SailPoint

IdentityIQ – L03

Date
–

Contents

Exercise 1
Defining a Role Model

Use Case ID:	L03 – E01		
Use Case Name:	Defining Role Model		
Created By:		**Last Updated By:**	
Date Created:		**Last Revision Date:**	
Actors:	Admin, IIQ System		
Description:	Learn how to define roles and to assign them to Identities and detect them from account entitlements		
Preconditions:	IIQ System is Up and Running		
Post conditions:	Defining role model		
Normal Flow:	1. Understanding roles 2. Creating role model		
Exceptions:	NA		
Dependent Usecase:	NA		
Assumptions:	NA		
Notes and Issues:	NA		

Overview:

In this usecase, we are going to setup the following:

- Understanding the roles
- Creating role modeling
- Assigning roles to identities

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 Setup ❼ Roles** and select **New Role** and choose **Role**

Name: **TRAKK**

Display Name: **TRAKK**

Type: **Organizational**

Owner: **The Administrator**

Click: **Submit**

2. Create Regions Container

    a. **New Role** and choose **Role**

i. Name: **Regions**

ii. Display Name: **Regions**

iii. Type: **Organizational**

iv. Owner: **The Administrator**

v. 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**

6. Observe the results of Role Mining

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

   b. Select the Role Mining results and observe:

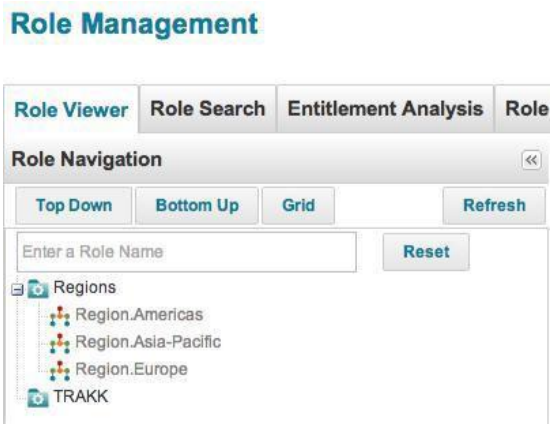
Details

Name	Business Roles - Regions	Started By	The Administrator
Type	Role Mining	Started	1/3/14 12:06:47 PM
Description	Mine Business Roles based on organizational and functional identity attributes	Completed	1/3/14 12:06:47 PM
Status	Success		

Business Roles - Regions Attributes

Attribute	Value
Identity Mining Attributes:	[region]
Roles mined:	3
Roles updated:	0
Coverage of mined roles:	97.4 percent

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



3. 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**

1 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**.

4. Configure the Role:
   - **a.** Name: **TRAKK – Basic**
   - **b.** Owner: **The Administrator**
   - **c.** Container Role: **TRAKK** Scroll down and click **Save**

1 Enable the **TRAKK – Basic** role

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

i. Edit this role and enable it.

j. Scroll down and select **Submit**

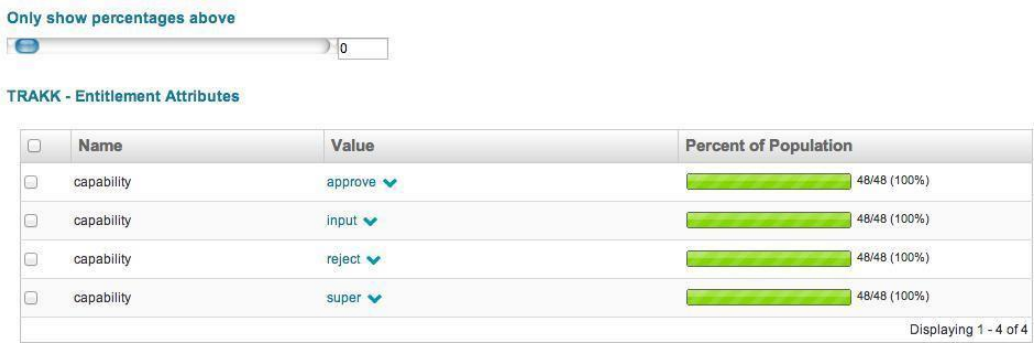
2 We will now create a child role to the **TRAKK – Basic**

