Identity Cubes, Authoritative Applications, and Aggregation

Fundamentals of IdentityIQ Implementation

IdentityIQ

Overview

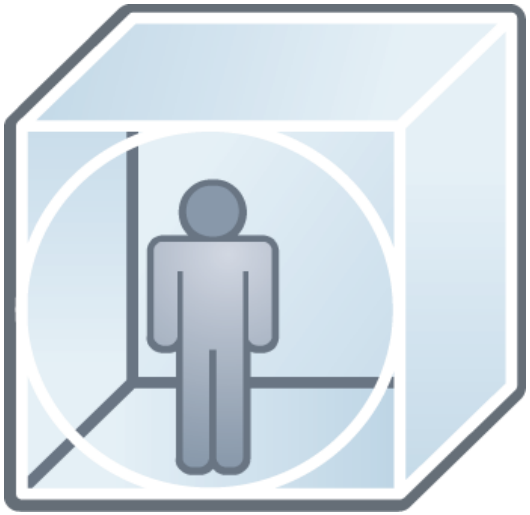
Identity Cubes, Authoritative Applications, and Aggregation

- Identity Cube Overview
  - What is an Identity cube?
  - What is stored on a cube?
  - How are they created?
- Applications/Connectors
  - Schemas
- Identity Mappings
- Aggregation and Refresh
- User Access
  - Capabilities
  - Scoping
  - Workgroups

Identity Cube

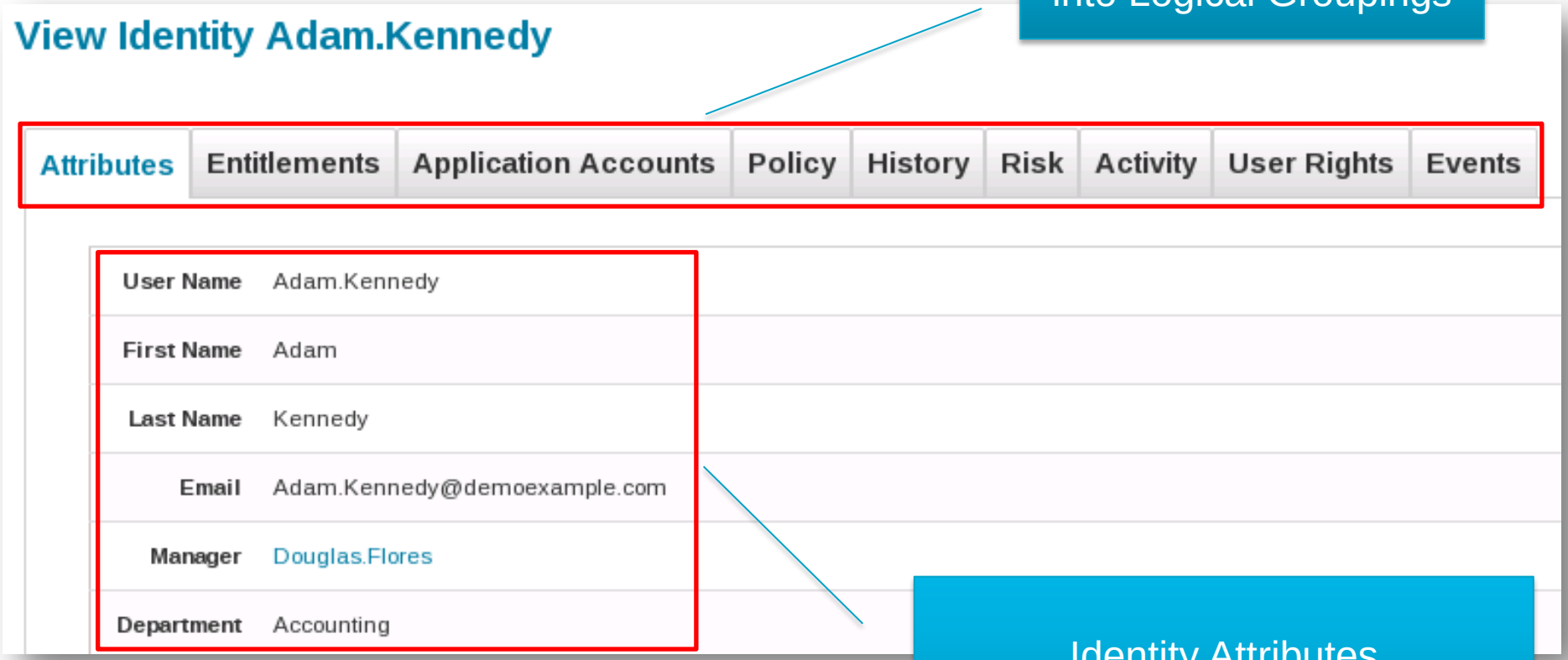
- Term to refer to each unique identity stored in IdentityIQ repository
- Stores all information known about an identity

  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

Tabs divide identity data into Logical Groupings



Identity Attributes are sourced from Authoritative Sources or by Rules

SailPoint

How are Identity Cubes Created?

- Identity Cubes may be created via two mechanisms
  - During Data Aggregation
    - By aggregating data from Authoritative Application(s)
      - HR Application
      - Enterprise Directory
    - By aggregating data from Non-authoritative Applications
      - Creates non-authoritative cube (more later)
  - Using Lifecycle Manager
    - Using the *Create Identity* or *Self-registration* option in Lifecycle Manager
      - Identity Attributes are entered as part of the creation process

Applications/Connectors

- Application
  - A representation of a target resource (like Active Directory, SAP)
  - Configuration includes
    - Meta Information
      - Application Name, Description, Application Owner, Revoker
    - Account Schema and Optional Group Schema
    - Connector

      Note: The connector options vary based on the available data format – flat file, direct connection, etc.
    - Application Rules
- Connector
  - Software component that allows IdentityIQ 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

Application Configuration

*indicates a required field.

