



# IdentityIQ Technical Overview

IdentityIQ Essentials

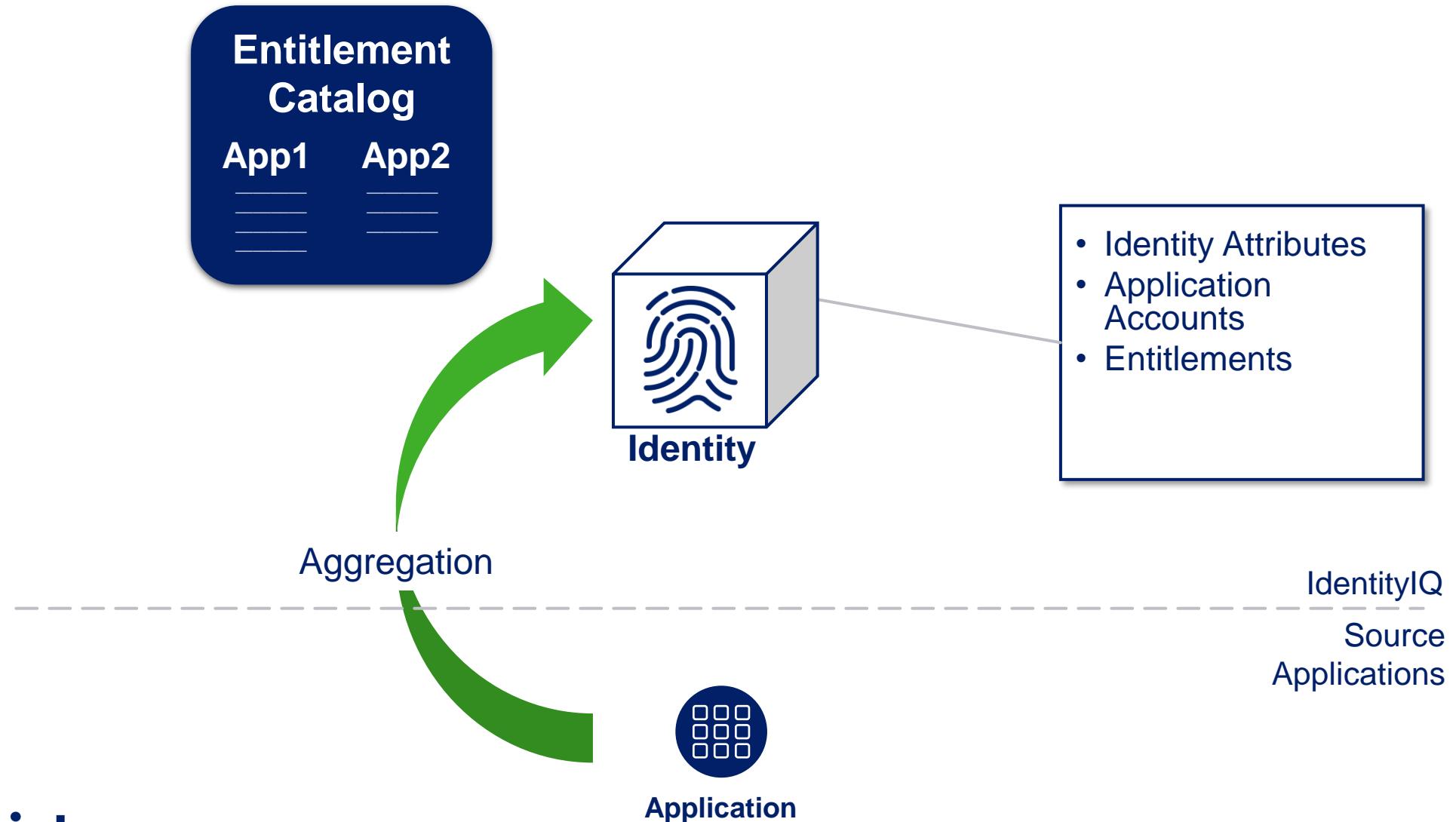
# IdentityIQ Technical Overview

---

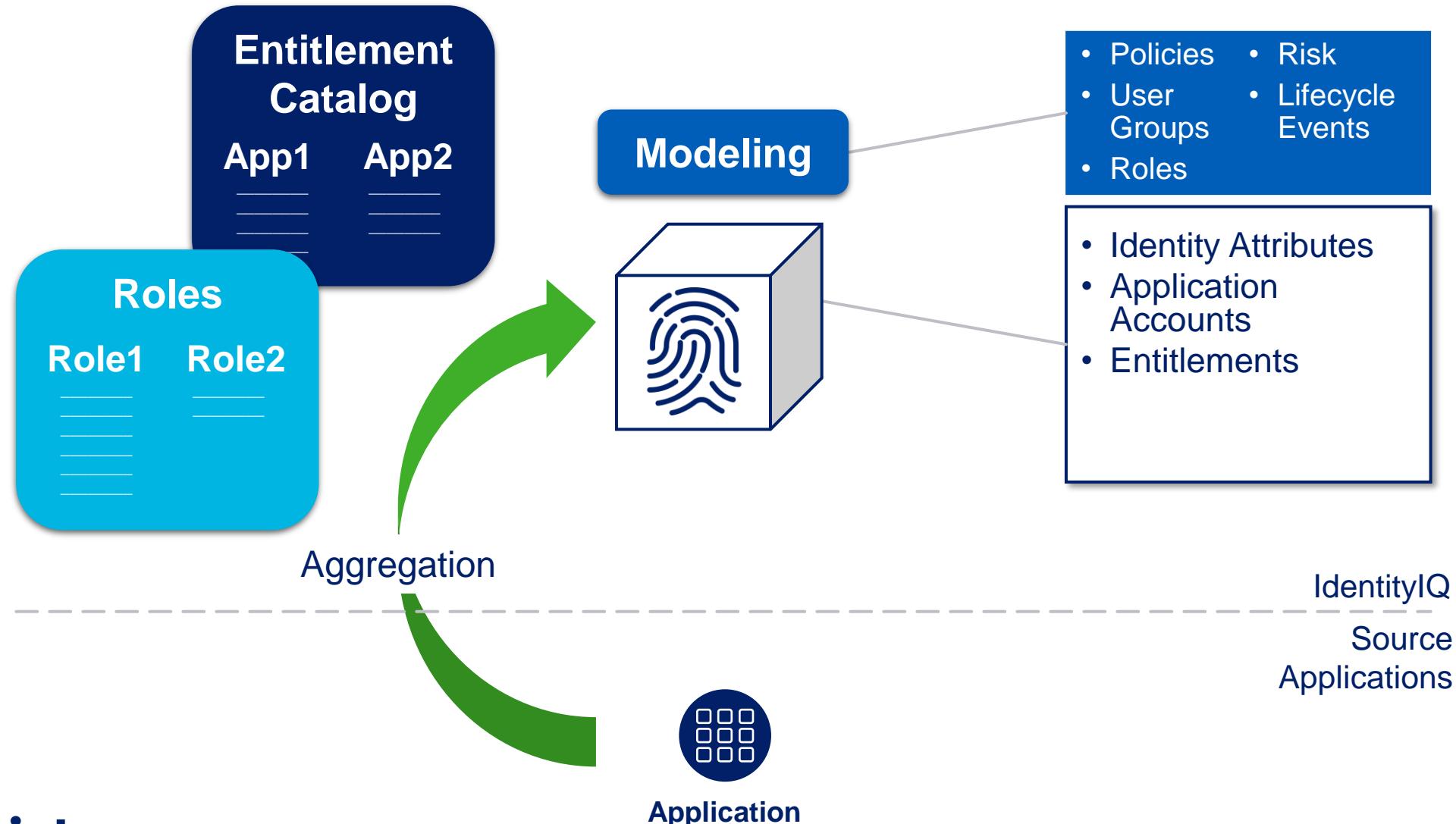
## Overview

- Reading data
- Business modeling
- Governance process
- Provisioning process

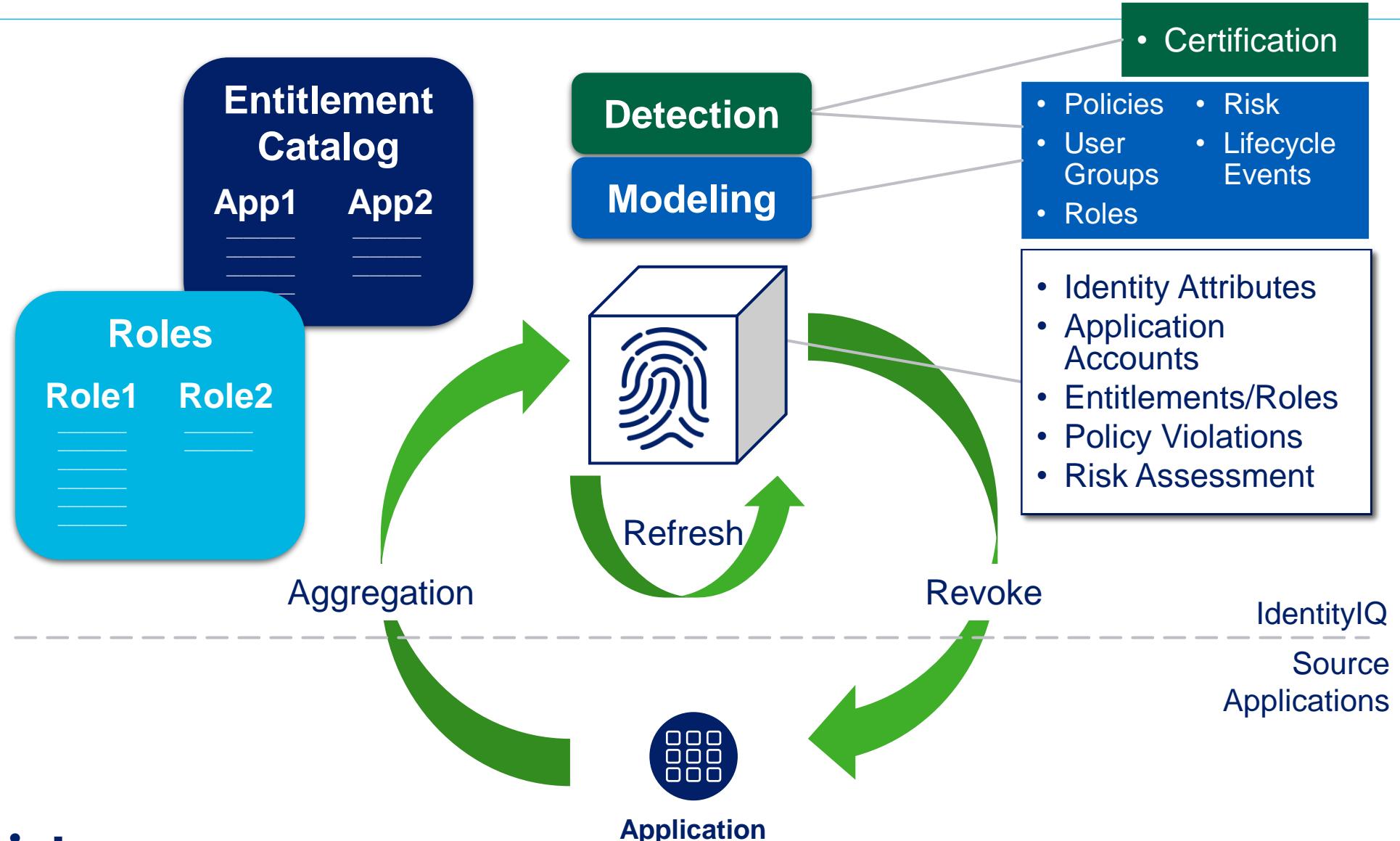
# IdentityIQ Process – Reading Data



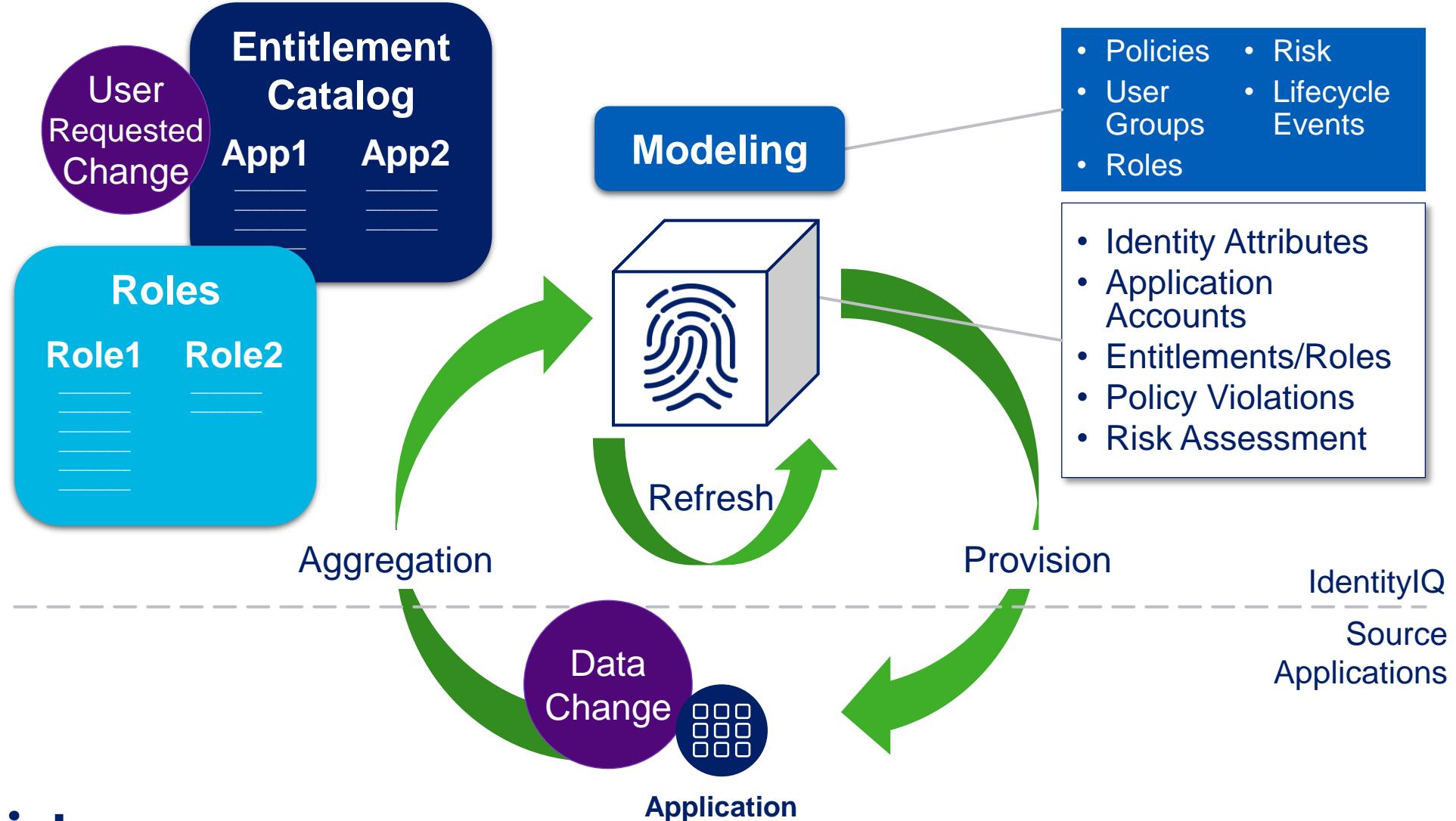
# IdentityIQ Process – Business Modeling



