IDENTITYIQ IMPLEMENTATION AND ADMINISTRATION: ESSENTIALS

SailPoint IdentityIQ Version 8.1

With Rapid Setup

www.sailpoint.com

Copyright and Trademark Notices.

Table of Contents

Course Overview

Introduction

The exercises contained in this document are meant to accompany the *IdentityIQ Implementation and Administration: Essentials* training presentations.

These exercises are run within a Virtual Machine environment, which contains the following software:

- Oracle/Sun JDK (Version 1.8)
- Tomcat Application Server (Version 9.0.19)
- MySQL Database Server (Version 5.7.26)
- OpenLDAP Server (Version 2.4.44)
- Apache Directory Studio (Version 2.0.0)

During these exercises, you will be configuring the following:

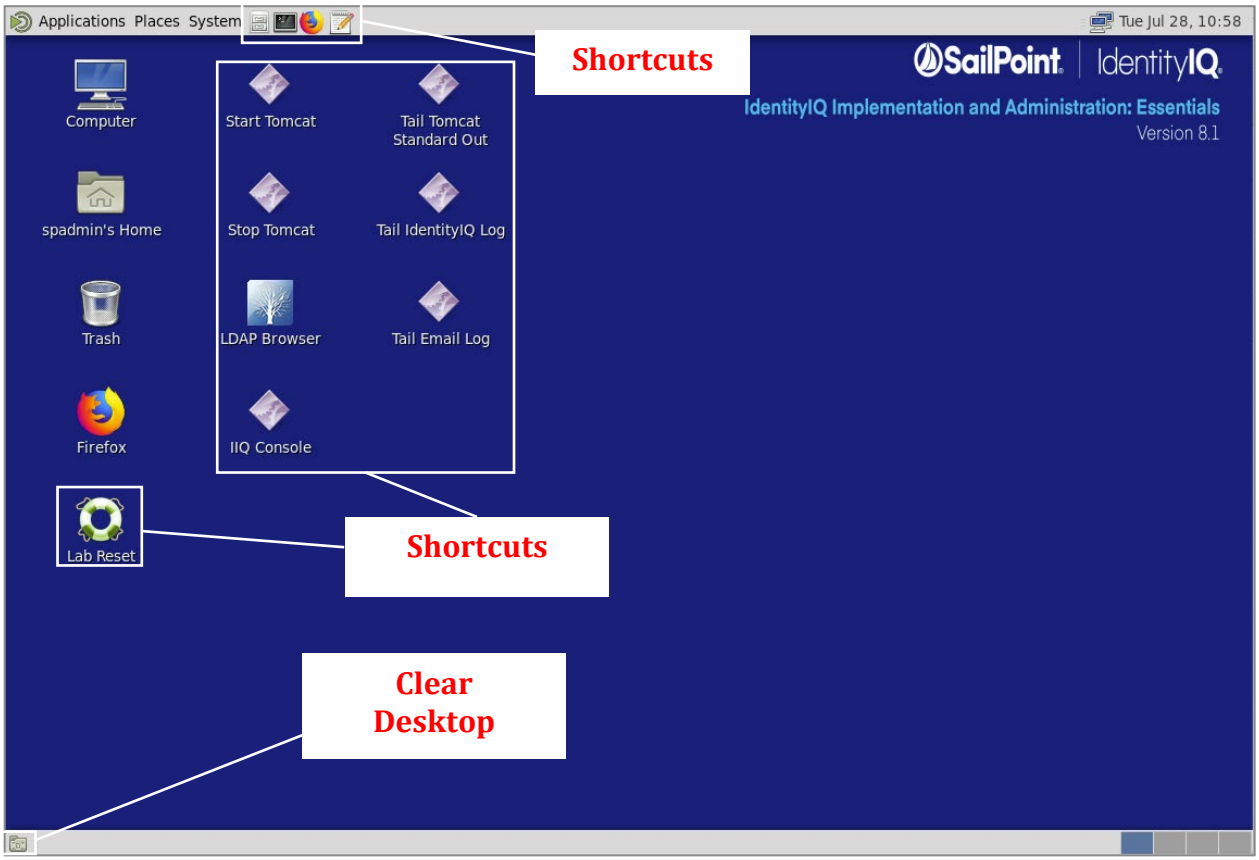
- IdentityIQ Version 8.1
    - Including Compliance Manager, Lifecycle Manager, and Rapid Setup components.

The Virtual Machine Environment

Logins	
Linux Username (VM Login)	User: spadmin Password: admin
IdentityIQ Administrator	User: spadmin Password: admin (in exercises, changed to: SailPoint1!)
MySQL Administrator	User: root Password: root
OpenLDAP Login	User: cn=Manager,dc=training,dc=sailpoint,dc=com Password: password
Install Directories	
IIQ Install Directory	/home/spadmin/tomcat/identityiq
Installer File Location	/home/spadmin/InstallImages
Training Files	/home/spadmin/ImplementerTraining
MySQL Details	
MySQL Database Name	identityiq

Shortcuts/Applications Provided

The Virtual Machine environment includes several useful shortcuts.



Application Shortcuts	Launcher Shortcuts on the Desktop
File Browser – Linux utility to browse the file system	Launchers to Start/Stop Tomcat
gedit – A common Linux text editor	Launcher to start the IdentityIQ Console
Firefox – Web browser	Launchers to observe the IdentityIQ Logs, IdentityIQ Email Logs, Standard Out Logs
Terminal – Launches a command line terminal	Launcher to start ApacheDirectoryStudio LDAP Browser
Lab Reset	Training tool to reset the lab environment: auto complete exercises; recover from errors; reset environment to rework a specific exercise; reset VM to clean state (see appendix for instructions)

Miscellaneous Commands and Keyboard Setup

- Clear Desktop – Use this to minimize windows to see the Desktop.
- If you have a non-US English keyboard, you can change the keyboard input to your native keyboard through these steps:
    - Navigate to **System** > **Preferences** > **Keyboard** > **Layouts** and click **Add**.
    - Use the dropdowns to select your keyboard and variant.
    - Once you have selected your keyboard, click **Add** in the bottom right corner.

Section One:

Authoritative Applications and Identity Creation

IDENTITYIQ IMPLEMENTATION AND ADMINISTRATION: ESSENTIALS

SailPoint IdentityIQ Version 8.1

www.sailpoint.com

Exercise #1: Configure IdentityIQ

Objective

In this exercise, you will confirm the installation of IdentityIQ, and you'll configure features of IdentityIQ that will assist you in your implementation efforts.

Overview

The training scenario represents a typical implementation. These pieces are already installed:

- A running database server with host, port and login information provided
- A pre-configured Tomcat Application Server instance
- IdentityIQ

In this exercise, you will update a few global IdentityIQ configurations to support your development efforts:

- Configure email redirection to send all system-generated emails to a local file instead of an SMTP Mail Server. This file is useful for debugging email notifications without sending real emails to users.
- Set the retention duration on various IdentityIQ objects.

Confirm and Explore Installation of IdentityIQ

Many students will never need to install IdentityIQ, thus we've already installed IdentityIQ in your virtual machine. In this section, you will configure your IdentityIQ instance to have the appropriate settings for your training environment.

Note: The Appendix has instructions for resetting the virtual machine to a clean state, which will uninstall IdentityIQ, and for installing IdentityIQ. This allows you to practice manually installing IdentityIQ. The manual installation instructions are intended for self-study; there is no class time allocated for the manual installation process.

1. Confirm the installation of IdentityIQ.

    a. Using the IdentityIQ Console, confirm the IdentityIQ version and patch. The console starts an instance of IdentityIQ and may take a few moments to start. You will know that it is running when you see the > prompt.

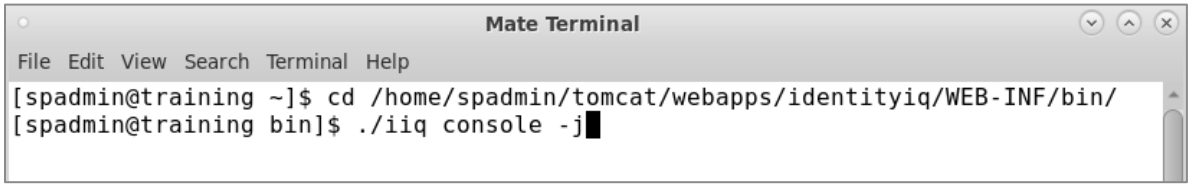
    Options to run IdentityIQ Console:

- **Option 1**: From the desktop, run the "**IIQ Console**" shortcut.

- **Option 2**: Using a Linux terminal, navigate to **/home/spadmin/tomcat/webapps/identityiq/WEB-INF/bin** and run the following command:

  ```
  ./iiq console -j
  ```

  Note: The -j option enables using the arrow keys to page through commands entered during the session.



b. Run the following command: **`about`**

c. The **Version** line lists the IdentityIQ version, patch version (if one is installed, you'll see p<number>), and the build. Note the IdentityIQ version and patch (if available):

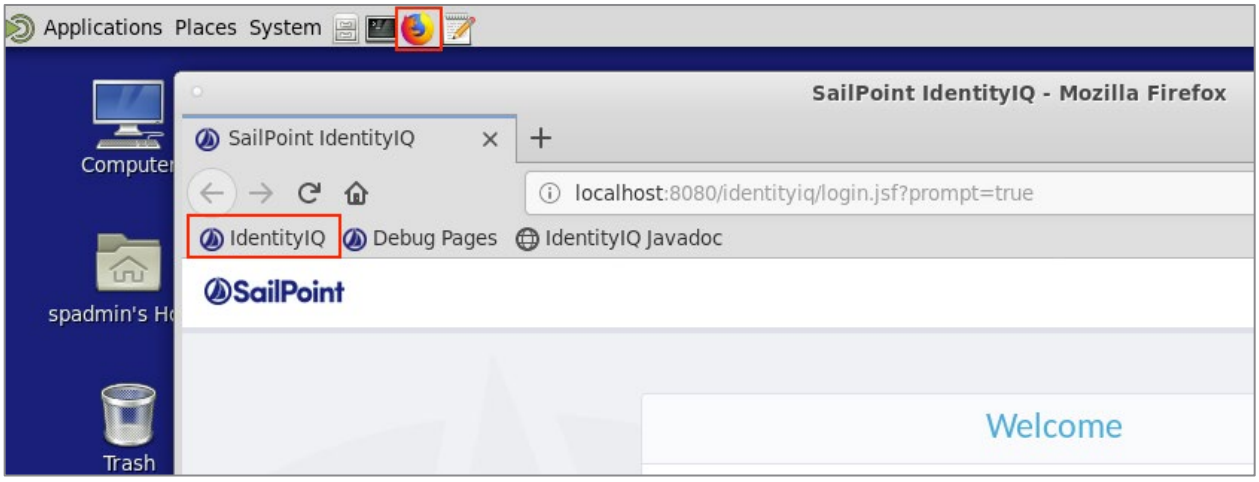
_____

d. Enter **quit** to exit the console.

2. Explore IdentityIQ.

a. Click the **Mozilla Firefox browser** (icon on Linux toolbar) in the VM and navigate to the IdentityIQ url: **http://localhost:8080/identityiq/**

The training environment also provides a bookmark in Firefox to take you to IdentityIQ.



b. Login to IdentityIQ as the IdentityIQ Administrator: **spadmin / admin**

Note: The **spadmin** login is the only identity that comes with IdentityIQ and is specifically used for product installation and initial configuration.

c. The **Home** page for the IdentityIQ Administrator includes many components. Briefly explore these components.

d. List the six menus available to System Administrators.

Menus Available to System Administrators	
1 **Home**	2
3	4
5	6

e. The **Home** page displays just below the menu after a user logs into IdentityIQ or clicks **Home**. The **Home** page functions as a dashboard with convenient access to specific areas of IdentityIQ through Quicklink Cards and Widgets that the user can rearrange. Click **Edit** to explore how users can rearrange these items according to their personal preference.

f. Homepage Widgets use bite-size visualizations and data grids to present information of interest to the logged-in user. Quicklinks are displayed as cards on the IdentityIQ Home page in addition to links in the Quicklink menu, which is available throughout the product. Click **Cancel** to return to the home page.

g. To the left of the **Home** menu, click the list menu icon  .

From this list, users can access Quicklinks. We'll discuss many of these during this training.

i. Expand the Quicklink category **My Tasks.** These Quicklinks provide filtered views for work you've been assigned.

ii. Expand the Quicklink categories **Manage Access** and **Manage Identity**. These Quicklinks support Lifecycle Manager functionality.

h. Navigate to **Identities > Identity Warehouse**

i. At this time, there is only one identity in IdentityIQ, the spadmin account you are currently using. Click on **spadmin** to open the identity cube.

ii. Explore the tabbed sections of the spadmin identity cube and list the nine sections available to System Administrators.

Nine Sections Available to System Administrators	
1 **Attributes**	2
3	4
5	6
7	8
9	

iii. Were there any accounts listed in the Application Accounts section? -Select-

i. To the far right on the main menu bar, 3 additional menu items are available. Click each item to explore its options.

i. The first, a gear icon, provides access to product settings for IdentityIQ.

ii. The second, a bell icon, serves as a quantity reminder for and provides access to work items assigned to the logged-in user.

iii. The third, the logged-in user's name, provides access to personal preference settings, the integrated help, and the logout command.

Configure Email Redirection and Default From Address

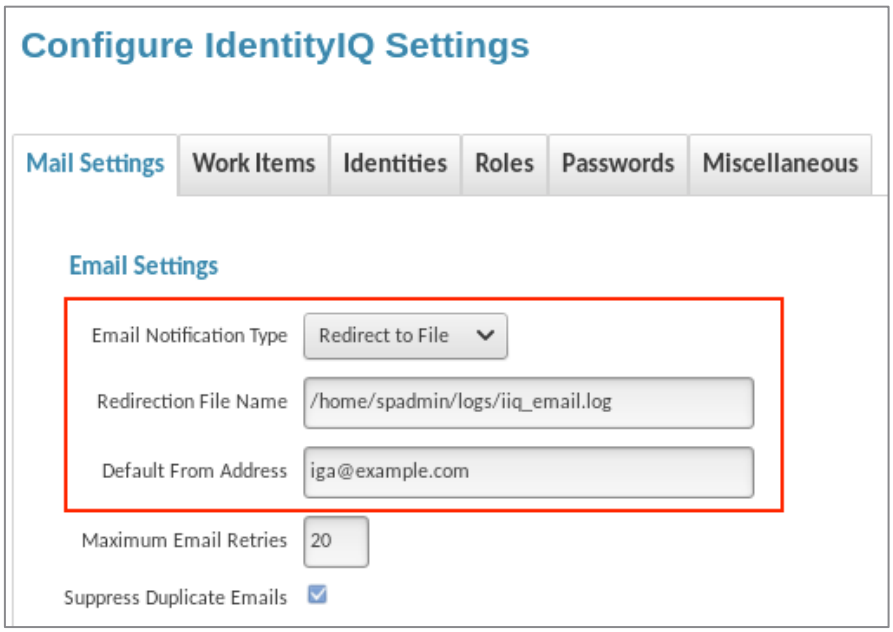
1. Within IdentityIQ, from the system setup gear, , navigate to **Global Settings** > **IdentityIQ Configuration**.

2. Configure the following options under **Email Settings**

   a. Email Notification Type: **Redirect to File**

   b. Redirection File Name: **/home/spadmin/logs/iiq_email.log**

   c. Default From Address: **iga@example.com**



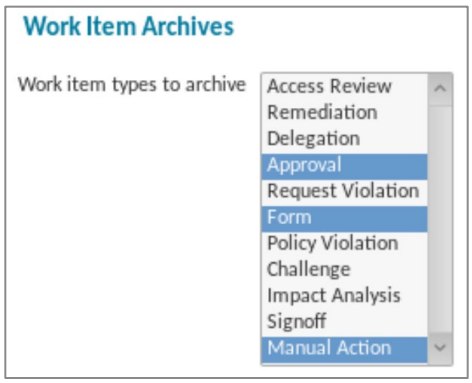
Notes:

- This is the location in the UI where you can also configure the default Email Templates used for many notification types within the IdentityIQ application.
- When you are ready to connect IdentityIQ to an SMTP mail server to send out real email notifications, change this configuration page to point to an SMTP mail server.

Configure Work Item Archiving

Work items in IdentityIQ are a unit of work assigned to a given user in the system that only exist until they are completed by a user. You may want to store archived versions of the work items after completion and that can be implemented by configuring work item archiving.

1. Still on the **Configure IdentityIQ Settings** page, navigate to **Work Items**
2. Under **Work Item Archives**, select the following **Work item types to archive:**
    a. **Approval**
    b. **Form**
    c. **Manual Action**

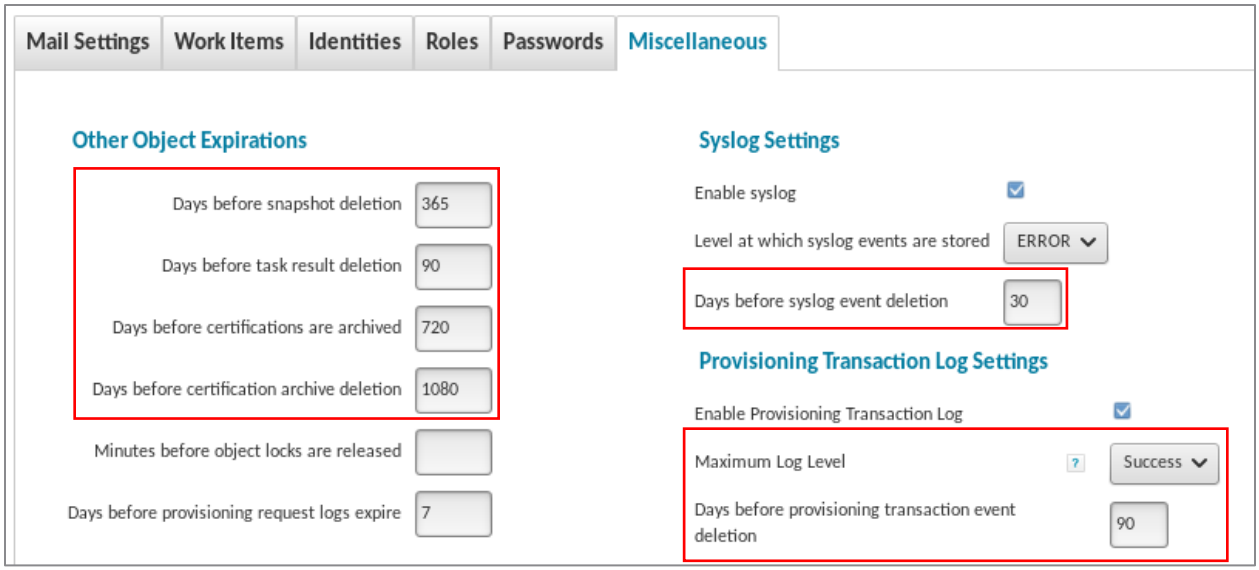


Note: To select multiple work item types, hold down the control key while you click the required types. Multi-selecting may vary across different operating systems and keyboard layouts. If you have issues multi-selecting, see the hints box at the end of the exercise for tips for multi-selecting.

Configure IdentityIQ Object Expiration

There are certain IdentityIQ objects that may not be necessary to store indefinitely. However, the default for object retention is often "forever". IdentityIQ should be configured to store the appropriate amount of historical data to optimize database size and overall system performance based on your business requirements for retaining this data. When the values are set to non-zero, IdentityIQ will automatically delete/archive objects that reach the expiration age.

1. Still on the **Configure IdentityIQ Settings** page, navigate to **Miscellaneous**
2. For **Other Object Expirations**, configure the following:
   a. Days before snapshot deletion: **365**
   b. Days before task result deletion: **90**
   c. Days before certifications are archived: **720**
   d. Days before certification archive deletion: **1080**
3. For **Syslog Setting**, configure the following:
   a. Days before syslog event deletion: **30**
4. For **Provisioning Transaction Log Settings**, configure the following:
   a. Maximum Log Level: **Success**
   Note: The *Success* option is selected for training purposes. For production it is typical to select *Retry* or *Failure*.
   b. Days before provisioning transaction event deletion: **90**



Note: We will discuss many of these items later in this training.

5. Scroll down to the bottom of the page and click **Save**

Review IdentityIQ Auditing Options

IdentityIQ can capture audit records on a variety of actions which occur in the system. Each installation may have different requirements for the types of activities that need to be audited, so IdentityIQ provides auditing flexibility through system configurations.

1. Navigate to **Gear** > **Global Settings** > **Audit Configuration**

2. In the **General Actions** tab, **review** the actions that are audited by default, including:

Audit Action	Audited Action
Identity Event	A Lifecycle event runs.
Authentication Answer Incorrect	Users entering invalid challenge question answers in Forgot Password.
Access Request Started	An Access Request is created.

3. There are additional audit actions that can be turned on through the IdentityIQ user interface on the Audit Configuration page. **Enable** these additional audit actions:

Audit Action	Audited Action
Login Failure	The username of a failed login attempt.
Import File	Import of IdentityIQ objects from XML file.
Email Sent	Emails sent from IdentityIQ.

4. Click through the other tabs and observe the other auditing options available.

   Note: You can turn on auditing for actions in the system, and you can also turn on auditing for any changes to identity attributes or even the create/update/deletion of system objects.

Also, it is possible to use the SailPoint API to audit additional items of your own choosing during rules or workflow steps.

5. Scroll to the bottom of page and click **Save**

6. Test the audit functions.

   a. Log out of IdentityIQ.

      i. Select **The Administrator** (top right) and then click **Logout**

   b. Attempt to log in using an incorrect username and password: example: **foo/foo**

   c. After this, log back in with the proper credentials: **spadmin/admin**

   d. Navigate to **Intelligence** > **Advanced Analytics**. Advanced Analytics provides detailed searching across IdentityIQ.

      i. How many different **search types** are provided? _____

      ii. Which **search type** do you think you would use to find the following:

         (1) Audited login failure? _____

         (2) Users who report to 'Bob Smith'? _____

         (3) The owner of the AccountsPayable entitlement on the Finance system?

         _____

   e. From the **Search Type** drop down, select **Audit**

   f. Click on **Run Search** from the bottom left to search all audit entries.

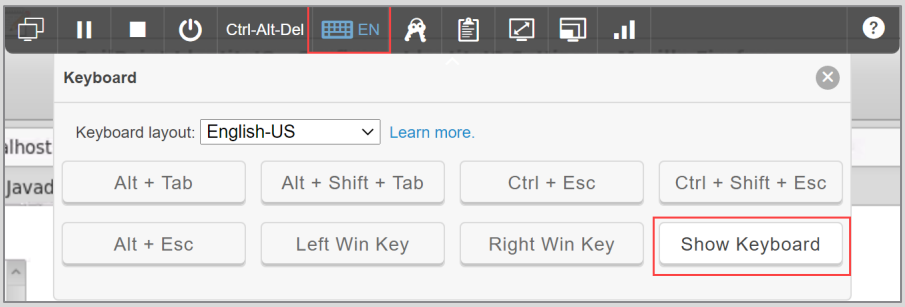
   g. Sort on Date descending and confirm that you see entries showing the *login failure*:

Multi-Select with Skytap

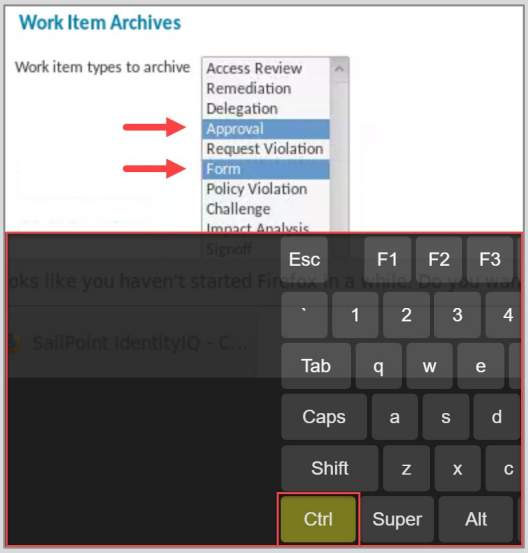
In this exercise and in later exercises you are instructed to multi-select items in a list. Most operating systems and keyboard layouts support holding down the control (ctrl) key while clicking. If ctrl+click does not work for you, one work around is to use the skytap hosted VM on-screen keyboard to hold down control while you click.

1. Open the on-screen keyboard from the skytap VM controls by clicking the **keyboard icon** 

then click on **Show Keyboard**



2. Once the keyboard is displayed on screen, click the **Ctrl** key. This single click will hold the ctrl key down while you click on your multi-selection.



3. When done selecting, click **Ctrl** again, and click the **X** to close the on-screen keyboard.

Exercise #2: Create Identity Cubes

Objective

In this exercise, you will define authoritative applications and create authoritative identity cubes.

Overview

The authoritative identity data for our exercises is stored in two sources. One application stores employee data, and the other application stores contractor data. This data exists in two flat files in comma-separated-values format.

- AuthEmployees.csv
- AuthContractors.csv

Each file has attributes from the HR systems to create new Identity Cubes within IdentityIQ.

Both files include comments, and the contractors file also has multiple rows for the same users. Because of this, you will also implement filtering and merging of the data when you read in the accounts from this application.

When defining the applications, you will use the “employeeId” or “contractorId” field as the Identity Attribute (unique value), and “fullName” as the Display Attribute (user friendly display name for the Identity).

There are a few requirements:

- For now, the default password for each identity should be **xyzzy** for testing purposes.
- Because employees and contractors can belong to several cost centers, the **Cost Center** attribute should be represented as a multi-valued field. To be able to search on an individual cost center, you need to mark this attribute as multi-valued so that the data is stored properly in IdentityIQ.
- Accounts should be classified as locked based on the values of the account’s inactiveUser attribute.

You will support these additional requirements by doing the following:

- Use a Creation Rule to set a default IdentityIQ password for each user as you create the Identity Cubes.
- Update account schemas and mark Cost Center as a multi-valued attribute.
- Use Rapid Setup functionality to classify accounts as disabled.

Define Employee Application

1. Create an Application Definition for the employee data.

   a. Log in to IdentityIQ as **spadmin/admin**

   b. Navigate to **Applications** > **Application Definition** and click **Add New Application**

2. Define the Application.

   Note: Ensure your free-text fields exactly match the exercise instructions, including case-sensitivity. IdentityIQ is case-sensitive. This is important because in later exercises, you will import objects that expect these names to match exactly.

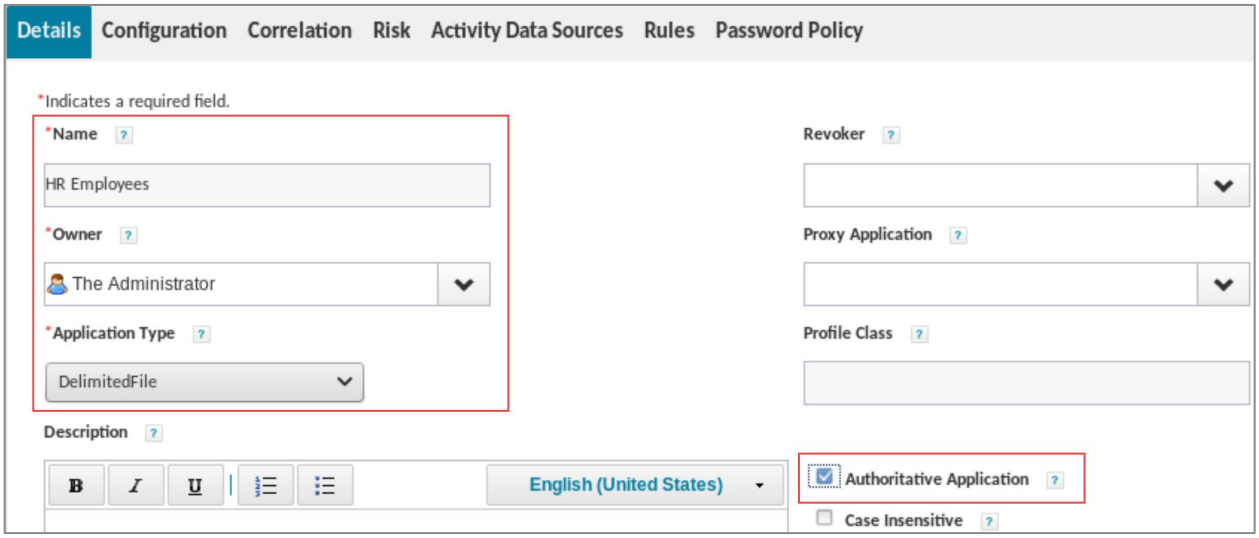
   a. Name: **HR Employees**

   b. Owner: **The Administrator**

      Note: In the last exercise, you observed that currently there is only one identity in your instance of IdentityIQ, but notice that there are multiple options in the Owner drop-down list. The Owner options you see here, in addition to spadmin, are workgroups. The workgroups in this list were imported with IdentityIQ Rapid Setup. Later, we will discuss workgroups in more detail, and you will change this Owner field in a future exercise once you have defined your own workgroups.

   c. Application Type: **DelimitedFile**

   d. Authoritative Application: **Checked**



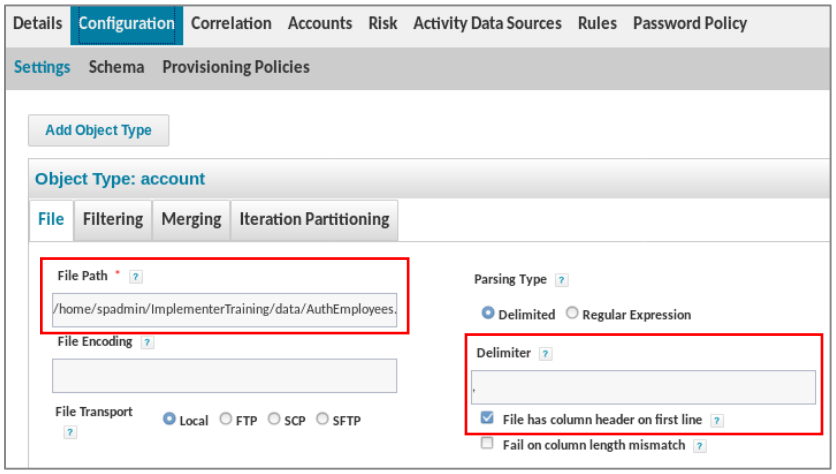
3. Configure the Application Definition file settings.

   a. Navigate to **Configuration** > **Settings** and configure as follows:

      i. File Path: **/home/spadmin/ImplementerTraining/data/AuthEmployees.csv**

ii. Delimiter: **,**

iii. File has column header on first line: **Checked**



4. Configure the account schema to specify which attributes to read from the file.

   a. Navigate to **Configuration** > **Schema**

   b. Scroll down and click **Discover Schema Attributes**

      This causes the connector to read just the header fields from the file you just specified defining what data is present in the file. The schema attributes discovered should match what is in the actual raw file:
      employeeId,firstName,lastName,managerId,fullName,email,department,region, location,inactiveUser,jobtitle,costcenter,workStatus

   c. For the **employeeId** attribute, click **Edit** (at far right of the row).

   d. Click **Set as Identity Attribute**.

      A successful "Identity Property Set on Schema" message will display.

   e. Click **Save**

   f. For the **fullName** attribute, click **Edit**

   g. Click **Set as Display Attribute**.

      A successful "Display Property Set on Schema" message will display.

   h. Click **Save**.

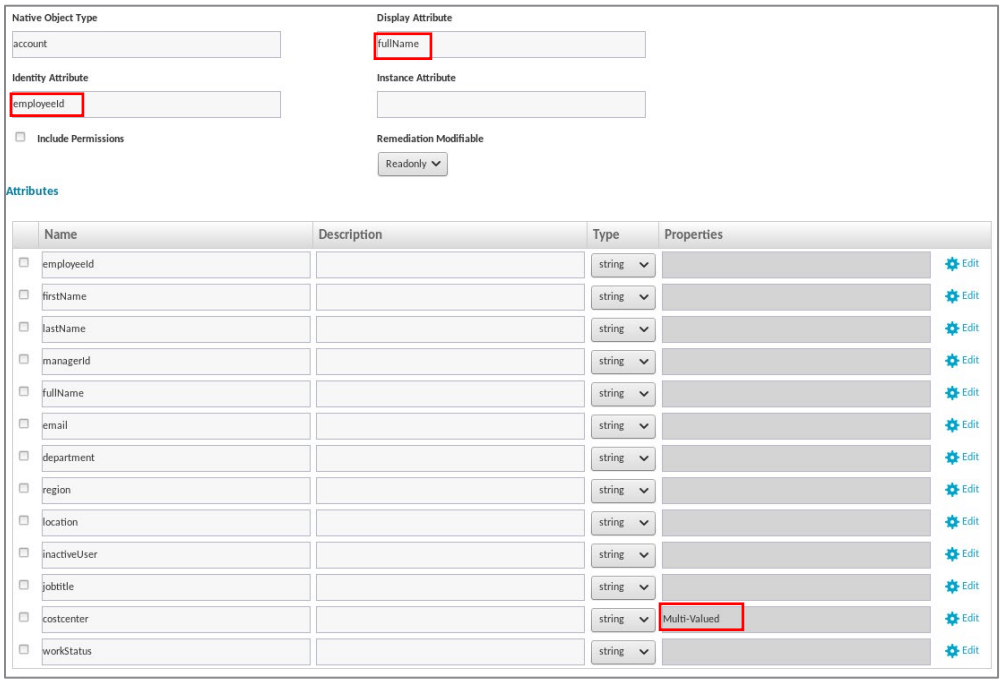
i. Scroll up to the schema Details section and confirm that **Identity Attribute** and **Display Attribute** have been set.

The Identity Attribute field defines the unique identifier for reading accounts. The Display Attribute field contains the user-friendly display name for the account and is used as the account name in IdentityIQ.

j. For the **costcenter** attribute, click **Edit**

k. Select **Multi-Valued** and click **Save**.

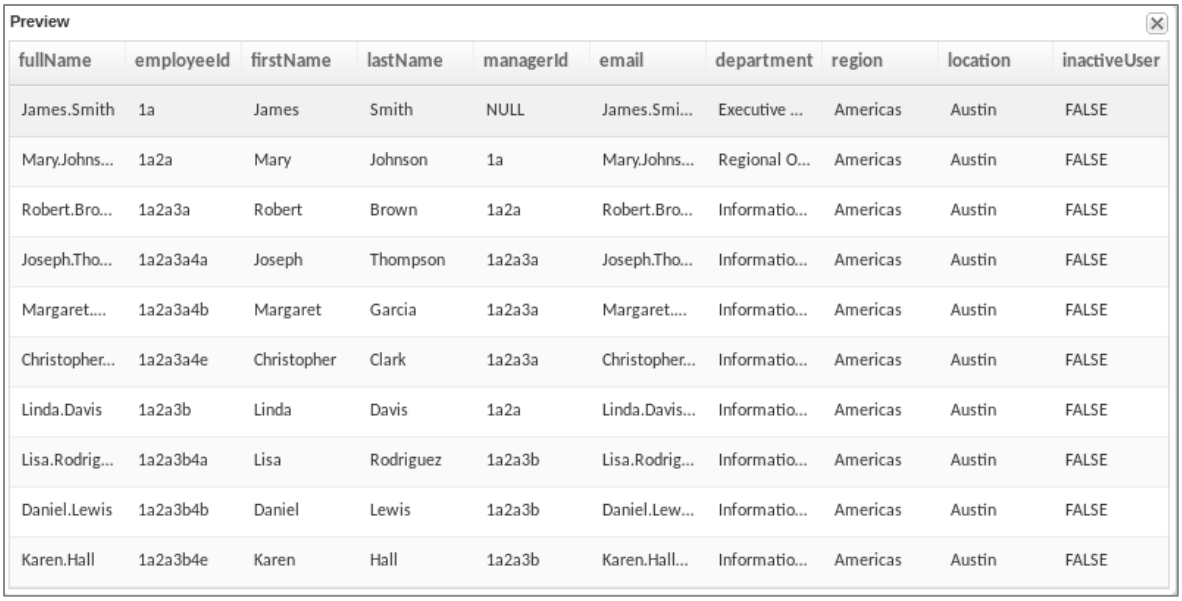
This indicates that the account attribute can have more than one value.



5. Preview account attributes.

Preview iterates over the first 10 accounts and displays the results in a popup window so you can spot check your schema configuration. This is especially helpful for validating any configured data manipulation actions (record merging, filtering, rules).

a. Remaining on the **Schema** page, click **Preview** and verify the data.


Preview

fullName	employeeId	firstName	lastName	managerId	email	department	region	location	inactiveUser
James.Smith	1a	James	Smith	NULL	James.Smi...	Executive ...	Americas	Austin	FALSE
Mary.Johns...	1a2a	Mary	Johnson	1a	Mary.Johns...	Regional O...	Americas	Austin	FALSE
Robert.Bro...	1a2a3a	Robert	Brown	1a2a	Robert.Bro...	Informatio...	Americas	Austin	FALSE
Joseph.Tho...	1a2a3a4a	Joseph	Thompson	1a2a3a	Joseph.Tho...	Informatio...	Americas	Austin	FALSE
Margaret....	1a2a3a4b	Margaret	Garcia	1a2a3a	Margaret....	Informatio...	Americas	Austin	FALSE
Christopher...	1a2a3a4e	Christopher	Clark	1a2a3a	Christopher...	Informatio...	Americas	Austin	FALSE
Linda.Davis	1a2a3b	Linda	Davis	1a2a	Linda.Davis...	Informatio...	Americas	Austin	FALSE
Lisa.Rodrig...	1a2a3b4a	Lisa	Rodriguez	1a2a3b	Lisa.Rodrig...	Informatio...	Americas	Austin	FALSE
Daniel.Lewis	1a2a3b4b	Daniel	Lewis	1a2a3b	Daniel.Lew...	Informatio...	Americas	Austin	FALSE
Karen.Hall	1a2a3b4e	Karen	Hall	1a2a3b	Karen.Hall...	Informatio...	Americas	Austin	FALSE

b. **Close** the preview.

6. Configure the Application Definition settings to exclude commented data rows.

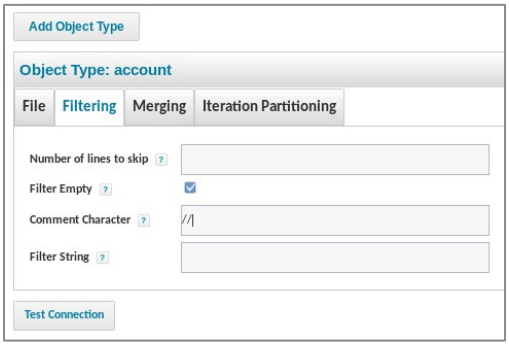
   The **AuthEmployees.csv** file includes comments that you do not want to read into IdentityIQ. Implement filtering of the data to exclude these rows during aggregation.

   a. Navigate to **Configuration** > **Settings** > **Filtering**

   b. Configure the settings as follows:

      i. Filter Empty: **Checked**

      ii. Comment Character: **//**



7. Verify the configuration settings by testing the connection.

   a. Remaining on the **Configuration** > **Settings** page, click **Test Connection** and verify it is successful.

8. **Save** the Application Definition for HR Employees.

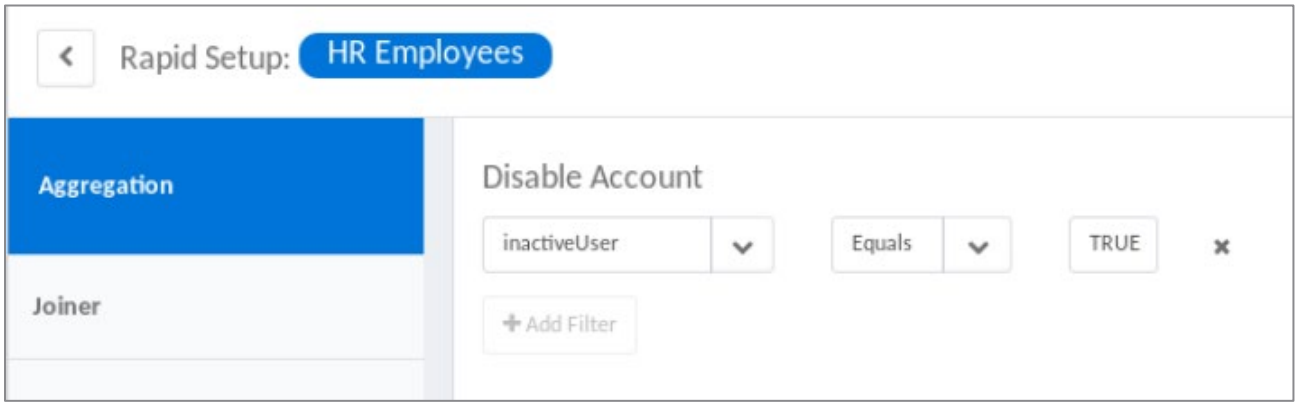
Configure the HR Employee Application with Rapid Setup

Attributes of account records may represent certain states or behaviors of the account, such as disabled and locked account designations. They may also represent special account types like service accounts or robotic process (bot/RPA) accounts.

You can specify these details to IdentityIQ through application *Rapid Setup*. Rapid Setup functions are separated onto their own pages of IdentityIQ, allowing you to grant access to these configurations to users, like business analysts, who might not be involved in defining connectivity and schema details for your applications. If your implementation does not use Rapid Setup, your implementation team can make these same configurations using rules.

For this application, you'll use Rapid Setup to specify the attribute and attribute value that indicates if the account is disabled.

1. Navigate to **Applications** > **Rapid Setup**
2. Choose **HR Employees** and click **Next**
3. On the **Aggregation** page, configure as follows:
    a. Disable Account:
        i. Click **Add Filter**
        ii. Application Attribute: **inactiveUser**
        iii. Operation: **Equals**
        iv. Value: **TRUE**



4. Click **Save**

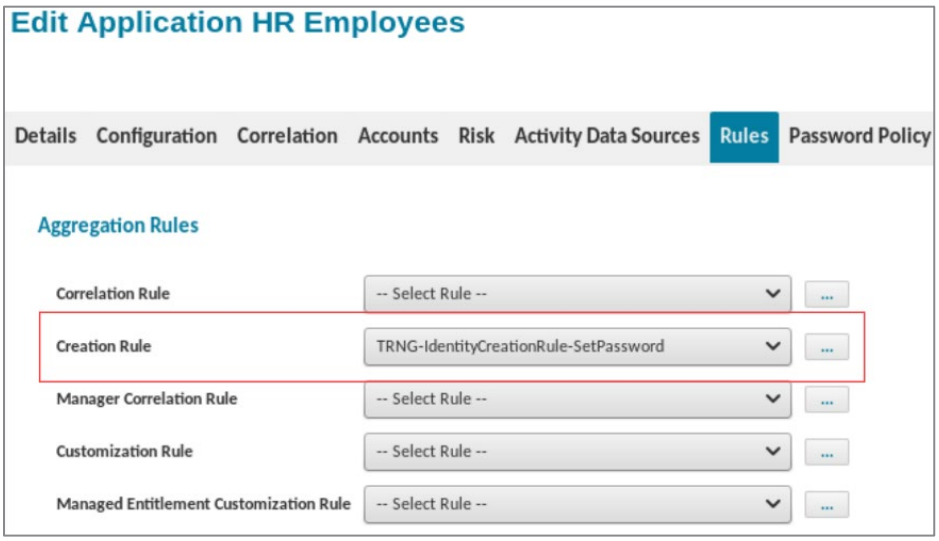
Set Default IdentityIQ Password for Employees

Because we're using IdentityIQ's native authentication to let users log in, all employees and contractors need an IdentityIQ password. You will set a default password of **xyzzy** using a creation rule.

Rules are snippets of code written by a member of the technical implementation team and provided to the rest of the implementation team for use. For the purposes of this class, your technical team member has written most of the rules for your use, so you will just need to import and apply them.

1. Import a pre-written creation rule.
    a. Navigate to **Gear** > **Global Settings** > **Import from File**
    b. In the **Import Objects** section, click **Browse…**
    c. Select the following file: **/home/spadmin/ImplementerTraining/config/Rule-CreationRule-SetPassword.xml** and click **Open**
    d. Click **Import**

2. Add the creation rule to the HR Employees application.
    a. Navigate to **Applications** > **Application Definition**
    b. Click the application named **HR Employees**
    c. Navigate to the **Rules** tab and locate the **Aggregation Rules** section.
    d. For Creation Rule, select **TRNG-IdentityCreationRule-SetPassword**



e. **Save** the application definition.

Define the Contractor Application

The two data files for employees and contractors have a similar structure; they both include comments, and they have similar column names. But in the contractors file, cost center details span multiple rows. See the screenshot below for an example: Thomas Martinez's account spans two rows. Because of this, you'll configure merging of this data as you read in the accounts from this file.

1. Create an Application Definition for the contractor data.
   a. Navigate to **Applications** > **Application Definition**
   b. Click **Add New Application**
2. Define the Application .
   a. Name: **HR Contractors**
   b. Owner: **The Administrator**
   c. Application Type: **DelimitedFile**
   d. Authoritative Application: **Checked**
3. Configure the Application Definition file settings.

a. Navigate to **Configuration** > **Settings** and configure as follows:

i. File Path: **/home/spadmin/ImplementerTraining/data/AuthContractors.csv**

ii. Delimiter: **,**

iii. File has column header on first line: **Checked**

4. Configure the schema.

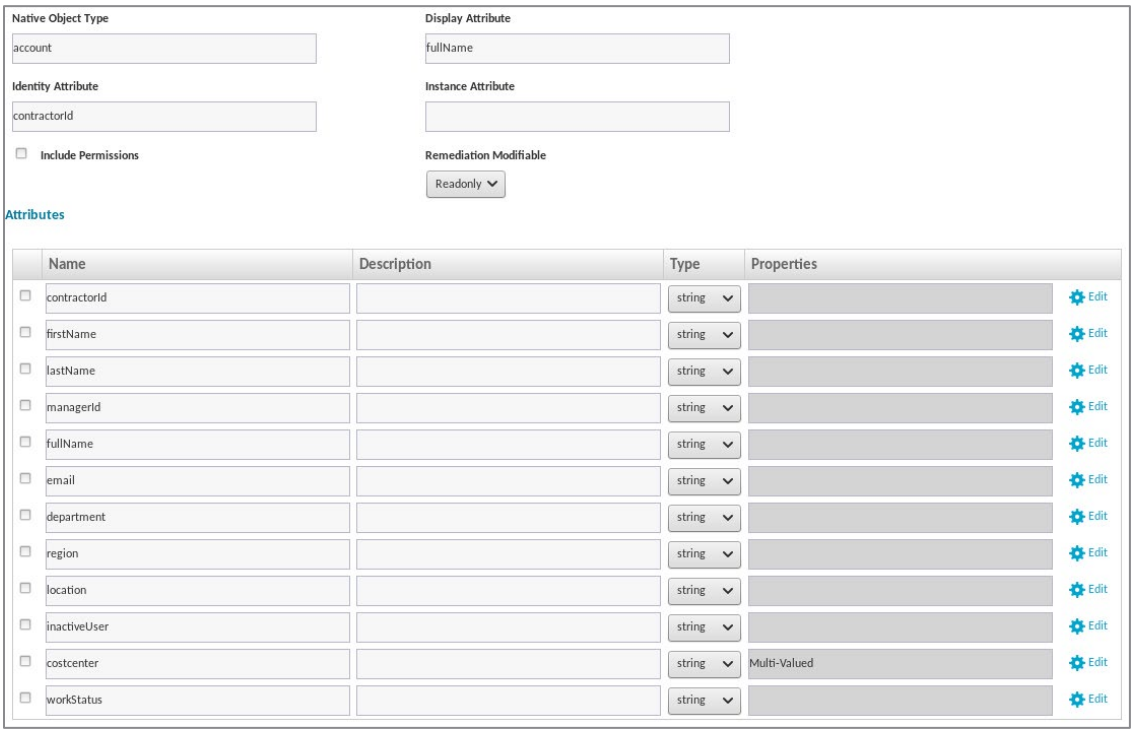
a. Navigate to **Configuration** > **Schema**

b. Scroll down and click **Discover Schema Attributes**

c. Set the **contractorId** attribute as the **Identity Attribute**

d. Set the **fullName** attribute as the **Display Attribute**

e. Mark the **costcenter** attribute as **Multi-Valued**



5. Implement merging of the data.

a. Navigate to **Configuration** > **Settings** > **Merging**

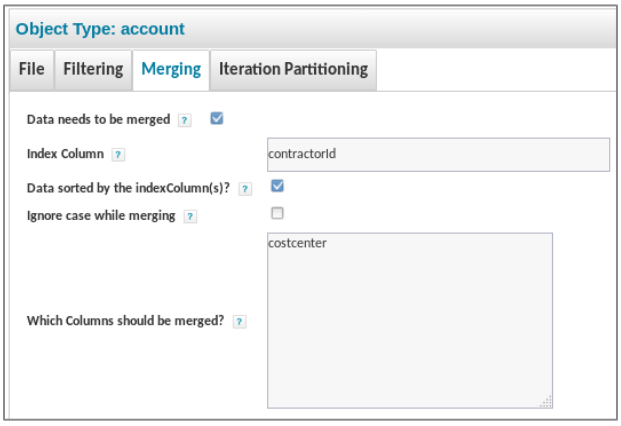
b. Configure the settings as shown:

i. Data needs to be merged: **Checked**

ii. Index Column: **contractorId**

iii. Data sorted by the indexColumn(s)?: **Checked**

iv. Which Columns should be merged?: **costcenter**



6. Implement filtering of the data.

   a. Navigate to **Configuration** > **Settings** > **Filtering**

   b. Configure the settings as shown:

      i. Filter Empty: **Checked**

      ii. Comment Character: **//**

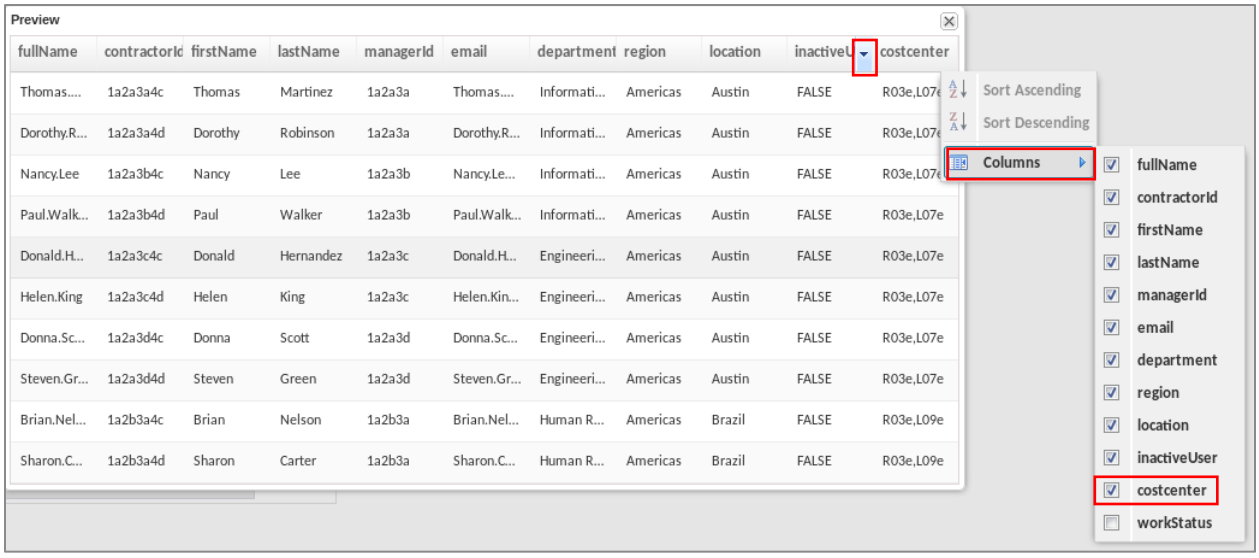
7. Remaining on the **Configuration** > **Settings** page, click **Test Connection** and verify it's successful.

8. Preview the account attributes.

   a. Navigate to **Configuration** > **Schema**

   b. Select **Preview**

   c. Hover over any column header until you see a dropdown arrow. Click the dropdown, expand **Columns**, and add the **costcenter** attribute.



d. Review the preview results. Notice that the comments row from the file is not included in these results and the cost center values are listed in a comma separated list in one row.

   Note: If your preview looks different than the screenshot above, go back and confirm your merging, filtering, and multi-valued account attributes are set correctly.

e. **Close** the preview.

9. Add the creation rule to the HR Contractors application.

   a. Navigate to the **Rules** tab and locate the **Aggregation Rules** section.

   b. For Creation Rule, select **TRNG-IdentityCreationRule-SetPassword**

10. **Save** the application definition.

Configure the HR Contractor Application with Rapid Setup

Use Rapid Setup to configure account classifications.

1. Navigate to **Applications** > **Rapid Setup**
2. Choose **HR Contractors** and click **Next**
3. On the **Aggregation** page, configure as follows:

   a. Disable Account:

      i. Click **Add Filter**

      ii. Application Attribute: **inactiveUser**

iii. Operation: **Equals**

iv. Value: **TRUE**

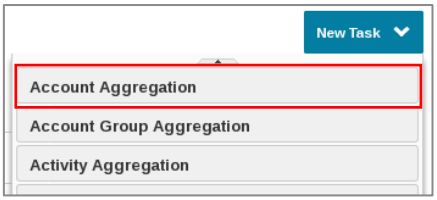
4. Click **Save**

Aggregate Employee and Contractor Data

Now, you will aggregate (or load) the Employee and Contractor data from the delimited files by creating Account Aggregation tasks. *This process of loading account data from authoritative applications will generate the authoritative identity cubes.*

1. Define and run an Employee account aggregation task.

   a. Navigate to **Setup** > **Tasks** and under **New Task,** click **Account Aggregation**



   b. Define the task as follows:

      i. Name: **Aggregate Employees**

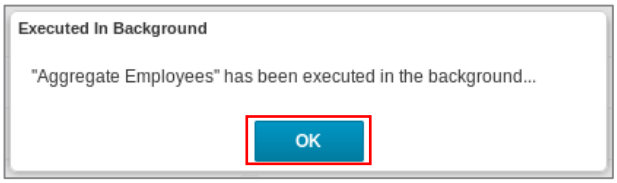
      ii. Previous Result Action: **Rename Old**

      iii. Select applications to scan: **HR Employees**

      iv. Select the **Detect deleted accounts** checkbox.

      v. Select the **Disable optimization of unchanged accounts** checkbox.

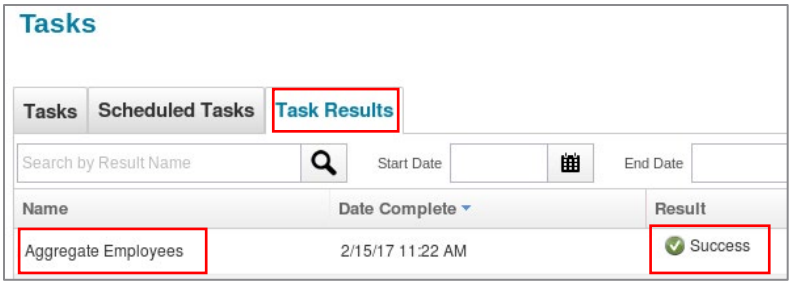
   c. Scroll down and choose **Save and Execute** and choose **OK** when prompted.



2. Once you are back on the main **Tasks** page, click **Task Results**.

3. Under **Name**, click **Aggregate Employees** to open the task result.

   While the task is pending, you can open it and view information about the processing. When the task is complete, you will see the results of the aggregation.



The task output should show that the HR Employees application was scanned, the number of accounts that were scanned, and that identities were created for each account.

Aggregate Employees Attributes	
Attribute	**Value**
Applications scanned	HR Employees
Accounts scanned	162
Identities created	162

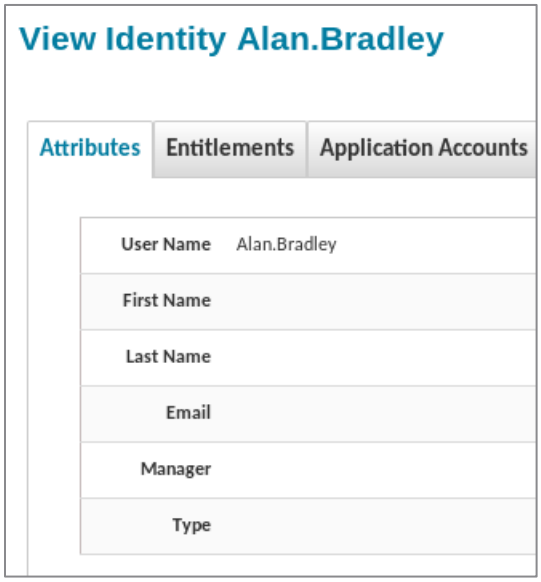
4. Define and run a Contractor account aggregation task.
   a. Navigate to **Setup** > **Tasks** and under **New Task**, click **Account Aggregation**
   b. Define the task as follows:
      i. Name: **Aggregate Contractors**
      ii. Previous Result Action: **Rename Old**
      iii. Select applications to scan: **HR Contractors**
      iv. Select the **Detect deleted accounts** checkbox.
      v. Select the **Disable optimization of unchanged accounts** checkbox.
   c. Scroll down and choose **Save and Execute** and choose **OK** when prompted.
5. View the task results and confirm that you created 72 identities.

Confirm Aggregations were Successful

1. View an Identity.

   a. Navigate to **Identities** > **Identity Warehouse**

   b. Click any user and confirm that an identity cube was created for this user.



   Notice that all of the identity attributes are blank. This is because we have not yet defined mappings between the identity attributes and the applications that are feeding data into IdentityIQ. You will do this in a later exercise.

2. Confirm that the Creation Rule was successful.

   a. Log into IdentityIQ as an employee: **Aaron.Nichols/xyzzy**

   b. Log out and log back in as a contractor: **Allen.Burton/xyzzy**

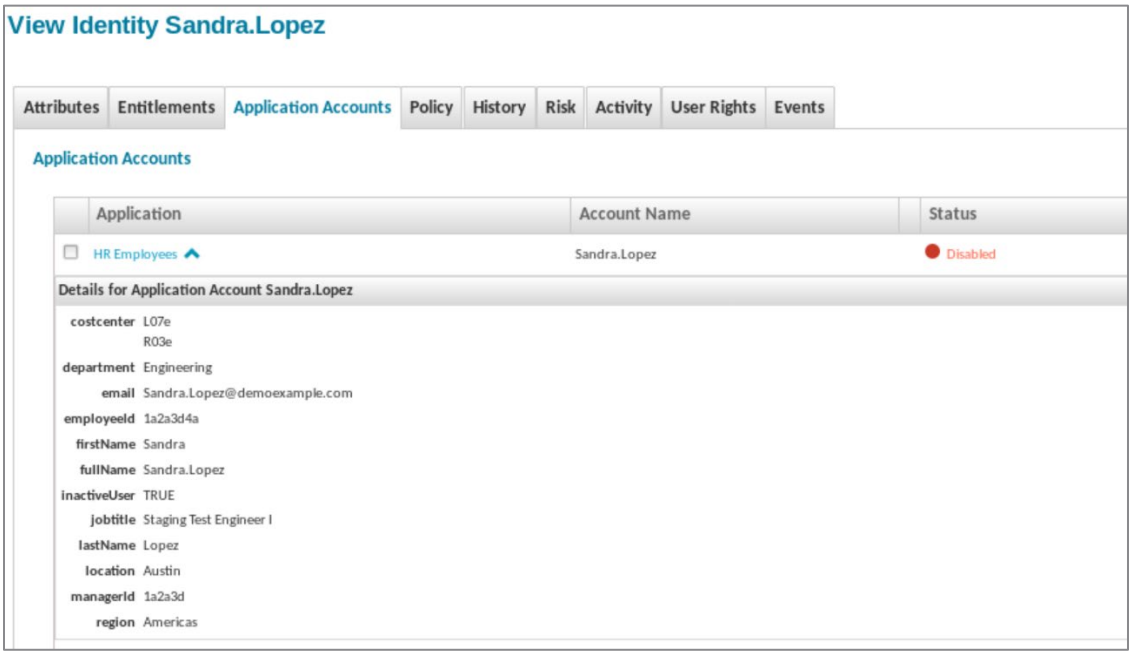
   Note: If you cannot log in to both accounts using the names and passwords, then you may have an issue with your Creation Rule. Check that both applications have the Creation Rule defined properly. If it was not, see the note at the end of the exercise about resetting identities.

Review Account Attributes

During aggregation, IdentityIQ loads the attributes specified in the application's schema and applies the Rapid Setup account categorizations to mark the account statuses. This application account data is available on the **Accounts** tab in the application definition or on the **Application Accounts** tab on identity cubes.

1. Log into IdentityIQ as **spadmin/admin**

2. Navigate to **Identities** > **Identity Warehouse** and view **Sandra.Lopez**
3. Click the tab named **Application Accounts**
4. View her account details for the **HR Employees** application.



a. How many cost centers are associated with the account? _____

Note: If your configuration is correct, there should be one cost center per line.

b. What was specified on the schema to include all of the cost centers as independent values?

_____

c. Why is her account status disabled?

_____

Resetting Identities

When working through these exercises, it is common to make some mistakes. You can always clear out all the identities in the system by using the IdentityIQ console.

Start the IdentityIQ Console using one of these methods:

(1) **./iiq console -j** (from within the /WEB-INF/bin directory)
Note: The -j option enables using the arrow keys to page through commands entered during the session.

(2) Use the **IIQ Console** shortcut from the Desktop of the training environment

From within the console, run **delete identity *** to clear out all Identities from the system.

Note: Use this option cautiously as this will remove all identities other than **spadmin**, which is a protected identity. If identities are used as values for other fields (such as an Application owner), the field will be emptied and must be reset. This command does not delete Workgroups.

Once you've cleared the identities, you can then re-run the aggregation and identity refresh tasks to reload the Identity Cubes.

Exercise #3: Populate Identity Cubes

Objective

In this exercise, you will define and map identity attributes, specifying logic for correlating managers, and updating the visible identity attributes in the user interface.