Name * HR System - Employees

Owner * The Administrator

Revoker

Description

English (United States)

7 of 1024 characters (including markup)

Application Type * DelimitedFile

Proxy Application

Profile Class

Authoritative Application

Application Meta Information

Application Type = Connector

Authoritative Checkbox

SailPoint

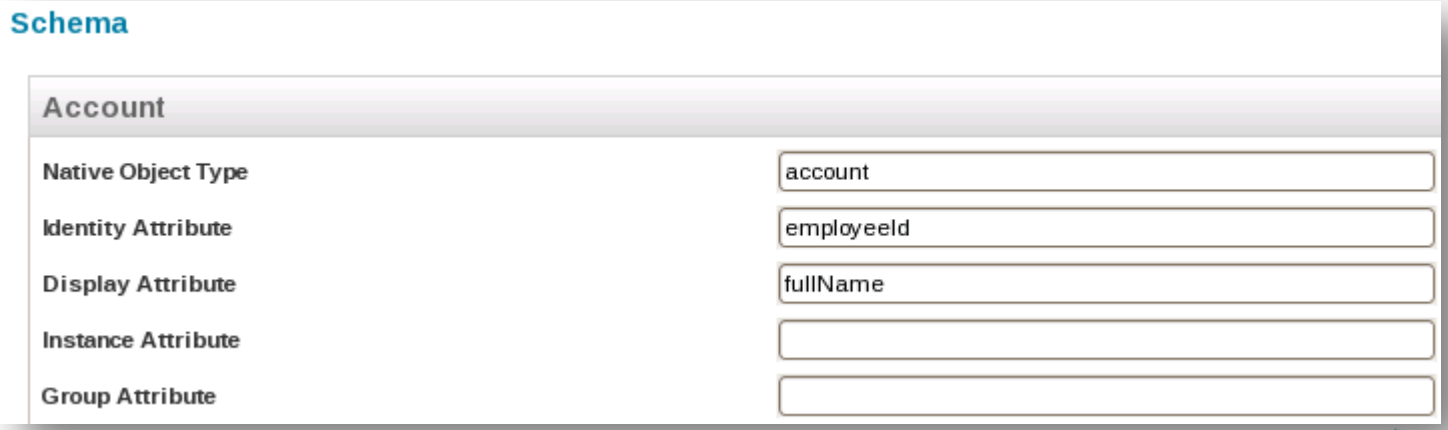
Schema

- Definition of what data to read from the target resource and how to interpret
- Schema types
  - Account – represent individual accounts on a target resource (AD or SAP Accounts, for example)
  - Group – represent native account groups from target resource (LDAP Groups or AD Groups, for example)

Account Schema

Account Data

- Defining the schema for accounts
  - Identity Attribute
    - Identifies which attribute holds unique identity id (username, id)
  - Display Attribute
    - Identifies which attribute holds display attribute
    - Used for friendly display name
  - Group Attribute
    - Identifies which attribute holds the group attribute
    - Used to identify group membership (groupmbr, memberOf)



Account Schema

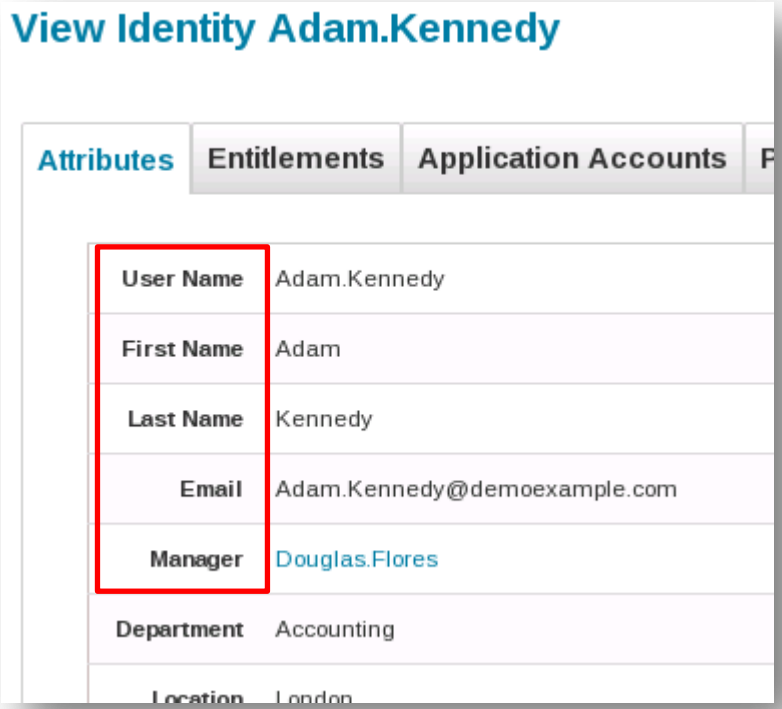
Attribute Data

- Define which attributes to collect
  - Pre-defined for certain Connectors
- Define how to interpret the data
  - What data type (string, long, int, boolean)?
  - Is the attribute multi-valued?
  - Managed and Entitlement covered later

Attributes

	Name	Description	Type	Managed	Entitlement	Multi-Valued
☐	costcenter		string	☐	☐	☑
☐	department		string	☐	☐	☐
☐	email		string	☐	☐	☐
☐	employeeId		string	☐	☐	☐
☐	firstName		string	☐	☐	☐

Identity Attributes



- Standard Attributes
  - Used to support basic system functionality
    - DisplayName
    - First Name
    - Last Name
    - Inactive
    - Manager
    - Email
  - Searchable by default
- Additional Identity Attributes are typically defined (called extended attributes)
  - Add as many as required to support your needs
  - Searchable attributes must 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*
- Identity Mappings define source for Identity Attributes
  - Source for all attributes must be specified (standard attributes ***and*** extended attributes)
  - Typically sourced from authoritative sources like HR and Corporate Directory
  - Can be sourced with a rule (Application or Global)