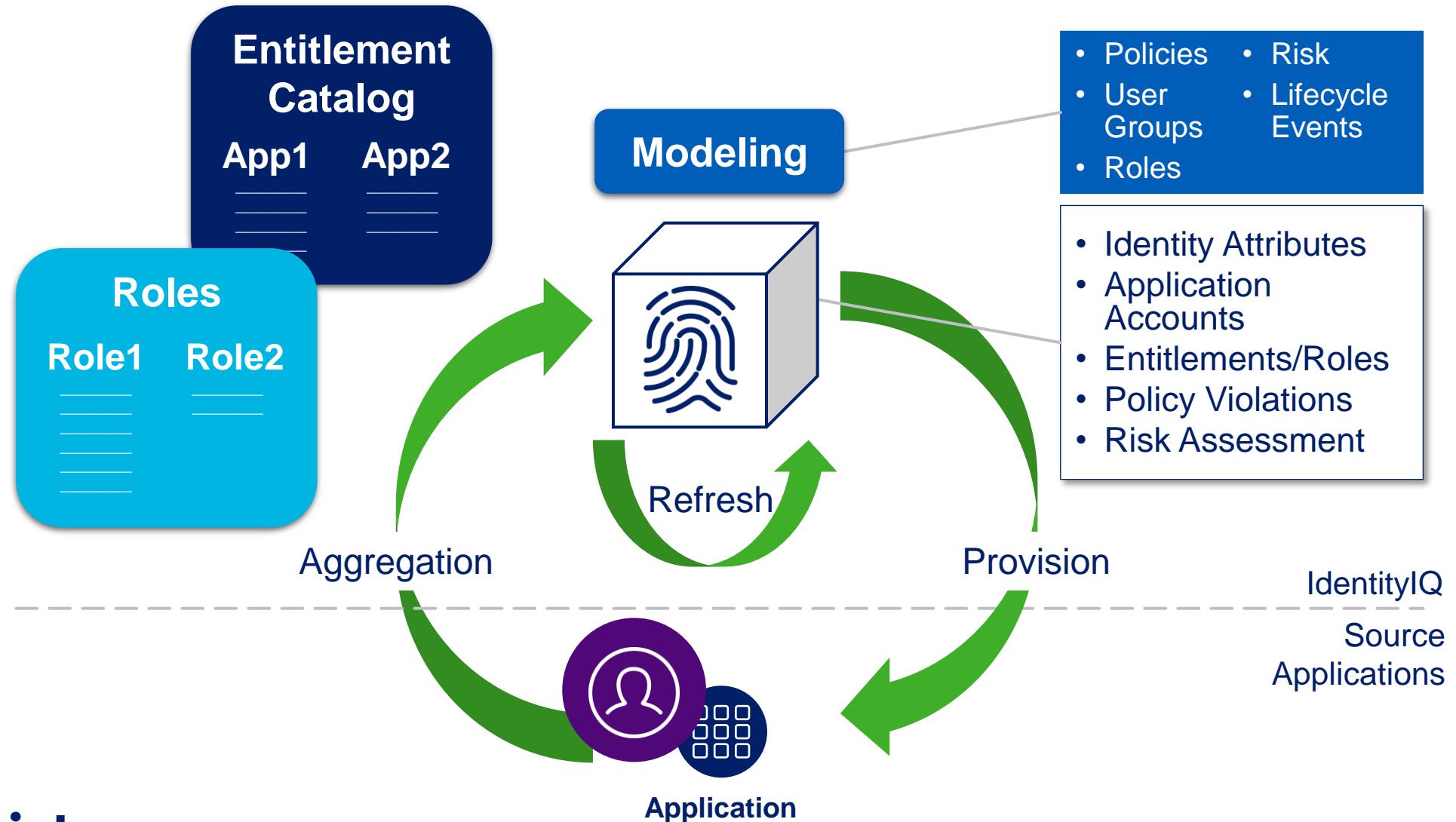
# IdentityIQ Governance Process



# IdentityIQ Provisioning Process – User Request



# IdentityIQ Provisioning Process – Lifecycle Event



# Knowledge Check





# IdentityIQ Functional Elements

IdentityIQ Essentials

# IdentityIQ Functional Elements

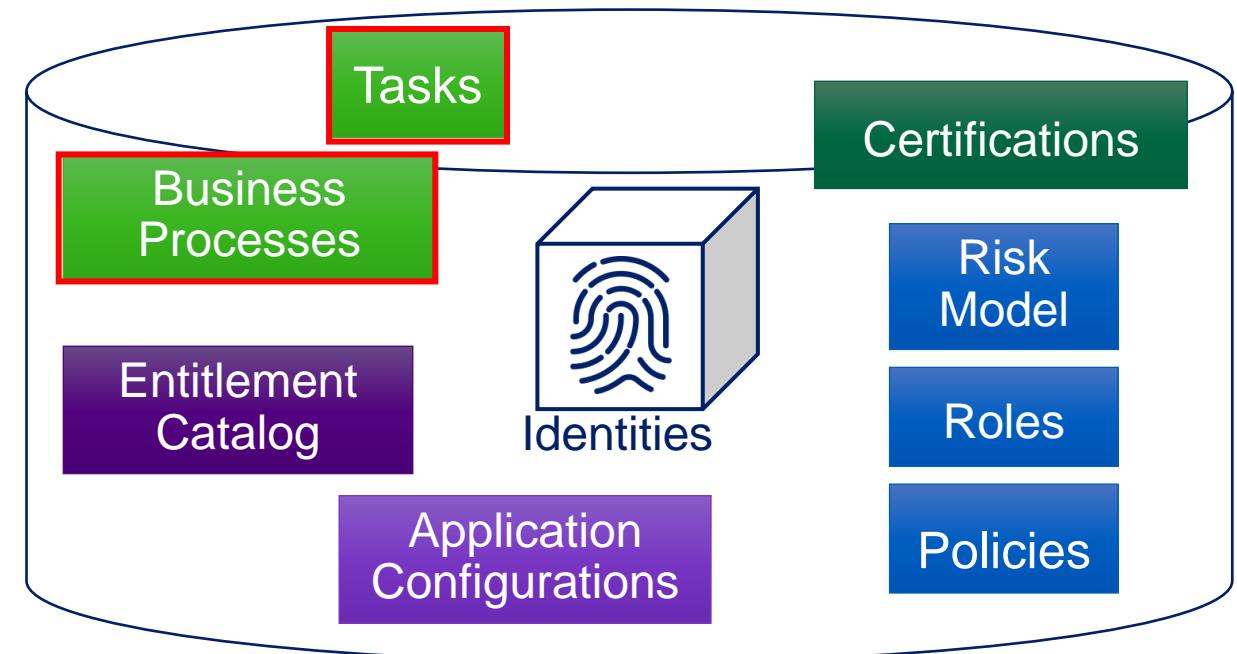
---

- Tasks
- Business Processes (workflows)
- Rules

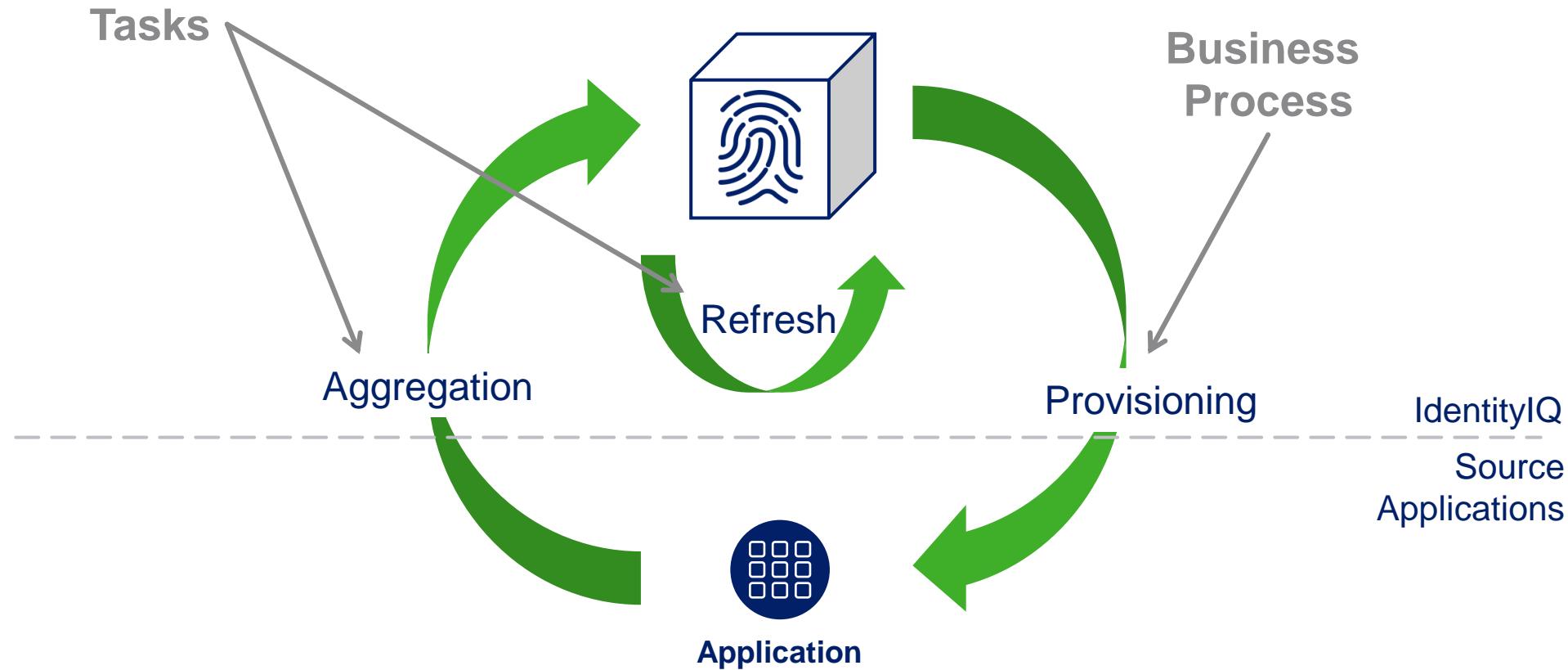
# IdentityIQ Objects: Data and Actors

## Tasks and Business Processes

- All data is stored in IdentityIQ as objects
- Tasks are batch jobs that act on objects
  - Scheduled or manually run
  - No user interaction
- Business processes are a set of executable steps that act on objects
  - Respond to actions in the system
  - Often interact with a user



# Example Task and Business Process



# Tasks

- Many standard tasks are pre-configured
- Many task templates are provided
- Implementation team
  - Configures tasks
  - Can develop tasks specific to your environment
- System administrator
  - Responsible for monitoring tasks

The screenshot shows the SailPoint Tasks interface. At the top, there are three tabs: 'Tasks' (selected), 'Scheduled Tasks', and 'Task Results'. Below the tabs is a search bar labeled 'Search by Task Name' with a magnifying glass icon. The main area displays a table with columns 'Name' and 'Description'. A dropdown menu titled 'type: Identity (9 Tasks)' is open, listing the following tasks:

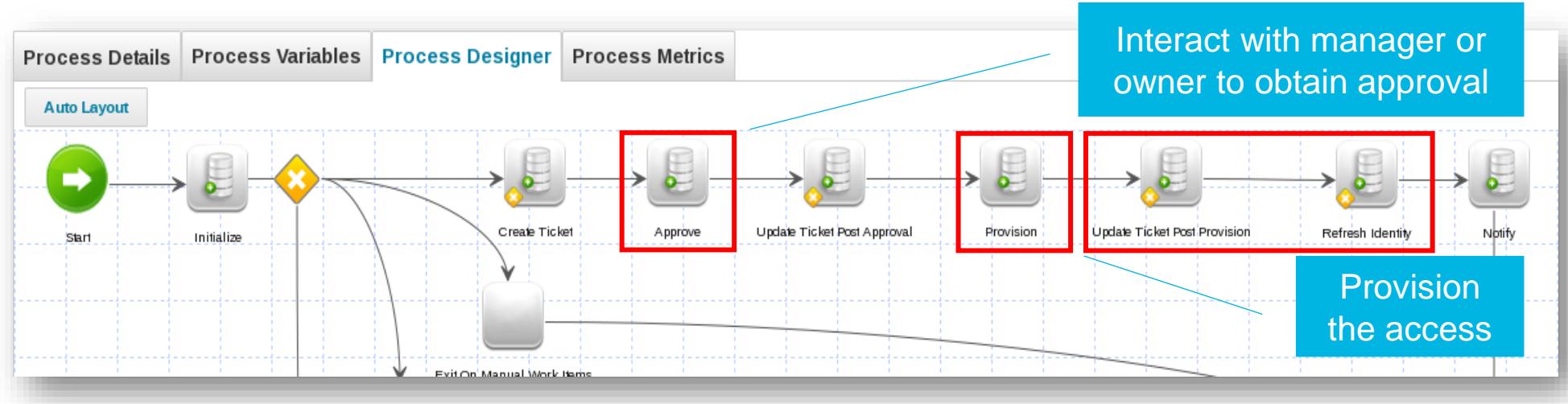
- Check Active Policies
- Prune Identity Cubes
- Refresh Entitlement Correlation
- Refresh Groups
- Refresh Identity Cube (highlighted with a red box)
- Refresh Identity Cubes and Scope
- Refresh Identity Cubes with Process Event
- Refresh Risk Scores
- Refresh and Provision Roles

A tooltip for 'Refresh Identity Cube' indicates it performs a full refresh of all identities. To the right of the table, a 'New Task' button is visible. On the far right, a sidebar titled 'Templates' lists various task types, each with a red box around its name:

- Account Aggregation
- Account Group Aggregation
- Activity Aggregation
- Alert Aggregation
- Alert Processor
- Application Builder
- ArcSight Data Export
- Data Export
- Effective Access Indexing
- Encrypted Data Synchronization Task
- Entitlement Role Generator
- FIM Application Creator

# Business Processes (Workflows)

- A runnable repeatable set of steps to perform work
- Triggered by system events or a user request



- Business processes are pre-defined in IdentityIQ
- Implementation team responsibilities
  - Configure business processes
  - Can develop business processes specific to your environment

# Incorporating Business Logic

## BeanShell Rules

- Snippets of user code written to inject business logic
- Common uses
  - Control certification behavior
  - Customize data during aggregation
  - Define unique business policies
  - Provide application provisioning logic
  - ...and many more!
- Rule “hooks” provided throughout IdentityIQ
- Stored as reusable objects in the database

Quicklink Example



Certification Example



# Knowledge Check





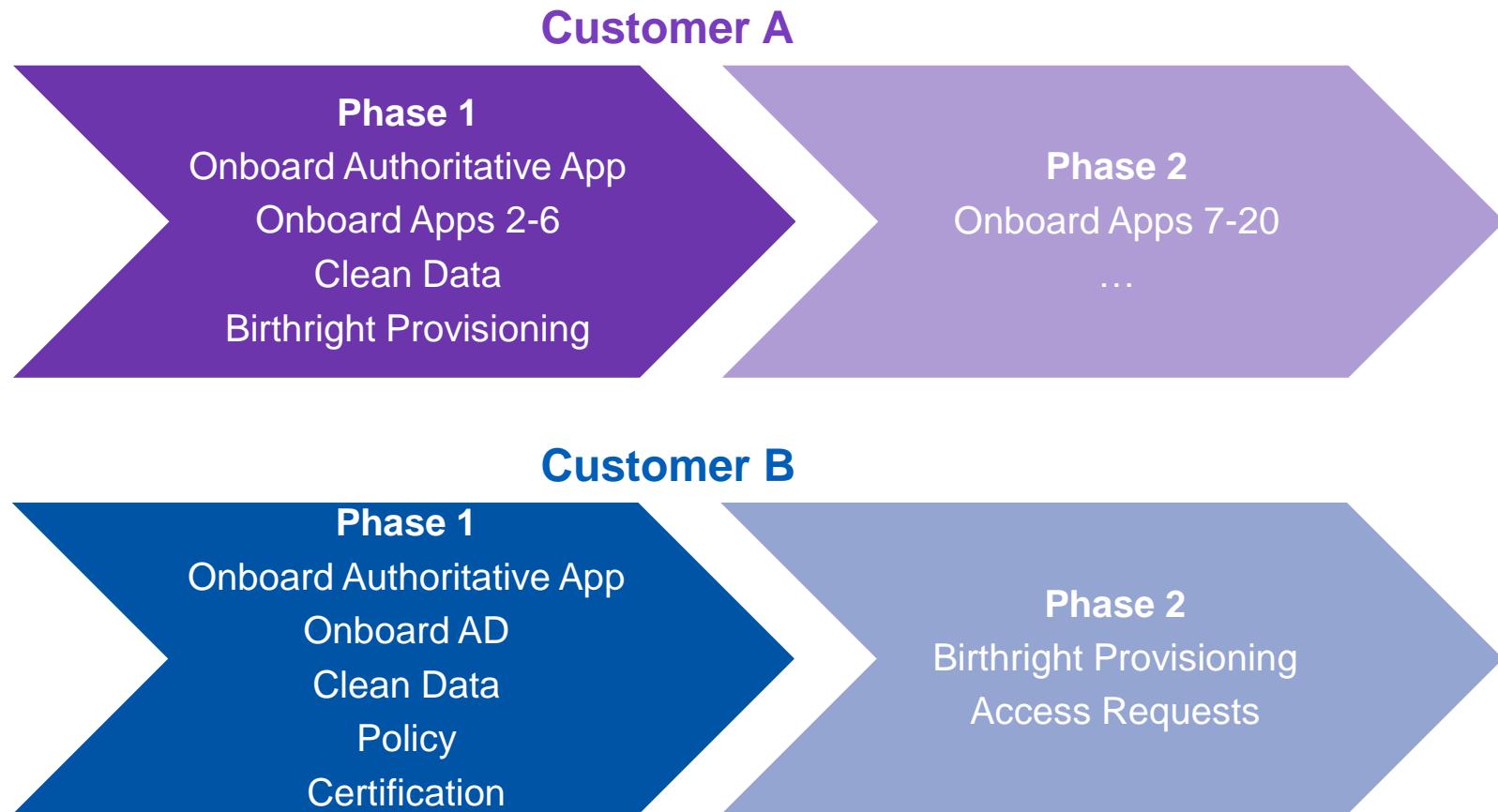
# IdentityIQ Implementation Overview

IdentityIQ Essentials

# Implementation Projects

## Key Considerations

- Phased Approach
  - By application
  - By functionality
- Clean-up Data
  - User accounts/entitlements
  - Entitlement catalog
  - Identity attributes



# Implementation Options

Rapid Setup	Standard IdentityIQ Configurations	Accelerator Park
<ul style="list-style-type: none"><li>Allows a broad team of people to participate in deployment</li><li>Supported by core product data structure</li><li>Framework for quick configuration of common scenarios</li><li>Available since IdentityIQ 8.1</li><li>Preferred option</li></ul>	<ul style="list-style-type: none"><li>Options for all configurations needs</li><li>Available in all versions of IdentityIQ</li><li>Leveraged by technical team</li></ul>	<ul style="list-style-type: none"><li>Same technical goal as Rapid Setup</li><li>Leverages IdentityIQ extension options</li><li>Available since IdentityIQ 7.3</li></ul>

# Knowledge Check

# Implementation Project from Class Exercises

---

## Phased Implementation

- Phase 1
  - Onboard identities
  - Organize identities and grant IdentityIQ capabilities
  - Aggregate account and entitlement data into IdentityIQ
  - Manage account and entitlement data
- Phase 2
  - Implement compliance
  - Define access model (roles)
- Phase 3
  - Set up for provisioning
  - Enable provisioning based on data changes
  - Enable provisioning based on user requests

Next Step?