Overview

You now have two properly configured application definitions for loading account data from the authoritative applications. Next, you will define the identity attributes for this installation of IdentityIQ. You will specify which data from your application accounts will be used to populate both the standard identity attributes, which are predefined in the Identity Mappings, and the extended attributes that are unique to this IdentityIQ installation, which you will define.

Other than identity name (User Name), which is populated by default from the Display Attribute in the application it is created from, identity attribute values are specified in Identity Mappings. Identity Mappings also let you specify behaviors for each attribute, like whether it is searchable or available for group generation as a Group Factory.

Configure Standard Identity Attributes

First, you will define the sources for values for the standard identity attributes.

1. Log in to IdentityIQ as **spadmin/admin**
2. Navigate to **Gear** > **Global Settings** > **Identity Mappings**

   This is the main interface for configuring Identity Attributes and how they are populated.

   a. Did you see the red information box at the top of the page?

      When we installed IdentityIQ, we created a named column for an extended identity attribute in the IdentityIQ database. This information box is a reminder to define that attribute in IdentityIQ. You will define it later in this exercise.
3. Click **First Name** in the Identity Attributes list.
4. Scroll down to **Source Mappings** and click **Add Source** to configure the source of this Identity Attribute.

   a. Select **Application Attribute**

   b. Application: **HR Employees**

   c. Attribute: **firstName**

   d. Click **Add** to add the source mapping.

Notice that attributes can be populated by application attributes, by an application specific, or global rule. They can also be populated by multiple sources, as you are about to see in the next few steps.

5. Click **Add Source** again to configure where this attribute will come from for a contractor identity.

   a. Select **Application Attribute**

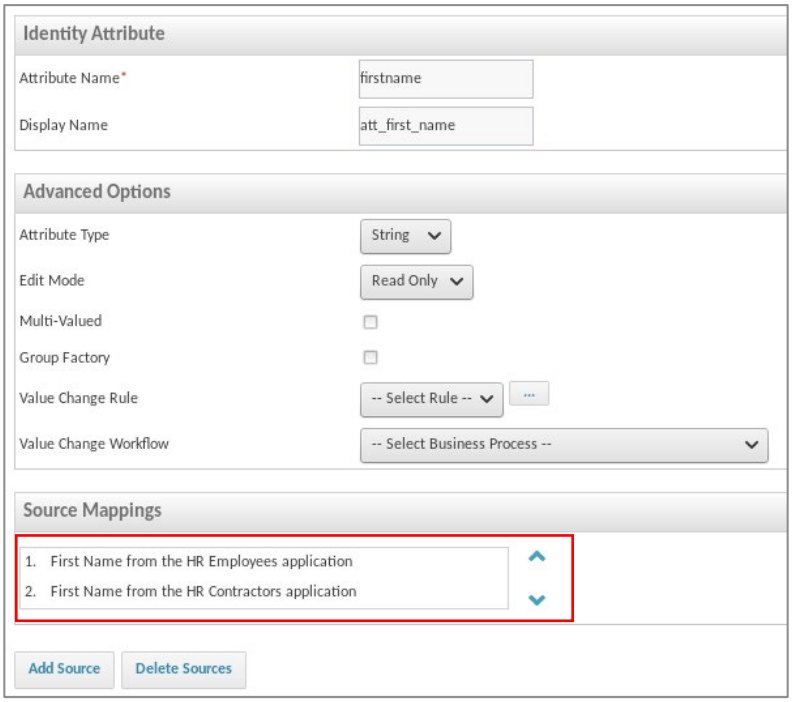
   b. Application: **HR Contractors**

   c. Attribute: **firstName**

   d. Click **Add** to add the source mapping.

6. Ensure that your attribute mappings match the following screenshot.

   You should have two Source Mappings. For Employees, the Identity Attribute will be sourced from the Employee data, and for Contractors, it will be sourced from the Contractor data.



   Note: Source mappings are processed from the top down. The first mapping, where the user has an account, is the mapping that populates the identity attribute. You can change the order of your mappings using the arrows on the right.

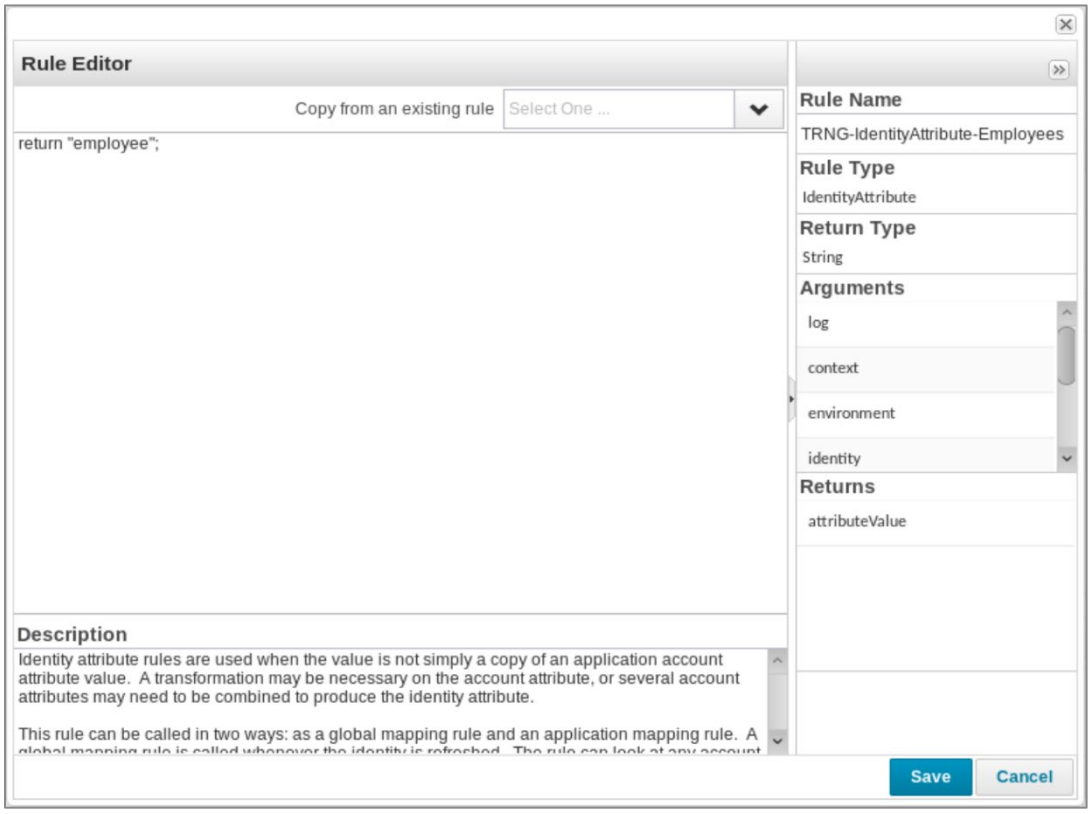
7. Click **Save** to complete the changes to the first name attribute.

8. Click **Type** in the Identity Attributes list.

9. Under **Source Mappings**, click **Add Source**
   a. Select **Application Rule**
   b. Application: **HR Employees**
   c. Click the ellipses ... to access the **Rule Editor**.
   d. Create the rule as follows:
      i. Rule Name: **TRNG-IdentityAttribute-Employees**
      ii. In the Rule Editor, type the following Java BeanShell script:

```
return "employee";
```

Note: Ensure **employee** is all lowercase.



      iii. Click **Save** to save the rule.
   e. Rule: select the rule you just created **TRNG-IdentityAttribute-Employees**
   f. Click **Add**
10. Under **Source Mappings**, click **Add Source**

a. Select **Application Rule**

b. Application: **HR Contractors**

c. Click the ellipses ... to access the **Rule Editor**.

d. Create the rule as follows:

i. Rule Name: **TRNG-IdentityAttribute-Contractors**

ii. In the Rule Editor, type the following Java BeanShell script:

```
return "contractor";
```

Note: Ensure **contractor** is all lowercase.

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

e. Rule: select the rule you just created **TRNG-IdentityAttribute-Contractors**

f. Click **Add**

11. **Save** your changes to the **Type** identity attribute.

12. To save time in class, you will import the remaining configurations for the Standard Attributes: Display Name, Inactive, Last Name, Manager.

a. Navigate to **Gear** > **Global Settings** > **Import from File**

b. In the **Import Objects** section, click **Browse**

c. Select the following file:
/home/spadmin/ImplementerTraining/config/ObjectConfig-Standard-Attributes.xml

d. Click **Open**

e. Click **Import**

This file merges the configuration for the remaining standard attributes with the work you just completed.

Note: When implementing IdentityIQ in your own environment, you will define the source mappings and appropriate Advanced Options for *each* Identity Attribute.

13. Navigate to **Gear** > **Global Settings** > **Identity Mappings**

    a. Make sure that the Identity Attributes: **Display Name**, **Inactive**, **Last Name**, and **Manager** have a Primary Source Mapping value.

       Note: The **Primary Source Mapping** column only lists the first source for each identity attribute. To see the full list of source mappings, open the attribute definition.

       Note: Email address will be populated later from another source.

Define Extended Identity Attributes

You will now define and configure additional identity attributes that are specific to this implementation.

1. Click **Add New Attribute** on the **Identity Attributes** page and enter the following:

   a. Attribute Name: **department**

   b. Display Name: **Department**

   c. Under **Advanced Options**, select **Searchable** and **Group Factory**

      Note: Selecting Searchable tells IdentityIQ to store this identity attribute in its own column in the database, which is either a placeholder column or a named column. Because we configured a named column specifically to store department, IdentityIQ will store the data within that column.

      Group Factory identifies those fields from which groups of users may be created, which you will do later.

   d. Under **Source Mappings**, click **Add Source**

      i. Select: **Application Attribute**

      ii. Application: **HR Employees**

      iii. Attribute: **department**

      iv. Click **Add**

   e. Click **Add Source**

      i. Select: **Application Attribute**

      ii. Application: **HR Contractors**

iii. Attribute: **department**

iv. Click **Add**

f. **Save** identity attribute **Department**

Note: Remember the red information box at the top of the page? If you correctly configured the department identity attribute, the reminder to define this attribute should no longer be displayed.

2. To save time in class, you will import the remainder of this implementation's extended identity attributes. The import will add these attributes: Cost Center, Employee ID, Job Title, Location, Region.

   a. Navigate to **Gear** > **Global Settings** > **Import from File**

   b. In the **Import Objects** section, click **Browse**

   c. Select the following file: **/home/spadmin/ImplementerTraining/config/ObjectConfig-Extended-Attributes.xml**

   d. Click **Open**

   e. Click **Import**

   This file merges the configuration for the extended identity attributes into the existing attribute configurations.

3. Navigate to **Gear** > **Global Settings** > **Identity Mappings**

4. Open the definition for the **Cost Center** identity attribute.

   a. Mark the Advanced Options selected for the Cost Center attribute:

   ☐ Searchable
   ☐ Multi-Valued
   ☐ Group Factory

   b. Notice that the Cost Center *identity* attribute is mapped from the costcenter *application* attribute.

   The *application* attribute was defined as multi-valued on the application schema. Both attributes have been marked as multi-valued to ensure that the data is represented correctly in IdentityIQ.

   c. Click **Cancel** to return to the **Identity Attributes** page.

5. Open the definition for the **Manager** identity attribute.

a. What is its attribute type? _____

b. Mark the Advanced Options selected for the Manager attribute:

- ☐ Searchable
- ☐ Multi-Valued
- ☐ Group Factory

c. Notice that the option **Searchable** is not displayed on this page.

Since **Manager** is a standard attribute that is shipped with IdentityIQ, it is searchable by default.

d. Click **Cancel**

Note: There will be a few identity attributes that do not have any source mappings. This is okay. Later, you will update the email attribute to be sourced from an LDAP account attribute.

Define Identity and Manager Correlation Logic

For this class, you're using Rapid Setup to configure simple identity correlation logic and manager correlation logic. Correlation logic can also be configured using either the correlation wizard found on the Correlation page of the application or a correlation rule.

The data you are reading from the delimited files includes manager data. Knowing who a user's manager is important for notifications and later you will configure manager approvals for requests for access. You will use Rapid Setup to define the manager correlation so that IdentityIQ can correctly build the organizational hierarchy. This correlation will describe which application attribute defines a user's manager, and which identity attribute to map this to in the Identity.

In the HR data, each managerId from the delimited files maps to a specific Employee ID.

1. Define Correlation Logic for HR Employees.

   a. Navigate to **Applications** > **Rapid Setup**

   b. Select **HR Employees** and click **Next**

   c. On the **Aggregation** page, locate the section named **Identity Correlation**

   d. Add identity correlation logic:

      i. Click **Add Filter**

      ii. Application Attribute: **employeeId**

      iii. Operation: **Equals**

iv. Identity Attribute: **Employee ID**

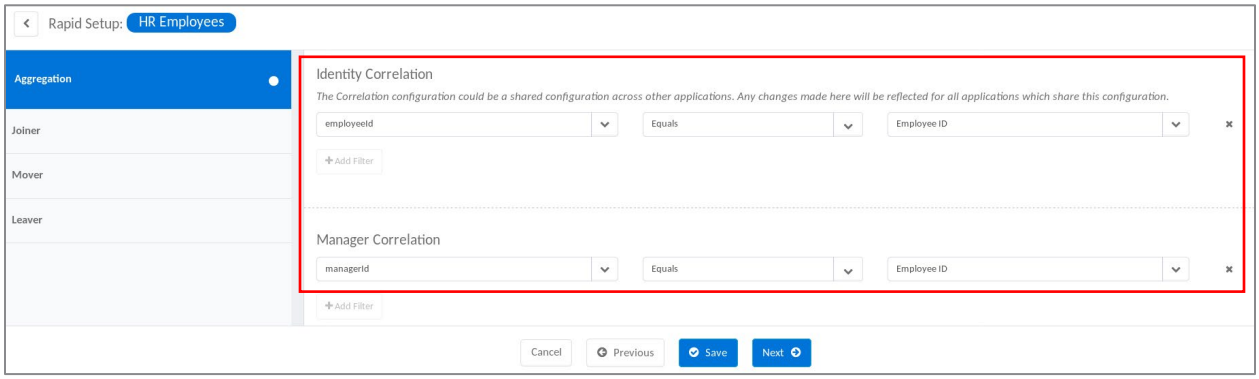
e. Locate the section named **Manager Correlation** and add this manager correlation logic:

i. Click **Add Filter**

ii. Application Attribute: **managerId**

iii. Operation: **Equals**

iv. Identity Attribute: **Employee ID**



f. Click **Save**

2. Define Correlation Logic for HR Contractors.

a. On the top left, click the **back arrow (<)** next to Rapid Setup to select another application.

b. Select **HR Contractors** and click **Next**

c. On the **Aggregation** page, add identity correlation logic:

i. Application Attribute: **contractorId**

ii. Operation: **Equals**

iii. Identity Attribute: **Employee ID**

d. Add manager correlation logic:

i. Application Attribute: **managerId**

ii. Operation: **Equals**

iii. Identity Attribute: **Employee ID**

e. Click **Save**

Refresh Identity Cubes

An **aggregation** task reads data from an external application, and a **refresh** task acts upon data within IdentityIQ.

1. Navigate to **Setup** > **Tasks** and search for **refresh**
2. Click the **Refresh Identity Cube** task to view its default configuration settings.

   There are five options in this task definition that are enabled by default.

   a. Notice **Refresh identity attributes** and **Refresh manager status** are already selected by default. Leave these options selected.

   b. Uncheck the following options:

      i. **Refresh assigned, detected roles and promote additional entitlements**

      ii. **Refresh the identity risk scorecards**

      iii. **Check active policies**

      When you deselect these options in the default Refresh Identity Cube task you are changing the data processing this task will perform when run. You are removing the **Refresh assigned, detected roles and promote additional entitlements** and **Check active policies** because, at this time, there are no entitlements, roles, or policies in your IdentityIQ instance. You will turn these options on in later exercises when appropriate. You are removing the **Refresh the identity risk scorecards** because we are not implementing risk scoring in this environment.

3. Scroll down and select **Save and Execute**
4. Navigate to **Task Results** and monitor the task named **Refresh Identity Cube**.

   If the task has not completed, it will be marked as pending. You can open a pending task and watch its progress.

5. Make sure this task refreshed **235** identities.
6. When the refresh is complete, navigate to **Identities** > **Identity Warehouse**
7. Click **Adam.Kennedy** and notice that this user now has a Manager listed, **Douglas.Flores**

   The manager name is a link to the manager's cube. IdentityIQ maintains the reporting hierarchy for use in approvals, escalations, etc.

   a. Why is the Manager attribute a hyperlink? (**Hint**: Check Identity Mappings)

   _____

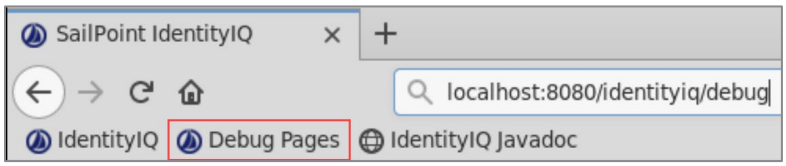
Note: Email address is blank because we have not yet defined its mapping.

Configure the UI to Display New Identity Attributes

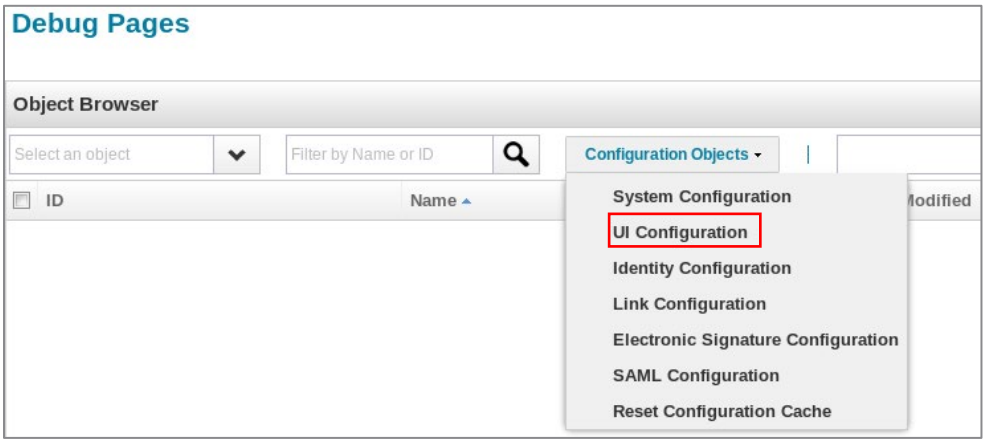
Now that you have defined extended identity attributes with their sources and populated them, next you need to configure the Identity Warehouse UI in the Debug Page to display all these new identity attributes.

By default, IdentityIQ only displays standard identity attributes. Debug Pages are used for advanced configuration and debugging of XML representation of objects, and other administrative tasks. You can use these pages to view the XML representation of an object or add an option that is not supported in the browser interface. Users must have the System Administrator capability to access the Debug Pages.

1. Configure IdentityIQ to display your Extended Identity Attributes.
2. Navigate to the **Debug Pages** using Firefox.
   a. Browse to **http://localhost:8080/identityiq/debug** or use the **Debug Pages** shortcut in your Firefox browser.



3. Click **Configuration Objects** and select **UI Configuration**



   The Object Editor opens with an XML representation of the UIConfig object within IdentityIQ.

4. Search (Ctrl+F) for the **entry key** named: **identityViewAttributes**.

   The keys are listed alphabetically. It will look like this:

<entry key="identityViewAttributes" value="name,firstname,lastname,email,manager,type,softwareVersion,administrator"/>

5. Edit the entry (as follows) to reflect the additional fields that you want to display. Take care to type the names of the attributes accurately (attributes you are adding are shown in bold below):

   <entry key="identityViewAttributes" value="name,firstname,lastname,email,manager,type,softwareVersion,administrator,**department,location,empId,region,jobtitle,costcenter**"/>

   Note: The 4th letter in **empId** is a capital "**i**"

6. At the bottom of the page, click **Save**

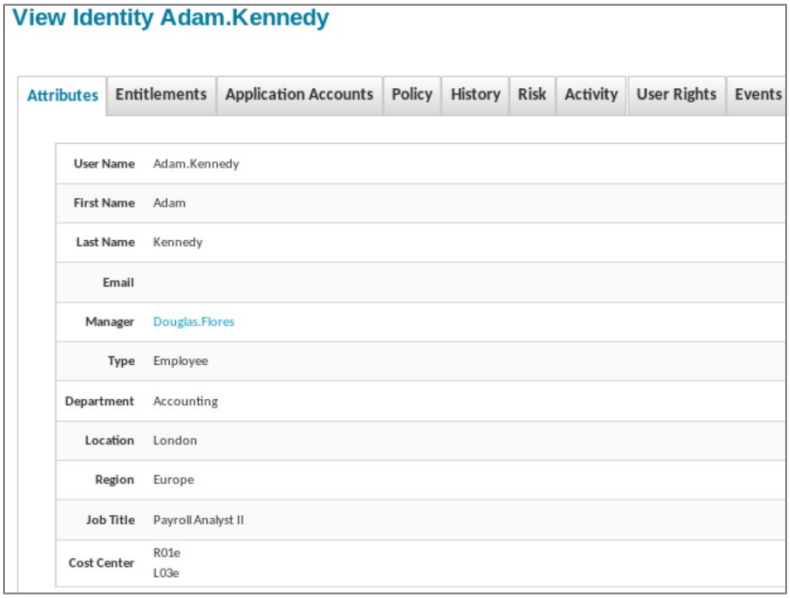
   You may have to reposition the window to see the **Save** button.

7. Confirm that additional identity attributes are displaying in the user interface.

   a. Navigate to **Identities** > **Identity Warehouse** and select **Adam.Kennedy**

   b. Notice that most identity attributes have values, but you can also see attributes without values (for example, **Email**).

   Note: The **Software Version** and **Administrator** attributes are only displayed on Identity Cubes where **Type**: **RPA/Bots**.

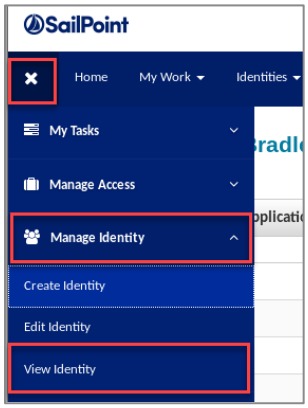


8. View Adam's identity attributes through the **View Identity** Quicklink.

   Note: Only installations with Lifecycle Manager will have access to the View Identity Quicklink.

   a. Expand the Quicklink Menu and **Manage Identity**

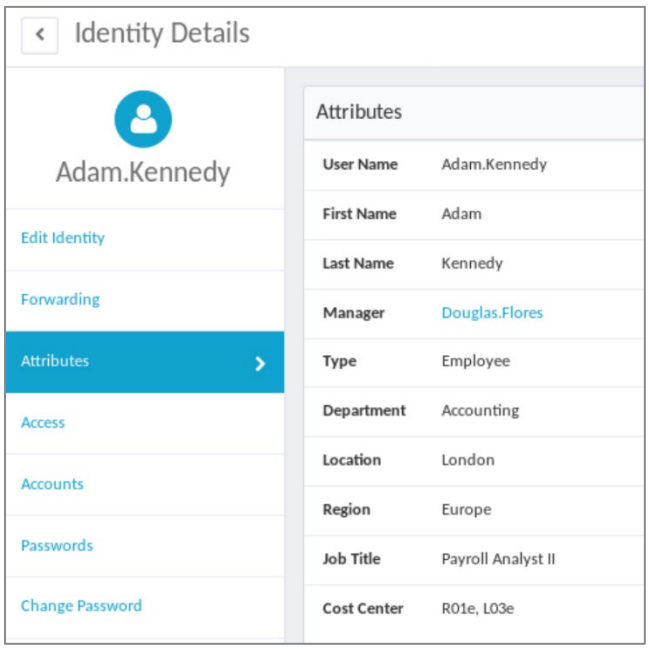
   b. Click **View Identity**



   c. Click **Manage** for **Adam.Kennedy**

   d. Notice that only the identity attributes with values are displayed.

      Since email is not yet populated, it is not shown.



Investigate your Data

1. Navigate to **Intelligence** > **Advanced Analytics** and select the **Identity** Search Type.

a. Is **Department** listed as a Searchable Attribute? _____

b. Where was this attribute classified as searchable?

_____

2. With **Advanced Analytics**, **Identity** search, find out how many contractors are inactive.

   Good practice is to clear search parameters prior to searching to ensure that no previously defined search parameters impact your search.

   a. At the bottom left, click **Clear Search**

   b. Set **Is Inactive** to **True**

   c. Set **Type** to **Contractor**

   d. Click **Run Search**

   e. How many *inactive* contractors are there? _____

3. Click **Refine Search** to return to the **Search Criteria** page.

4. Now, on your own, answer the following question:

   a. How many inactive employees are there? _____

5. Search for identities without managers.

   a. Click **Refine Search** to return to the **Search Criteria** page and remove all search parameters. Click **Clear Search** to reset everything.

   b. Under **Fields to Display,** select these **Identity Fields**:

      - Department
      - Employee ID
      - First Name
      - Job Title
      - Last Name
      - Manager
      - Region
      - Username

   c. Click **Run Search**

   d. Sort on **Manager**

e. There are 4 identities without managers: the default identity spadmin and 3 others (Jerry Bennett, James Smith, Aaron Nichols). What department is listed for the 3 identities without managers?

_____

Exercise #4: Organize Identities

Objective

In this exercise, you will work with the different options for grouping identities in IdentityIQ based on users' access needs or IdentityIQ responsibilities.

Overview

In this exercise, you will create populations, groups, and workgroups.

Populations and groups are used to specify sets of identities to include in various activities. For example, the refresh task can be limited to a pre-defined set of identities, or a pre-defined set of identities can be certified.

Workgroups are used to define sets of identities who should have additional responsibilities within IdentityIQ. Rapid Setup includes workgroups which you will update to include the appropriate members and IdentityIQ capabilities.

Create Populations

For your implementation, you want to use Advanced Analytics to define populations based on specific identity criteria. You will create six populations that will be used to assign birthright access to new employees and contractors when they join the company. You will use these populations later when creating birthright roles and configuring Rapid Setup.

Population	Membership Criteria
Active Employees	Is Inactive: False Type: Employee
Active Contractors	Is Inactive: False Type: Contractor
Global	Is Inactive: False Is Correlated: True
Americas	Is Inactive: False Region: Americas Type: Employee
Asia-Pacific	Is Inactive: False Region: Asia-Pacific Type: Employee
Europe	Is Inactive: False Region: Europe Type: Employee

1. Create a population for your active employees.

    a. Log into IdentityIQ as **spadmin/admin**

    b. Navigate to **Intelligence** > **Advanced Analytics**

c. Make sure Search Type is **Identity**

d. Click **Clear Search**

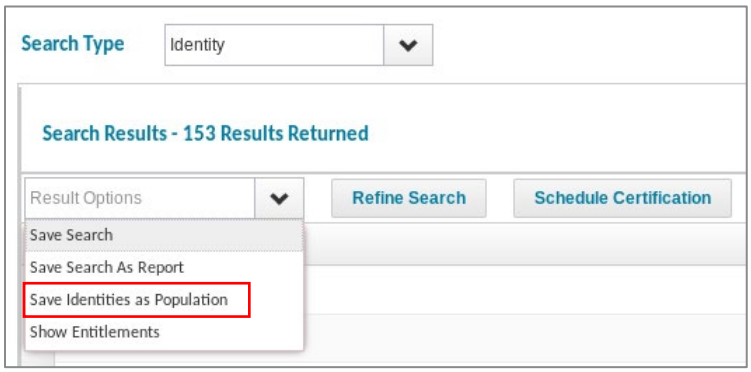
e. Select the following search criteria:

i. Is Inactive: **False**

ii. Type: **Employee**

f. Click **Run Search**

g. From the **Result Options** drop down menu, select **Save Identities as Population**



i. Name: **Active Employees**

ii. Description**: Active employee identities**

Important: For each of these populations, ensure you're typing the **Name** exactly as shown. These names are referenced in training XML files later, which you'll import into IdentityIQ to define birthright roles.

iii. Click **Save**

2. Create a population for your active contractors.

a. First click **Refine Search**,

b. Update the search parameters:

i. Is Inactive: **False**

ii. Type: **Contractor**

c. Click **Run Search**

d. From the **Result Options** drop down menu, select **Save Identities as Population**

i. Name: **Active Contractors**

ii. Description**: Active contractor identities**

iii. Click **Save**

3. Create a population for authoritative identity cubes.

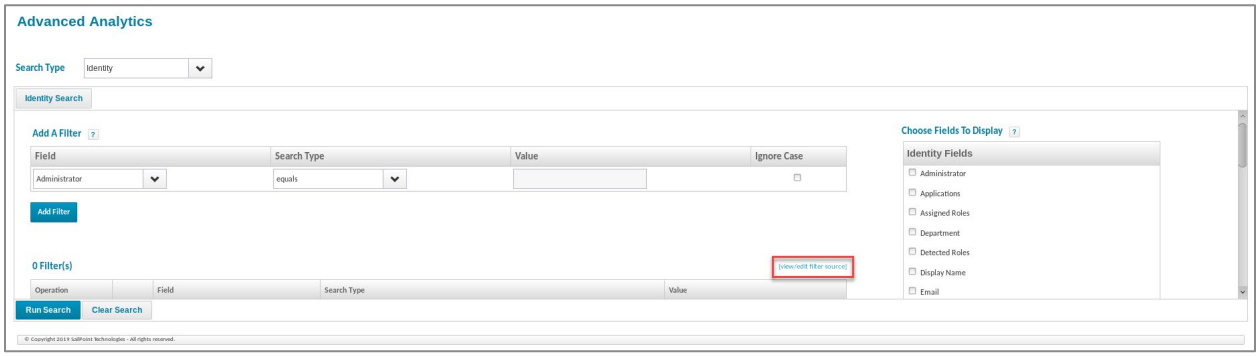
   a. Click **Refine Search**

   b. Click **Clear Search** to reset everything.

   c. Click **Advanced Search**

   d. In the **Choose Fields To Display** section, make sure at least one field is selected; if none are selected, select **Username**.

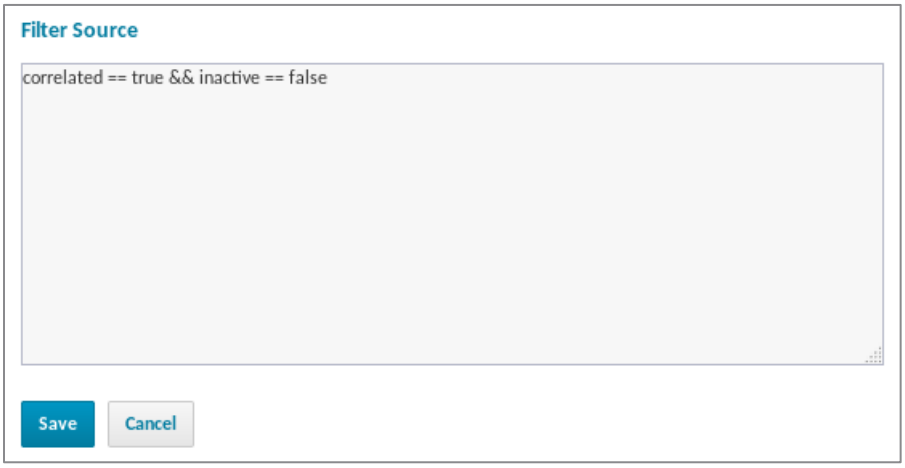
   e. Click **view/edit filter source**



   f. In the **Filter Source** text box, type:

```
correlated == true && inactive == false
```

   Note: This search looks for active, authoritative identity cubes. IdentityIQ sets the attribute 'correlated=true' on identity cubes that are authoritative.



   g. Click **Save**

h. Click **Run Search**

i. Save resulting identities as a population with the following:

i. Name: **Global**

ii. Description: A**ctive authoritative identities**

4. Update the three new populations' visibility settings to "public".

Populations are initially created with a "private" visibility setting; therefore, you'll update the visibility settings to "public" so your colleagues will be able to view and use these populations.

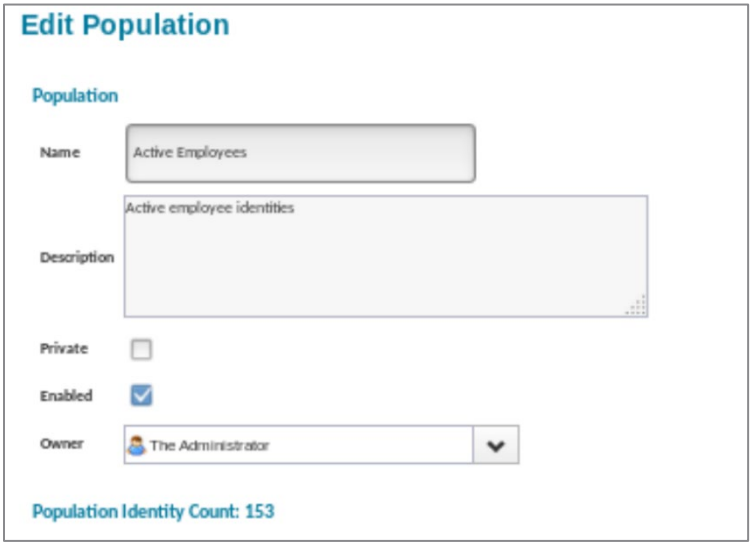
a. Navigate to **Setup** > **Groups** > **Populations**

b. Make the **Active Employees** population publicly visible.

i. Click the population named **Active Employees**

Notice the list of the members of this population. Populations are dynamic queries, so every time you view a population, you are viewing its current members at that point in time.

ii. Deselect the **Private** option.



iii. **Save** population.

c. Repeat these steps for the **Active Contractors** population to make its visibility public.

d. Repeat these steps for the **Global** population to make its visibility public.

5. To save time in this class, import the remaining populations: Americas, Europe, and Asia-Pacific.

   a. Navigate to **Gear** > **Global Settings** > **Import from File**

   b. In the **Import Objects** section, click **Browse…**

   c. Open the following file:
   /home/spadmin/ImplementerTraining/config/Populations.xml

   d. Click **Import**

   Loading this file will create 3 populations: **Americas**, **Europe**, and **Asia-Pacific**. All three have similar search criteria:

   - Is Inactive: **False**
   - Type: employee
   - Region: either Americas or Europe or Asia-Pacific
   - Visibility: Public

Use Group Factories to Generate Groups

You have been asked to generate groups of identities based on the departments in your organization. Because you defined the department Identity Attribute as a group factory earlier when you defined the identity mappings, IdentityIQ can calculate and generate groups of identities based on this field. These groups can be used in reporting and other portions of the product. Groups are similar to populations, except that groups are statically defined based off a single identity attribute, whereas populations are driven off of multiple search criteria. You will use a rule to assign ownership to each group.

Sub-groups are created based on the attribute values found for each attribute at the time you run the **Refresh Groups** task. Thus, you must periodically run the task to update the sub-groups. Between runs of **Refresh Groups**, the sub-groups themselves remain static, but the *sub-group membership is always based off a dynamic query.*

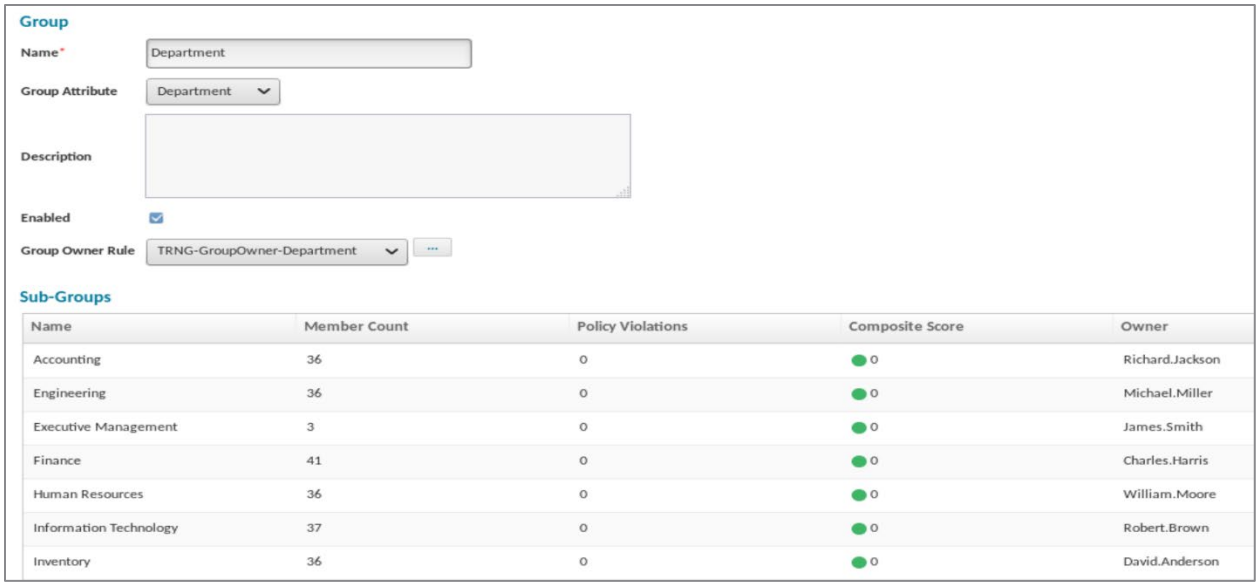
To help explain this concept, consider this example: you have a "location" group factory that currently only has 2 sub-groups: Dallas and Boston. Your employee Joe moves from Dallas to Boston. The next time you use that group factory, for example, when running a report, IdentityIQ will immediately recognize that Joe is now part of the Boston sub-group.

Later, your company adds another office location in Miami. Joe moves from Boston to Miami. If you haven't run a "Refresh Groups" task, then IdentityIQ will not recognize Miami as a sub-group. Instead, IdentityIQ will remove Joe from all sub-groups. You must run a "Refresh Groups" task to create the Miami sub-group.

1. Load the rule that will be used to set Group ownership.
    a. Navigate to **Gear** > **Global Settings** > **Import from File**
    b. In the **Import Objects** section, click **Browse…**
    c. Open the following file: **/home/spadmin/ImplementerTraining/config/Rule-GroupOwner-DepartmentOwner.xml**
    d. Click **Import**
2. Navigate to **Setup** > **Groups** > **Groups** tab
3. Click **Create New Group** and fill in the following fields:
    a. Name: **Department**
    b. Group Attribute: **Department**
    c. Description: **Identities grouped by department**
    d. Enabled: **Checked**
    e. Group Owner Rule: **TRNG-GroupOwner-Department**
4. Click **Save**
5. Generate Groups using the newly created group configuration and confirm that they were created correctly.
    a. Navigate to **Setup** > **Tasks** and search for the task **Refresh Groups**
    b. Click the task to view its configuration options.

        Notice this is an Identity Refresh task with only one option selected: **Refresh the group scorecards**

    c. Scroll down and choose **Save and Execute**
6. Confirm that the groups were created correctly.
    a. Navigate to **Setup** > **Groups**
    b. On the **Groups** tab, click **Department**
    c. Make sure that there are many sub-groups and the owner fields are populated.



Update Workgroups

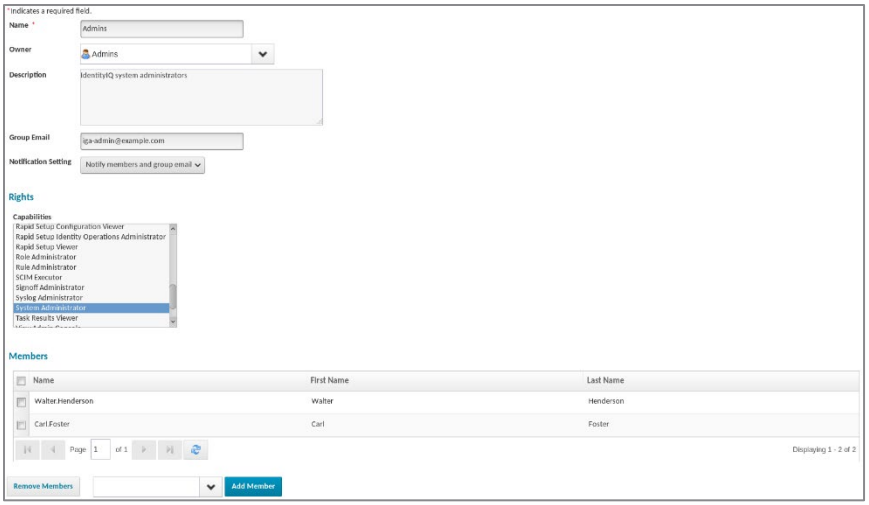
Workgroups allow identities to share responsibilities and object ownership within IdentityIQ. They also support assigning capabilities and scope to these groups so that you do not have to assign the same scopes and capabilities to each individual member of the group.

IdentityIQ and Rapid Setup include several workgroups. In this exercise, you will create your own workgroups, add identities to workgroups, and update their configuration settings. Note that you are not changing all workgroups.

1. Create the Admins workgroup.
    a. Navigate to **Setup** > **Groups** > **Workgroups**
    b. Click **Create Workgroup** and fill in the following fields:
        i. Name: **Admins**
        ii. Description: **IdentityIQ system administrators**
        iii. Group Email: **iga-admin@example.com**
        iv. Notification Setting: **Notify members and group email**
        v. Capabilities: **System Administrator**

        Note: If you accidentally select the wrong capability, to de-select, hold down the control key and click the capability.

        vi. Members: type or select **Walter.Henderson** and click **Add Member**
        vii. Members: type or select **Carl.Foster** and click **Add Member**



c. **Save** this workgroup.

2. Create the Business Analysts workgroup.

   a. Click **Create Workgroup** and fill in the following fields:

      i. Name: **Business Analysts**

      ii. Description**: IdentityIQ analysts responsible for interpreting and making changes based on business data**

      iii. Notification Setting: **Notify members only**

      iv. Rights:

         (1) **Identity Correlation Administrator**

         (2) **Rapid Setup Administrator**

         Note: To select multiple capabilities, hold down the control key while you click the required capabilities.

      v. Members:

         (1) **Jim Lee**

         (2) **Lauren Harrison**

   b. **Save** this workgroup.

3. Create the Operations workgroup.

   a. Click **Create Workgroup** and fill in the following fields:

      i. Name: **Operations**

ii. Description: **IdentityIQ operators responsible for monitoring certifications, provisioning, tasks, and modifying Rapid Setup global configurations**

iii. Group Email: **operations@example.com**

iv. Notification Setting: **Notify members and group email**

v. Rights:

(1) **Compliance Officer**

(2) **Full Access Admin Console**

(3) **Rapid Setup Configuration Administrator**

vi. Members:

(1) **Mary Johnson**

(2) **Dennis Barnes**

(3) **Tyler Petrick**

b. **Save** this workgroup.

4. Update the Rapid Setup No Manager workgroup.

a. Click **Rapid Setup No Manager** and update the following:

i. Description: **Receives Rapid Setup manager emails for users with no manager defined**

ii. Group Email: **security@example.com**

iii. Notification Setting: **Notify group email only**

b. **Save** this workgroup.

Configure Rapid Setup Error Notifications

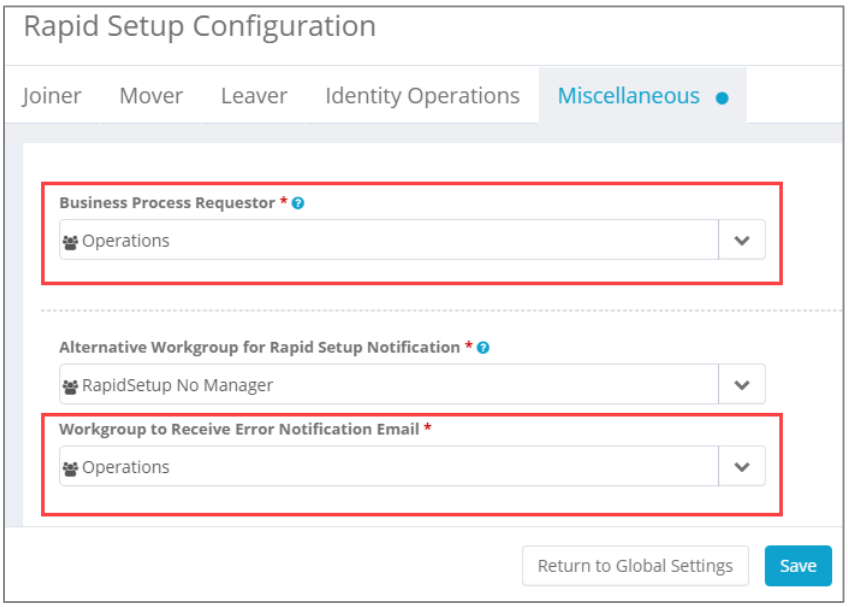
Now that you have created workgroups with members and the appropriate capabilities to facilitate identities sharing responsibilities within IdentityIQ, you will update the Rapid Setup configuration. If any provisioning errors occur in the Rapid Setup workflows, we want IdentityIQ to notify our Operations workgroup. Additionally, we want the Rapid Setup workflows requestor to be listed as the Operations workgroup.

1. Navigate to **Gear > Global Settings > Rapid Setup Configuration**

2. Navigate to the **Miscellaneous** tab and configure as follows:

a. Business Process Requestor: **Operations**

b. Workgroup to Receive Error Notification Email: **Operations**



c. Click **Save**

Run Report to View Identities' Capabilities

1. Navigate to **Intelligence** > **Reports** and select the **Reports** tab.

   From the **Reports** tab, reports can be used in two ways:

   - As a default report: right click the desired report and select **Execute**. This will run a report with no filtering.
   - As a template: click the desired report to open it and use it as a template. This will create a new copy of the report which you can filter as provided by the report options. This new report will be saved on the My Reports tab.

2. Find the **Identity to Capabilities** Report, **right click** and select **Execute**
3. Wait for the report to finish and then view the report results on the **Report Results** tab.
4. Notice the identities and workgroups that have capabilities – these identities have these capabilities because they are part of those workgroups.

View an Identity's Capabilities on their Identity Cube

1. Navigate to **Identities** > **Identity Warehouse** and view **Mary Johnson**'s identity cube.
2. Navigate to the **User Rights** tab.

Here you could directly assign capabilities to Mary. However, it's a best practice to assign capabilities through workgroup membership rather than to individuals.

In the Workgroups list, you can see all workgroups Mary is a member of.

a. List her workgroups:

_____

In the Indirect Rights list, you can see all capabilities that Mary holds because of her workgroup memberships.

b. List her indirect rights:

_____

Retire the spadmin Account

A best practice for IdentityIQ implementations is to "retire" the spadmin identity. Once you've created identities in IdentityIQ and granted them the appropriate capabilities, including granting certain identities the **System Administrator** capability you should enable work item forwarding and reset the spadmin password. Additionally, you should check to see if spadmin is the owner of any objects. When you onboarded the HR applications, you selected spadmin as the owner because in the early phase of implementation, there were no other identities to specify as owner. It is a best practice to find objects that you may have specified spadmin as the owner early in your implementation and update them as part of the retiring process.

All IdentityIQ installations come with the default user: spadmin/admin. The password should be changed to something unique and secure for your organization. While the password for spadmin is "admin", *no authentication is required to access the IdentityIQ Console*. After changing this password, users will be prompted for their credentials when accessing the IdentityIQ Console. Only users who have System Administrator capability can access the IdentityIQ Console.

1. Navigate to **Applications** > **Application Definition**
2. Edit the **HR Employees** application.
    a. Select Owner: **Admins**
    b. Click **Save**
3. Edit the **HR Contractors** application.
    a. Select Owner: **Admins**
    b. Click **Save**

4. At the far right of the main menu, navigate to **The Administrator** > **Preferences**

   a. On the **General** tab set the following:

      i. Email Address: **iga-admin@example.com**

      ii. Select Forwarding User: **Admins**

   b. On the **Password** tab, set the following:

      i. Current Password: **admin**

      ii. New Password: **SailPoint1!**

      iii. Confirm New Password: **SailPoint1!**

   c. **Save** preferences.

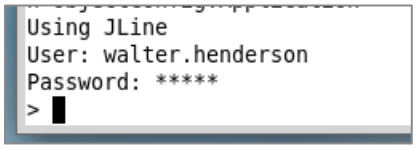
5. **Log out** of IdentityIQ.

6. Launch the **IIQ Console**

7. Wait for the **User:** prompt to enter the credentials of a System Administrator

   a. User: **walter.henderson**

   b. Password: **xyzzy**



   c. How does Walter have the System Administrator capability?

   _____

8. **Quit** the console.

Exercise #5: Define LDAP Application

Objective

In this exercise, you will onboard account and group data from an LDAP application.

Overview

Your virtual machine includes a running instance of LDAP. You will onboard this LDAP application using the OpenLDAP direct connector.

Define LDAP Application

1. Log in to IdentityIQ as **Carl.Foster/xyzzy**

   Note: since Carl is part of the **Admins** workgroup, he has the System Administrator capability.

2. Navigate to **Applications** > **Application Definition**

3. Click **Add New Application**

4. On the **Details** page, set the following:

   a. Name: **LDAP**

   b. Owner: **Admins**

   c. Application Type: **OpenLDAP – Direct**

      Note: As you work with the OpenLDAP – Direct connector, you'll see that there are predefined account and group schemas, as well as several fields for which the connector provides default values. This is typical of IdentityIQ connectors.

5. Navigate to **Configuration** > **Settings** tab and set the following:

   a. Use TLS: **not checked**

   b. Authorization Type: **Simple**

   c. User: **cn=Manager,dc=training,dc=sailpoint,dc=com**

   d. Password: **password**

   e. Host: **training.sailpoint.com**

   f. Port: **389**

   g. Page Size: **100**

h. Authentication Search Attributes:

i. **cn**

ii. **uid**

iii. **mail**

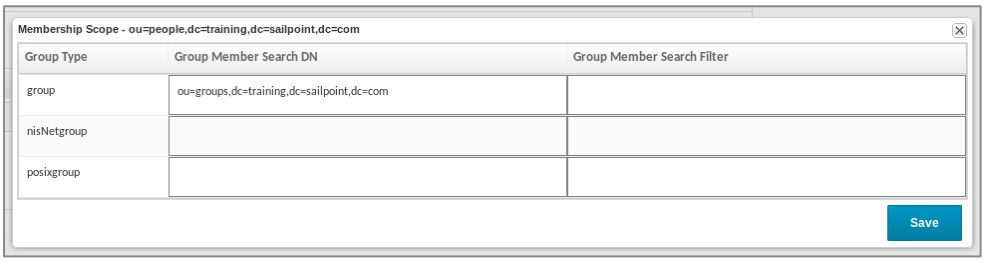
6. Still on **Configuration** > **Settings** page, in **Account Search Scope**, set the following:

a. Search DN: **ou=people,dc=training,dc=sailpoint,dc=com**

b. On same row, click **Configure** under **Group Membership Scope**

c. On **group** row, set Group Member Search DN: **ou=groups,dc=training,dc=sailpoint,dc=com**

d. Click into another cell, and then **Save**



e. Click **Add**

i. This will add another row, so your screen should look as follows:

f. Click the **Group** tab.

g. For Object Type **group** set the following:

i. Search DN: **ou=groups,dc=training,dc=sailpoint,dc=com**

ii. Click **Add**

7. View the predefined account schema.

a. Navigate to **Configuration** > **Schema**

b. View the account schema under **Object Type: account**

c. Find the **groups** attribute.

i. What are its properties?

_____

ii. In the box below, match these options with their functionality.

Option	**Functionality**
A) Managed Functionality: _____	1) Designates an attribute that represents entitlements on the native application. Used to promote an identity's value(s) for this attribute to their Entitlement tab on their Identity Cube
B) Entitlement Functionality: _____	2) Designates an attribute that has multiple values
C) Multi-Valued Functionality: _____	3) Designates an attribute that should be managed in IdentityIQ. Used to promote all values for this attribute to the Entitlement Catalog

iii. What is its type?

_____

Note: "group" is an available option for Type because the OpenLDAP – Direct connector includes three group schemas (group, posixgroup, and nisNetgroup). This field is how IdentityIQ links the identity's group membership (designated in the account schema, group field) to the group details (designated in the group schema).

8. View the predefined group schema.
   a. Scroll down to the **Object Type: group** section.
   b. Find the **Description Attribute** in the group section details. The description attribute identifies the attribute that contains the group description that will be loaded in the entitlement catalog. This information in the entitlement catalog helps your business users correctly review and request access. The description will be loaded into the entitlement catalog when the group is first aggregated, allowing changes made in the entitlement catalog UI to supersede the aggregated data. If you want the description updated at every aggregation, you could leverage the Group Aggregation Refresh Rule.
9. Navigate back to **Configuration** > **Settings** to test the connection.
   a. Click **Test Connection** and verify it's successful.
10. **Save** application.

Configure LDAP Application

Use Rapid Setup to configure entitlement request status, correlation logic, and account classification configurations for LDAP.

1. Navigate to **Applications > Rapid Setup**
2. Choose **LDAP** and click **Next**
3. On the **Aggregation** page, set the following:
   a. Create Entitlements That Cannot Be Requested: **Enabled**

      This specifies that entitlements aggregated from this application will be marked as non-requestable in the entitlement catalog. You can override the requestability of individual entitlements after aggregation.

   b. Add identity correlation logic:
      i. Application Attribute: **cn**

ii. Operation: **Equals**

iii. Identity Attribute: **Display Name**

Note: You can also specify correlation logic through a correlation rule or the correlation wizard found on the Correlation page of the application.

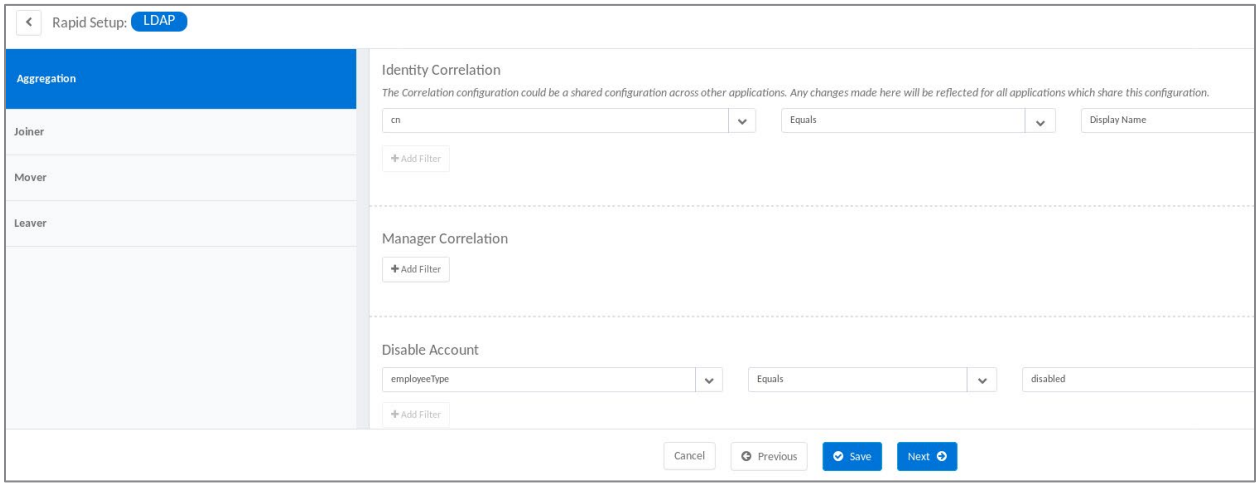
4. Add disable account logic.

   LDAP implementations may be customized to use custom attributes to store the account status. In our lab environment of LDAP we are using the employeeType account attribute to store the account status. If an account has employeeType = disabled we want to show that account as disabled within IdentityIQ.

   a. Application Attribute: **employeeType**

   b. Operation: **Equals**

   c. Value: **disabled**



5. Click **Save**

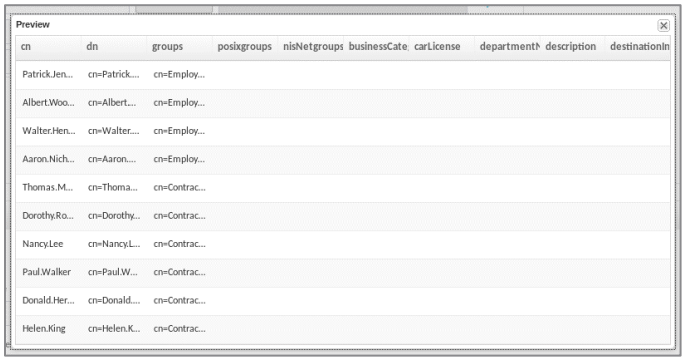
Preview LDAP Account and Group Data

Before aggregating you can use Preview to test and confirm that your configurations result in expected behaviors. Preview iterates over the first 10 accounts and displays the results in a popup window instead of loading the accounts into IdentityIQ. Remember that Preview does not write any information to the IdentityIQ database, but instead it is very useful to ensure that you are properly reading and manipulating the data and that your schema is correct.

1. Navigate to **Applications** > **Application Definition** > **LDAP**

2. Navigate to **Configuration** > **Schema**

3. In the **Object Type: account** section, scroll down and select **Preview**



Important: if you do not see "groups" populated, this is likely because you have a problem with the Group Membership Scope. If necessary, correct as follows.

4. Navigate to the **Account** tab of the **Configuration** > **Settings** page.

   a. Under **Account Search Scope**, find the row with a populated Search DN

   b. Click **Configure** under **Group Membership Scope**

   c. For the group row, ensure that the **Group Member Search DN** matches the following:

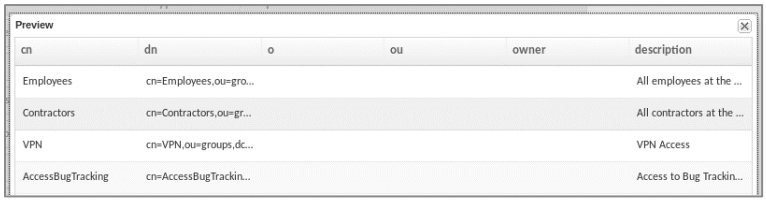
   ```
   ou=groups,dc=training,dc=sailpoint,dc=com
   ```

   d. **Save** application.

5. Navigate back to the **Schema** page, select **Preview**, and confirm that the groups column is populated.

6. **Close** the preview and on the same page, scroll down to the last schema, **Object Type: group**, and select **Preview**

   This command will iterate through the group information, and you can confirm that the Groups and Permissions are being extracted from the file correctly.



7. **Close** the preview.

8. At the bottom of the page, click **Cancel** to exit the application definition.

Use connectorDebug to Review LDAP Application Account Data

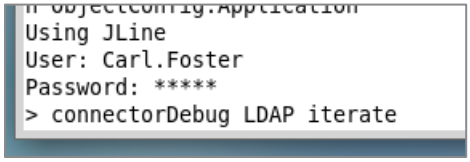
The console **connectorDebug** command iterates over all of the accounts in an application and displays the results of the iteration, resource objects, to the console screen instead of loading them into IdentityIQ. Like the Preview button, this command can be extremely useful when doing initial work onboarding applications to make sure that you are properly reading and manipulating the data and that your schema is correct.

1. Open the IdentityIQ Console.
2. Login as **Carl.Foster/xyzzy**
   a. What capability gives Carl access to the IdentityIQ Console?

      _____

3. Use connectorDebug to confirm the configuration.
   a. Within the IIQ Console, enter:

      ```
      connectorDebug LDAP iterate
      ```

      All the accounts are scanned, and the resource objects are displayed to the screen. To send the output to a file, use the commands appropriate to the operating system in use.

      Here is the example for the Linux environment:

      ```
      connectorDebug LDAP iterate > ldap_accounts.txt
      ```

   Caution: Be aware of how much data you will process. The connectorDebug command will iterate through *all* accounts for the application, whether 200 or 200,000. To test an application with a large number of accounts, apply a filter on the application definition prior to using the connectorDebug command.

4. In the screenshot below, circle the multi-valued attributes and all of their values.

   Hint: The values for multi-valued attributes are contained within List tags.

   a. Where did you designate that these attributes can have multiple values?

      _____

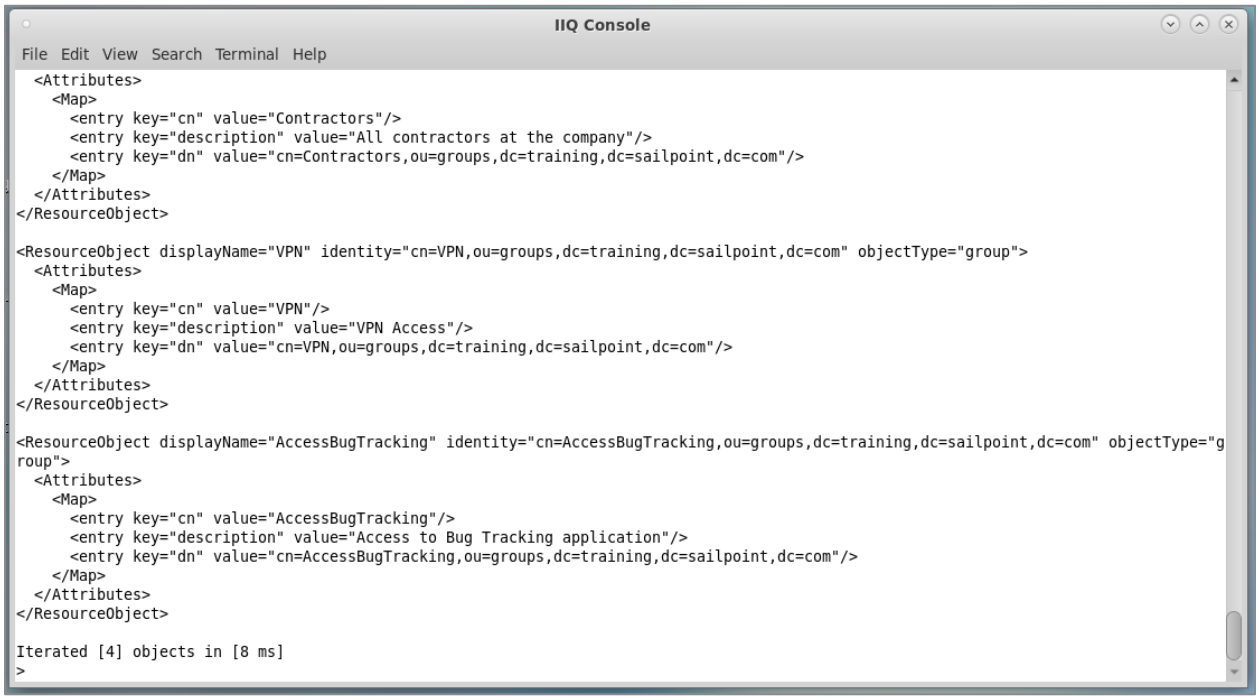
   Note: Best practice is to start by using Preview (the only option for those who do not have console access). The connectorDebug command is useful for debugging problems with multi-valued attributes and when debugging build map rules (you see the output from the rule interspersed with the account information), etc. Remember to use available filtering to limit the data processed.

