SailPoint

# IdentityIQ – L02

Date

–

# Contents

# Exercise 1

## Groups and Populations

| | | | |
|---|---|---|---|
| **Use Case ID:** | L02 – E01 | | |
| **Use Case Name:** | Groups and Population | | |
| **Created By:** | | **Last Updated By:** | |
| **Date Created:** | | **Last Revision Date:** | |
| **Actors:** | Admin, IIQ System | | |
| **Description:** | The objective of this exercise is to use built-in features of the product to organize identities through the use of Groups and Populations. We will also explore some reports that are useful when dealing with Identities | | |
| **Preconditions:** | IIQ System is Up and Running | | |
| **Post conditions:** | Understanding Groups and Population | | |
| **Normal Flow:** | 1. Entitlements handling<br>2. Creation of population | | |
| **Exceptions:** | NA | | |
| **Dependent Usecase:** | NA | | |
| **Assumptions:** | NA | | |
| **Notes and Issues:** | NA | | |

## Overview:

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

- Entitlements
- Rules to assign ownership
- Advanced analytics understanding
- Creating populations

For our implementation, we have been asked to generate some groups based on the following Identity Attributes:

- Status (whether an Employee or Contractor)
- Location (Austin, Tokyo, etc.)
- Manager

Because we defined these Identity Attributes as group factories earlier when we defined the identity mappings, it is extremely easy to use IdentityIQ to automatically calculate and generate groups of identities based on these fields. These groups can be used in reporting and other portions of the product.

We will also be using rules to assign ownership to each group.

Additionally, we want to use Advanced Analytics to define some populations based on specific criteria. Populations are similar to groups, except that they are driven off of multiple search criteria whereas Groups are statically defined based off a single Identity attribute.

For our implementation, we want to generate two populations.

- Active Managers who are not Contractors in Asia-Pacific Region only
- All users who have Privileged accounts on any application

# Using Group Factories to Generate Groups

We will now configure and generate groups for the Status, Location and Manager attributes on our identities.

1. Load Rules to determine Group ownership

   Navigate to **Global Setting ➔ Import from File** and load the following two rules:
   **/C:\Training\admin\backup\Rule-GroupOwner-AssignManagerAsOwner.xml**

   **/C:\Training\admin\backup\Rule-GroupOwner-HighestRanking.xml**

2. Review the attributes for which the Group Factory option was selected.
    1. **Navigate to Global Setting ➔ Identity Mappings** and list the 6 attributes fr

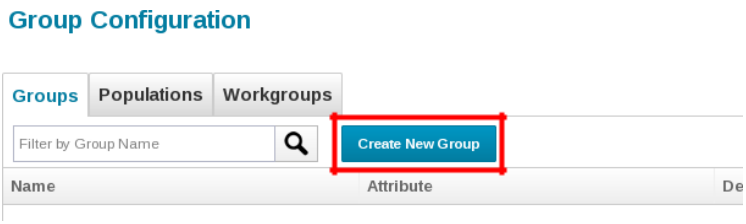
       which Group Factory was selected:

       _____ _____

       _____ _____

       _____ _____

3. **Navigate to Setup ➔ Groups** and select **Create New Group** and fill in the following fields:




**d.** Name: **Status**

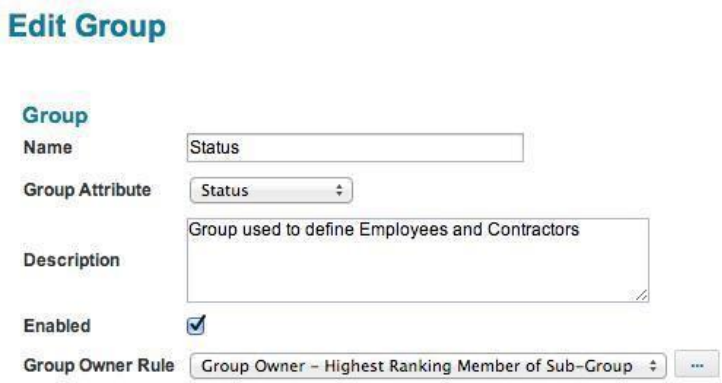
**e.** Group Attribute: **Status**

i. Notice that the choices for Group Attribute is populated from the list of attributes for which Group Factory was selected.