# Practice Exercises

# Exercise Preview

---

## Section 1, Exercise 1

- Exercise 1: Configure IdentityIQ
  - Confirm installation of IdentityIQ
    - Manual installation instructions
      - Included in appendix
      - Useful for reference and later practice
    - Redirect email
    - Update object expiration
    - Configure auditing

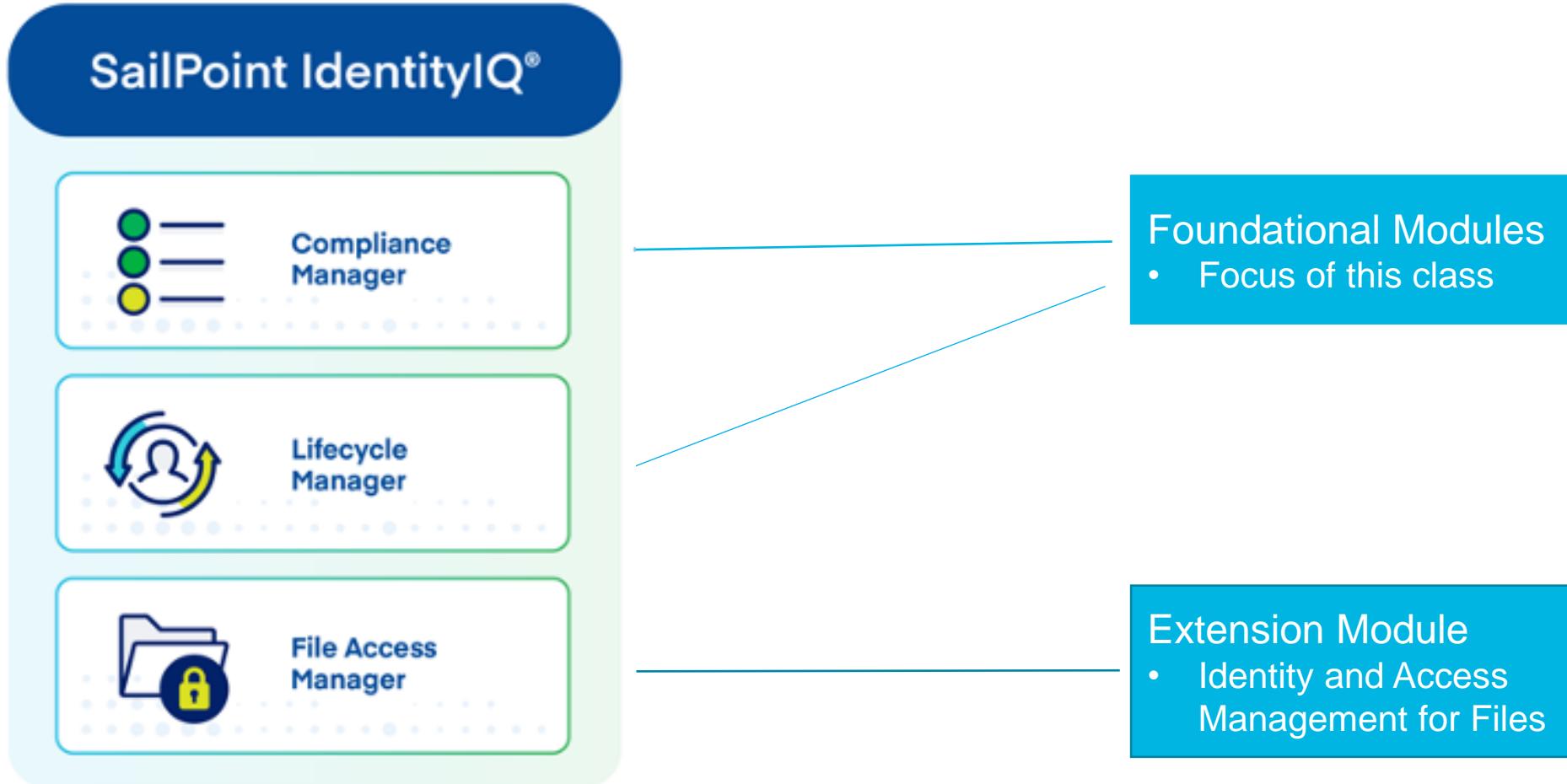




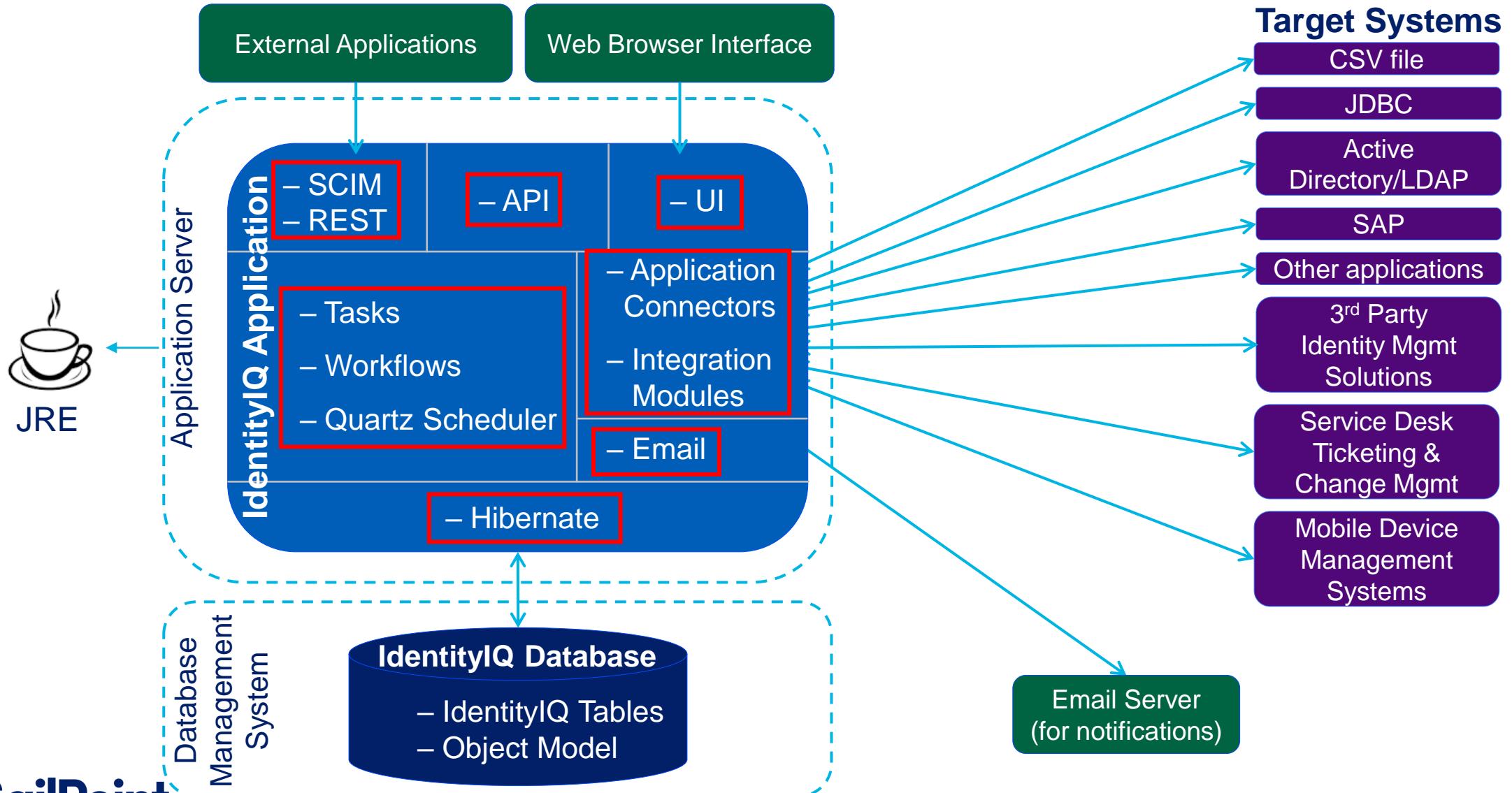
# Product Architecture

IdentityIQ Essentials

# IdentityIQ Platform Modules



# Detailed Architecture Overview



# System Choices

---

## Supported Platforms

- Application Servers
  - Tomcat
  - WebSphere & WebSphere Liberty
  - WebLogic
  - JBoss
- Databases
  - MySQL
  - Oracle
  - MS SQL Server
  - DB2
  - AWS Aurora (cloud)
  - Azure SQL (cloud)
- Java Platform
  - Oracle JDK
  - Red Hat OpenJDK (Linux)
  - AdoptOpenJDK (Windows)
- Supported Cloud Platforms
  - AWS EC2
  - Azure VM
- Browsers
  - Firefox
  - Internet Explorer and Edge
  - Google Chrome
  - Safari

*Deploy what you are most comfortable maintaining!!!!*

# Knowledge Check

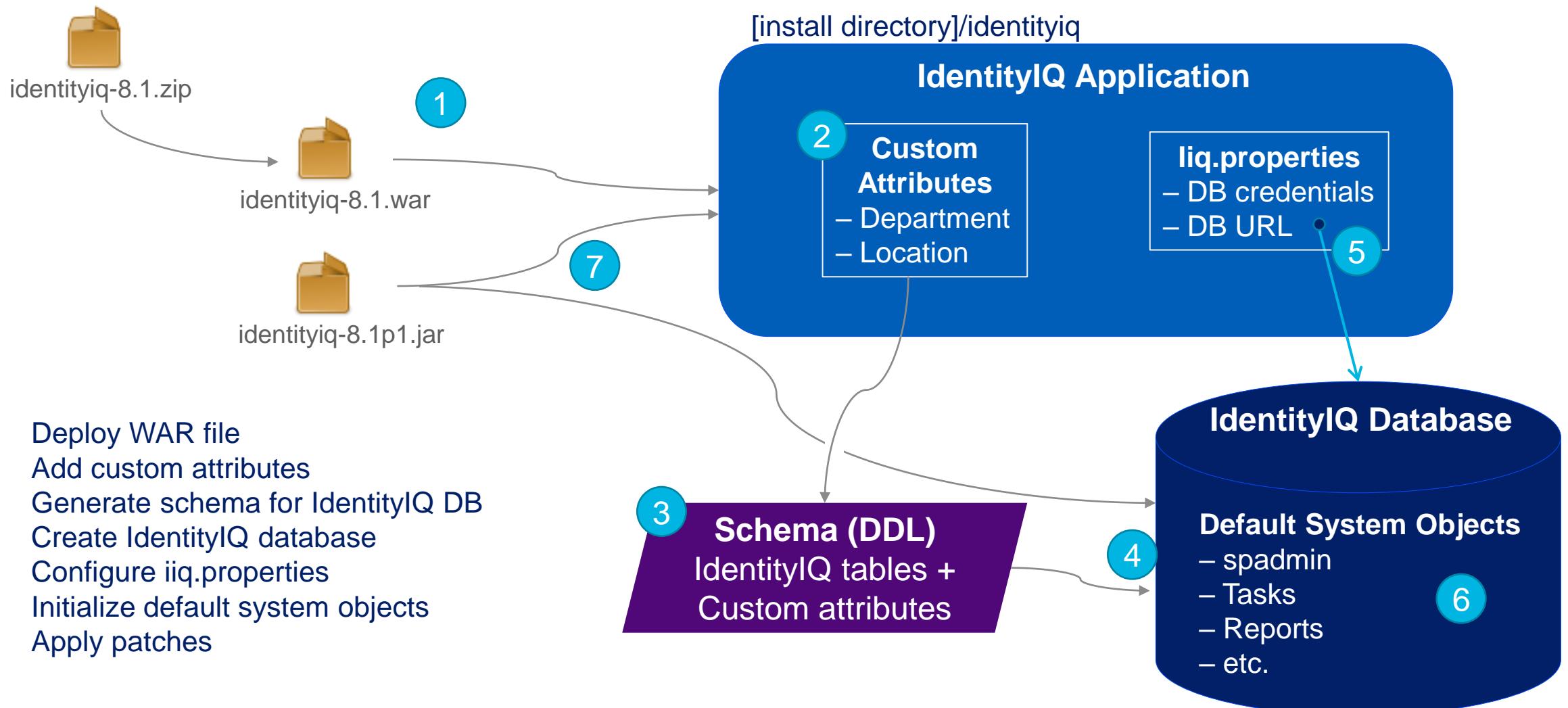




# IdentityIQ Installation

IdentityIQ Essentials

# IdentityIQ Installation Process



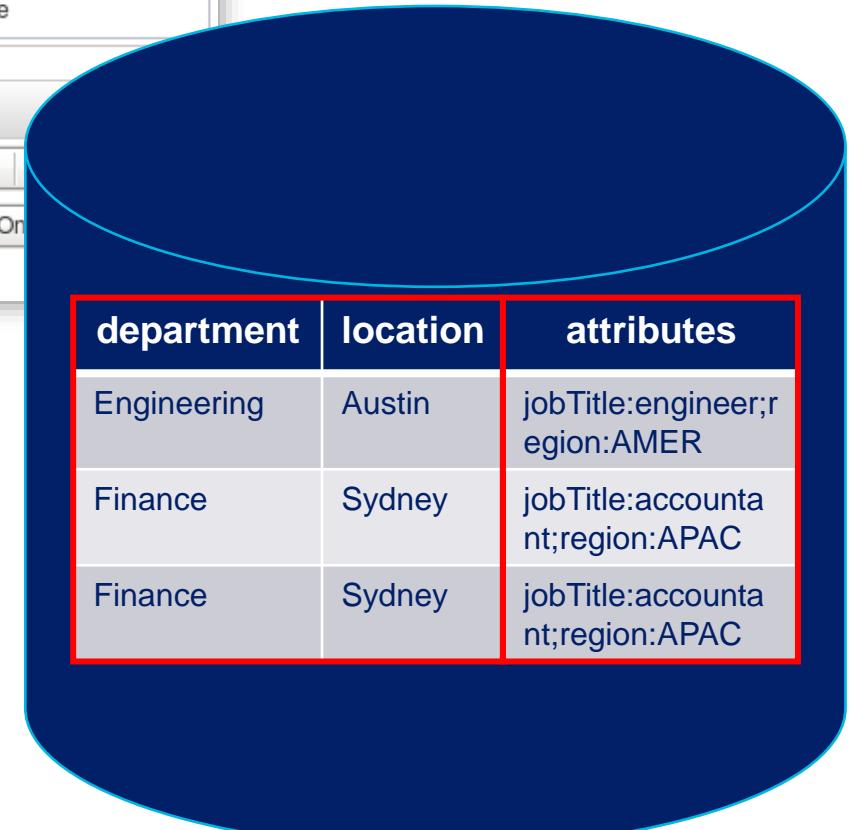
# IdentityIQ Extended Attributes

## Storage

- Several objects can be extended
  - Applications
  - Roles (bundle)
  - Certification Items
  - Identities
  - Accounts (link)
  - Entitlements (managed attributes)
- Created through GUI
  - Not marked searchable
    - Stored in a CLOB
    - Efficient loading and storage
  - Marked searchable
    - Stored in their own column
    - Efficient for searching
    - Supports ad hoc queries, correlating accounts to identities, etc.

Edit Identity Attribute

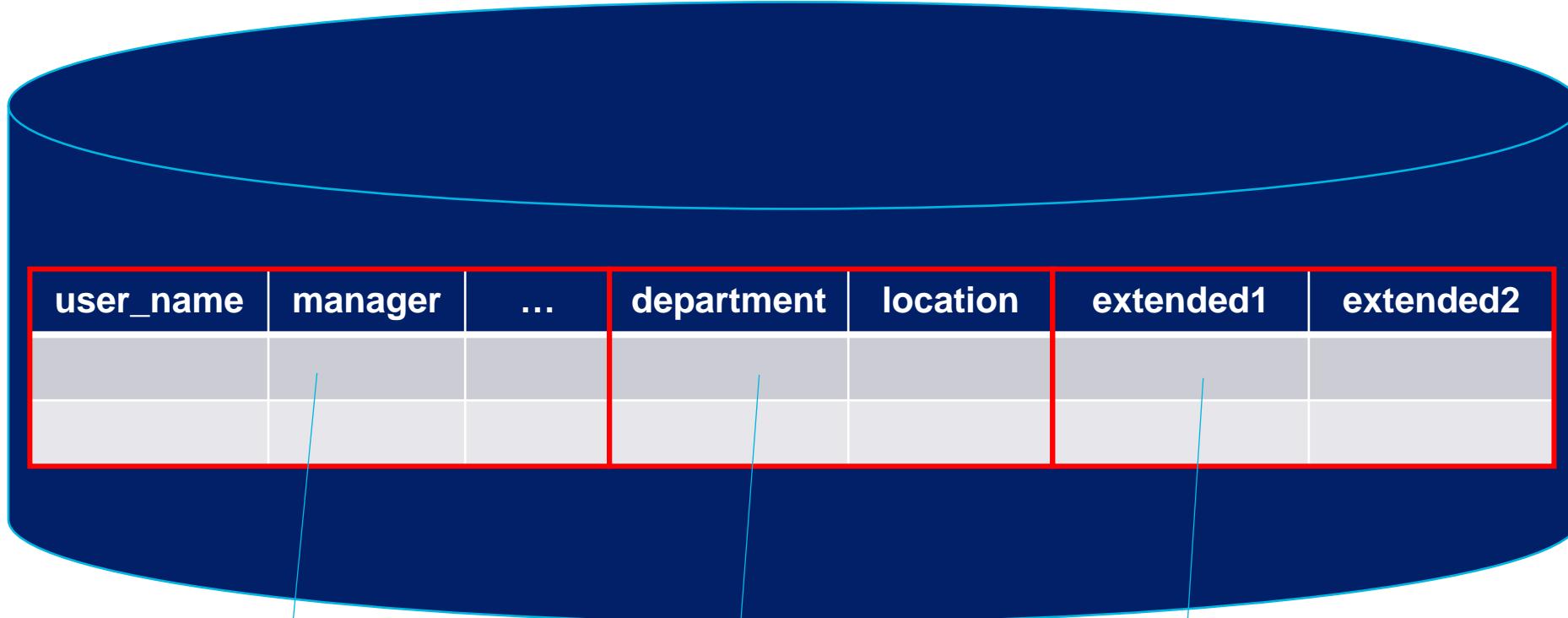
Identity Attribute	
Attribute Name	jobTitle
Display Name	Job Title
Advanced Options	
Attribute Type	String
Edit Mode	<input type="checkbox"/> Read Only <input checked="" type="checkbox"/> Searchable



department	location	attributes
Engineering	Austin	jobTitle:engineer;region:AMER
Finance	Sydney	jobTitle:accountant;region:APAC
Finance	Sydney	jobTitle:accountant;region:APAC

