Identity Cubes, Authoritative Applications, and Aggregation

Fundamentals of IdentityIQ Implementation

IdentityIQ 7.0

Overview

Identity Cubes, Authoritative Applications, and Aggregation

- Identity Cube Overview
- Authoritative Application Configuration
- Identity Mappings
- Aggregation and Refresh
- IdentityIQ User Access Management

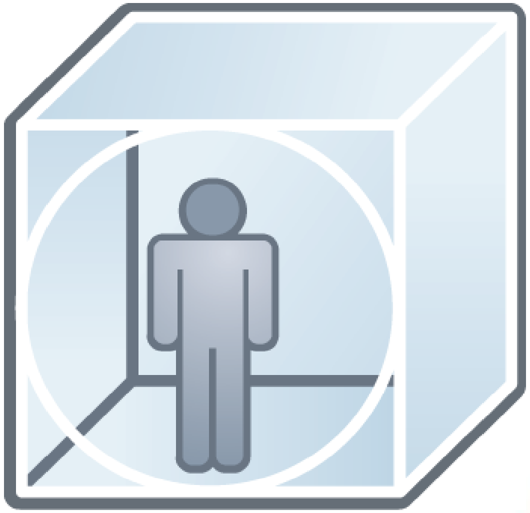
Identity Cubes

Identity Cube

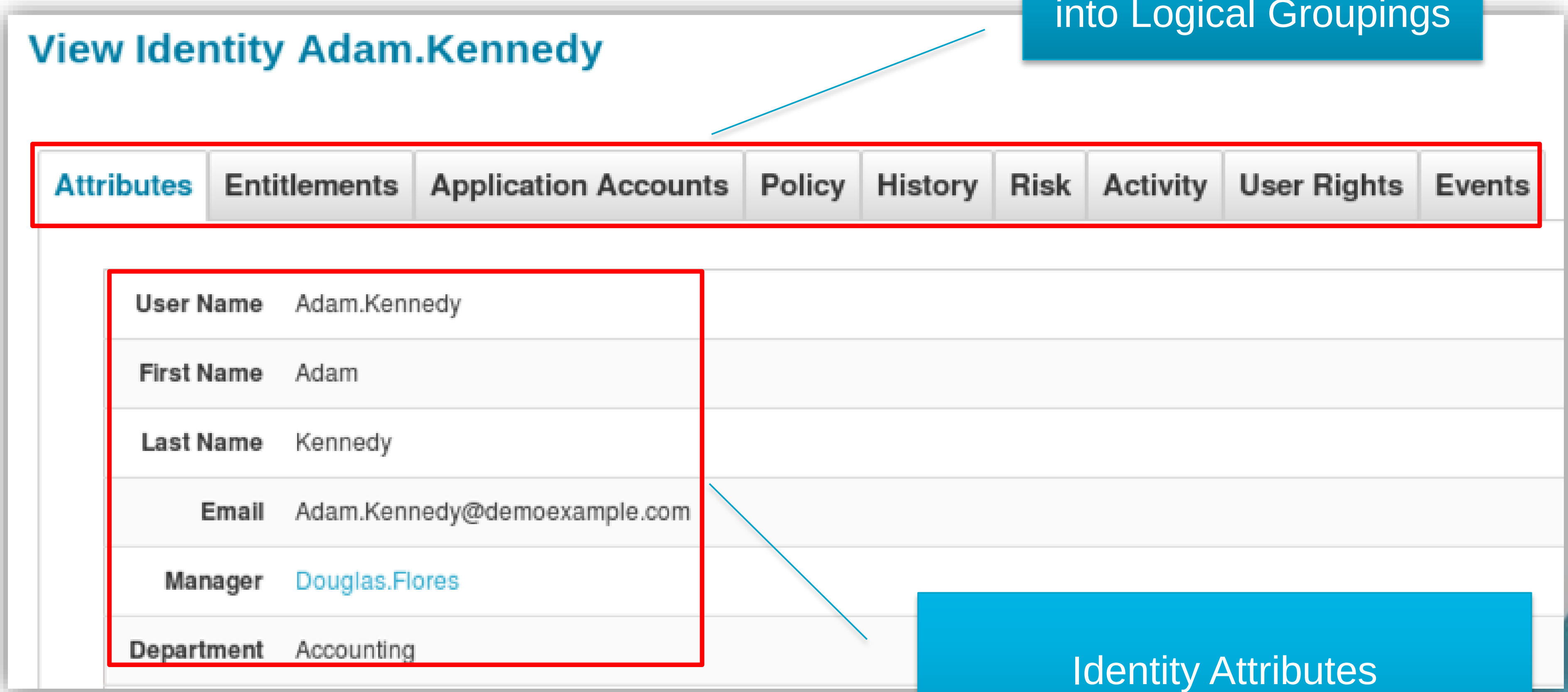
- Term to refer to each unique identity stored in IdentityIQ repository
- Stores all information known about an identity

  Examples:

  - Identity Attributes
  - Application Accounts
  - Entitlements/Roles
  - History
  - Risk Score
  - Policy Violations
  - User Rights (Capabilities/Scoping)
- Information on the cube is
  - Discovered
  - Requested
  - Assigned
  - Calculated



Identity Cube – User Interface



View Identity Adam.Kennedy

User Name	Adam.Kennedy
First Name	Adam
Last Name	Kennedy
Email	Adam.Kennedy@demoexample.com
Manager	Douglas.Flores
Department	Accounting

Tabs divide identity data into Logical Groupings

Identity Attributes are sourced from Authoritative Sources or by Rules

How are Identity Cubes Created?

- Identity Cube creation – two mechanisms
  - Automatically through account aggregation
    - Aggregate from systems of record – *Authoritative Application(s)*
      - Creates authoritative cubes
    - Aggregate from systems of interest – *Non-Authoritative Applications*
      - If account not matched to authoritative cube, creates non-authoritative cube (more later)
  - Manually using Lifecycle Manager
    - Using the *Create Identity* or *Self-registration* option in Lifecycle Manager
      - Identity Attributes are entered as part of the creation process

Initial Configuration

Overview

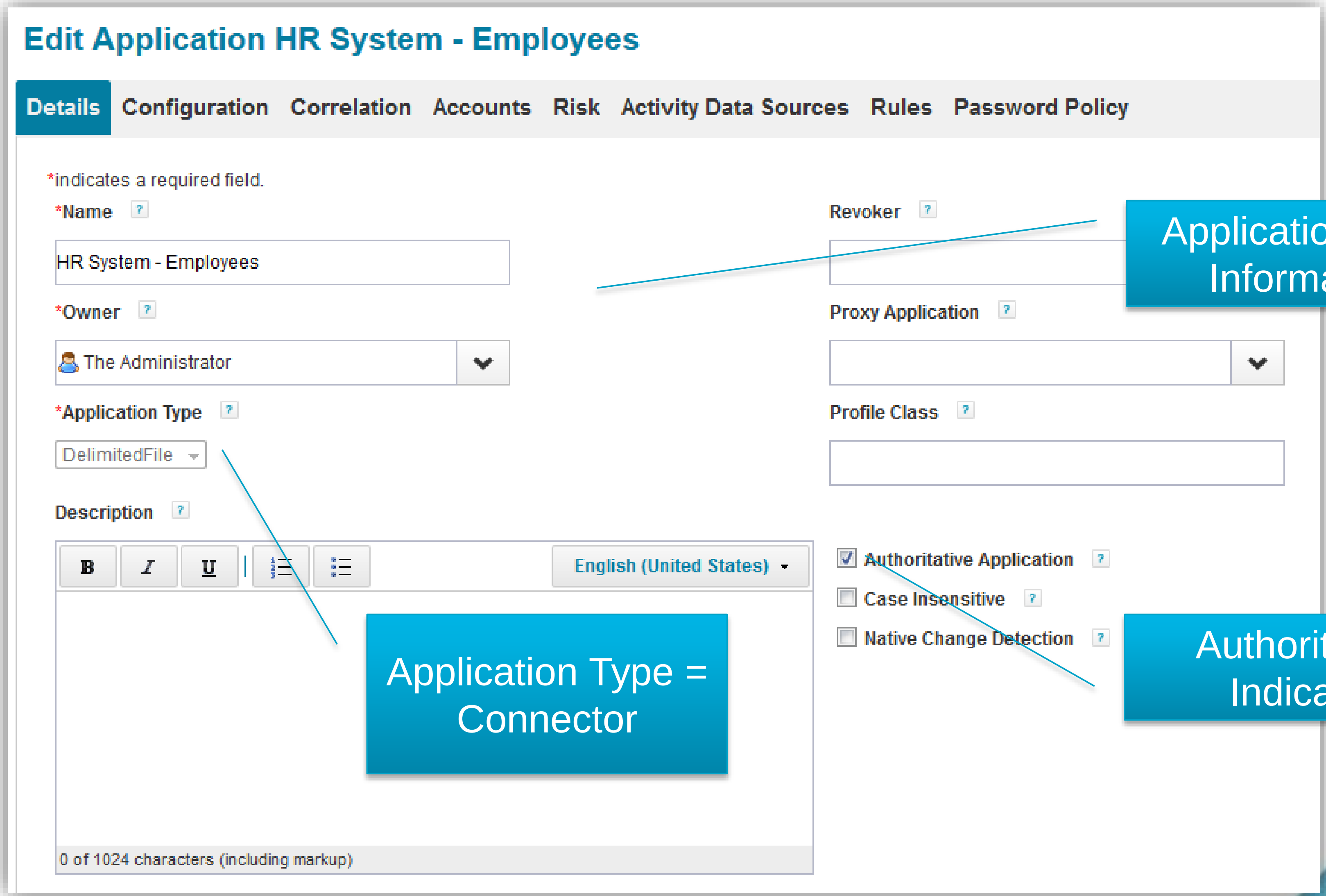
- Configure authoritative application(s)
- Configure identity attributes
  - Define custom identity attributes
  - For custom and standard, define how they are populated
- Define and run aggregation task(s)
  - Read authoritative accounts
  - Create authoritative cubes
- Run default refresh task
  - Populate identity attributes
  - Mark managers
- Specify users with special capabilities (i.e. System Administrator)
- Reset spadmin password