**f.** Description: **Group used to define Employees and Contractors**

**g.** Enabled: **Checked**

**h.** Group Owner Rule: **Group Owner – Highest Ranking Member of Sub-Group**




Select **Save**

1. Repeat the same steps for the Location attribute

   **a.** Select **Create New Group**

   **b.** Name: **Location**

   **c.** Group Attribute: **Location**

   **d.** Description: **Groups based off of each Identity's location attribute.**

   **e.** Enabled: **Checked**

   **f.** Group Owner Rule: **Group Owner – Highest Ranking Member of Sub-Group**

   **g.** Select **Save**

2. Repeat the same steps for the Manager attribute

   **a.** Select **Create New Group**

   **b.** Name: **Manager**

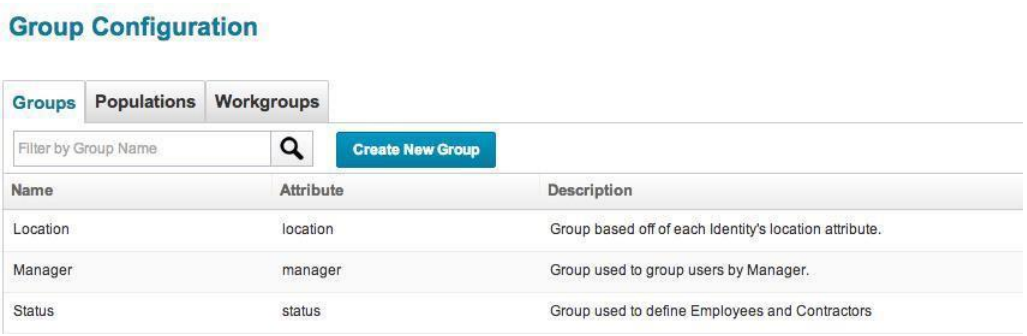
   **c.** Group Attribute: **Manager**

   **d.** Description: **Users grouped by Manager.**

   **e.** Enabled: **Checked**

   **f.** Group Owner Rule: **Group Owner – Assign Manager**

   **g.** Select **Save**




3. Generate Groups using the newly created group configurations and confirm that they were created correctly:

   **a.** Run the task: **Refresh Groups**

b. **Navigate to Setup ➔ Groups** and check all three group factories to determine if the groups were created correctly. Look for there to be many subgroups and the owner fields should be populated.

Here is an example of the Location groups:

**Sub-Groups**

| Name | Member Count | Policy Violations | Composite Score | Owner |
|---|---|---|---|---|
| Austin | 27 | 0 | 166 | James.Smith |
| Brazil | 25 | 0 | 170 | John.Williams |
| Brussels | 26 | 0 | 173 | Jerry.Bennett |
| London | 25 | 0 | 250 | Amanda.Ross |
| Munich | 25 | 0 | 170 | Dennis.Barnes |
| No Location | 6 | 0 | 208 | The Administrator |

**Note:** These group themselves are not dynamic. You must run the **Refresh Groups** task periodically to update them. Between runs of **Refresh Groups**, the groups themselves remain static, but the membership is always based off a dynamic query.

# Generate Populations

Next, we will generate some populations of users that represent some interesting sets of users. Populations can be generated off any of the data that is available via the Advanced Analytics feature of IdentityIQ.

For our implementation, we want to generate the populations.

1. Active Managers who are not Contractors in Asia-Pacific Region only

1. **Navigate to Inteligence ➔ Advanced Analytics**
2. Under the **Identity Search** tab, click **Clear Search** and enter the following search criteria:

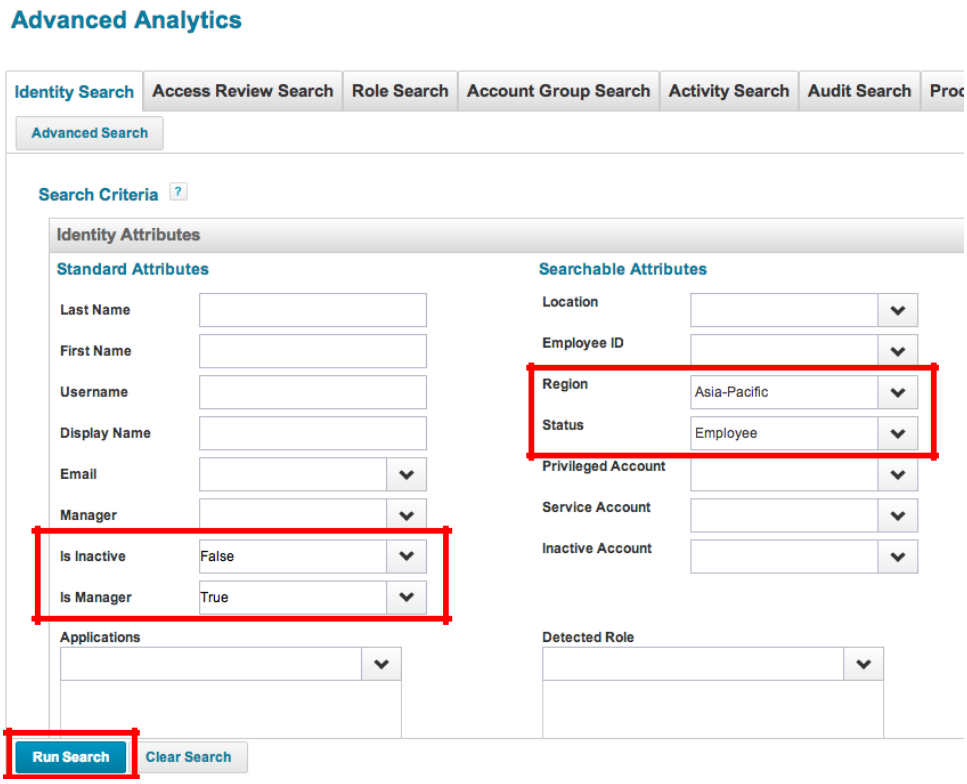
   **a.** Is Inactive: **false**

   **b.** Is Manager: **true**

   **c.** Region: **Asia-Pacific**

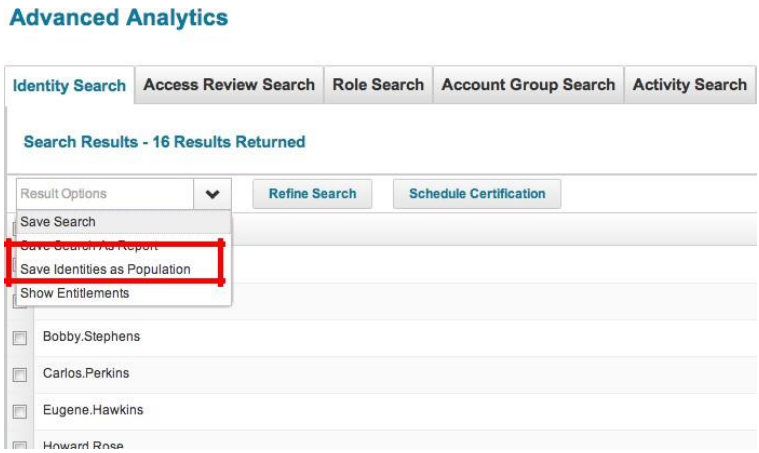
   **d.** Status: **Employee**

1 Click **Run Search**




4. You should get 16 results returned.

**5.** From the drop-down menu, select **Save Identities as Population**




**e.** Name: **Active Managers – Asia-Pacific**

**f.** Click **Save**

6. Click the population and see that you can list the members within the given population.

   **Note**: By default, these populations are only visible to the user who created them. You can edit the populations and make them Public.

   **Note:** Populations are dynamic queries, so every time you view a population, you are viewing its current members at that point in time.

# Exercise 2
## Create Policies

| | | | |
|---|---|---|---|
| **Use Case ID:** | L02 – E02 | | |
| **Use Case Name:** | Creating Policies | | |
| **Created By:** | | **Last Updated By:** | |
| **Date Created:** | | **Last Revision Date:** | |
| **Actors:** | Admin, IIQ System | | |
| **Description:** | The objective of this exercise is to create some policies. These policies will analyze identity data to determine who has violated the policies we define and to allow managers and other users to learn about the policy violations. | | |
| **Preconditions:** | IIQ System is Up and Running | | |
| **Post conditions:** | SOD policies configured | | |
| **Normal Flow:** | 1. Understanding and creating policies<br>2. Handling policy violations | | |
| **Exceptions:** | NA | | |
| **Dependent Usecase:** | NA | | |
| **Assumptions:** | NA | | |
| **Notes and Issues:** | NA | | |

## Overview:

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

- Creating different policy violations
- Handling policy violation exceptions

Now that we have loaded a rich assortment of account and account group data, we can start to mine this data to determine if we have any Policy Violations in the data set.

The client has requested that we implement three policies.

1. No user can simultaneously have the **super** and **input** access to the **TRAKK** application

2. No user can have more than one account on any system

3. For the **PAM** application, any user who has not used the system in 180 days will be considered in violation of policy

## Create an Entitlement Separation of Duties Policy

**b. Navigate to Setup ❼ Policies**

**c.** In the upper right, click **New Policy** and select **Entitlement SOD Policy**

d. Configure as follows:

**i.** Name: **TRAKK SOD Policy**

**ii.** Owner: **The Administrator**

**iii.** Violation Owner: **Manager is Violation Owner**

**iv.** State: **Active**

**v.** Send Alerts: **Checked**

Initial Notification Email: **Policy Violation**

Observers: **Aaron.Nichols**

**vi.** SOD Policy Rules: click **Create New Rule**

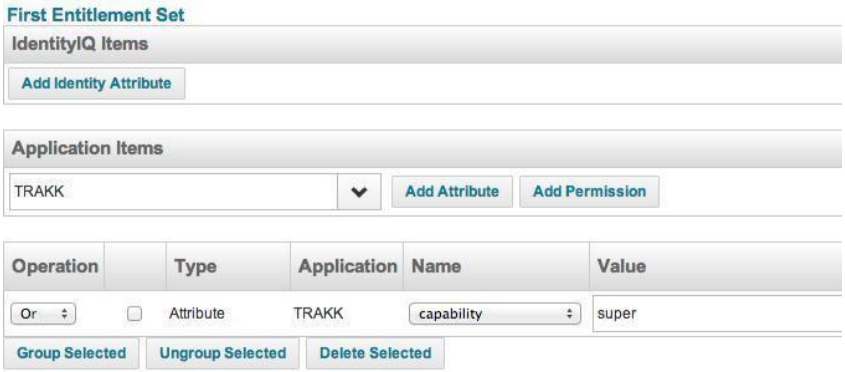
Summary: **Cannot be Super and Input at the same time**

First Entitlement Set:

**a** Application Items: **TRAKK** Select **Add Attribute**

**b** Select Name: **capability**

**c** Select Value: **super**



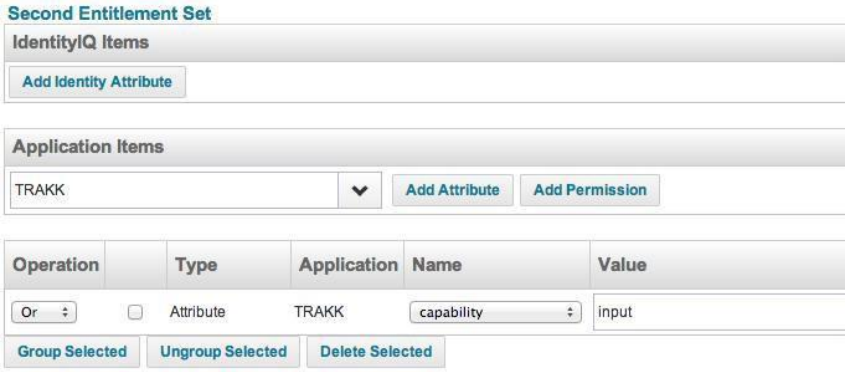

c. Second Entitlement Set:

**i** Application Items: **TRAKK**

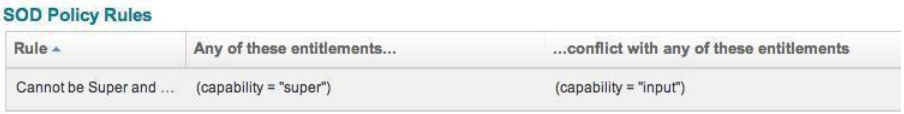
**ii** Select **Add Attribute**

**iii** Select Name: **capability**

**iv** Select Value: **input**




e. Click **Done** to complete the rule




g. Scroll down and click **Save** to complete the policy

## Create a Policy to detect more than one account per application

2. **Navigate to Setup ❼ Policies**

3. In the upper right, click **New Policy** and select **Account Policy**

4. Configure as follows:

    **a.** Name: **More than one account**

    **b.** Owner: **The Administrator**

    **c.** Violation Owner: **Manager is Violation Owner**

    **d.** State: **Active**

    **e.** Send Alerts: **Checked**

    **f.** Initial Notification Email: **Policy Violation**

    **g.** Observers: **Aaron.Nichols**

    **h.** Summary: **Multiple Application Accounts**

    i. Scroll down and click **Save** to complete the policy

## Create an Advanced rule-based Policy to detect dormant accounts

**b. Navigate to Setup ❼ Policies**

**c.** In the upper right, click **New Policy** and select **Advanced Policy**

d. Configure as follows:

    **i.** Name: **Last Login more than 180 days ago**

    **ii.** Owner: **The Administrator**

    **iii.** Violation Owner: **Manager is Violation Owner**

    **iv.** State: **Active**

    **v.** Send Alerts: **Checked**

    **vi.** Initial Notification Email: **Policy Violation**

    **vii.** Observers: **Aaron.Nichols**

    **viii.** Policy Rules: click **Create New Rule**

        **i.** Summary: **Last Login > 180 Days**

a. Selection Method: Choose **Rule**

b. Click "**...**" to edit the rule

c. Rule Name: **Violation Rule - No login for last 180 days**

d. Rule body: Copy and paste from the:

**/home/spadmin/ImplementerTraining/beanshell/PolicyViolation-NoLoginFor180Days.txt**

e. Click **Save** to save the rule

f. Make sure to choose the rule once you've saved it, then click **Done**

1. Click **Save** to save the policy

# Scan Identities for Policy Violations

3. Run the task: **Check Active Policies**

**Note:** This task is an Identity Refresh task with **Check active policies** checked

4. Check the **Task Results** tab when the task ends and confirm:

| Check Active Policies Attributes | |
|---|---|
| **Attribute** | **Value** |
| Identities examined | 235 |
| Policies checked | Last Login more than 180 days ago, More than one account, TRAKK SOD Policy |
| Policy violations | 56 |
| Policy notifications | 15 |

b. Confirm that Policy Violations were found. There are several ways you can see policy violations:

Navigate to **Manage ❼ Policy Violations**. This will show all policy violations. Click any of the TRAKK SOD policy violations to interact with it.

For **Violation Decision,** choose **Correct Violation** from the dropdown

f. Notice that you are presented with an option to remove one of the offending entitlements.


h. Navigate to **Carl.Foster's** cube and check the **Policy** tab to see a policy violation.

i. Look in each manager's Inbox for incoming workitems for each policy violation detected.

Check the Administrator's Inbox.
**Note:** The administrator will get any violations for users who don't have managers

Log out and back in as **Aaron.Nichols/xyzzy** and check his Inbox

j. Check the Email log

Launch the **Tail Email Log** shortcut and confirm that you can see emails that were sent out when policy violations were discovered.

# Exercise 3

## Defining Identity Risk Scoring

| | | | |
|---|---|---|---|
| **Use Case ID:** | L02 – E03 | | |
| **Use Case Name:** | Identity Risk Scores | | |
| **Created By:** | | **Last Updated By:** | |
| **Date Created:** | | **Last Revision Date:** | |
| **Actors:** | Admin, IIQ System | | |
| **Description:** | The objective of this section is to learn how to configure the IdentityIQ risk scoring and apply the configured scoring settings to existing Identities. | | |
| **Preconditions:** | IIQ System is Up and Running | | |
| **Post conditions:** | Identity Risk Scores population | | |
| **Normal Flow:** | 1. Understanding Identity Risk Scores<br>2. Creating different risk scores<br>3. Generating Identity risk scores | | |
| **Exceptions:** | NA | | |
| **Dependent Usecase:** | NA | | |
| **Assumptions:** | NA | | |
| **Notes and Issues:** | NA | | |

## Overview:

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

- Understanding the Identity Risk Scores
- Defining risk scores
- Populating Identity Risk Scores