# Database Schema Configuration

## 3 Types of Searchable Attributes



**Standard Attributes**  
*Predefined by IdentityIQ*

**Named Extended Attributes**  
*Named column*  
*Defined by user*

**Placeholder Extended Attributes**  
*Column space*  
*Defined by user*

# Configure Database Schema

## Adding Database Columns for Extended Attributes

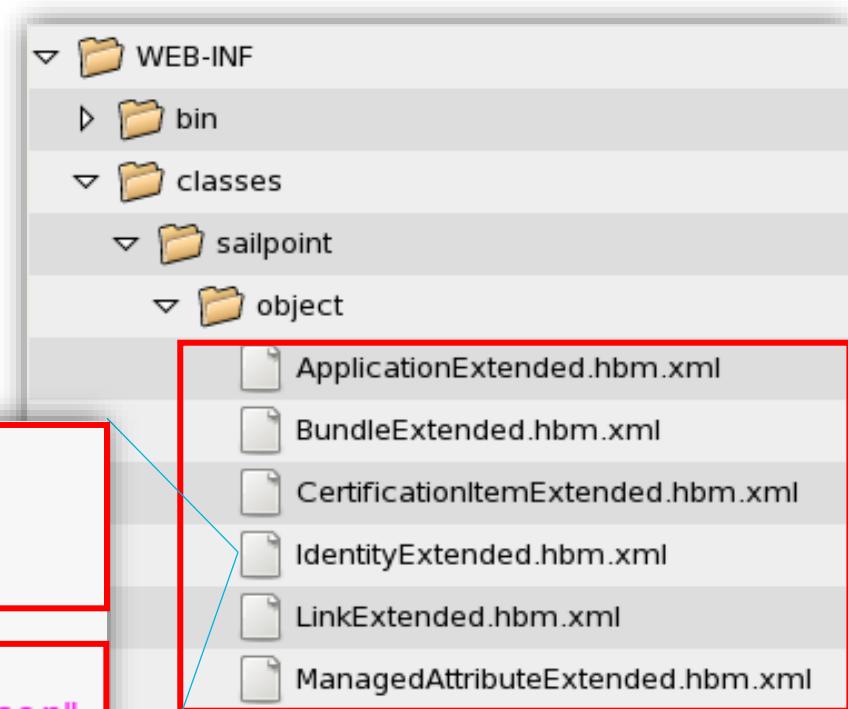
- Edit the appropriate Hibernate XML files
  - Add columns
  - Optionally specify indices

IdentityExtended.hbm.xml

```
<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="department" type="string" length="450"
          access="sailpoint.persistence.ExtendedPropertyAccessor"
          index="spt_identity_department_ci"/>
<property name="location" type="string" length="450"
          access="sailpoint.persistence.ExtendedPropertyAccessor"
          index="spt_identity_location_ci"/>
```

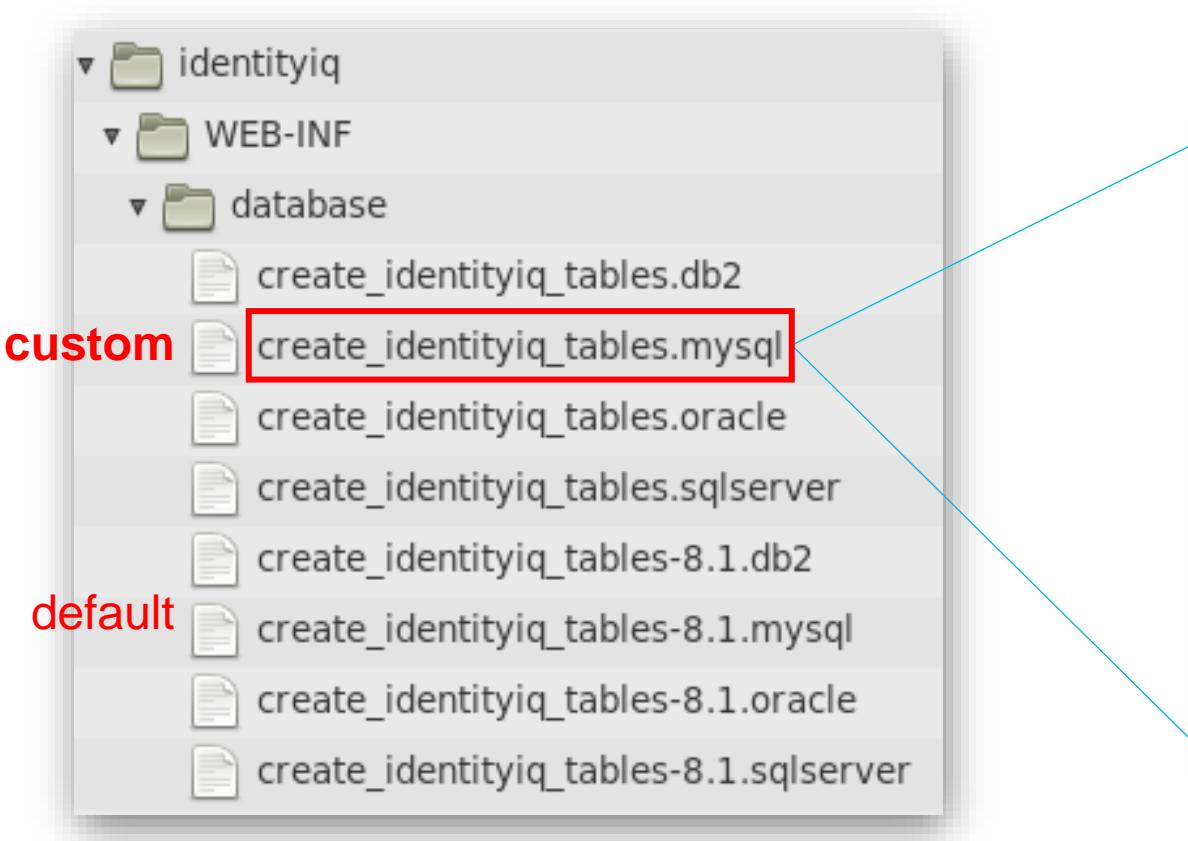
Placeholder  
(max 20 per object)



Named  
(up to DB limit)

# Generate Database Schema (DDL)

- Create IdentityIQ database  
.../WEB-INF/bin/iiq schema



## create\_identityiq\_tables.mysql

```
create table identityiq.spt_identity
  id varchar(32) not null,
  extended1 varchar(450),
  extended2 varchar(450),
  department varchar(450),
  location varchar(450),
  manager varchar(32),
  display_name varchar(128),
  firstname varchar(128),
  lastname varchar(128),
  email varchar(128),
  inactive bit
  ...
  ...
```

# Create IdentityIQ Database

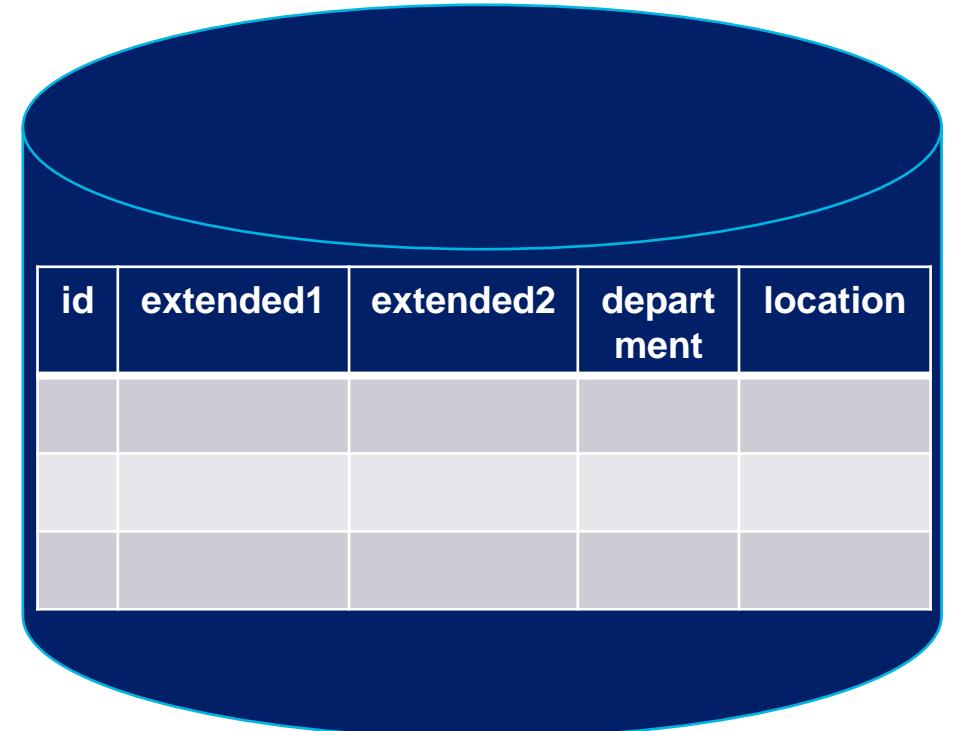
`create_identityiq_tables.mysql`

```
create table identityiq.spt_identity
  id varchar(32) not null,
  extended1 varchar(450),
  extended2 varchar(450),
  department varchar(450),
  location varchar(450);
```



```
spadmin@training:~/tomcat/webapps/identityiq/WEB-INF/database$ mysql -u root -p
Welcome to the MySQL monitor.

mysql> source create_identityiq_tables.mysql
```

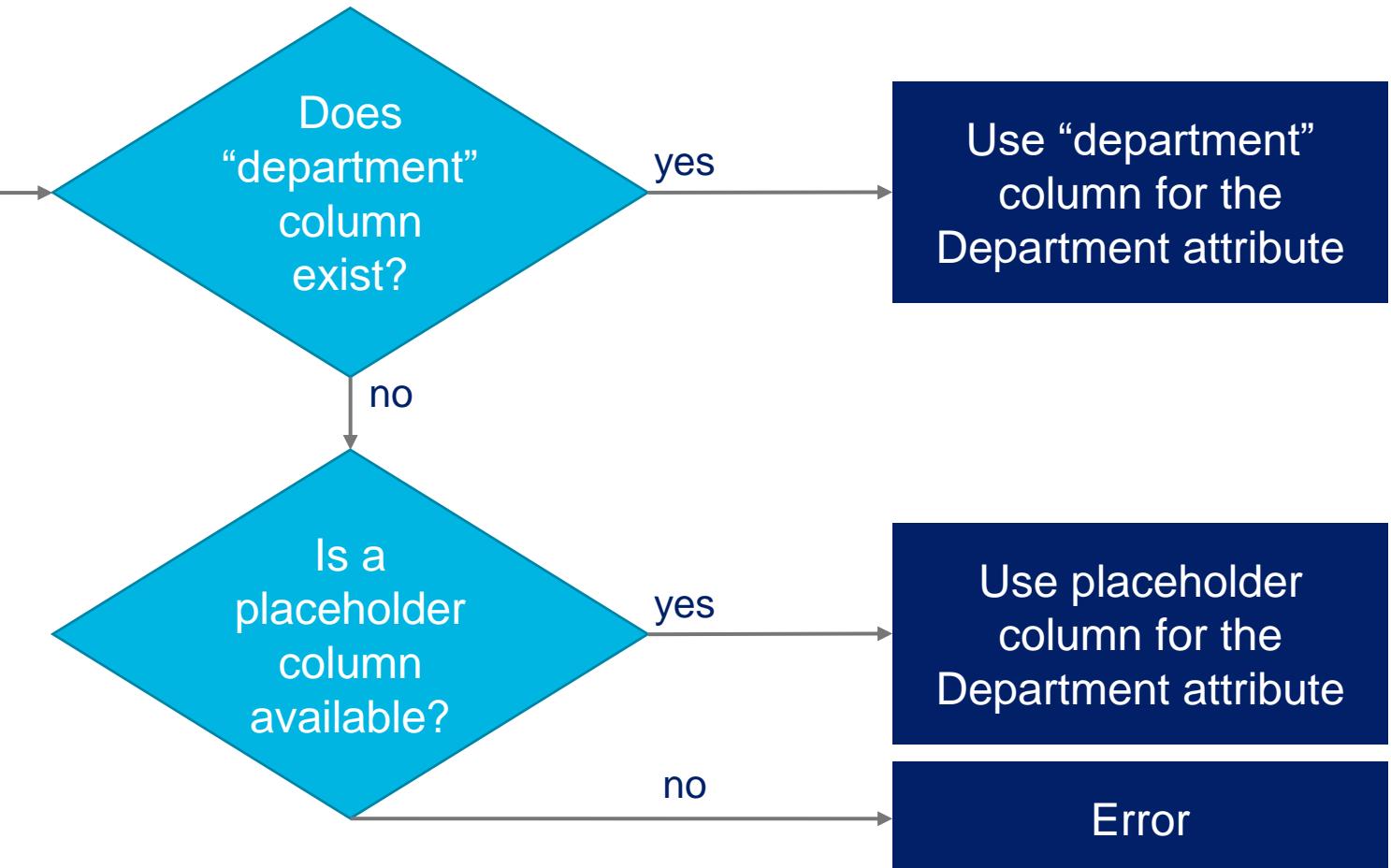


# Using New Database Columns

## Searchable Attributes

Edit Identity Attribute

Identity Attribute	
Attribute Name	department
Display Name	Department
Advanced Options	
Attribute Type	String
Edit Mode	Read Only
Searchable	<input checked="" type="checkbox"/>



# Extend Database

---

## Reusing Placeholder Columns

- Add named columns to hibernate file
- Create delta DDL
  - .../WEB-INF/bin/iiq extendedSchema
- Locate new database schema files (DDL) in database directory
  - .../WEB-INF/database
- Use delta DDL to update existing IdentityIQ database
- Move data from placeholder columns to named columns
  - See whitepaper *Managing Extended Attributes* for details

# Configure IdentityIQ Properties

## Identify Database to IdentityIQ

- /WEB-INF/classes/iiq.properties

```
dataSource.username=IdentityIQ  
dataSource.password=1:iCAlakm5CVUe7+Q6hVJIBA==
```

```
##### MySQL/Aurora (without SSL) #####
```

```
dataSource.url=jdbc:mysql://localhost/identityiq?useServerPrepStmts=true&tinyInt1isBit=true&useUnicode=true&  
characterEncoding=utf8&useSSL=false&serverTimezone=UTC  
dataSource.driverClassName=com.mysql.cj.jdbc.Driver  
sessionFactory.hibernateProperties.hibernate.dialect=org.hibernate.dialect.MySQL57Dialect
```

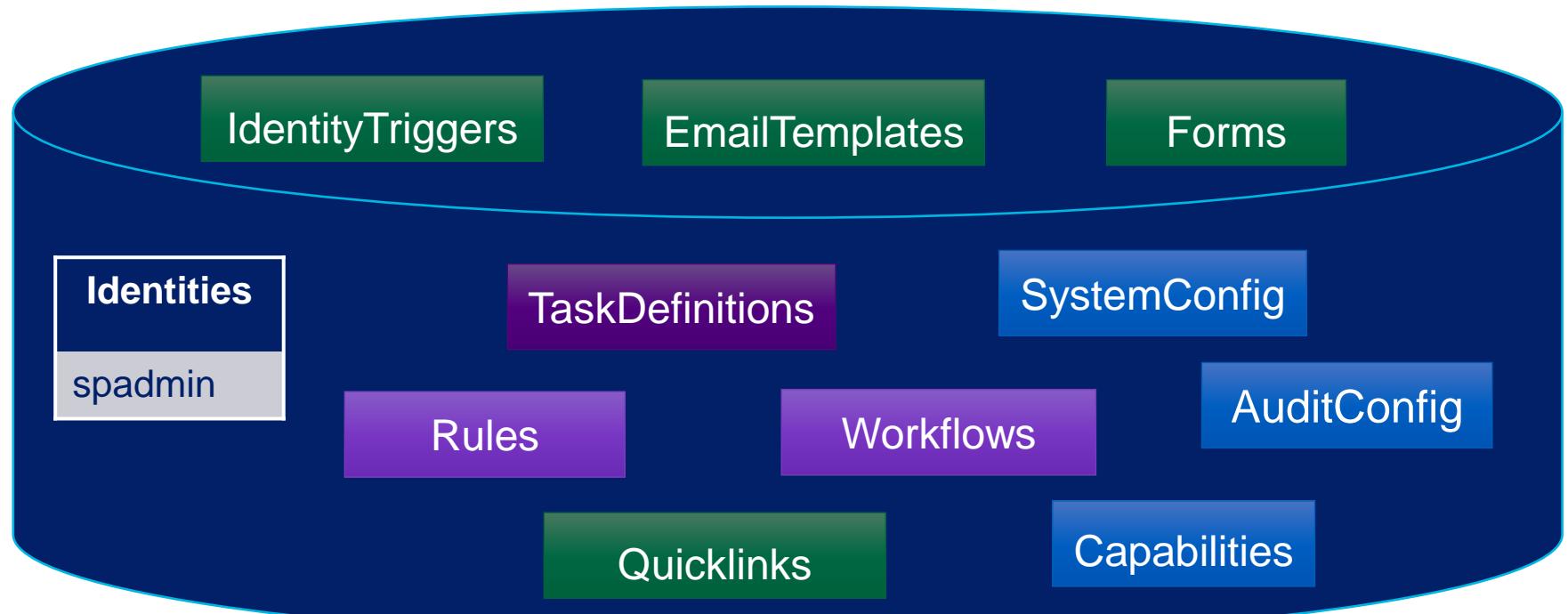
Database Username

Database Password  
Encrypt using *iiq encrypt*  
command

Data Source URL  
specifying  
host/port/database

# Initialize IdentityIQ Default Objects

- Initializing IdentityIQ  
.../WEB-INF/bin/iiq console  
> **import init.xml**
- Initializing IdentityIQ Lifecycle Manager  
.../WEB-INF/bin/iiq console  
> **import init-lcm.xml**