Configuring Authoritative Applications

Applications/Connectors

- Application
  - Representation of a target resource (i.e. Active Directory, SAP)
  - Configuration includes
    - Meta Information: name, description, owner, revoker
    - Account Schema and optional Group Schema
    - Connector
    - Application Rules
- Connector
  - Software component to connect to a target resource and read/write data
  - Configuration includes
    - Connection Specifics (i.e. Hostname, Port, Authentication)
    - Connector Rules (for data manipulation)
  - Provides normalized resource object

Application/Connector Configuration



Edit Application HR System - Employees

*indicates a required field.

*Name: HR System - Employees

*Owner: The Administrator

*Application Type: DelimitedFile

Description

0 of 1024 characters (including markup)

Revoker

Proxy Application

Profile Class

☑ Authoritative Application

□ Case Insensitive

□ Native Change Detection

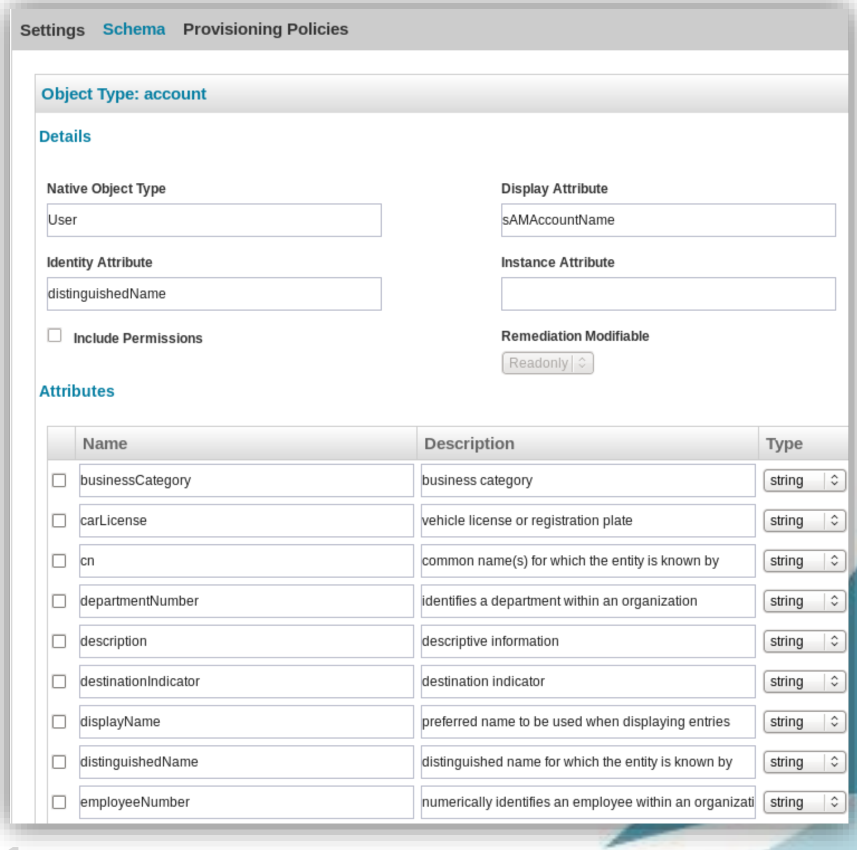
Application Meta Information

Application Type = Connector

Authoritative Indicator

Account Schema

- Represents individual accounts on a target resource
- Defines what data to read
- Defines how to interpret data
- Required for each application



Object Type: account

Details

Native Object Type: User

Display Attribute: sAMAccountName

Identity Attribute: distinguishedName

Instance Attribute:

□ Include Permissions

Remediation Modifiable: Readonly

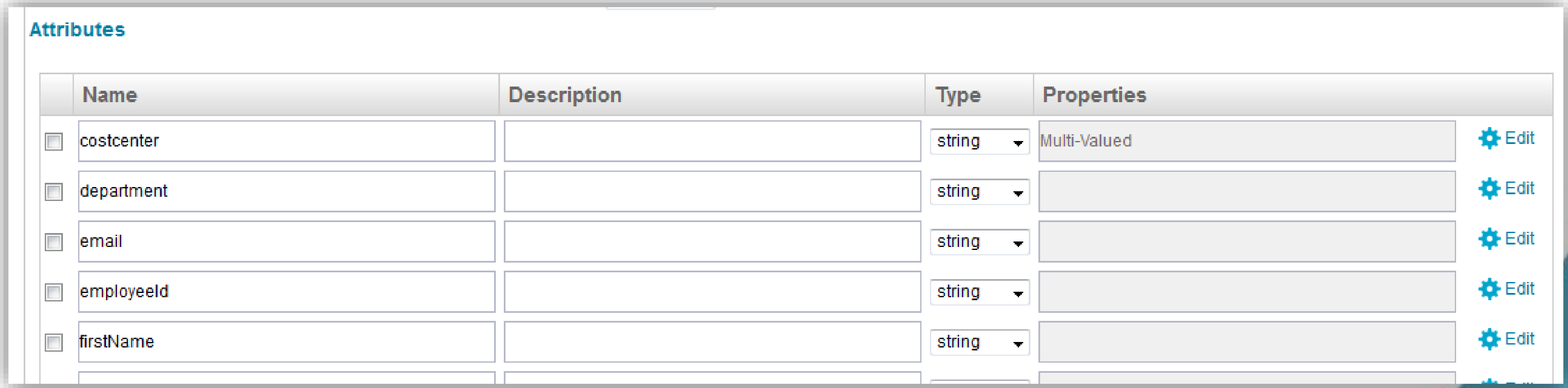
Attributes

	Name	Description	Type
□	businessCategory	business category	string
□	carLicense	vehicle license or registration plate	string
□	cn	common name(s) for which the entity is known by	string
□	departmentNumber	identifies a department within an organization	string
□	description	descriptive information	string
□	destinationIndicator	destination indicator	string
□	displayName	preferred name to be used when displaying entries	string
□	distinguishedName	distinguished name for which the entity is known by	string
□	employeeNumber	numerically identifies an employee within an organizati	string

Account Schema

Account Attribute Data

- Define which account attributes to collect
  - Pre-defined for certain connectors
- Define how to interpret the data
  - What data type (string, long, int, boolean, group reference)?