h. Select the **Entitlement Analysis** tab

i. Select **TRAKK** as the application

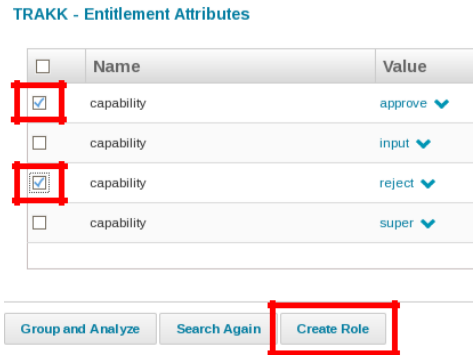
j. Under Identity Attributes: Is Manager: **True**

k. Select **Search**

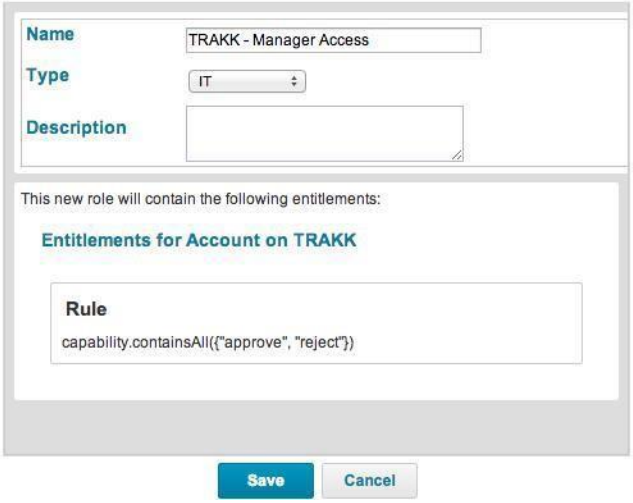


6. From these results, we can see that all Managers that have TRAKK access have the same set of entitlements, which include the ability to approve and reject entitlements.

7. 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**



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

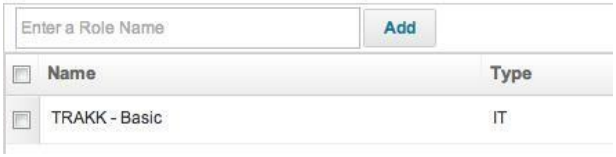


b. Go back to the **Role Viewer** tab and **Refresh**. You should see the **TRAKK – Manager Access** role in the role hierarchy.

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

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

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



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

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

h. 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.

i. 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.

a **Navigate to Setup ❼ Roles** and make sure the **Role Viewer** tab is selected

b Click **Add**

c Define a new role as follows:

iv. Name: **TRAKK - Super User**

v. Display Name: **TRAKK - Super User**

vi. Type: **IT**

vii. Owner: **The Administrator**

viii. Inherited Roles: select **Modify Inheritance**

Choose **TRAKK (Organizational Role)**

Add, then **Save**

ix. Entitlements: click **Add**

Application: **TRAKK**

Field: **capability**

Select Entitlement: **super**

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.

c. **Navigate to Global Setting ❼ Import from File** and load the following file:

C:\Training\config\PRISM\Roles-PRISM.xml

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

1 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

Use Case ID:	L03 – E02		
Use Case Name:	Assign and Detect Business Roles		
Created By:		**Last Updated By:**	
Date Created:		**Last Revision Date:**	
Actors:	Admin, IIQ System		
Description:	To learn how roles are assigned and detected as part of the identity refresh process		
Preconditions:	IIQ System is Up and Running		
Post conditions:	Assigning roles		
Normal Flow:	1. Defining Business roles 2. Assigning roles		
Exceptions:	NA		
Dependent Usecase:	NA		
Assumptions:	NA		
Notes and Issues:	NA		

Overview:

In this usecase, we are going to setup the following:

- Understanding the business roles and creation
- Assigning roles to identities

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

2. Iterate over each identity
3. Look at the Identity Attributes and Entitlements that are possessed by each Identity
4. Determine if any Business Roles should be assigned to an Identity
5. 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.

a) Navigate to **Monitor ➔ Tasks** and open the task called: **Refresh Entitlement Correlation**

i. List the option selected for this task:

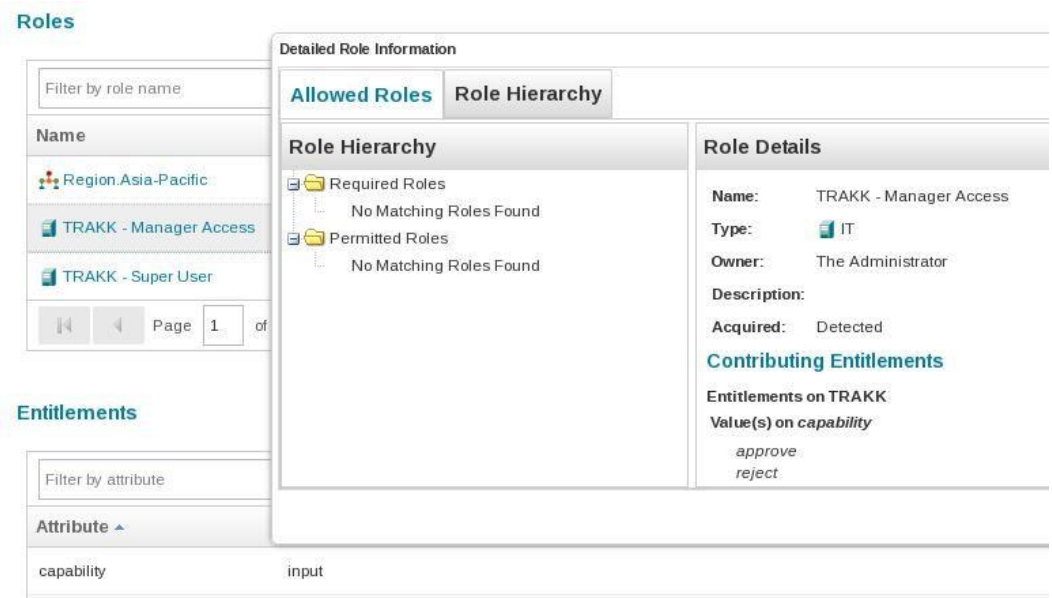
_____

ii. Execute the task.

Refresh Entitlement Correlation Attributes	
Attribute	**Value**
Identities examined	235
Role changes	157
Extra entitlement changes	157

b) **Navigate to identities ➔ Identity Warehouse** and confirm that Business Roles have been assigned, and that the IT Roles have been detected.

1. 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.



2. 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:

Attribute	Entitlement
capability	input

Details for capability/input on account Aaron.Nichols

Type	Entitlement
Assigned	False
Granted by a role	True
Assigned Role Sources	None
Detected Role Sources	TRAKK - Manager Access
Exists on account	True
Source	Aggregation

capability	reject

Details for capability/reject on account Aaron.Nichols

Type	Entitlement
Assigned	False
Granted by a role	True
Assigned Role Sources	None
Detected Role Sources	TRAKK - Manager Access
Exists on account	True
Source	Aggregation

Exercise 3

Using Roles to Provision Access to the PRISM Application

Use Case ID:	L03 – E03		
Use Case Name:	Role based access control to PRISM		
Created By:		**Last Updated By:**	
Date Created:		**Last Revision Date:**	
Actors:	Admin, IIQ System		
Description:	In this section we will use Role assignments to provision IT access to the PRISM application		
Preconditions:	IIQ System is Up and Running		
Post conditions:	Assigning roles		
Normal Flow:	1. Defining Business roles 2. Assigning roles		
Exceptions:	NA		
Dependent Usecase:	NA		
Assumptions:	NA		
Notes and Issues:	NA		

Overview:

In this usecase, we are going to setup the following:

- RBAC (Role based access control)

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

β. PRISM ADMIN – An Out of the Box Account that came with the software

χ. 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

f. Edit the **PRISM – Manager** role

g. Scroll down to **Assignment Rule**

Select **Rule**

Click the … to edit the Rule

Rule Name: **Role Assignment to Managers**

Script: **return identity.getManagerStatus();**

Click **Save**

Choose the rule you just created:

Scroll down and **Submit** to save the role changes.

h. 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

h. Navigate to **Setup** ❼ **Tasks** and create a new task of type **Identity Refresh**

Name: **Refresh and Provision Roles**

Select both options on the task:

Refresh assigned, detected roles and promote additional entitlements

Provision assignments

Click **Save and Execute**

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.

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)
```