# Knowledge Check





# Creating Identity Cubes

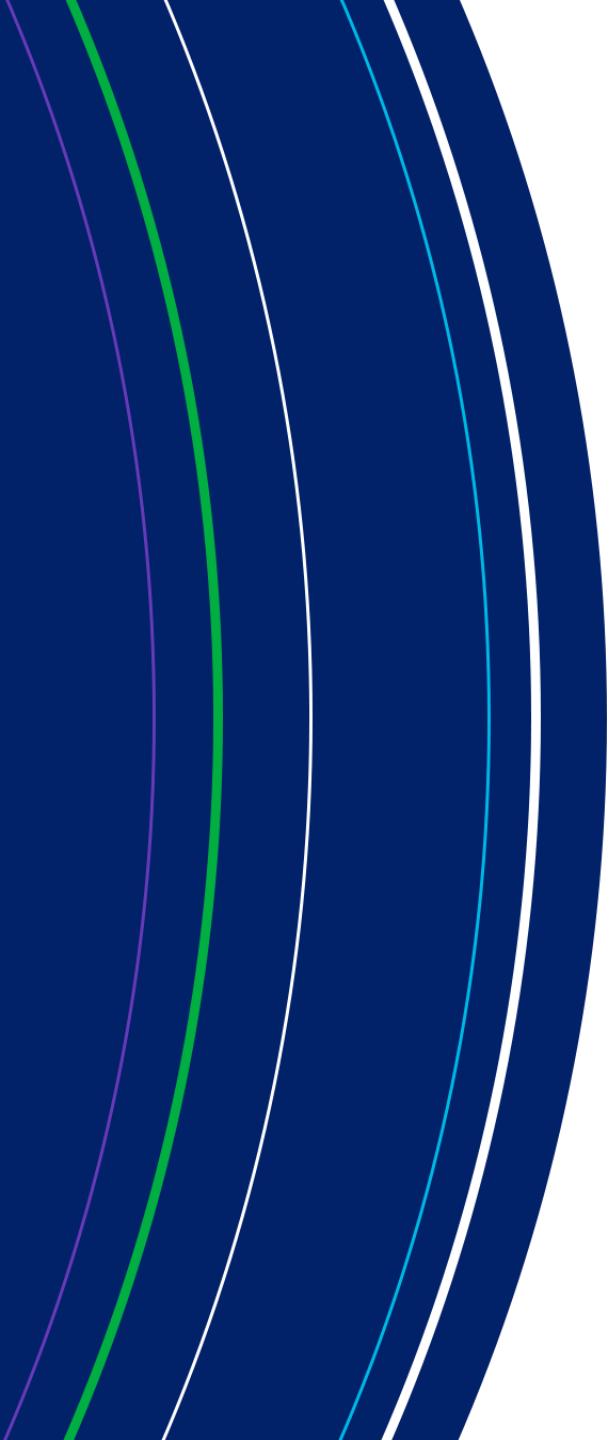
IdentityIQ Essentials

# Overview

---

## Creating Identity Cubes

- Identity Cube overview
- Authoritative application configuration
- Aggregation task



# Identity Cubes

# Identity Cube

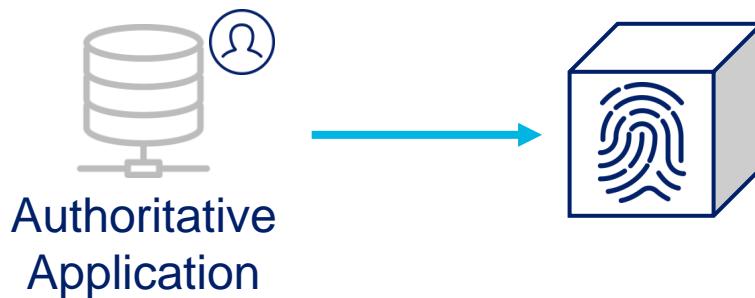
---

- Term to refer to all information we have collected in IdentityIQ about any given identity (e.g. person or access-holding entity)
- Stores all information known about an identity
  - Examples:
    - Identity Attributes
    - Application Accounts
    - Entitlements/Roles
    - Risk Score
    - Policy Violations
    - User Rights
  - Information on the cube is
    - Discovered
    - Requested
    - Assigned
    - Calculated



# How are Identity Cubes Created?

- Automatically through account aggregation
  - Mark “system of record” application as authoritative
  - Process creates authoritative Identity Cube for each account
  - Identity Attributes populated from authoritative applications
- Manually using Lifecycle Manager
  - Form presented to user to enter Identity Attributes



**Create Identity**

If you would like to request that a new identity be created, please fill in the fields below. Fields marked with an asterisk are required.

Identity Name *	<input type="text"/>
Password *	<input type="password"/>
Confirm Password *	<input type="password"/>
First Name	<input type="text"/>
Last Name	<input type="text"/>
Email	<input type="text"/>
Manager	<input type="text"/>

# Identity Cube – User Interface

## Identity Attributes

The screenshot shows the 'View Identity Adam.Kennedy' page. At the top, there is a navigation bar with tabs: Attributes (highlighted with a red box), Entitlements, Application Accounts (highlighted with a red box), Policy, History, Risk, Activity, User Rights, and Events.

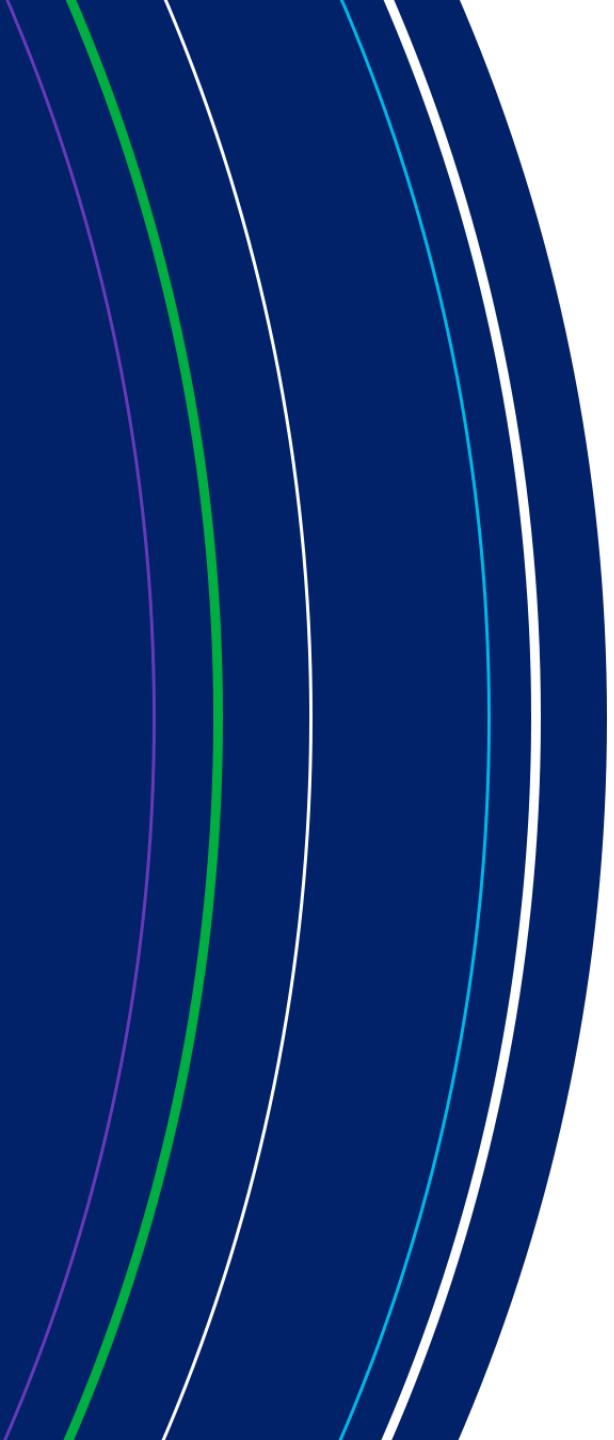
Below the navigation bar, there is a table with user information:

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

A blue callout box labeled 'User's identity data Sourced from user's accounts or by rules' points to the table.

To the right, a separate window titled 'User's Accounts' shows a list of application accounts:

Application
<input type="checkbox"/> Financials ▾
<input type="checkbox"/> HR System - Employees ▾
<input type="checkbox"/> LDAP ▾
<input type="checkbox"/> TRAKK ▾



# **Configuring Authoritative Applications**

# Application/Connector Configuration

Edit Application HR System - Employees

Details Configuration Correlation Accounts Risk Activity Data Sources Rules Password Policy

\*indicates a required field.

\*Name ?

HR System - Employees

\*Owner ?

The Administrator

\*Application Type ?

DelimitedFile

Description ?

English (United States)

0 of 1024 characters (including markup)

Revoker ?

Proxy Application ?

Profile Class ?

Authoritative Application ?

Case Insensitive ?

Native Change Detection ?

Application Meta Information

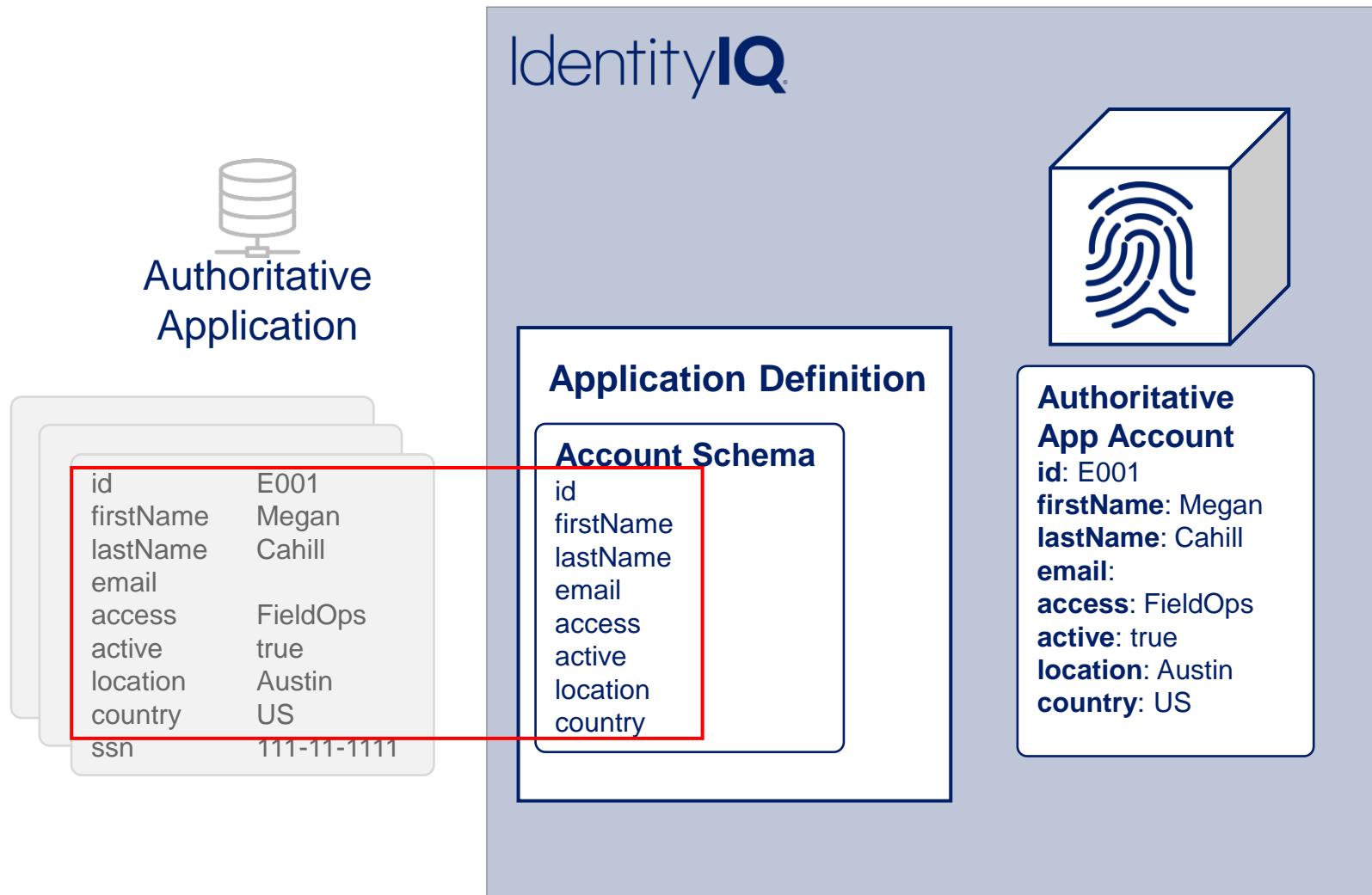
Application Type = Connector

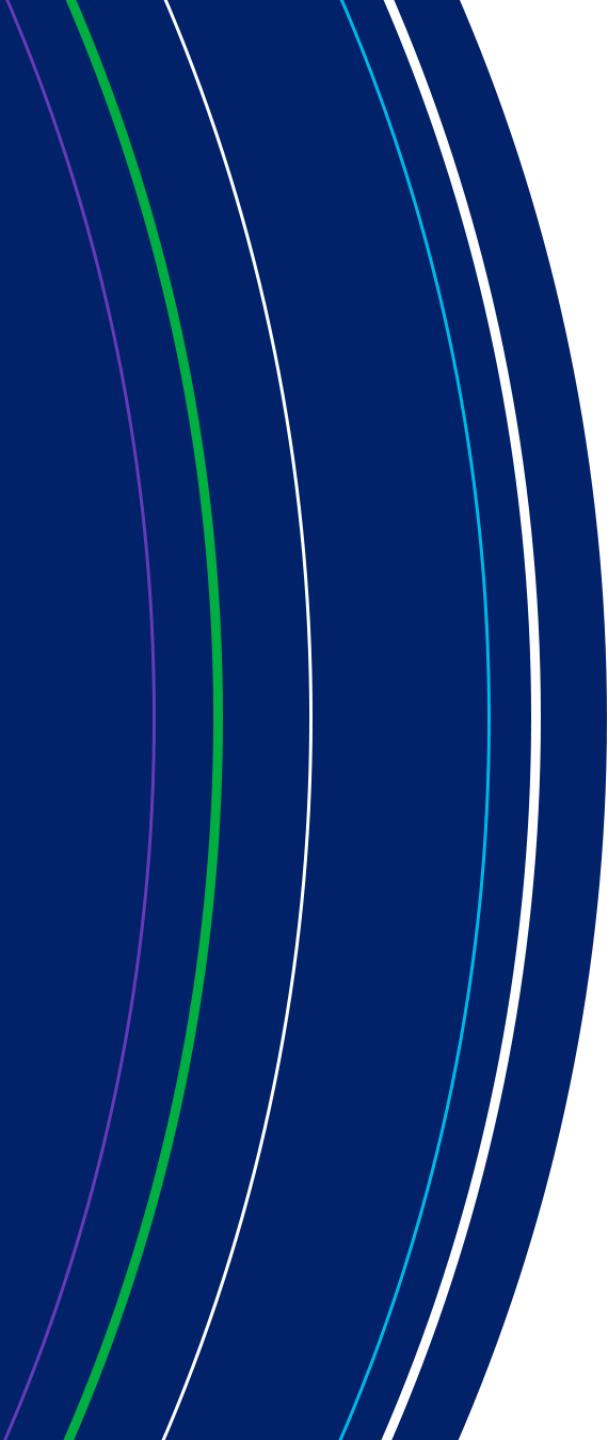
Authoritative Indicator

This screenshot shows the 'Edit Application' interface for 'HR System - Employees'. The 'Details' tab is selected. The 'Name' field contains 'HR System - Employees'. The 'Owner' field is set to 'The Administrator'. The 'Application Type' dropdown is set to 'DelimitedFile'. The 'Description' field is empty. In the 'Authoritative Indicator' section, the 'Authoritative Application' checkbox is checked. A callout box labeled 'Application Type = Connector' points to the 'Application Type' dropdown. Another callout box labeled 'Authoritative Indicator' points to the 'Authoritative Application' checkbox. A callout box labeled 'Application Meta Information' points to the 'Revoker', 'Proxy Application', and 'Profile Class' fields.

# Account Schema

- Represents application account
- Defines which account attributes to read
- Often pre-defined
- Required for each application



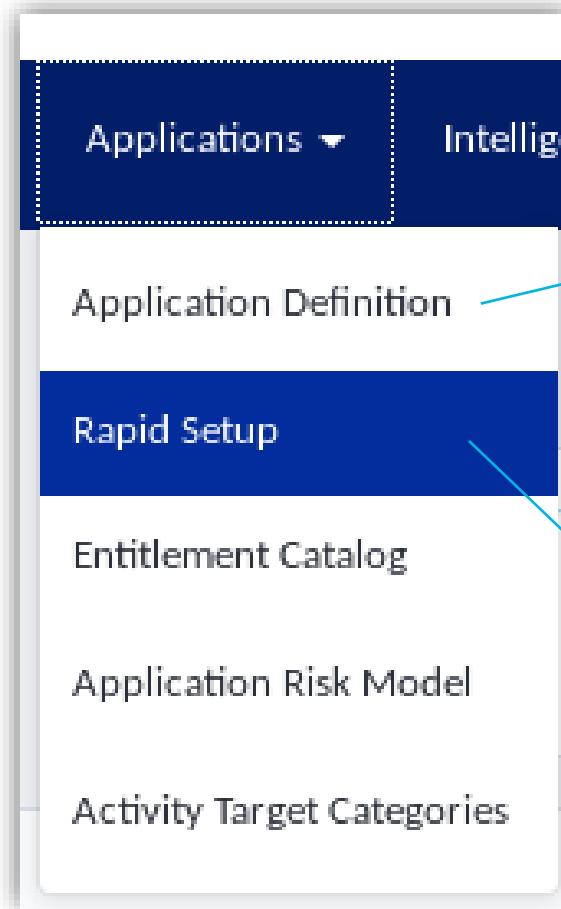


# Rapid Setup

# Rapid Setup

## Additional Configuration Settings

- Correlation Configurations
- Data Categorization
  - Account Status
  - Identity Type



First, define application connectivity

Then, configure application behavior

# Rapid Setup Aggregation Configuration

## Correlation

The screenshot shows the 'Rapid Setup' interface for the application 'HR Employees'. The left sidebar lists 'Aggregation' (selected), 'Joiner', 'Mover', and 'Leaver'. A blue callout box labeled 'Identity Correlation Logic' points to the 'Identity Correlation' section, which contains fields for 'fullName' (\_Equals\_ 'User Name'). Another blue callout box labeled 'Manager Correlation Logic' points to the 'Manager Correlation' section, which contains fields for 'managerId' (\_Equals\_ 'Select Identity Attribute...'). The main area is titled 'Aggregation' with the sub-instruction 'Provide classification and categorization details for this application aggregation'. It includes a toggle switch for 'Create Entitlements That Cannot Be Requested'.