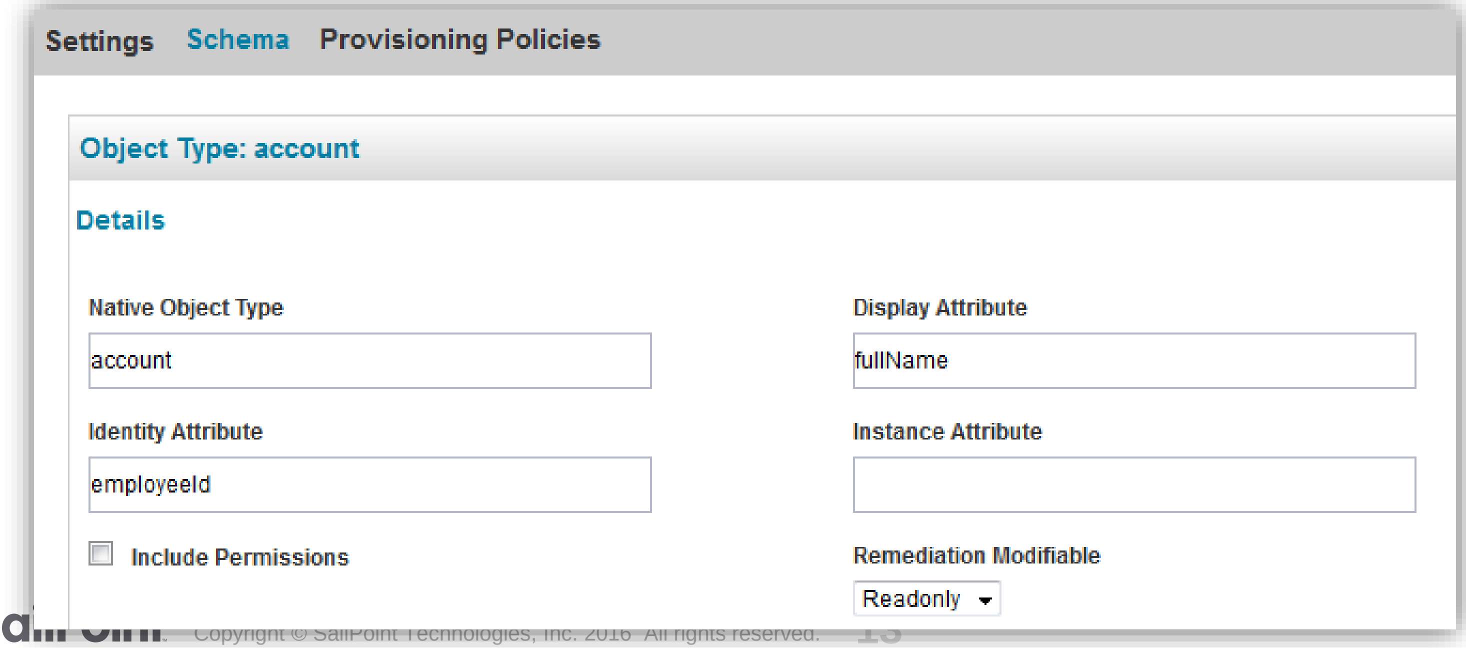
Attributes

	Name	Description	Type	Properties	
□	costcenter		string ▾	Multi-Valued	Edit
□	department		string ▾		Edit
□	email		string ▾		Edit
□	employeeId		string ▾		Edit
□	firstName		string ▾		Edit

Account Schema

Schema Header

- Identify key data to IdentityIQ
  - Identity Attribute
    - Identifies which attribute holds unique identity id (username, id)
  - Display Attribute
    - Identifies which attribute holds display attribute
    - Used for friendly display name



Settings | Schema | Provisioning Policies

Object Type: account

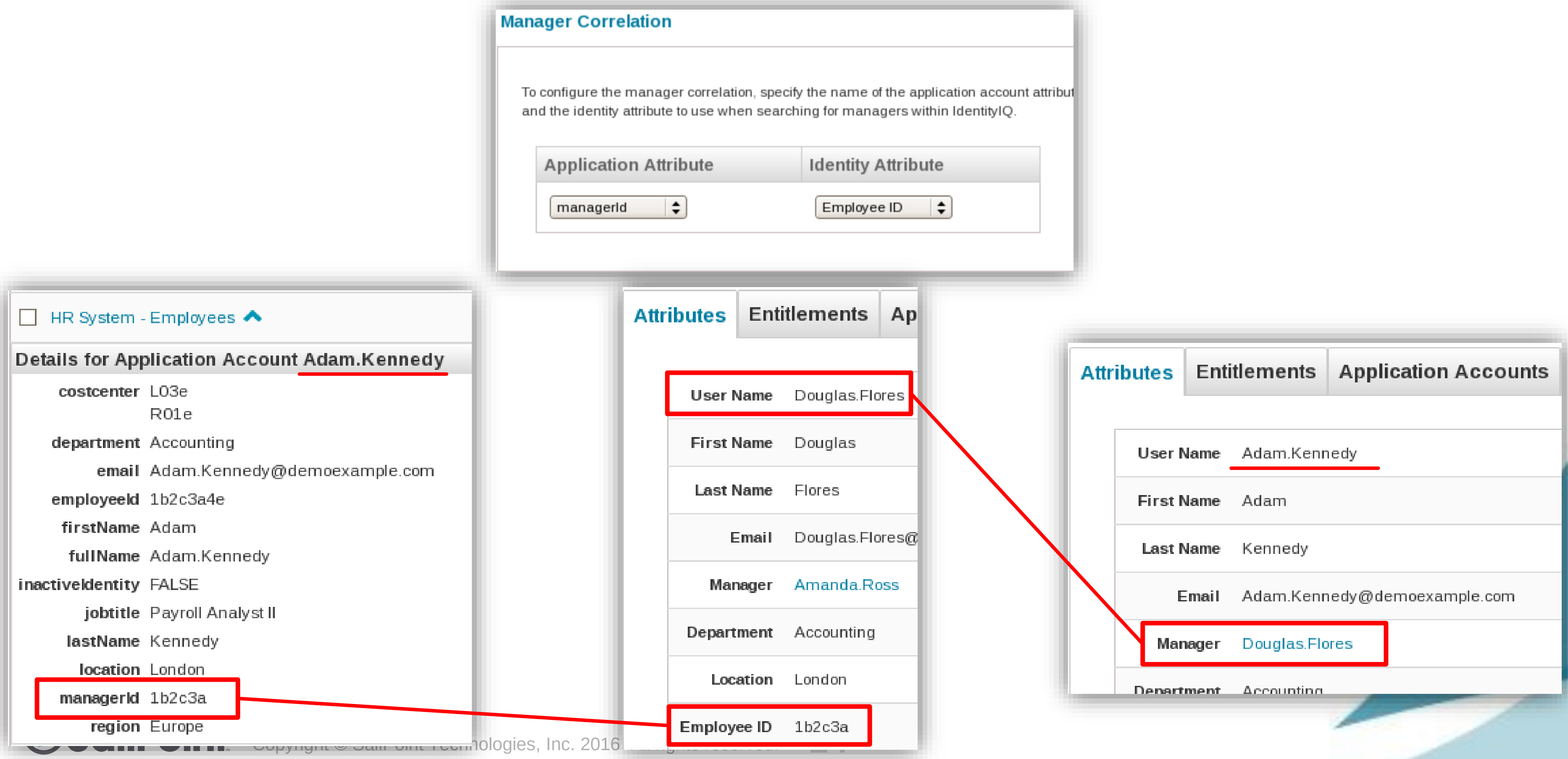
Details

Native Object Type: account	Display Attribute: fullName
Identity Attribute: employeeId	Instance Attribute:
□ Include Permissions	Remediation Modifiable: Readonly

Manager Correlation

Authoritative Applications

- Define which application attribute defines a user’s manager
- Map the application attribute to the manager’s Identity Attribute



Manager Correlation

To configure the manager correlation, specify the name of the application account attribut
and the identity attribute to use when searching for managers within IdentityIQ.

Application Attribute	Identity Attribute
managerId	Employee ID

☐ HR System - Employees

Details for Application Account Adam.Kennedy

costcenter	L03e R01e
department	Accounting
email	Adam.Kennedy@demoexample.com
employeeId	1b2c3a4e
firstName	Adam
fullName	Adam.Kennedy
inactiveIdentity	FALSE
jobtitle	Payroll Analyst II
lastName	Kennedy
location	London
managerId	1b2c3a
region	Europe

User Name	Douglas.Flores
First Name	Douglas
Last Name	Flores
Email	Douglas.Flores@
Manager	Amanda.Ross
Department	Accounting
Location	London
Employee ID	1b2c3a

User Name	Adam.Kennedy
First Name	Adam
Last Name	Kennedy
Email	Adam.Kennedy@demoexample.com
Manager	Douglas.Flores
Department	Accounting