Use connectorDebug to Confirm LDAP Application Group Data

1. Return to the IIQ Console and run the following command:

   ```
   connectorDebug LDAP iterate group
   ```

Like Preview Groups, running the connectorDebug command with the group option will iterate through the application group information.



2. **Quit** the console.

   Remember, the connectorDebug command only shows a debug view of the data; you haven't actually loaded any Account and Account Group data into the system.

Update Source for Identity Attribute Email

Most of the identity attributes for the training implementation were sourced from the authoritative applications, HR Employees and HR Contractors, but the email attribute should be sourced from LDAP. You will add this source mapping before aggregation to update the identity cubes with the email address sourced from the LDAP application.

1. Navigate to **Gear** > **Global Settings** > **Identity Mappings**
2. Click the attribute named **Email**.
3. Under **Source Mappings**, click **Add Source**
   a. Select: **Application Attribute**
   b. Application: **LDAP**
   c. Attribute: **mail**
   d. Click **Add**

4. **Save** the email identity attribute.

Load LDAP Accounts and Groups

Now you are ready to aggregate account and group data from the LDAP system.

1. Define and execute an account aggregation task.
   a. Navigate to **Setup** > **Tasks** and under **New Task**, choose **Account Aggregation**
   b. Define the task as follows:
      i. Name: **Aggregate LDAP**
      ii. Previous Result Action: **Rename Old**
      iii. Select applications to scan: **LDAP**
      iv. Select the **Detect deleted accounts** checkbox.
      v. Select the **Disable optimization of unchanged accounts** checkbox.
      vi. Select the **Promote managed attributes** checkbox.
      vii. Below, match these selected options with their functionality.

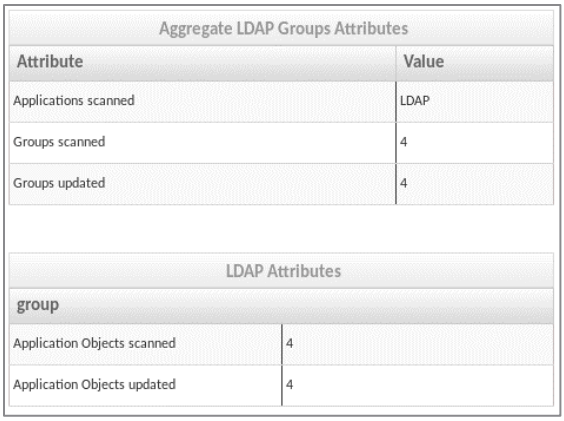
Option	**Functionality**
A) Detect deleted accounts Functionality: _____	1) Force all accounts to be read, even if unchanged since the last aggregation
B) Disable optimization of unchanged accounts Functionality: _____	2) Delete accounts in IdentityIQ that no longer exist in the native application
C) Promote managed attributes Functionality: _____	3) Add any values for "Managed" entitlements or permissions to the Entitlement Catalog

   c. Scroll down and click **Save and Execute** and click **OK** when prompted.
   d. Make sure that your task results match the following.

Aggregate LDAP Attributes	
Attribute	**Value**
Applications scanned	LDAP
Accounts scanned	234
Identities updated	234
Managed entitlements promoted	4
Identity Entitlements Created	236

2. Define and execute an account group aggregation task.
   a. Navigate to **Setup > Tasks** and under **New Task**, choose **Account Group Aggregation**
   b. Define the task as follows:
      i. Name: **Aggregate LDAP Groups**
      ii. Previous Result Action: **Rename Old**
      iii. Select applications to scan: **LDAP**
      iv. Select the **Detect deleted account groups** checkbox.
      v. Set Automatically promote descriptions to this locale: **en_US**

      Note: Remember the group schema Description Attribute? Here is where we specify what locale the description should be updated to. IdentityIQ supports language localization, showing the user the appropriately translated description based on their browser language settings.
   c. Click **Save and Execute** and click **OK** when prompted.
   d. Make sure your task results match the following picture.



Aggregate LDAP Groups Attributes

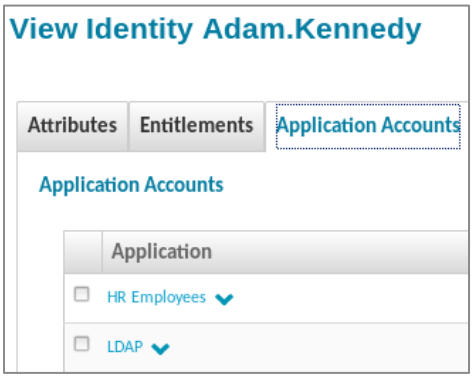
Attribute	Value
Applications scanned	LDAP
Groups scanned	4
Groups updated	4

LDAP Attributes

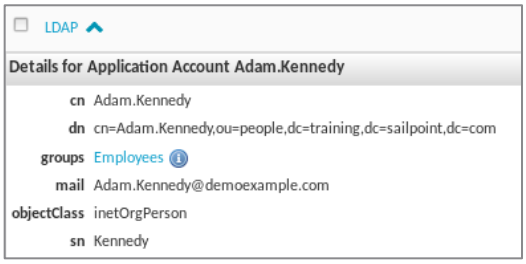
group	
Application Objects scanned	4
Application Objects updated	4

View Aggregation Results

1. Navigate to **Identities** > **Identity Warehouse** and find **Adam.Kennedy**
2. Click **Application Accounts** and verify that the LDAP account correlated successfully.



3. Click the **LDAP** account and observe the details for the **LDAP** application account.



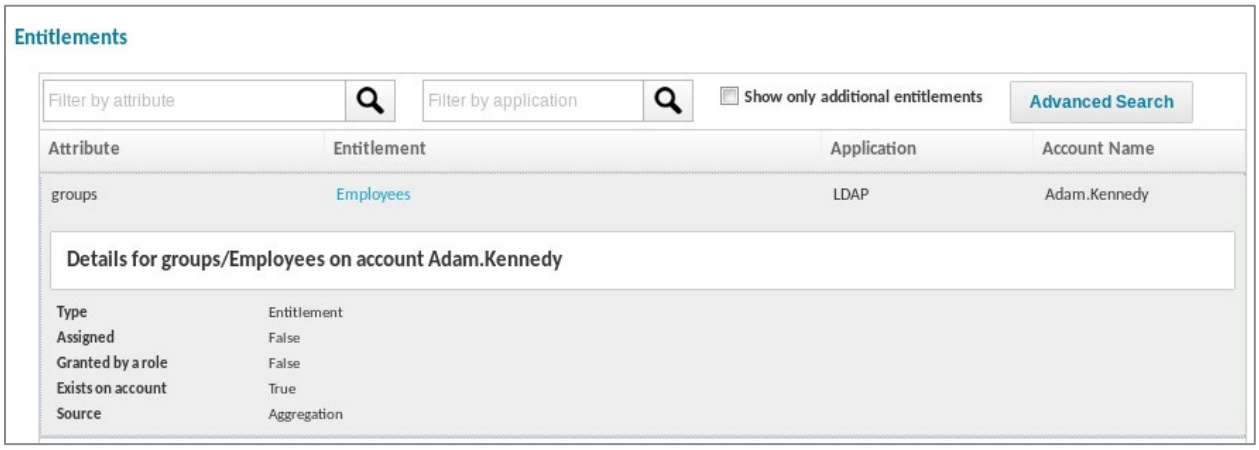
4. Consider your identity attribute mapping for email. Compare Adam's LDAP account attributes to the identity cube's Attributes tab data.
   a. Was your mapping configuration applied to populate the identity attribute during the LDAP aggregation process or do we still need a Refresh task to manage this?

_____

5. Within the same Identity (Adam.Kennedy), click **Entitlements**
6. Under **Entitlements**, click the **groups** row to expand the information related to this group.
   a. What is the source of this entitlement?

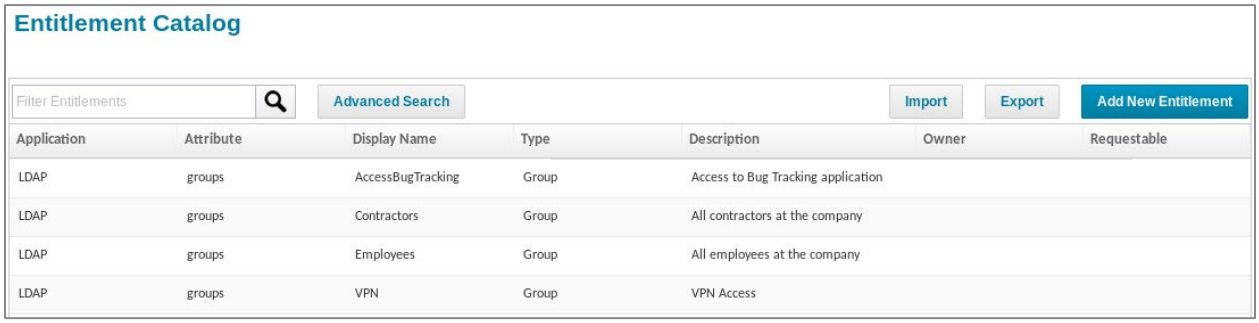
      _____

   b. Was this entitlement assigned through IdentityIQ? -Select-



The **Source** is aggregation and **Assigned** is false. This means this is a detected entitlement that IdentityIQ discovered from your environment via **Aggregation**.

7. Navigate to **Applications** > **Entitlement Catalog** and notice that the entitlement values from the **LDAP** application have been loaded.



These values were loaded because the **groups** attribute is marked as **Managed** in the application schema and you selected options on the aggregation task.

a. On the **Aggregate LDAP** task, which option did you select that told IdentityIQ to promote the groups as managed attributes to the Entitlements Catalog?

   _____

8. From the **Entitlement Catalog**, click the **Employees** group and view the options on the **Standard Properties** tab.

    a. What configuration specified the **Requestable** option was unchecked?

    _____

9. Click the **Members** tab to view the identities in the LDAP Employees group.

    a. How many identities are in this group? _____

Refresh Identity Cubes

Once all aggregations are complete, an identity refresh is required to complete processing of the identity data. Though aggregations result in entitlement attributes appearing on the Identity Cube Application Accounts and Entitlements tabs, one more step (a refresh) is required to fully promote entitlements and make them usable by other processes, such as certification.

1. Navigate to **Setup** > **Tasks** and search for the task **Refresh Identity Cube**

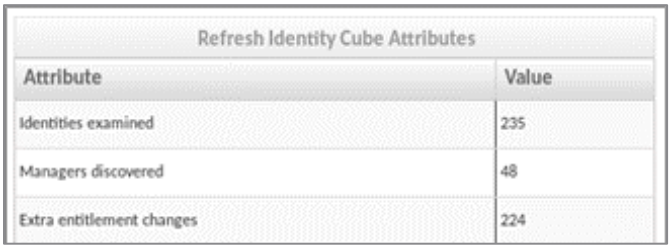
    a. Select the **Refresh Identity Cube** task to edit it.

    b. Find the option **Refresh assigned, detected roles and promote additional entitlements** and enable it by checking the box next to it.

    Previously you disabled this option. Now that you have onboarded an application with entitlements to promote, we are enabling this option before executing the task.

    c. Scroll down and select **Save and Execute**

2. Confirm the results of the identity refresh.



Refresh Identity Cube Attributes	
Attribute	Value
Identities examined	235
Managers discovered	48
Extra entitlement changes	224

Exercise #6: Enable Pass-Through Authentication

Objective

Now that you've onboarded the LDAP application, you will update IdentityIQ settings.

Overview

Now that LDAP is connected to IdentityIQ, you can configure additional settings that are dependent on LDAP. You will configure pass-through authentication and learn how to allow users to reset their forgotten password by answering a series of authentication questions.

Enable Pass-Through Authentication to LDAP

In pass-through authentication, one application delegates the authentication request to another application, such as LDAP or Active Directory. In many environments, businesses do not want to create a new login and password when a new Identity Management solution is deployed. To make it easier for users to access IdentityIQ, customers choose to use single sign-on (SSO) or directory credentials to log in. This lab will have you configure pass-through authentication, from IdentityIQ to LDAP.

1. Test IdentityIQ credentials
    a. Log out of IdentityIQ and attempt to log back into IdentityIQ using Catherine Simmon's LDAP credentials: **Catherine.Simmons/password**
    b. Log out of IdentityIQ and attempt to log back into IdentityIQ using Catherine Simmon's IdentityIQ credentials: **Catherine.Simmons/xyzzy**
    c. Which credentials allowed you to log in as Catherine? -Select-
2. Log out of IdentityIQ and back in as **Carl.Foster/xyzzy**
3. Navigate to **Gear** > **Global Settings** > **Login Configuration**
4. On the **Login Settings** tab, set Pass through application: **LDAP**
   Note: Only applications that support the pass-through authentication feature will be available to select. In the training environment, only LDAP supports pass through authentication
5. Click the **Save** button.
6. Update the LDAP application to change the account attributes to be used for pass-through authentication.
    a. Navigate to **LDAP** application

b. On the **Configuration** page, view the **Authentication Search Attributes**.

These are default values set by the LDAP connector.

c. Delete the values **uid** and **mail**

Note: You are deleting these 2 attributes because you are only using the cn attribute for pass-through authentication.

d. **Save** the application definition.

7. **Log out** of IdentityIQ

Now that you have enabled pass-through authentication to LDAP, users can log into IdentityIQ with either their IdentityIQ credentials or their LDAP credentials.

8. Log into IdentityIQ using Catherine Simmon's LDAP credentials:
Catherine.Simmons/password

Note: This feature allows users to use a known login, reducing the operational impacts of rolling out a new Identity Management solution. Best practice is to remove the password you have been using that is unique to IdentityIQ (xyzzy) once pass-through authentication is enabled. While it is present, the IdentityIQ internally-stored password will be treated as a valid, fallback login option.

Note: In the IIQ Console or IdentityIQ log file, you'll notice errors from LDAP that report failed authentication. This error is triggered when you use the native password (xyzzy) to log into IdentityIQ. This is because pass-through authentication is enabled, which allows IdentityIQ to confirm the identity's password on that application (LDAP) before checking the internal password.

Configure Forgot-Password Password-Reset

Many times, users forget their passwords after vacation or other leaves of absence. Password resets typically represent the largest volume of requests to the helpdesk. By providing users the ability to reset their own passwords, IdentityIQ can help increase user productivity and reduce the workload for helpdesk administrators.

1. Enable Forgot Password.

a. Log out of IdentityIQ and log back in as **Carl.Foster/password**

b. Navigate to **Gear** > **Global Settings** > **Login Configuration**

c. Navigate to the **User Reset** tab.

i. Check the box for **Enable Forgot Password**

ii. Check the box for **Enable Security Questions**

d. Briefly review the Security Question Configuration to see the default behavior.

Here you can configure the quantity of required questions and the set of possible questions that users must answer to authenticate successfully when they forget their password.

e. Scroll down to the **Settings** section and check the box for **Prompt users for answers to unanswered security questions upon successful login**

This option will force users to provide answers to their security questions the next time they login, to prepare for the possibility of forgetting their password in the future.

f. Click **Save**

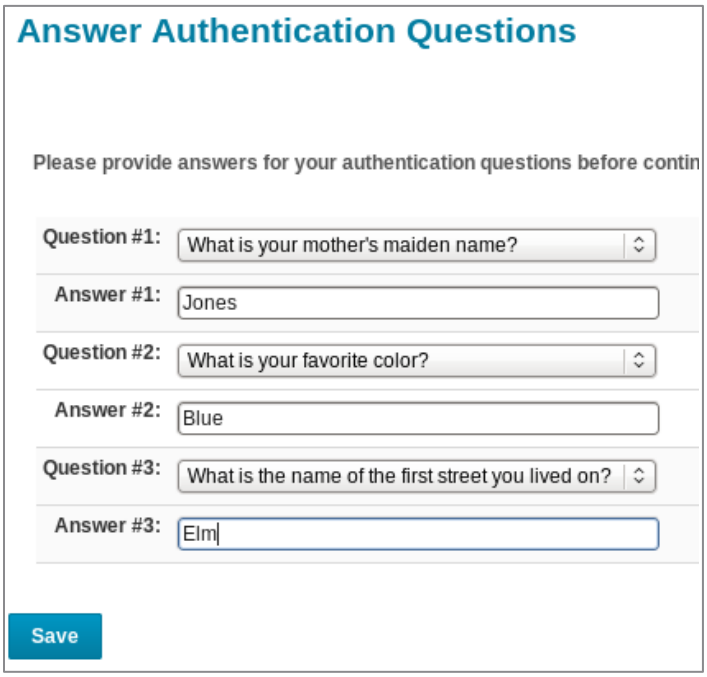
g. **Log out** of IdentityIQ.

2. Answer Authentication Questions.

a. Log into IdentityIQ as **Catherine.Simmons/password**.

This time Catherine is prompted to answer three of her authentication questions before she can proceed.

b. For demonstration purposes, select the questions and answers as shown below.

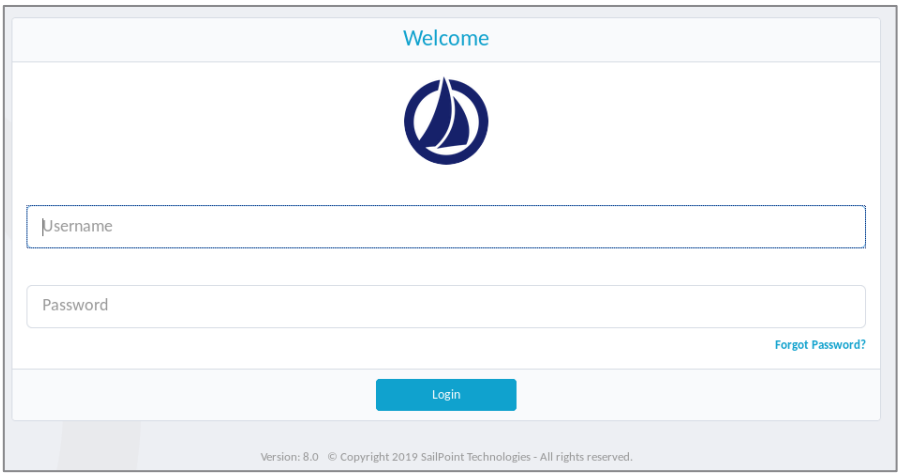


c. **Save**

d. **Log out** of IdentityIQ.

3. Test Forgot Password functionality.

   a. Now that you have enabled the Forgot Password feature, you should now see a **Forgot Password?** link on the Login screen.



   b. Enter **Catherine.Simmons** for the Username and click **Forgot Password?**

   c. Catherine will be presented with a form to enter the answers to her authentication questions and to specify a new password.

      i. Select the questions and enter the appropriate answers, **all in lowercase**.

      ii. Enter **rsty1234** for **Password** and **Confirm Password** and click **Submit**

      iii. Were the password reset answers case sensitive?

      _____

      iv. Why were only 2 authentication questions presented to Catherine?

      _____

   d. On your desktop, launch the **Tail Email Log** shortcut to check the email log file.

      You should see an email notification was sent to Catherine notifying her that her password was successfully changed.

   e. Upon which application was the password changed? Why?

      _____

f. To simplify the rest of the exercises, go back and turn off the prompt for security questions configurations. This will prevent you from having to answer everyone's security questions.

   i. Log in to IdentityIQ as **Carl.Foster/password**

   ii. Although you are prompted for answers to security questions, you will not use these in future exercises. Use the same questions and answers as before:

      (1) Question: **What is your mother's maiden name?** Answer: **Jones**

      (2) Question: **What is your favorite color?** Answer: **Blue**

      (3) Question: **What is the name of the first street you lived on?** Answer: **Elm**

   iii. Navigate to **Gear** > **Global Settings** > **Login Configuration**

   iv. On the **User Reset** page, **uncheck** the box for **Prompt users for answers to unanswered security questions upon successful login** and **Save**.

Section Two:

Managed Applications and Account Correlation

IDENTITYIQ IMPLEMENTATION AND ADMINISTRATION: ESSENTIALS

SailPoint IdentityIQ Version 8.1

With Rapid Setup

www.sailpoint.com

Table of Contents

Exercise #1: Define Business Applications

Objective

In this exercise, you will onboard account and entitlement data from multiple business applications.

Overview

In this exercise, you'll experience how different teams can share responsibility for configuring IdentityIQ. First, you'll log in as a Technical Implementer (Carl Foster) and define two JDBC applications. Once these applications are defined, additional configuration can be completed by members of the Business Analysts workgroup – they have access to the Rapid Setup pages. You'll log in as a member of the Business Analysts workgroup, Jim Lee, to specify the logic for correlating accounts and classifying the applications' account and entitlement data.

For this exercise, you will onboard four applications:

- Time Tracking
- Chat
- Finance
- Bug Tracking

Define Time Tracking Application

The Time Tracking application will use the JDBC connector to connect to the Time Tracking MySQL database, where account and entitlement data is stored in one table.

1. Log into IdentityIQ as **Carl.Foster/xyzzy**
2. Navigate to **Application** > **Application Definition**
3. Click **Add New Application**

4. Create an application definition based on the following table.

Application	
Name	**Time Tracking**
Owner	**Admins**
Application Type (Connector)	**JDBC**
Connector Attributes Configuration > Settings > Object Type: account > Settings	
JDBC Connection Settings	
Connection User	**root**
Connection Password	**root**
Database URL	**jdbc:mysql://localhost/timetracking?serverTimezone=UTC**
JDBC Driver	**com.mysql.jdbc.Driver**
Query Settings	
SQL Statement	**select * from users;**
getObjectSQL	**select * from users where id = '$(identity)';**

5. Click **Test Connection** to verify.

6. Define the Account Schema

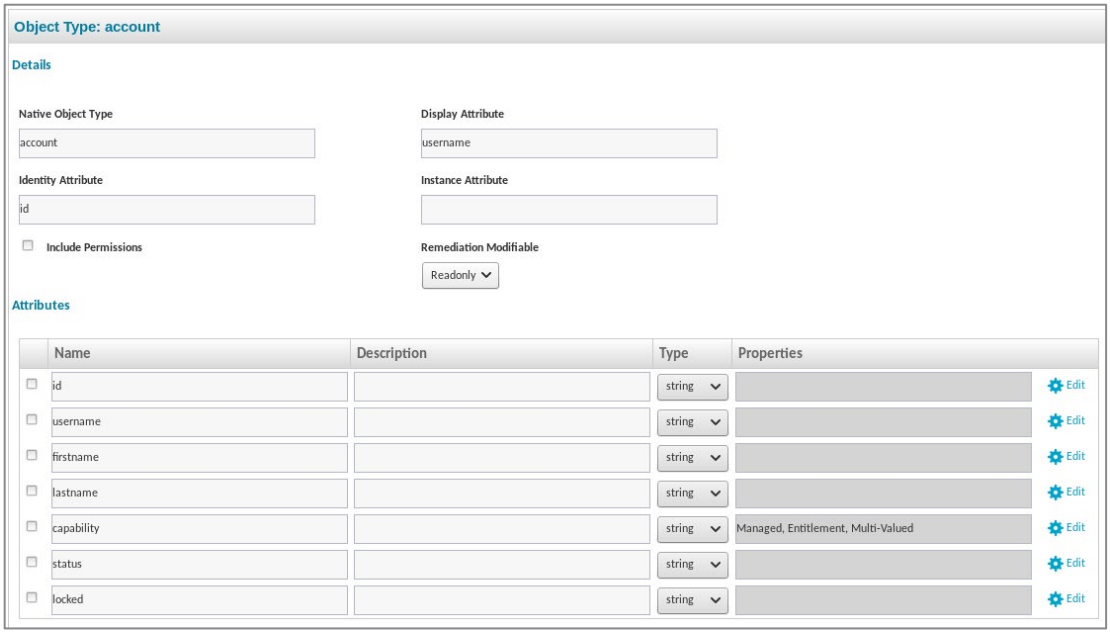
   a. Navigate to **Configuration** > **Schema**

   b. Click **Discover Schema Attributes**

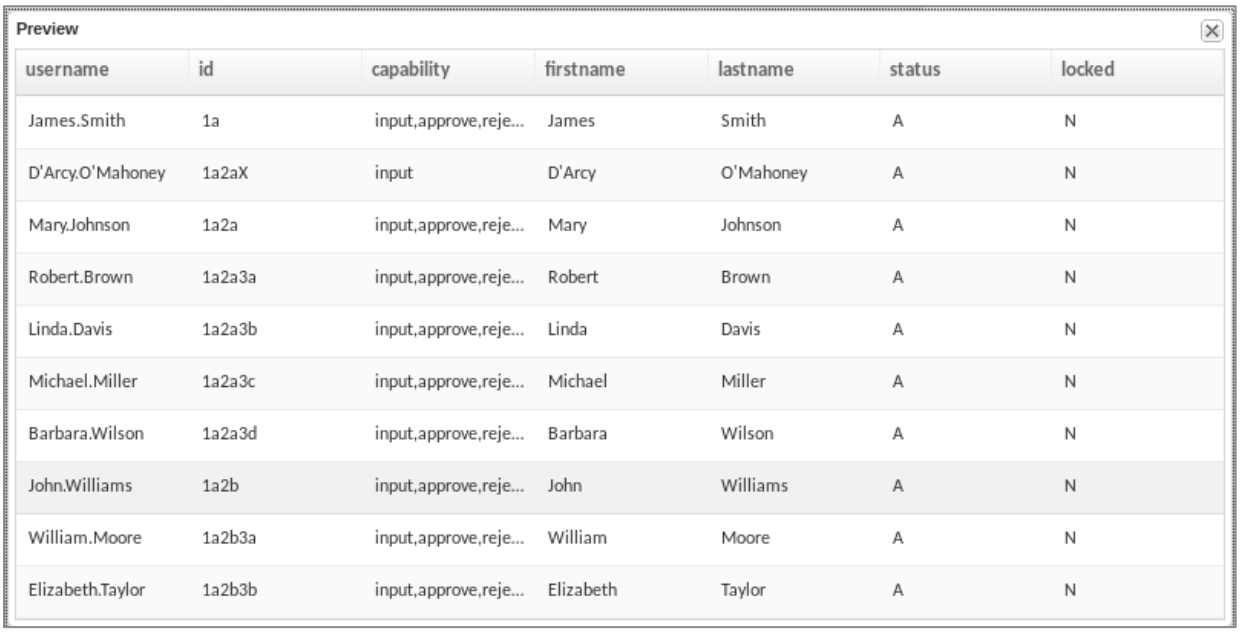
   c. Set **Identity Attribute** to **id**

   d. Set **Display Attribute** to **username**

   e. In **Attributes**, set **capability** to **Managed, Entitlement, Multi-Valued**



7. **Preview** account details.



Preview

username	id	capability	firstname	lastname	status	locked
James.Smith	1a	input,approve,reje...	James	Smith	A	N
D'Arcy.O'Mahoney	1a2aX	input	D'Arcy	O'Mahoney	A	N
Mary.Johnson	1a2a	input,approve,reje...	Mary	Johnson	A	N
Robert.Brown	1a2a3a	input,approve,reje...	Robert	Brown	A	N
Linda.Davis	1a2a3b	input,approve,reje...	Linda	Davis	A	N
Michael.Miller	1a2a3c	input,approve,reje...	Michael	Miller	A	N
Barbara.Wilson	1a2a3d	input,approve,reje...	Barbara	Wilson	A	N
John.Williams	1a2b	input,approve,reje...	John	Williams	A	N
William.Moore	1a2b3a	input,approve,reje...	William	Moore	A	N
Elizabeth.Taylor	1a2b3b	input,approve,reje...	Elizabeth	Taylor	A	N

8. **Close** the preview and **save** the application definition.

Define Chat Application

The Chat application will use the JDBC connector to connect to the Chat MySQL database, which maintains application permissions in account groups. An account group is an indirect method of defining access to a system. A user will have an account on a system with entitlement to a defined set of account groups. These account groups indirectly define the user's access to the application.

The Chat MySQL database consists of two tables:

- Users – Contains user account information for the Chat application, including user's account groups
- Groups – Contains information about the groups themselves

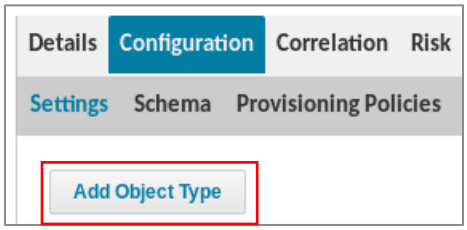
When onboarding the Chat application, you will need to define two schemas, one for the accounts that you're aggregating and another for the account groups that you're aggregating.

1. Create an application definition based on the following table

Application Applications > Application Definition > Add New Application	
Name	**Chat**
Owner	**Admins**
Application Type (Connector)	**JDBC**
Connector Attributes Configuration > Settings > Object Type: account > Settings	
JDBC Connection Settings	
Connection User	**root**
Connection Password	**root**
Database URL	**jdbc:mysql://localhost/chat?serverTimezone=UTC**
JDBC Driver	**com.mysql.jdbc.Driver**
Query Settings	
SQL Statement	**select * from users;**
getObjectSQL	**select * from users where login = '$(identity)';**

2. Click **Test Connection** to verify.

3. Remaining on **Configuration** > **Settings** page, scroll to top and click **Add Object Type**



4. Name Object Type: **group** and click **OK**

5. Scroll down to **Object Type: group** and set the following:

Connector Attributes Configuration > Settings > Object Type: group > Settings	
JDBC Connection Settings	
Connection User	**root**
Connection Password	**root**
Database URL	**jdbc:mysql://localhost/chat?serverTimezone=UTC**
JDBC Driver	**com.mysql.jdbc.Driver**
Query Settings	
SQL Statement	**select * from groups;**
getObjectSQL	**select * from groups where name = '$(identity)';**

6. Define account schema.

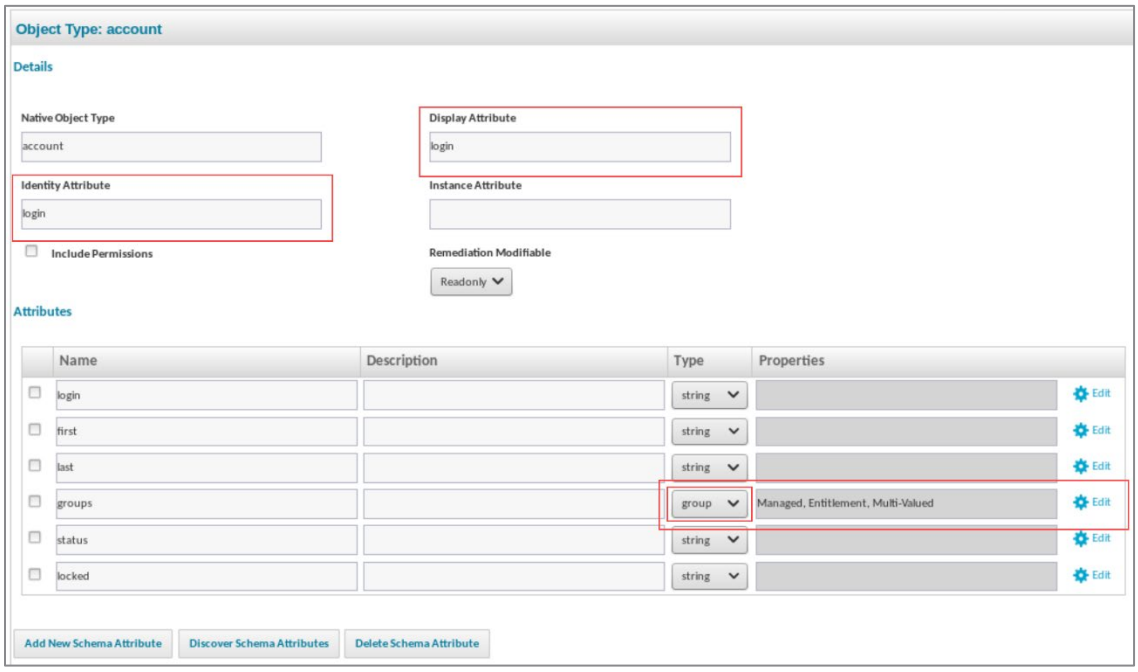
   a. Navigate to **Configuration** > **Schema**

b. For **Object Type: account**, click **Discover Schema Attributes**

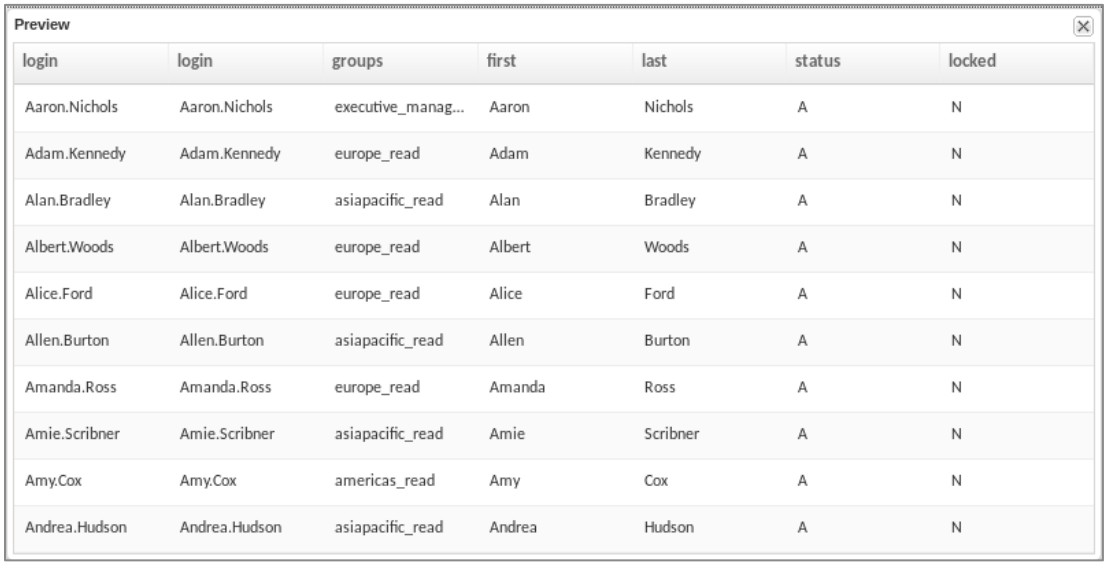
c. Set both **Identity Attribute** and **Display Attribute** to **login**

d. In **Attributes**, set **groups** to **Managed, Entitlement, Multi-Valued**

e. For the **groups** attribute, change the Type to **group**



f. **Preview** the accounts.



Preview

login	login	groups	first	last	status	locked
Aaron.Nichols	Aaron.Nichols	executive_manag...	Aaron	Nichols	A	N
Adam.Kennedy	Adam.Kennedy	europe_read	Adam	Kennedy	A	N
Alan.Bradley	Alan.Bradley	asiapacific_read	Alan	Bradley	A	N
Albert.Woods	Albert.Woods	europe_read	Albert	Woods	A	N
Alice.Ford	Alice.Ford	europe_read	Alice	Ford	A	N
Allen.Burton	Allen.Burton	asiapacific_read	Allen	Burton	A	N
Amanda.Ross	Amanda.Ross	europe_read	Amanda	Ross	A	N
Amie.Scribner	Amie.Scribner	asiapacific_read	Amie	Scribner	A	N
Amy.Cox	Amy.Cox	americas_read	Amy	Cox	A	N
Andrea.Hudson	Andrea.Hudson	asiapacific_read	Andrea	Hudson	A	N

7. Define group schema.

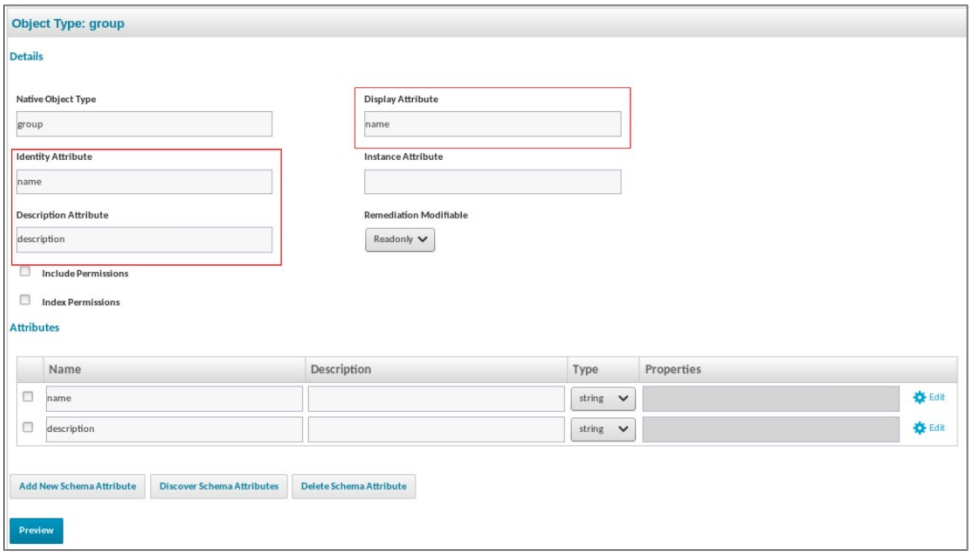
   a. Remaining on **Configuration** > **Schema** page, scroll down to **Object Type: group**

   b. Click **Discover Schema Attributes**

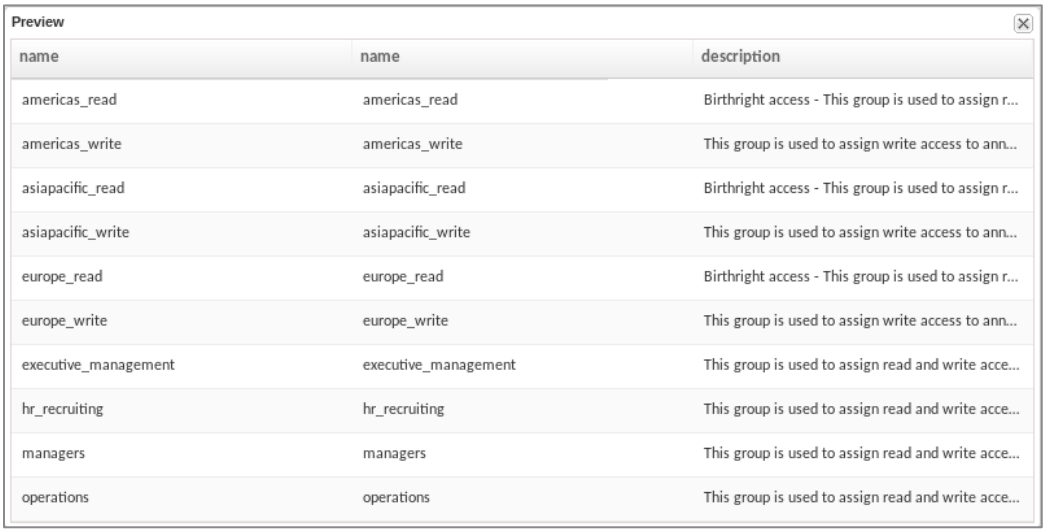
   c. Set both **Identity Attribute** and **Display Attribute** to **name**

   Note: Be mindful to edit the correct object type. After modifying attribute properties, the user interface returns the focus to the top of the screen, where you may accidentally modify the account object type rather than the group object type.

   d. For **Description Attribute**, type **description**



   e. **Preview** the groups.



8. **Close** the preview and **save** application.

Import Additional Business Applications

This time, rather than manually configuring application definitions and their associated aggregation tasks, you will import the application definition, correlation configuration, and aggregation task objects. Importing objects is commonly done to move them from one environment to another.

Let's suppose that your colleague created the Finance application definition and the related aggregation task in their sandbox environment. Rather than duplicating the work, they provided the XML representation of the objects for you to load into your environment for further configuration.

If you're interested, take a look at the XML file using the editor provided in the VM. Note that the XML file is one large XML file containing many individual SailPoint objects.

1. Navigate to **Gear** > **Global Settings** > **Import from File** and **Import** the following file: **/home/spadmin/ImplementerTraining/config/Business_Apps_and_Agg_Tasks.xml**

   This file includes:

   Application Definitions

   - Finance: This is a Delimited File application, with separate CSVs and schemas for accounts and groups
   - Bug Tracking: This is a JDBC application with a similar structure to the Time Tracking application

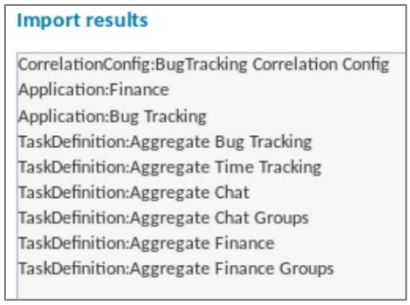
   Correlation Configuration

   - Bug Tracking

   Task Definitions

   - Aggregate Bug Tracking
   - Aggregate Time Tracking
   - Aggregate Chat
   - Aggregate Chat Groups
   - Aggregate Finance
   - Aggregate Finance Groups

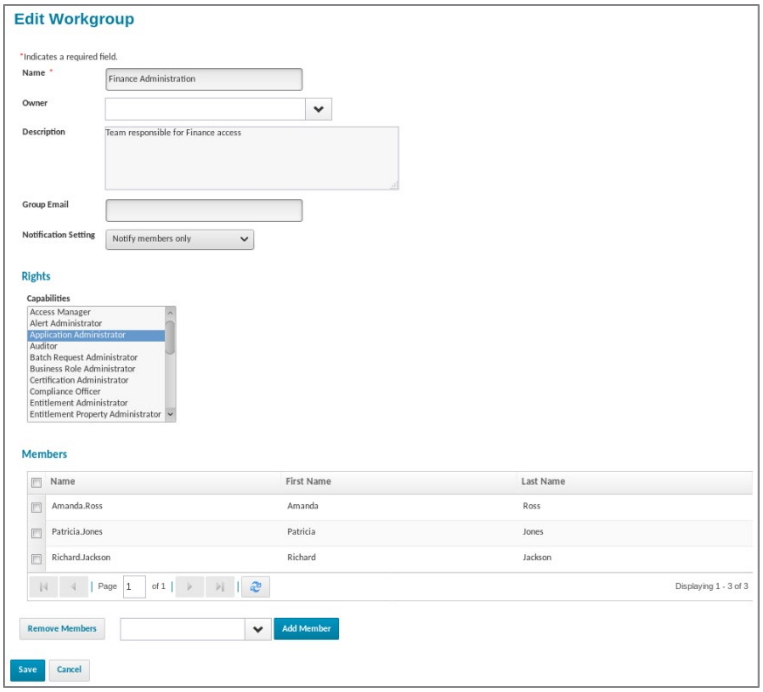
2. Once the file import completes, compare your results to the list below and confirm that everything loaded.



Update Owner for Finance Application

Currently, the owner of the Finance application is the spadmin identity. Best practice is to set workgroups as owners of IdentityIQ objects.

1. Create a workgroup with responsibility for the Finance system.
    a. Navigate to **Setup** > **Groups** > **Workgroups**
    b. Create a workgroup:
        i. Name: **Finance Administration**
        ii. Owner: **Richard.Jackson**
        iii. Description: **Team responsible for Finance access**
        iv. Notification Setting: **Notify members only**
        v. Capabilities: **Application Administrator**
        vi. Members:
            (1) **Amanda Ross**
            (2) **Patricia Jones**
            (3) **Richard Jackson**



c. **Save** workgroup.

2. Update the owner for the Finance application.

   a. Navigate to **Applications** > **Application Definition** > **Finance**

   b. Change Owner to **Finance Administration**

   c. **Save** application.

Configure Account Attribute Mappings

Accounts from various applications may share common attributes that you want to reflect in IdentityIQ and use in access management processes. These may have similar or very different native representations on the original systems that you need to "normalize" in IdentityIQ to support common behaviors.

A common use case is marking appropriate accounts as privileged accounts. Though the definition of a privileged account could vary widely across systems, you can map them to a consistent representation in IdentityIQ.

You will define and configure an extended account attribute to record whether the account is privileged. Then you will define, per application, how that attribute gets populated.

1. Navigate to **Gear** > **Global Settings > Account Mappings**

2. Click **Add New Attribute** and add a "privileged" account attribute

   a. Attribute Name: **privileged**

b. Display Name: **Privileged Account**

c. Attribute Type: **Boolean**

3. Under **Source Mappings**, click **Add Source**

a. Select **Application Attribute**

b. Application: **Finance**

c. Attribute: **privileged**

d. Click **Add**

4. Under **Source Mappings**, click **Add Source**

a. Select **Application Rule**

b. Application: **Time Tracking**

c. Click the ellipses  to access the **Rule Editor** and create the following rule:

i. Rule Name: **TRNG-LinkAttribute-ContainsAdmin**

ii. In the Rule Editor, type the following BeanShell script:

```
return link.getNativeIdentity().toLowerCase().contains("admin");
```

This rule identifies any account with "admin" in its account name.

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

d. Rule: select the rule you just created **TRNG-LinkAttribute-ContainsAdmin**

e. Click **Add**

5. **Save** your changes to the privileged account attribute.

Configure User Interface (UI) to Display Account Attribute

The next goal is to configure the UI to leverage the newly created account attribute. In this section, we will configure the UI to display an icon indicating at a glance the privileged classification of an account.

1. With the file browser, navigate to and open file (with gedit):
/home/spadmin/ImplementerTraining/config/UIConfig-AccountIcon.xml

2. What is the value of the ImportAction? _____

3. To which configuration object are we adding? _____

   Notice that we are associating an icon to display in the UI for our account attribute.

4. Why is the **accountIconConfig** merged into the **UIConfig** rather than copied?

   _____

   Note: Recall in the previous exercise section, when you loaded the remaining Identity Mappings, you also used this merge technique to merge the new definitions into the existing Identity ObjectConfig object.

5. Close the file.

6. In IdentityIQ, navigate to **Gear > Global Settings > Import from File**

7. Import the following file:
   /home/spadmin/ImplementerTraining/config/ UIConfig-AccountIcon.xml

Configure Time Tracking Application with Rapid Setup

Now that these applications are defined, members of the Business Analysts workgroup can configure additional settings for these applications using the *Rapid Setup* pages. Splitting these responsibilities supports efficient implementation processes.

1. Log out of IdentityIQ and log back in as **Jim.Lee/xyzzy**

   Note: Since Jim is a member of the **Business Analysts** workgroup, he has access to the **Applications** > **Rapid Setup** page.

   a. Expand Jim's main menu items.

      Notice that he doesn't have access to all of the pages that were available to Carl Foster. Carl can access all pages within IdentityIQ because Carl has the System Administrator capability.

2. Navigate to **Applications** > **Rapid Setup**

3. Select **Time Tracking** and click **Next**

   Note: If you do not see Time Tracking in the list of applications, click **Load More** applications. You can also begin typing the name to bring it into focus for selection.

4. On the **Aggregation** page, add identity correlation logic.

   a. Under Identity Correlation, click **Add Filter**

      i. Application Attribute: **id**

ii. Operation: **Equals**

iii. Identity Attribute: **Employee ID**

5. Click **Save**

Configure Chat Application with Rapid Setup

1. On the top left, click the **back arrow (<)** next to Rapid Setup to select another application.
2. Select Application **Chat** and click **Next**
3. On the **Aggregation** page, add identity correlation logic.

Application Attribute	Operation	Identity Attribute
Login	Equals	Display Name

4. Click **Save**

Configure Finance Application with Rapid Setup

1. On the top left, click the **back arrow (<)** next to Rapid Setup to select another application.
2. Select the application **Finance** and click **Next**
3. Navigate to the **Aggregation** page.
4. Add **Identity Correlation** logic.

Application Attribute	Operation	Identity Attribute
User Name	Equals	Display Name

5. Add **Disable Account** logic.

Application Attribute	Operation	Value
Status	Equals	I

6. Add **Lock Account** logic.

Application Attribute	Operation	Value
Locked	Equals	Y

7. Click **Save**

Exercise #2: Explore Aggregation and Refresh Tasks

Objective

In this exercise, you will work with task options. You will learn how to:

- Run a set of tasks sequentially
- Schedule tasks
- Monitor tasks
- Constrain the identities upon which a refresh task runs
- Run a report to view identity details

Overview

Tasks are the primary actors of IdentityIQ; they act upon the objects in the database and are critical to the functioning of IdentityIQ. This exercise provides additional practice with controlling, manipulating, and monitoring tasks.

Define Sequential Task

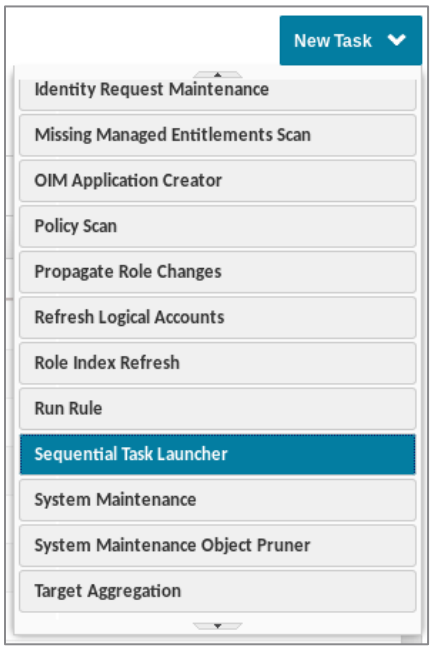
IdentityIQ can run multiple tasks in a connected sequence using a **Sequential Task Launcher**. For example, during this training when you needed to refresh data from the authoritative sources, you ran three separate tasks: **Aggregate Employees**, **Aggregate Contractors**, and **Refresh Identity Cube**. You did this in three steps.

With the Sequential Task Launcher task, you can group, order, and run these three tasks as one - with the order and completion controlled by the Sequential Task Launcher.

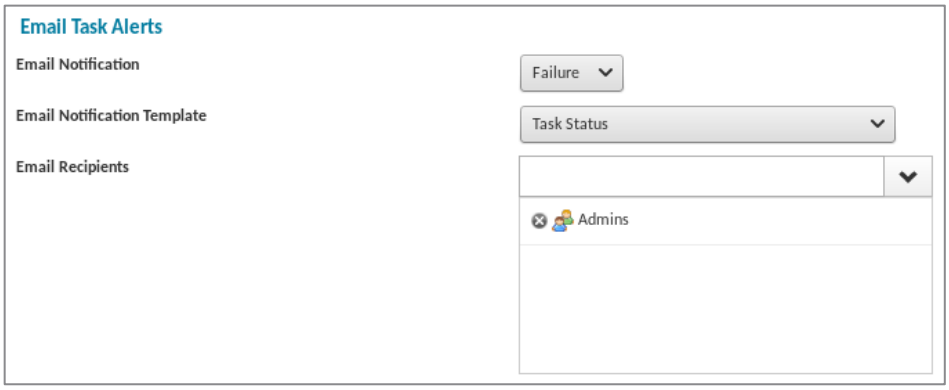
You will now create a task that will invoke the aggregation tasks for the non-authoritative applications, and then end with the Refresh Identity Cube task. You'll also enable notifications, so the **Admins** workgroup will receive an email if this task execution fails.

1. Log into IdentityIQ as **Carl.Foster/xyzzy**
2. Navigate to **Setup** > **Tasks**

3. In the top right corner, click **New Task**.
4. Scroll down the list and select **Sequential Task Launcher**



5. Configure the sequential task launcher task.
   a. Set **Standard Properties.**
      i. Name: **Aggregate Non-Authoritative Applications**
      ii. Previous Result Action: **Rename Old**
   b. Set **Email Task Alerts**
      i. Email Notification: **Failure**
      ii. Email Notification Template: **Task Status**
      iii. Email Recipients: **Admins**



c. Under **Aggregate Task Options**, add tasks to the list for sequential execution.

Note: Order matters. The tasks will be executed in the order selected.

d. For **Enter the list of tasks you would like to run**, click the dropdown menu and select:

i. **Aggregate LDAP**

ii. **Aggregate LDAP Groups**

iii. **Aggregate Time Tracking**

iv. **Aggregate Chat**

v. **Aggregate Chat Groups**

vi. **Aggregate Finance**

vii. **Aggregate Finance Groups**

viii. **Aggregate Bug Tracking**

ix. **Refresh Identity Cube**

Note: Tasks may be on the second page of options; type in the first few letters to filter the list or use the arrows that appear in the dropdown list to navigate between pages.

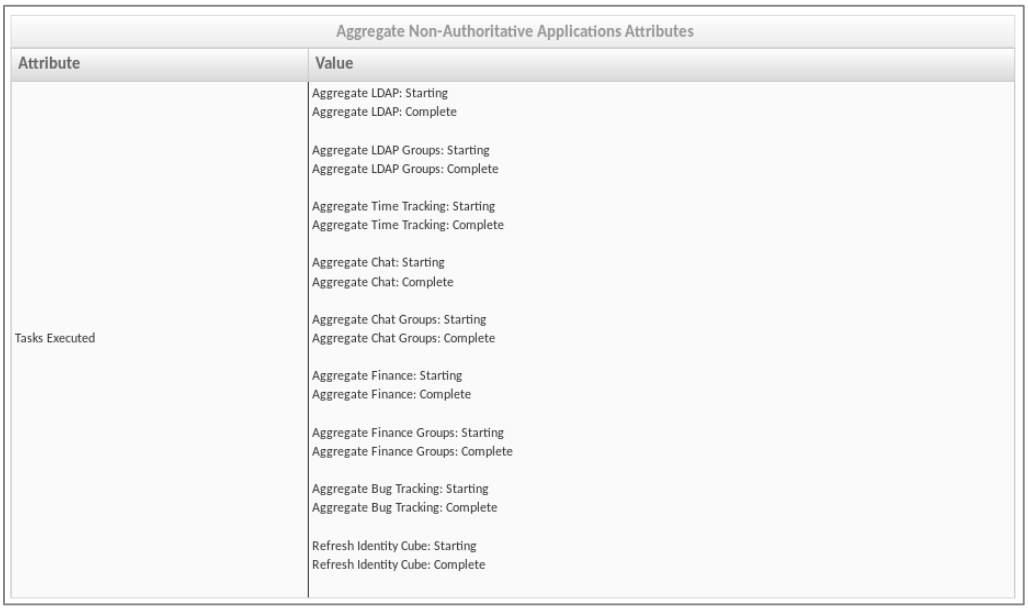
e. Click **Save and Execute**.

A dialog box will inform you that the task is being run in the background.

6. View **Task Results** for **Aggregate Non-Authoritative Applications**. Notice the Progress.

Because this task runs multiple tasks, it may take a few minutes for the task to complete. While you are waiting, scroll to the end of the task results list and view the tasks that are currently pending.

7. Once the **Aggregate Non-Authoritative Applications** task completes, your results should be similar to those shown below - informing you that each task started and completed.



Aggregate Non-Authoritative Applications Attributes

Attribute	Value
Tasks Executed	Aggregate LDAP: Starting Aggregate LDAP: Complete Aggregate LDAP Groups: Starting Aggregate LDAP Groups: Complete Aggregate Time Tracking: Starting Aggregate Time Tracking: Complete Aggregate Chat: Starting Aggregate Chat: Complete Aggregate Chat Groups: Starting Aggregate Chat Groups: Complete Aggregate Finance: Starting Aggregate Finance: Complete Aggregate Finance Groups: Starting Aggregate Finance Groups: Complete Aggregate Bug Tracking: Starting Aggregate Bug Tracking: Complete Refresh Identity Cube: Starting Refresh Identity Cube: Complete

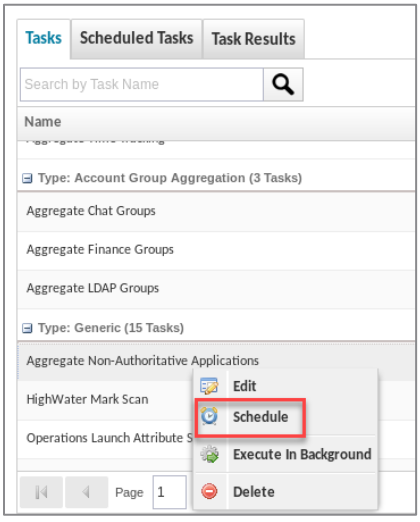
Schedule Tasks

You have successfully performed individual tasks and created a sequential task launcher that will perform individual tasks in the required order. Now, you'll see how to schedule tasks to be repeated at regular intervals, such as by the hour, week, or month.

1. Schedule the **Aggregate Non-Authoritative Applications** task to be performed weekly.

   a. Navigate back to the **Tasks** tab and search for **Aggregate Non-Authoritative Applications**.

   b. Right-click and select **Schedule**



c. Define the new schedule.

i. Name: **Weekly Non-Authoritative Application Aggregation and Refresh**

ii. First execution: notice this is set for 5 minutes in the future.

iii. Execution Frequency: **Weekly**

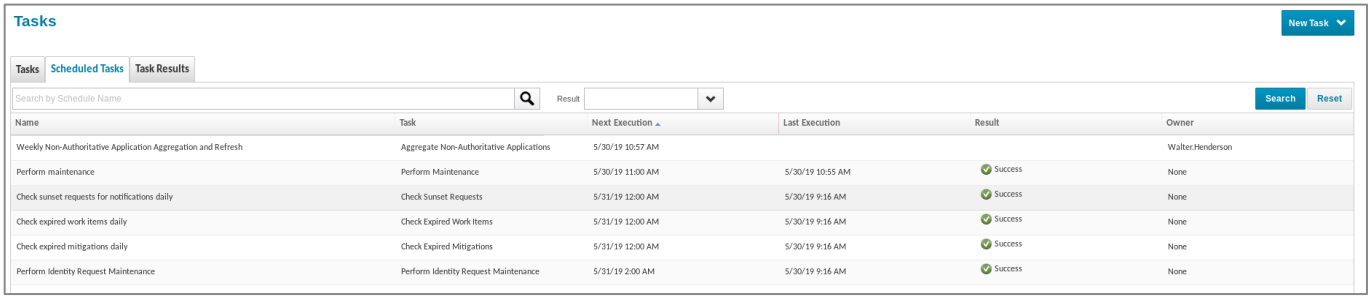
2. Click **Schedule**

3. View the scheduled task.

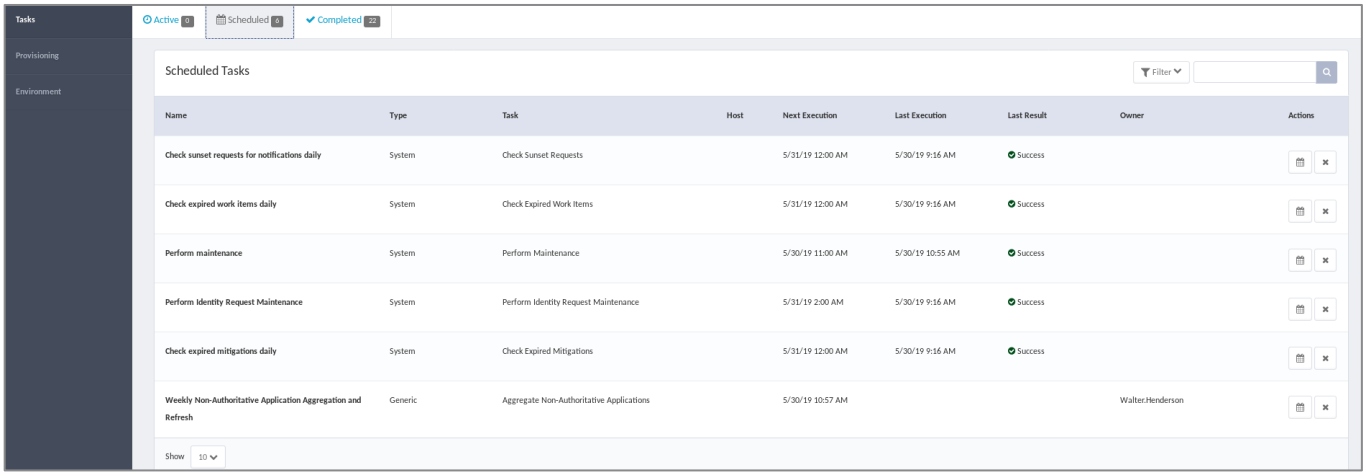
You can view this scheduled event in two places in the interface.

a. Navigate to the **Scheduled Tasks** tab.

You should see the next scheduled date and time of your task.



b. Navigate to **Gear** > **Administrator Console** > **Tasks** > **Scheduled**



Monitor Tasks

You can see details about active, scheduled, and completed tasks in the Administrator Console.

1. Explore the **Administrator Console** > **Tasks** tab

2. Click the **Active** tab

   On this page, you can see all tasks that are currently running

3. Click the **Scheduled** tab

   What are the two options presented in the **Actions** column?

   _____

4. Click the **Completed** tab

   On this page, you can see the last runtime, average runtime, and difference from average for the completed tasks.

   All of these pages allow you to limit the results through a search textbox or through the Filter.

   a. Click **Filter** and display tasks with Type: **AccountAggregation**

Investigate the Default Task - Refresh Identity Cube

1. Navigate to **Setup** > **Tasks**
2. Click **Refresh Identity Cube** task to view its configured options.

   As a reminder, you previously modified this task.

3. Review the enabled options.

   a. From the following list, mark the options that are not checked:

   - ☐ Refresh identity attributes
   - ☐ Refresh manager status
   - ☐ Refresh assigned, detected roles and promote additional entitlements
   - ☐ Refresh the identity risk scorecards
   - ☐ Check active policies
   - ☐ Process events

   b. Scroll up to the beginning of the **Refresh Identity Cube Options** section. List the two methods for constraining the identities that will be refreshed (complete the phrases).

      i. Optional _____ string

      ii. Optional list of _____ or _____

c. Click **Cancel** to close without changing anything.