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

HR-System employeeId → Identity Attribute empId

Identity Attribute Mappings

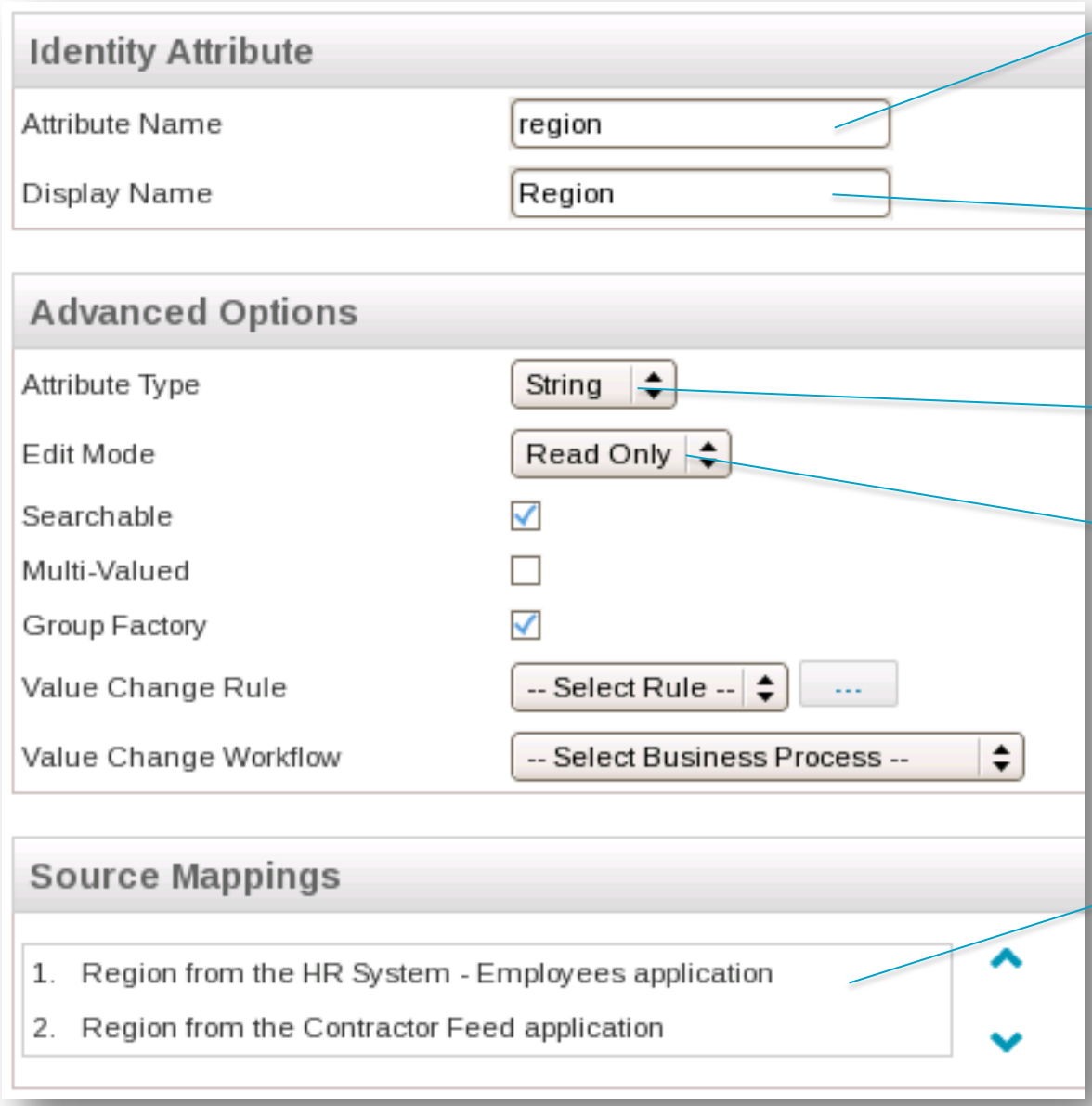
Utilizing the Data

- Identity Mappings specify how to use the data
  - Mark as searchable to support
    - Correlation
    - Analytics, Reporting, Searching
  - Mark as multi-valued
    - Indicate more than one value is allowed for the attribute

    Example: *User may belong to more than one AD group*
  - Mark as group factories
    - Support dynamically generated groupings of identities based on the attribute

    Example: *All users in each region become a group*

Identity Mappings Configuration



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

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

Attributes | Entitlements | Ap

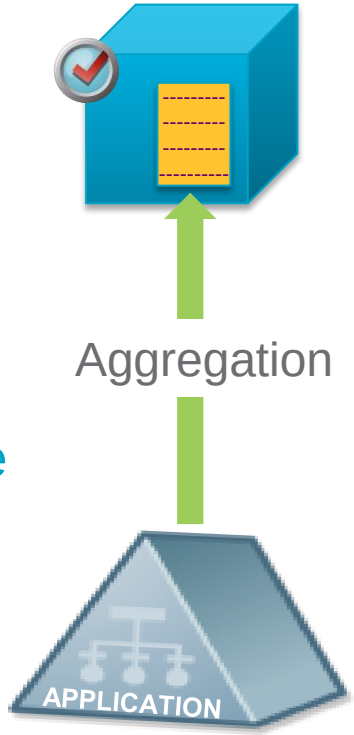
User Name	Douglas.Flores
First Name	Douglas
Last Name	Flores
Email	Douglas.Flores@
Manager	Amanda.Ross
Department	Accounting
Location	London
Employee ID	1b2c3a