Our client has stated that they want their risk score to be calculated based on several qualities:

λ. 50% of the risk score needs to be based on certification age (how recently has the identity been certified)

μ. 25% of the risk score needs to be based on Policy Violations

1. Having multiple accounts is higher risk

a. Having conflicting role is higher risk

Having not logged into PAM for 180 days is lower risk

δ. 25% of the risk score needs to be based on Entitlements owned by a user

Having Super User (super) access to TRAKK is higher risk

a Having Manager (approve, reject) access to TRAKK is medium risk

# Define Identity Risk Model

**a** Login as **spadmin/admin**
**b** **Navigate to Identities ➔ Identity Risk Model**
c Click the **Composite Scoring** tab
d Configure:

i. Role Compensated Score: 0%

ii. Entitlement Compensated Score: 25%

iii. Policy Violation Compensated Score: 25%

iv. Certification Age: 50%

e Click the **Baseline Access Risk** tab
i. Click **Entitlement Baseline Access Risk** Configuration

1 When prompted, **Save**

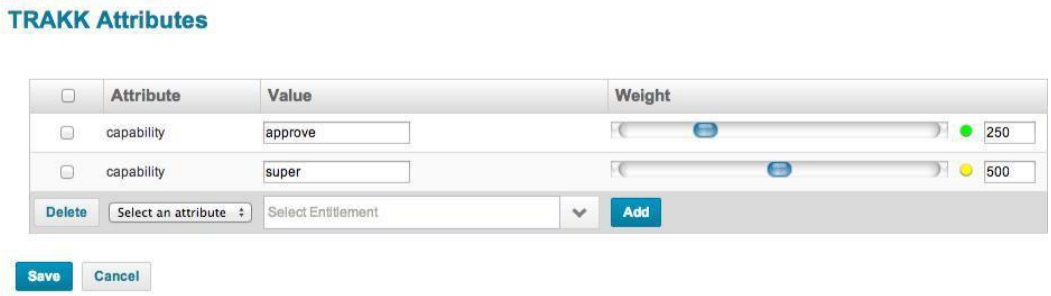
2 Select **TRAKK** as the application and click **Add**

3 Choose **Configure Attributes**

4 Configure the attributes:

e. capability: super: **500**

f. capability: approve: **250**




a Click **Save** twice to save the configuration.

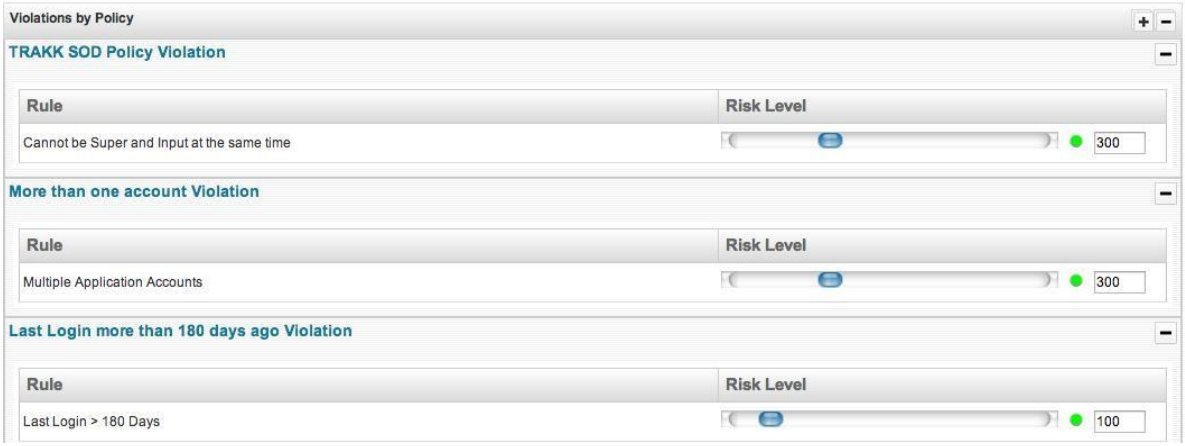
f. Click **Policy Violation Baseline Access Risk** and configure:

a Cannot be Super and Input at the same time: **300**

**1.** Multiple Application Accounts: **300**

**iii.** Last Login > 180 Days: **100**

**iv.** Click **Save** and then **Yes** to confirm



# Compute Identity Risk Scores

i Run the task: **Refresh Risk Scores**

ii Confirm the results once the task is done running:

| Refresh Risk Scores Attributes | |
|---|---|
| **Attribute** | **Value** |
| Identities examined | 235 |
| Scores changed | 186 |

iii Confirm the scoring in several places.

1 Navigate to any identity cube and check the **Risk** tab to see if risk scoring has been updated. Here is **Richard.Jackson's** cube:

Attributes | Entitlements | Application Accounts | Policy | History | Risk | Activity | User Rights | Events

**Scorecard**

| Score Category | Base Score | Compensated Sc |
|---|---|---|
| Role Compensated Score | 0 | 0 |
| Entitlement Compensated Score | 760 | 760 |
| Policy Violation Compensated Score | 600 | 600 |
| Certification Age | 1000 | ------ |

**Top Composite Score Contributors**

| Score Category | Contributor | Score | Percentage c |
|---|---|---|---|
| Certification | Identity has not been certified | 1000 | 60% |
| Entitlement | TRAKK : capability = Input,reject,approve,super | 752 | 22% |
| Policy | TRAKK SOD Policy : Cannot be Super and Input at the same time | 300 | 9% |
| Policy | More than one account : Multiple Application Accounts | 300 | 9% |

i Navigate to **Intelligence ➔ Identity Risk Scores**

2. This view organizes Risk scores into Low/Medium/High groupings

3. A user can schedule certifications for identities from this screen

ii Use Advanced Analytics to search based on Risk Score criteria. **Note:** You could use risk scoring as part of the criteria to create populations.