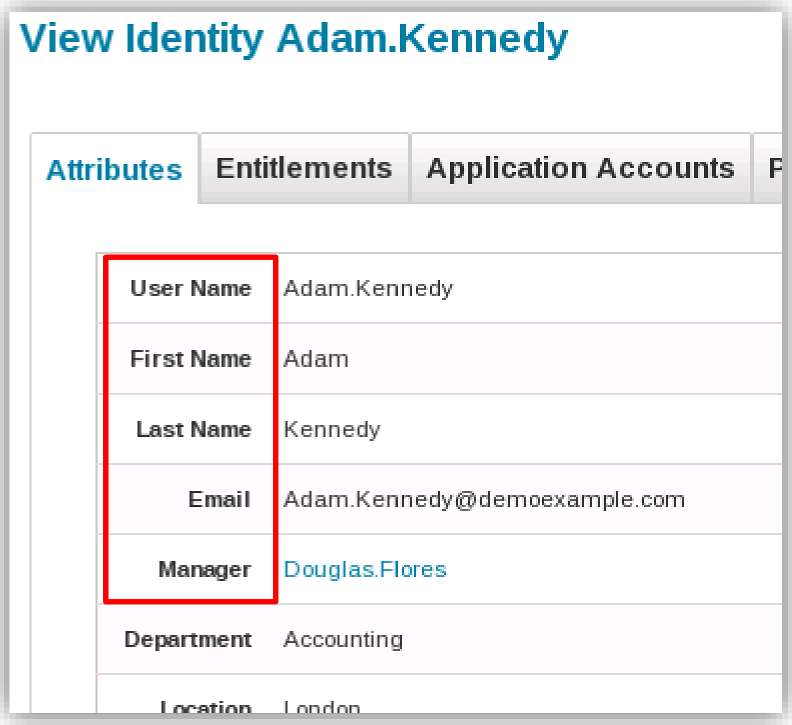
Application Rules

- Types
  - Manager Correlation Rule (when simple matching is not enough)
    - Build and maintain manager hierarchy
  - Creation Rule
    - Perform customizations at cube creation time

      Example: *Set default IdentityIQ password*
  - Correlation Rule (more in next presentation)
    - Build and maintain account correlations
  - Customization Rule
    - Modify/normalize incoming account data prior to saving to an Identity
- Can be shared between applications

Identity Attributes and Mappings

Identity Attributes



View Identity Adam.Kennedy

User Name	Adam.Kennedy
First Name	Adam
Last Name	Kennedy
Email	Adam.Kennedy@demoexample.com
Manager	Douglas.Flores
Department	Accounting
Location	London

- Standard Attributes
  - Used to support basic system functionality
    - DisplayName
    - First Name
    - Last Name
    - Inactive
    - Manager
    - Email
  - Searchable by default
- Extended Attributes
  - Identity Attributes defined specifically for an installation
  - Add as many as required to support your needs
  - Searchable attributes can be specified
    - Limited by number of searchable extended attributes defined in DB

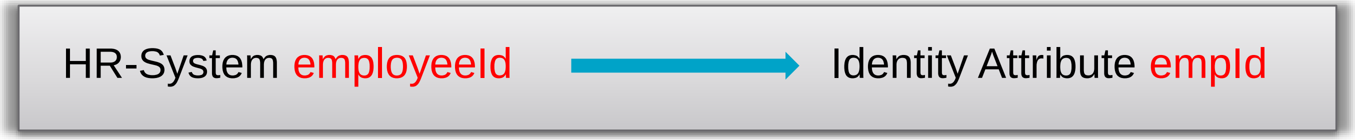
Identity Attribute Mappings

- Identity Mappings used to add new Identity Attributes

  Example: *Cost Center, Employment Status, Job Title*

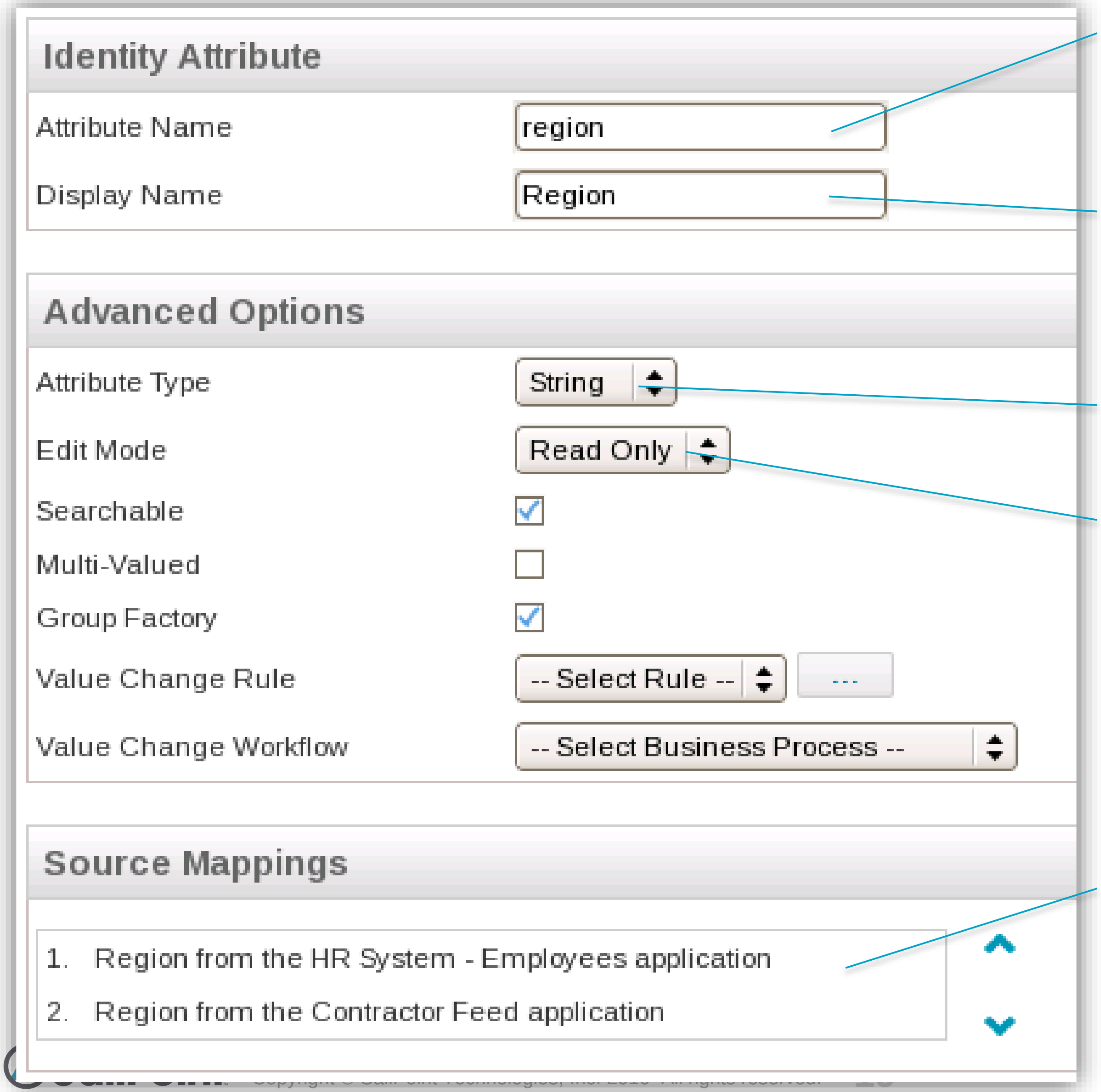
- Identity Mappings define source for Identity Attributes
  - Source for all attributes (standard and extended) must be specified
  - Typically sourced from authoritative sources
  - Can be sourced/modified with a rule

    Example: *Parse Job Code value to determine if employee is full-time or part-time*



HR-System employeeId → Identity Attribute empId

Identity Mappings Configuration



Identity Attribute

Attribute Name	region
Display Name	Region

Advanced Options

Attribute Type	String
Edit Mode	Read Only
Searchable	☑
Multi-Valued	□
Group Factory	☑
Value Change Rule	-- Select Rule --
Value Change Workflow	-- Select Business Process --

Source Mappings

1. Region from the HR System - Employees application
2. Region from the Contractor Feed application

Property name for the attribute

Value to display – can be a message key for localization support

String or Identity

Read only or editable attribute

Source of Attribute: Application Attribute or Rule

Identity Attribute Mappings

Utilizing the Data

- Identity Mappings specify how to use the data
  - Searchable
    - Correlation
    - Analytics, Reporting, Searching
  - Multi-valued