Attributes | Entitlements | Application Accounts

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

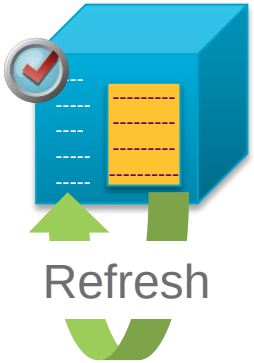
SailPoint

Account Aggregation Tasks



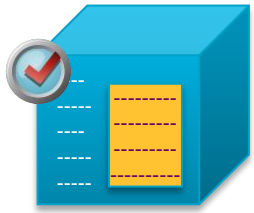
- Purpose
  - Read data from target applications to identify account attributes
- Typically one aggregation task per application
- Use Application/Connector/Schema information to manage the aggregation
- Created from an Account Aggregation task template
- Many configuration options
  - Which Applications to Aggregate
  - Detect Deleted Accounts
  - 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)

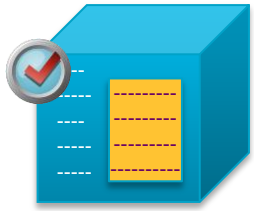
Identity Refresh Tasks



- Purpose
  - Update identity attributes from the identity 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

Overview – Identity Cube Creation



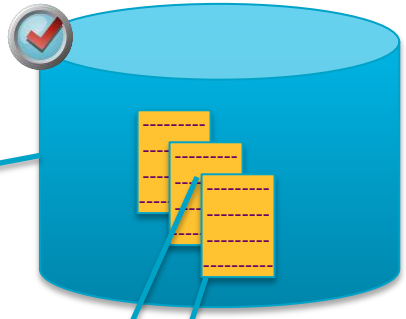


Creation Rule

Application
Schema
Rules

Connector
Config
Rules

Authoritative Resources



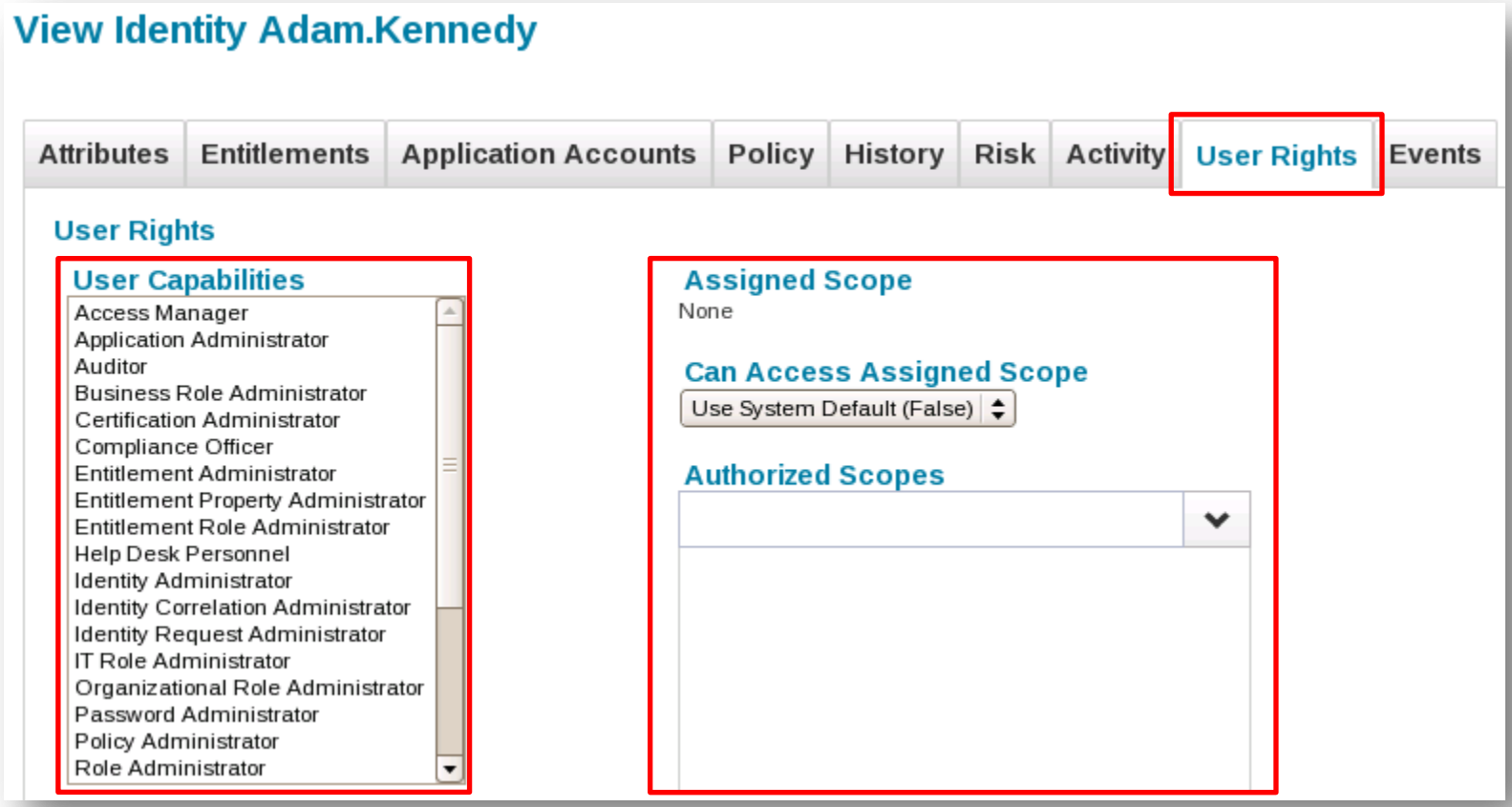
Aggregation Task

Account
- User Name
- Email Address
- First Name
- Last Name
- Location

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

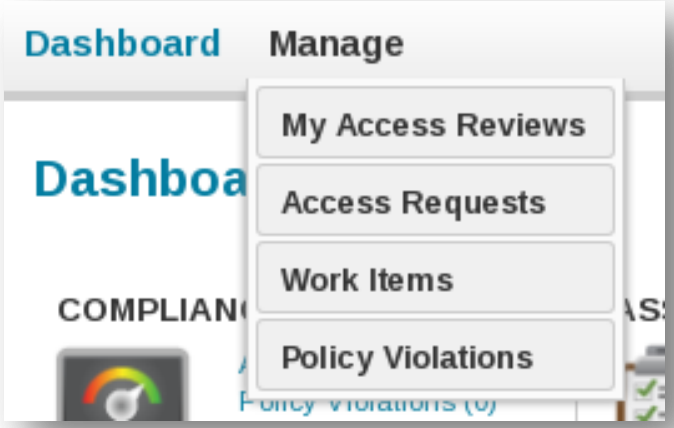
Access Rights for Identities

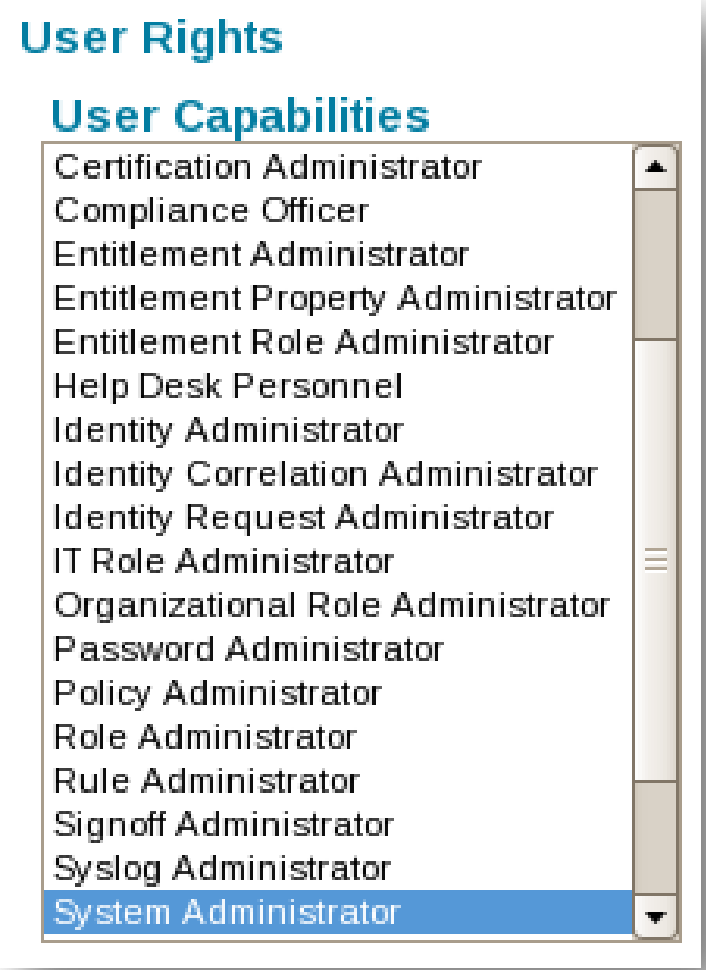
- Identities can possess Capabilities and Scoping (if configured)
- Together, these define what a user can do in the system



Capabilities – Definition

- Capabilities
  - Define what a user's rights are within the IdentityIQ Application
- Default Capabilities Include
  - Dashboard
  - Manage Access Reviews, Requests, Work Items and Policy Violations

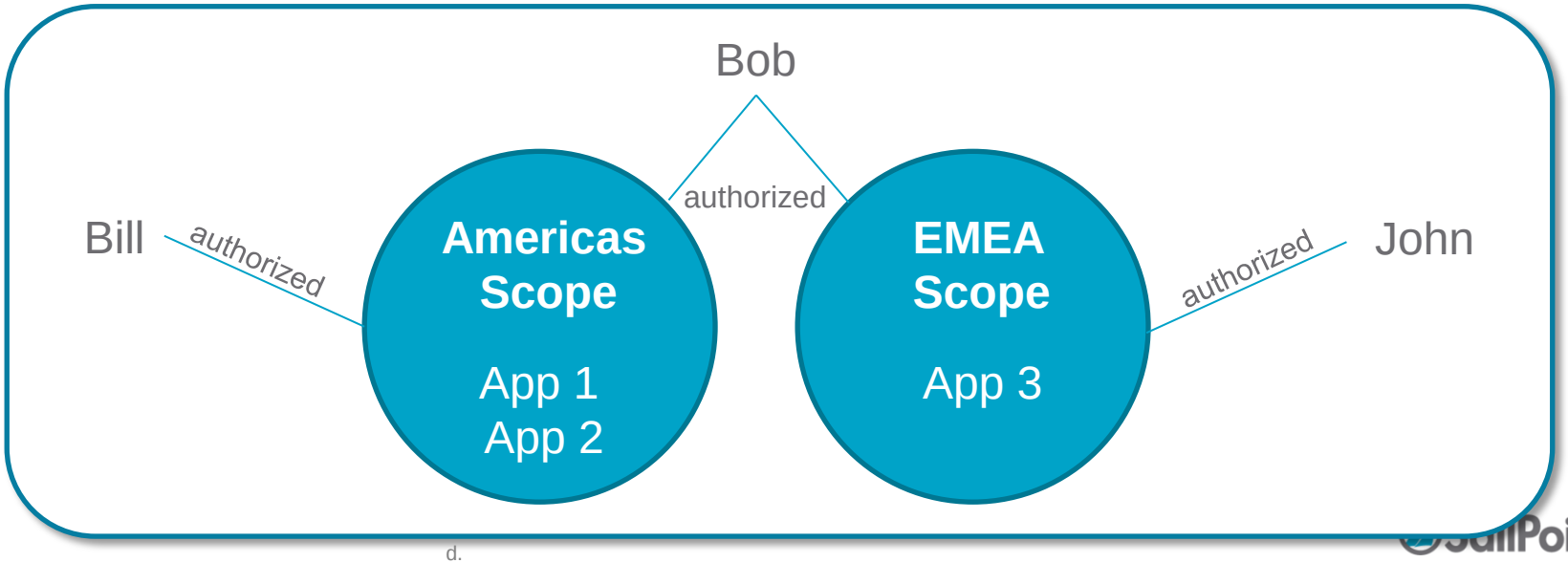




See the *Capabilities Matrix* for details.