# Exercise 4

## Certification of PAM Application and Account Groups

| | | | |
|---|---|---|---|
| **Use Case ID:** | L02 – E04 | | |
| **Use Case Name:** | Certification of PAM | | |
| **Created By:** | | **Last Updated By:** | |
| **Date Created:** | | **Last Revision Date:** | |
| **Actors:** | Admin, IIQ System | | |
| **Description:** | Certify the PAM Application and the Account Groups that accompany it | | |
| **Preconditions:** | IIQ System is Up and Running, PAM application | | |
| **Post conditions:** | Certification related to PAM application | | |
| **Normal Flow:** | 1. Creating certifications<br>2. Certifying the accounts and entitlements<br>3. Certifications life cycle | | |
| **Exceptions:** | NA | | |
| **Dependent Usecase:** | NA | | |
| **Assumptions:** | NA | | |
| **Notes and Issues:** | NA | | |

## Overview:

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

- Understanding the Certifications
- Creating the certification campaign
- Access reviews handling

Our customer wants us to perform an initial certification of all PAM application accounts and the PAM Account Groups as well. We will do this by kicking off a certification against the Application Owner and the Owner of the Account Groups.

When creating the PAM application, we configured an Application owner for the PAM application: Patrick.Jenkins. The Account Groups on the PAM application are owned by Patrick.Jenkins as well, unless we decide to define individual Account Group owners as well.

# Generate an Application Owner Certification

i. **Navigate to Setup ➐ Certification** and from the drop-down on the right, select **Application Owner** certification.

ii. Under the **Basic** section, configure the following:

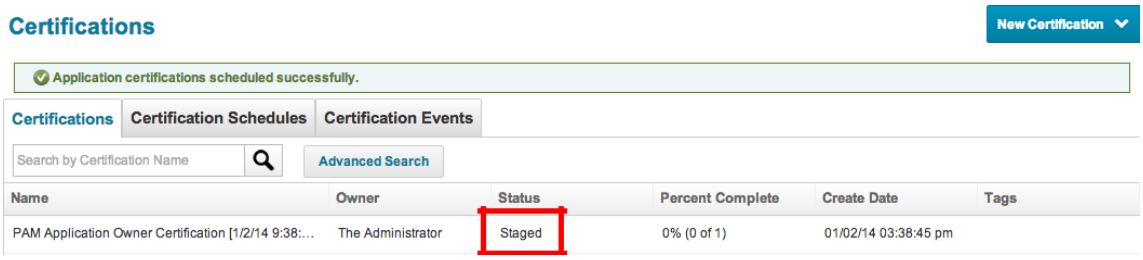
   **a.** Certification Name: **PAM Application Owner Certification [${fullDate}]**
   **b.** Certification Owner: **The Administrator**
   **c.** Applications: **PAM**
   **d.** Run Now: **Checked**

iii. Under the **Lifecycle** section, configure the following:

   **a.** Enable Staging Period: **checked**

**iv.** Choose **Schedule Certification**

v. **Note:** It can take awhile for the certification to generate. Eventually it will show up in the **Monitor ➐ Certifications** list. During this time, the system is building the certification. You can hit the refresh button periodically until the Certification shows up in a **Staged** status.

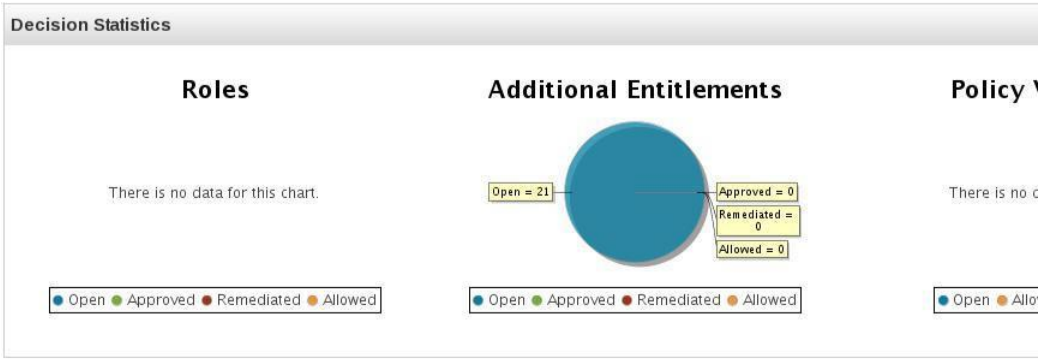


**a.** Once it shows up, click the certification, to see a staged view of the certification. During staging, the certification owner can review the entire certification, and decide whether to **Activate** or **Cancel Certification.**


**i.** Scroll down to the **Access Reviews** section and see that the overall certification consists of one Access Review assigned to Patrick.Jenkins (the Owner of the PAM application.) View the access review details by selecting the **Application Owner Access Review for PAM**

**ii.** At the bottom of the page, click **Back**

2. Click **Activate** to send the certification out to the reviewers. You can always return to the overview page to see the current status of the active certification. At this point, the certification is showing 0% complete, as we would expect.