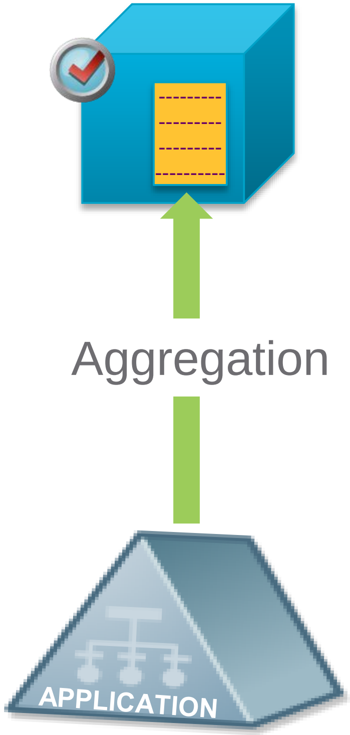
    Example: *User may belong to more than one cost center*
  - Group factories
    - Support dynamically generated groupings of identities based on the attribute

      Example: *All users in each region become a group*
    - Groups used to filter cubes included in actions

      Example: *Refresh only identities from a particular region*

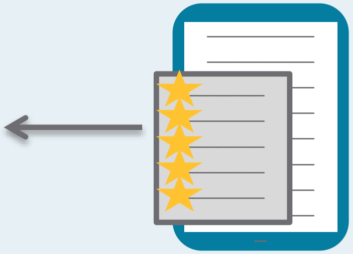
Aggregation and Refresh Tasks

Account Aggregation Tasks



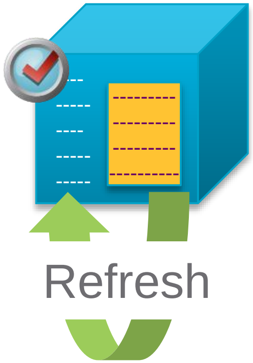
- Purpose
  - Read data from target applications to account attributes
- Use Application/Connector/Schema information
- Created from an Account Aggregation task template
- Many configuration options
  - Which Applications to Aggregate (required)
  - Detect Deleted Accounts (best practice)
  - And many more…
- Schedule frequency dependent upon
  - Use case
    - Compliance – prior to certification campaign (i.e. quarterly)
    - Provisioning – often daily
  - Importance of source application (i.e. authoritative, sensitive/risky)

Aggregation Strategies

	IdentityIQ	Application
Process All - Every account read and processed - Task option ***Disable optimization of unchanged accounts*** = ***true***		
IdentityIQ-based Optimization (default) - Every account read - Only those with changes are processed - Task option ***Disable optimization of unchanged accounts*** = ***false***		
Custom Delta Processing - Manage own change (i.e. write changed accounts to a flat file and process flat file) - Task option ***Detect deleted accounts*** = ***false***		
Connector-based Delta Aggregation* - Read and process only accounts with changes that have taken place after benchmark - lastModData, usnChanged, etc. - Task option ***Enable Delta Aggregation*** = ***true***		

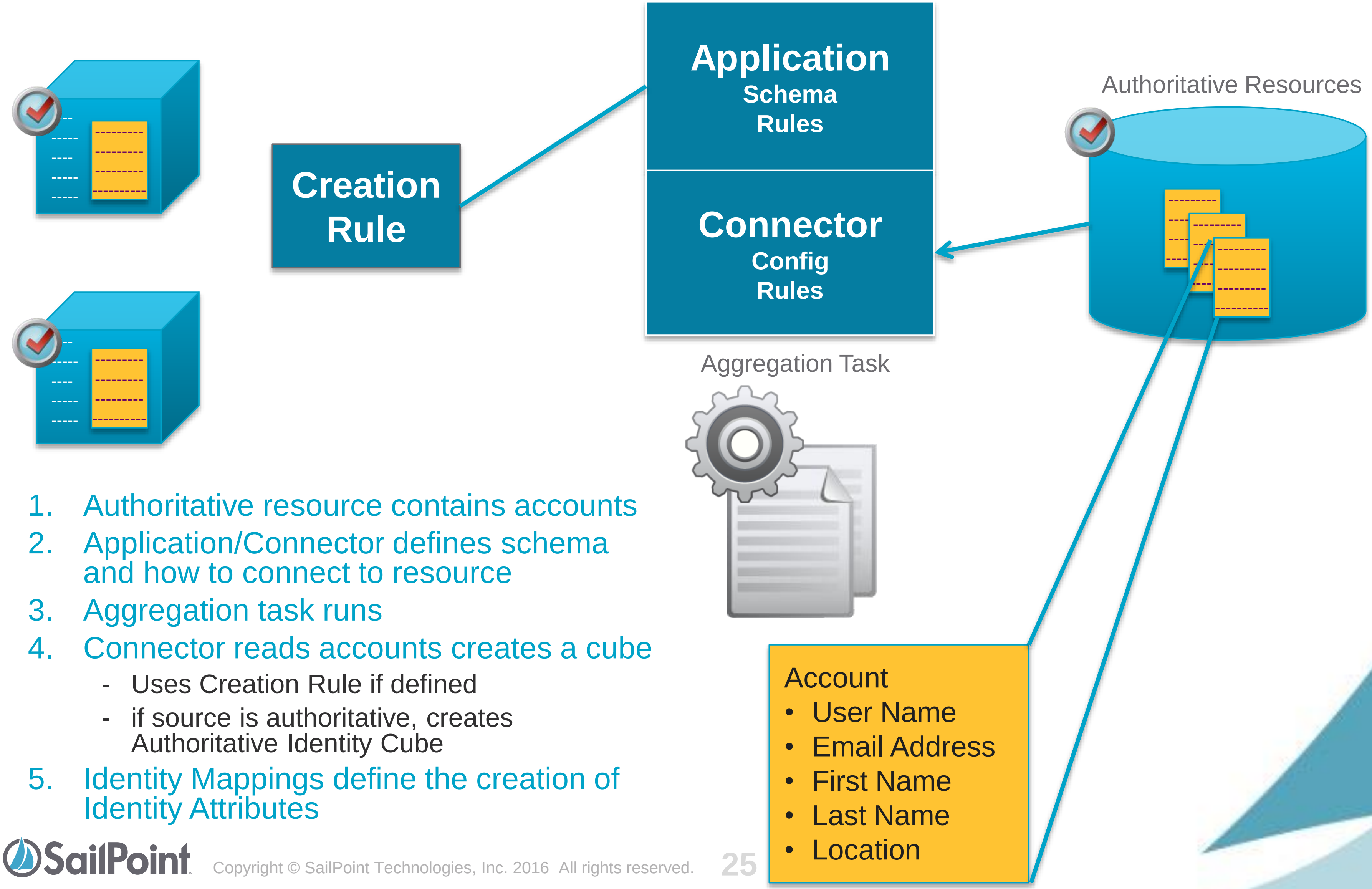
*Not supported by all connectors

Identity Refresh Tasks



- Purpose
  - Update identity attributes from the application account attributes and through calculations
- Run against all identities (default)
- Predefined or created from a task template
  - May have multiple Identity Refresh tasks
- Configuration options
  - Promote account attributes to identity attributes (per identity mappings)
  - Mark manager status for each identity
  - Update role assignments/detections
  - Promote entitlements to a certifiable state
  - Look for policy violations
  - And many more…
- Run after aggregations are complete or when cube data needs re-calculation
- Schedule frequency dependent upon
  - Aggregation schedules
  - Data calculation needs