Scoping – Definition

- Scoping
  - The act of subdividing data into logical groups and granting access based on those subdivisions
- Any IdentityIQ Object can be **Assigned** to Scopes
  - Identities, Applications, etc
- Users can have **Authorized** Scopes
  - These are the scopes that they can interact with



Capabilities and Scoping

- Capabilities control the **actions** that a user can perform
- Scoping controls **which objects** a user can act upon
- Both affect what the user can see in IdentityIQ
  - Capabilities control which menu options are available
  - Scoping controls which objects are available

Capabilities Matrix (selective listing)

	Application Administrator	Access Manager	Auditor	Business Role Administrator	Certification Administrator	Compliance Officer	Administrator Rule	Administrator Identity	Administrator Password	Administrator Policy	Administrator Role	Administrator Signoff	Administrator System
Define	✓	✓	✓	✓		✓		✓	✓	✓	✓		✓
Applications	✓										✓		✓
Identities			✓			✓		✓	✓	✓			✓
Activity Target Categories													✓
Policies													✓
Identity Risk Model													✓
Application Risk Model	✓												✓
Entitlement Catalog	✓												✓
Business Processes													✓
Lifecycle Events (LCM Only)		✓											✓
Roles			✓	✓		✓				✓	✓		✓
Role Viewer						✓							✓
Role Search						✓							✓
Entitlement Analysis						✓							✓
Role Mining													✓
Role Mining Results											✓		✓
Groups	✓					✓		✓					✓
Groups (tab)	✓					✓		✓					✓
Populations	✓					✓		✓					✓
Workgroups	✓					✓		✓					✓
Monitor						✓						✓	✓
Certifications						✓							✓
Tasks												✓	✓
Analyze	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓

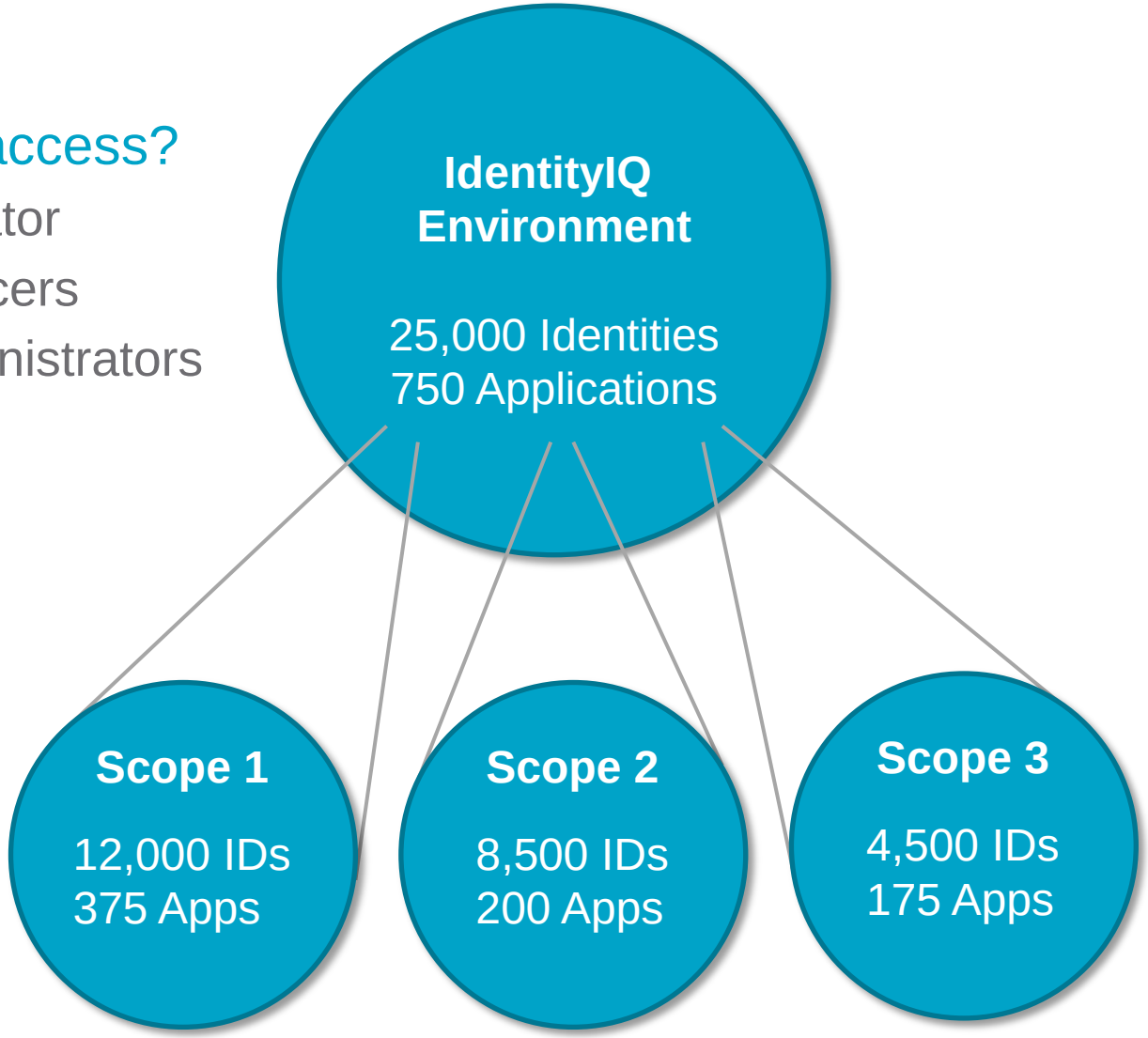
System Administrator can define **applications** and **identities**