1. Investigate the certification and answer the following questions:

b. How many Access Reviews are included in this certification? _____

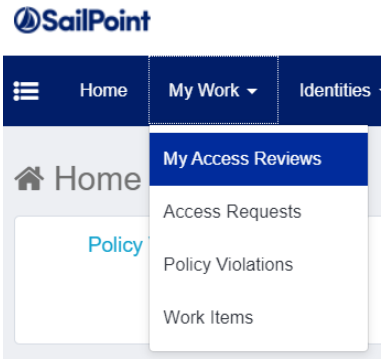
c. How many identities are included in the first Access Review? _____

d. Why is Patrick.Jenkins the certifier? _____

## Perform the Certification as Patrick Jenkins

1. Log out and back in as **Patrick.Jenkins/xyzzy**

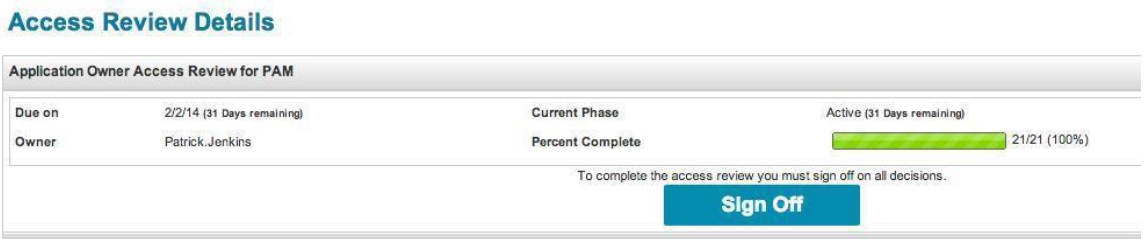
2. On the dashboard, you can see the following shortcuts. Clicking on **Access Reviews** will take you to the access review for **Patrick.Jenkins**




**Note**: You could also go to **My Work ➐ My Access Reviews**, or select the **Work Items** link to see all assigned work items, including access reviews

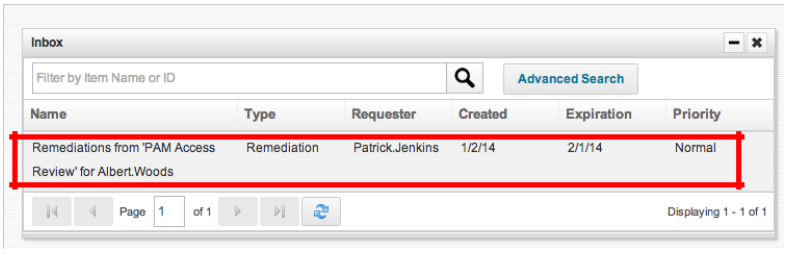
1. You can choose to perform this access review one of two ways (Worksheet View or Identity View.)

2. Either route you follow, approve everything except the three entitlements for the user **John Connor.** For the three entitlements for **John Conner,** revoke them and select **Save Changes.**
3. Once done, scroll up and **Sign Off**, then select **Finish.**




a. If we had provisioning configured for this application, we could create an external help ticket or directly de-provision to the target resource. Since we don't have either configured, an IdentityIQ work item will be generated and delivered to **Albert.Woods** (the revoker configured for the PAM application.)

b. Logout and log in as **Albert.Woods/xyzzy**. Look in his dashboard and Inbox, for a Remediation work item. Note it may take awhile, because we must wait for the certification to finish. Notice that a user can click the Work Items link or look in the Inbox to see the remediation work item.



3. Click this work item. Notice that this work item contains the remediations that were asked for during the access review:

| | |
|---|---|
| **Work Item ID** | 60 |
| **Requester** | Patrick.Jenkins |
| **Owner** | Albert.Woods |
| **Description** | Remediations from 'PAM Access Review' for Albert.Woods |
| **Created** | Jan 2, 2014 5:34:47 PM |
| **Next Event Date** | Feb 1, 2014 5:34:47 PM |
| **Expiration** | Feb 1, 2014 5:34:47 PM |
| **Priority** | Normal |
| **History** | None |

**Send Comment to Requester**

None

Add Comment

| Name | First Name | Last Name | Application | Account | Completed | Entitlements |
|---|---|---|---|---|---|---|
| John Conner | | | PAM | T1T2T3 | N/A | Remove IT from Permission Group for T1T2T3 |
| John Conner | | | PAM | T1T2T3 | N/A | Remove ADMINISTRATORS from Permission Group for T1T2T3 |
| John Conner | | | PAM | T1T2T3 | N/A | Remove TEST01 from Database Name for T1T2T3 |

4. At this point, Albert could revoke these entitlements on the PAM application manually and mark them as complete. Later in the class we will see how these changes can be provisioned automatically.

# Create an Account Group Certification

Account Group ownership will default to the owner of the application, but you could define account group owners if you wanted to. In our case, we will leave all the account groups without an owner, which means that ownership will default to the PAM application owner for all of the PAM Account Groups. This time around, we will not stage the certification.