Identity Cube Creation Process

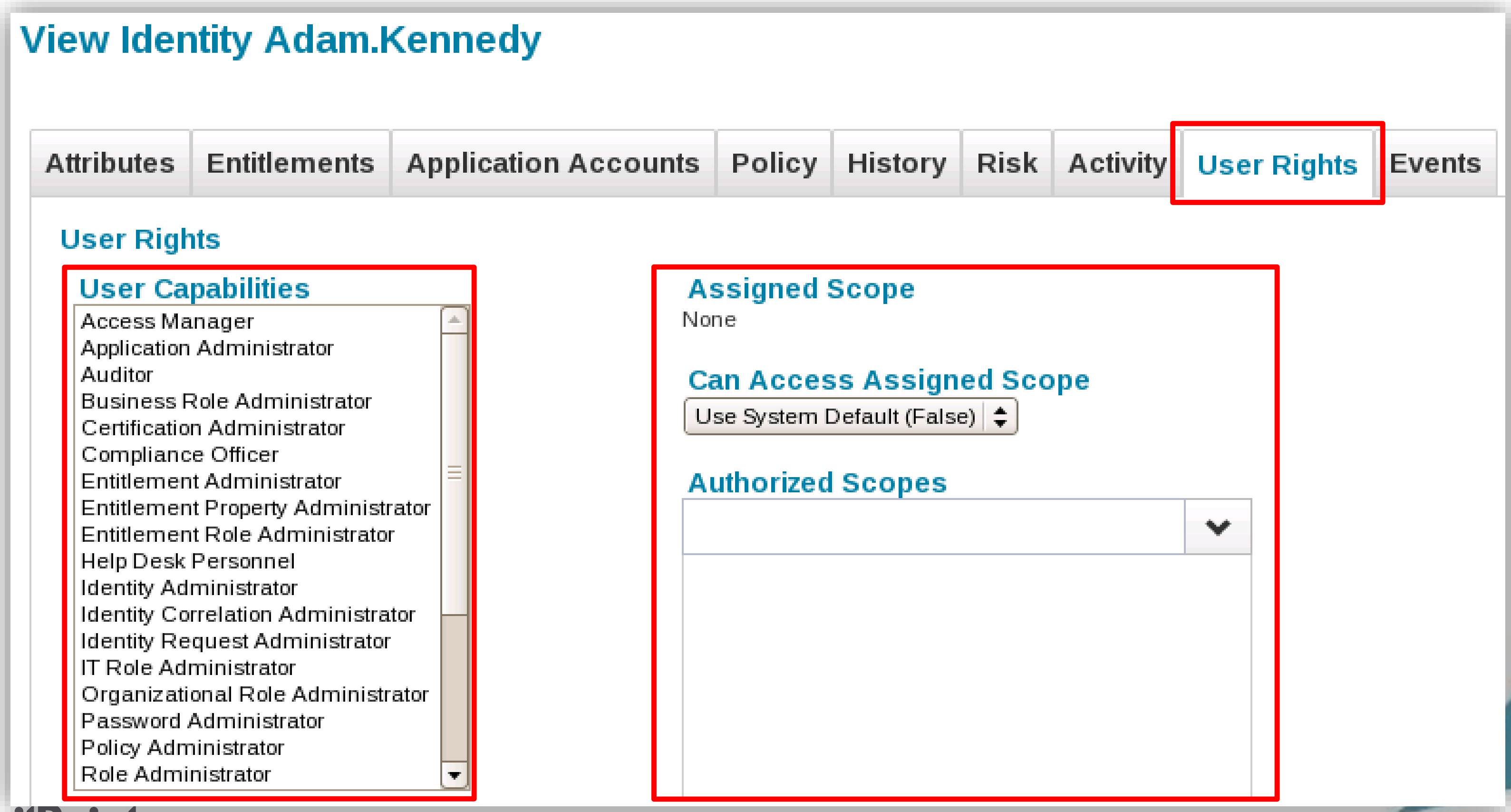


1. Authoritative resource contains accounts
2. Application/Connector defines schema and how to connect to resource
3. Aggregation task runs
4. Connector reads accounts creates a cube
   - Uses Creation Rule if defined
   - if source is authoritative, creates Authoritative Identity Cube
5. Identity Mappings define the creation of Identity Attributes

Managing IdentityIQ User Access

Access Rights for Identities

- Identities can possess Capabilities and Scope (if configured)
- Together, these define what a user can do in the system



User Rights

User Capabilities

Access Manager
Application Administrator
Auditor
Business Role Administrator
Certification Administrator
Compliance Officer
Entitlement Administrator
Entitlement Property Administrator
Entitlement Role Administrator
Help Desk Personnel
Identity Administrator
Identity Correlation Administrator
Identity Request Administrator
IT Role Administrator
Organizational Role Administrator
Password Administrator
Policy Administrator
Role Administrator

Assigned Scope
None

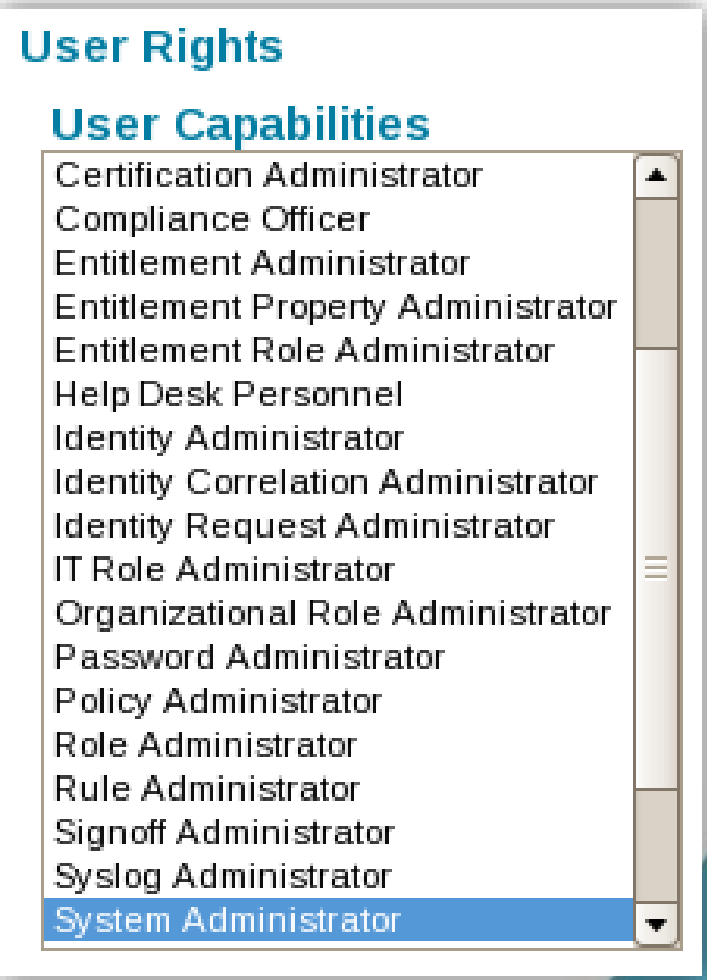
Can Access Assigned Scope
Use System Default (False)

Authorized Scopes

Capabilities – Definition

- Capabilities
  - Define what a user’s rights are within the IdentityIQ Application
  - Control which menu options are available

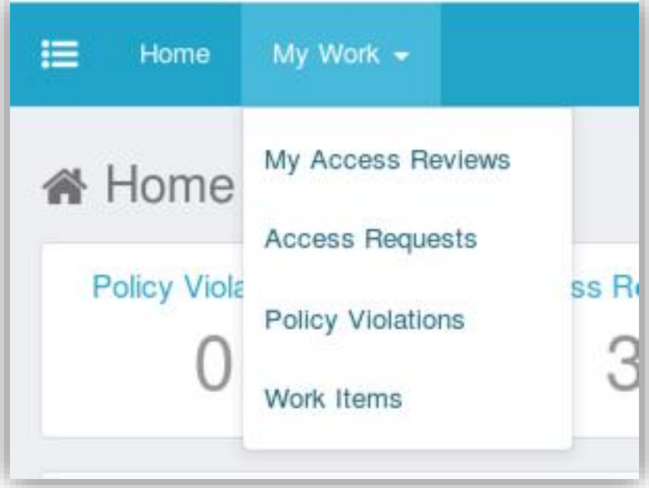
- Default Capabilities Include
  - Home page
  - Quicklinks
  - My Work: Access Reviews, Requests, Work Items and Policy Violations



User Rights

User Capabilities

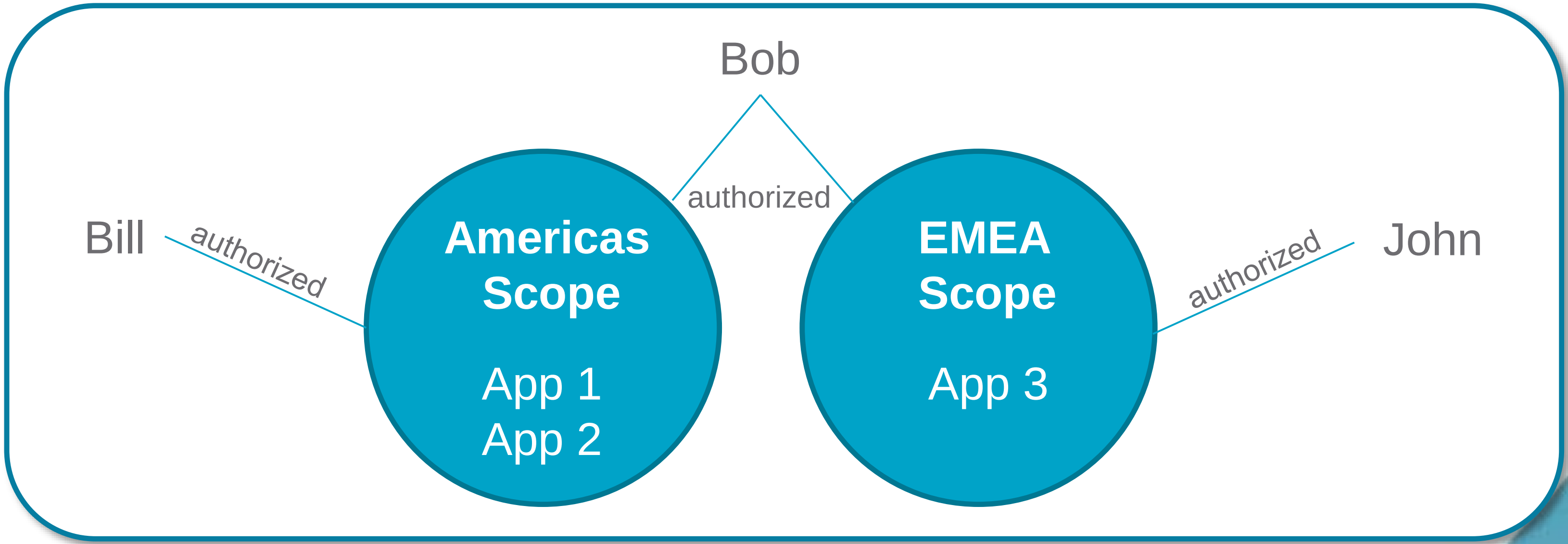
Certification Administrator
Compliance Officer
Entitlement Administrator
Entitlement Property Administrator
Entitlement Role Administrator
Help Desk Personnel
Identity Administrator
Identity Correlation Administrator
Identity Request Administrator
IT Role Administrator
Organizational Role Administrator
Password Administrator
Policy Administrator
Role Administrator
Rule Administrator
Signoff Administrator
Syslog Administrator
System Administrator