4. Navigate to **Setup** > **Tasks** > **Task Results** .
5. View the results for the last run of the **Refresh Identity Cube** task.
   a. How many identities were examined? _____
   b. How many identities are there in your IdentityIQ instance? _____

      Hint: Navigate to **Identities** > **Identity Warehouse**

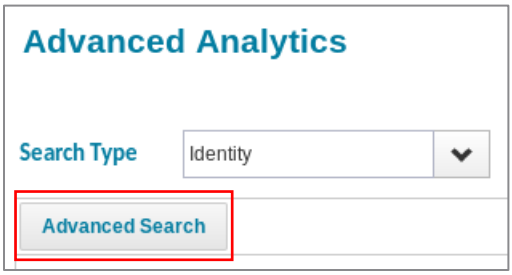
   c. Notice that the default Refresh task ran against all identities in the environment.

Constrain the Refresh Identity Task

Earlier, you performed a refresh on all identities within the system. Now, you will perform a refresh on only identities who have accounts on the Finance application. You could configure either a filter or a list to achieve this goal.

In this exercise, you will use Advanced Analytics to provide the filter syntax. With the Advanced Identity Search feature, you can write a complex set of criteria. Once you've defined your search parameters, you can see the filter code produced using the view/edit filter source link. From here you can make minor changes to the code, or you can copy the filter code in order to paste it into another area in IdentityIQ where the filter string input is necessary. This is helpful because you can use Advanced Analytics to build your filter using the GUI, and you don't have to understand the filter syntax to use it.

1. Navigate to **Intelligence** > **Advanced Analytics**.
2. Make sure Search Type is **Identity**
3. Click **Advanced Search**



4. Select the fields to display in the output
   a. Under **Choose Fields to Display**, select **First Name** and **Last Name**

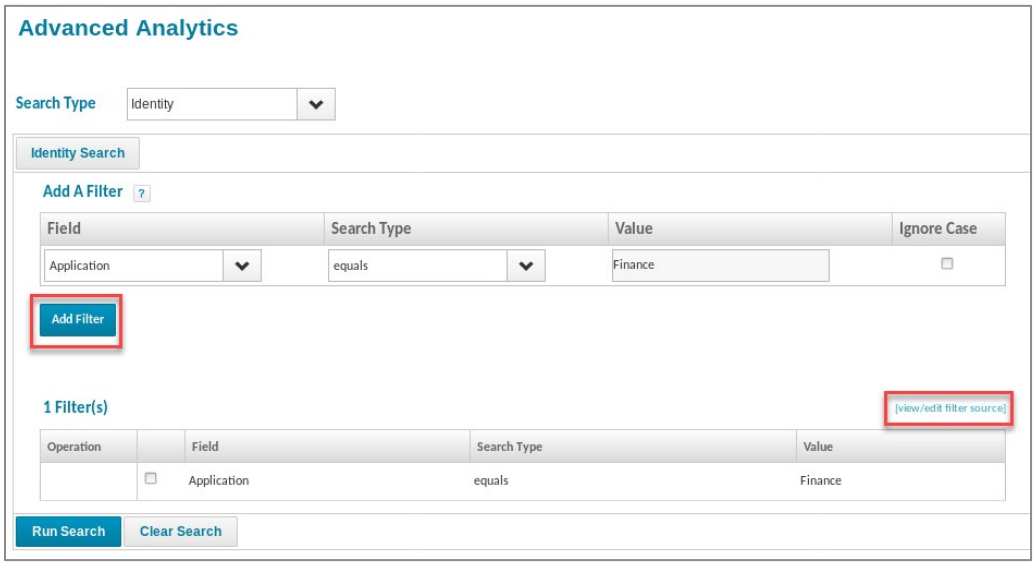
5. Specify a query filter.

   a. Build this filter logic.

Field	Search Type	Value
Application	equals	Finance

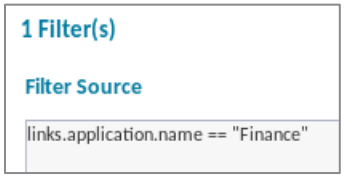
   b. Click **Add Filter**

   c. Click **[view/edit filter source]**



   d. Under **Filter Source**, copy (Ctrl-C) the generated filter string.

   This is the filter syntax that you will paste into the filter constraint for the Refresh Identity Cube Task.



   Notice the term **links**. In IdentityIQ, **link** is synonymous with *account*. The term *Link* is typically used internally to the product, and the term *Account* is typically used in the user interface. See the Appendix for a list of common terms and their synonyms.

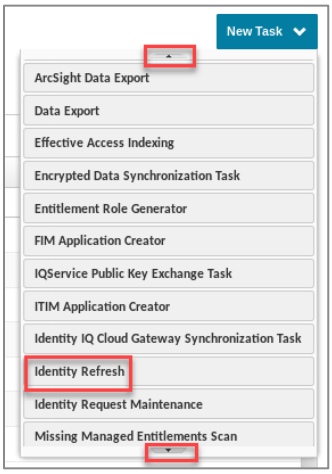
6. Click **Run Search**.

   a. How many identities were returned? _____

7. Navigate to **Setup** > **Tasks**

8. Click **New Task** and click the arrow at the bottom to scroll.
9. Choose **Identity Refresh**.

   This will create a new, blank Identity Refresh task.



10. Define the task.
    a. Name: **Refresh Finance Identities**
    b. Previous Result Action: **Rename Old**
    c. Optional filter string to constrain the identities refreshed: **links.application.name == "Finance"**

       Hint: Paste the copied filter string (Ctrl-V)

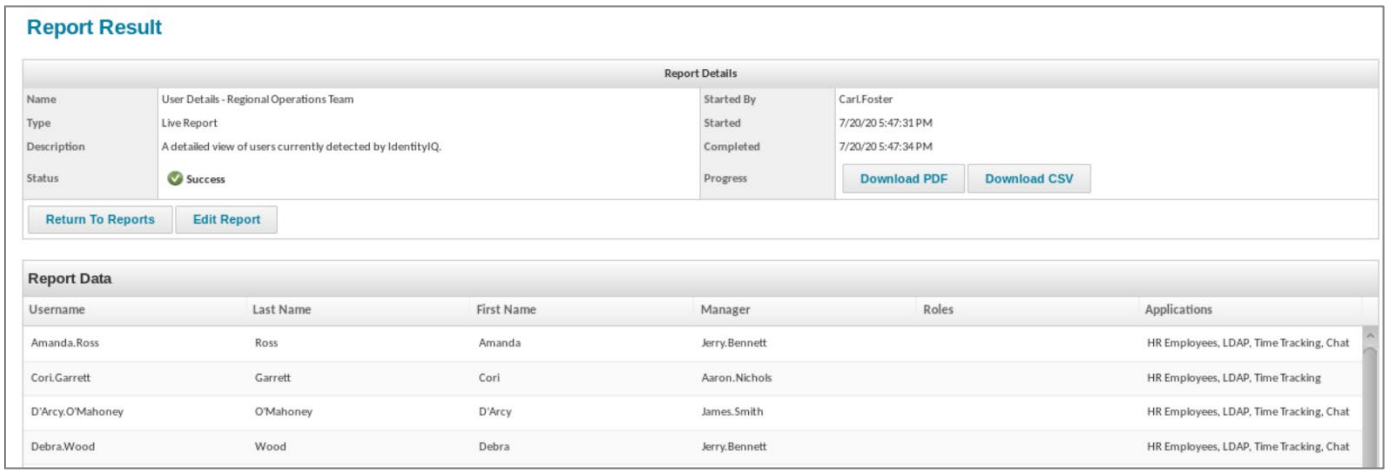
    d. Enable these Identity Cube Refresh task options:
       - Refresh identity attributes
       - Refresh manager status
       - Refresh assigned, detected roles and promote additional entitlements
    e. Scroll to the bottom and click **Save and Execute**
11. Navigate to **Task Results** tab and confirm that the number of identities examined matches the number of identities from the search.

View Identity Details in a Report

Groups and Populations are used for filtering which Identities will be acted on in a number of places in the product. One of those is in reporting. Here you will run a report using one of the department Groups created previously to narrow down the results.

1. Navigate to **Intelligence** > **Reports** and select the **Reports** tab
2. Search for and open the **User Details Report** to use it as a template.
3. Specify the following configuration:
   a. On the **Standard Properties** page:
      i. Report Name: **User Details – Regional Operations Team**
   b. On the **Additional Identity Properties** page:
      i. Groups: **Regional Operations**

4. Click **Save and Execute**
5. Wait for the report to finish and then select **View Report Results** to see the report results.



Exercise #3: Fix Uncorrelated Accounts, Data Maintenance

Objective

In this exercise, you will search for uncorrelated accounts and then manually correlate an account to the appropriate authoritative identity cube. Then you will update the entitlement catalog to ensure your access data is accurate and informative to your business users.

Overview

When correlation fails, IdentityIQ creates non-authoritative (uncorrelated) identity cubes to house the accounts that did not correlate. There are three solutions to this problem:

- Check the accounts being read. Are they current? Is the data good? Sometimes the application itself needs to clean up accounts.
- Determine what went wrong with the correlation, adjust your correlation logic or correlation rule and re-aggregate the accounts.
- Manually correlate the accounts using the UI. This involves moving the uncorrelated account to the proper Identity Cube.

Once the data is cleaned up, empty, non-authoritative identity cubes remain in the system. Empty (no associated accounts), non-authoritative identity cubes are removed by running the Prune Identity Cubes task.

In this exercise, you will check if you have any orphan accounts in the system (those accounts that cannot be linked to authoritative identity cubes) and then you'll use manual correlation to deal with these accounts appropriately.

Additionally, as part of your data maintenance activities you will update entitlement information to ensure your users see accurate and helpful information about the entitlements managed in IdentityIQ.

Run Report to Identify Uncorrelated Accounts

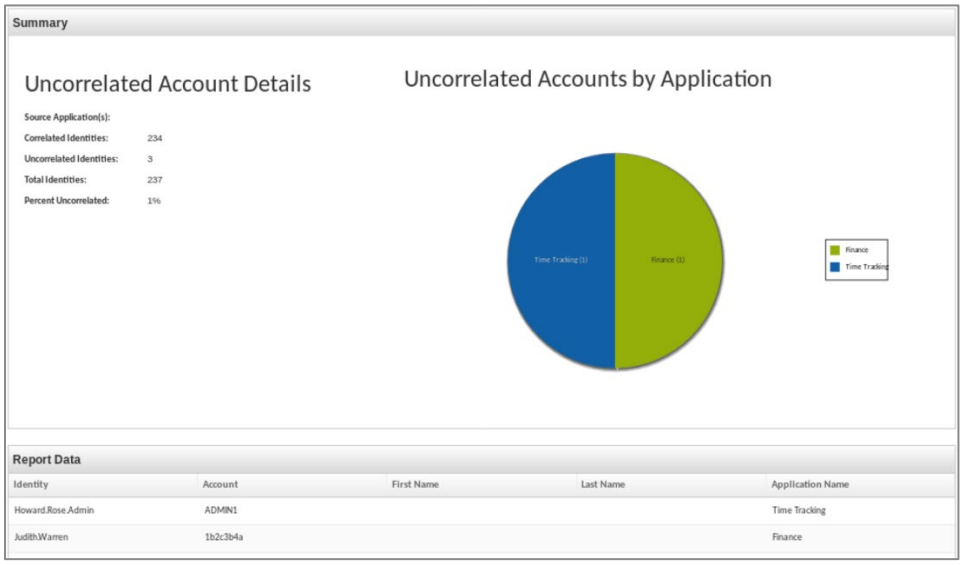
1. Log into IdentityIQ as **Lauren.Harrison/xyzzy**

   Since Lauren is part of the **Business Analysts** workgroup, she has the Identity Correlation Administrator capability; therefore, she is able to run Reports.

2. Navigate to **Intelligence** > **Reports** > **Reports**
3. Search for **Uncorrelated Accounts Report**
4. Right click and **Execute**

5. Click **OK** on the pop-up.

6. Navigate to the **Report Results** tab and view the report data.



7. Notice there are 2 uncorrelated account in your system: the **Howard.Rose.Admin** account on the Time Tracking application and **Judith.Warren** account on the Finance application.

   Note: The Report Summary states Uncorrelated Identities: 3. The other identity is the spadmin identity, which is the default System Administrator identity loaded with IdentityIQ.

Investigate Uncorrelated Accounts

1. Navigate to **Identities** > **Identity Warehouse**

2. Search for **Howard**

3. Investigate the identity cube for **Howard.Rose.Admin**.

   a. Open this cube and view **Attributes**

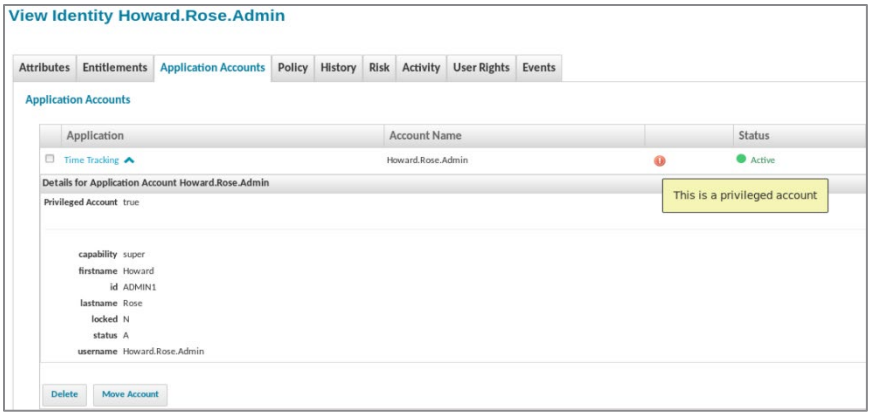
      Notice that the only populated attribute is the User Name. This is a good clue that you're looking at a non-authoritative identity cube created to temporarily house an account.

   b. Navigate to **Application Accounts**

      Notice that the Time Tracking account name matches the User Name on the Attributes tab

   c. Expand **Time Tracking**

      Notice this account was classified as a Privileged account, indicated by the red icon



Earlier, when you configured the Time Tracking application, you specified that its accounts will correlate to their account owners, identities within IdentityIQ, by matching the identity attribute Employee ID to the account attribute id. This logic worked for all Time Tracking accounts, except for this account. As you can see in the screenshot above, this account's id doesn't have the same format as normal "user" accounts. This privileged account has the extra string 'admin' in the account name, so it failed correlation.

d. Click **Cancel** to return to the **Identity Warehouse**

4. Search for **Howard** again.

5. Are there any other identity cubes for a user named Howard Rose? During your investigation, you determine that the **Howard.Rose.Admin** account belongs to **Howard.Rose**

6. Clear your search and search the **Identity Warehouse** for **Judith**

7. Open the identity cube for **Judith.Warren**.

   a. View **Attributes**

      Again, only the _____ attribute is populated.

   b. Click cancel to return to the **Identity Warehouse**

8. Search for **Judith** again.

   a. Do you see the identity that this account belongs to? _____

9. Clear your search and search for the last name **Warren**

10. During your investigation, you determine the **Judith.Warren** Finance account belongs to **Judy.Warren**

11. Why did the **Judith.Warren** Finance account not correlate? _____

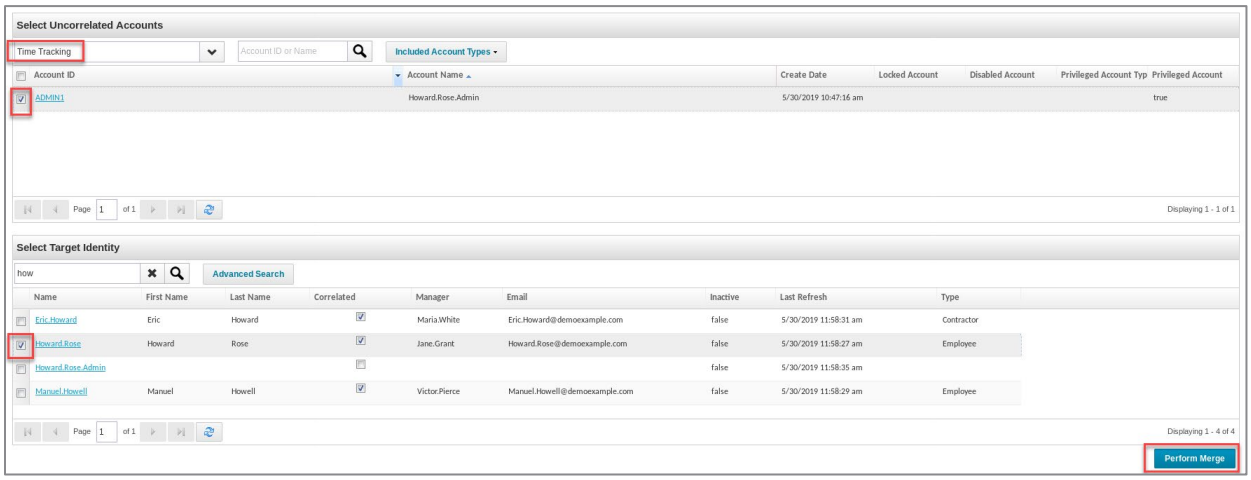
Resolve Uncorrelated Accounts

1. Navigate to **Identities** > **Identity Correlation**
2. Manually correlate accounts for the Time Tracking application.
   a. In the **Select Uncorrelated Accounts** section, select **Time Tracking**
      i. In the list, check the box for **ADMIN1**
   b. Scroll down to **Select Target Identity**
      i. Search for **Howard** to find the identity cube: **Howard.Rose**

      Notice that his cube is marked as **Correlated**, which also means that it is an authoritative cube – one that has been created through the process of aggregating from an authoritative application (for example, HR).

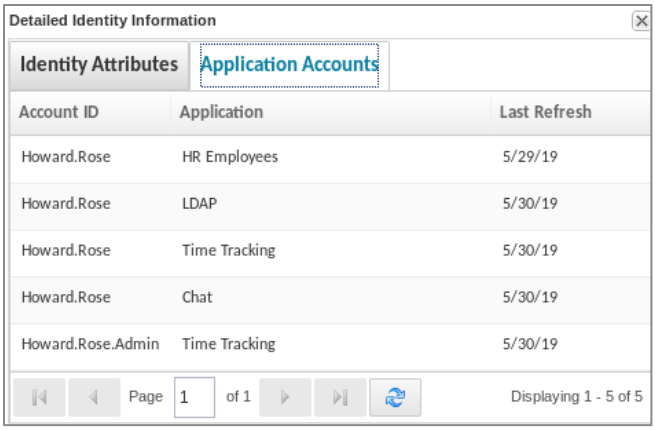
      ii. Check the box next to **Howard.Rose**
   c. Click **Perform Merge**

      The button is on the bottom right of the screen. This will move the uncorrelated account from the correct owner's identity cube.



   d. After the merge is complete, click **Howard.Rose**
      i. Confirm that the **Howard.Rose.Admin** account was moved properly.

      This privileged Time Tracking account is now on the proper cube.



ii. Close the Detailed Identity Information window.

3. Manually correlate accounts for the Finance application.

   a. Scroll back up and select the **Finance** application.

   b. In the list, check the box for **1b2c3b4a**

   c. Scroll down to **Select Target Identity** and search for **Judy** to find the identity cube: **Judy.Warren**

   d. Check the box next to **Judy.Warren**

   e. Click **Perform Merge** on the bottom right of the screen.

      This will move the uncorrelated account to the correct owner's identity cube.

Prune Identity Cubes

When IdentityIQ reads an account from a connected application, it will try to correlate it to an existing identity cube and if that fails, create a new identity cube. When the uncorrelated account is manually correlated to another identity cube, or accounts are automatically re-correlated to another identity cube due to updated correlation logic the identity cube still exists but is empty as the account that created it is now associated with a different identity cube. Most of the time these empty identity cubes do not serve any purpose and should be removed by the Prune Identity Cubes task. This task could be scheduled to run periodically.

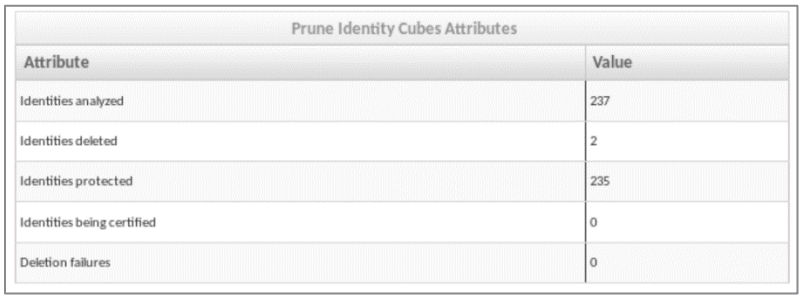
Since Lauren does not have the necessary capabilities to run tasks within IdentityIQ, she asks her IdentityIQ Administration team to clean up the empty identity cubes.

1. Log out of IdentityIQ and back in as **Carl.Foster/xyzzy**

2. Navigate to **Setup** > **Tasks** and run the **Prune Identity Cubes** task.

3. View **Task Results** to see that two identity cubes have been pruned from the environment.

Note: The spadmin identity is protected, meaning that it cannot be deleted through the IdentityIQ Console, Debug Pages, or Prune Identity Cubes task.



Prune Identity Cubes Attributes

Attribute	Value
Identities analyzed	237
Identities deleted	2
Identities protected	235
Identities being certified	0
Deletion failures	0

4. Navigate to **Identities** > **Identity Warehouse**
   a. Search for **Howard**.
      i. Confirm that the **Howard.Rose.Admin** cube was pruned from your environment.
   b. Search for **Judith**.
      i. Confirm that the **Judith.Warren** cube was pruned from your environment.

Update Entitlement Catalog

Maintaining the information in the entitlement catalog is an important maintenance activity. In this section you will perform a bulk update to entitlement information through an import/export. In later exercises, you will use the UI to update entitlement information.

1. Navigate to **Applications** > **Entitlement Catalog**
2. View the entitlements from the Finance application.
   a. Search for **finance** to filter the list.
   b. Which process loaded the Finance entitlements into the entitlements catalog?

      _____

   c. Click the **AP** entitlement to view its information.

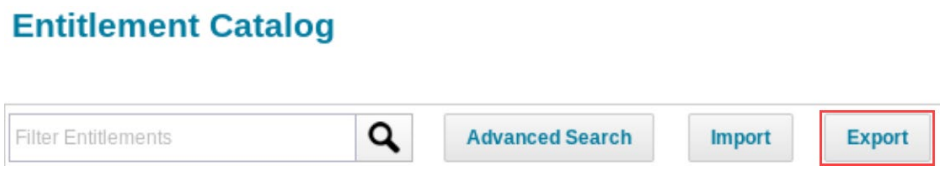
      Notice that the description of this entitlement states it represents the Accounts Payable Group for Finance Application. While some users may know that AP stands for Accounts Payable, this may be confusing for some users.

   d. Scroll down and look at **Owner**

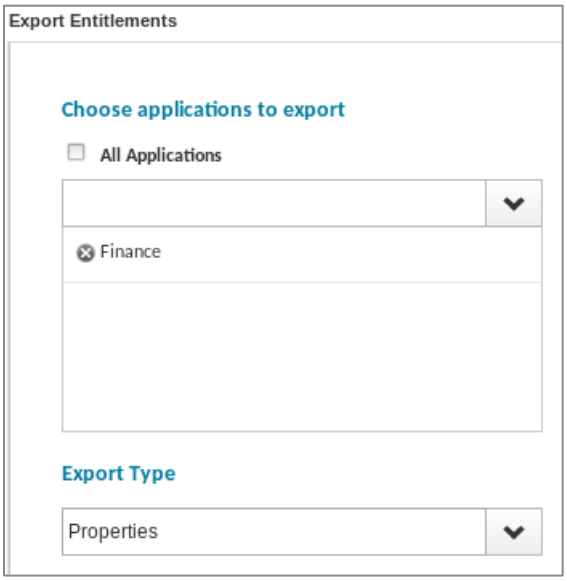
      There is no **Owner** defined on this entitlement.

   e. Click **Cancel** to return to the entitlement catalog.

3. Export only the Finance application.
   a. Click **Export**



      i. Application: **Finance**
      ii. Export Type: **Properties**

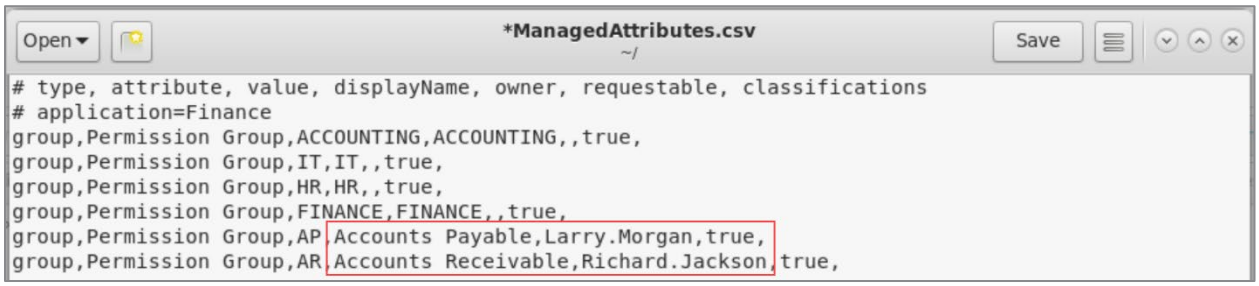


4. Click **Export**
   a. Select **Save File** and click **OK**

      This will save the ManagedAttributes.csv to **/home/spadmin/**

5. In the file browser, use gedit to open **/home/spadmin/ManagedAttributes.csv**
6. Update the CSV to change the following:
   a. Update the **AP** entitlement:
      i. displayName: **Accounts Payable**
      ii. owner: **Larry.Morgan**
   b. Update the **AR** entitlement:
      i. displayName**: Accounts Receivable**

ii. owner: **Richard.Jackson**



c. **Save** the ManagedAttributes.csv

7. Import the updated CSV

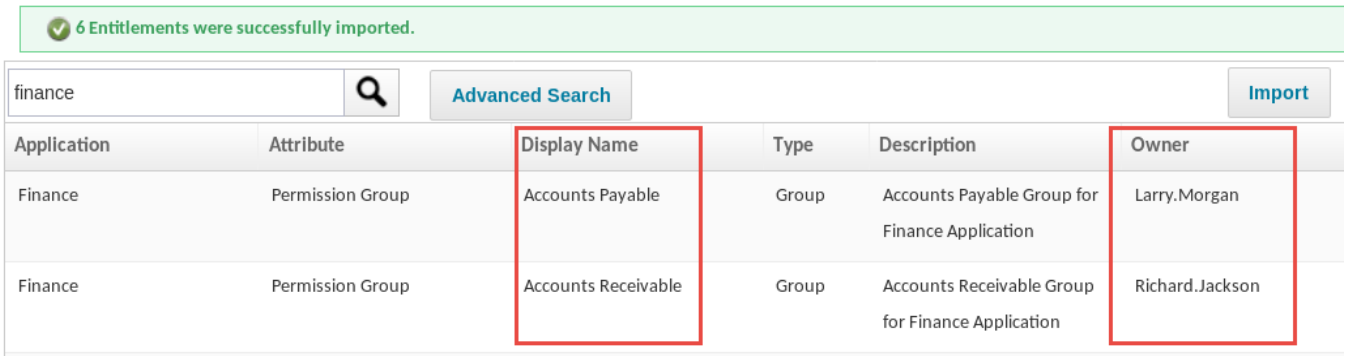
   a. In IdentityIQ, navigate to **Applications** > **Entitlement Catalog**

   b. Click **Import**

   c. Select **Browse…** and select **/home/spadmin/ManagedAttributes.csv**

   d. Click **Import**

8. Verify the updated display names and owners in the user interface. Maintaining the information in the entitlement catalog is an important activity that will improve the experience of users searching for access and will allow reviewers to quickly make accurate decisions in certification campaigns.



Section Three:

System Management, Policies, and Certifications

IDENTITYIQ IMPLEMENTATION AND ADMINISTRATION: ESSENTIALS

SailPoint IdentityIQ Version 8.1

With Rapid Setup

www.sailpoint.com

Table of Contents

Exercise #1: Explore Task Management Options

Objective

In this exercise, you will practice and learn more about task management options.

Overview

Performance of aggregation and refresh tasks is very important to the overall health of your implementation. In this exercise, you will turn on the aggregation optimization and test delta refresh, configuring IdentityIQ to only process data that has changed.

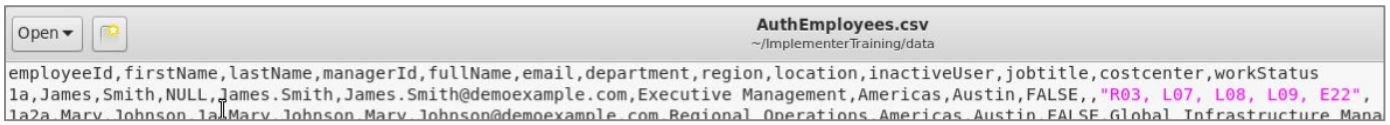
Often additional processing or database cleanup is done through a rule written by your technical implementation team. In this exercise, you'll use the *run rule* task to run a rule. This is often done in place of writing and deploying custom tasks. As a part of configuring the rule runner task, you'll also learn to schedule tasks to run in less than hourly increments.

You'll also explore the standard maintenance tasks and learn about application maintenance windows. Finally, you'll learn more about monitoring tasks with the Administrator Console.

Configure and Test Delta Refresh

Performance of aggregation and refresh tasks can be critical to a healthy implementation. For example, if your enterprise has frequent updates to your HR systems, you might run your aggregation tasks hourly for your authoritative applications. With this schedule, you'll also need efficient refresh processing. In this exercise, you'll enable and test delta refresh.

1. Log into IdentityIQ as **Carl.Foster/xyzzy**
2. Update an account in the employee authoritative application that we will use for testing delta aggregation.
    a. In the file browser, navigate to **/home/spadmin/ImplementerTraining/data**
    b. Right click on **AuthEmployees.csv** and select **Open With gedit**
    c. The first row contains the account for James Smith. Add an additional cost center, **E22**, to his account.



    d. **Save** and close AuthEmployees.csv

3. Update the **Aggregate Employees** task to optimize account reading.

   a. Disable optimization of unchanged accounts: **Uncheck**

      Optimized aggregation means the task skips re-processing of records which match previously aggregated values. This is the default behavior unless you disable it. In development, it is often disabled, as it has been for this task, so IdentityIQ will apply frequently-changing configurations to unchanged data records. But for this activity, we want only the changed record to be processed/updated.

   b. Click **Save and Execute**

   c. How many identities do you expect to be updated? _____

   d. View the task results and confirm your assumption.

4. Create a new task of type **Identity Refresh** to perform delta refreshes.

   a. Name: **Delta Identity Refresh**

   b. Previous Result Action: **Rename Old**

   c. Description: **An Identity Refresh that will only process identities marked as needing to be refreshed by a recent aggregation**

   d. Refresh only identities marked as needing refresh during aggregation: **Checked**

   e. Refresh identity attributes: **Checked**

   f. Refresh manager status: **Checked**

   g. Refresh assigned, detected roles and promote additional entitlements: **Checked**

   h. Click **Save and Execute**

   i. View the task results. How many identities were refreshed? _____

5. Disable optimized aggregation in **Aggregate Employees** task.

   Now that this test is over, turn off optimization again for the duration of the development cycle, to ensure that any configuration changes get applied even if data changes do not occur.

   a. Edit the **Aggregate Employees** task.

      i. Disable optimization of unchanged accounts: **Check**

      ii. Click **Save**

Configure and Test Run Rule Task

The run rule task can execute any specified rule. This task can often be used in place of writing a custom task – a technical implementer can write a rule, and then use this task to schedule and run the rule.

1. Navigate to **Gear > Global Settings > Import from File** and import the following file:

   /home/spadmin/ImplementerTraining/config/Rule-Example-Test-Rule-Runner-Task.xml

2. Investigate the rule.

   a. What is the name of the rule displayed in the **Import results** window?

   _____

   b. The rule you just imported is listed below.

      i. In the code below, view the line that starts **System.out.println**. This rule simply determines the date and prints it to the log file.

      ii. In the code below, circle the value that is returned by the rule. The return value will be displayed in the task results.

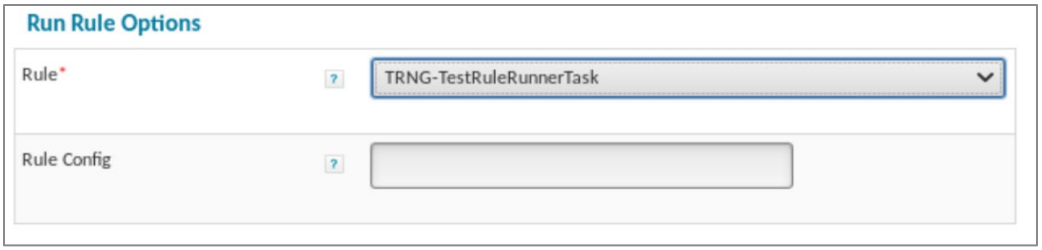
```
import java.util.Date;
import java.text.DateFormat;
import java.text.SimpleDateFormat;

DateFormat dateFormat = new SimpleDateFormat("yyyy/MM/dd
HH:mm:ss");
Date date = new Date();
System.out.println("Rule Runner Test... Current Time/Date
= " + dateFormat.format(date));

return "Success";
```

3. Create a task of type **Run Rule**

   a. Name: **Rule Runner Test**

   b. Previous Result Action: **Delete**

   c. Rule: **TRNG-TestRuleRunnerTask**



d. Click **Save and Execute**

4. Check the execution.

   a. View the task results.

      All the rule returns is the status, so there is no other information listed.

   b. View the output from the Tomcat Standard Out log to see that a time stamp gets printed when the task runs:

      ```
      Rule Runner Test... Current Time/Date = 2020/02/19 12:52:43
      ```

      Hint: On your virtual machine desktop, double click **Tail Tomcat Standard Out**

5. Schedule this new task to run **hourly**.

   a. Name the schedule **Rule Runner Test Schedule**

6. Navigate to **Debug Pages** to run this task more frequently than hourly.

   When scheduling the task, the most frequent execution schedule you can select through the IdentityIQ user interface is hourly. However, you can configure the task schedule to execute more frequently if needed.

   To run this task more frequently than hourly, you must edit the TaskSchedule XML through the Debug Pages and adjust the schedule parameters to run it more often.

   a. Select Object Type: **TaskSchedule** and filter on **Rule Runner Test Schedule**

   b. Click the row to open the **Rule Runner Test Schedule**

c. Find the **CronExpressions** tag in the TaskSchedule object and replace it with the new CronExpressions block shown below.

Note: Your task schedule details, including the values in the original CronExpressions block, may differ based on the time when you created it.

```
<?xml version='1.0' encoding='UTF-8'?>
<!DOCTYPE TaskSchedule PUBLIC "sailpoint.dtd" "sailpoint.dtd">
<TaskSchedule id="Rule Runner Test Schedule" name="Rule Runner Test
Schedule" nextExecution="1582138500000">
  <Arguments>
    <Map>
      <entry key="TaskSchedule.host"/>
      <entry key="executor"
          value="7f000001705a1e0c81705ebdaad90846"/>
      <entry key="launcher" value="Carl.Foster"/>
      <entry key="nextActualFireTime" value="1582138500000"/>
    </Map>
  </Arguments>
  <CronExpressions>
    <String>0 55 * * * ? </String>
  </CronExpressions>
  <Description></Description>
</TaskSchedule>
```

Replace the **<CronExpressions>** block with this:

```
<CronExpressions>
  <String>0 0/5 * * * ? </String>
</CronExpressions>
```

Note: *Cron* is a software utility used for time-based job scheduling. Detailed information about cron expressions can be found at www.quartz-scheduler.org

d. **Save** the TaskSchedule

e. Check back periodically to the Tomcat Standard Out log to see that the task continues to run and executes the rule that writes test messages to the log file.

Explore Standard Maintenance Tasks

The standard maintenance tasks are crucial for proper functioning of IdentityIQ. These tasks are shipped with a pre-defined schedule and will start running as soon as IdentityIQ is installed. In this exercise, we'll look more closely at these 5 important tasks: Perform Maintenance, Perform Identity Request Maintenance, Check Expired Mitigations, Check Expired Work Items, and Check Sunset Requests.

1. View the scheduled tasks and list the next execution time for each maintenance task.

Task Name	Next Execution
Perform Maintenance	
Perform Identity Request Maintenance	
Check Expired Mitigations	
Check Expired Work Items	
Check Sunset Requests	

2. Navigate to the **Tasks** tab and open the **Perform Maintenance** task.
   a. How many prune options are available? _____

      Prune options remove objects from the database at the frequency specified in the system configuration.

   b. In the initial configuration, you set many retention durations for various objects. On the Miscellaneous tab (**Gear > Global Settings > IdentityIQ Configuration**), how many days did you set before "task result deletion"?

      _____

   c. View the Perform Maintenance task again. How many certification related options are available (**Hint**: you may have to hover your mouse over the "?" to find all of them)?

      _____

   d. How many workflow related options are available?

      _____

Manage Aggregations with Application Maintenance Windows

There are times when you need to bring an application down for maintenance. In this exercise, you'll first test what happens when an aggregation task is run and the application is not available. Then, you'll set a maintenance window and again perform an aggregation and note the behavior.

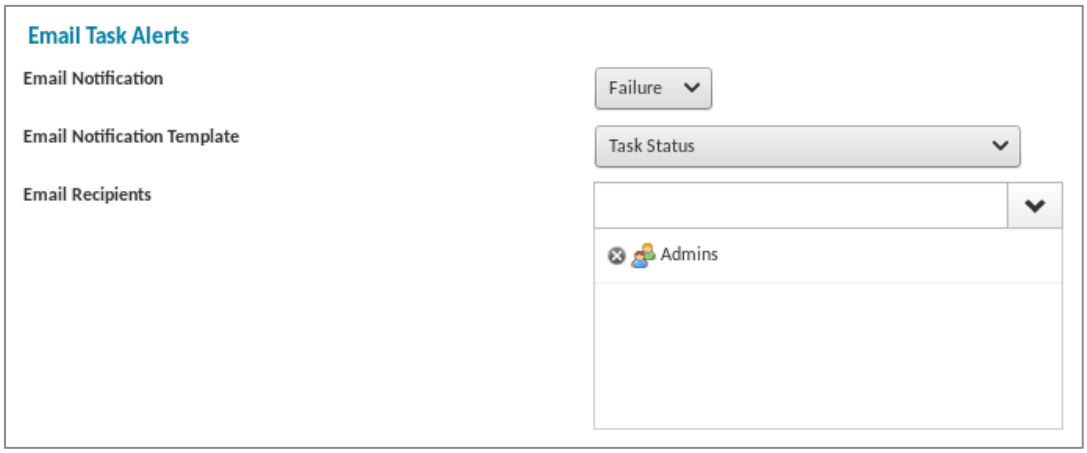
1. Update the **Aggregate LDAP** task to notify when the task fails.

a. Configure the **Email Task Alerts** to match the following settings:

i. Email Notification: **Failure**

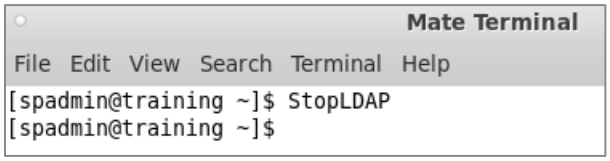
ii. Email Notification Template: **Task Status**

iii. Email Recipients: **Admins**



b. **Save** the task.

2. From a Linux command prompt, stop the LDAP service. Enter **StopLDAP**



3. Run the **Aggregate LDAP** task.

a. What was the task result? _____

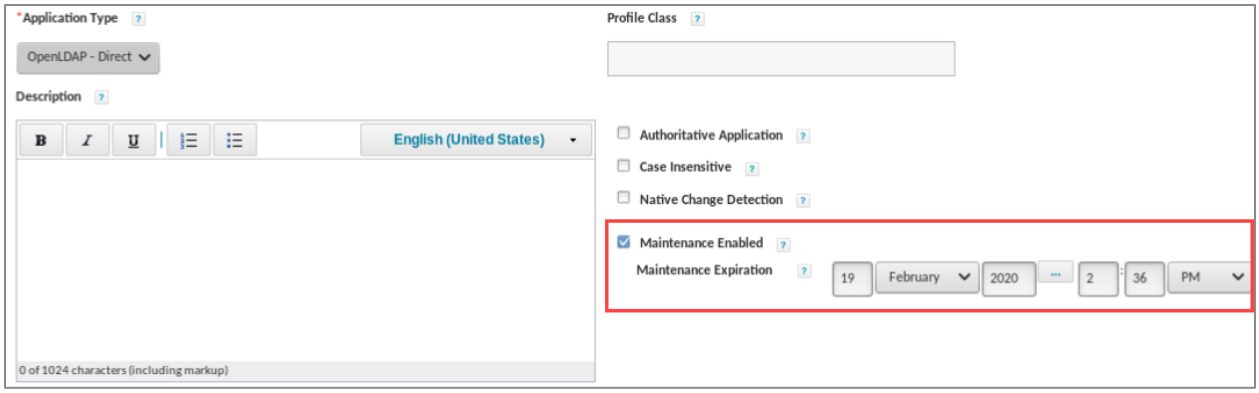
b. View the email log. Who was notified of the aggregation failure?

_____

4. Navigate to **Applications > Application Definition > LDAP > Details**

a. Enable a 10-minute maintenance window.

Hint: Look in the top right corner of your lab environment for the current time. The environment time may differ from your local time.



b. **Save** application.

5. Run the **Aggregate LDAP** task a second time.

   a. What was the task result? _____

   b. View the email log. Was an email sent? -Select-

      No attempt will be made to aggregate from an application during a scheduled maintenance window. By default, provisioning activities will be retried after the maintenance window is complete.

      Note: For more information about maintenance windows, see the *Maintenance Windows* whitepaper on Compass.

6. At the Linux command prompt, start the LDAP service.

   a. Enter **StartLDAP**

Monitor Tasks

You previously viewed the Administrator Console as a user with the System Administrator capability. Administrative users who need to monitor the Administrator Console but who should not have full system access can be given the *Full Access Admin Console* or *View Admin Console* capabilities. In this exercise, you'll use the Capabilities report to view users who currently have the capability to use the Administrator Console. Then, as a user with that access, you'll perform several activities using the Administrator Console.

1. With a report, identify users that have the capabilities required for Administrator Console access.

   a. On the Reports tab (**Intelligence** > **Reports**), open the **Capability to Identities Report** and configure as follows:

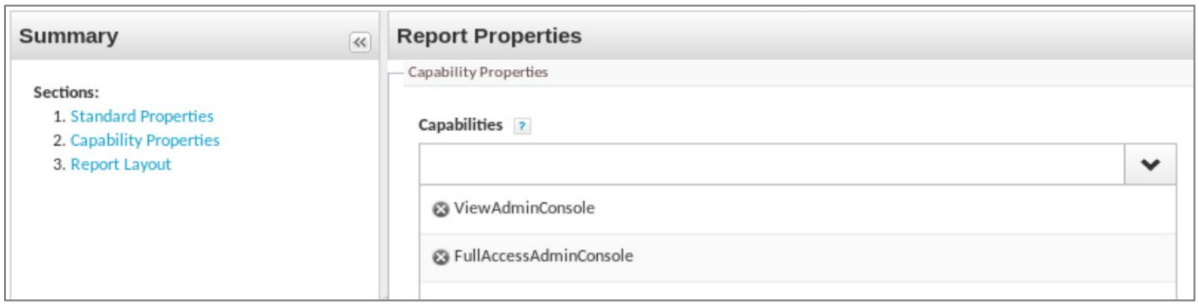
      i. Standard Properties:

         (1) Name: **Admin Console Access**

(2) Description: **Displays identities that have Administrator Console access**

ii. Capability Properties:

(1) Capabilities: **ViewAdminConsole, FullAccessAdminConsole**



b. Click **Save and Execute** and view the report results.

c. Do any users have the Full Access Admin Console capability? -Select-

IMPORTANT: Follow the next 4 steps quickly. The task you're about to run provides approximately *two minutes* to view an active task in the Administrator Console.

1. Run the **Aggregate Non-authoritative Applications** task.
2. Logout, and login as **Mary.Johnson/xyzzy**
3. Navigate to **Gear > Administrator Console** > **Tasks**

a. On the **Active** tab, view all tasks that are currently running.

i. Click back and forth from the **Active** and **Completed** and watch as multiple tasks are run.

ii. Which task is running each time you view the **Active** tab? Why?

_____

_____

b. On the **Scheduled** tab, you can view execution information, postpone scheduled tasks or delete a schedule.

i. When was the last time the Rule Runner Test ran?

_____

ii. Click the calendar next to **Rule Runner Test Schedule** and postpone this task for one month.

c. On the **Completed** tab, you can see the last runtime, average runtime, and difference from average for the completed tasks.

i. What is the *average run time* for the task **Aggregate Non-Authoritative Applications**?

_____

ii. What is the *run time* for the **Admin Console Access** report? _____

Note: IdentityIQ reports are a special type of task.

4. Notice what access the **Full Access Admin Console** capability provides.

a. Can Mary access **Setup > Tasks**? (Circle one) -Select-

b. Can Mary access **Applications > Application Definitions**? (Circle one) -Select-

c. What other access does Mary have? _____

_____

5. Why does Mary have the **Full Access Admin Console** capability? _____

Exercise #2: Explore Log4j

Objective

In this exercise, you will work with log4j.

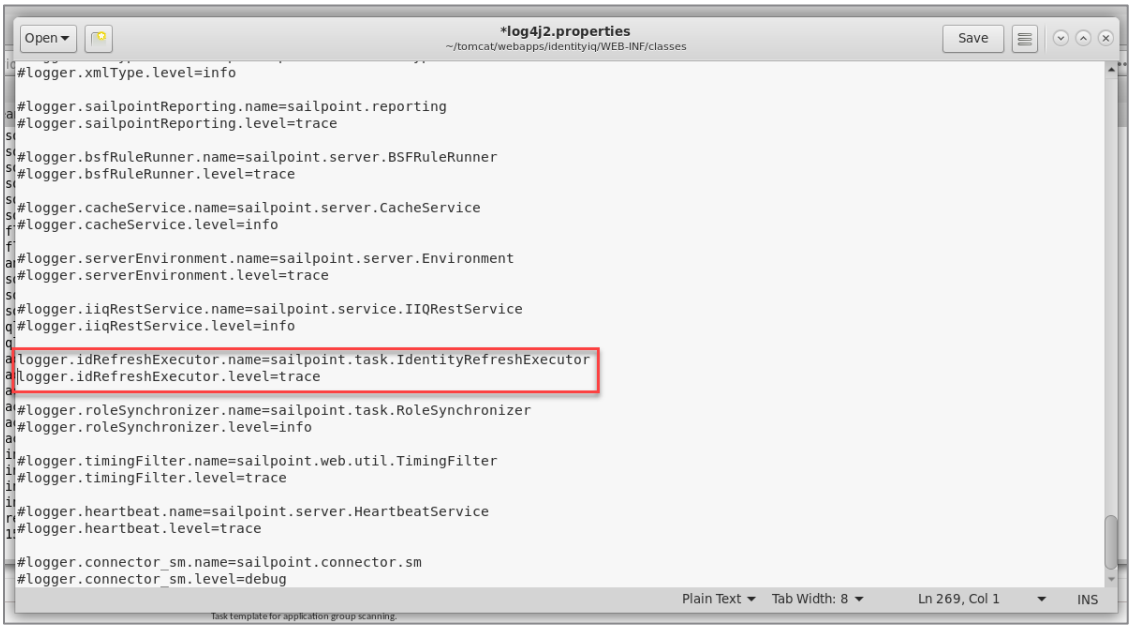
Overview

Log4j is useful when trying to debug a problem. For example, if an identity refresh failed at a certain point, tracing could be turned on to see upon which identity the refresh was failing. In this exercise, you will enable trace level logging for the refresh task, reload the log4j properties file and view the results. Finally, you'll rerun the test using debug level logging and compare the results.

Enable Trace Level Logging

Explore the trace-level logging information available from the Identity Refresh task executor.

1. In a file browser, navigate to **/home/spadmin/tomcat/webapps/identityiq/WEB-INF/classes**
2. Use gedit to open the **log4j2.properties** file.
   a. Search for **Refresh**
   b. Enable logging for the **IdentityRefreshExecutor** Java class by removing the # characters from the front of both lines. The # character makes the line a comment.
   c. Leave the logging option at **trace**



3. **Save**, but do not close, the **log4j2.properties** file.

   Note: with previous versions of log4j, you had to reload the properties file after making any changes. You could reload this file either by restarting the application server, or by navigating to the Debug Pages, logging page and reloading the logging configuration. You do not need to perform these steps for log4j2. Log4j2 supports change monitoring on the logging configuration file so it will automatically pick up any configuration changes without any further administrative action required. By default, IdentityIQ's log4j2 properties file is refreshed every 20 seconds.

4. Launch the desktop shortcut named: **Tail IdentityIQ Log** and leave this window running.

   This window will show any log messages generated by IdentityIQ as we work through the lab exercises.

5. After 20 seconds have passed, use the IdentityIQ Console to execute the task: **Refresh Finance Identities**

   a. You can run tasks through the IdentityIQ Console. In the IdentityIQ Console, execute the command:

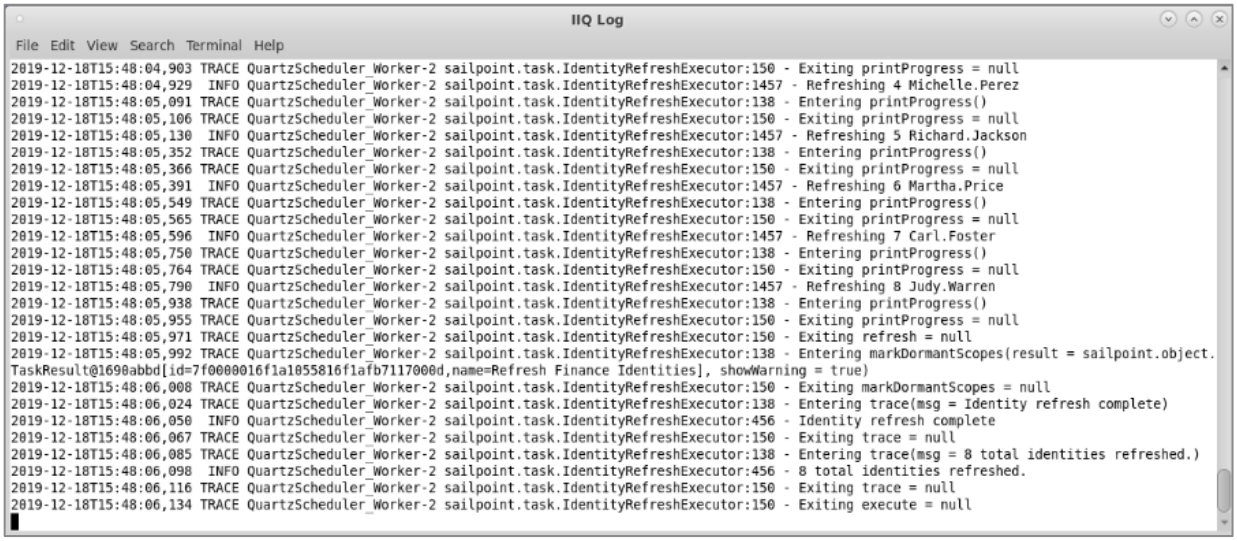
      ```
      run "Refresh Finance Identities"
      ```

   b. Watch the Tail IdentityIQ Log for the log file entries.

      Each new entry begins with a date/time stamp (e.g. 2019-12-18 15:48:06,134). Then it follows with the error level (TRACE & INFO as shown below), thread name, Java class and further details of the entry.

   c. Look at the trace output listed below the "Identity refresh complete" message.

      i. List the total number of identities refreshed. _____



d. In the previous picture, circle the trace step just above the total, and the trace step just below the total.

Trace is designed to log every step in the code being processed – the log statements you circled show the progress as the trace routine was entered and then exited. Trace can provide a very large amount of data.

Enable Debug Level Logging

1. Use gedit to edit the **log4j2.properties** file

   a. On the second line of the **IdentityRefreshExecutor** entry, change **trace** to **debug**

   ```
   logger.idRefreshExecutor.level=debug
   ```

2. **Save** the **log4j2.properties** file.

3. After 20 seconds have passed, use the IdentityIQ Console to rerun the task: **Refresh Finance Identities**

   Note: In the IdentityIQ Console, use the up-arrow on your keyboard to recall the previously entered command.

4. Watch the Tail IdentityIQ Log for the log file entries.

   a. How many lines total are displayed when using debug level logging? _____

   Note: When troubleshooting a problem, it is a best practice to start with logging at the debug level, and only move to trace if you really need the additional detail.

   b. Enter **quit** to exit the IdentityIQ Console.

Add Additional Rapid Setup Logging

The entries in a log4j file are named for the specific class of code related to the issue you are investigating. The default log4j2 file provides commented-out statements for common classes where you can simply un-comment the statements that provide the logging you want as you just experienced. However, the default log4j file is not exhaustive. There are more classes in IdentityIQ for which you can add additional entries to the log4j file to increase logging. Some examples of these classes may be specific application connectors, your implementation's BeanShell logging methods, or classes related to Rapid Setup. In this section, you will add some entries for Rapid Setup logging.

1. Use gedit to edit the **log4j2.properties** file

   a. Replace the # on both lines to disable logging for the **IdentityRefreshExecutor** Java class to **turn off** the increased logging for this class.

   b. Scroll to the bottom of the file and add the following lines commented lines:

```
#logger.rs.name=sailpoint.rapidsetup
#logger.rs.level=debug
#logger.rslibrary.name=sailpoint.workflow.RapidSetupLibrary
#logger.rslibrary.level=debug
```

2. What is the result of adding these lines? Will this cause logging to occur?

_____

Remember these lines later if you encounter any issues with your Rapid Setup configurations. You can come back and uncomment them to help with troubleshooting.

3. **Save** and **close** the **log4j2.properties** file.

Exercise #3: Explore IdentityIQ Debug and Console

Objective

In this exercise, you will work with two additional tools that are used for administering and troubleshooting IdentityIQ: Debug Pages and IdentityIQ Console.

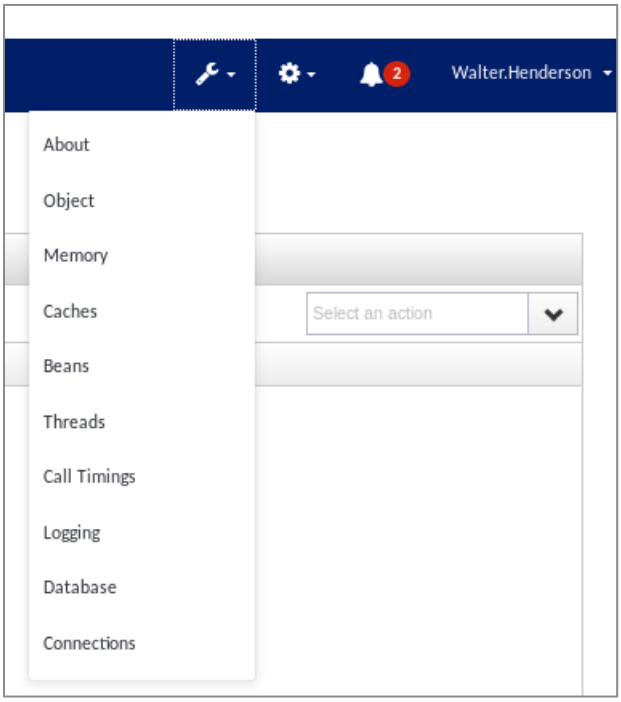
Overview

This exercise allows practice with the tools necessary for advanced configuration, troubleshooting, and providing support data to the SailPoint support team.

Explore the Debug Pages

Sometimes you may need to view the XML representation of an object or add an option that is not supported in the browser interface. Debug Pages are used for advanced configuration and debugging of XML representation of objects, and other administrative tasks.

1. Explore the About IdentityIQ Page.
    a. Log into IdentityIQ as **Carl.Foster/xyzzy**
    b. Navigate to the **Debug Pages**
    c. Click the **tool icon** to view the dropdown menu.
    d. Choose **About**



e. View the **Product Information** section and list the version of IdentityIQ that is running in the training environment.

_____

The first two numbers, 8.1, are the release version. If there is a patch, this is followed with the patch level, using a pX indicator, where X is a number, such as 8.1p1.

i. Is there a patch level for this installation? If so, what is the patch level?

_____

2. Select the **tool icon** and view some of the other pages.

- **Logging** – used to reload the log4j properties file or to load a new log4j properties file.
- **Call Timings** – used to monitor performance of IdentityIQ code and custom code (if configured to leverage Call Timings).

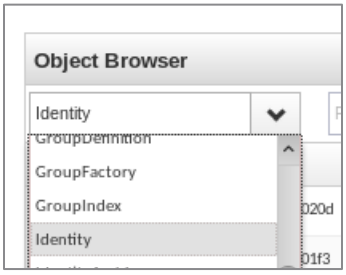
Note: Many of these pages are used when working with SailPoint support.

3. Explore the Object Browser Page.

You will view an identity cube and look at the identity attributes in XML format. This is useful because attributes can be stored on the cube that have not been configured to be seen through the UI. For other objects (i.e. tasks and applications), advanced options can be set here.

a. Click the **tool** icon, then **Object** to return to the **Object Browser**

b. From **Select an object** dropdown, choose **Identity**



All of the identities in the system are listed.

c. Search for **Amanda.Ross**

i. In the **Filter by Name or ID** box, enter **Amanda** and click the **search** icon.

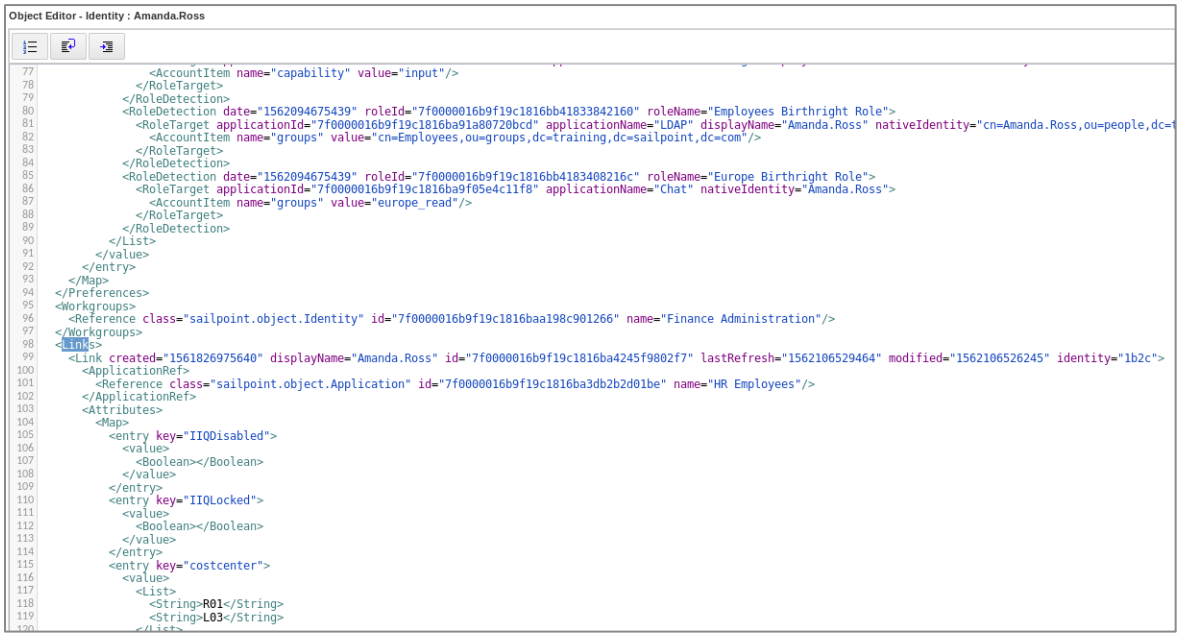
d. Click the entry for **Amanda.Ross** and view the XML representation of the identity cube.

e. The first data you see are the Attributes. Which attribute is listed first?

_____

All identity attributes are visible in the identity XML, even those that are not configured to be seen with the UI.

f. Within this page, search for **link** (remember, *link* is the internal term for *account*).



The first account on this cube follows. Details about this account continue from the **<Link>** tag to the **</Link>**

g. Inside the Link tag, look at the **ApplicationRef** tag. List the application associated with this account.

_____

h. Find the next link (after **</Link>**). List the application associated with the next account.

_____

i. **Close** the Object Editor and clear the identity search by clicking the **X** next to the magnifying glass.

Debug Pages - Create a copy of an object

Sometimes you need to quickly create an object such as a rule or an email template, that is slightly modified from the original. You can use the Debug Page to copy and edit objects.

Note: This is *not* a recommended practice for production installations.

1. Using the object browser, search for and view the rule **TRNG-TestRuleRunnerTask**

```
1  <?xml version='1.0' encoding='UTF-8'?>
2  <!DOCTYPE Rule PUBLIC "sailpoint.dtd" "sailpoint.dtd">
3  <Rule created="1596008064574" id="7f00000173811e6e8173997e663e12fd" language="beanshell" name="TRNG-TestRuleRunnerTask">
4    <Description>Example rule to test the run rule task. When run, it returns "Success" to be displayed in the task result and
5    <Source>
6
7  import java.util.Date;
8  import java.text.DateFormat;
9  import java.text.SimpleDateFormat;
10
11 DateFormat dateFormat = new SimpleDateFormat("yyyy/MM/dd HH:mm:ss");
12 Date date = new Date();
13 System.out.println("Rule Runner Test... Current Time/Date = " + dateFormat.format(date));
14
15 return "Success";
16
17   </Source>
18 </Rule>
19
```

   Cloning an object involves renaming it and removing its system-generated ID so IdentityIQ can generate a new unique ID for the new object.