**e.** Logout and log in as **spadmin/admin**

**f.** **Navigate to Setup ➔ Certifications** and from the drop down, select **Account Group Permissions**

g. Under the **Basic** Section, configure the following:

Name: **PAM Account Group Permissions Certification [${fullDate}]**

Certification Owner: **The Administrator**

Applications: **PAM**

Run Now: **Checked**

**h.** Click **Schedule Certification**

### *Perform the Account Group Certification*

1. Login as **Patrick.Jenkins/xyzzy** and open up the access review
2. Within the access review, click **FINANCE.** Notice that this certification is different from the application owner certification. We are now certifying the individual permissions that make up the Account Group **FINANCE**.
3. Do not perform the certification; just continue to the next exercise.

# Exercise 5

## Manager Certification with Rules

| | | | |
|---|---|---|---|
| **Use Case ID:** | L02 – E04 | | |
| **Use Case Name:** | Manager certificaition | | |
| **Created By:** | | **Last Updated By:** | |
| **Date Created:** | | **Last Revision Date:** | |
| **Actors:** | Admin, IIQ System | | |
| **Description:** | The objective of this exercise is to certify all the employees within a manager's department but exclude all inactive and contractor identities. We will also run the certification a second time, using pre-delegation rules to assign all inactive identities to the **The Administrator** | | |
| **Preconditions:** | IIQ System is Up and Running, Identities with managers | | |
| **Post conditions:** | Manger certification | | |
| **Normal Flow:** | 1. Creating certifications<br>2. Certifying the accounts and entitlements<br>3. Certifications life cycle | | |
| **Exceptions:** | NA | | |
| **Dependent Usecase:** | NA | | |
| **Assumptions:** | NA | | |
| **Notes and Issues:** | NA | | |

## Overview:

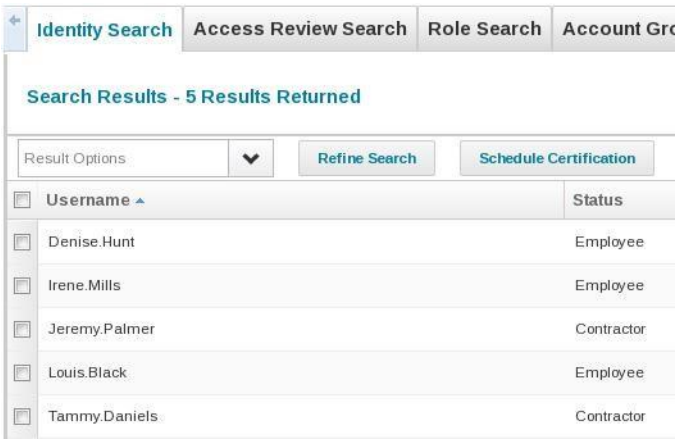
In this usecase, we are going to setup the following:

- Understanding the Manager Certification
- Generating the certification campaign
- Certifying the identities

In order to accomplish this objective, we will need to kick off a manager certification for a specific manager (in this case we will perform a certification for Catherine Simmons' direct reports.)

Catherine Simmons has five direct reports. Of these, three are Employees, and two are Contractors.

One of the identities (Denise Hunt) is currently inactive, as she has left the company. If you want to confirm, use **Advanced Analytics** to search for users with manager **Catherine.Simmons.**




We will perform a certification for this department, but we are going to create a special type of rule called an exclusion rule to exclude all contractors and inactive identities. If we set this up correctly, the only users that get certified will be Irene Mills and Louis Black.

In order to perform the pre-delegation, we will use a special rule called a pre-delegation rule to assign the access reviews to a different user (**spadmin)** if an account is inactive.

# Create a Certification for Managers using an Exclusion Rule

1. Logout and log in as **spadmin/admin**
2. **Navigate to Setup ❼ Certifications** and from the drop down, select **Manager**
3. Under the **Basic** Section, configure the following:
    a. Name: **Manager Certification – Active Employees [${fullDate}]**
    b. Certification Owner: **The Administrator**

Recipient: **Catherine.Simmons**

Run Now: **Checked**

c. Under the **Advanced** Section, configure the following:

**d.** Generate Certification(s): **For the specified managers only**

e. Exclusion Rule:

**Import Rule from**

**C:\Training\admin\backup\ManagerCertExclusion-Rule.txt**

**Save** the Rule

Make sure to **Select** the newly created rule once you are done editing it.

**4.** Click **Schedule Certification**

5. From the desktop, run the shortcut **Tail Tomcat Standard Out** and notice the output messages from the exclusion rule. You can see the logic progression as we walked through all the direct reports to determine who we should certify:

```
Entering Exclusion Rule.
Identity is Inactive : Denise.Hunt
Do not certify.
Entering Exclusion Rule.
Identity is Active and Employee: Irene.Mills
Do the certification.
Entering Exclusion Rule.
Identity is a Contractor: Jeremy.Palmer
Do not certify.
Entering Exclusion Rule.
Identity is Active and Employee: Louis.Black
Do the certification.
Entering Exclusion Rule.
Identity is a Contractor: Tammy.Daniels
Do not certify.
```

8. Also, login as **Catherine.Simmons/xyzzy** and notice that the final Account Review itself is only for two identities.