Application Administrator can define **applications** but not identities

Compliance Officer can define **identities** but not applications

Scoping – Limiting the Extraneous

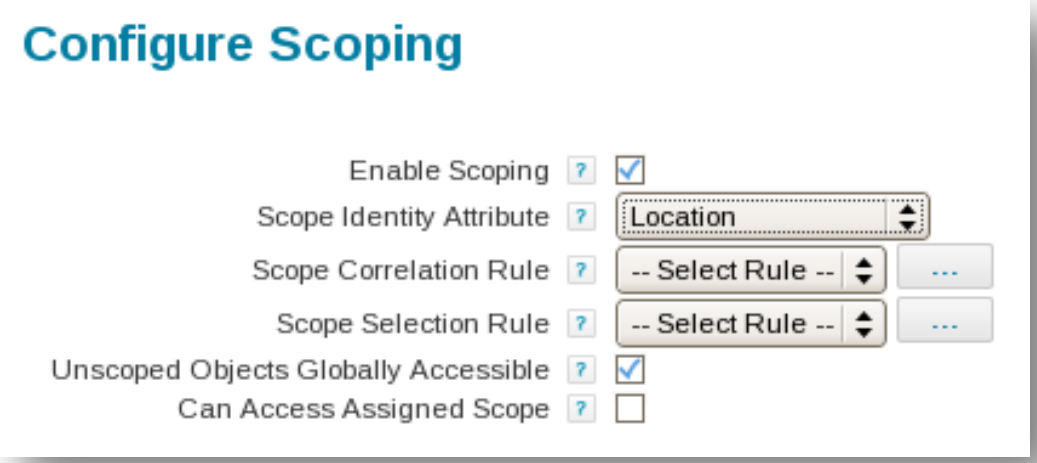
- What can the staff access?
  - System Administrator
  - 3 Compliance Officers
  - 3 Application Administrators



Scoping – Configuration

- Scoping must be enabled (default is disabled)
  - System Setup → Scopes → Configure Scoping
- Scoping generally derived from Identity Attribute

  Example: Location or Division
- Rules can be used to assign scopes to individuals
- Un-scoped objects visible to all users or only System Administrators