See the *Capabilities Matrix* for details.

Scoping – Definition

- Scoping
  - The act of subdividing data into logical groups and granting access based on those subdivisions
  - Scopes control the objects a user can see and act upon

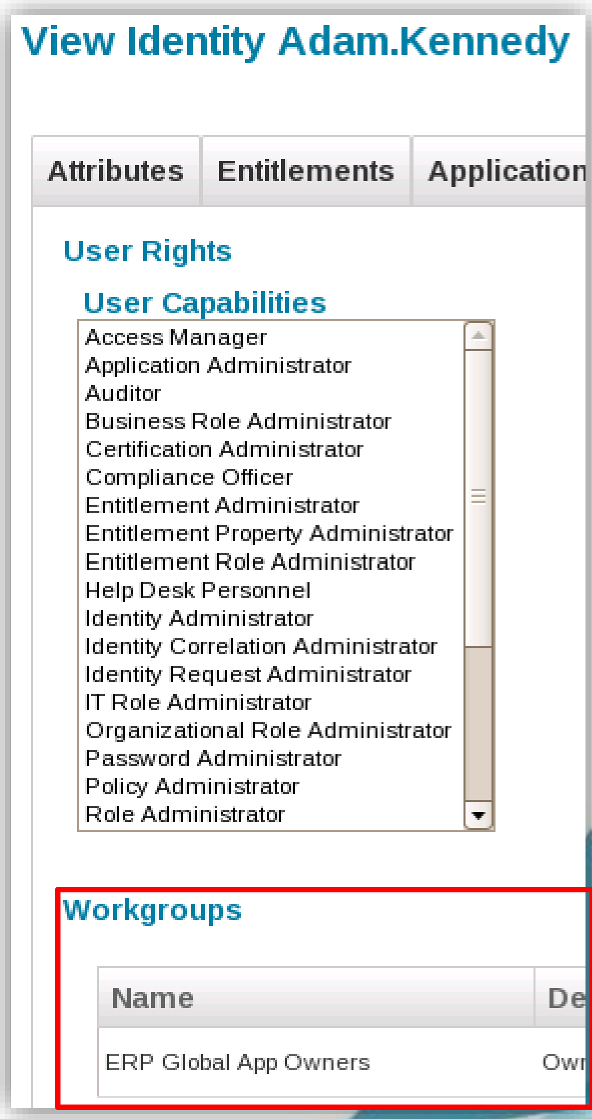


Workgroups – Definition

- Workgroup
  - Set of identities treated as a single IdentityIQ identity

    Example:

    Group: Active Directory Application Owners
    Members: John Smith, Sue Jones
- Workgroups are used for
  - Sharing of IdentityIQ responsibilities
    - Team based work via work items
    - Ownership of objects (best practice)
      - Applications, Certifications, Roles, Entitlements, Policies, etc.
  - Assigning access to IdentityIQ
    - Assignment of capabilities
    - Assignment of scope



View Identity Adam.Kennedy

User Rights

User Capabilities

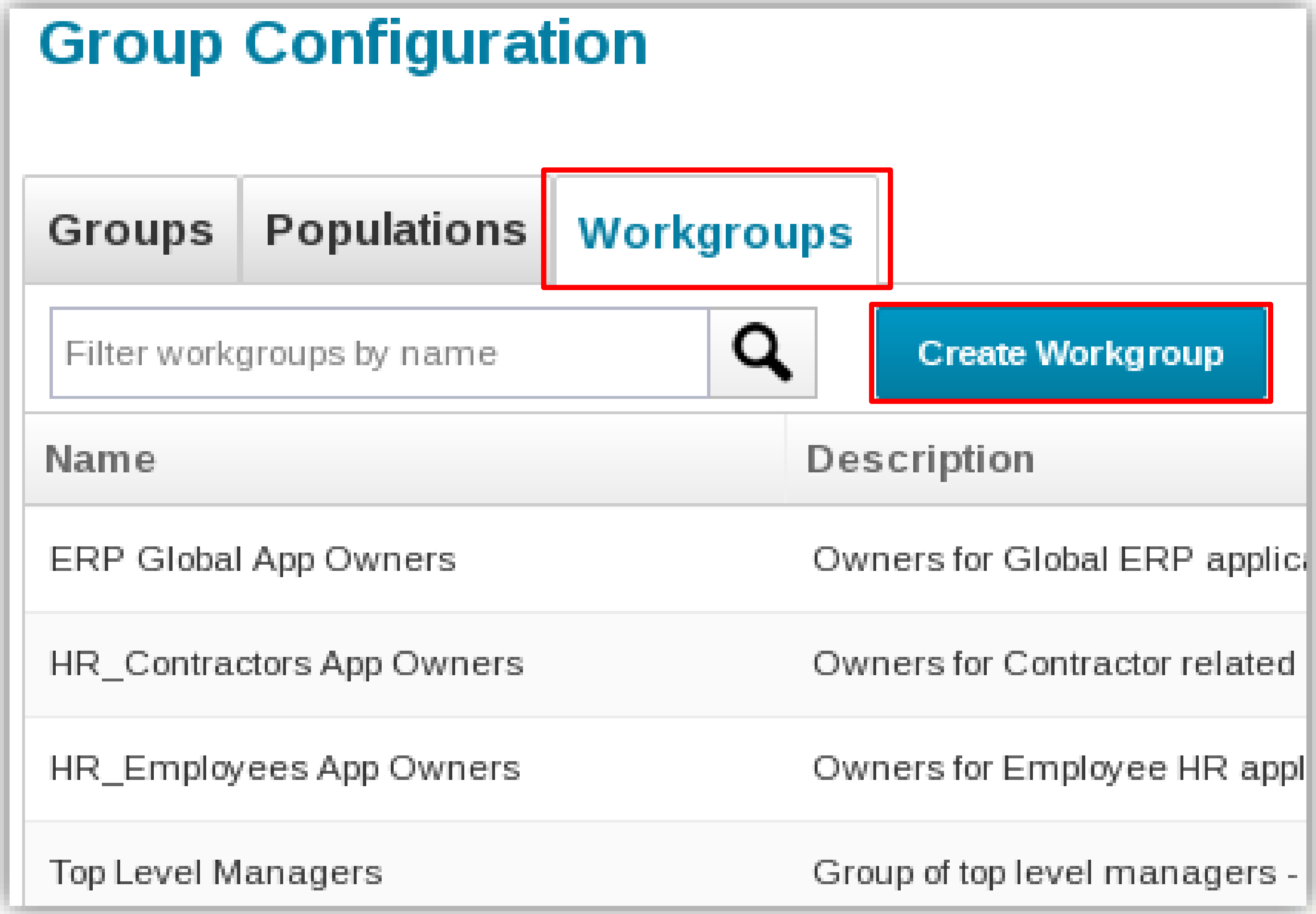
Access Manager
Application Administrator
Auditor
Business Role Administrator
Certification Administrator
Compliance Officer
Entitlement Administrator
Entitlement Property Administrator
Entitlement Role Administrator
Help Desk Personnel
Identity Administrator
Identity Correlation Administrator
Identity Request Administrator
IT Role Administrator
Organizational Role Administrator
Password Administrator
Policy Administrator
Role Administrator