Rapid Setup: HR Employees

Aggregation

Joiner

Mover

Leaver

Identity Correlation Logic

Manager Correlation Logic

Aggregation

Provide classification and categorization details for this application aggregation

Create Entitlements That Cannot Be Requested ?

Identity Correlation

The Correlation configuration could be a shared configuration across other applications. Any changes made here will be reflected for all applications which share this configuration.

fullName Equals User Name

+ Add Filter

Manager Correlation

managerId Equals Select Identity Attribute...

+ Add Filter

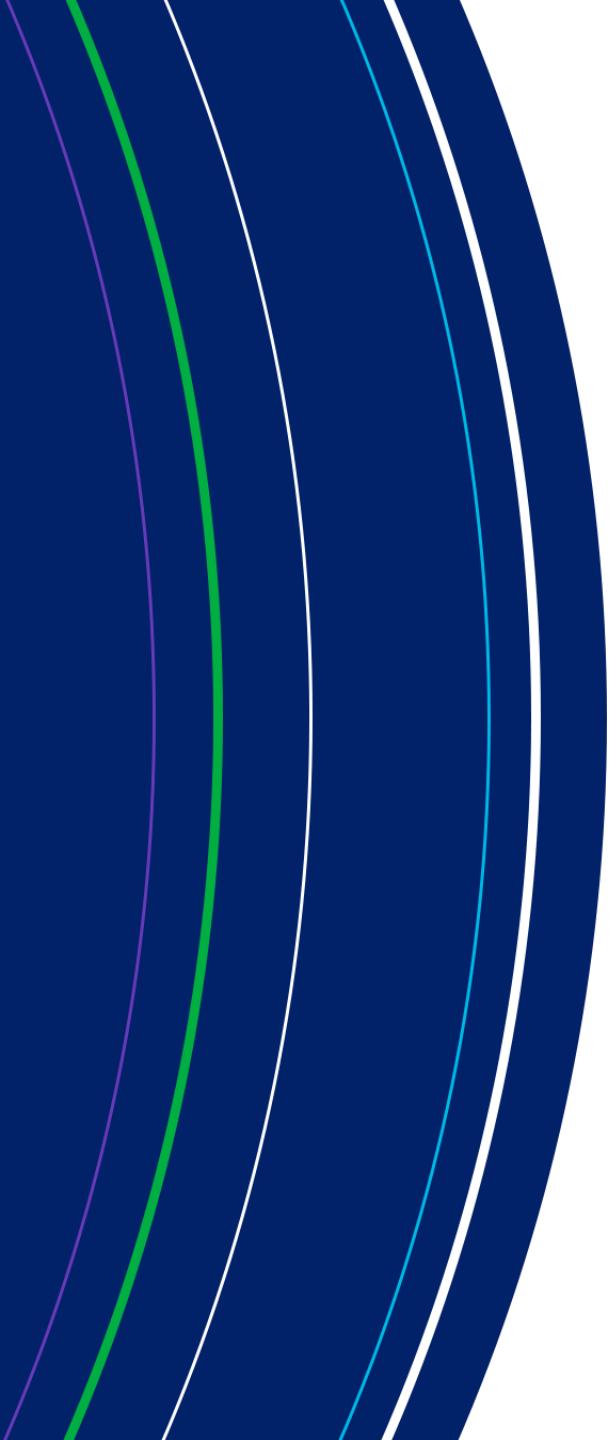
# Rapid Setup Aggregation Configuration

## Categorization

The screenshot shows the 'Rapid Setup' configuration interface for 'HR Employees'. On the left, there are two blue boxes: 'Account Status' and 'Identity Type'. Blue lines connect these boxes to the corresponding sections in the main configuration area.

**Aggregation** (Top Left):

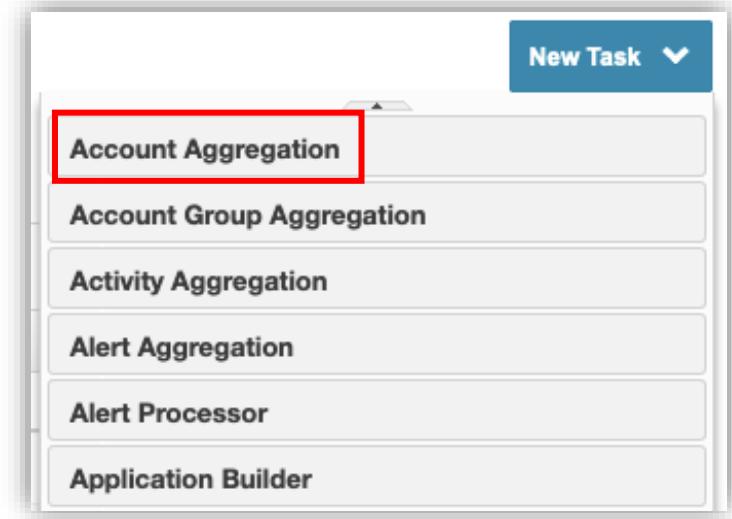
- Joiner**: A blue box containing 'Account Status' and 'Identity Type'.
- Disable Account**: Filter: inactiveUser Equals TRUE
- Lock Account**: Filter: + Add Filter
- Service Account**: This will change the identity type of the identity to which this account correlates. Filter: fullName Starts With SRV
- RPA Account**: This will change the identity type of the identity to which this account correlates. Filter: workStatus Equals RPA



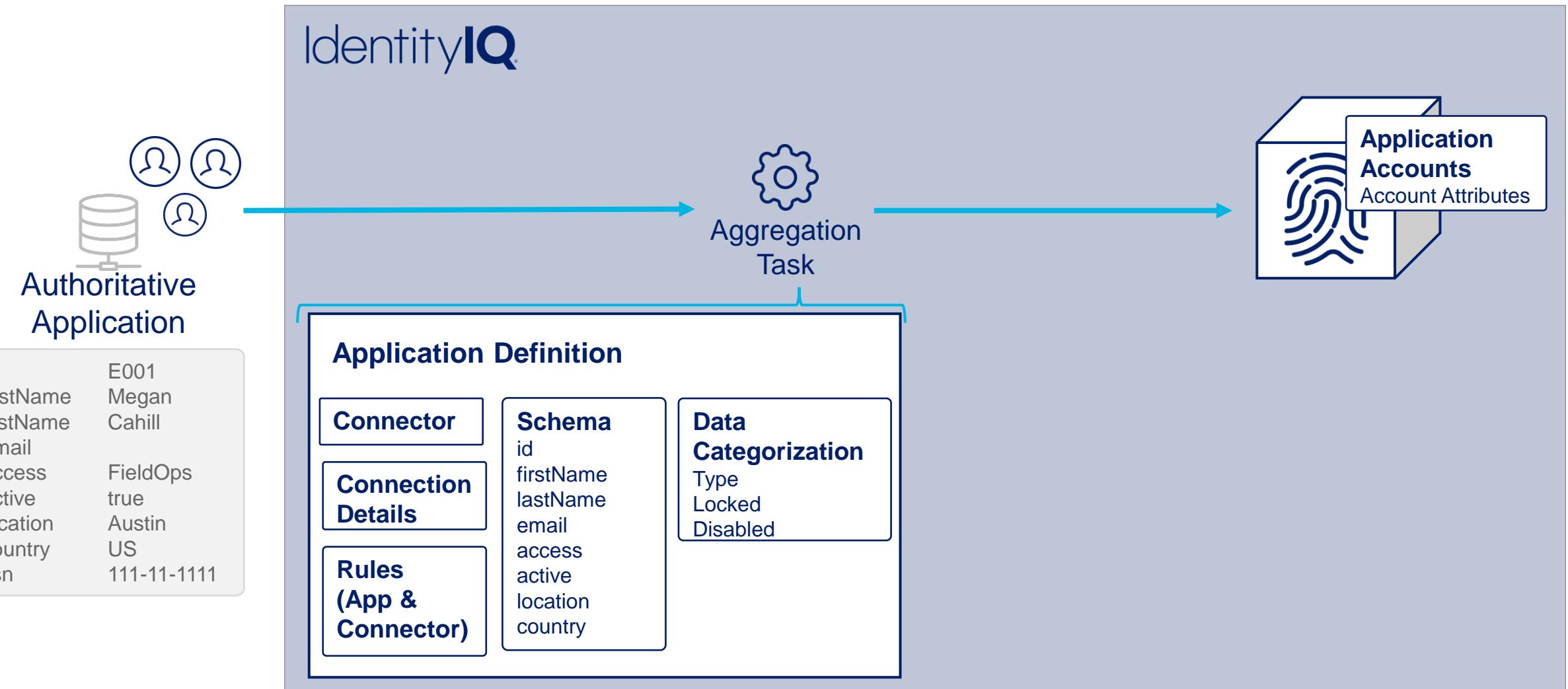
# Account Aggregation

# Account Aggregation Tasks

- Many configuration options
  - Which Applications to Aggregate (required)
  - Detect Deleted Accounts (best practice)
  - And many more...
- Use Application/Connector/Schema information



# Identity Cube Creation Process



# Account Aggregation Tasks

Purpose: Read Application Accounts

View Identity Kennedy

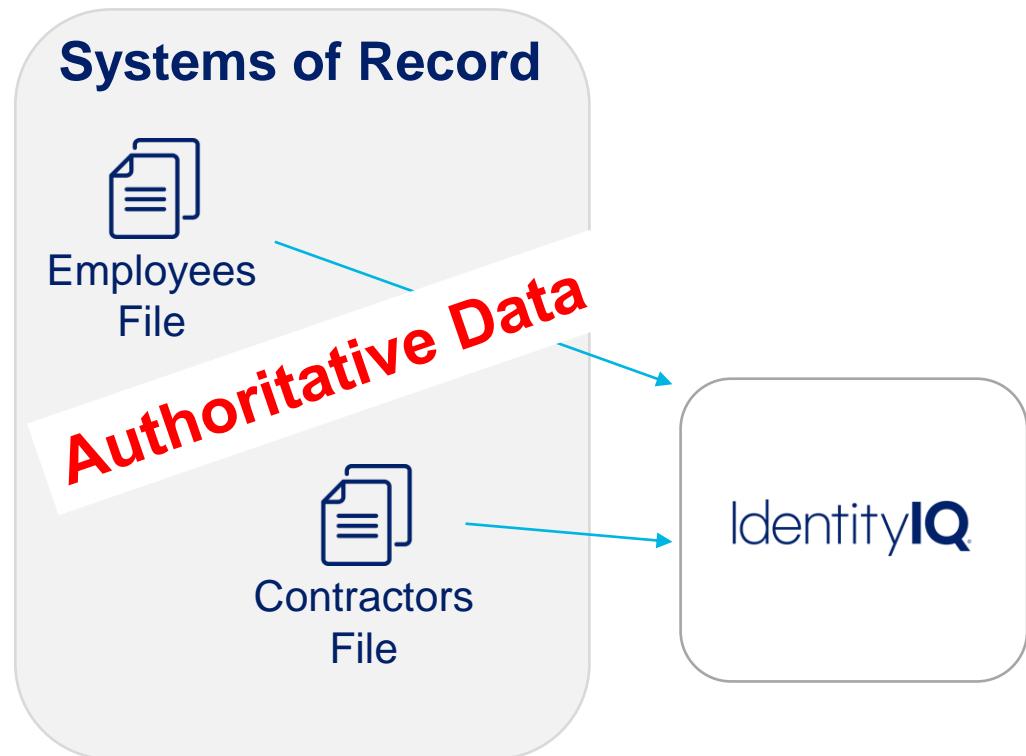
Attributes	Entitlements	Application Accounts	Policy	History	Risk	Activity	User Rights	Events
Application Accounts								
Application	Account Name							
<input type="checkbox"/> HR Employees ▾	Adam.Kennedy							
<a href="#">Delete</a>	<a href="#">Move Account</a>							

# Knowledge Check

# Practice Exercises

# Exercise Preview

## Section 1, Exercise 2



- Create Identity Cubes
  - Define authoritative applications
  - Set default passwords
  - Rapid Setup classification
  - Aggregate accounts to create Identity Cubes





# Identity Attributes and Mappings

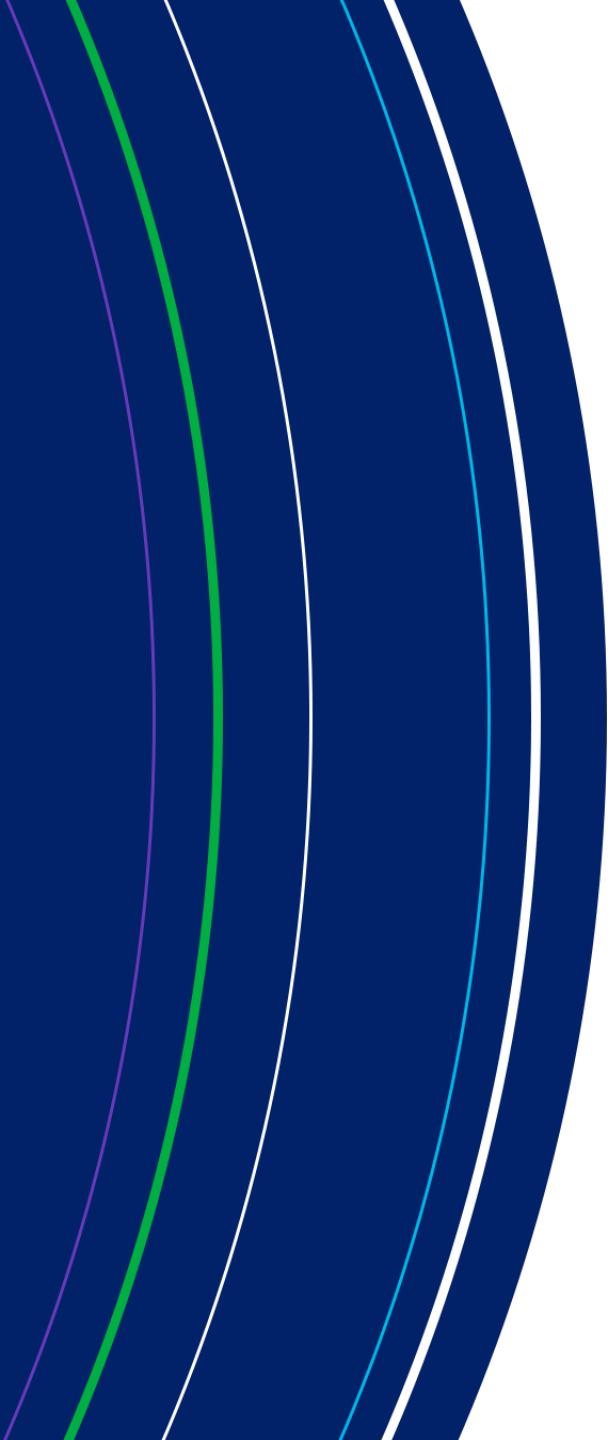
IdentityIQ Essentials

# Overview

---

## Identity Attributes and Mappings

- Identity Mappings: Identity attribute configuration
- Identity Refresh tasks



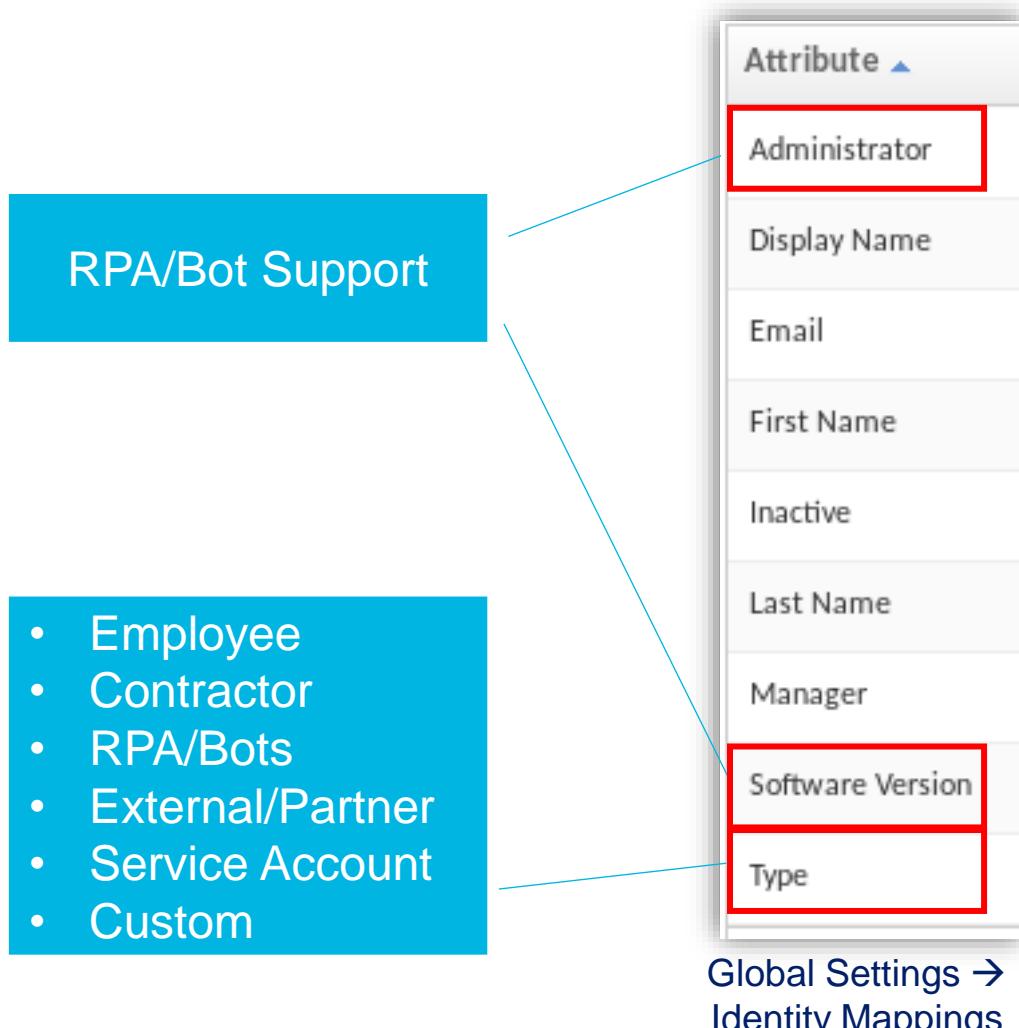
# **Identity Attributes and Mappings**

# Identity Attributes

- Identity data used to drive processes in IdentityIQ  
Examples:
  - Searching
  - Assigning roles
- Standard Attributes
  - Support basic system functionality
  - Searchable by default
- Extended Attributes
  - Identity Attributes defined specifically for an installation
  - Add as many as required to support implementation needs
  - Searchable attributes can be specified
    - Limited by number of searchable extended attributes defined in DB

View Identity Adam.Kennedy		
Attributes	Entitlements	Application Account
User Name	Adam.Kennedy	
First Name	Adam	
Last Name	Kennedy	
Email	Adam.Kennedy@demoexample.com	
Manager	Douglas.Flores	
Department	Accounting	
Location	London	
Employee ID	1b2c3a4e	
Region	Europe	
Job Title	Payroll Analyst II	
Cost Center	R01e L03e	
Status	Employee	

# Standard Identity Attributes



# Configuring Identity Attributes

## Identity Mappings

The screenshot shows the 'Identity Attribute' configuration page. It includes sections for 'Attribute Name' (region), 'Display Name' (Region), 'Advanced Options' (Attribute Type: String, Edit Mode: Read Only, Searchable: checked, Multi-Valued: unchecked, Group Factory: checked, Value Change Rule: -- Select Rule --, Value Change Workflow: -- Select Business Process --), and 'Source Mappings' (List: 1. Region from the HR System - Employees application, 2. Region from the Contractor Feed application).