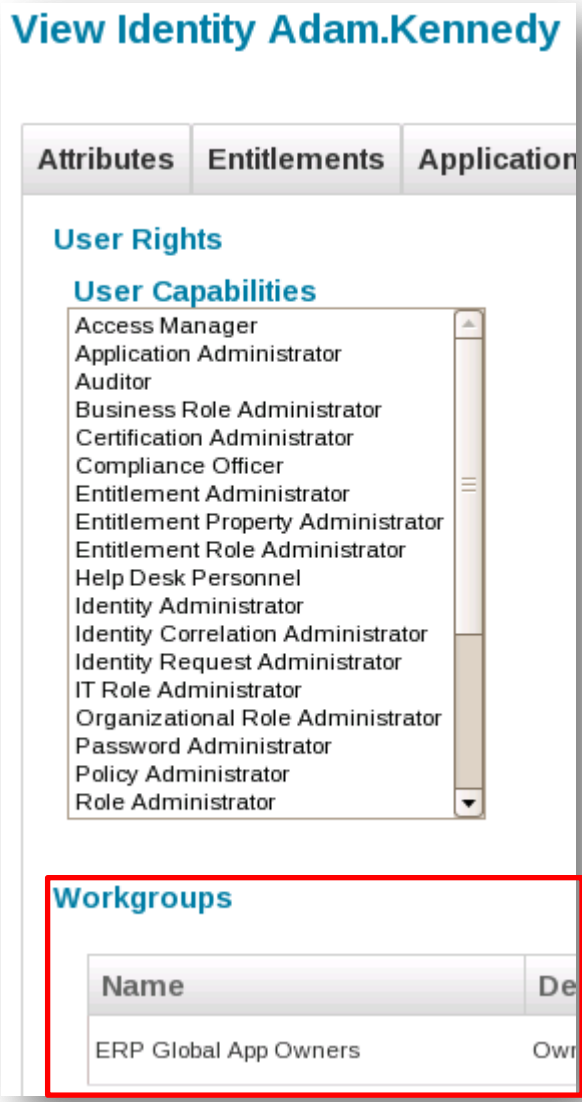


Workgroups – Definition

- Workgroup
  - A grouping of identities treated as a single IdentityIQ identity

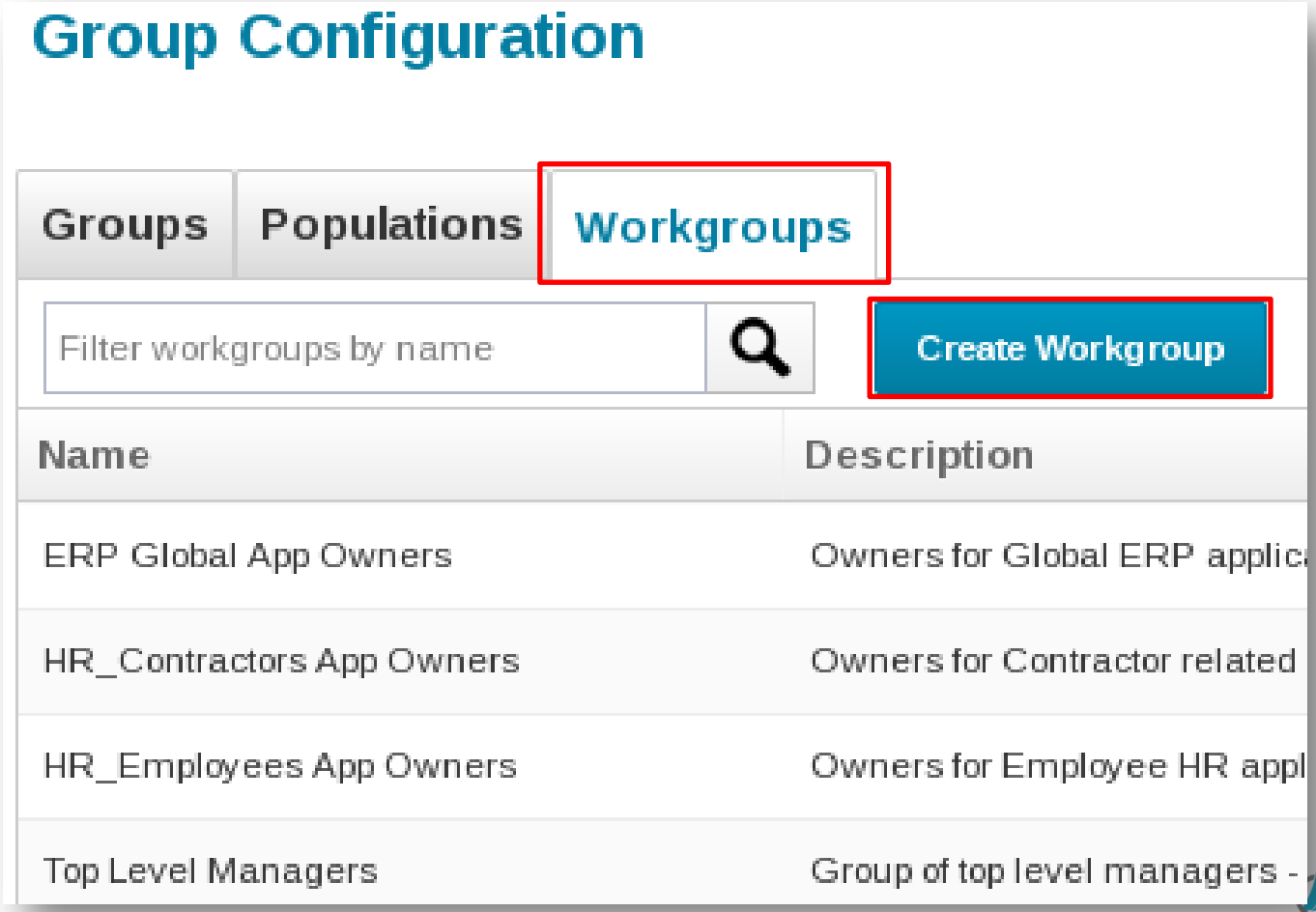
    Example:

    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 scoping



Workgroups – Configuration

- Configured
  - Define → Groups → Workgroup Tab



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

Page 0 of 0

Remove Members | Add Member

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

SailPoint

Assigning Capabilities, Scopes, & Workgroups

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

SailPoint

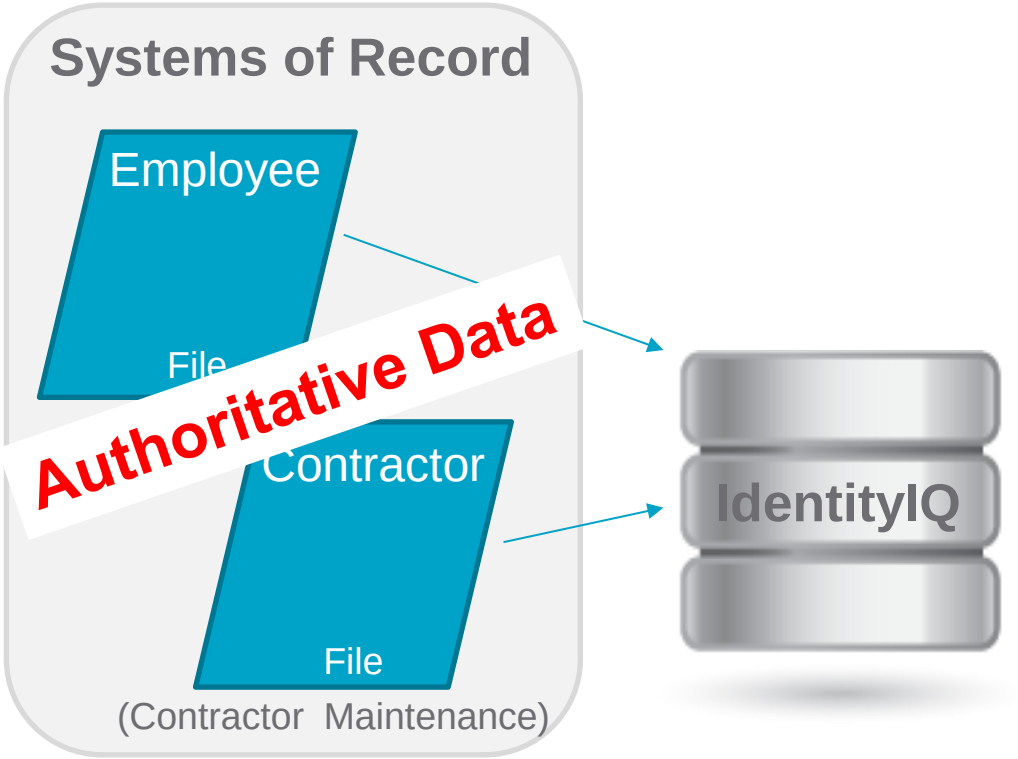
Summary

- 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
  - Applications specify a schema to be used when reading data from the resource
- Aggregation Tasks control how and when we pull data 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