2. On line 3, in the <Rule> line, change the value of the **name** attribute to **TRNG-ManuallyRunRule**

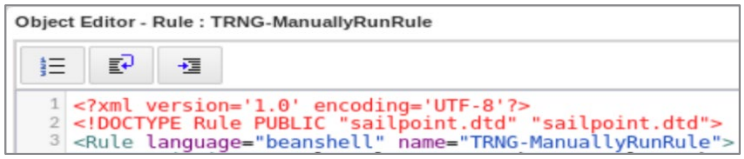
3. In that same line, delete the **id** attribute, along with its value.

4. Also delete the **created** and **modified** attributes.

   It is good practice to also delete the **created** and **modified** attributes. They are system-generated date values signifying when the object was created and last modified, and their values in the old object are incorrect for the new object you are creating. IdentityIQ will re-generate these values, as appropriate, for the new object.

5. Make sure that your <Rule> element (line 3) looks like this:

   ```
   <Rule language="beanshell" name="TRNG-ManuallyRunRule">
   ```

6. **Save** the rule.

7. Open the new rule, **TRNG-ManuallyRunRule**, and edit the code.

   This is now a completely independent rule object from the original. Changes you make here do not affect the other rule.

   a. Before you edit, notice the new ID and created date assigned by IdentityIQ.

      These were generated by IdentityIQ when you saved the new rule.

   b. On line 13, change the text:

      From: Rule Runner Test
      To: **Manual Test**

   c. **Save** the rule.

8. Manually run the rule from the Debug (Object Browser) page.

   a. In the drop down to the left of the Run Rule button, select **TRNG-ManuallyRunRule**

   b. Click **Run Rule**

      The results returned by the rule are displayed in the white pop-window – in this case the success message.

   c. View Tomcat Standard Out for the println statement.

   d. Verify that you see the update println statement you changed to **Manual Test**.

Delete an object through Debug Pages

Sometimes you may need to delete an object that cannot be deleted through the UI. Many objects can be deleted from the Debug Object Browser page. Be very careful with object deletion, as **once an object has been deleted, it cannot be recovered**.

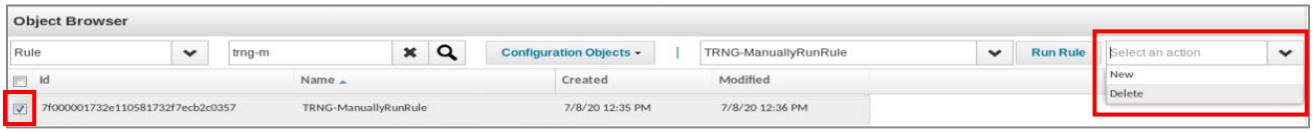
You'll walk through the process here, but **do not** actually perform the deletion yet. You will delete this later through the IdentityIQ Console.

Note: Deletion is *not* an action typically performed through Debug in a production instance.

1. In the Object Browser, find the rule you just created **TRNG-ManuallyRunRule**

2. Select the box next to the object to be deleted.

3. On the far right of the Object Browser, in the **Select an action** menu, select **Delete**



4. When prompted to confirm this delete action, click **No** to abort the deletion.

Explore IdentityIQ Console Commands

The IdentityIQ Console is a command-line driven interface to the IdentityIQ database. With the console, you can do many of the same things that can be done through the UI and the Debug Pages. There are also commands that can only be run from the console. The only way to export objects is through the console. In this exercise, you will learn to export individual objects and sets of objects.

1. Recall that in the training environment, there are two ways to access the IdentityIQ Console. Select from the following:

   a. In the training environment, a desktop shortcut has been provided. From the desktop, double-click the IIQ Console shortcut.

   b. In all environments, the console can be accessed from the bin directory: *Installation Directory*/WEB-INF/bin. The command in your environment is: **/home/spadmin/tomcat/webapps/identityiq/WEB-INF/bin/iiq console -j**

      The IdentityIQ console will take several seconds to start.

2. Log into the console as **Carl.Foster/password**.

   Only IdentityIQ users with the System Administrator capability can use the Console.

3. Enter **?** or **help** to view the list of console commands.

   Notice that the list of commands is grouped.

   a. Review the groupings.

b. From the following list, mark the options that are groupings of console commands:

- ☐ Objects
- ☐ Identities
- ☐ Applications
- ☐ Workflow
- ☐ Roles
- ☐ Certifications

4. The IdentityIQ console shows you the syntax for a command if you enter the command with no parameters.

   a. At the prompt, type **get** and press enter.

      The **get** command allows you to view an object.

   b. What command would display the **TRNG-ManuallyRunRule** rule object XML?

      _____

5. Now try this with the **list** command.

   a. At the prompt, type **list** and press enter.

      The list command includes two levels of functionality. Without any parameters is a good way to get the exact name of the objects (classes) for use in other commands. It can also be used to retrieve lists of objects of a given class.

   b. Scroll up to see the syntax: **list <class> [<filter>]**

      This command *requires* that you specify a class, and the [square brackets] indicate optional syntax. You must enter a class and you may optionally add a filter.

   c. Type the following:

      ```
      list rule
      ```

   d. Now apply a filter by typing:

      ```
      list rule trng*
      ```

6. There is a command that provides the quantity of a specified object type. See if you can find it in the list of commands when entering **?**

   a. What command would determine the number of rules?

_____

b. How many rules are in this instance of IdentityIQ? _____

7. Use the **rule** command to run the rule **TRNG-ManuallyRunRule** from the console.

   a. Where is the return result displayed?

   _____

   b. Where is the println output displayed?

   _____

8. In the console, use the **delete** command to delete the rule **TRNG-ManuallyRunRule**

   a. Enter the command:

   ```
   delete rule TRNG-ManuallyRunRule
   ```

   b. What important difference did you notice between the behavior of the command line delete and the Debug page delete option?

   _____

   c. Enter the command you used to determine the number of rules again to verify that the rule was deleted.

9. A primary use for the console is to export all objects of a certain type or to checkout an individual object. A best practice is to always use the -clean option to strip out the data specific to the current instance of IdentityIQ.

   a. **Export** all **applications** from IdentityIQ to a file on the **Desktop** called **apps.xml**. Use the **clean** option.

      i. Enter **export** to see the syntax for this command.

      ii. Perform export:

      ```
      export -clean /home/spadmin/Desktop/apps.xml application
      ```

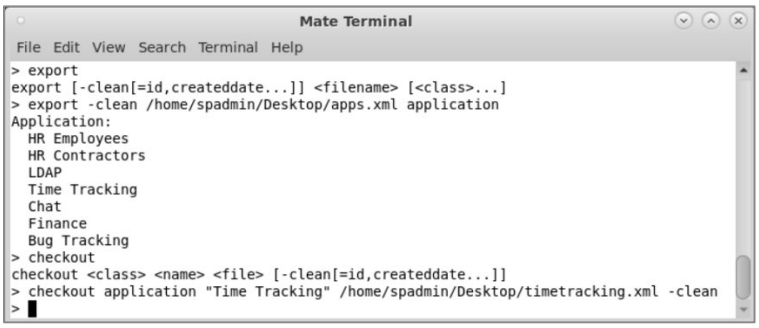
      iii. From the desktop, open and view the **apps.xml** file. When finished, close this file.

   b. Return to the IdentityIQ Console. **Checkout** only the **Time Tracking** application from IdentityIQ to a file call **timetracking.xml**. Use the **clean** option.

      i. Enter **checkout** to see the syntax for this command.

ii. Perform checkout:

```
checkout application "Time Tracking"
/home/spadmin/Desktop/timetracking.xml -clean
```



iii. From the desktop, open and view **timetracking.xml** file in gedit.

c. Add a description for the Time Tracking application.

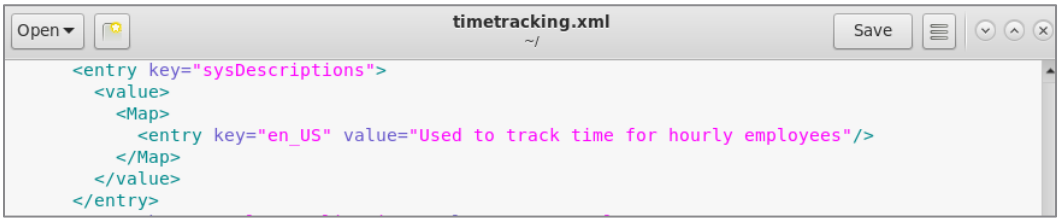
i. In **timetracking.xml**, find the row for the **sysDescriptions** entry and update it:

From:

```
<entry key="en_US"/>
```

To:

```
<entry key="en_US" value="Used to track time for hourly
employees"/>
```



ii. **Save** and **close** the **timetracking.xml** file.

d. **Import** the Time Tracking application.

i. Enter **import** in the IdentityIQ Console to see the syntax for this command.

ii. Import the updated application definition.

```
import /home/spadmin/Desktop/timetracking.xml
```

e. Enter **`quit`** to quit the Console.

10. Confirm the change to the Time Tracking application in the IdentityIQ user interface.

a. Log into IdentityIQ as **Carl.Foster/xyzzy**

b. Navigate to **Applications** > **Application Definition**

c. Open the **Time Tracking** application and view the updated description.

Exercise #4: Define Policies

Objective

In this exercise, you will define a policy to analyze identity data to determine who is in violation, and to allow managers and other users to learn about the policy violations.

Overview

IdentityIQ Policies are used for audit, legal, and regulatory compliance (such as SOX, GDPR, HIPAA and CCPA), as well as for alignment of access controls to business standards. The objective of this exercise is to define a policy to detect conflicting access and to test your configuration to ensure that policies are working correctly in your environment.

Define an Entitlement Separation of Duties Policy

Your company may choose to define and monitor for access policy violations to help ensure that users are complying with business and regulatory requirements. In this exercise, you will create an entitlement separation of duties policy, and then scan for identities who are in violation of this policy.

You will set a policy definition to restrict users from having both of these entitlements on the Finance application: Accounts Payable and Accounts Receivable.

1. Log into IdentityIQ as **Carl.Foster/xyzzy**
2. Navigate to **Setup** > **Policies**
3. In the upper right, click **New Policy** and select **Entitlement SOD Policy**
4. Configure as follows:
    a. Name: **Accounts Payable and Accounts Receivable**
    b. Owner: **Admins**

       Note: This is the owner of the policy *definition* itself, for example, a Compliance Officer.

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

       Note: This is the owner of the policy *violation*. This is the person who receives notification of the violation and is expected to act on it. This is frequently the manager of the person with the violation. However, notice there are other options, including a rule.

d. State: **Inactive**

Note: You can mark an entire policy as inactive, and you can also individually activate or deactivate rules within a policy. It's smart to leave policies inactive until you're certain you're ready to assess them.

e. Send Alerts: **Checked**

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

ii. Observers: **Admins**

Note: The policy violation owner, which in this case is the identity's manager, are automatically notified the policy violation work item is created. We also want the policy owner to be notified via email, so we are specifying them as an observer.

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

i. Summary: **Cannot have access to Accounts Payable and Accounts Receivable at the same time**

ii. Correction Advice: **Align access with the user's primary work responsibility**

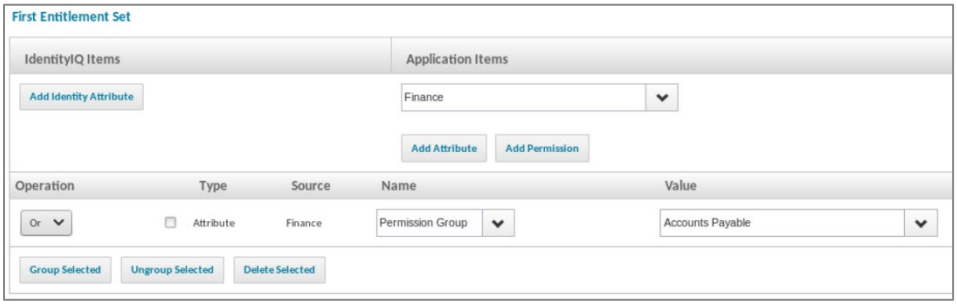
iii. First Entitlement Set:

(1) Application Items: **Finance**

(2) Click **Add Attribute**

(3) Name: **Permission Group**

(4) Value: **Accounts Payable**



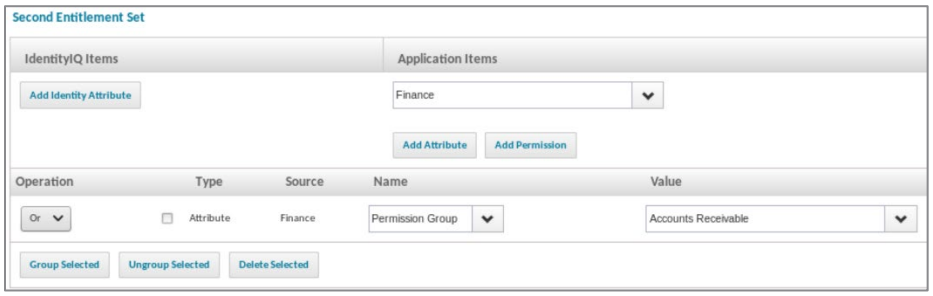
iv. Second Entitlement Set:

(1) Application Items: **Finance**

(2) Click **Add Attribute**

(3) Name: **Permission Group**

(4) Value: **Accounts Receivable**



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

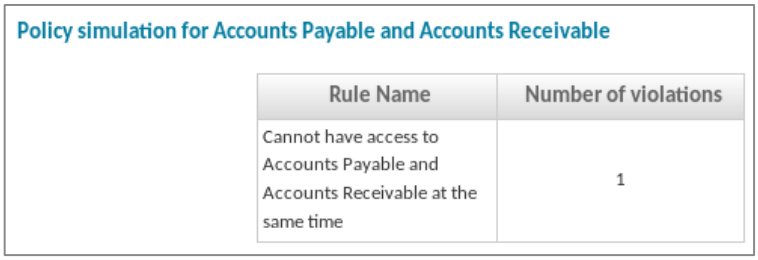
5. Scroll down and click **Save** to complete the policy.

Run Simulation

Before activating policies, it is a best practice to run simulations and confirm that your policy definitions are accurate. These simulations will check identity cubes against the policy definitions and display the number of identities who will be in violation of this policy when it becomes active. You can run simulations for the entire policy, and you can also run simulations at the policy rule level. You will run the simulation at the policy level.

1. Navigate to **Setup** > **Policies**
2. Click the **Accounts Payable and Accounts Receivable** policy.
3. Scroll to bottom and click **Run Simulation** 

and click **OK** when prompted.
4. View the results of this simulation in Task Results.
   a. Open the results for **Policy Impact Analysis: Accounts Payable and Accounts Receivable**
   b. Confirm that one identity will be in violation of this policy:



Scan Identities for Policy Violations

1. Navigate to **Setup** > **Policies** and open the **Accounts Payable and Accounts Receivable** policy

   a. Change State to **Active**

   b. **Save** the policy.

2. Edit the **Refresh Identity Cube** task you have previously configured.

   a. Enable the option: **Check active policies**

   b. **Save and Execute** this task.

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

Refresh Identity Cube Attributes	
Attribute	**Value**
Identities examined	235
Managers discovered	48
Policies checked	Accounts Payable and Accounts Receivable
Policy violations	1
Policy notifications	2

Note: If your task results do not show the detection of the policy violation, see the troubleshooting tips at the end of the exercise.

Observe Notifications about Policy Violations

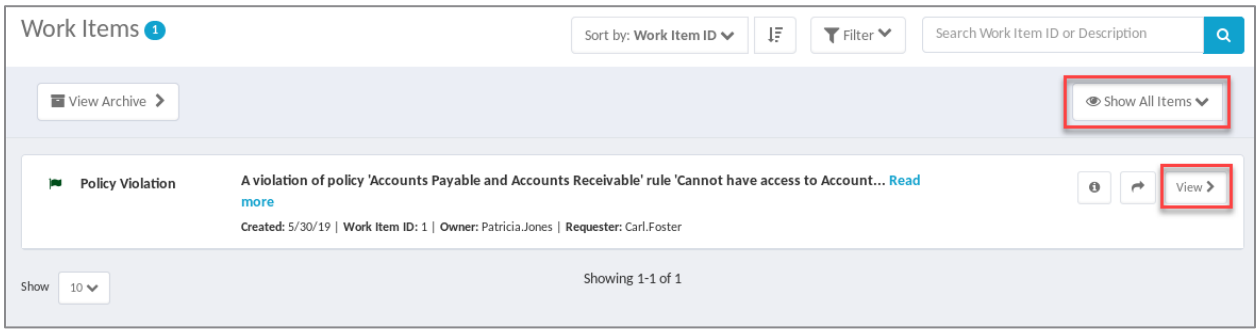
View the policy violation work items and emails.

1. View Work Items.

   a. Navigate to **My Work** > **Work Items**

   b. Since Carl has the System Administrator capability, he can see all work items. Explore his different view settings: change the filter from **Show All Items** to **Show My Items** and **Admins** to see the work items within each view.

c. Ensure the filter is set to **Show All Items** and **View** the policy violation.



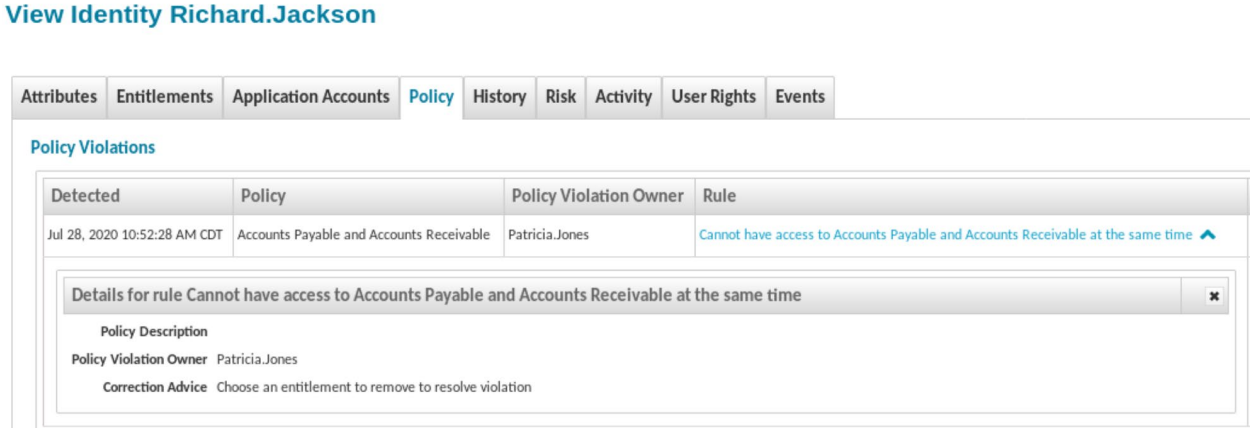
Notice that Richard Jackson is in violation of the policy because he has both Accounts Payable and Accounts Receivable entitlements. His manager, Patricia Jones, is the owner of the policy violation, meaning she is responsible for resolving the violation.

2. View Richard Jackson's Identity Cube.

   a. Navigate to **Identities > Identity Warehouse**

   b. Search for **Richard.Jackson**

   c. Open this cube and view Policy



3. Check the Email Log.

   a. On your desktop, launch the **Tail Email Log** shortcut and confirm that you can see emails that were sent out when policy violations were discovered.

   Two emails were sent out:

   - One was sent to Admins workgroup because they were configured as an Observer on the policy definition.
   - The other was sent to Patricia because she is Richard's manager, and you specified that Managers are the Policy Violation Owners.

Troubleshooting Violation Detection

In this exercise you run a policy simulation. When the simulation is run, the policy will be disabled, and the policy must manually be re-enabled once the simulation has completed.

There is an additional option to simulate not the entire policy, but just an individual policy rule. If you selected this option, the rule will be disabled in response to your request to run the rule simulation, and the policy rule must manually be re-enabled once the simulation has completed.

Check to see if the policy and policy rule are enabled

1. Open the policy.
2. Click the policy rule under **SOD Policy Rules** to edit the rule.
3. Ensure the rule disabled flag is **not checked** and click **Done**
4. Ensure the policy State: **Active**
5. **Save** the policy.
6. Run the task **Check Active Policies** to see if the policies are now detected as expected.

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

Exercise #5: Certify Access

Objective

In this exercise, you will create a certification and perform an access review so you will understand the available configurations and the user experience in this compliance process. You will certify employees' access on the Finance application.

Overview

Access certifications (also known as access reviews or attestations) help a business ensure and verify that users have only the access they should have to perform their jobs. Once you have loaded account and entitlement data from applications, you can run certifications to confirm your users' access is appropriate for their current job responsibilities. This helps ensure your access data is "clean" and accurate. Certain users may have too much access; in that case, the certifier can revoke those unnecessary entitlements during the access review. Other users may not have enough access; in that case, you should submit an access request for that user for the missing required entitlements.

In this exercise, you will kick off a targeted certification to confirm employees' access on the Finance application.

Execute Targeted Certification to Confirm Finance Data

1. Log into IdentityIQ as **Dennis.Barnes/xyzzy**

   Since Dennis is part of the **Operations** workgroup, he has the Compliance Officer capability, and therefore, he can define certification campaigns.

2. Navigate to **Setup** > **Certifications**

3. Click **New Certification** > **Targeted**

4. Configure the certification as follows:

   a. In the **Who do you want to certify?** section, set:

      i. Select **Filter**

      ii. Click **Filter Identities**

      iii. Select Attribute: **Type**

      iv. Operation: **Equals**

      v. Value: **Employee**

      vi. Exclude Inactive Identities: **Checked**

b. In the **What do you want to certify?** section, set:

   i. **Uncheck** the Roles checkbox.

   ii. Under **Additional Entitlements**, click **Filter Entitlements**

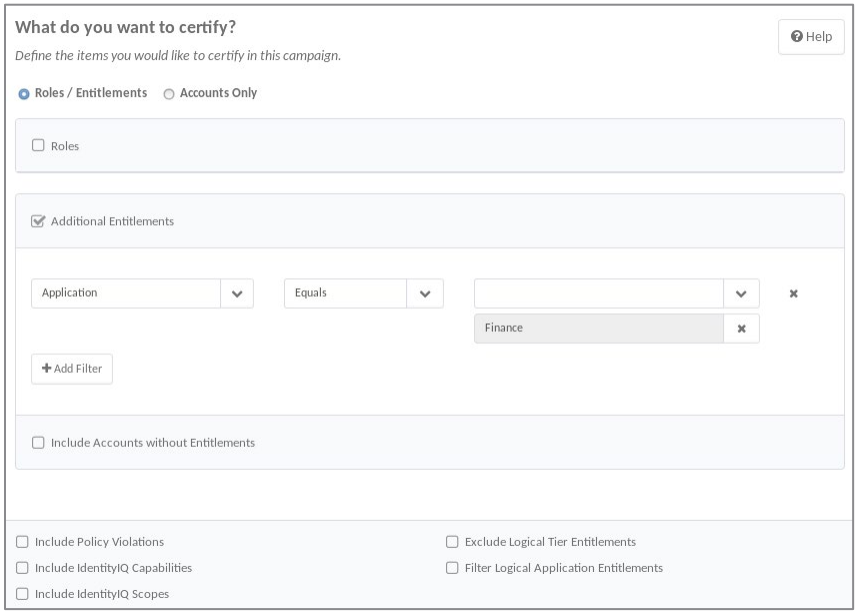
      (1) Select Attribute: **Application**

      (2) Operation: **Equals**

      (3) Value: **Finance**

   iii. Target Permissions: **uncheck**

   iv. Include Policy Violations: **uncheck**

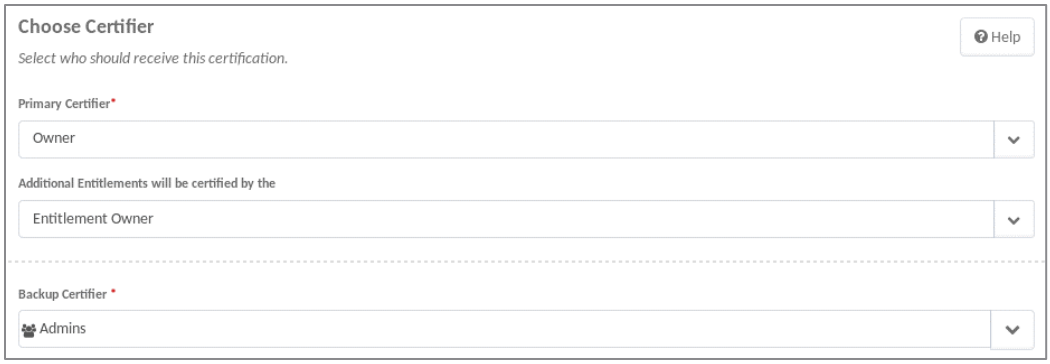


c. In the **Choose Certifier** section, set:

   i. Primary Certifier: **Owner**

   ii. Additional Entitlements will be certified by the: **Entitlement Owner**

   iii. Backup Certifier: **Admins**



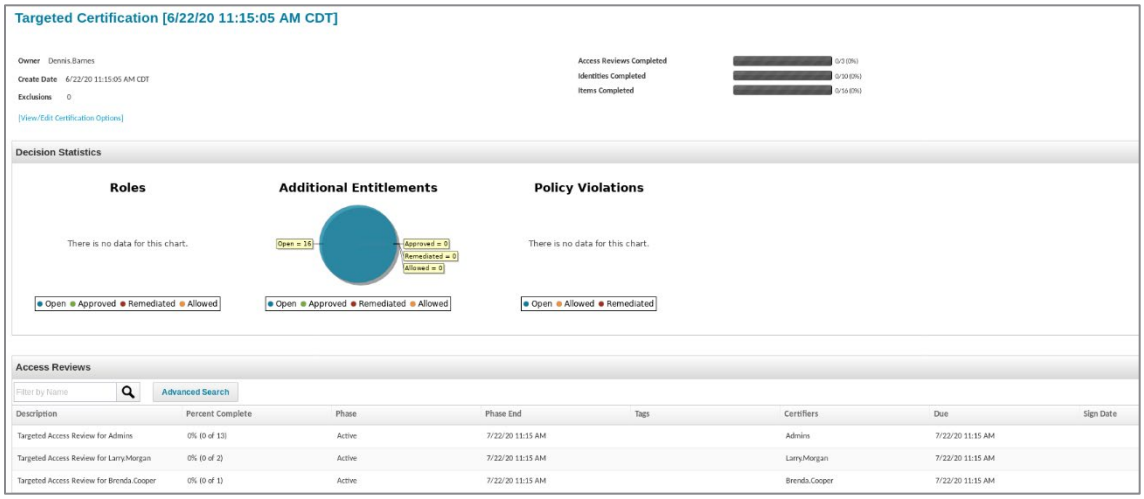
d. In the **Schedule Certification** section:

   i. Select **Run Now**

e. Click **Schedule Certification**

View Certification Details

1. On the **Setup** > **Certifications** page, open the **Targeted Certification**

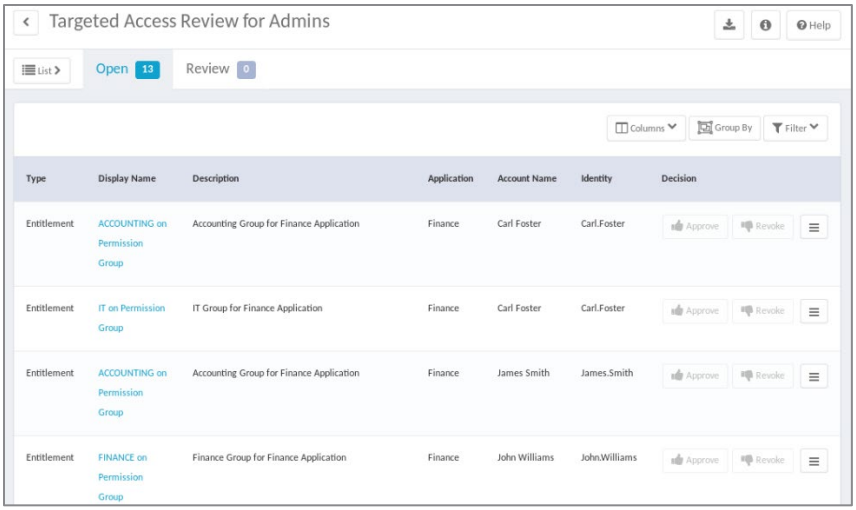


2. Why did 2 of the access reviews go to specific users instead of the Admins work group?

   _____

3. Open the access review for **Larry.Morgan** and view the entitlements included in this certification.

4. Open the access review for the **Admins** workgroup and view the entitlements included in this certification.



Complete the Access Review

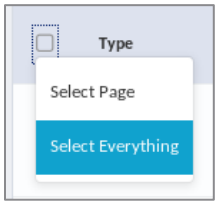
Since Carl Foster is a member of the Admins workgroup, you will have Carl perform the certification.

1. Log out and back in as **Carl.Foster/xyzzy**
2. Click the **Access Reviews** widget on your home page.
3. Click **Start** to begin the **Access Review for Admins**

   Carl is presented with the access review, which has 13 items split on two pages. He can choose to work with this access review in one of two ways – individual decisions (default) or bulk, which allows a single decision for multiple items.

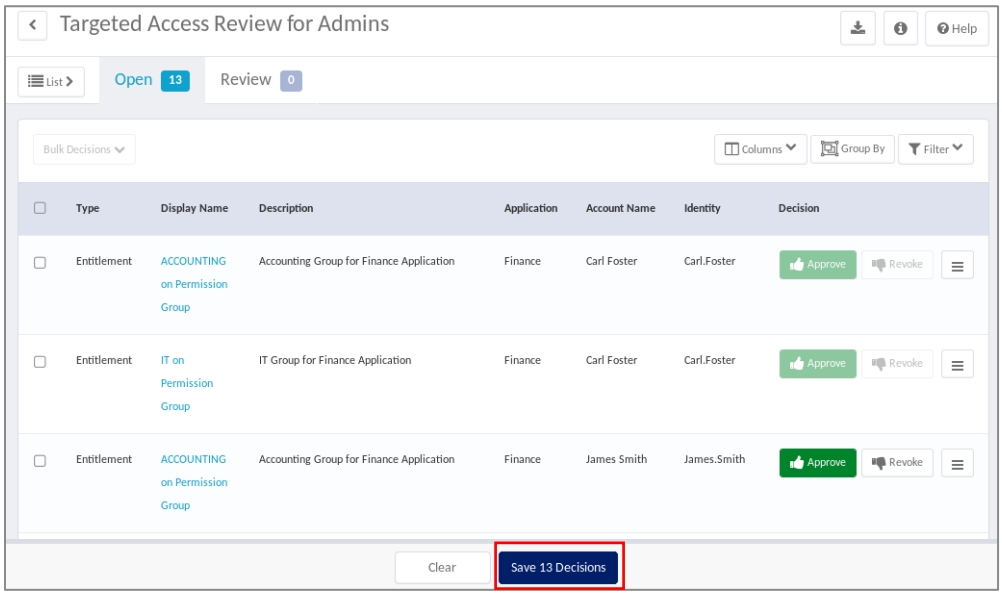
4. Use the bulk decision to approve these items:

   a. In the grey header, select the **checkbox** to the left of Type and choose **Select Everything**



b. Select **Bulk Decisions** and **approve** all items.

5. At the bottom of the page, click **Save 13 Decisions**



When Carl tries to complete this access review, he is met with errors telling him that he cannot certify his own access. The decisions Carl made for his own access are removed. In order to complete this access review, another member of the Admins workgroup will have to certify Carl's access.

6. Click **OK** on the error message and log out of IdentityIQ.

7. Log into IdentityIQ as **Walter.Henderson/xyzzy**

8. Since Walter is a member of the Admins workgroup, the access review is also available for him to take action. Identify three places where he can find the **Access Review for Admins**

   _____

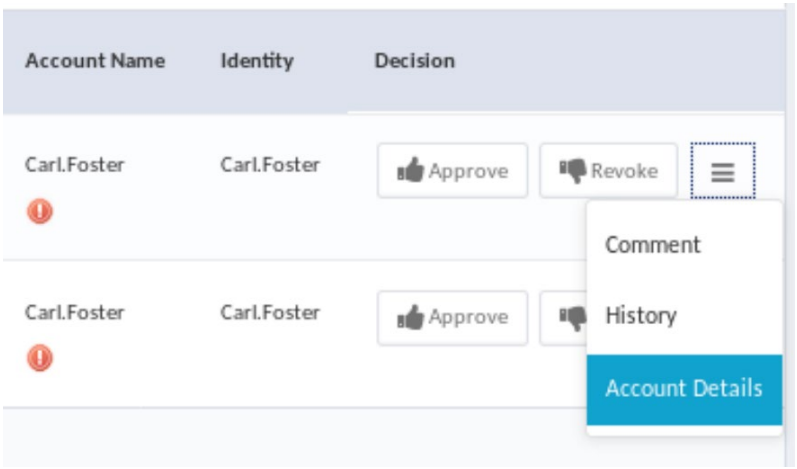
   _____

   _____

9. Click **Continue** on the **Access Review for Admins** work item from any one of the places you identified above.

   IdentityIQ displays the open items page for this access review.

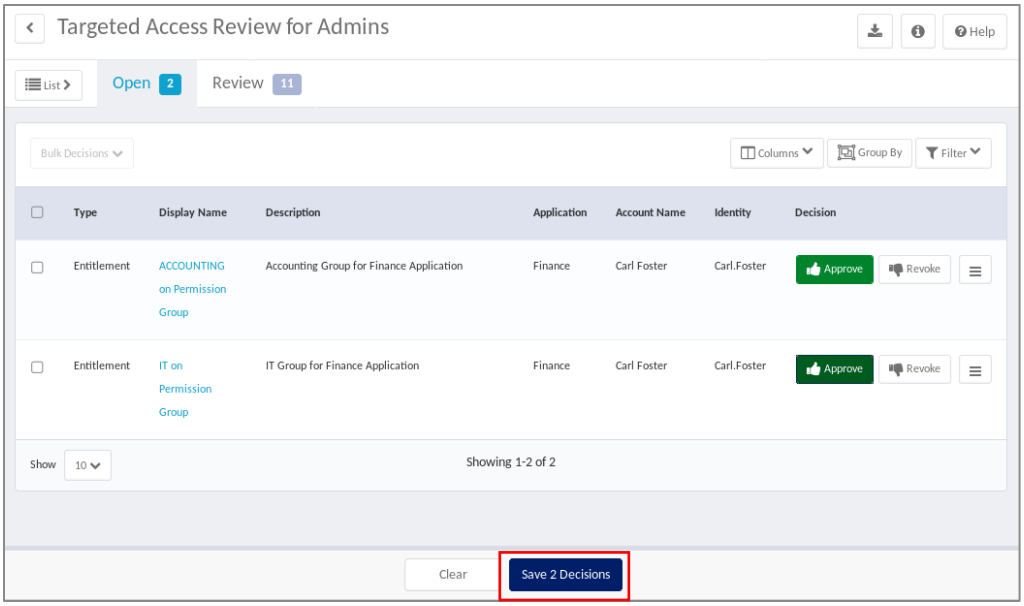
10. Click the details icon to view Carl's **Account Details** and see if you can determine why Carl's account is listed with the red privileged indicator.



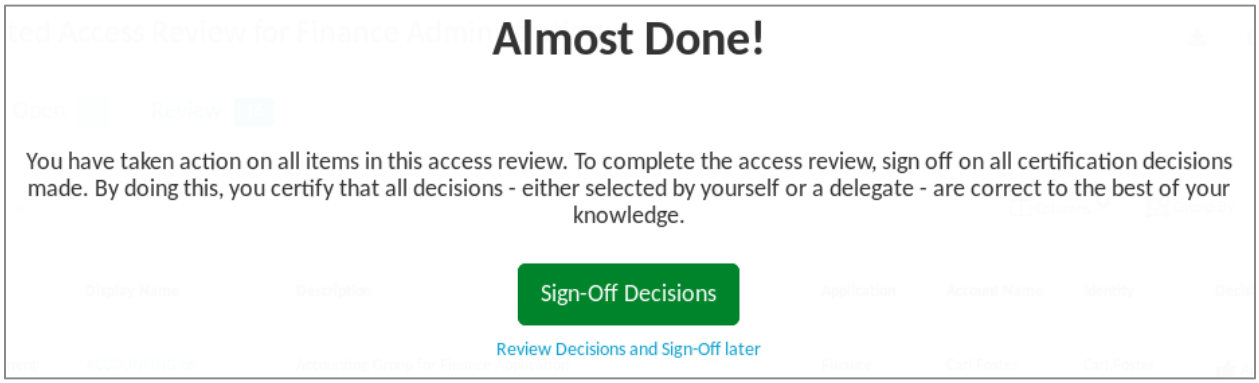
   Walter can review the open decisions for Carl or choose the **Review** page to see decisions already made.

11. Using the **Decision** buttons, **approve** both of Carl's entitlements.

12. Click **Save 2 Decisions** at the bottom of the screen.



13. Now that all decisions have been made for this access review, you can sign off on this access review. Click the **Sign-Off Decisions** button.



Monitor the Certification Progress

Certifications are automatically moved to the next phase by the standard IdentityIQ task, *Perform Maintenance*.

Since Walter has the System Administrator capability, he can review the certification's progress at any point during the certification cycle. IdentityIQ users with Auditor, Compliance Officer, or Certification Administrator capabilities can also see progress of certifications.

1. View the schedule for the **Perform Maintenance** task.

    a. When was the last completed execution of the **Perform Maintenance** task?

    _____

b. When is the next scheduled execution of the **Perform Maintenance** task?

_____

Note: This task is scheduled to run every 5 minutes. In the training environment, you will manually run the Perform Maintenance task to avoid waiting for it to run.

c. If the Perform Maintenance task has not completed since you finished the certification review, run the task manually now.

i. Navigate to the **Tasks** tab and search for the **Perform Maintenance** task.

ii. Right-click and **Execute in Background**

2. View the status of the access review.

a. Navigate to **Setup** > **Certifications** and click on the **Targeted Certification**

b. What is the **phase** for the **Targeted Access Review for Admins**?

_____

The **Perform Maintenance** task recognized that the Admins access review was completed and signed off, so it moved it to the next certification phase, revocation. The default configuration setting for Targeted Certifications is to enable a revocation period for one month.

Exercise #6: Explore Business, IT, and Birthright Roles

Objective

In this exercise, you will explore Business, IT, and Rapid Setup Birthright roles.

Overview

For this training, one of your implementation team members created the roles that you need in their sandbox environment and exported them for your use.

You will first load two types of roles: Business and IT. Business roles can be assigned to users either by matching membership criteria or through an approved access request. Business roles are linked to IT roles, which contain the entitlements that should be provisioned when somebody receives that role.

Business Roles

- Manager access

IT Roles

- Manager access for Time Tracking
- Manager access for Chat

You will manually create some, and import other, birthright roles.

Import Business and IT Roles

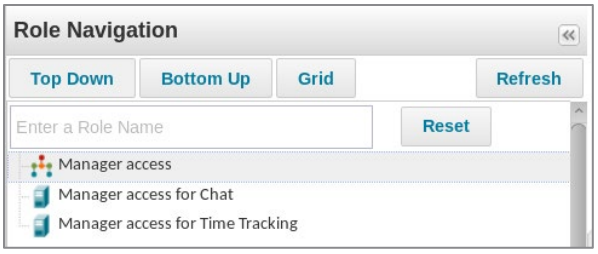
1. Log into IdentityIQ as **Carl.Foster/xyzzy**
2. Navigate to **Gear** > **Global Settings** > **Import from File** and **Import** the following file: **/home/spadmin/ImplementerTraining/config/Roles-Business and IT.xml**

Explore Business and IT Roles

1. Navigate to **Setup** > **Roles**

   Roles are listed on the **Role Viewer** page, under the **Role Navigation** panel.

   Notice the different icons. The hierarchy icon is used for Business roles, and the desktop icon is used for IT roles.



2. Select the **Manager access for Chat** IT role to view its details

   a. Scroll down to and expand (if necessary) the **Direct Entitlements** section.

      i. Which group from the **Chat** application does this IT role contain?

      _____

3. View the **Manager access for Time Tracking** IT role and scroll down to and expand (if necessary) its **Direct Entitlements** section.

   a. Which two entitlements from the **Time Tracking** application does this IT role contain?

      _____

4. View the **Manager access** business role.

5. Under **Role Information**, scroll down and view the **Assignment Rule**, **Required Roles**, and **Permitted Roles** sections – use the arrows on the far right to expand as needed.

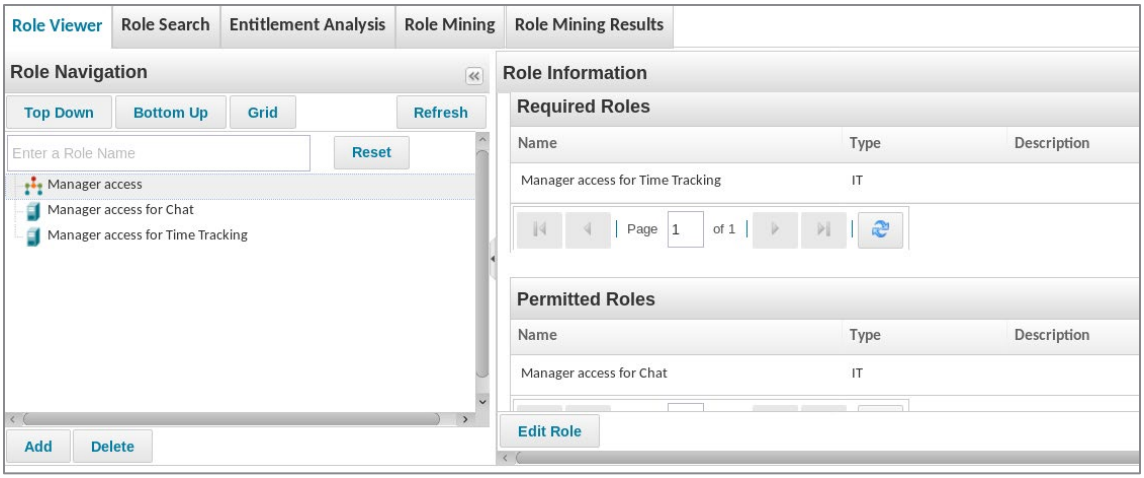
   a. Assignment Rule: _____

   b. Required Roles: _____

   c. Permitted Roles: _____

   This configuration means this role will be assigned to active identities with at least one person reporting to them within IdentityIQ. They will automatically get the Manager access for Time Tracking entitlements and they are eligible to request the Manager Access for Chat entitlements.

   Note: Requests for permitted IT role can be made at any time for a user who already has the business role, or if the permitted access can be requested at the same time the business role is requested. But unlike required roles, permitted roles' entitlements will not be auto-provisioned if the business role is assigned automatically.



Run Identity Refresh Task to Assign and Detect Roles

1. Navigate to **Setup** > **Tasks**
2. Edit the **Refresh Identity Cube** task.
3. Ensure **Refresh assigned, detected roles and promote additional entitlements** is checked

   Note: This option of the refresh identity task uses assignment rules that can be included in the business roles to assign or remove business roles to or from identities who match (or no longer match) the assignment rule. This option also detects identity cubes who hold access that matches the IT roles. You previously turned this option on to promote entitlements to a certifiable state when you were onboarding applications.
4. Click **Save and Execute**

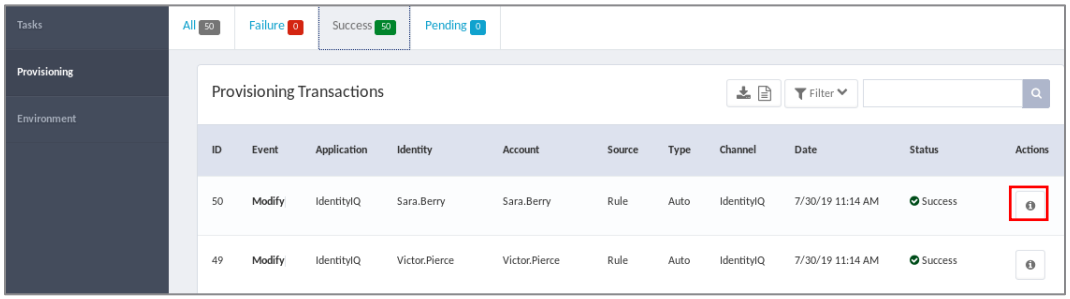
Refresh Identity Cube Attributes	
Attribute	**Value**
Identities examined	235
Managers discovered	48
Role changes	48
Extra entitlement changes	48
Policies checked	Accounts Payable and Accounts Receivable
Policy violations	1

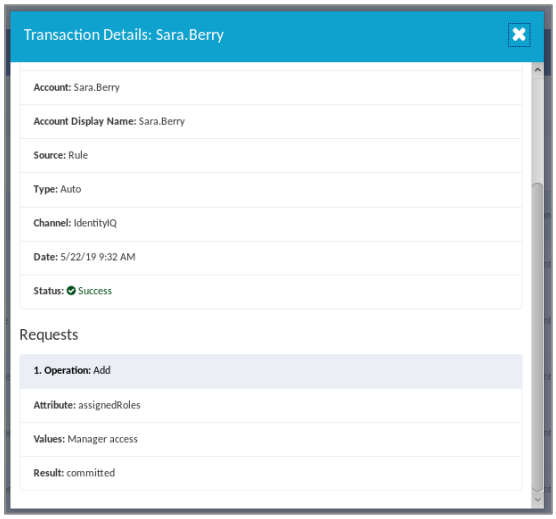
Review Provisioning Activity

1. Navigate to **Gear** > **Administrator Console** > **Provisioning** > **Success**
2. Notice the **Event** and the **Application** columns. Why does this say the application being modified is IdentityIQ?

   _____

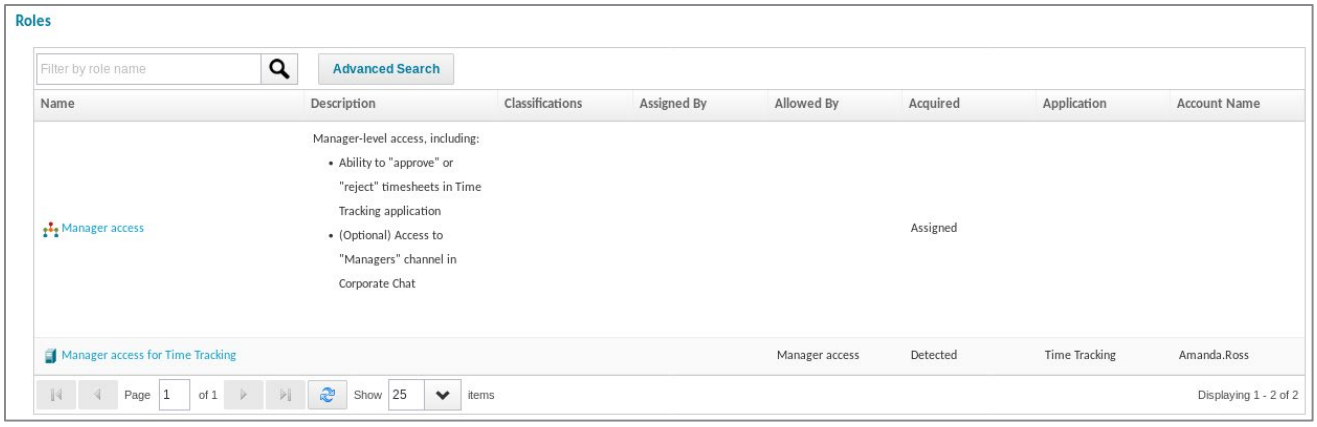
3. Click the **info** button (under Actions) to see more details.



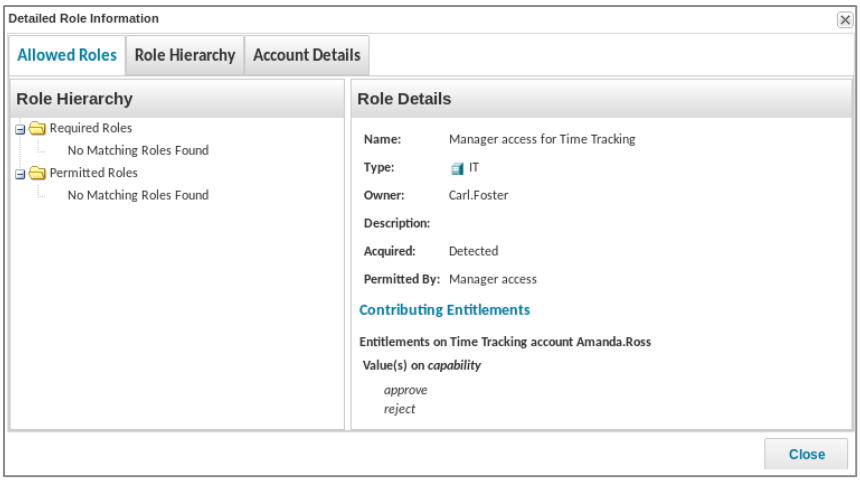


View Roles on the Identity Cube

1. Navigate to **Identities** > **Identity Warehouse**
2. Select **Amanda.Ross**
3. View her **Roles** on her **Entitlements** tab



4. Click the IT role **Manager access for Time Tracking**



a. How was this role acquired?

_____

b. Which entitlements are included in this role's entitlement profile?

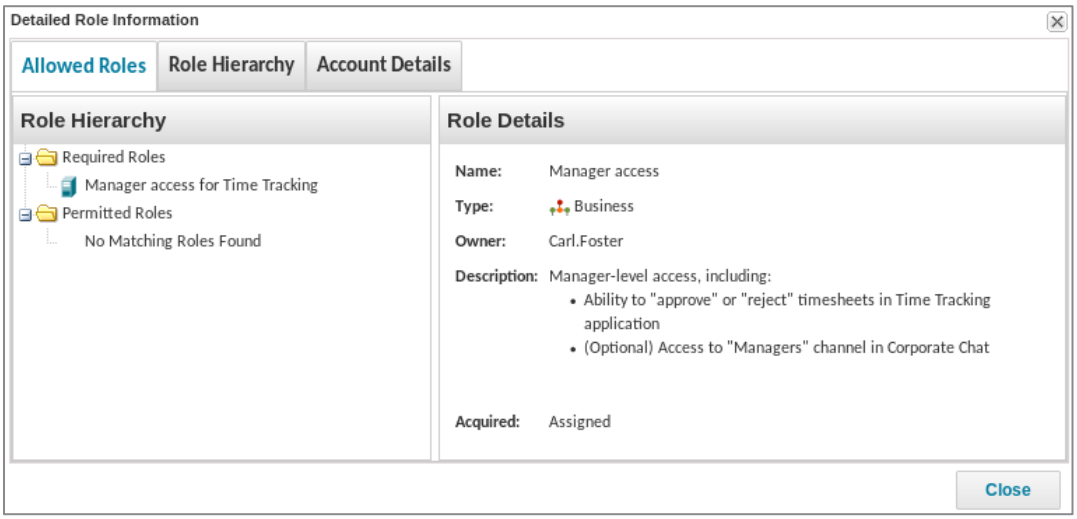
_____

c. Is this role permitted by any other roles? If so, which one(s)?

_____

Her **Manager access for Time Tracking** IT role was detected because Amanda currently has all of the entitlements included in its entitlement profile. In other words, she already has the approve and reject entitlements on the Time Tracking application.

5. Click the business role **Manager access**



   a. How was this role acquired?

   _____

   b. Does Amanda have any of the IT roles that are required or permitted by this business role? If so, which one(s)?

   _____

   c. How would you give Amanda the Manager access for Chat role, now that she has this business role assigned?

   _____

Define Birthright Roles

Birthright roles contain baseline access that should be granted to new individuals who join your organization. Note that the birthright role type is an extension to the role model added to support Rapid Setup. Without Rapid Setup, your implementation team could also extend the role model to specify a birthright role type.

In this exercise, you will define one and import five birthright roles. These roles will be assigned to identities during joiner lifecycle events in the next section.

1. Create a birthright role for the LDAP Employees group.

   a. Navigate to **Setup** > **Roles**

   b. On the top right, click **New Role** and select **Role**

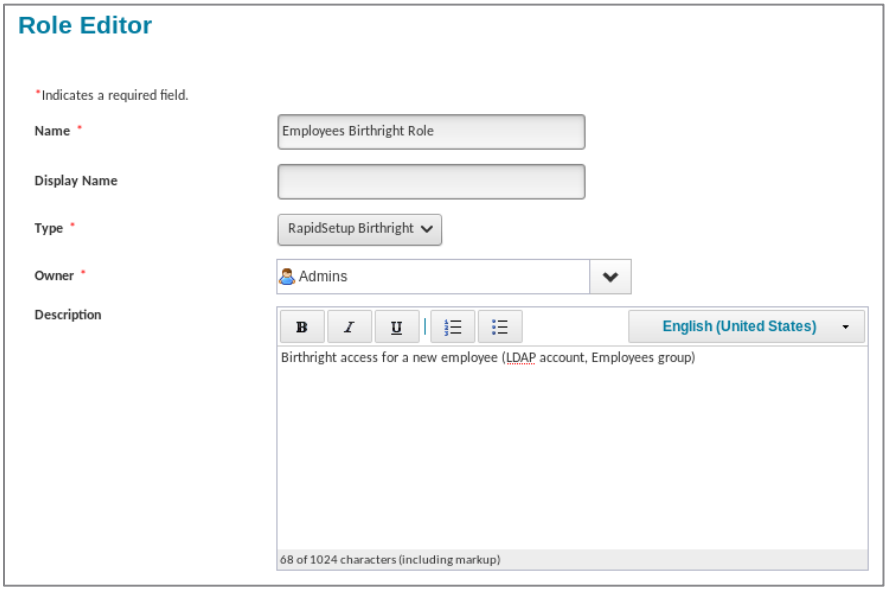
c. Configure the role as follows:

i. Name: **Employees Birthright Role**

ii. Type: **RapidSetup Birthright**

iii. Owner: **Admins**

iv. Description: **Birthright access for a new employee (LDAP account, Employees group)**



v. Assignment Rule: **Population**, **Active Employees**

Note: If this population does not appear in the list, check the "Private" and "Enabled" settings on your Populations (*Setup* > *Groups*). Remember creating this population in the *Categorize Identities* exercise? It searches for Identities with the attributes Inactive = False and Type = Employee.

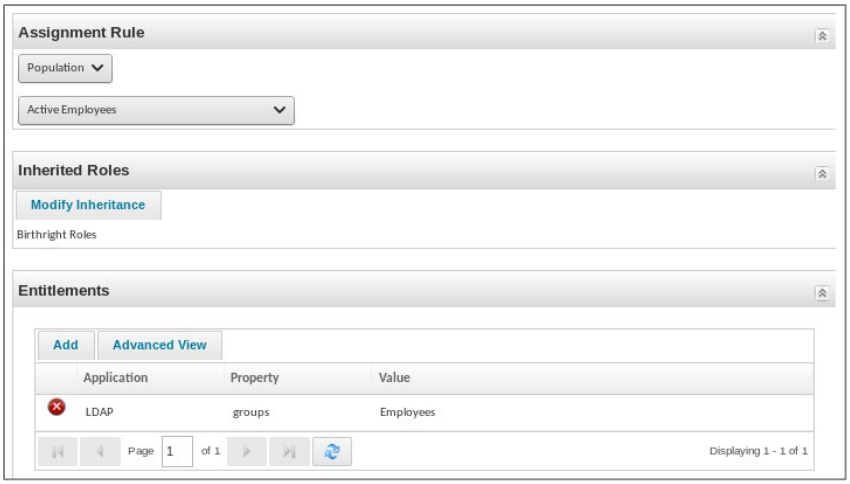
vi. Under **Entitlements**, click **Add**

(1) Select application **LDAP**

(2) Select **List of groups a user is a member**

(3) Select **Employees**

(4) **Save**



d. Click **Submit**

2. Per the role you just defined, which identities will be assigned to which group in LDAP as they join the organization?

   Identity criteria: _____

   Assigned group on the LDAP application: _____

   You will see this role in use in the next section.

3. To save time in a class environment, you will import the remaining birthright roles, for a total of six birthright roles.

   a. Navigate to **Gear** > **Global Settings** > **Import from File** and **Import** the following file: **/home/spadmin/ImplementerTraining/config/Roles-Birthright.xml**

4. **Observe** the imported roles and complete the assignment criteria and entitlements in the table below. These are the implementation's business requirements for birthright role provisioning.

Birthright Role	Membership Criteria	Entitlements
Employees Birthright Role	**Active Employees** Population • Is Inactive: False • Type: Employee	**Employees** group on **LDAP**
Contractors Birthright Role	**Active Contractors** Population • Is Inactive: False • Type: Contractor	**Contractors** group on **LDAP**
Global Birthright Role	**Global** Population • Is Inactive: False • Is Correlated: True	input capability on _____ application
Americas Birthright Role	**Americas** Population • Is Inactive: False • Region: Americas • Type: Employee	**americas_read** group on **Chat**
Asia-Pacific Birthright Role	**Asia-Pacific** Population • Is Inactive: False • Region: Asia-Pacific • Type: Employee	_____ group on **Chat**
Europe Birthright Role	_____ Population • Is Inactive: False • Region: Europe • Type: Employee	**europe_read** group on **Chat**

5. Explain the meaning of the Global population criteria: **Is Inactive: False** and **Is Correlated: True**.

   _____

Section Four:

Provisioning: Automated Actions and User Requests

IDENTITYIQ IMPLEMENTATION AND ADMINISTRATION: ESSENTIALS

SailPoint IdentityIQ Version 8.1

With Rapid Setup

www.sailpoint.com

Table of Contents

Exercise #1: Configure Applications to Support Provisioning Actions

Objective

In this exercise, you will work with the necessary configurations that support provisioning to the applications in your environment.

Overview

In this exercise, you will set up your applications to support provisioning. You will:

- Define provisioning polices
- Set provisioning rules for your JDBC applications

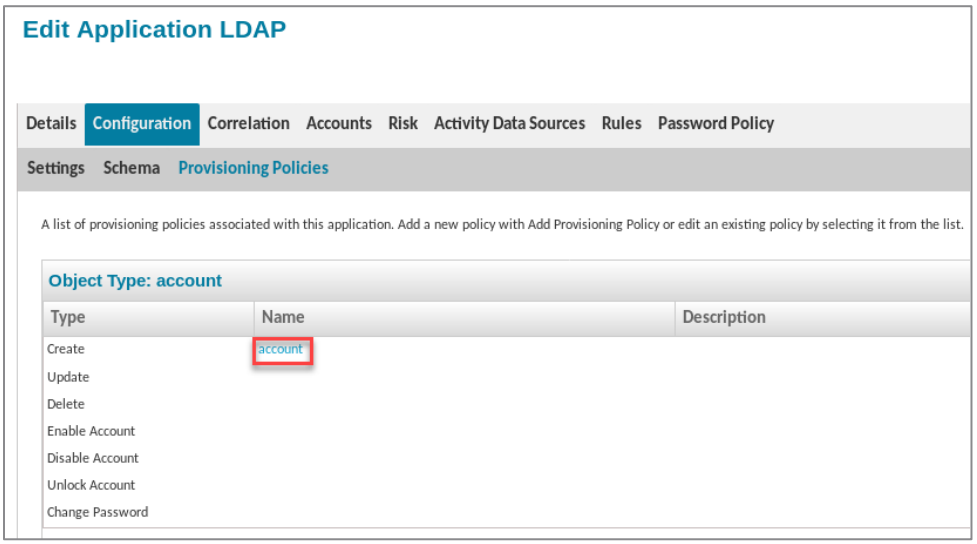
Explore the Default LDAP Provisioning Policy

Provisioning policies define the fields required by the provisioning action. For example, "create account" provisioning policies include the account attributes that are required by the native system for creating an account on that application. These forms often include default values, scripts, and rules for calculating values for these fields. When a field cannot be calculated by the system during provisioning of an account or role, it must be presented to a user through a form to get the required value.

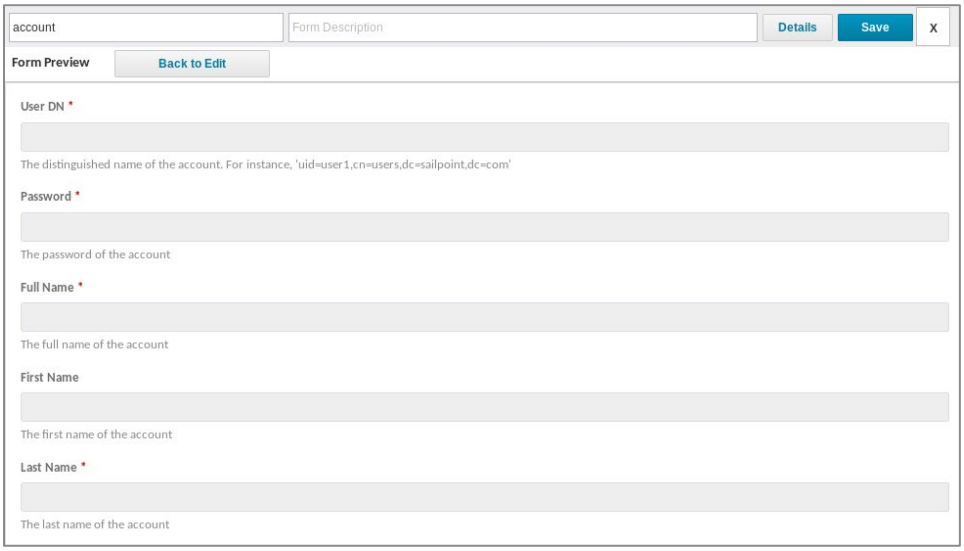
Your LDAP application is using the OpenLDAP – Direct connector, which has a few pre-defined provisioning policies. Its default "create account" provisioning policy contains five fields. None of the fields have logic for calculating values or providing allowed values. Therefore, if you were to request a new LDAP account, you would be presented with a form where you would have to input the value for each attribute.

1. Log into IdentityIQ as **Carl.Foster/xyzzy**
2. Navigate to **Applications > Application Definition > LDAP**
3. Navigate to **Configuration > Provisioning Policies**

4. Click **account**



5. Click **Preview Form** and review the default fields.



6. Click **Back to Edit**

Update LDAP's Create Account Provisioning Policy

Update LDAP's "create account" provisioning policy so it includes a new field, email, and calculates all attribute values using data from IdentityIQ. This will enable you to define an automated process where new employees and contractors who join your organization automatically get LDAP access with appropriate group membership as part of the birthright joiner event.