Field	Description
Attribute Name	Property name for the attribute
Display Name	Display value – can be a message key for localization support
Attribute Type	String or Identity
Edit Mode	Read only or editable attribute
Source Mappings	Source of Attribute: application account attribute or Rule

# Configuring Identity Attributes

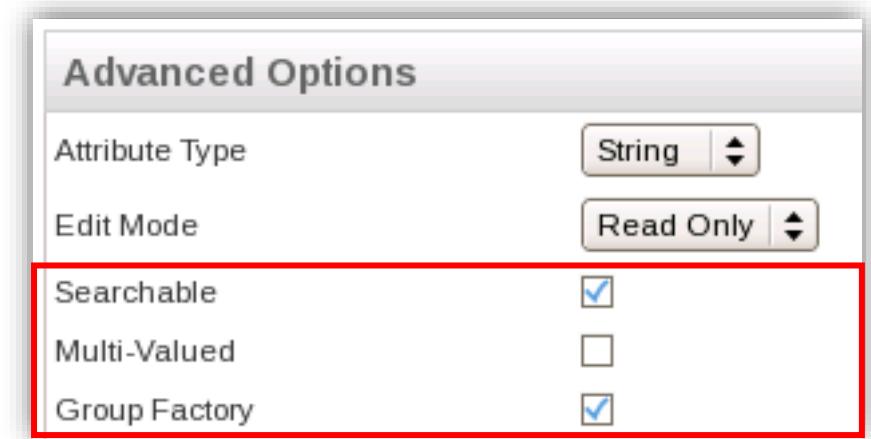
## Utilizing the Data

- Searchable
  - Correlation
  - Analytics, Reporting, etc.
- Multi-Valued

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

Example: Region attribute – *all users are grouped by their region*
  - Groups used to filter identities included in actions

Example: *Run report for identities with region: Europe*



# Configuring Identity Attributes

## Identity Datatype

- Supports one to many identity relationship
- Max 5 many-to-one extended attributes

### Edit Identity Attribute

Identity Attribute	
Attribute Name	manager
Display Name	Manager
Advanced Options	
Attribute Type	Identity

### View Identity Adam.Kennedy

Attributes	Entitlements	Application Accounts
User Name	Adam.Kennedy	
First Name	Adam	
Last Name	Kennedy	
Email	Adam.Kennedy@demoexample.com	
Manager	Douglas.Flores	

# Manager Correlation

## Definition

- Define which application attribute defines a user's manager
- Map the application attribute to the manager's Identity Attribute
- Application Definition or Rapid Setup

**Manager Correlation**

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

Application Attribute	Identity Attribute
managerId	Employee ID

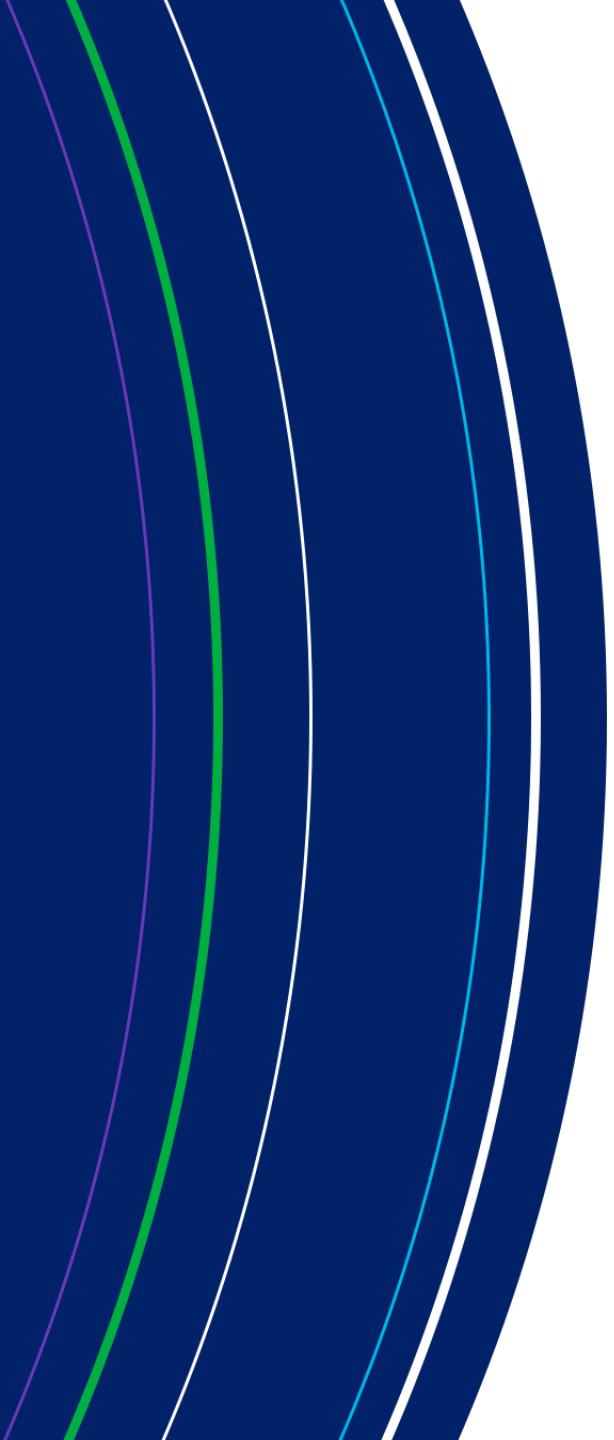
Applications → Application Definition

**Manager Correlation**

managerId	Equals	Employee ID
-----------	--------	-------------

Applications → Rapid Setup

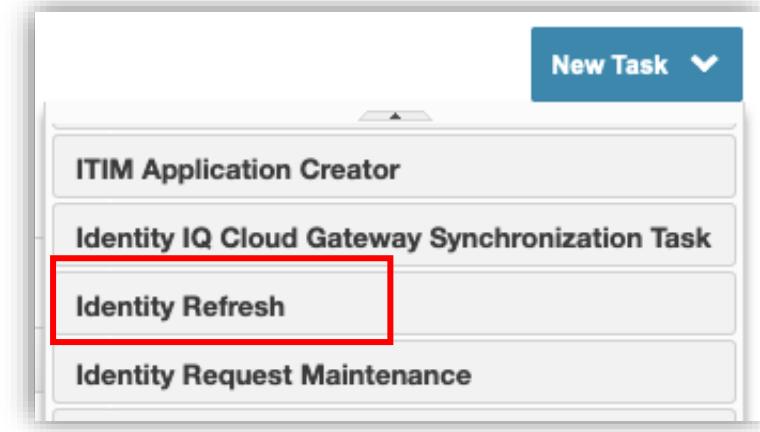
- Alternative: Manager Correlation Rule



# Identity Refresh Tasks

# Identity Refresh Tasks

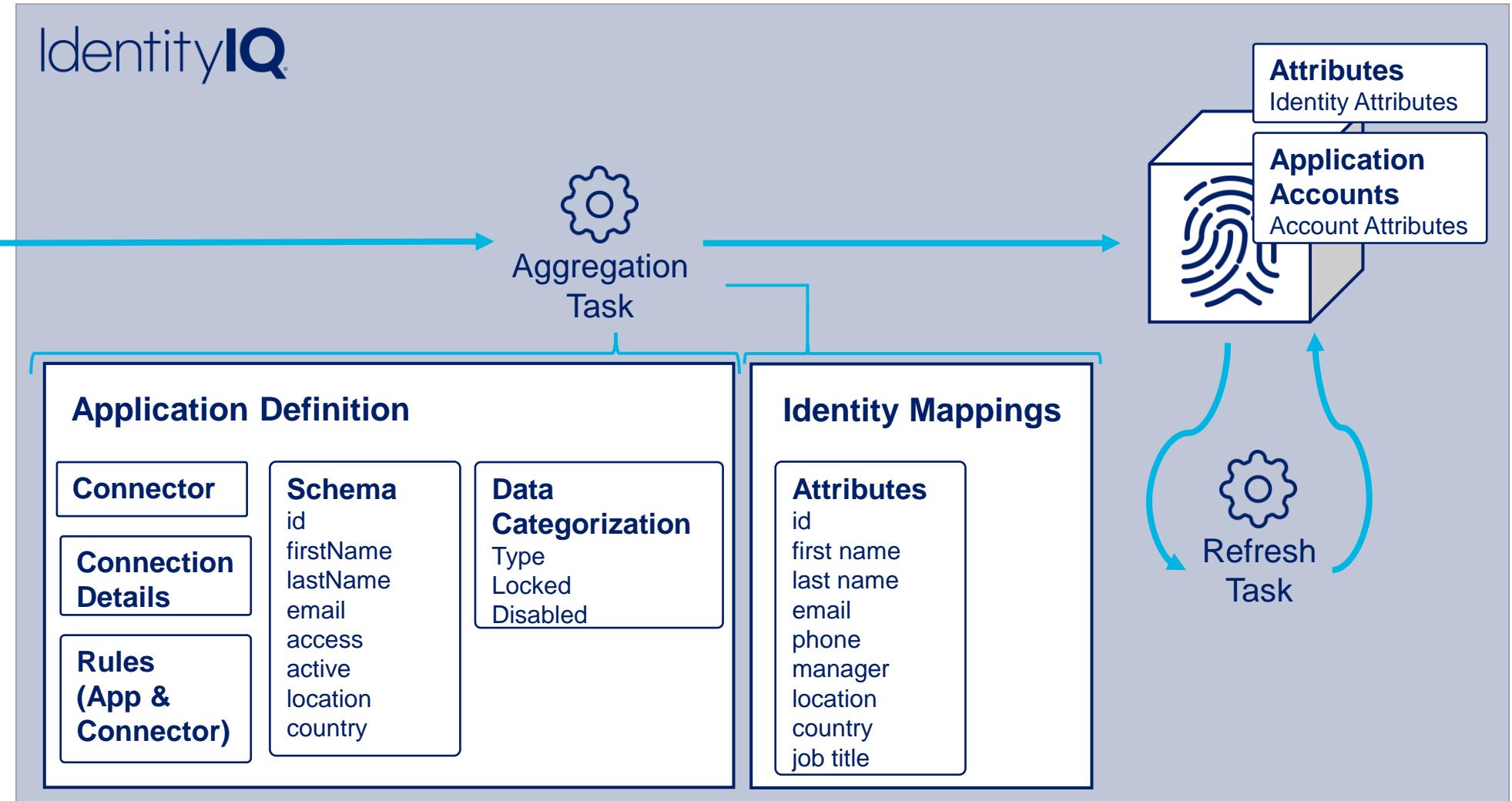
- Many configuration options
  - Mark manager status for each identity
  - Promote account attributes to identity attributes
  - Promote entitlements to a certifiable state
  - Update role assignments/detections
  - Process lifecycle events
  - Look for policy violations
  - And many more...
- Run against all identities (default)
  - Optional: filter by attributes, population, date



# Identity Attribute Population

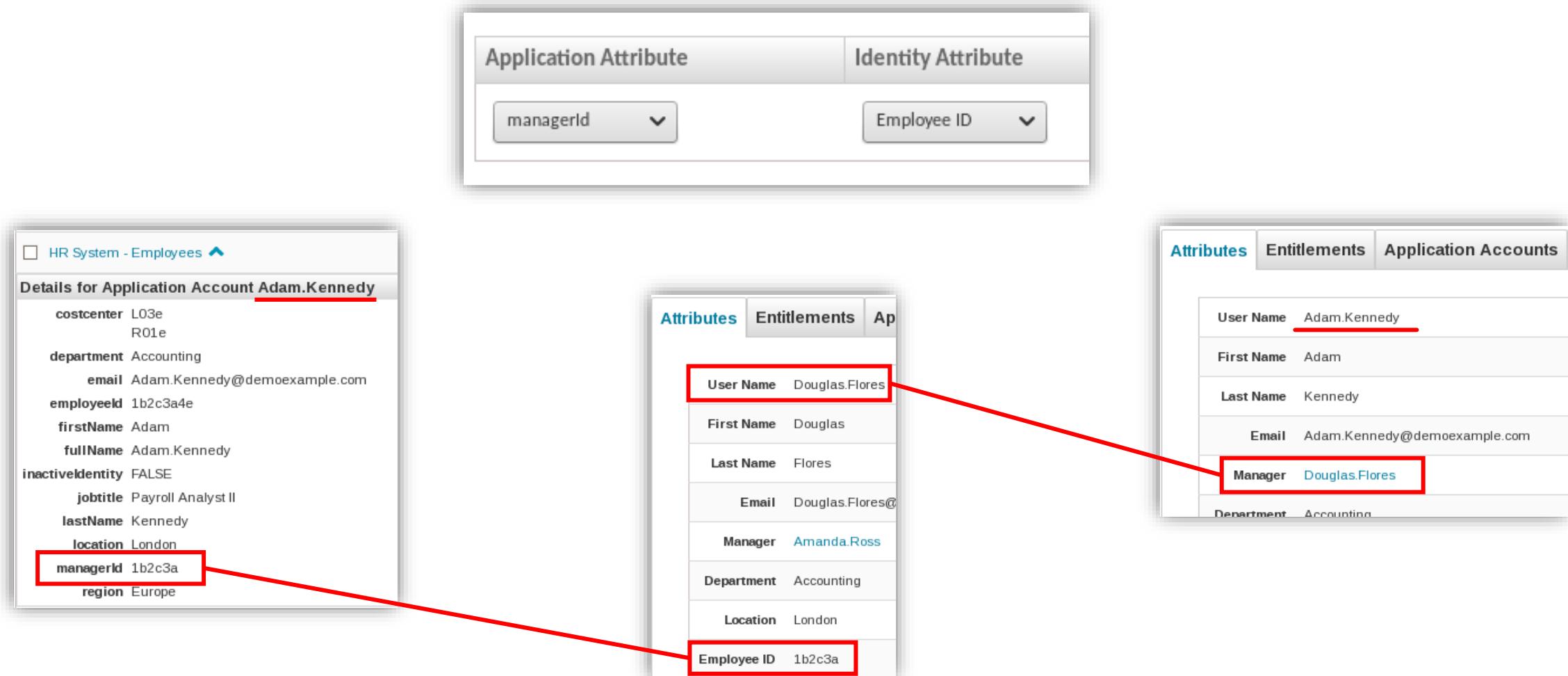


id	E001
firstName	Megan
lastName	Cahill
email	FieldOps
access	true
active	Austin
location	US
country	US
ssn	111-11-1111



# Manager Correlation

## Making the Connection



# Identity Refresh Tasks

Purpose: Update Identity Attributes and Perform Calculations

View Identity Adam.Kennedy

Attributes Entitlements Application Accounts Policy History Risk Activity User Rights

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

# Task Scheduling

---

## Aggregation and Refresh

- **Aggregation** schedule frequency depends upon
  - Use case
    - Compliance – prior to certification campaign (i.e. quarterly)
    - Provisioning – often daily
  - Importance of source application (i.e. authoritative, sensitive/risky)
- **Refresh** schedule frequency depends upon
  - Aggregation schedules
  - Data calculation needs
  - Best Practice: execute the various options as needed, in a just-in-time manner

# Knowledge Check

Next Step?

