name	First Name	Capability	Region	Location
Aaron.Nichols	Nichols	Aaron		Asia-Pacific	Singapore
Adam.Kennedy	Kennedy	Adam		Europe	London
Alan.Bradley	Bradley	Alan		Asia-Pacific	Singapore
Albert.Woods	Woods	Albert		Europe	Brussels
Alice.Ford	Ford	Alice		Europe	Brussels

6. Hover over **Last Name** to activate the menu. From the menu click **Columns** and remove **Last Name** and **First Name** from the report.



   a. Save the report.

7. From the **Select an action** menu (top, left), select **Run Now**, and when the report is complete click **View Report Results**.

   a. What are the two format options for downloading a report?

______________________________ ______________________________