1. For **User DN**, click the **pencil** icon and update **Edit** options.

   Notice the **Display Name** and **Help Text** entries are mappings for the localization message catalog. These values will be replaced with the appropriate text based on the user's browser language settings. For example, the message catalog entry **con_prov_policy_ldap_user_DN** is replaced with the text **User DN** from the English language catalog, hence why the field is labeled **User DN**.

2. Expand **Value Settings**

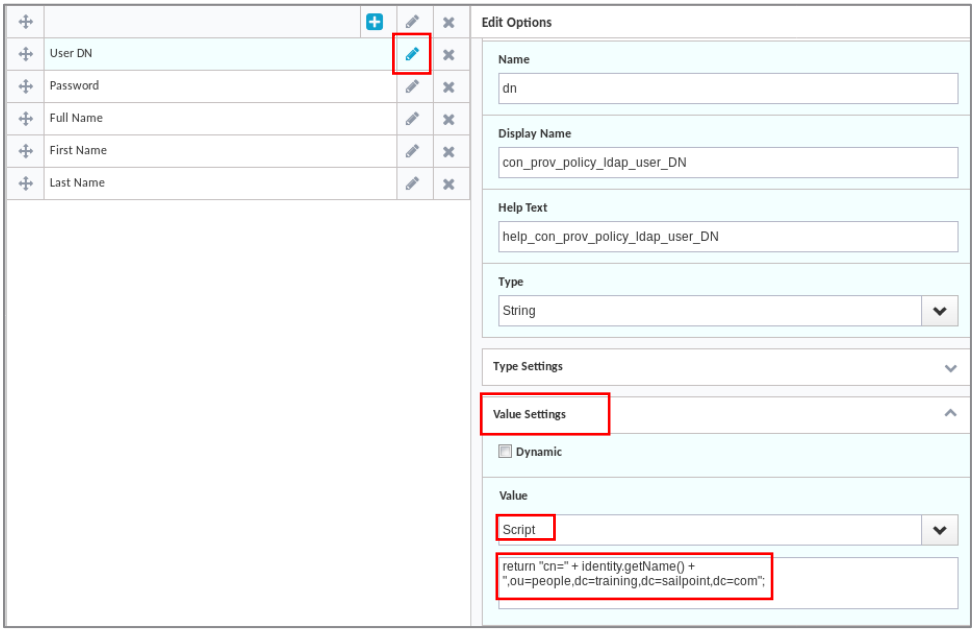
   a. For the **Value** field, select **Script**

      Note: Value: Script means you are inputting BeanShell code to calculate the value for this attribute.

   b. Enter:

      ```
      return "cn=" + identity.getName() +
      ",ou=people,dc=training,dc=sailpoint,dc=com";
      ```

      Note: The above phrase is a snippet of BeanShell code. It calculates the value of the User DN field for the given identity. For example, if the identity were Carl.Foster, the returned value would be:
      `cn=Carl.Foster,ou=people,dc=training,dc=sailpoint,dc=com`



   c. Scroll down and click **Apply.**

      Important: You must click "Apply" after editing a field. Later in this exercise, once you have completed all edits to the policy, then you will save twice: first, save the policy and then save the application definition.

After applying, you'll notice the User DN field displays a red triangle at the upper left, which indicates there are updates to the form that need to be saved:

3. Click the **pencil** icon next to **Password**
   a. Expand **Value Settings**
      i. Set Value: **Value**

      Note: Value: Value means you are inputting text that will be the string value of this attribute.

      ii. Enter:

      ```
      password
      ```

   b. Click **Apply**
4. Click the **pencil** icon next to **Full Name**
   a. Expand **Value Settings**
      i. Set Value: **Script**
      ii. Enter:

      ```
      return identity.getDisplayName();
      ```

      Note: this piece of BeanShell provides the identity's display name as the value of Full Name.

   b. Click **Apply**
5. Click the **pencil** icon next to **First Name**
   a. Expand **Type Settings**
      i. Uncheck **Review Required**
   b. Expand **Value Settings**
      i. Set Value: **Script**
      ii. Enter:

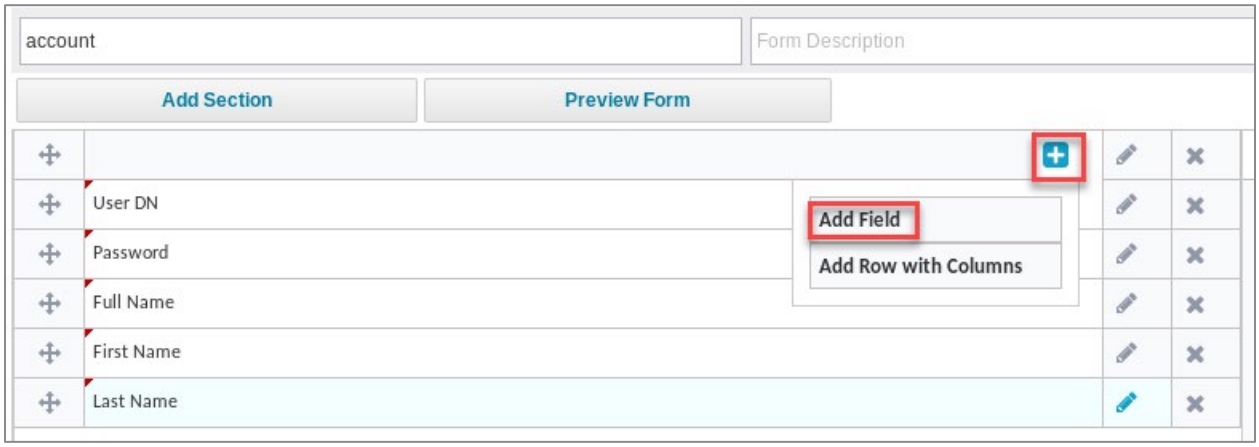
      ```
      return identity.getFirstname();
      ```

   c. Click **Apply**

6. Click the **pencil** icon next to **Last Name**
   a. Expand **Value Settings**
      i. Set Value: **Script**
      ii. Enter:

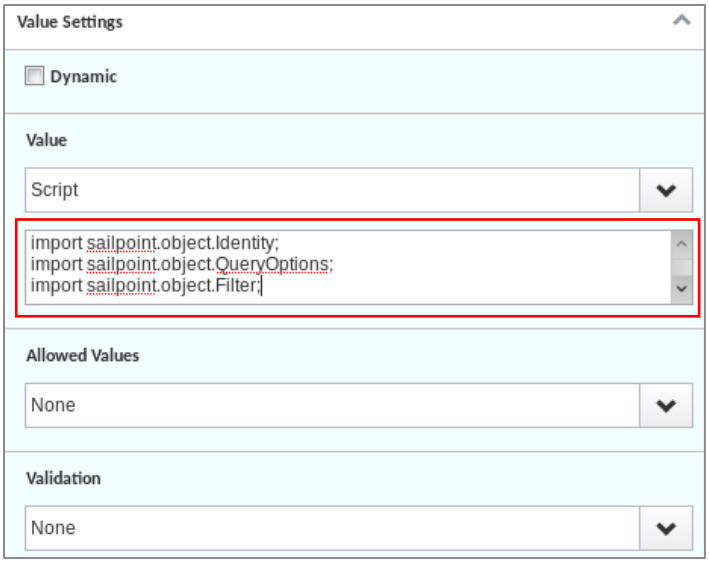
```
return identity.getLastname();
```

   b. Click **Apply**
7. Click the blue **+** button and choose **Add Field**



8. Update **Field 6**
   a. Name: **mail**
   b. Display Name: **Email**
   c. Expand **Value Settings**
      i. Set Value: **Script**
      ii. Enter text from LDAP Email Provisioning file by copying and pasting the contents from:

/home/spadmin/ImplementerTraining/beanshell/LDAP_Email_Provisioning.txt



iii. Click **Apply**

9. **Save** form.
10. **Save** application.

    Important: Remember this second save! Once you complete all edits to an application's provisioning policy, you then must save twice: first, save the policy, and then save the application definition.

Import Provisioning Policies and Add Rules for JDBC Applications

To provision with the JDBC connector, you must provide a provisioning rule and provisioning policies for each JDBC application. For the class scenario, you will import the objects created by your colleague to configure provisioning for the three JDBC applications:

- Bug Tracking
- Chat
- Time Tracking

This file includes provisioning rules and updated application definitions. All three applications now include account create provisioning policies. Two applications, Bug Tracking and Chat, include a reference for their provisioning rules. Once you've imported the Time Tracking provisioning rule, you will add it to the Time Tracking application.

1. Import the following file:
   /home/spadmin/ImplementerTraining/config/Applications_With_Provisioning.xml
2. Add the provisioning rule for the Time Tracking application.

a. Navigate to **Applications > Application Definition** and click **Time Tracking**

b. Navigate to **Rules** tab.

c. Under the **Connector Rules** section, set the following:

   i. Provision Rule Type: **Global Provision Rule**

   ii. Provision Rule: **TRNG-JDBCProvision-TimeTracking**

d. **Save** application.

Exercise #2: Define and Test Joiner Lifecycle Event

Objective

In this exercise, you will configure and test the joiner lifecycle event.

You will configure Email Templates, so emails generated by the Rapid Setup Lifecycle events are sent from IdentityIQ matching the style of your organization.

You'll use Rapid Setup to select the appropriate birthright access and provisioning actions, per application. Once you've defined the joiner event, you'll run a test to verify the provisioning actions are successful.

Overview

Lifecycle Events can be configured in IdentityIQ to represent activities that occur during the normal course of a person's employment at a company. These activities include events such as joining the company, moving within the company, and leaving the company.

When a person joins the company, they can automatically receive baseline access and accounts on a few applications. You will define this behavior through the Rapid Setup Joiner configurations.

With Rapid Setup, the configuration process consists of three steps:

- Define supporting artifacts
    - You configured populations, roles, etc. in previous exercises
    - In this exercise, you will configure Email Templates so emails sent from IdentityIQ match the style of your organization
- Define global Rapid Setup configurations, including trigger filters
- Define application-specific actions, per application

Modify and Update Rapid Setup Email Templates

Email templates can be configured to match the style of your organization. Rapid Setup email templates are designed to share a header, footer, and style sheet. By editing three template objects, all Rapid Setup emails share the updated configuration. You can optionally edit or create other email templates, used anywhere in IdentityIQ, to include these components.

IdentityIQ email templates can be created externally then imported or edited with the IdentityIQ Debug Pages. You will modify an XML file to configure your Rapid Setup emails, import the email templates and configure IdentityIQ Rapid Setup to use these templates.

1. In the file browser, use gedit to open **/home/spadmin/ImplementerTraining/config/ EmailTemplate_RapidSetup.xml**

    Note: this XML file contains three IdentityIQ email templates

2. Edit the email header.

   HTML defined in this object will be applied to the top or "header" of all IdentityIQ Rapid Setup email templates.

   a. Modify **TRNG-RapidSetup-Email-GlobalHeader**

      i. Replace: `<p>Global Header</p>`

      ii. With: `<p>Welcome to SailPoint Training</p>`

3. Edit the email footer.

   HTML defined in this object will be applied to the bottom or "footer" of all IdentityIQ Rapid Setup email templates.

   a. Modify **TRNG-RapidSetup-Email-GlobalFooter**

      i. Replace: `<p>Global Footer</p>`

      ii. With: `<p>TRNG Company Proprietary</p>`

4. Observe the third email template **TRNG-RapidSetup-Email-GlobalStyleSheet**

   This HTML Style Sheet defined in this object will be applied to all IdentityIQ Rapid Setup email templates.

```
<?xml version='1.0' encoding='UTF-8'?>
<!DOCTYPE EmailTemplate PUBLIC "sailpoint.dtd" "sailpoint.dtd">

<sailpoint>


<EmailTemplate name="TRNG-RapidSetup-Email-GlobalHeader">
  <Body>
    &lt;p&gt;Welcome to SailPoint Training&lt;/p&gt;
  </Body>
  <Subject>Global Header</Subject>
</EmailTemplate>

<EmailTemplate name="TRNG-RapidSetup-Email-GlobalFooter">
  <Body>
    &lt;p&gt;TRNG Company Proprietary&lt;/p&gt;
  </Body>
  <Subject>Global Footer</Subject>
</EmailTemplate>
```

5. **Save** the XML file.

6. Log into IdentityIQ as **Carl.Foster/xyzzy**

7. Import the updated xml file:
   /home/spadmin/ImplementerTraining/config/ EmailTemplate_RapidSetup.xml

   You could use either the **Identity Console**, or the **Global Settings > Import from File**.

8. Point the system to the new email templates.

   a. Navigate to **Gear > Global Settings > Rapid Setup Configuration**

   b. On the **Miscellaneous** page, update the Rapid Setup email templates to the implementation-specific templates.

      i. Notification Style Sheet Email Template: **TRNG-RapidSetup-Email-GlobalStyleSheet**

      ii. Notification Header Email Template: **TRNG-RapidSetup-Email-GlobalHeader**

      iii. Notification Footer Email Template: **TRNG-RapidSetup-Email-GlobalFooter**

9. **Optional**: If you want to see how these header and footer templates are added to the email messages, navigate to the Debug page and view the **EmailTemplate** called **Joiner Completed Notification**.

   a. Lines 6-11 of that template are programmatic components which retrieve the contents of the Rapid Setup email header and footer for inclusion in the email message.

   b. Lines 15-17 applies the style sheet, and lines 20-22 and 78-80 print the header and footer (respectively) into the message.

Enable and Configure Joiner Lifecycle Event

When new people join your company, they should receive birthright access on three applications. The level of access the users receive will be based on their identity data. Recall the Birthright role configuration that will support your joiner processing. Review the table below listing the implementation goals.

	Employee Access	**Contractor Access**
Time Tracking	**input** capability	**input** capability
LDAP	**Employees** group	**Contractors** group
Chat	Read entitlement based on Identity region	Account only, no additional entitlements

Define Actions for Joiner Event

The Business Analyst team in this implementation is responsible for configuring the per-application behaviors of the Joiner event. These configurations can be completed even if the event is not yet globally enabled. They will not be applied until the global configuration is enabled.

Note: All of these configurations occur under **Applications** > **Rapid Setup**

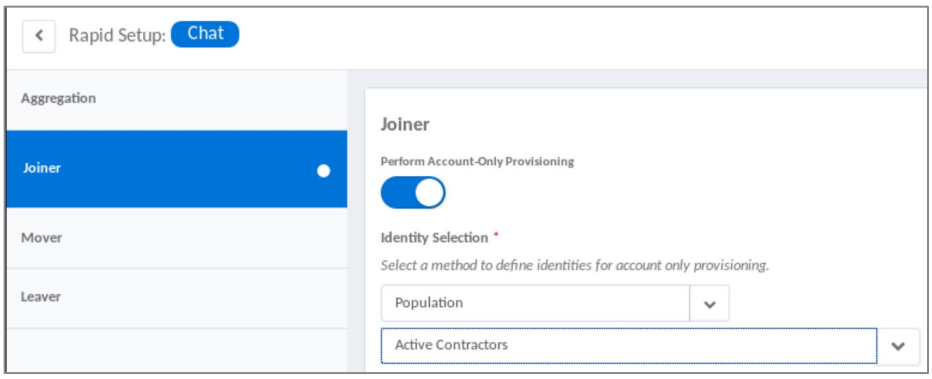
1. Sign into IdentityIQ as **Jim.Lee/xyzzy**
2. Specify both authoritative applications as sources of Joiner identities.
   a. Navigate to **Applications > Rapid Setup**
   b. Select the **HR Employees** application and click **Next**
   c. Navigate to **Joiner** page
   d. Enable **Automatically Start Joiner Processing for Newly Created Identities**
   e. Click **Save**
   f. Repeat for the **HR Contractors** application.

   Tip: You can navigate back to the application selection page within Rapid Setup by clicking the back arrow **(<)** next to Rapid Setup at the top left.

3. Users will get access to the Time Tracking application through birthright roles, but specific content needs to be added to the email message related to this application.
   a. Select the **Time Tracking** application and click **Next**
   b. Navigate to **Joiner** page
   c. Add the following text for **Joiner Email Instructions**:

   New user now has access to input their timesheet hours. Please review corporate time tracking policies in HR Manual.

   d. Click **Save**
4. Configure account-only provisioning on Chat for contractors.
   a. Select the **Chat** application and click **Next**
   b. Navigate to **Joiner** page
   c. Enable **Perform Account-Only Provisioning**
   d. In Identity Selection, select **Population : Active Contractors**



In the birthright role model, Chat access is provisioned to employees granting them read access to the channel appropriate based on their region.

5. Click **Save**

Configure Global Rapid Setup Joiner

For our installation, the Global Rapid Setup configurations have been assigned to the Operations workgroup.

1. Sign into IdentityIQ as **Tyler.Petrick/xyzzy**
2. Navigate to **Gear > Global Settings > Rapid Setup Configuration**
3. Enable joiner at the global level.
   a. On the **Joiner** page, enable **Joiner Processing**
4. Observe, and leave selected, the following settings:
   a. **Automatically Join New Empty Identities**: This setting performs joiner processing on new identities created through Lifecycle Manager (Create Identity or Self-service Registration), even though they did not come from any source application (i.e. they have no accounts anywhere).
   b. **Exclude Uncorrelated Identities**: This setting excludes identities created from non-authoritative systems from joiner processing, preventing the per-application Rapid Setup configuration from triggering joiner for non-authoritative identities.
5. Click and read the tooltip help next to **Alternative Workgroup for Joiner Completed Notification Email**
   a. Since you will not specify a workgroup here, who will receive the email sent when the Joiner process is complete?

_____

6. What is the name of the default business process provided for Joiner processing?

   _____

7. For this implementation, you want to trigger joiner for all identities created from the specified sources, so you will not specify a joiner **Trigger Filter**.

8. Review the birthright role configuration.

   a. On the **Miscellaneous** page, scroll to the bottom to review the **Role Types to Treat as Rapid Setup Birthright Roles**

      What role type is specified? _____

9. Click **Save**

Test Joiner Processing

Scenario: Sara Berry is a manager who has 2 new hires.

- Caroline Martin is a new employee in the Taipei office, Finance department. Her information has been added to your HR Employees application.
- Michael Brooks is a new contractor in the Taipei office, Accounting department. His information has been added to your HR Contractors application.

For training purposes, in this exercise, you will directly edit the authoritative sources CSV file to add the new information, simulating their addition to the actual source systems.

Then, the next time you run the **Aggregate Employees** and **Aggregate Contractors** task, you'll create new identity cubes in IdentityIQ. After aggregation, you will run an **Identity Refresh** task with the **Process events** option selected, which will trigger the joiner lifecycle events. This is the desired outcome:

User	Access
Caroline Martin	• Create her Time Tracking account, with birthright access (input entitlement) • Create her LDAP account, with birthright access (employees group) • Create her Chat account, with birthright access (asiapacific_read group)
Michael Brooks	• Create his Time Tracking account, with birthright access (input entitlement) • Create his LDAP account, with birthright access (contractors group) • Create his Chat account, with no additional entitlements

Add New Hires to IdentityIQ

1. Update the **HR Employees** CSV file.

    a. In the file browser, use gedit to open **/home/spadmin/ImplementerTraining/data/AuthEmployees.csv**

    b. Scroll to the bottom of the file.

    Caroline's information is included on the last row as a comment.

    c. **Uncomment** (by removing the //) the last line

    This simulates adding Caroline's information to the HR source.

    d. **Save** AuthEmployees.csv

11. Update the **HR Contractors** CSV file.

    e. In the file browser, use gedit to open **/home/spadmin/ImplementerTraining/data/AuthContractors.csv**

    f. Scroll to the bottom of the file.

    Michael's information is included on the last 2 rows as a comment.

    g. **Uncomment** (by removing the //) the last 2 lines

    This simulates adding Michael's information to the HR source.

    h. **Save** AuthContractors.csv

2. Aggregate Employees and Contractors.

    a. Run **Aggregate Employees** and **Aggregate Contractors** tasks as **Carl.Foster/xyzzy**

    b. Review **Task Results** and confirm that the new identities were created.

Aggregate Employees Attributes	
Attribute	**Value**
Applications scanned	HR Employees
Accounts scanned	163
Identities created	1
Identities updated	162

Aggregate Contractors Attributes	
Attribute	**Value**
Applications scanned	HR Contractors
Accounts scanned	73
Identities created	1
Identities updated	72

Run an Identity Refresh task to trigger the Joiner Lifecycle Event

The new identities are now in IdentityIQ, but you still need to kick off the business process (workflow) for the joiner event. You must run an Identity Refresh task with the **Process events** option selected to start this workflow.

1. Navigate to **Setup** > **Tasks**
2. Click **New Task** and choose **Identity Refresh** to create a new Identity Refresh task.
3. Configure the task:
    a. Name: **Refresh with Process Events**
    b. Previous Result Action: **Rename Old**
    c. Select the following:
        i. **Refresh identity attributes**
        ii. **Refresh manager status**
        iii. **Process events**
4. Click **Save and Execute**

Refresh with Process Events Attributes	
Attribute	**Value**
Identities examined	237
Managers discovered	48
Events processed	2

5. Once the task completes, review the results though **Track My Requests**.

a. Navigate to **Home > Track My Requests**

b. Click **Details** to open the event for **Caroline Martin**

c. Notice the **Request Items** and **Provisioning Engine** items

i. Optional: Compare the attributes in the Provisioning Engine section against the applications' account create provisioning policies (**Application** > **Configuration** > **Provisioning Policies**)

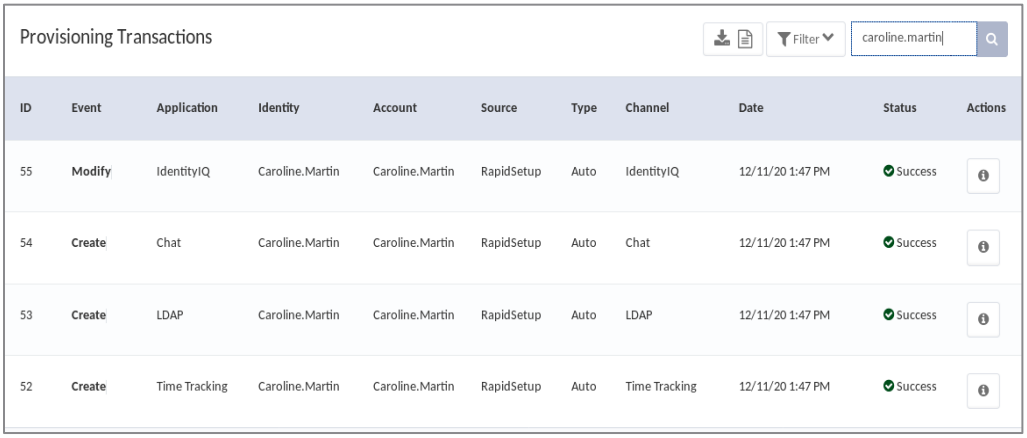
Note: Request tracking is built into the workflows used by Rapid Setup. If you use a different workflow or have a custom lifecycle event that runs a custom workflow, your implementation team must include request tracking in those workflows to see this information in Track My Requests.

6. Review provisioning activities in Administrator Console.

a. Navigate to **Gear > Administrator Console > Provisioning**

b. Filter for Identity: **Caroline Martin**

c. Explore the different **information** buttons (under **Actions**)



7. View the lifecycle event through Advanced Analytics.

a. Navigate to **Intelligence > Advanced Analytics**

b. Search Type: **Audit**

c. Click **Run Search** and observe the various audit actions.

Note: Recall that you can change which actions are audited on the **Gear > Global Settings > Audit Configuration** page.

d. Click **Refine Search** and specify action: **identityLifecycleEvent**

e. Click **Run Search**

f. View Caroline's event.

8. View the new Identity Cube.

a. Navigate to **Identities > Identity Warehouse**

b. Search for **Caroline**. Open and explore her Identity Cube.

i. Navigate to **Attributes** and view her identity attributes.

(1) Type: _____

(2) Region: _____

ii. Navigate to **Application Accounts** and view her account attributes.

(1) On what applications does she have accounts?

_____

(2) Expand her LDAP account details. Note the email address attribute value.

_____

This value got populated during account creation. Later you will see this value promoted to her identity attribute email, and we will use it in the attribute synchronization process.

iii. Navigate to **Entitlements** and view her roles and entitlements.

(1) What roles does she have?

_____

(2) What entitlements does she have on which applications?

_____

_____

iv. Navigate to **Events** and view the **Past Identity Events**

(1) Click on the access request to expand the access request details.

9. Review the same information for Michael.
    a. Type: _____
    b. Region: _____
    c. On what applications does he have accounts?

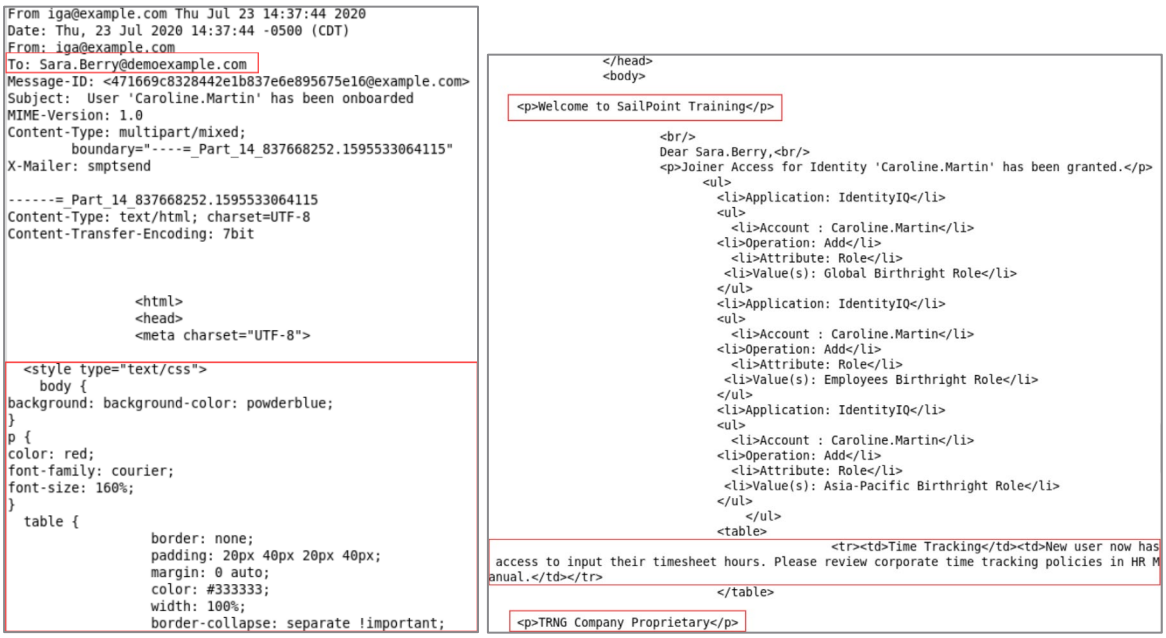
       _____
    d. What roles does he have?

       _____
    e. What entitlements does he have on which applications?

       _____

       _____
10. Check the email log.
    a. On your desktop, launch the **Tail Email Log** shortcut
    b. Confirm that you see emails sent out to the user's managers.
    c. Observe the formatting of the email.

       This email contains the email template header, footer, and stylesheet. This is being printed to a plain text file, so the markup renders "as-is". If emails were being sent through a mail server, the user's mail client could interpret the HTML tags and render the message properly.



```
From iga@example.com Thu Jul 23 14:37:44 2020
Date: Thu, 23 Jul 2020 14:37:44 -0500 (CDT)
From: iga@example.com
To: Sara.Berry@demoexample.com
Message-ID: <471669c8328442e1b837e6e895675e16@example.com>
Subject:  User 'Caroline.Martin' has been onboarded
MIME-Version: 1.0
Content-Type: multipart/mixed;
        boundary="----=_Part_14_837668252.1595533064115"
X-Mailer: smptsend

------=_Part_14_837668252.1595533064115
Content-Type: text/html; charset=UTF-8
Content-Transfer-Encoding: 7bit



                <html>
                <head>
                <meta charset="UTF-8">

   <style type="text/css">
     body {
background: background-color: powderblue;
}
p {
color: red;
font-family: courier;
font-size: 160%;
}
  table {
                    border: none;
                    padding: 20px 40px 20px 40px;
                    margin: 0 auto;
                    color: #333333;
                    width: 100%;
                    border-collapse: separate !important;
                </head>
                <body>

 <p>Welcome to SailPoint Training</p>

                        <br/>
                        Dear Sara.Berry,<br/>
                        <p>Joiner Access for Identity 'Caroline.Martin' has been granted.</p>
                              <ul>
                                <li>Application: IdentityIQ</li>
                                <ul>
                                  <li>Account : Caroline.Martin</li>
                                <li>Operation: Add</li>
                                  <li>Attribute: Role</li>
                                 <li>Value(s): Global Birthright Role</li>
                                </ul>
                                <li>Application: IdentityIQ</li>
                                <ul>
                                  <li>Account : Caroline.Martin</li>
                                <li>Operation: Add</li>
                                  <li>Attribute: Role</li>
                                 <li>Value(s): Employees Birthright Role</li>
                                </ul>
                                <li>Application: IdentityIQ</li>
                                <ul>
                                  <li>Account : Caroline.Martin</li>
                                <li>Operation: Add</li>
                                  <li>Attribute: Role</li>
                                 <li>Value(s): Asia-Pacific Birthright Role</li>
                                </ul>
                                    </ul>
                                <table>
                                                    <tr><td>Time Tracking</td><td>New user now has
 access to input their timesheet hours. Please review corporate time tracking policies in HR M
anual.</td></tr>
                                </table>

 <p>TRNG Company Proprietary</p>
```

Exercise #3: Define and Test Mover Lifecycle Event

Objective

In this exercise, you will configure and test the mover lifecycle event using Rapid Setup.

Overview

A mover lifecycle event occurs when a person moves within your company, for example, when somebody changes departments, job titles, or managers.

You must define the lifecycle triggers for your mover event. Unlike the joiner event, the mover event requires that you specify which attribute changes represent a move for your organization.

Then, you'll configure the resulting actions from a mover event.

- When anybody moves in your organization, their manager should certify they have the appropriate Finance access.
- Additionally, IdentityIQ should re-evaluate their identity cube against the joiner logic you configured earlier.

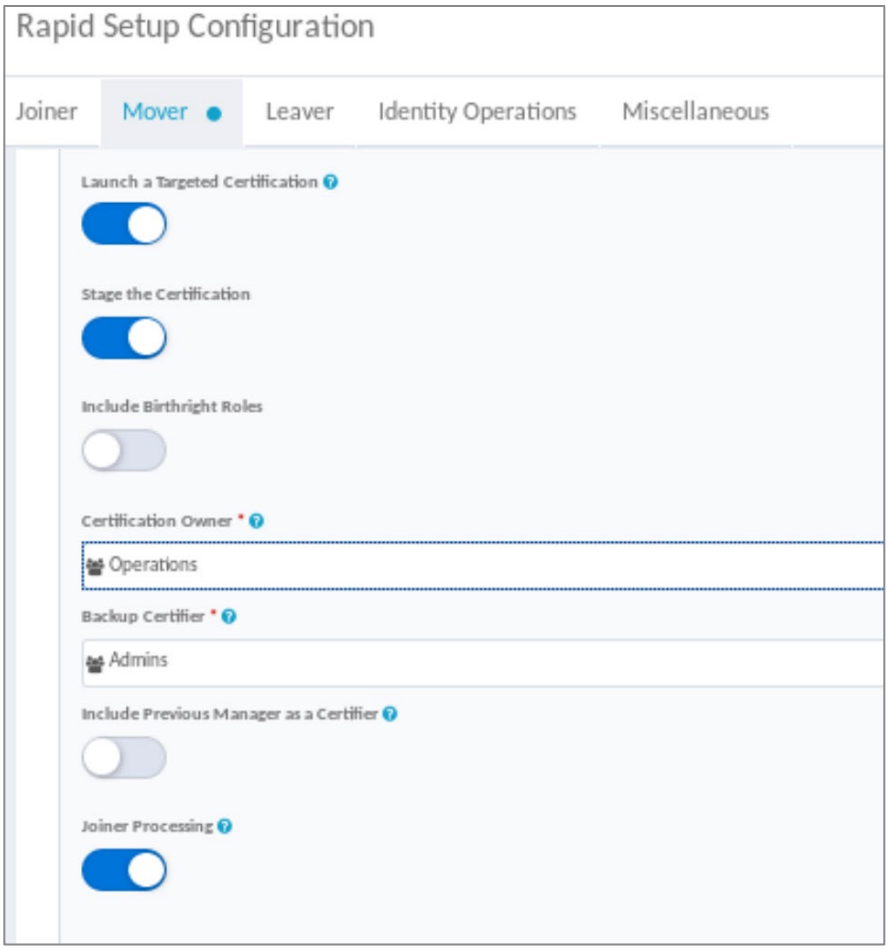
Define Mover Lifecycle Event with Rapid Setup

Since Tyler is part of the **Operations** workgroup, he has the Rapid Setup Configuration Administrator capability, so he can define the Rapid Setup global settings.

1. Log in as **Tyler.Petrick/xyzzy**
2. Navigate to **Gear > Global Settings > Rapid Setup Configuration**
3. Navigate to the **Mover** tab and choose the following options:
    a. Enable **Mover Processing**
    b. Enable **Launch a Targeted Certification**
        i. Enable **Stage the Certification**
        ii. Certification Owner: **Operations**
        iii. Backup Certifier: **Admins**

        The user's manager will be the certifier. The Admins workgroup will only get the access review if the user has no manager on record.
    c. Make sure **Joiner Processing** is enabled.
        i. This causes all birthright roles to be re-evaluated for the mover user.

Note: For any application that included a *Joiner* account-only provisioning configuration, you can choose (in the application mover configuration) whether account-only provisioning should also occur on mover.



4. Scroll down and add a **Trigger Filter**.

   The Trigger Filter for mover specifies the data change(s) or state(s) that represent the mover event. For this installation the mover requirements are:

   - Active and Correlated identities whose job title or region changes
   - Active and correlated are the criteria defined for the Global population.

   Note: This is a complex filter designed to illustrate the flexibility of the configuration options. Pay careful attention to these instructions to build it correctly.

   a. Click **Add Row** and choose **Population**

      i. Select Population: **Global**

      ii. Contains Identity

b. Click **Add Group**

i. Click **Add Row** and choose **Attribute**

(1) Select Attribute: **Job Title**

(2) String

(3) Changed

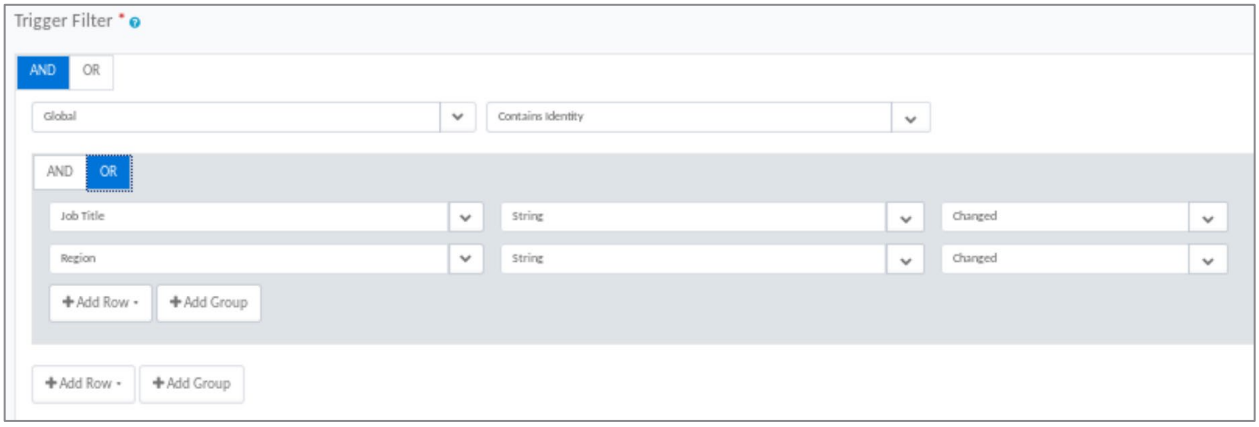
ii. Within the same group click **Add Row** and choose **Attribute**

(1) Select Attribute: **Region**

(2) String

(3) Changed

c. In the group with **Job Title** and **Region** attributes, click **OR**



This trigger defines the movers we want to watch for; Identities in the Global population [AND] whose job title OR region change. Make sure your AND OR operations are selected as specified.

5. Click **Save**

6. Recall the Global population definition.

a. Navigate to **Setup > Groups > Populations**

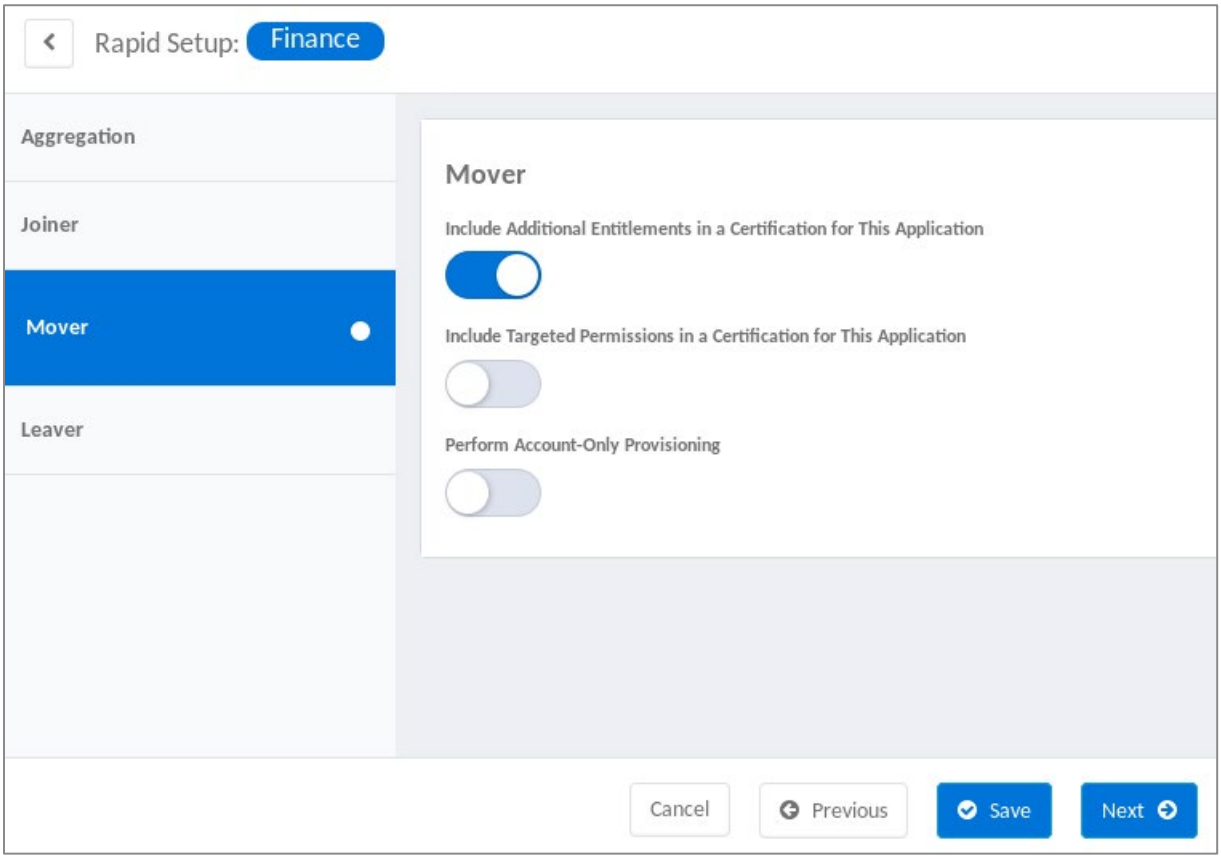
b. Open the population named **Global**

The identities matching this population definition and active authoritative identities are displayed.

Define Behavior for Mover Lifecycle Event

Globally, you configured that a certification should run. Per application, you can configure whether that application's entitlements should be included in the certification. This installation's requirement is that when somebody moves in your organization, their Manager should perform an access review to certify their Finance access is still correct.

1. Log out and back in as a member of the Business Analysts workgroup, **Jim.Lee/xyzzy**
2. Navigate to **Applications > Rapid Setup**
3. Select the **Finance** application and click **Next**
4. On **Mover** page, set:
    a. Enable **Include Additional Entitlements in a Certification for This Application**



5. Click **Save**

Test Mover Event

Scenario: Michelle Perez is taking a position in a different office, relocating from Brazil to London.

In this exercise, you will act as her manager, Elizabeth Taylor, and you will edit her details in IdentityIQ to change Michelle's region, which will trigger a Mover event. As a result, Michelle's manager will receive an access review to certify her access on the Finance application, and her joiner processing (birthright roles) will be reevaluated.

Enable editing for Region identity attribute

To allow the identity attribute changes to occur in IdentityIQ, the attribute must be made editable.

1. Log out and back in as **Carl.Foster/xyzzy**
2. Navigate to **Gear > Global Settings > Identity Mappings**
3. Select **Region** attribute
    a. Change Edit Mode: **Temporary**

    Note: The **Temporary** setting means the edited value lasts until the next time the value changes in the source, then aggregation will overwrite the value. The **Permanent** setting means that IdentityIQ becomes authoritative for identities where the attribute has been edited. It will never change through aggregation.

    b. Click **Save**

Enable Rapid Setup Debug Level Logging

You added the Rapid Setup class loggers in an earlier exercise. Now you will enable them to see the debugging information that is provided.

1. In a file browser, navigate to **/home/spadmin/tomcat/webapps/identityiq/WEB-INF/classes**
2. Use gedit to edit the **log4j2.properties** file.
3. Enable logging for the sailpoint.rapidsetup and sailpoint.workflow.RapidSetupLibrary class by removing the # characters from the front of the four lines you previously added.

```
logger.rs.name=sailpoint.rapidsetup
logger.rs.level=debug
logger.rslibrary.name=sailpoint.workflow.RapidSetupLibrary
logger.rslibrary.level=debug
```

4. **Save** the log4j2.properties file.

Edit Michelle's region

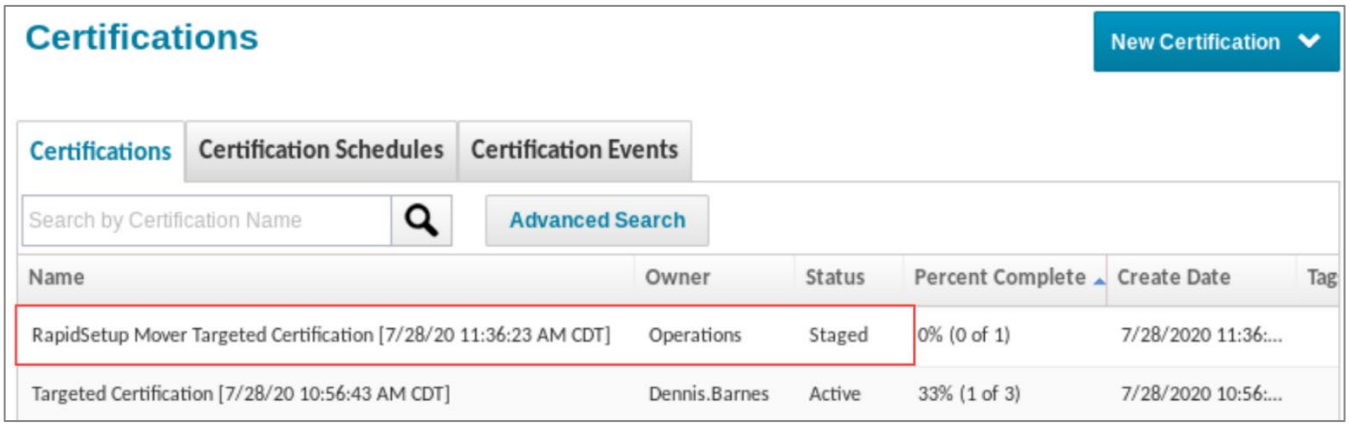
Use Lifecycle Manager - Edit Identity to edit Michelle's region attribute. As configured, this change will trigger the mover event. We will discuss this feature in more detail in a later lesson.

1. Log out and back in as Michelle's manager, **Elizabeth.Taylor/xyzzy**
2. Navigate to **Quicklink Menu > Manage Identity > Edit Identity**
3. Click **Manage** for Michelle.Perez
   a. Change Region: **Europe**
4. Click **Submit**

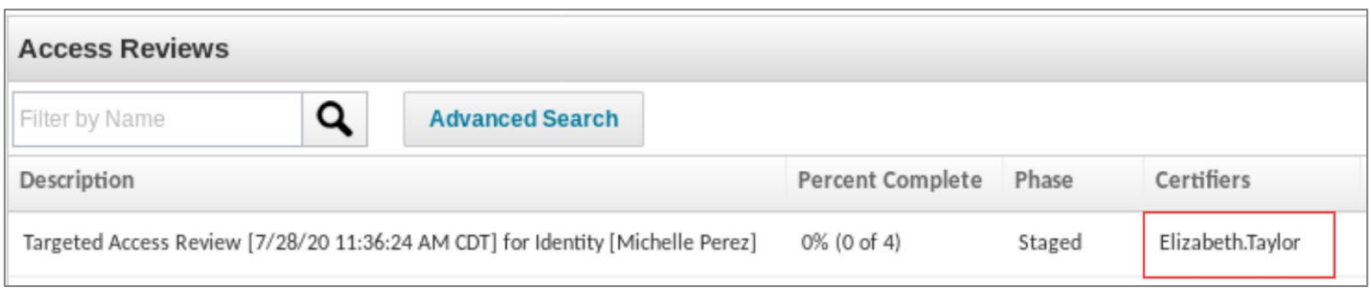
Verify Mover Processing

In the mover configuration, you specified to stage the mover certifications. This is useful for testing purposes. Once you have confirmed that mover certifications are correct, you can disable staging.

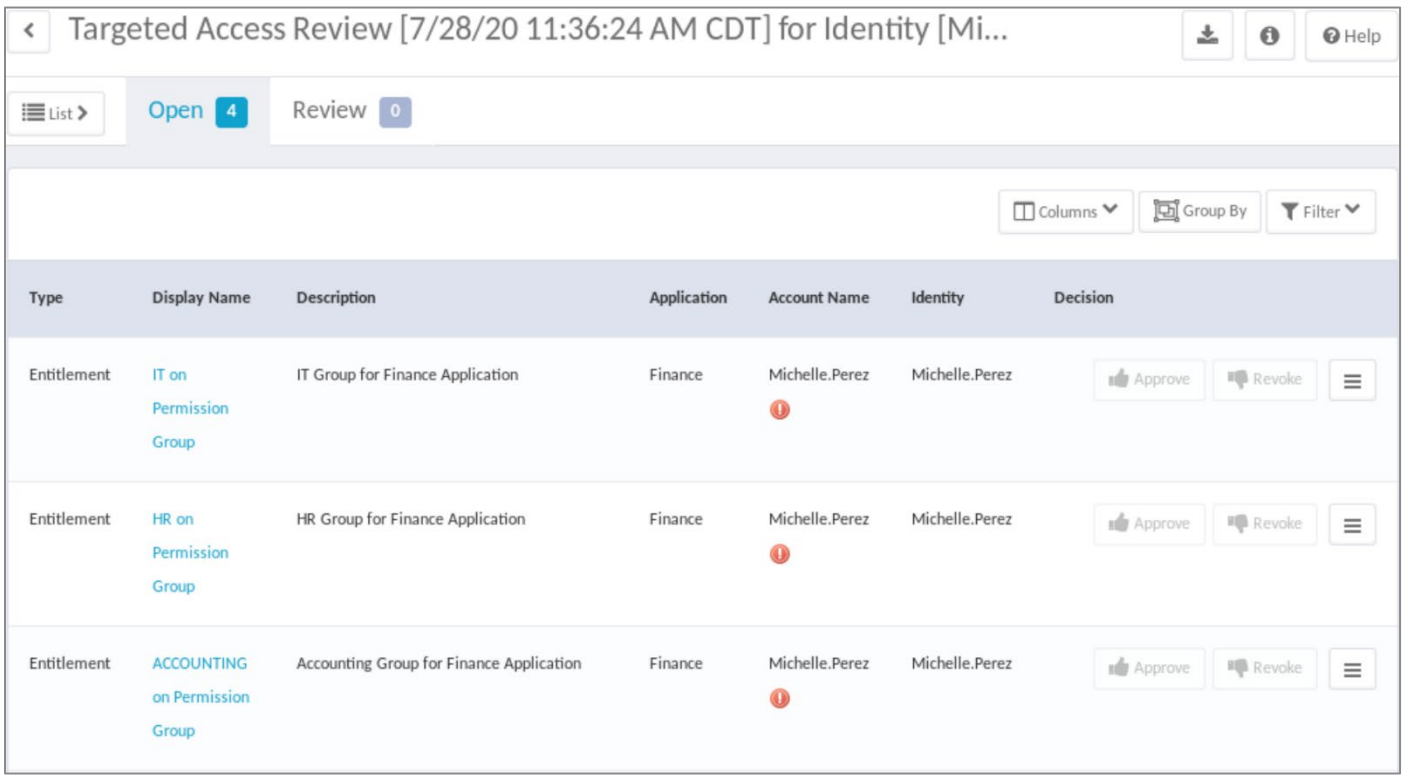
1. Log out and back in to IdentityIQ as **Carl.Foster/xyzzy**
2. Navigate to **Setup > Certifications**
3. View the **Status** column and open the **Staged** RapidSetup Mover Targeted Certification.



4. Notice the access review is assigned to Elizabeth.



5. Open the Access Review and observe the access that's included.
   - You configured mover for the Finance application to include those entitlements.
   - The default Rapid Setup certification definition template specifies automatic inclusion of any empty accounts (accounts without entitlements). That is why the HR Employees account appears in the review. If you did not want to include empty accounts, you could change that default template.



6. Navigate to **Track My Requests** to find the Lifecycle access request for Michelle and open the details.
   a. Observe that in addition to the mover certification, Michelle's joiner access was reevaluated.
   b. What access got added for her in the joiner reprocessing?

   _____

7. Navigate to **Advanced Analytics** and perform an **Audit** search.
   a. Observe the audit activity associated with Michelle's mover event.

Examine Rapid Setup Logging

1. Open the Tail IdentityIQ Log for the log file entries to view the debug level logging messages associated with the mover processing. Look for DEBUG log messages.

```
2020-07-28T11:36:16,247 DEBUG http-nio-8080-exec-5 sailpoint.rapidsetup.constraint.TriggerPredicate:42 - Evaluating lifecycleTrigger RapidSetup Joiner for pro
cess = joiner
2020-07-28T11:36:16,248 DEBUG http-nio-8080-exec-5 sailpoint.rapidsetup.constraint.TriggerPredicate:44 - Enter evaluate..Michelle.Perez
2020-07-28T11:36:16,255 DEBUG http-nio-8080-exec-5 rapidsetup.constraint.implicits.JoinerImplicitCheck:76 - rapidSetupProcessingState = null
2020-07-28T11:36:16,257 DEBUG http-nio-8080-exec-5 rapidsetup.constraint.implicits.JoinerImplicitCheck:90 - Return CANCEL_IMMEDIATELY, rapidSetupProcessingSta
te != 'needed' .. identityName..Michelle.Perez
2020-07-28T11:36:16,258 DEBUG http-nio-8080-exec-5 sailpoint.rapidsetup.constraint.TriggerPredicate:70 - Trigger RapidSetup Joiner evaluated to false for iden
tity Michelle.Perez
2020-07-28T11:36:16,259 DEBUG http-nio-8080-exec-5 sailpoint.rapidsetup.constraint.TriggerPredicate:42 - Evaluating lifecycleTrigger RapidSetup Mover for proc
ess = mover
2020-07-28T11:36:16,259 DEBUG http-nio-8080-exec-5 sailpoint.rapidsetup.constraint.TriggerPredicate:44 - Enter evaluate..Michelle.Perez
2020-07-28T11:36:16,262 DEBUG http-nio-8080-exec-5 rapidsetup.constraint.implicits.MoverImplicitCheck:31 - Return CONTINUE
2020-07-28T11:36:16,278 DEBUG http-nio-8080-exec-5 sailpoint.rapidsetup.constraint.ConstraintContext:81 - START -> [ type='Group' booleanOperation='AND' items
<nested>]
2020-07-28T11:36:16,280 DEBUG http-nio-8080-exec-5 sailpoint.rapidsetup.constraint.ConstraintContext:81 - START -> [ type='Population' attributes='{population
Value={contains=true, displayName=Global, id=7f00000173951cb481739595981e0032}}']
2020-07-28T11:36:16,296 DEBUG http-nio-8080-exec-5 rapidsetup.constraint.impl.PopulationEvaluator:103 - Enter filterGd..(correlated == true && inactive == fal
se)..
2020-07-28T11:36:16,298 DEBUG http-nio-8080-exec-5 rapidsetup.constraint.impl.PopulationEvaluator:109 - Enter isMemberOf ops..Filters: Filter [1] == (id == "7
f00000173781de68173782d59f7005e" && (correlated == true && inactive == false))
, Scope extensions: none defined,scope results [null],unscoped globally accessible [null],Ordering ==[],Group by == [],Query [null],ResultLimit [0],First Row
[0],Distinct [false],Cache results [false],Flush before query [false]
2020-07-28T11:36:16,305 DEBUG http-nio-8080-exec-5 sailpoint.rapidsetup.constraint.ConstraintContext:88 - COMPLETE (result=true) -> [ type='Population' attrib
utes='{populationValue={contains=true, displayName=Global, id=7f00000173951cb481739595981e0032}}']
2020-07-28T11:36:16,306 DEBUG http-nio-8080-exec-5 sailpoint.rapidsetup.constraint.ConstraintContext:81 - START -> [ type='Group' booleanOperation='OR' items<
nested>]
2020-07-28T11:36:16,308 DEBUG http-nio-8080-exec-5 sailpoint.rapidsetup.constraint.ConstraintContext:81 - START -> [ type='Attribute' attributes='{attributeVa
lue={property=jobtitle, operation=Changed}, dataType=String, coercedType=String}']
2020-07-28T11:36:16,313 DEBUG http-nio-8080-exec-5 sailpoint.rapidsetup.constraint.ConstraintContext:88 - COMPLETE (result=false) -> [ type='Attribute' attrib
utes='{attributeValue={property=jobtitle, operation=Changed}, dataType=String, coercedType=String}']
2020-07-28T11:36:16,314 DEBUG http-nio-8080-exec-5 sailpoint.rapidsetup.constraint.ConstraintContext:81 - START -> [ type='Attribute' attributes='{attributeVa
lue={property=region, operation=Changed}, dataType=String, coercedType=String}']
2020-07-28T11:36:16,316 DEBUG http-nio-8080-exec-5 sailpoint.rapidsetup.constraint.ConstraintContext:88 - COMPLETE (result=true) -> [ type='Attribute' attribu
tes='{attributeValue={property=region, operation=Changed}, dataType=String, coercedType=String}']
2020-07-28T11:36:16,318 DEBUG http-nio-8080-exec-5 sailpoint.rapidsetup.constraint.ConstraintContext:88 - COMPLETE (result=true) -> [ type='Group' booleanOper
ation='OR' items<nested>]
2020-07-28T11:36:16,318 DEBUG http-nio-8080-exec-5 sailpoint.rapidsetup.constraint.ConstraintContext:88 - COMPLETE (result=true) -> [ type='Group' booleanOper
ation='AND' items<nested>]
2020-07-28T11:36:16,332 DEBUG http-nio-8080-exec-5 sailpoint.rapidsetup.constraint.TriggerPredicate:59 - Check process joiner, which is higher precedence than
```

2. What analysis are these statements reporting?

   _____

3. Using gedit, replace the # on the four lines to disable logging the **`sailpoint.rapidsetup`** and **`sailpoint.workflow.RapidSetupLibrary`** in the **log4j2.properties** file.

   ```
   #logger.rs.name=sailpoint.rapidsetup
   #logger.rs.level=debug
   #logger.rslibrary.name=sailpoint.workflow.RapidSetupLibrary
   #logger.rslibrary.level=debug
   ```

4. **Save** and close the **log4j2.properties** file.

Exercise #4: Configure Access Requests

Objective

In this exercise, you will configure the appropriate access request and approval settings for your environment.

Overview

IdentityIQ provides users with a quick and easy way to request access for both themselves and for others.

A submitted request will be used as input to a business process, creating a workflow case for each user with appropriate approval steps, and will eventually (assuming all approvals are affirmative) result in provisioning of the access. In this exercise, you'll set up your environment to prepare for access requests, including:

- Specifying which entitlements are requestable
- Allowing users to attach documents to access requests
- Modifying the default approval process

Update Entitlements

Within the Entitlement Catalog, you can change which entitlements and groups are requestable through Lifecycle Manager. You can also add descriptions to help users understand the access and specify owners to assign oversight responsibilities.

1. Log in as **Carl.Foster/xyzzy**
2. Make the VPN entitlement requestable.
    a. Navigate to **Applications > Entitlement Catalog**
    b. Search for and click **VPN** to edit this entitlement:

    Note: Since this entitlement is from the LDAP application, its default status is "not requestable." Earlier you used Rapid Setup to onboard LDAP, and you specified that its entitlements cannot be requested. While this is true for most LDAP entitlements, you'd like for users to be able to request VPN access.

        i. Requestable: **Checked**
        ii. **Save** the entitlement.
3. Update an entitlement's description and owner.
    a. In the Entitlement Catalog, search for **Bug**

b. Select the **user** entitlement on **Bug Tracking** to edit this entitlement:

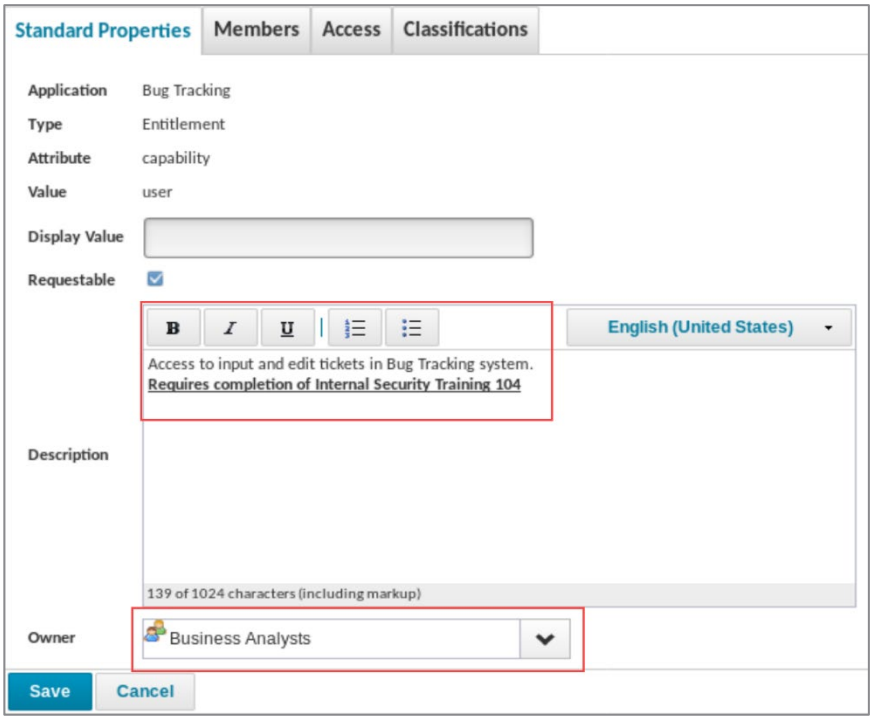
i. Description: **Access to input and edit tickets in Bug Tracking system. Requires completion of Internal Security Training 104**

ii. Use the description editor to make the 2nd sentence bold and underlined.

iii. Owner: **Business Analysts**

(1) How does IdentityIQ use entitlement owner information?

_____



iv. **Save** entitlement.

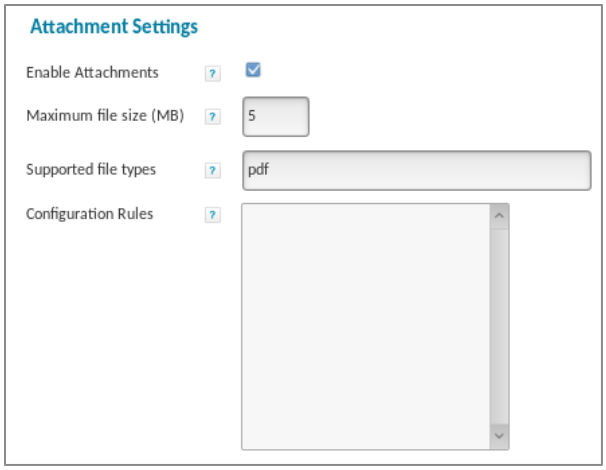
Enable Attachments on Access Requests

IdentityIQ's attachments feature enables users to add attachments to single-user access requests. For example, you could attach a training certificate or a document of authorization to a request.

1. Navigate to **Gear > Global Settings > IdentityIQ Configuration > Miscellaneous**
2. Scroll to **Attachment Settings** and select **Enable Attachments**

   For this implementation, the only attachment users ever need to provide is a training completion certificate, which will always be a PDF.

3. Update the **Supported file types**: delete the three current types and add **pdf**



4. **Save** settings.

Modify Approval Process for Access Requests

In your training environment, IdentityIQ currently has the default Lifecycle Manager approval configuration. The implementation requires requests to be first approved by the identity's manager, followed consecutively by the requested item's owner. These requirements can be implemented by simple changes in the IdentityIQ business process configuration.

1. Clone the LCM Provisioning business process to create your own new copy that you will modify.

   a. Navigate to **Setup > Business Processes**

   b. Choose **LCM Provisioning** from the list of existing processes.

   c. On the bottom right, select **Save As**

   d. Name your process **TRNG LCM Provisioning** and click **OK**

   Note: This cloning operation is a recommended practice both to provide clarity that you have modified the default workflow configuration in some way *and* to ensure any changes you make won't be overwritten on upgrade by a new version of the default workflow.