Workgroups

Name	De
ERP Global App Owners	Owr

Workgroups – Configuration

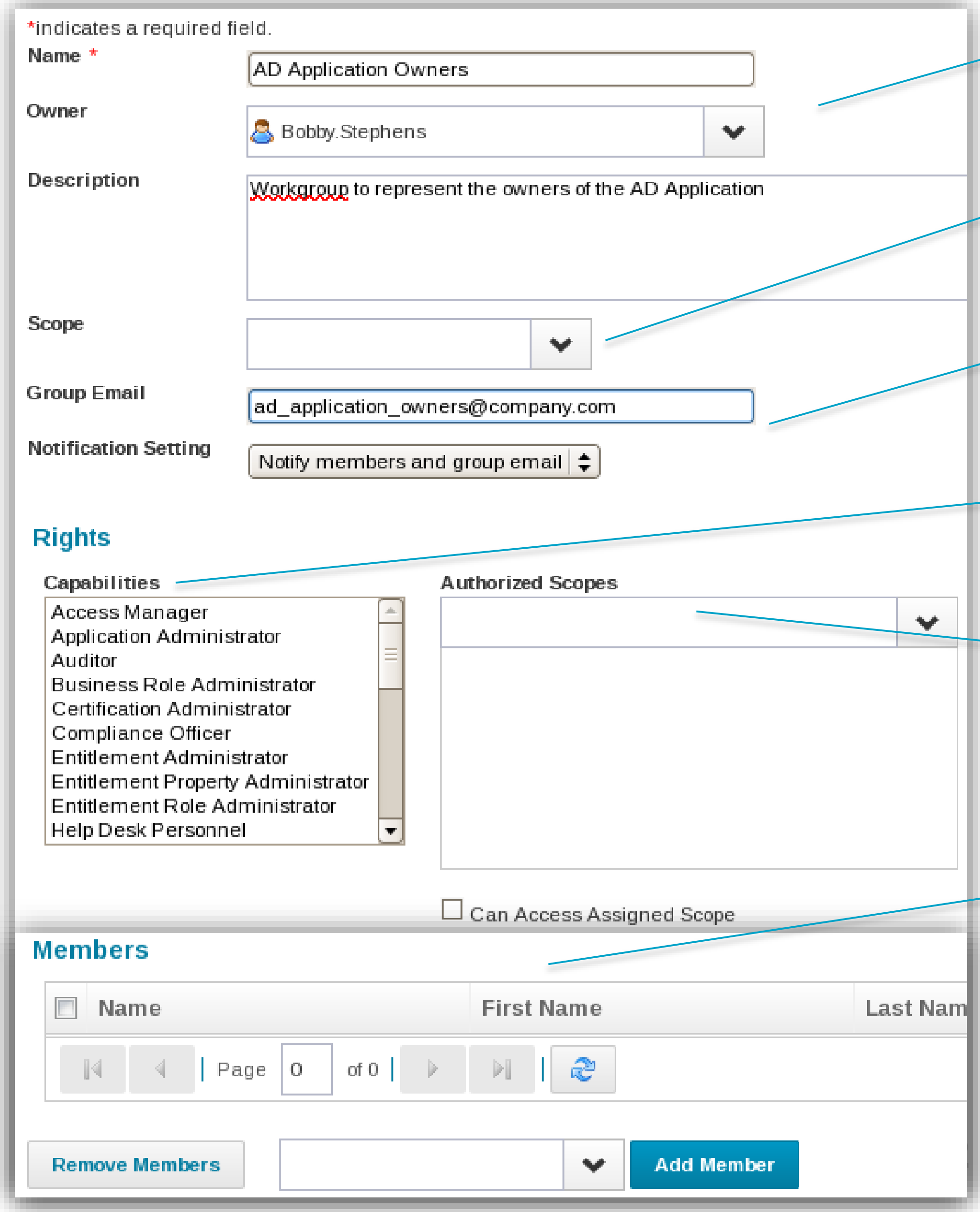
- Setup→ Groups → Workgroups Tab



Group Configuration

Name	Description
ERP Global App Owners	Owners for Global ERP applic
HR_Contractors App Owners	Owners for Contractor related
HR_Employees App Owners	Owners for Employee HR appl
Top Level Managers	Group of top level managers -

Workgroups – Configuration



*indicates a required field.

Name * AD Application Owners

Owner Bobby.Stephens

Description Workgroup to represent the owners of the AD Application

Scope

Group Email ad_application_owners@company.com

Notification Setting Notify members and group email

Rights

Capabilities

- Access Manager
- Application Administrator
- Auditor
- Business Role Administrator
- Certification Administrator
- Compliance Officer
- Entitlement Administrator
- Entitlement Property Administrator
- Entitlement Role Administrator
- Help Desk Personnel

Authorized Scopes

□ Can Access Assigned Scope

Members

□	Name	First Name	Last Nam

Name, Owner and Description

Assigned Scope for the Workgroup

Notification Parameters Email Address and Settings

Capabilities for the Workgroup

Authorized Scopes for the Workgroup

Add/Remove Identities

Assigning Capabilities, Scopes, & Workgroups

- Manual
  - Use the UI
    - Tedious
    - Slow
    - Error-prone
- Use Rules
  - Creation or Customization Rule
    - A user’s AD group membership could define the workgroup, capabilities or scope
    - A user’s department could define the workgroup, capabilities or scope

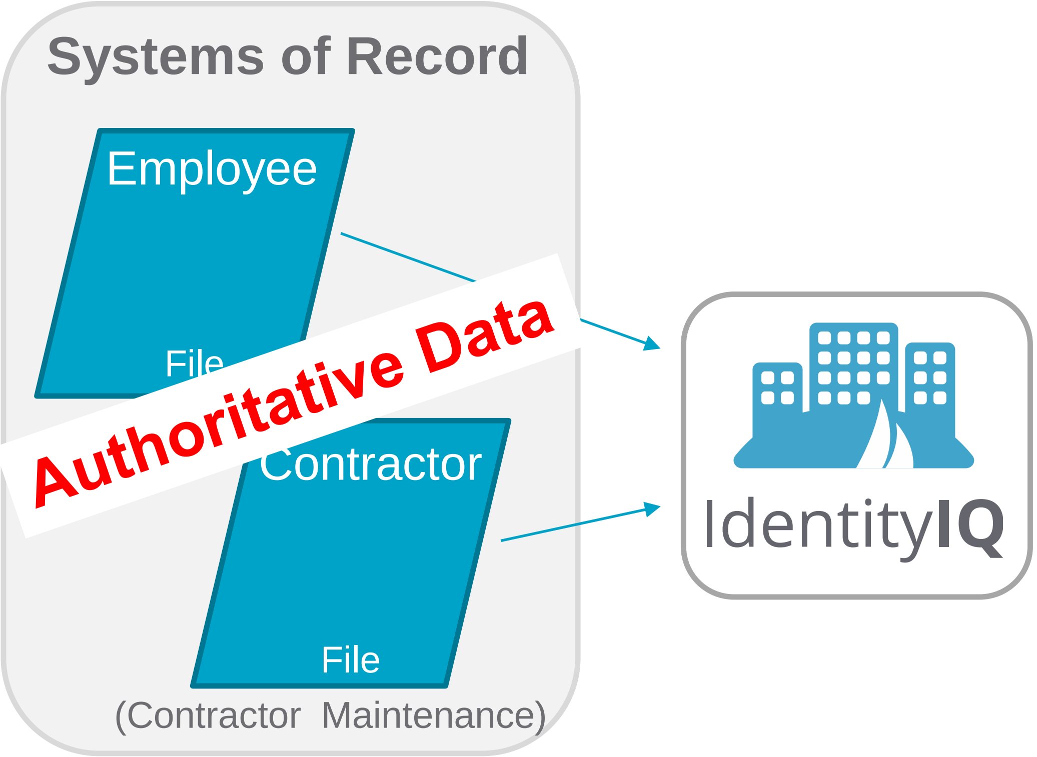
Summary

- Identity Cubes
  - Represent users within IdentityIQ
  - Store all information regarding a user
  - Created by loading data from Authoritative sources or from the UI
- Applications define target resources
  - Applications specify how to connect to the resource by defining a Connector
  - Schemas define the data to be read from the resource
- Aggregation Tasks control how and when data is read from the target resource
- Identity Mappings control how Identity Attributes are "sourced"
- Capabilities/Scoping and Workgroups control an Identities' access to IdentityIQ

Questions?

Exercise Preview

Section 1, Exercise 4



- Installed and configured IdentityIQ
- Populating Identity Cubes
  - Loading authoritative data