2. Modify the approval configuration.

   a. Select **TRNG LCM Provisioning** from the list of existing processes.

   b. Navigate to the **Process Variables** tab

c. Examine the form. What is the default approval configuration (**Approvers** value) displayed?

_____

d. Click the **Advanced View** button.

Note: The "Basic View" presents a user-friendly form and displays some but not all of the variables you need to modify. The Advanced View displays them all.

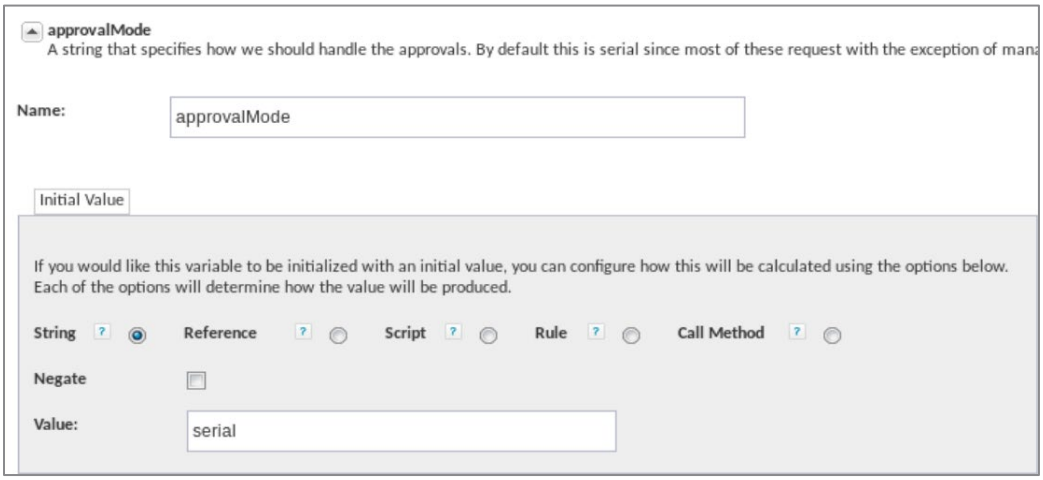
e. Scroll down to and click on the **approvalMode** variable to expand it.

i. Read the variable description. The approvalMode variable controls how the business process handles generated approval items.

ii. What are the valid values for approvalMode?

_____

iii. In the initial value box, set Value: **serial**



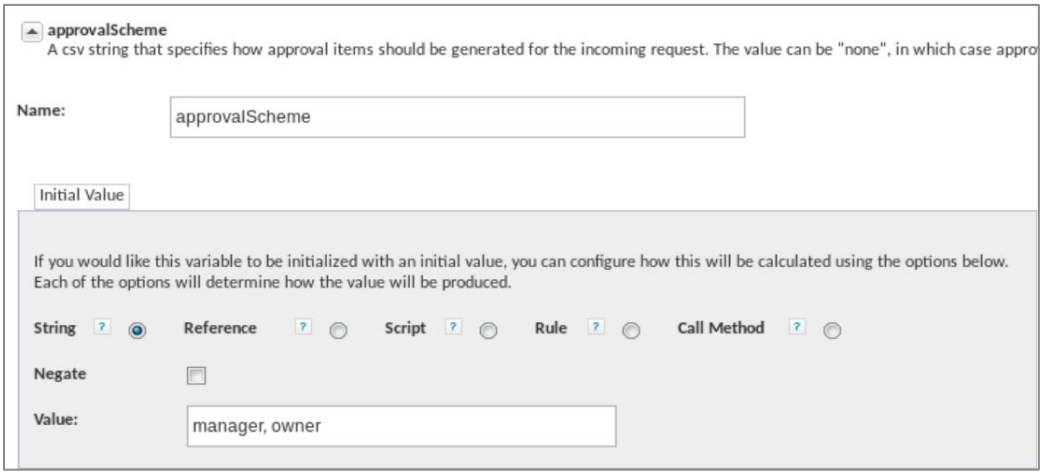
f. Scroll down to and click the **approvalScheme** variable to expand it.

i. Read the variable description.

ii. What does the **approvalScheme** variable control?

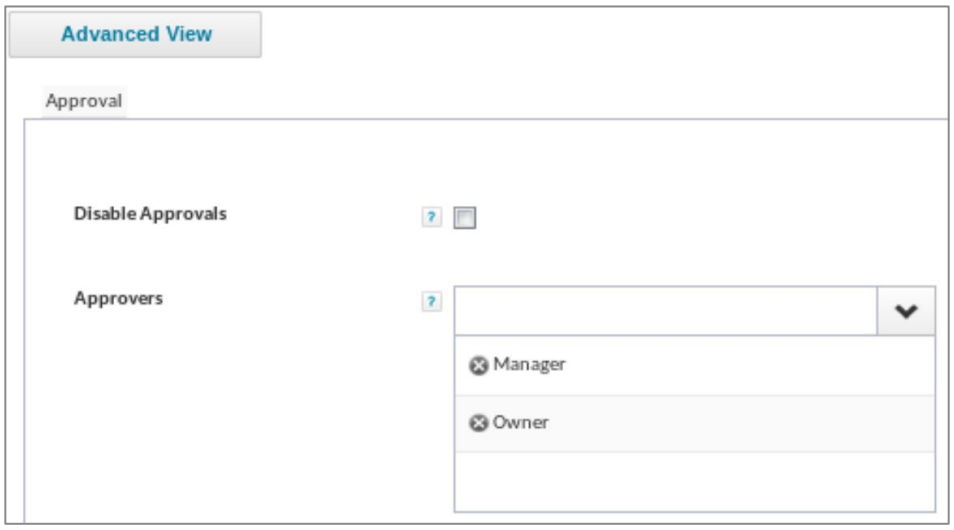
_____

iii. In the initial value box, set Value: **manager, owner**



g. Scroll back up and click **Basic View**.

h. Verify the Approvers are listed in order as Manager, Owner.



i. Based on what you see here, which process variable is being rendered as "Approvers" in this form?

_____

i. **Save** your updates to the TRNG LCM Provisioning workflow.

3. Configure Lifecycle Manager to use your configured workflow.

a. Navigate to **Gear > Lifecycle Manager**

b. Navigate to the **Business Processes** tab.

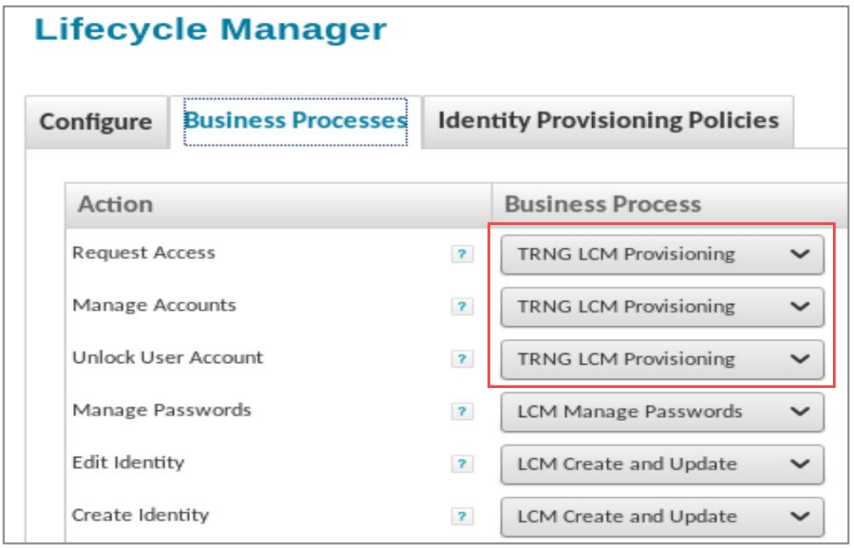
c. Replace these instances of LCM Provisioning with your custom business process. Update the business process for the following LCM actions:

   i. Request Access: **TRNG LCM Provisioning**

   ii. Manage Accounts: **TRNG LCM Provisioning**

   iii. Unlock User Account: **TRNG LCM Provisioning**

   Note: You could also replace the others (i.e. the Batch process related entries), but this is unnecessary since we won't be executing batch requests in this class. See Lifecycle Manager Business Process Selection hints at the end of this exercise for more details.



4. **Save** your changes.

Modify User Access to Lifecycle Manager Functions

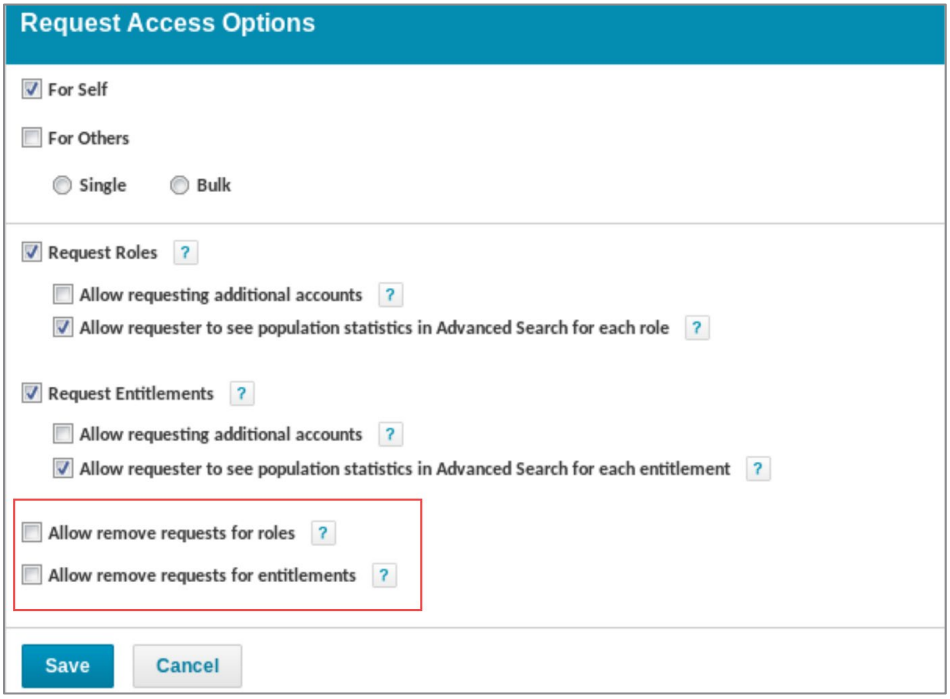
This implementation will not use IdentityIQ for user password change requests on managed applications. You will remove the Manage Passwords Quicklink from all LCM Quicklink Populations. Then you will limit other functions for specific Quicklink Populations.

1. Observe the default LCM Quicklinks by clicking on list menu icon  .
2. Expand the Quicklink category **Manage Access** observe the **Manage Passwords** Quicklink.
3. Expand the Quicklink category **Manage Identity** observe the **Create Identity** Quicklink.

By default, all Quicklink Populations have access to the Manage Passwords and Create Identity Quicklinks.

4. Navigate to **Gear > Global Settings > Quicklink Populations**

5. Disable Manage Passwords for the Help Desk Quicklink Population.
   a. Click the **Help Desk** Quicklink Population.
   b. Click the Quicklinks tab for the **Help Desk** Quicklink Population.
   c. Uncheck **Manage Passwords**.
   d. Click **Save** to save the changes to the Quicklink Population.
6. Repeat the steps above to disable Manage Passwords for **Manager** and **Self Service** Quicklink Populations.
7. Disallow the Help Desk to create identities.
   i. Click the **Help Desk** Quicklink Population.
   ii. Disable the **Create Identity** Quicklink and **Save**
8. Prevent users from requesting removal of roles or entitlements from their own identities.
   i. Click the **Self Service** Quicklink Population.
   ii. Click **configure** on the **Request Access** Quicklink and uncheck these options:
      (1) Allow remove requests for entitlements
      (2) Allow remove requests for roles



iii. Click **Save** to save the Request Access Options.

iv. Click **Save** to save the changes to the Quicklink Population

Note: Quicklink access changes are calculated at login, so these changes will not be reflected in the interface until you sign back in. You will see the effect of these configuration changes in later exercises.

Disable Full Text Search

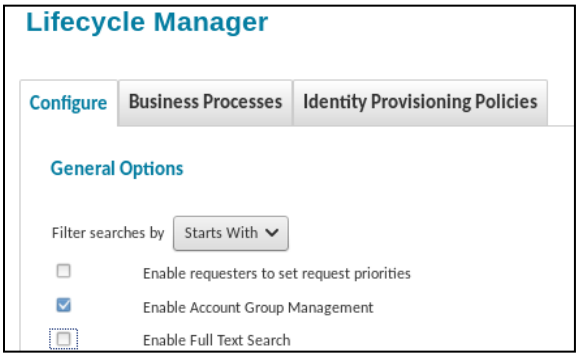
The Full Text Index enables searching across a broad array of attributes but also requires a scheduled process to update its index. Since you are in a testing environment and are updating configurations frequently, it can be helpful to temporarily disable reliance on that index for searching in LCM. This is particularly important if you are using the lab reset tool to jump around.

1. In IdentityIQ as **Carl.Foster/xyzzy** navigate to **Gear** > **Lifecycle Manager** > **Configure**

   a. What is the default refresh interval for the full text search indexes? _____

   With full text search enabled, your entitlement edits will be available for searching when the index is updated (hourly).

2. Disable full text search: uncheck the box next to **Enable Full Text Search**



3. Click **Save**

   Notes:

   - Disabling full text search allows you to use the database search rather than the full text search for your development testing of access requests. With the database search, updated entitlements and roles are immediately searchable. With the full text search, the indexes must be updated prior to searching for updated entitlements and roles. When development is complete, enable full text search for faster and more thorough searching (unlike database search, full text search includes descriptions).

   - An alternative to disabling full text search is to run the *Full Text Index Refresh* task to force the indexes to update.

Lifecycle Manager Business Processes Selection

When you created the TRNG LCM Provisioning workflow with modified approval processes you configured globally which LCM Quicklinks will launch this workflow. You may have noticed that there are additional LCM Quicklinks that use the LCM Provisioning workflow that you did not update, specifically Batch Request Access and Batch Manage Accounts.

Because LCM allows this granular control of what workflow is launched via a Quicklink, you can have different process details for batch request than you may require for user requests. For example, if you wanted to skip all notifications for batch requests you could create an additional copy of LCM Provisioning with the notifications disabled, and then specify this new workflow for the Batch Request Access Quicklink.

If you wanted batch requests to follow the same flow as user requests, you could specify the same workflow.

Exercise #5: Test Access Requests

Objective

In this exercise, you will perform a variety of tests to confirm your provisioning and access request configurations are correct.

Overview

This exercise contains several tests that explore different access request and provisioning scenarios. Note that these scenarios do not have dependencies on each other, but you may notice small changes in output results if you work them out of order.

- Retry Provisioning
- Access Request with Attachments
- Preventive Policy and Multi-Step Approvals
- Request Permitted IT Roles
- Explore Provisioning Policy for Creating Identities

LDAP Retry Configuration

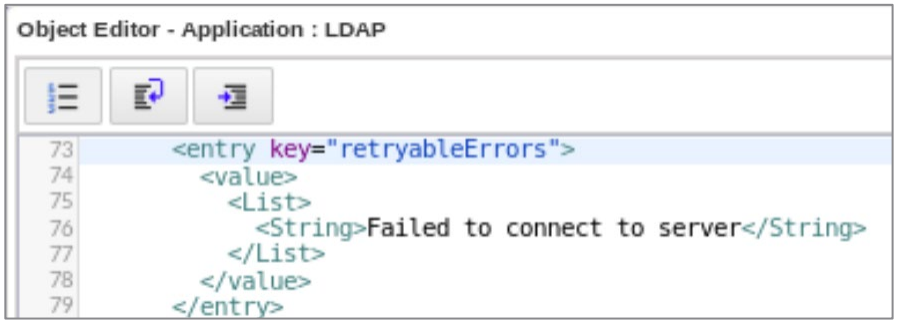
In the earlier exercise *Configure Applications to Support Provisioning Actions*, you imported an update to the LDAP application to enable the retry of provisioning transactions to LDAP that have failed with known errors. This is an XML-only configuration that can be specified on any application.

1. View the LDAP application configuration to support retries.

   a. In IdentityIQ as **Carl.Foster/xyzzy**, navigate to the **Debug Pages**

   b. Use the Object Browser to view the LDAP application.

   c. Search for the attribute entry **`retryableErrors`** and observe the list of retryable error messages.



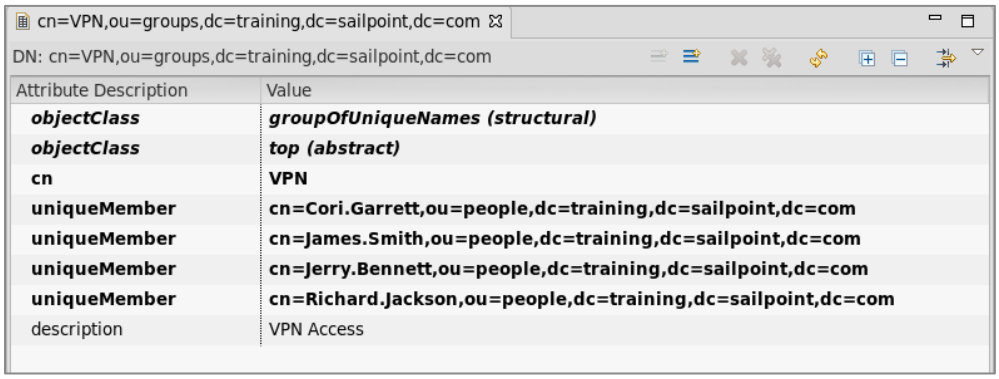
Note: The text strings in this list must be substrings of the error messages that will be returned to the connector in the event of a retryable failure.

Common retryable errors represent system downtime or network connectivity issues. Your implementation team will define errors that should be considered retryable, per application.

View Current Members of LDAP VPN Group

1. Using the desktop shortcut, launch the **LDAP Browser**
2. In the Connections window, select **Training** and click **Open Connection**

   Note: If you're not able to connect, you can check if LDAP is running (from a terminal window, enter **CheckLDAP**). If necessary, start LDAP (from a terminal window, enter **StartLDAP**).
3. Expand **dc=training,dc=sailpoint,dc=com**, then expand **ou=groups**
4. View the current members of the **cn=VPN** group.

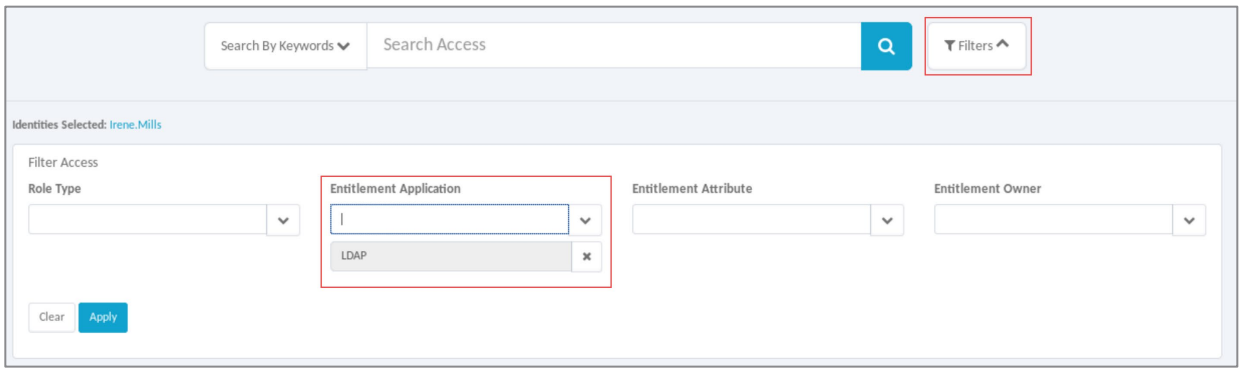


Request VPN Access and Approve Request

Test your access request and approval configurations.

1. Still as Carl.Foster, navigate to **Manage User Access**

   Note: You can access this Quicklink two ways: either select the **Manage User Access** Quicklink card on your home page, or expand the Quicklink menu and navigate to **Manage Access** > **Manage User Access**
2. Search for and select user: **Irene Mills** and click **Next**
3. On the next page (Manage Access), click **Filters** to expand the access filters.
   a. Filter access on:
      i. Entitlement Application: **LDAP**

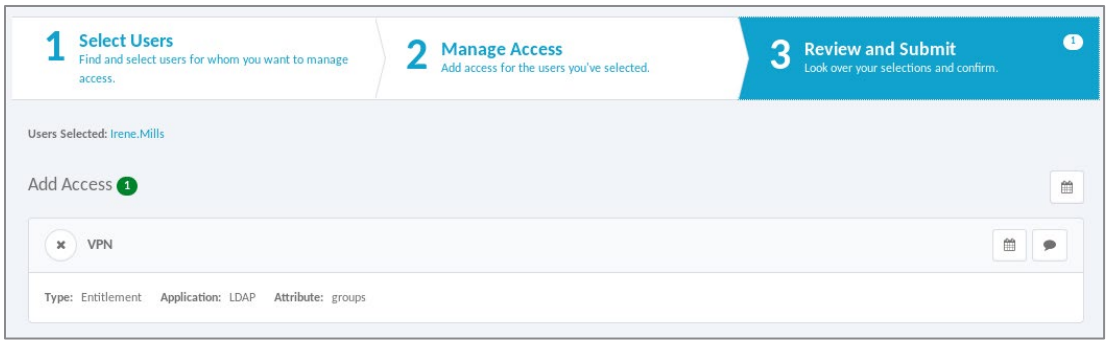


b. Click **Apply**

4. The **VPN** entitlement is the only result. Why is VPN the only requestable entitlement on the LDAP application (**Hint:** You made this configuration earlier)?

_____

5. Select **VPN**
6. Click **Next**
7. Review your selection and **Submit**



8. Check status of the request.
   a. Navigate to **Home** > **Track My Requests** and view the **Details** for the request for Irene.
   b. Scroll down and review the **Interactions**. What interaction is the requesting waiting on?

_____

   c. Why did Carl's request for Irene go to Catherine?

_____

9. Log out of IdentityIQ and back in as Irene's manager, **Catherine.Simmons/xyzzy**
10. Approve request.
    a. Select the **Approvals** card on your home page.
    b. Click **Approve All** and **Complete**
11. Observe how the system behavior changes when the request is submitted by the user's manager. As Catherine Simmons, request VPN access for Tammy Daniels.
    a. Still signed in as Catherine, select **Manage User Access**
    b. Search for and select user: **Tammy Daniels** and click **Next**
    c. On the next page (Manage Access), search for and select **VPN**
    d. Click **Next**
    e. Review your selection and **Submit**
12. Check status of the request.
    a. Navigate to **Home** > **Track My Requests** and view the **Details** for the request for Tammy.
    b. Scroll down and review the **Interactions**. What interaction is the requesting waiting on?

       _____

    c. Why did Catherine's request for Tammy go to the Admins workgroup?

       _____

       Note: Catherine is Tammy's manager and did not receive an approval because by default if the approver is the requester, IdentityIQ assumes they implicitly approve the request they are submitting.
13. Approve the request.
    a. Log out and back in as a member of the Admins workgroup, **Walter.Henderson/xyzzy**

       Remember that the Admins workgroup owns the entitlement so is responsible for its owner approval.

    b. Select the **Approvals** card on your home page.

c. How many approvals do you have waiting and for which request(s)?

_____

d. Who submitted the request for Irene? _____

Because Carl is also a member of the Admins group, he is both the requester and an approver for Irene's request and IdentityIQ, again, assumes implicit approval by the requester. So the only remaining required approval is owner approval for Tammy.

e. Click **Approve All** and **Complete** on the approval.

14. Check status of the request.

a. View **Track My Requests** and view the **Details** for the request for Irene and Tammy.

Walter can see all Access Requests in IdentityIQ because he has the System Administrator capability.

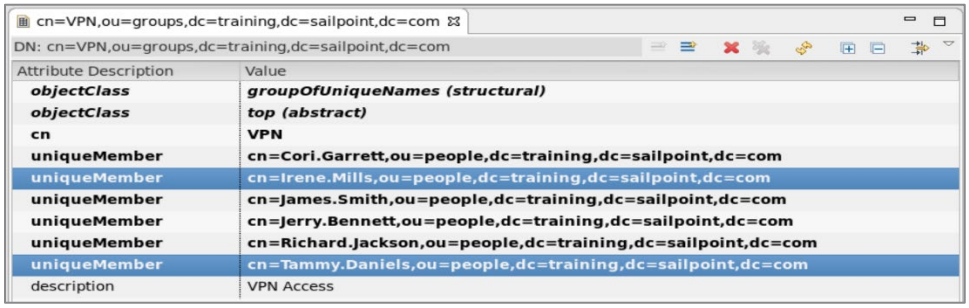
The **Execution Status** is either **Executing** or **Verifying**, depending on when you check the request and when the **Perform Maintenance** task last ran.

i. Either wait for the next scheduled execution of this task or run it now manually (your choice).

15. Check LDAP to see that the provisioning completed.

a. Once the execution status is **Verifying**, open LDAP and **refresh** VPN group (right click > Reload Entry [F5]).

b. Notice Irene and Tammy are members of this group.



c. **Close** the LDAP Browser.

Complete the request

Requests get "verified" and marked as complete by the **Perform Identity Request Maintenance** task. This task is responsible for checking access requests and confirming that the changes have been made. If all of the changes from the request are not represented on the Identity Cube for whom the request was made, the status will remain as verifying.

1. Navigate to **Setup > Tasks > Scheduled Tasks**
2. When is the **Perform Identity Request Maintenance** task next scheduled to run in your environment?

   _____

   This task comes pre-scheduled in IdentityIQ to run once a day by default. You could run this more often as determined by your needs.
3. Navigate back to **Tasks** tab and run the task **Perform Identity Request Maintenance**
4. Check **Track My Requests** and confirm the requests' **Execution Status** has changed to **Completed**

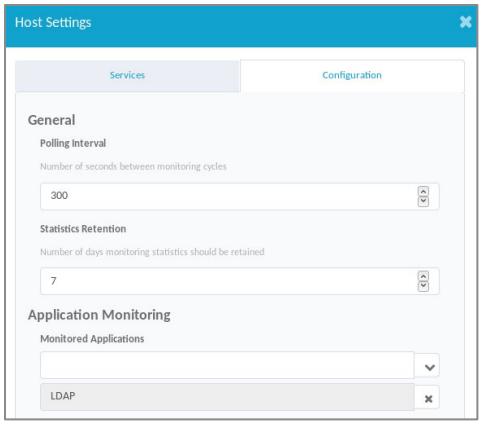
Test Retry Settings – Stop LDAP and Request VPN Access

Now you'll stop the LDAP service to simulate an LDAP system outage, and then make a request to remove VPN access. The request will fail because the server is unavailable. After observing the results of the failure, you'll enable LDAP, retry the provisioning, and observe results.

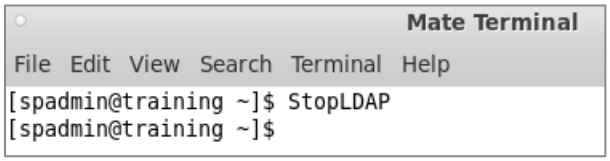
1. First you will configure application monitoring for the LDAP application.

   This enables administrative oversight of the system availability.

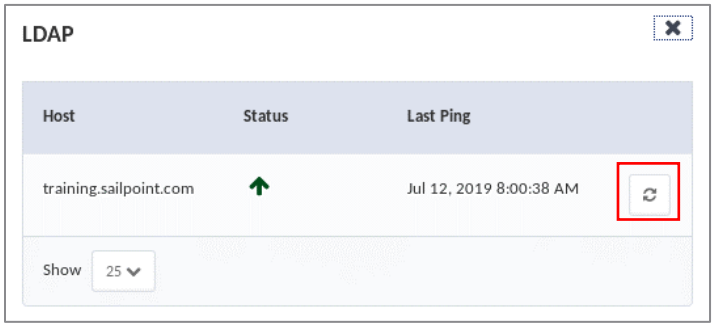
   a. Navigate to **Gear > Administrator Console > Environment**
   b. On the **Hosts** page, click the gear icon by the host you want set up to monitor applications: **training.sailpoint.com**
   c. Navigate to the **Configuration** tab.
   d. In the **Application Monitoring** section, add Monitored Applications: **LDAP**

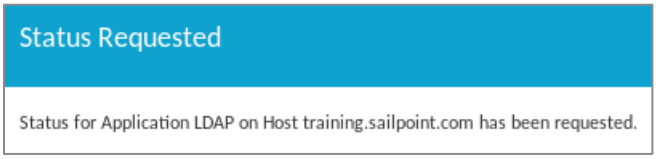


2. Scroll down and **Save**
3. From a Linux command prompt, stop the LDAP service.
   a. Enter **StopLDAP**

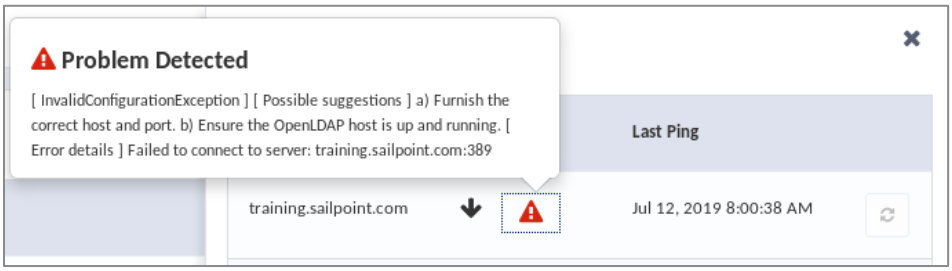


4. Use Administrator Console to check the status of LDAP.
   a. Navigate to **Gear > Administrator Console > Environment**
   b. Navigate to **Applications** tab.
   c. LDAP's **Status** will either display one up arrow or one down arrow. Select **LDAP** to expand its details.
      i. If the status still has an upward arrow, select **refresh** to update the status.





d. Refresh the Administrator Console and click on the red triangle in the LDAP monitoring details to view details about the detected problem.



5. While LDAP is offline, request to remove VPN Access.

   a. Log out of IdentityIQ and back in as **Catherine.Simmons/xyzzy**

   b. Expand the Quicklink menu, and select **Manage Access** > **Manage User Access**

   c. Select User: **Irene.Mills** and click **Next**

   d. On the next page (Manage Access), click **Remove Access**

   e. Select **VPN**

   f. Click **Next**

   g. Review your removal request and click **Submit**

6. Approve the request.

   a. Log out of IdentityIQ and back in as **Carl.Foster/xyzzy**

   b. Select the **Approvals** widget on your home page.

   c. Approve All and Complete.

7. Check status of the request.

   Note: this action will appear after *Perform Maintenance* has run. Either wait for the next scheduled execution of this task or run it now.

   a. Check **Track My Requests** and click on the Details button.

   b. What is the **Provisioning Status** in the Request Items? _____

   c. Scroll down to the **Errors and Warnings** section and note the error listed.

   _____

8. Navigate to **Administrator Console** > **Provisioning**

a. Search for the provisioning action for Irene.

b. What is the status of this provisioning transaction?

_____

c. Click the **information box** to review the details of this transaction.

d. What error message was captured for this transaction?

_____

9. What configuration caused IdentityIQ to recognize this as a retryable error?

_____

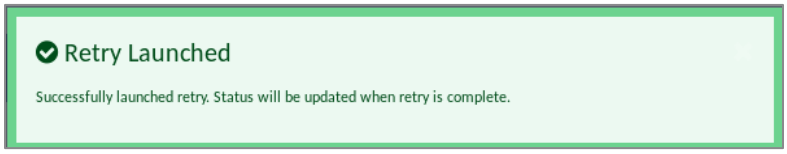
Resolve LDAP System Outage and Retry Request

Now that you know what happens to a failed transaction for an application configured for retries, resolve the LDAP outage and allow the transaction to complete successfully. IdentityIQ will retry the provisioning transaction by default once an hour. Admins can force a retry immediately from the Administrator Console.

1. From a Linux command prompt, start the LDAP service. Enter **StartLDAP**
2. Return to the **Administrator Console** and check the status of LDAP.
   a. Navigate to **Environment > Applications** tab.
   b. View status of **LDAP** application.

Note: You may need to request a status refresh.

3. In **Administrator Console**, force the transaction to retry.
   a. On the **Provisioning** tab, locate the **pending** access request for **Irene Mills**
   b. Click **Retry** for this transaction.



Observe how this retried attempt completes and review any new information associated with the transaction.

4. Check status of the request.
    a. Navigate to **Home** > **Track My Requests** and view the **Details** for the request for Irene.
    b. Review the **Request Items** and observe the Provisioning Status is now **Committed**
    c. Scroll down and review the **Provisioning Engine** and **Errors and Warnings** sections.
        i. Does it retain the history of the error? -Select-
        ii. How many retry attempts occurred? _____

Access Request with Attachments and Comments

Scenario: Users must complete Internal Security Training 104 before they can input and edit tickets in your Bug Tracking system. Norma Armstrong is a QA Analyst in Singapore. She has completed this training course, and she needs this access for her job responsibilities.

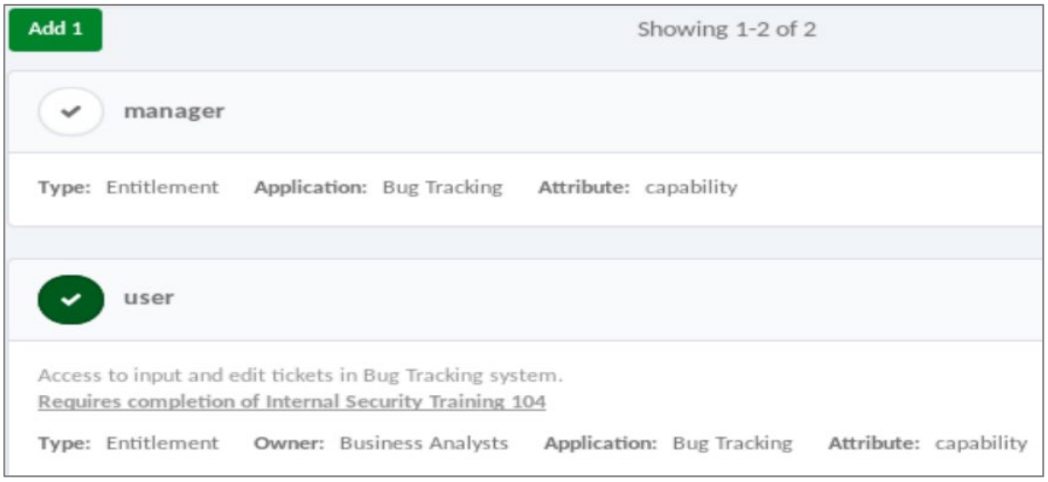
In this exercise, you will act as Norma and request access to the Bug Tracking application. You will include your Proof of Completion (PoC) of the training course.

1. Log into IdentityIQ as **Norma.Armstrong/xyzzy**
2. Click **Manage My Access**
    a. Why is this labeled **Manage My Access** instead of **Manage User Access**, as you have seen with other users, like Catherine Simmons?

    _____
3. Click **Remove Access** and look at her entitlements. Norma cannot request to remove any access. Why not?

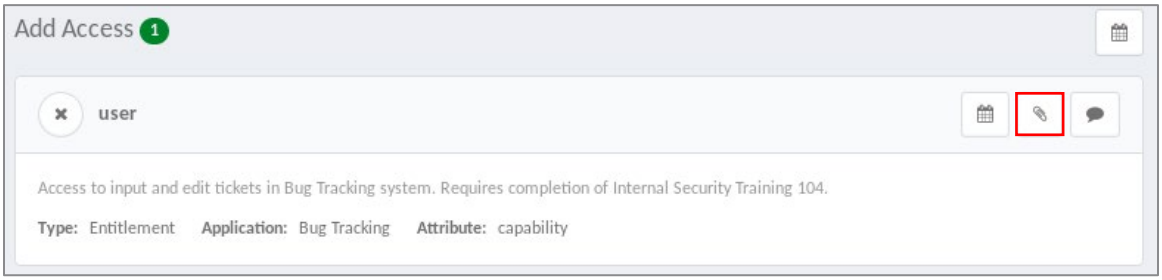
    _____
4. Return to **Add Access**.
5. Search for **bug** to find entitlements on the Bug Tracking application, and select the **user** entitlement.

6. Notice the description with formatting that you previously added.



7. Click **Next**

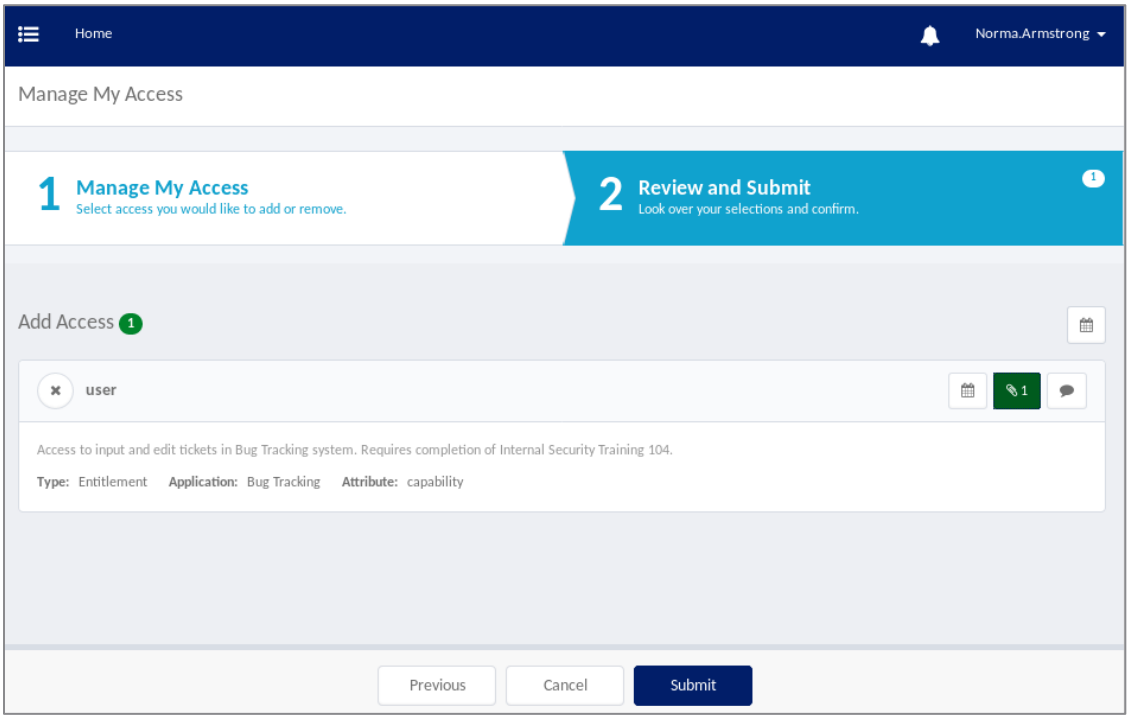
8. Click the **paperclip icon** to attach a file.



9. On the Attach a File to user page, click the hyperlink *or click to upload a file* and select **/home/spadmin/ImplementerTraining/config/POC Norma Armstrong.pdf**

10. Click **OK**

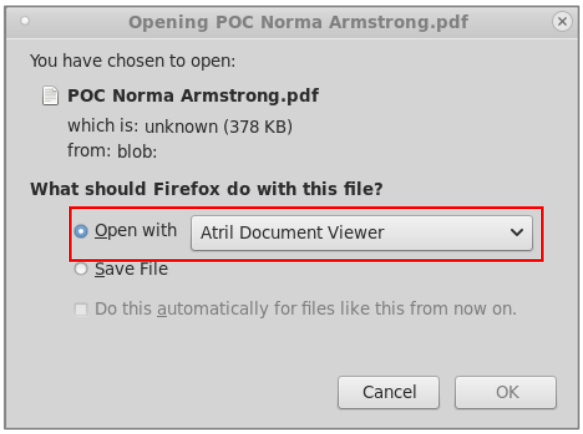
The paperclip icon indicates there is 1 attachment.



11. Click **Submit**

View Attachment, Add Comments, and Approve Request

1. Log out and back in as Norma's manager, **Marilyn.Dunn/xyzzy**
2. Click **Approvals**
3. Click the **paperclip icon** and click **download** to download the POC document.
4. Open document with the **Atril Document Viewer** to view the Proof of Completion.



5. Back in IdentityIQ, click the comments icon on the approval and enter: **Training PoC verified**
6. Click **Post** to post the comment to the approval.

   The comment icon will change to indicate this approval now contains a comment.
7. Click **Approve All** and **Complete** on Norma's request.

   Earlier you specified the User entitlement on Bug Tracking was owned by Business Analysts so the next approval is assigned to this workgroup. If an entitlement does not have an owner, the approval process would have gone to the Bug Tracking application owner, the Admins workgroup.
8. Log out and back in as a member of the Admins workgroup, **Jim.Lee/xyzzy**
9. Click **Approvals**

   Notice Jim can also view Marilyn's comment and download and view the attachment.
10. **Approve** Norma's request.

Change Business Process Preventive Policy Checking Behavior

The business requires that access requesters be notified if they attempt to submit a request that will cause a policy violation.

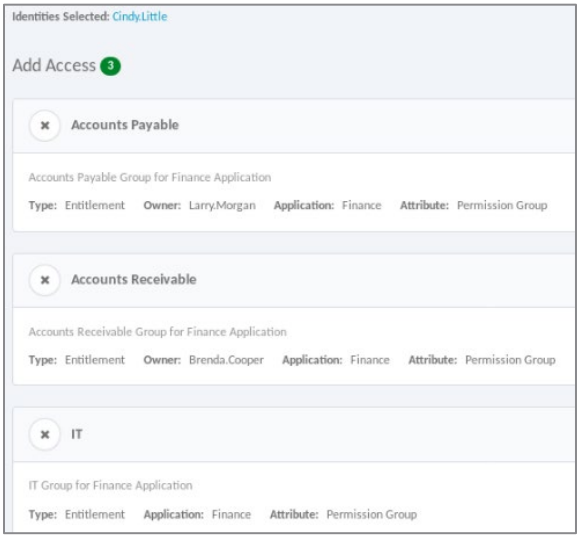
1. Log into IdentityIQ as **Carl.Foster/xyzzy**
2. Navigate to **Setup > Business Processes**
3. Select the **TRNG LCM Provisioning** business process from the list.
4. Navigate to the **Process Variables** tab.
5. Note the **Policy Settings** value: _____

   This option allows the request to be submitted but it does notify the approver(s) of the violation so they can make an informed approval decision.
6. Set the following for **Policy Checking**:
   a. Policy Settings: **Present Failures to Requester**
   b. Policies to Check: **All**
7. **Save** your changes to the **TRNG LCM Provisioning** business process.

Request Access and Incur Policy Violation

Request conflicting access to see the policies applied.

1. Log in as Cindy's manager, **Sara.Berry/xyzzy**
2. Click **Manage User Access**
3. Select **Cindy.Little** and click **Next**
4. On the **Manage Access** page, search for **Finance**
5. Select these 3 Finance entitlements:
   a. Accounts Payable
   b. Accounts Receivable
   c. IT
6. Click **Next**
7. **Review** and **Submit**



8. What policy does this violate?

_____

You configured and applied this policy definition to *detect* users with these conflicting entitlements in an earlier exercise. Now you are seeing that same policy applied *preventively*.

9. Click the text **Accounts Payable and Accounts Receivable: Cannot have access to Accounts Payable and Accounts Receivable** at the same time to view details about the potential Policy Violation.
10. Click on the **Correction Advice**, then close the details pop-up.
11. Click **X** to remove Accounts Receivable
12. Before you submit, who do you think the next approver will be for the items you are requesting?
    a. Accounts Payable entitlement: _____
    b. IT entitlement: _____
13. **Submit** the request.

Track Request and Complete Approvals

Since Cindy's manager, Sara, made the request on behalf of Cindy, IdentityIQ assumes approval for the first approval step (manager approval) and is directed to second step, getting approval from the application and entitlement owners.

1. Navigate to **Home** > **Track My Requests**
    a. View **Details** and observe the next approvers.
    b. Were the approvers who you recorded above? If not, investigate the following in the Entitlement Catalog and Application Definition:
        i. Does the Accounts Payable entitlement have an owner? If so, who?

        _____

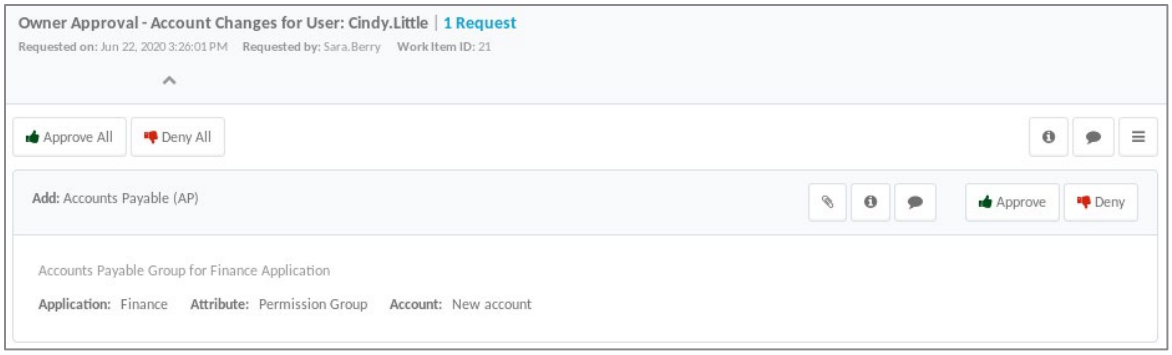
        ii. Does the IT entitlement have an owner? If so, who?

        _____

        iii. Does the Finance application have an owner? If so, who?

        _____

        Owner approval for entitlements goes to the Entitlement owner first and to the Application owner if there is no entitlement owner specified.
2. Approve each entitlement in this request for Finance access.
    a. Log in as **Larry**.**Morgan**/**xyzzy** and approve Accounts Payable entitlement request.



Note: You can view completed approval items in **My Work** > **Work Items** > **View Archive**

b. What configuration (from the first exercise in this class) made viewing archived work items possible?

_____

c. Log in as **Patricia.Jones/xyzzy** and approve the IT entitlement request.

The Finance application is a disconnected application and relies on manual provisioning As the application owner, the Finance Administration workgroup receives an additional workitem to implement the change. Since Patricia is a member of that workgroup, she sees this work item appear.

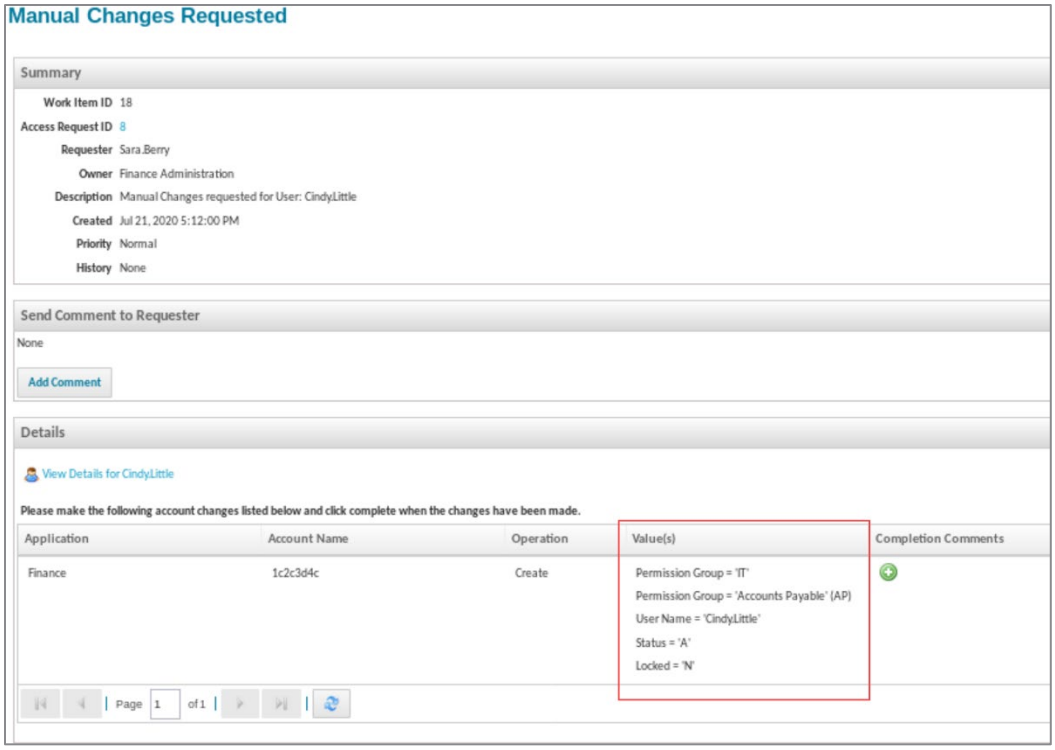
d. Click the **View Work Item** button on the pop-up Patricia received after approving the request.

i. What exactly is being requested for Cindy in this work item? Why?

_____

ii. How did IdentityIQ know what attributes to include in the account creation request?

_____



In a real-world scenario, somebody from the Finance Administration workgroup would create Cindy's account on Finance and then come back to IdentityIQ to mark this request as complete. Because you only have a delimited file representing Finance accounts, for the purposes of this test, you do not need to create that account or complete this request.

Request Duplicate Access and Permitted Access

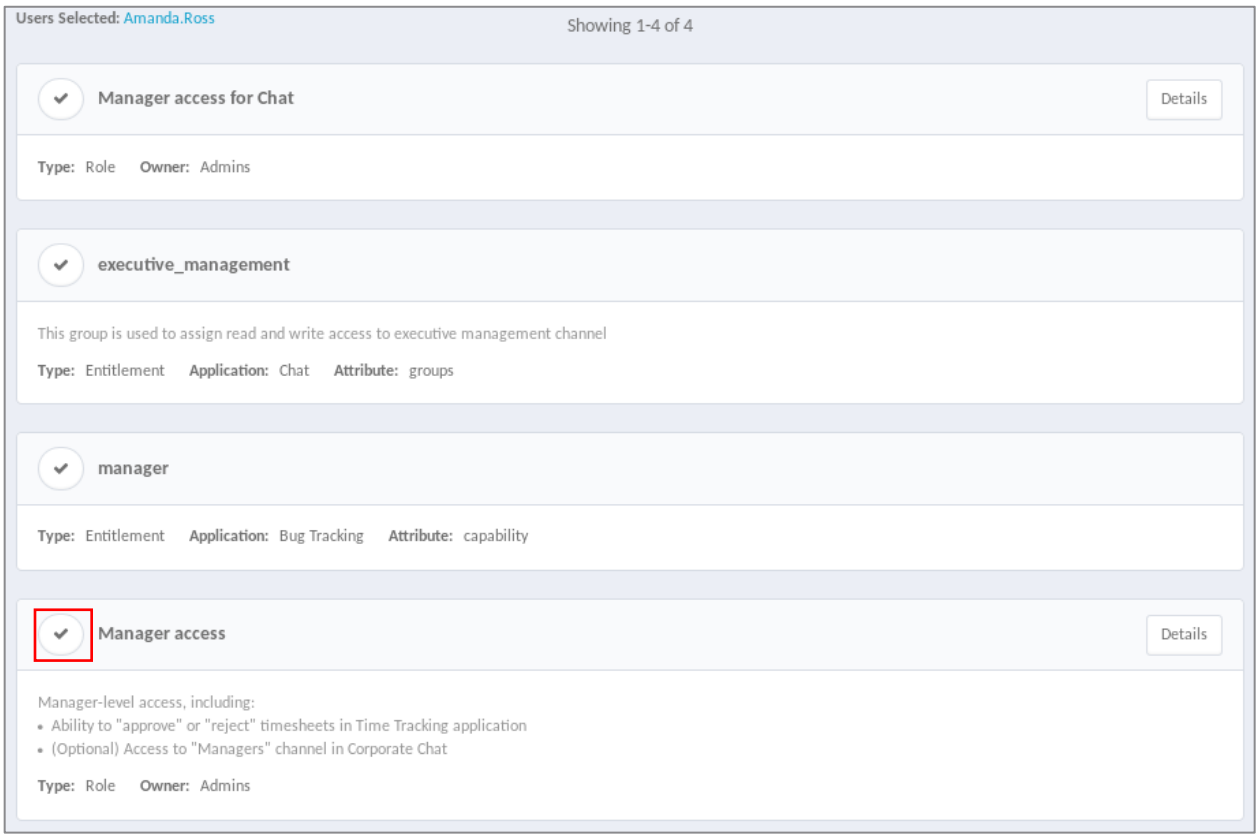
Earlier, you loaded a role model that included one Business Role **Manager access**. This Business Role has one permitted IT Role: **Manager access for Chat**. Normally, only Business roles appear in the access request pages. To be requested, permitted access can be requested as part of the request for the business role. However, IT roles also appear in the list when the target user (requestee) in a request already has a Business role which *permits* the IT role but the user does not yet *have* the IT role.

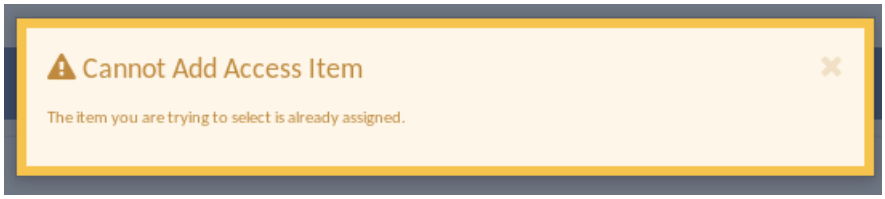
Plus, IdentityIQ detects and prevents requests for access a user already holds.

1. Log into IdentityIQ as **Amanda.Ross/xyzzy**
2. Click **Manage User Access**
3. Select yourself, **Amanda Ross**, and click **Next**
4. Search for **manage**
5. Select the **Manager access** business role.

a. Why is IdentityIQ preventing you from adding this access for yourself?

_____





b. **Close** the popup.

c. View **Details** for **Manager access for Chat** role.

i. What type of role is it? _____

ii. Which entitlement(s) are included in this role's entitlement profile?

_____

This role is included as an option for Amanda because it is permitted to her through the Manager Access role she already has. You can review the role definition for the Manager Access role to observe this relationship.

d. **Close** the Details.

e. At this time, you do not need to request this access for Amanda; therefore, click **Previous** or **Select Users** to return to the first screen.

Request Business Role with Permitted Role

Amanda is going on leave and Adam Kennedy will be taking on some of her duties temporarily. She will request the Manager access for him, along with the permitted Manager access for Chat.

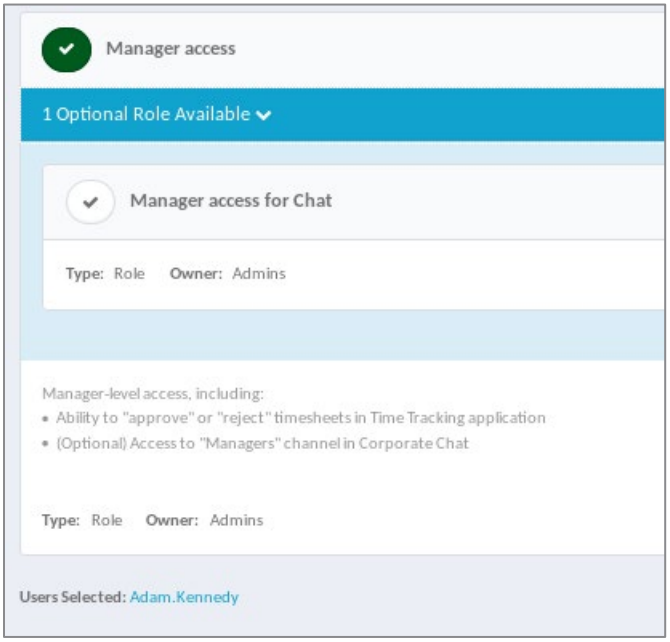
1. **Uncheck** yourself, Amanda, and select **Adam Kennedy**

   Adam is not a manager, so he has not been assigned the Manager access Business role automatically, but it can still be requested for him.

2. Click **Next** and search for **manage**

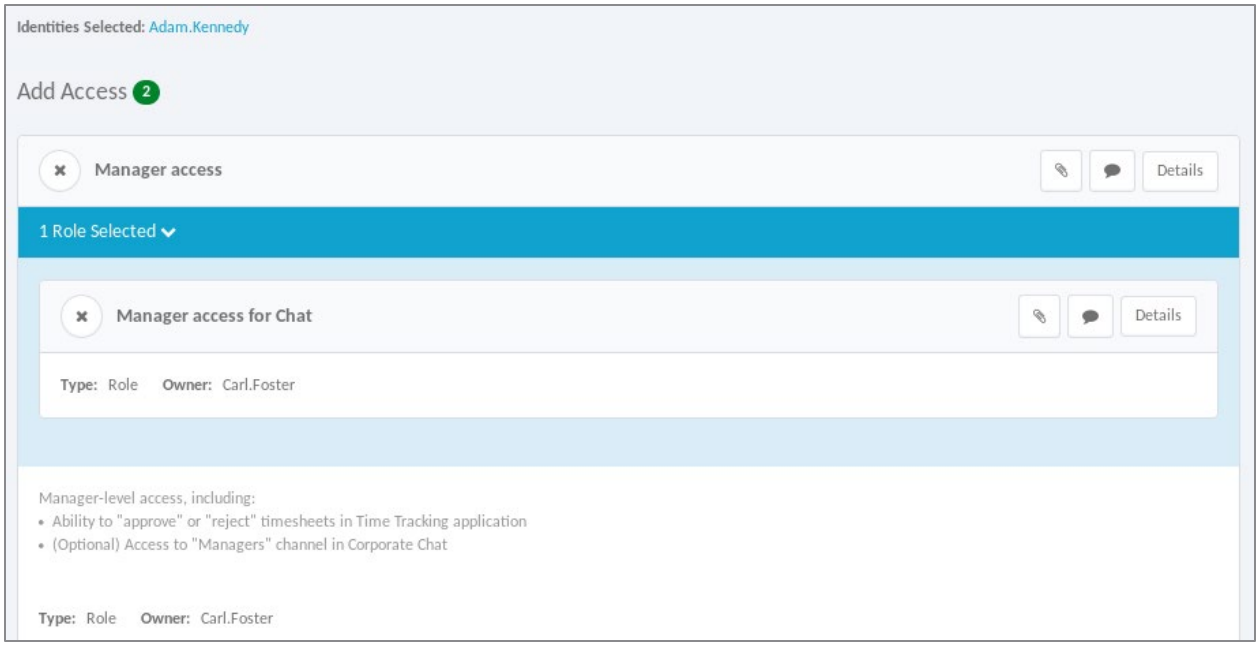
3. Select the Business role **Manager access**

4. Amanda is asked if she would also like to request the optional role, **Manager access for Chat**



5. Select the **Manager access for Chat** permitted role as well as the business role.

6. Click **Next**



7. Review your selections and click **Submit**
8. Track Amanda's request to see whose approval it is waiting on. Why was this the next approver?

_____

Exercise #6: Explore Provisioning Policy for Creating Identities

Objective

In this exercise, you will explore creating Identities using IdentityIQ, both with and without Identity Provisioning Policies.

Overview

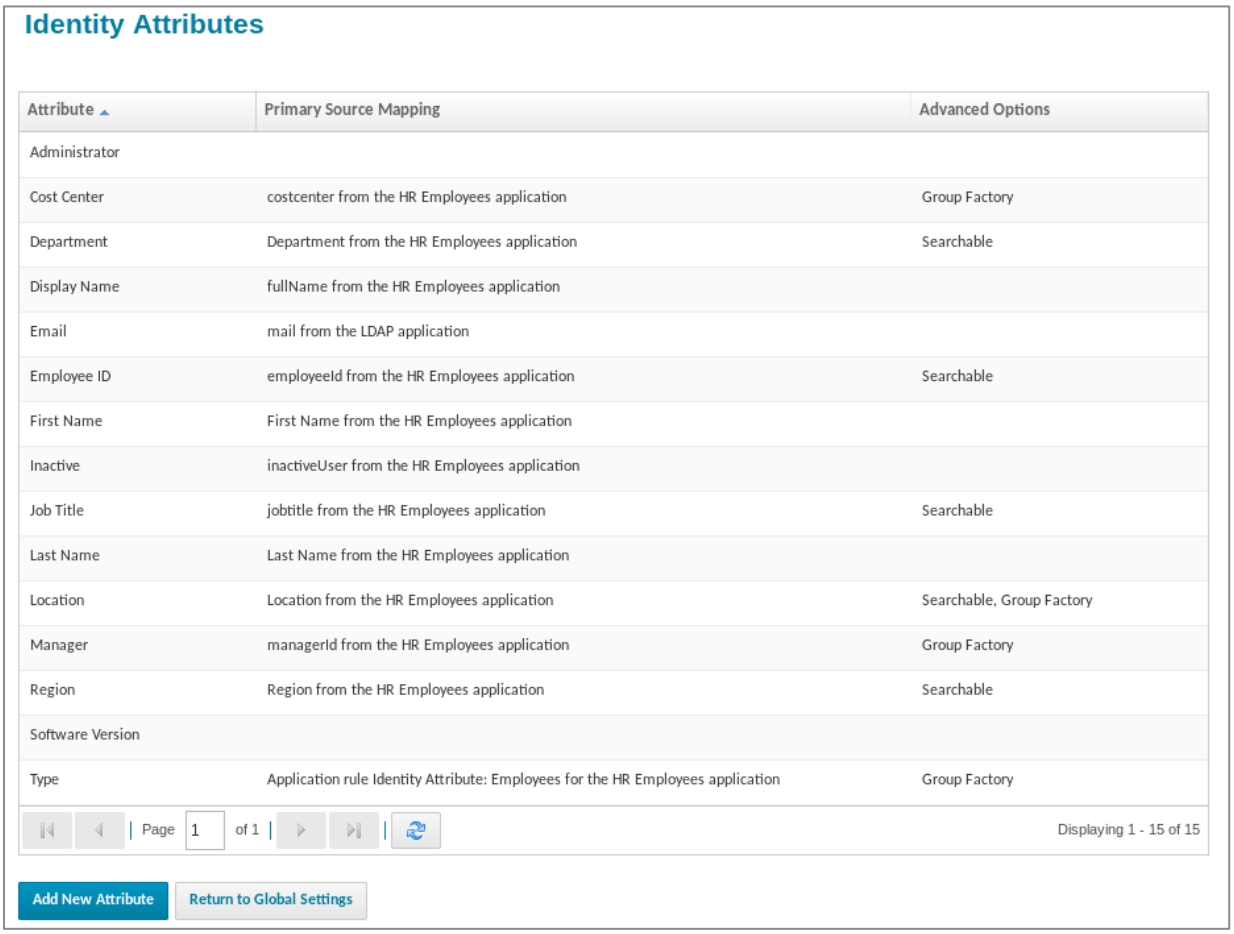
Some implementations have the requirement to create new Identities directly in IdentityIQ. One way to create them is by using the **Create Identity** Quicklink. You can use this Quicklink without a provisioning policy, or you can define a policy that will help your end users define the choices that are made when creating Identities in the system. In this implementation, you will use the Create Identity Quicklink with a policy as an additional way to onboard new users, supplemental to the aggregation of the authoritative sources.

Investigate the Create Identity Quicklink

1. Log in as **Carl.Foster/xyzzy**
2. Navigate to the Quicklink menu: **Manage Identity > Create Identity**
3. Explore the form and notice that a few fields have drop-down selections, but most fields are text entry.

4. Do not submit a request. Click **Cancel**

    a. Compare the fields against the attributes on the Identity Mappings page



Identity Attributes

Attribute	Primary Source Mapping	Advanced Options
Administrator		
Cost Center	costcenter from the HR Employees application	Group Factory
Department	Department from the HR Employees application	Searchable
Display Name	fullName from the HR Employees application	
Email	mail from the LDAP application	
Employee ID	employeeId from the HR Employees application	Searchable
First Name	First Name from the HR Employees application	
Inactive	inactiveUser from the HR Employees application	
Job Title	jobtitle from the HR Employees application	Searchable
Last Name	Last Name from the HR Employees application	
Location	Location from the HR Employees application	Searchable, Group Factory
Manager	managerId from the HR Employees application	Group Factory
Region	Region from the HR Employees application	Searchable
Software Version		
Type	Application rule Identity Attribute: Employees for the HR Employees application	Group Factory

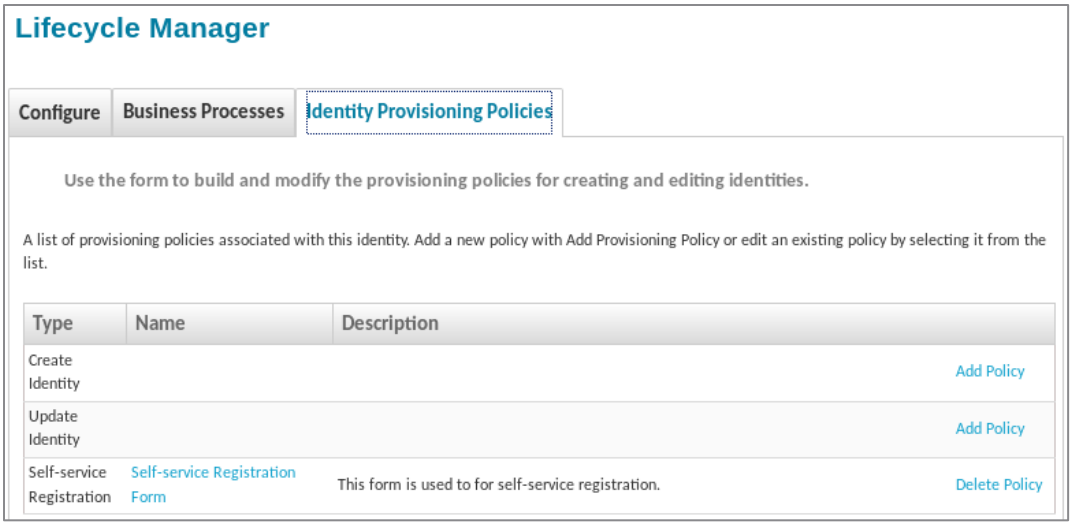
Page 1 of 1 Displaying 1 - 15 of 15

Add New Attribute | Return to Global Settings

As you can see, the form presented by the default provisioning policy provided a tedious (and potentially error-prone) approach to creating an identity. In this section, you will import a provisioning policy that will allow IdentityIQ to present your own form to the user. It will support entering the same information, but the provisioning policy will make creating an identity easier and provide nice features like field help text or presenting a list of allowed values for a field.

Investigate and Load the Create Identity Provisioning Policy

1. Navigate to **Gear > Lifecycle Manager > Identity Provisioning Policies**
2. Notice that you do not have a provisioning policy for creating identities.

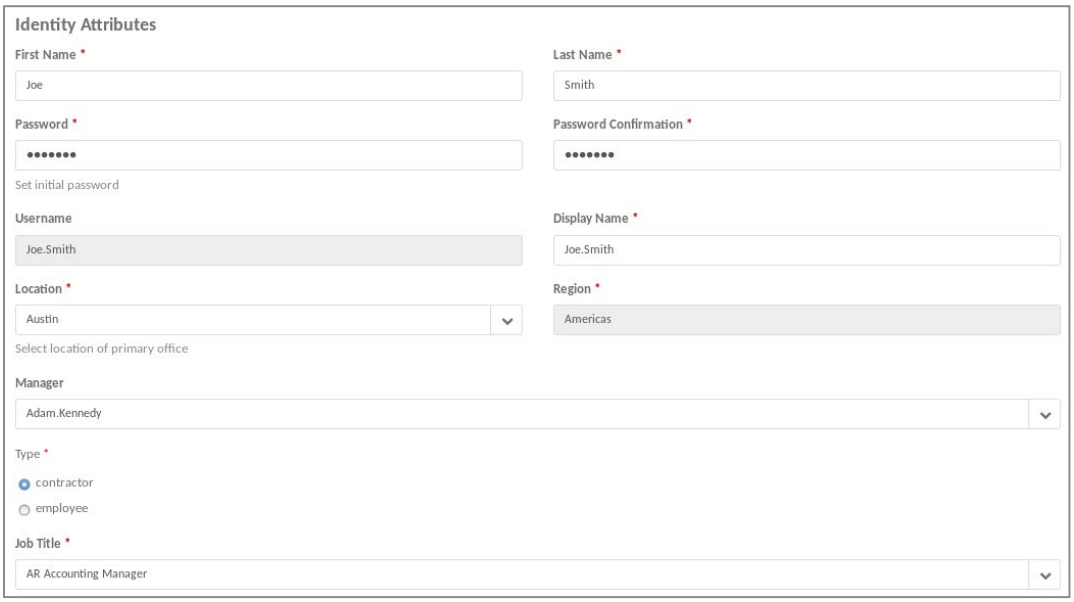


3. Load a form to be used as the Create Identity Provisioning Policy.
   a. Navigate to **Gear > Global Settings > Import from File** and import the following file: **/home/spadmin/ImplementerTraining/config/Form-Identity-Create.xml**
4. Click **Manage Identity** > **Create Identity** and observe how the form is different.
5. Fill out the form to explore its updated fields:
   a. First Name: **Joe**
   b. Last Name: **Smith**
      i. Which fields auto-populate after you enter these two values?

      _____
   c. Password: **password**
   d. Password Confirmation: **password**
   e. Location: **Austin**
      i. What other field automatically updates when you choose a location?

      _____
   f. Manager: **Adam.Kennedy**
   g. Type: **Contractor**
   h. Job Title: **AR Accounting Manager**

iii. Notice how **Job Title** has a fixed list of selectable values.

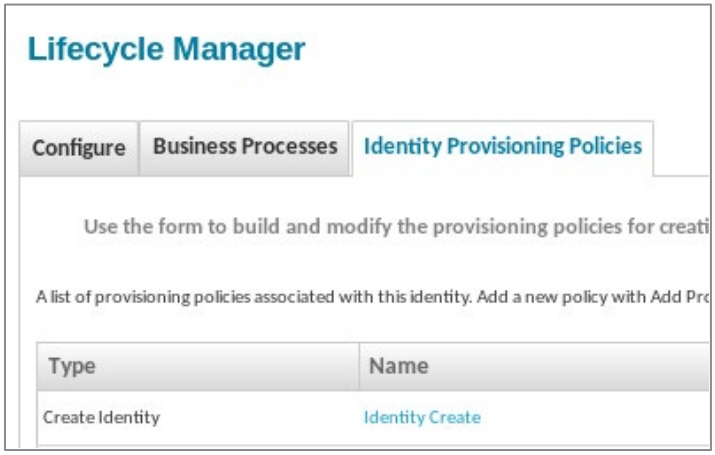


iv. Click **Submit**

6. Review the Create Identity Provisioning Policy

a. Navigate to **Gear > Lifecycle Manager > Identity Provisioning Policies**

e. Select the **Identity Create** policy



b. Explore this form and its settings.

Notice that the form editor is the same as that used for editing the application provisioning policy. Many of the form field values are calculated or generated based on input in other fields in the form.

i. Click the pencil for **Username** and view its **Value Settings**

(1) What fields are referenced to calculate identity name?

_____

ii. Click the pencil for **Region** and view its **Value Settings**

(1) What field is referenced to calculate region?

_____

iii. Click the pencil for **Type** and view its **Value Settings**

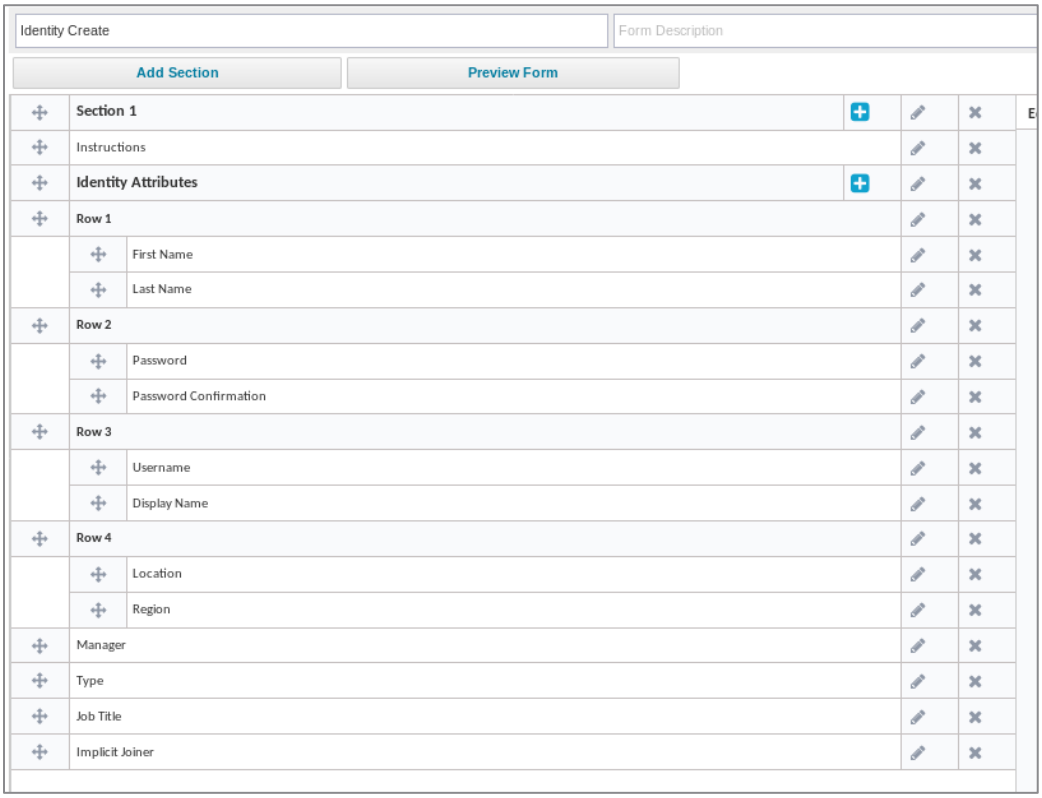
(1) How is the list of selectable values specified?

_____

iv. Click the pencil for **Job Title** and view its **Value Settings**

(1) How is the list of selectable values specified?

_____



c. When you are finished, **close** the provisioning policy and **logout** of IdentityIQ.

d. Login as **Adam.Kennedy/xyzzy** and approve the request to create the Identity.

7. Log in as **Carl.Foster/xyzzy** and review the lifecyle event that was processed for Joe.

8. Use the Identity Warehouse to view Joe's identity cube.

   a. What Application Accounts did IdentityIQ provision for Joe?

   _____

Exercise #7: Define and Test Attribute Synchronization

Objective

In this exercise, you will configure and test attribute synchronization.

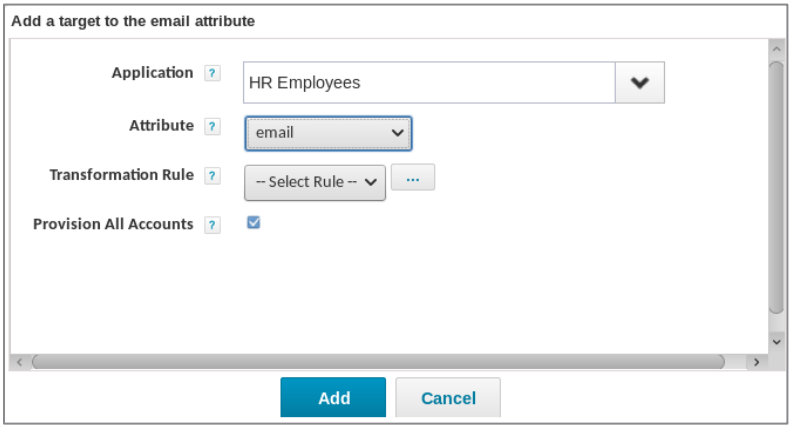
Overview

In this exercise, you'll configure attribute synchronization for the email attribute. Your email identity attribute is sourced from the LDAP mail account attribute. For new users, this email address is generated when the LDAP account is created. The business wants to keep email address in sync between the LDAP system and the authoritative applications. In this exercise, you will configure attribute synchronization for the two authoritative applications (HR Employees and HR Contractors).

Configure Attribute Synchronization

Set up attribute synchronization of the email address to your authoritative applications, HR Employees and HR Contractors. If a user's email *identity attribute* changes in IdentityIQ (through aggregation or a UI edit), then the updated value should be pushed out to their email *account attribute* on either HR Employees or HR Contractors.

1. Log in to IdentityIQ as **Carl.Foster/xyzzy**
2. Navigate to **Gear > Global Settings > Identity Mappings**
3. Click **Email**
    a. Click **Add Target**
        i. Application: **HR Employees**
        ii. Attribute: **email**
        iii. Click **Add**



b. Click **Add Target**

i. Application: **HR Contractors**

ii. Attribute: **email**

iii. Click **Add**

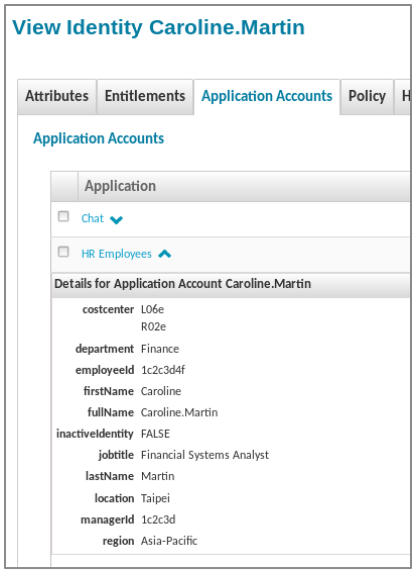
c. Click **Save** to save your changes.

View Caroline's Identity Cube

During the joiner event, you saw the email address for Caroline's LDAP account. At this point, the email attribute is not yet synced back to HR Employees.

1. Navigate to **Identities > Identity Warehouse**
2. Search for **Caroline.Martin**.
3. Open her Identity Cube.
4. Navigate to the **Application Accounts** tab

   Notice that her LDAP account has a mail attribute (mail:) but her HR Employees account does not have an email attribute.



Run Identity Refresh Task to Trigger Attribute Synchronization

Now that the target mappings are defined for email, you'll run another refresh task with the synchronize attributes option selected, which will kick off attribute synchronization to the HR Employees application.

1. Navigate to **Setup** > **Tasks**
2. Create an **Identity Refresh** task.
    a. Name: **Synchronize Attributes**
    b. Previous Result Action: **Rename Old**
    c. Refresh identity attributes: **Enabled**
    d. Synchronize attributes: **Enabled**
    e. Enable the generation of work items for unmanaged parts of the provisioning plan: **Enabled**
3. **Save and Execute** this task.

Check for Attribute Synchronization Work Item

Since the HR Employees application uses the delimited file connector, this request cannot be provisioned automatically. Instead, IdentityIQ created a work item to direct a user to perform the required action.

1. View work item to update email by navigating to **My Work > Work Items**
    a. Click **View** to view the details of the work item.

2. How did IdentityIQ determine who should receive this work item?

_____

For the purposes of this exercise, it is not necessary to act upon or complete this work item.

Exercise #8: Define and Test Leaver Processes

Objective

In this exercise, you will configure and test the Rapid Setup leaver lifecycle event and the Identity Operations terminate process.

Overview

In this exercise, you define and test leaver processing both through a lifecycle event. Then you will configure and use the immediate identity operation termination.

For this installation, leavers are people whose identity record changes to "inactive". You will configure the global behaviors and the per-application behaviors which your organization requires upon exit.

When people leave your company, their access should change on four applications:

- LDAP
- Time Tracking
- Chat
- Finance

Define Global Options for Leaver Event

This configuration includes specifying how to handle IdentityIQ object ownership, manager relationships, and role assignments. It also defines the requirements that should trigger the leaver event.

1. Log into IdentityIQ as **Carl.Foster/xyzzy**
2. Navigate to **Gear > Global Settings > Rapid Setup Configuration**
3. On the **Leaver** page, enable **Leaver Processing**
    a. **Observe** and record the various default Leaver options (which you will not change):
        i. **Generate Approvals** _____
        ii. **Exclude Uncorrelated Identities** _____

        Note: Enabling this option prevents detection of a non-authoritative identity as a leaver, even if it meets the trigger filter criteria.

        iii. **Remove Assigned Roles** _____

iv. Reassign Artifacts (objects owned by the user) _____

(1) **To whom**? _____

v. Reassign Identities (identities who report to the user) _____

(1) **To whom**? _____

b. Add the following configurations:

These serve as fall-back owners if the user does not have a manager.

i. Reassign Artifacts Alternate: **Admins**

ii. Reassign Identities Alternate: **Operations**

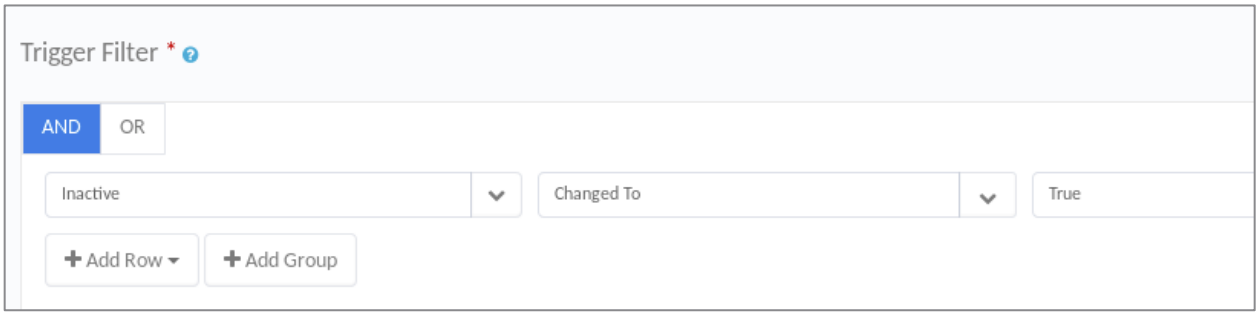
4. Scroll down and add a Trigger Filter:

a. Click **Add Row** and select **Attribute**

i. Attribute: **Inactive**

ii. Changed To

iii. True



5. Click **Save**

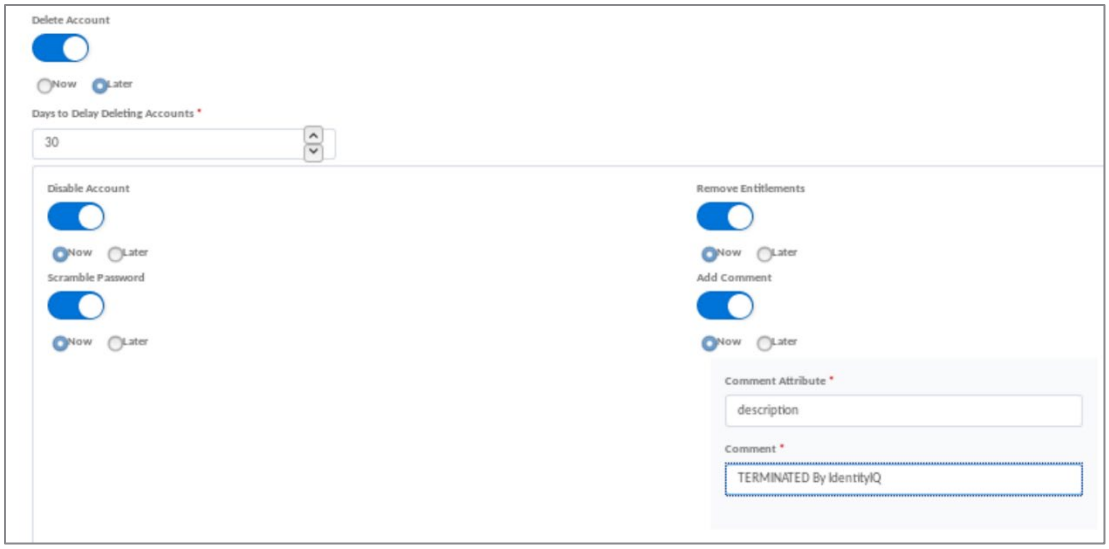
Define LDAP Actions for Leaver Event

When somebody leaves your organization, these actions must immediately occur on their LDAP account :

- Disable the account
- Remove entitlements
- Change the account password
- Add comments to the account's description.

Additionally, the account must be deleted after 30 days of the termination date.

1. Navigate to **Applications > Rapid Setup**
2. Select the **LDAP** application and click **Next**
3. On the **Leaver** page, enable the following **Leaver Options**:
    a. Delete Account
        i. Later
            (1) Days to Delay Deleting Accounts: **30**
    b. Enable these remaining options, and select **Now** for immediate processing.
        i. Disable Account
        ii. Remove Entitlements
        iii. Scramble Password
        iv. Add Comment
            (1) Comment Attribute: **description**
            (2) Comment: **TERMINATED BY IdentityIQ**



4. Click **Save**

Define Time Tracking Actions for Leaver Event

When somebody leaves your organization, their Time Tracking account should immediately be deleted.

1. On the top left, click the back arrow (**<**) next to Rapid Setup to select another application. Select the **Time Tracking** application and click **Next**
2. On **Leaver** page, set:
    a. Leaver Options: **Delete Account**
        i. Now
3. Click **Save**

Define Chat Actions for Leaver Event

When somebody leaves your organization, their Chat account should be disabled immediately.

1. On the top left, click the back arrow **(<)** next to Rapid Setup to select another application. Select the **Chat** application and click **Next**
2. On **Leaver** page, set:
    a. Leaver Options: **Disable Account**
        i. Now
3. Click **Save**

Define Finance Actions for Leaver Event

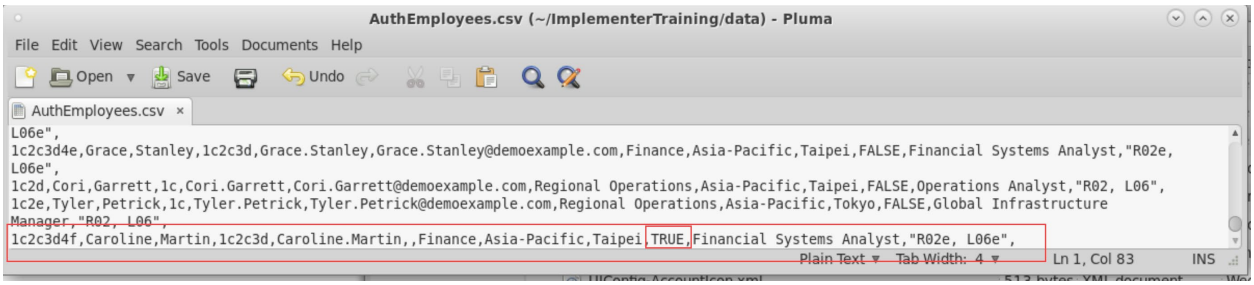
When somebody leaves your organization, their Finance account should be deleted immediately.

1. On the top left, click the back arrow **(<)** next to Rapid Setup to select another application. Select the **Finance** application and click **Next**
2. On **Leaver** page, set:
   a. Leaver Options: **Delete Account**
3. Click **Save**

Simulate Leaver Data Change

Typically, when users leave the organization, the termination is first recorded in the HR system. Then, when the updated information is aggregated into IdentityIQ you can use the Identity Refresh task to process the leaver events. You will simulate this scenario by updating the status of an employee in the HR Employees file.

1. In the file browser, use gedit to open **/home/spadmin/ImplementerTraining/data/AuthEmployees.csv**
2. Scroll to the bottom of the file. Caroline's information is on the last row of this file.
3. Update Caroline's inactiveUser attribute from FALSE to **TRUE**



> **Note:** If you have utilized the Lab Reset tool, this line may be commented out. Ensure this line is as shown, without a preceding // comment character.

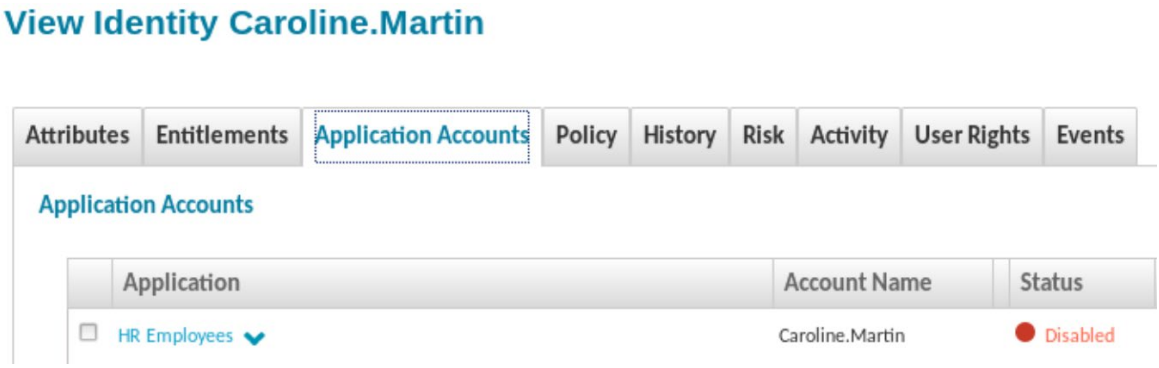
4. **Save** AuthEmployees.csv

Test Leaver Configuration

Aggregate and refresh the identities to test your leaver configuration.

1. Run the task **Aggregate Employees**
2. Once the task completes, navigate to the **Identity Warehouse** and view Caroline's identity cube.

a. Verify that her HR employee account status is displayed as disabled.



3. Run the task **Refresh with Process Events**
4. Once the task completes, use Track My Requests to observe the results.
   a. Navigate to **Home > Track My Requests**
   b. Click **Details** to open the event for Caroline Martin.
   c. Review the **Request Items** and **Provisioning Engine** items.
   d. Note the operations being performed for each account and validate them against the requirements.
      i. LDAP: _____
      ii. Time Tracking: _____
      iii. Chat: _____
5. Review provisioning activities in the Administrator Console.
   a. Navigate to **Gear > Administrator Console > Provisioning**
   b. Filter for Identity: **Caroline Martin**
   c. Explore the different **information** buttons (under **Actions**).
6. Use Advanced Analytics to view the lifecycle event and related audits.
   a. Navigate to **Intelligence > Advanced Analytics**
   b. Search Type: **Audit**
   c. Under **Filter by: Date**, choose **Start Date** and specify today's date
   d. Click **Run Search**
   e. Note the various audit actions triggered by this leaver event.

_____

f. How/where can you specify which of these actions to audit or not (e.g. if you did not want or need all these records)?

_____

7. View the Caroline's identity cube.
   a. Navigate **to Identities > Identity Warehouse**
   b. Search for **Caroline** and open her identity cube.
      i. Navigate to **Application Accounts** and view her account attributes.
      ii. Navigate to **Entitlements** and view her roles and entitlements.
      iii. Navigate to **Events** and view the Past Identity Events. Click on the access request to expand the access request details.
8. Check email log.
   a. Who received the "termination complete" email notification? _____
   b. Why did they receive it? _____

Define Immediate Termination Identity Operation

Rapid Setup provides an immediate termination identity operation for terminating user out-of-band of the regular aggregation refresh cycles. This allows users to process leaver processing directly from IdentityIQ without waiting for updated information in an HR system. First you will enable this functionality then test it.

Note: You will configure these settings to be the same as your Leaver processing, but observe that you can modify these settings such that the immediate termination can be handled differently than regular leaver processing if desired.

1. Signed into IdentityIQ as **Carl.Foster/xyzzy**
2. Navigate to **Global Settings > Rapid Setup Configuration**
3. On the **Identity Operations** page, enable **Terminate Processing**
   a. Observe the various default options. How do these compare to the default options for Leaver processing?

_____

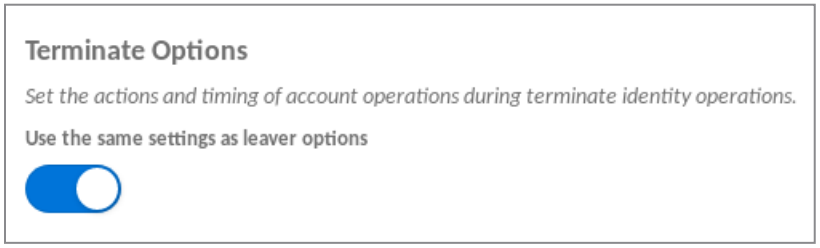
b. Set fallback assignees:

   i. Reassign Artifacts Alternate: **Admins**

   ii. Reassign Identities Alternate: **Operations**

c. Save

4. Navigate to **Applications > Rapid Setup**
5. Select the **LDAP** application and click **Next**
6. On the **Leaver** page, scroll down to **Terminate Options**
7. Enable **Use the same settings as leaver options**



8. Click **Save**
9. On the top left, click the back arrow **(<)** next to Rapid Setup to select another application.
10. For each of the following applications, on the **Leaver** page, scroll down to **Terminate Options** and enable **Use the same settings as leaver options** and **Save**

    a. Time Tracking

    b. Chat

    c. Finance

11. Permit the Operations group access to the Identity Operations so they can manage terminations for the organization.

    a. Navigate to **Setup > Groups > Workgroups** and edit the **Operations** workgroup.

    b. Add the additional capability **Rapid Setup Identity Operations Administrator** to the members of this workgroup.

       Hint: Hold ctrl to select additional capabilities without removing existing.

       This capability permits the Identity Operations menu navigation to process terminations.

    c. Click **Save**

Test Immediate Termination

You have just received an urgent request to terminate Richard Jackson. Instead of waiting for the employment status to update in the HR system, you will use the Identity Operations – Terminate function to terminate access immediately.

Note: Though you just granted the Operations team the appropriate capability to perform the termination, for the sake of time and exercise simplicity, you can continue this exercise signed into IdentityIQ as **Carl.Foster/xyzzy**. Carl is a System Administrator and can process the termination. If you prefer, you can perform the terminate action as Tyler.Petrick from Operations.

1. Examine existing data to understand Richard's pre-termination account, entitlement, and ownership data.

    a. Review the Identity Cube for **Richard.Jackson** to view his account and entitlement details. Note where he has accounts and which entitlements/roles he has.

        i. Accounts: _____

        ii. Entitlements: _____

        iii. Roles: _____

    b. Navigate to **Advanced Analytics**.

    c. Use the **Entitlement** search to find the entitlement(s) which Richard owns.

    _____

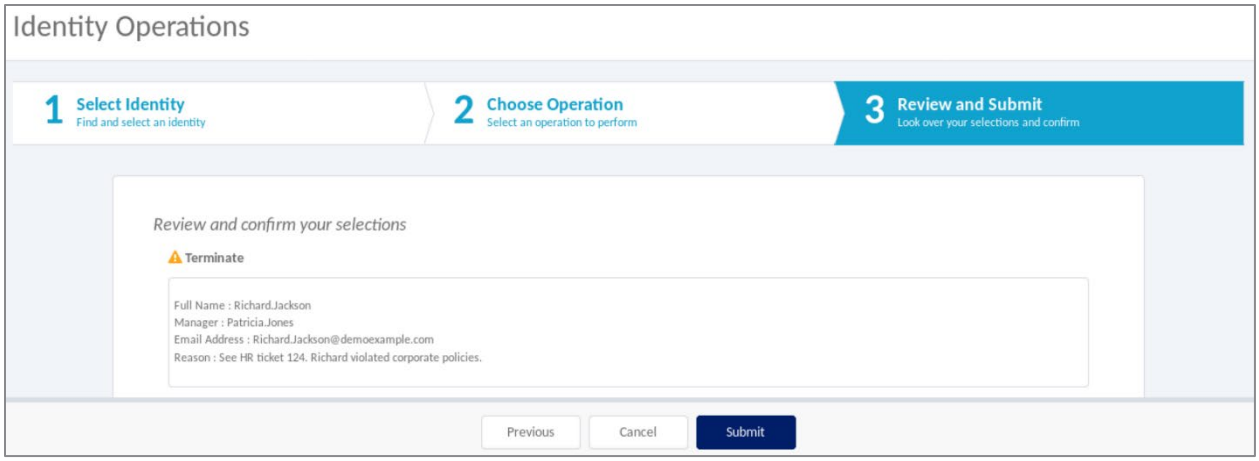
2. Terminate Richard.

    b. Navigate to **Identities > Identity Operations**

    a. Select **Richard.Jackson** and click **Next**

    b. Select the **Terminate** operation and enter reason: **See HR ticket 124. Richard violated corporate policies**

    c. Click **Next** then click **Submit**



Confirm Termination Activities

1. View the event details.
   a. Navigate to **Home > Track My Requests**
   b. Open the **Details** for this request and observe the **Request Items** and **Provisioning Engine** and **Interactions** items.

      Note: The status of the items within the request depends on when you're checking the request and when the *Perform Maintenance* task was last executed. Once Perform Maintenance runs, you should see an interaction for the **Finance Administration** workgroup and the other request items should have a provisioning status.

2. Review provisioning activities in Administrator Console.
   a. Navigate to **Gear > Administrator Console > Provisioning**
   b. Filter for Identity: **Richard.Jackson**
   c. Explore the different **information** buttons (under **Actions**)

3. Check email log.
   a. Find the emails sent to Richard's manager Patricia Jones. What objects does this tell her have been reassigned to her?

      _____

4. Navigate to the **Entitlement Catalog**
   a. View the **Accounts Receivable** entitlement on the Finance application
   b. Confirm that Patricia is now the owner.

Note: IdentityIQ reflects Richard's current account states, but you can also verify the provisioning actions were completed on the target systems themselves. For LDAP, use the LDAP Browser view the account. For Time Tracking and Chat, you can issue SQL statements against their databases. See the appendix for instruction on these validation actions, if you are interested.

Appendix

IDENTITYIQ IMPLEMENTATION AND ADMINISTRATION: ESSENTIALS

SailPoint IdentityIQ Version 8.1

With Rapid Setup

www.sailpoint.com

Table of Contents

Common IdentityIQ Synonyms

IdentityIQ terms as used internally to the product and their user interface synonyms:

Internal	User Interface
IdentityRequest	Access Request
Certification	Access Review
Link	Account
Workflow	Business Process
CertificationGroup	Certification
ManagedAttribute	Entitlement
Bundle	Role
TaskDefinition	Task

Basic Linux Commands

Command	Purpose
pwd	Displays current directory
cd *directorypath* cd */directorypath* cd .. cd ../../mydir/targetdir	Change directory starting from the current directory Change directory starting from the topmost directory Move backwards (or up) one directory level This example changes directory from the current directory, back two levels and then forward (or down) two levels
ls ls -l	List contents of current directory List detailed contents of current directory
alias	Displays Training virtual machine shortcuts
./*programname*	In the current directory, find and run the program called *programname*
[tab]	Used to autocomplete directory and file names Method: Enter the first few characters of a name (enough to represent a unique name) and press tab

IdentityIQ Installation Instructions

Your training virtual machine contains a Lab Reset tool which can be used to perform the IdentityIQ installation. Selecting the "1 – Install IdentityIQ, a patch (if present)" activity from the Lab Reset tool does the following:

- Removes existing IdentityIQ installation (if applicable).
- Installs IdentityIQ.
- Applies the patch (if applicable).
- Configures the database for your training environment.

The instructions below are the manual instructions for performing these same activities.

Overview

Our training scenario represents a typical implementation cycle with a customer. The client has provided us with the following:

- A running database server with host, port and login information provided.
- A pre-configured Tomcat Application Server instance.

We need to install IdentityIQ with the following requirements.

- Install IdentityIQ into the identityiq directory in the Tomcat webapps folder.
- Adjust the IdentityIQ Hibernate files to support our installation. Our installation needs to support the following:
    - 1 named extended identity attribute.
    - 10 searchable and indexed placeholder extended identity attributes.
- Generate the IdentityIQ database schema files and use these to create the IdentityIQ database within the MySQL database instance.
- Initialize IdentityIQ, Lifcycle Manager, and Rapid Setup.
- Start the application server.
- Confirm that everything is running okay.

Reset Virtual Machine to Remove IdentityIQ Installation

1. Navigate to the Desktop and open the **Lab Reset** tool.
2. Select the **3 – Reset VM to initial state** activity and select OK.

3. Select **OK** on the pop-up window.

4. After the activity completes, navigate to the **/home/spadmin/tomcat/webapps/identityiq** directory and confirm that it is empty.

Prepare Application Server and Install IdentityIQ war

1. Stop the Tomcat Application Server.

Note: It doesn't hurt to issue the stop command when Tomcat isn't running, and it's important to ensure that it is stopped before IdentityIQ is installed.

   a. From the desktop, run the shortcut labeled **Stop Tomcat** or;

   b. Alternatively, you can open a Linux terminal window and type the following command: **`StopTomcat`**

2. Unzip and extract the IdentityIQ war file.

   The IdentityIQ installation files have been downloaded from Compass for you and placed in the InstallImages directory.

Note: For help navigating in Linux, see Basic Linux Commands earlier in the Appendix.

   a. Open a Linux terminal window and navigate to the directory: **/home/spadmin/InstallImages**

      i. At the $ command prompt, type:

```
cd InstallImages
```

   b. Enter the following command to view the contents of the directory:

```
ls
```

   c. Enter the name of the IdentityIQ zip file:

      i. IdentityIQ zip file: _____

   d. If there is a jar file, we will install this patch. Enter the name of the IdentityIQ jar file:

      i. IdentityIQ patch file: _____

   e. Run the following command to extract the **identityiq.war** file from the IdentityIQ-**X**.**X**.zip file and place it in the installation directory for IdentityIQ: **/home/spadmin/tomcat/webapps/identityiq**

   Note: Change the **X** to the appropriate version number as noted on the zip file, and do not include patches. For example, for both IdentityIQ v8.0 and IdentityIQ v8.0p2, the command is *unzip identityiq-8.0.zip identityiq.war -d /home/spadmin/tomcat/webapps/identityiq*

```
unzip identityiq-X.X.zip identityiq.war -d
/home/spadmin/tomcat/webapps/identityiq
```

f. Run the following command to navigate to the installation directory for IdentityIQ:

```
cd /home/spadmin/tomcat/webapps/identityiq
```

g. Extract the war file:

```
jar -xvf identityiq.war
```

Configure Extended Searchable Attributes

1. For our implementation, we have documented requirements for an extended identity attribute that needs to be searchable: *department*. Thus, we will add it as a named attribute.

CAUTION: The attribute names used for the database must exactly match those defined in IdentityIQ, including case.

a. Configure the Hibernate XML file to add a named, searchable, indexed, extended attribute.

b. Using the File Browser, locate the file:
/home/spadmin/tomcat/webapps/identityiq/WEB-INF/classes/sailpoint/object/IdentityExtended.hbm.xml

c. Edit the file using any editor (gedit is provided in the VM and is a good editor for editing XML files) and add the following two lines to the XML.

Note: There is a comment in this file with an example named attribute called *costCenter*. To reduce the amount of typing for adding the named attributes, copy and edit the example.

```
<property name="department" type="string" length="450"
access="sailpoint.persistence.ExtendedPropertyAccessor" index="
spt_identity_department_ci"/>
```

About gedit: If red highlights are displayed, there is a syntax error in the XML.

d. This exercise provides for the *department* extended attribute to be created in the database. Later in this training course, after IdentityIQ is installed, you will create this extended attribute within IdentityIQ. Until it is created within IdentityIQ, you will see an error that it is not defined in the Identity object configuration.

We know that we will need additional searchable and indexed extended identity attributes, but we don't yet know which ones. For these, we will specify 10 placeholder attributes. The default is 5 searchable and indexed attributes and another 5 searchable but not indexed. Configure the Hibernate XML file to support 10 searchable *and indexed* attributes per identity. Edit the file to add the indexing to match the following:

```
<property name="extended1" type="string" length="450"
            index="spt_identity_extended1_ci"/>
    <property name="extended2" type="string" length="450"
            index="spt_identity_extended2_ci"/>
    <property name="extended3" type="string" length="450"
            index="spt_identity_extended3_ci"/>
    <property name="extended4" type="string" length="450"
            index="spt_identity_extended4_ci"/>
    <property name="extended5" type="string" length="450"
            index="spt_identity_extended5_ci"/>
    <property name="extended6" type="string" length="450"
            index="spt_identity_extended6_ci"/>
    <property name="extended7" type="string" length="450"
            index="spt_identity_extended7_ci"/>
    <property name="extended8" type="string" length="450"
            index="spt_identity_extended8_ci"/>
    <property name="extended9" type="string" length="450"
            index="spt_identity_extended9_ci"/>
    <property name="extended10" type="string" length="450"
            index="spt_identity_extended10_ci"/>
```

2. Check for common errors.
   a. Confirm that the case used for the named attributes is correct.
   b. Confirm that the entries for extended6 through extended10 include only one tag closure: "/>".
3. Save the changes to the file.

Configure the Database

1. Configure permissions on the iiq command so that we may execute it.

a. Using a Linux terminal window, navigate to the **/home/spadmin/tomcat/webapps/identityiq/WEB-INF/bin** directory

b. Run the following command to mark the iiq command as executable:

```
chmod +x iiq
```

2. Generate IdentityIQ Schema files.

a. Run the following command from the Linux terminal to generate the database schema files:

```
./iiq schema
```

3. Load the MySQL Schema file into MySQL to create the IdentityIQ database.

a. Using the command prompt, navigate to the **/home/spadmin/tomcat/webapps/identityiq/WEB-INF/database** directory and run the following commands to log in to MySQL:

```
mysql -u root -p
Enter password: root
```

b. Within the MySQL command line utility, type the following to load the schema into MySQL:

```
mysql> source create_identityiq_tables.mysql
```

c. When the command finishes running, type the following to confirm that the **identityiq** database has been created properly. The other databases are not important. Make sure that **identityiq** is in the list of databases.

```
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| bugtracking        |
| chat               |
| identityiq         |
| identityiqPlugin   |
| mysql              |
| performance_schema |
| sys                |
| timetracking       |
+--------------------+
9 rows in set (0.00 sec)
```

d. Type **quit** to exit the MySQL command line utility.

4. Review and update the Database Settings that IdentityIQ uses to connect to the database.

    a. Open the configuration file for the IdentityIQ database:
    /home/spadmin/tomcat/webapps/identityiq/WEB-INF/classes/iiq.properties

    b. In the MySQL/Aurora (without SSL) section, append the following to the useServerPrepStmts and dataSource.url lines

    ```
    &serverTimezone=UTC
    ```

    c. The table below lists the most commonly edited values. Confirm the default values.

Database Type	Determined by which database section is uncommented. **Default**: MySQL
dataSource.username	Username to use when connecting to the database **Default**: identityiq
dataSource.password	Encrypted password to use when connecting to the database. **Default**: identityiq **Note**: generated using the **iiq encrypt <password>** command
dataSource.url	Defines the host name, port and database to connect to. **Default**: use the standard port on localhost, database name = identityiq
dataSource.driverClassName	Defines the driver to use when connecting to the database **Default**: com.mysql.jdbc.Driver

Note: For best performance, it is ***VERY*** important to update the default JDBC driver supplied with IdentityIQ to the most current driver supplied by your database vendor.

Patch IdentityIQ

Overview

The patch process involves three major steps. Note that each patch install may not require all three steps. Always read the release notes for any patch in their entirety before patching a system.

- Deploy new product code (deploy the patch jar file in our install directory).
- Upgrade the database tables to support any changes required by the patch.
    - New Tables
    - Deprecated Tables
- Run the patch script to convert any data as required by the new patch.

Confirm Necessity of Patch

Verify that your virtual machine contains a patch by reviewing your entry a few pages back in the section *Prepare Application Server and Install IdentityIQ War File*. Alternatively, view the contents of the directory **/home/spadmin/InstallImages**.

If it does not contain a patch, skip this section.

Patch Installation

1. Stop the Tomcat Application Server.

   Options to stop Tomcat:

   Option 1: From the desktop, run the shortcut labeled "**Stop Tomcat**" -or-

   Option 2: Type the following command at a Linux terminal window: **`StopTomcat`**

2. Extract the IdentityIQ Patch file.

   a. Use the File Browser to locate the **identityiq-X.XpX.jar** (where 'X' represents the version and patch numbers) file under **/home/spadmin/InstallImages** and copy it to the installation directory for IdentityIQ: **/home/spadmin/tomcat/webapps/identityiq**

   b. Open a Linux terminal window and navigate to the directory: **/home/spadmin/InstallImages**

   c. Run the following command to copy the **identityiq-X.XpX.jar** file and place it in the installation directory for IdentityIQ: **/home/spadmin/tomcat/webapps/identityiq**

Note: Change the **X** to the appropriate version and patch numbers

```
cp identityiq-X.XpX.jar
/home/spadmin/tomcat/webapps/identityiq
```

   d. Using a Linux terminal window, navigate to the **/home/spadmin/tomcat/webapps/identityiq** directory and run the following command to extract the patch jar file (change the X to the version and patch):

```
jar –xvf identityiq-X.XpX.jar
```

3. Patch the IdentityIQ Database.

   a. Using the command prompt, navigate to the **/home/spadmin/tomcat/webapps/identityiq/WEB-INF/database** directory and run the following commands to log in to MySQL:

```
mysql –u root –p
Enter password: root
```

b. Within the MySQL command line utility, type the following to upgrade the IdentityIQ schema (change the X):

```
mysql> source upgrade_identityiq_tables-X.XpX.mysql
```

c. Type **quit** to exit the MySQL command line utility.

4. Apply the Patch.

a. Using your Linux terminal, navigate to:
/home/spadmin/tomcat/webapps/identityiq/WEB-INF/bin

b. Run the following command (change the X):

```
./iiq patch X.XpX
```

c. Wait for the patch command to finish and watch for any errors. You should see an error regarding the extended attribute department. You have not yet completed defining this attribute to IdentityIQ. If you also see a Pool not open error, ignore it.

5. Confirm the installation.

a. Run the IdentityIQ Console either through the provided desktop shortcut or through a Linux terminal.

b. Run the following command and confirm that the version and patch match your virtual machine's name.

```
>about
```

c. **Quit** the console.

6. Start the Tomcat Application Server and wait while the application server starts.

Options to start Tomcat:

Option 1: From the desktop, run the "**Start Tomcat**" shortcut -or-

Option 2: Type the following command in a Linux terminal: **`StartTomcat`**

Initialize IdentityIQ and Verify your Installation

1. Using the IdentityIQ Console, import the default IdentityIQ objects to initialize the system. The console starts an instance of IdentityIQ and may take a few moments to start. You will know that it is running when you see the > prompt.

a. Using a Linux terminal, navigate to:
/home/spadmin/tomcat/webapps/identityiq/WEB-INF/bin

b. Run the following command: **`./iiq console`**

Note: In the training environment, the console can also be run from the desktop shortcut.

c. At the console command prompt, load the default IdentityIQ objects using the following commands:

```
import init.xml
import init-lcm.xml
import init-rapidsetup.xml
```

d. When the import is complete, **quit** the console.

2. Start the Tomcat Application Server and wait 30 to 60 seconds while the application server starts.

   Options to start Tomcat:

   Option 1: From the desktop, run the "**Start Tomcat**" shortcut

   Option 2: Type the following command in a Linux command terminal: **`StartTomcat`**

To monitor the start process in the log file, use the desktop shortcut, **Tail Tomcat Standard Out**. The server has started when you see the phrase: **INFO: Server startup in xxxxx ms.**

3. When Tomcat has started, log in to IdentityIQ using Firefox.

   a. Click the Firefox bookmark in the VM and go to: http://localhost:8080/identityiq/

   b. Log into IdentityIQ as **spadmin/admin**

   c. If you can successfully log in and see the IdentityIQ application, then your installation was successful. If not, review the preceding steps.

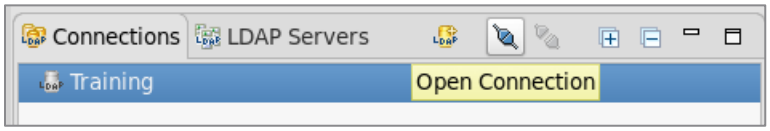
Congratulations! You have completed the process to install IdentityIQ and Rapid Setup.

Natively Verifying Provisioning in Lab environment

The IdentityIQ Administrator Console provisioning transaction log contains the provisioning actions generated from IdentityIQ however sometimes it is informative to verify provisioning activity natively in the simulated applications. You can use these instructions to view the state of an application account before and after you initiate a provisioning action from within IdentityIQ.

LDAP

1. Using the desktop shortcut, launch the **LDAP Browser**
2. In the Connections window, select **Training** and click **Open Connection**

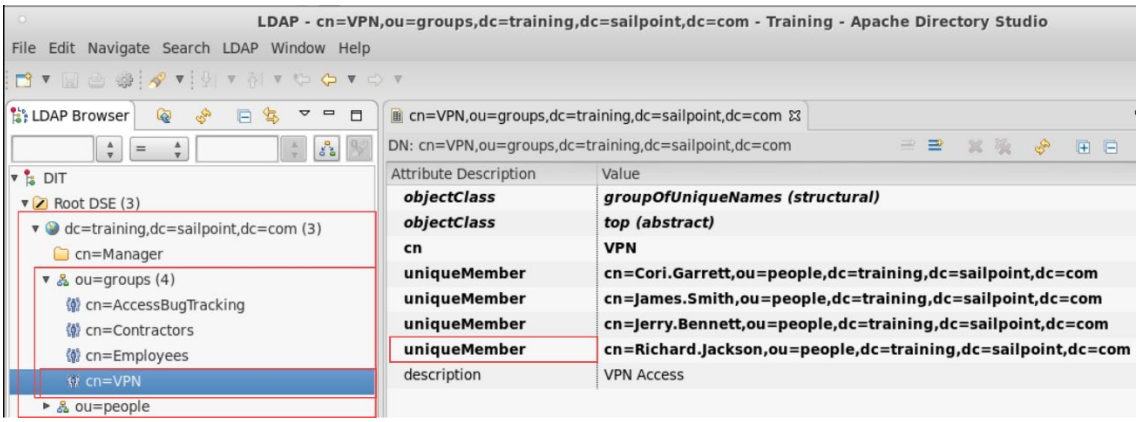


Note: If you're not able to connect, you can check if LDAP is running (from a terminal window, enter **CheckLDAP**). If necessary, start LDAP (from a terminal window, enter **StartLDAP**)

LDAP Group Membership

In IdentityIQ, LDAP group membership is show as an entitlement associated with an application account. However, in the LDAP instance in your training environment, LDAP group membership is stored on the group object itself. This means if you want to verify if an account is or is not a member of a LDAP group you must find the group itself, not the account you are interested in.

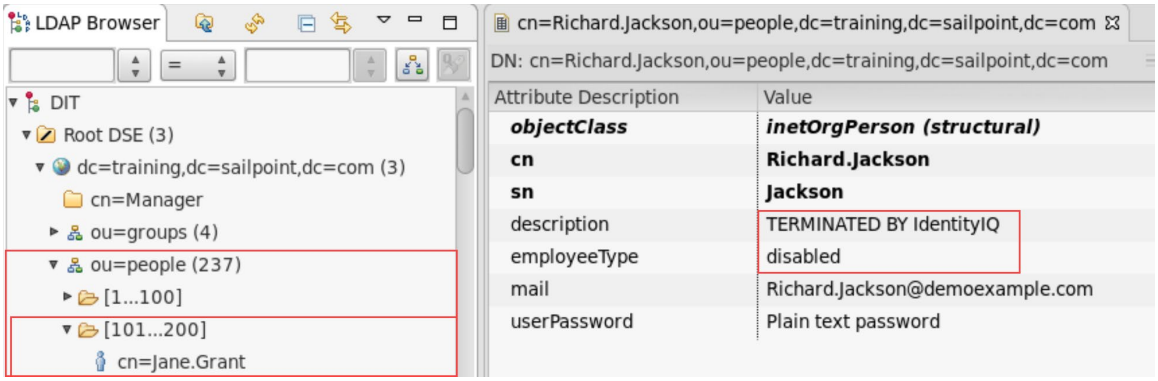
3. Expand **dc=training,dc=sailpoint,dc=com**, then expand **ou=groups**
4. Confirm the user account dn is listed as a uniqueMember of the group.



LDAP Account Attributes

5. Expand **ou=people**

6. User accounts are listed alphabetically by dn and group by 100 accounts. Expand these groupings of user account and select the account to view the account details.



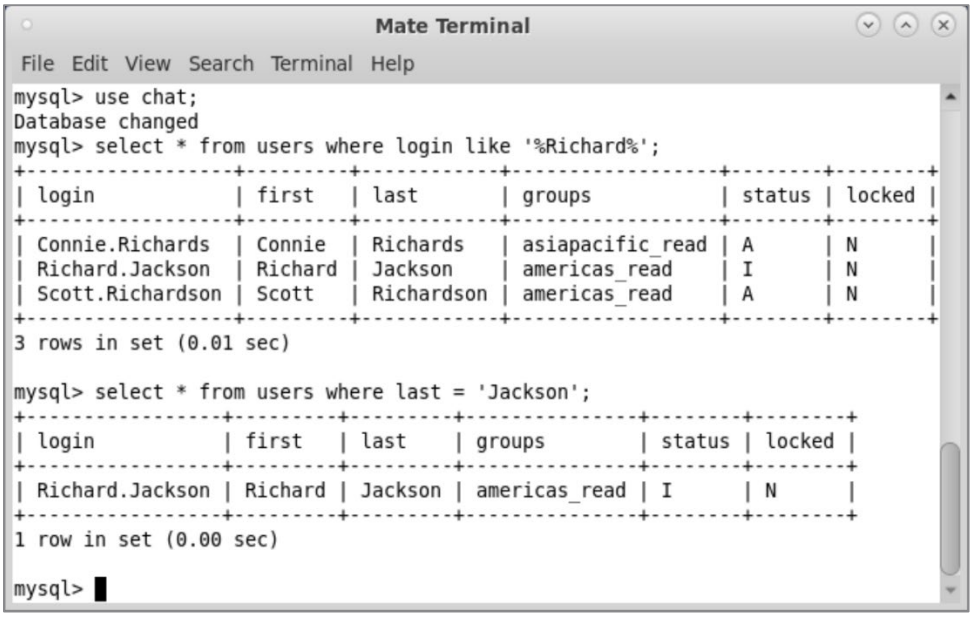
Chat

1. Open a Linux terminal window, and login to MySQL:

```
[spadmin@training ~]$ mysql -u root -p
Enter password: root
```

a. Search for identities with a select statement. Remember the names are case-sensitive.

```
mysql> use chat;
mysql> select * from users where login LIKE '%Richard%';
mysql> select * from users where last = 'Jackson';
```



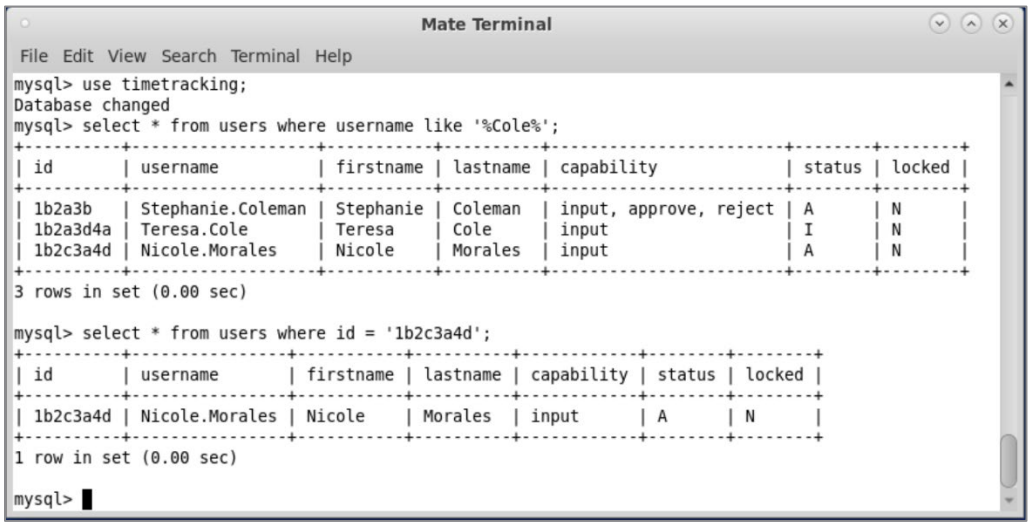
Time Tracking

1. Open a Linux terminal window, and login to MySQL:

```
[spadmin@training ~]$ mysql -u root -p
Enter password: root
```

2. Search for identities with a select statement. Remember the names are case-sensitive.

```
mysql> use timetracking;
mysql> select * from users where username LIKE = '%Cole%';
mysql> select * from users where id = '1b2c3a4d';
```



Bug Tracking

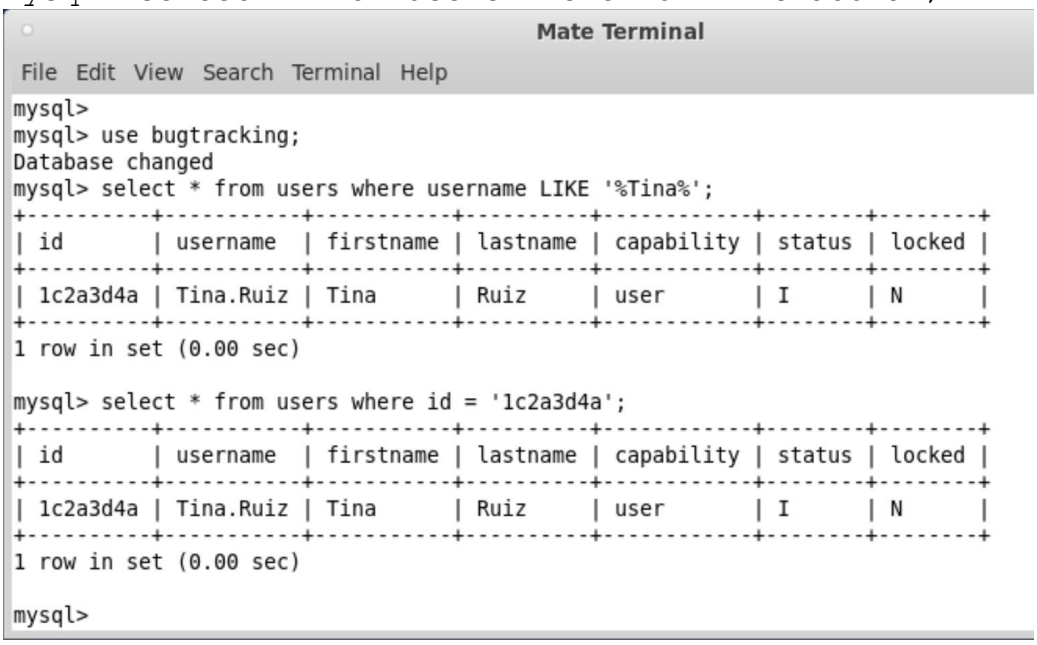
1. Open a Linux terminal window, and login to MySQL:

```
[spadmin@training ~]$ mysql -u root -p
Enter password: root
```

2. Search for identities with a select statement. Remember the names are case-sensitive.

```
mysql> use bugtracking;
mysql> select * from users where username LIKE = '%Tina%';
```

```
mysql> select * from users where id = '1c2a3d4a';
```



Using Lab Reset Tool

Your training virtual machine contains a Lab Reset tool that can be used for resetting IdentityIQ to a certain state.

The Lab Reset tool has three options:

1 – Install IdentityIQ, a patch (if present)

This activity does the following:

- Removes existing IdentityIQ databases.
- Installs IdentityIQ with the appropriate version and patch.
- Resets the class databases (LDAP, Time Tracking, Bug Tracking, Chat).
- Resets the class files to the initial state as these may have been modified during lab execution.

2 – Reset exercise state from backup files

IdentityIQ must be installed in order to run this activity. If IdentityIQ is not installed, you will see an error and the tool will abort the operation.

This activity does the following:

- Sets IdentityIQ to the point where the specified exercise can be started.
- Resets the class databases (LDAP, Time Tracking, Bug Tracking, Chat) to the proper point.
- Resets the class files to the initial state as these may have been modified during lab execution.

3 – Reset VM to initial state

This activity will reset the virtual machine to a fresh state. Choose this activity if you want to perform the manual IdentityIQ installation steps (see instructions in Appendix). This activity does the following:

- Removes IdentityIQ
- Resets the class databases (LDAP, Time Tracking, Bug Tracking, Chat) to their initial state.
- Resets the class files to the initial state as these may have been modified during lab execution.