# Practice Exercises

# Exercise Preview

---

## Section 1, Exercise 3

- Exercise 3: Populate Identity Cubes
  - Define/populate identity attributes
  - Define account and manager correlation logic
  - Refresh identity cubes
  - Update UI to display new identity attributes
  - Investigate identity cubes





# Authentication and Authorization

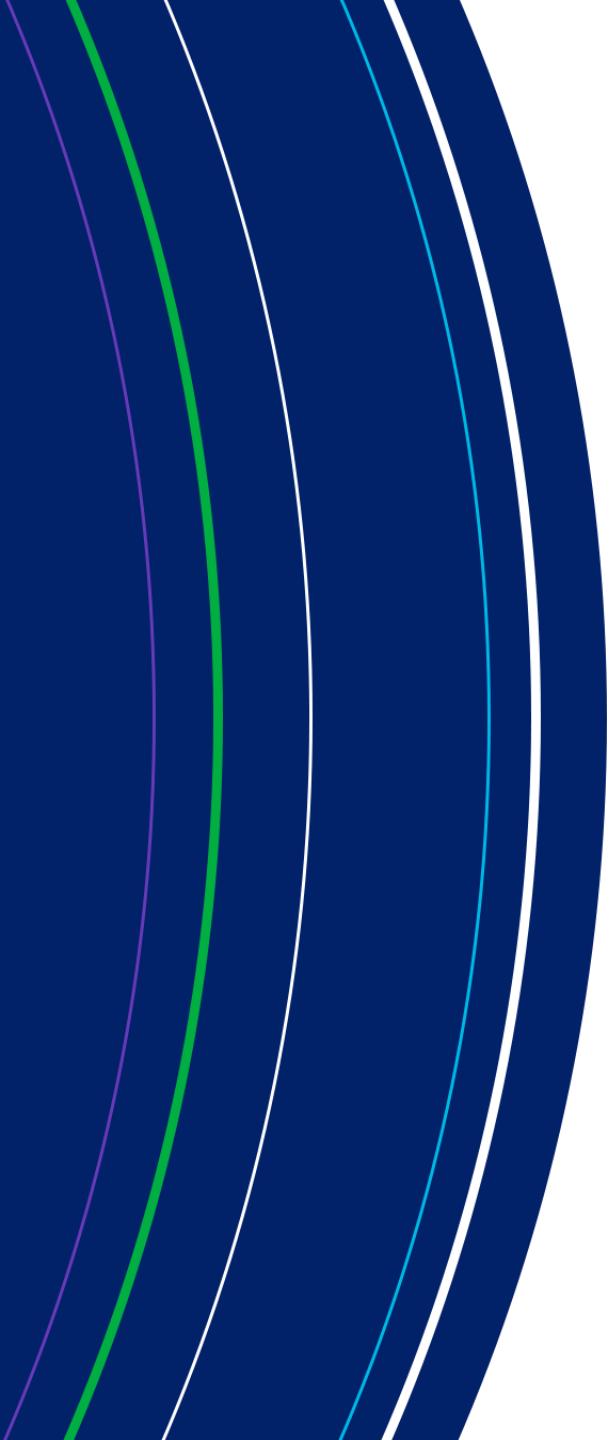
IdentityIQ Essentials

# Overview

---

## Authentication and Authorization

- Authentication Options
- Authorization Options
  - Capabilities
  - Scopes
  - Workgroups
  - Quicklink Populations



# Authentication Options

# IdentityIQ Authentication

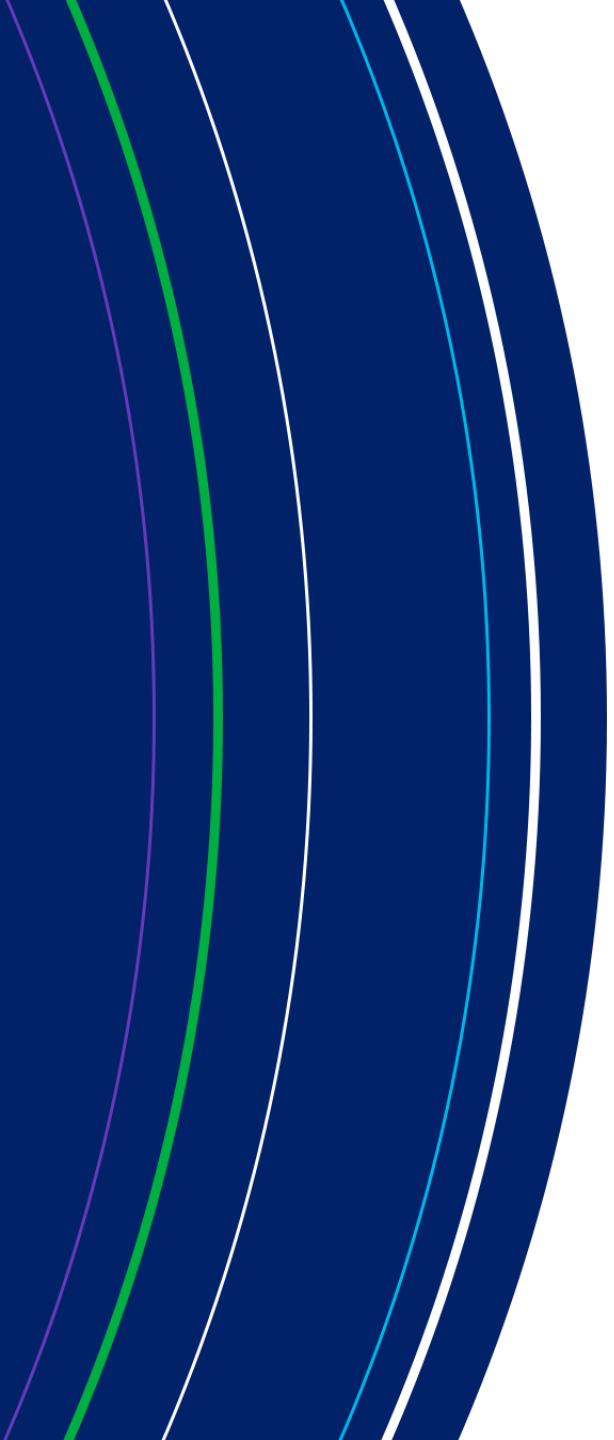
---

## Supported Options

- Native IdentityIQ authentication
- Pass through authentication
  - Active Directory
  - LDAP
- Single Sign On (SSO)
  - Rule-based (passed in header, and validated in rule)
  - SAML
- Multi-factor authentication (MFA)
  - RSA
  - DUO

See Compass:

*IdentityIQ Administration guide; IdentityIQ SAML Support guide; IdentityIQ Login Configuration whitepaper*



# **Capabilities and Scope**

# Access Rights for Identities

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

**View Identity Adam.Kennedy**

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

**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**

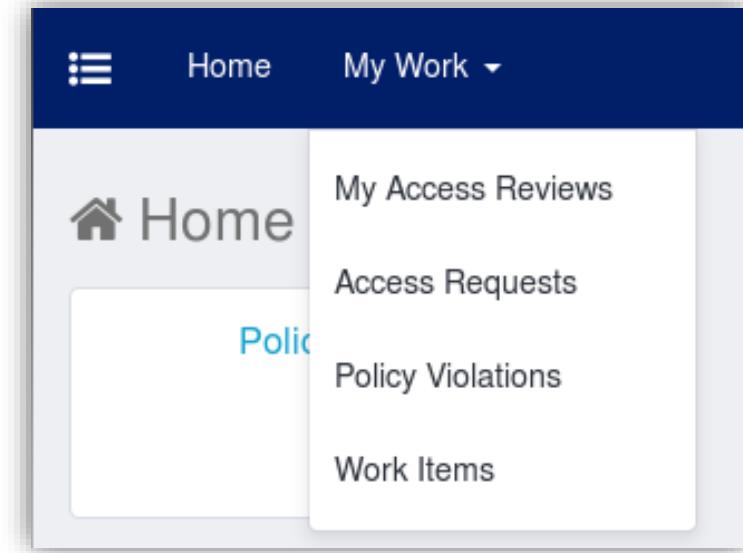
Use System Default (False)

**Authorized Scopes**

# Capabilities

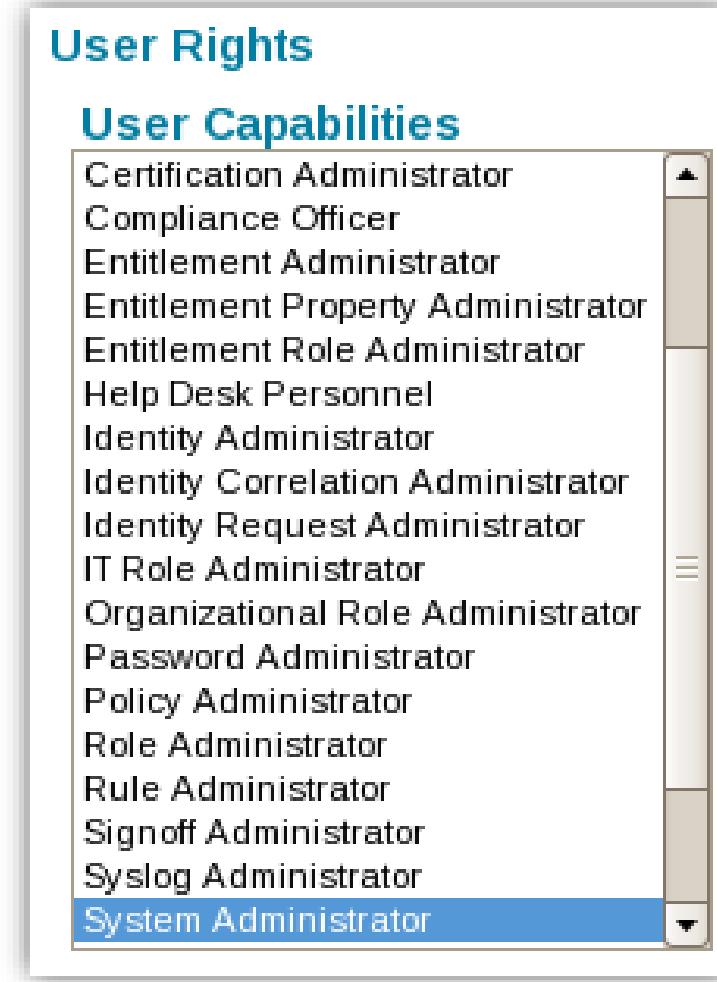
---

- Default user rights include
  - Home page
  - Quicklinks
  - My Work



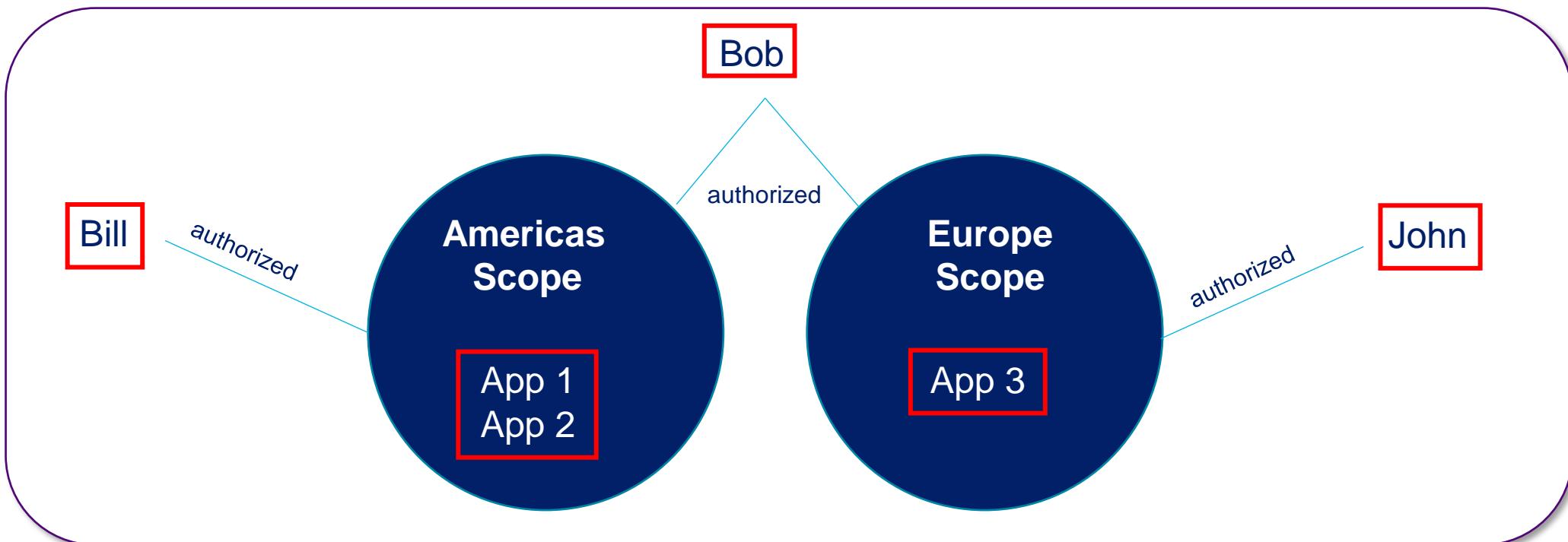
# Capabilities

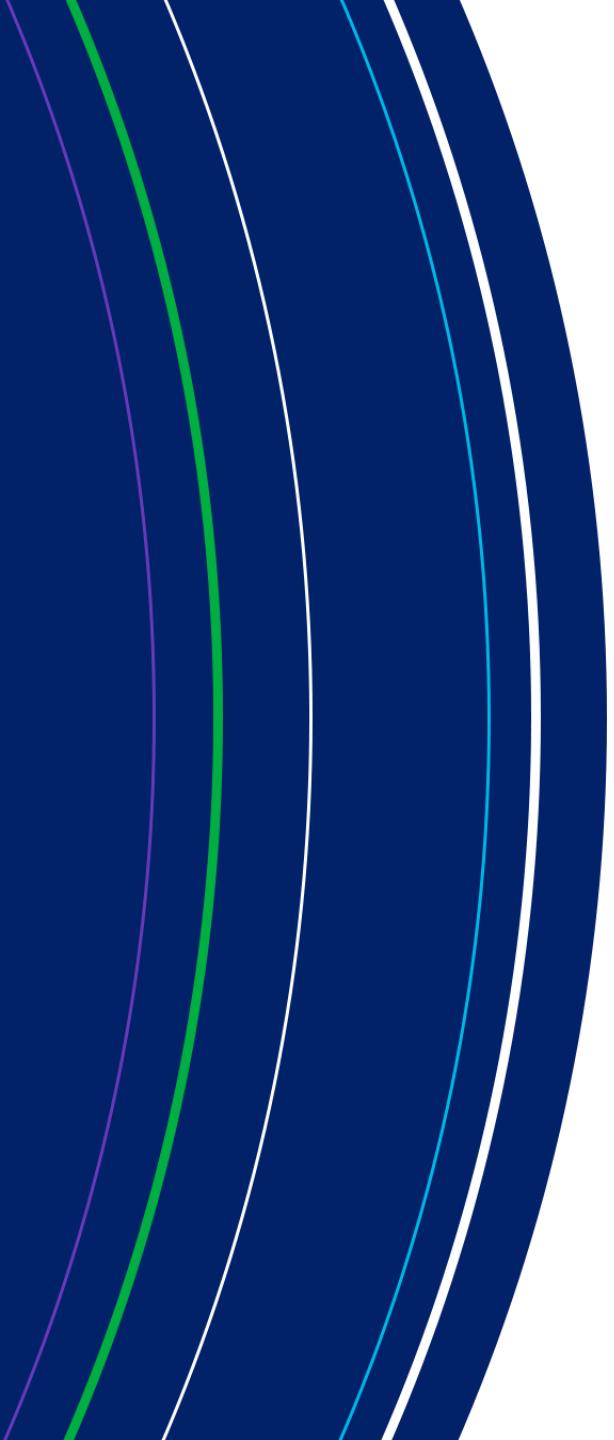
- Default User Rights include
  - Home page
  - Quicklinks
  - My Work
- Capabilities
  - Define what additional rights a user has within IdentityIQ
  - Control which menu options are available
- See Compass documents
  - *IdentityIQ Capabilities Matrix*
  - *IdentityIQ Rights and Capabilities - Definitions*



# 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

# Workgroups

## Definition

- Workgroup
  - Set of identities treated as a single IdentityIQ identity
- Example:
  - **Work Group:** Active Directory Application Owners
  - **Members:** John Smith, Sue Jones
- Workgroups are used for
  - Assigning access to IdentityIQ
    - Capabilities
    - Scopes
  - Sharing IdentityIQ responsibilities
    - Team-assigned work items
    - Object ownership (best practice)
      - Applications, Certifications, Roles, Entitlements, etc.

View Identity Adam.Kennedy

Attributes	Entitlements	Application
<b>User Rights</b>		
<b>User Capabilities</b>		
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		
<b>Workgroups</b>		
Name	De	
ERP Global App Owners	Owr	

# Knowledge Check





# Organizing Identities

IdentityIQ Essentials

# Overview

---

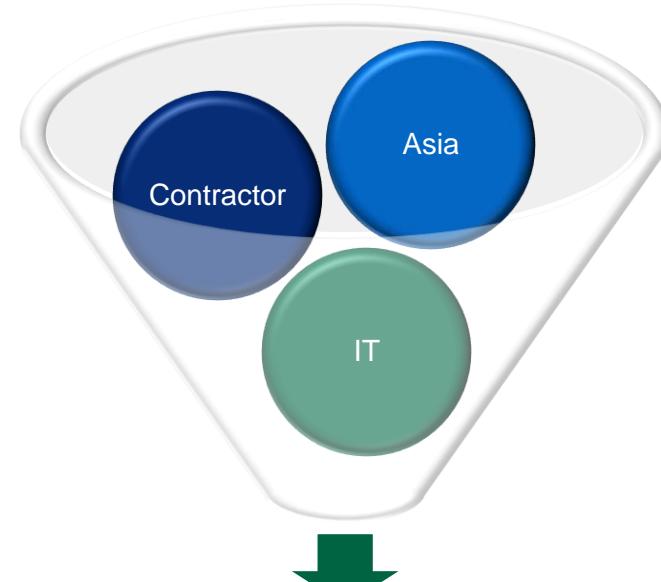
## Organizing Identities

- Populations
- Group Factories

# Populations

## Definition

- Definition
  - Identity search that defines a set of Identities that share a common set of attributes
- Purpose
  - Used as a filter on the set of Identities included in a task, certification, or report



# Creating Populations

- Populations can include multiple attributes in search criteria
- Saving a population saves the search parameters for reuse

The screenshot shows the SailPoint search interface. The 'Search Type' dropdown is set to 'Identity'. The 'Search Criteria' section is expanded, showing 'Identity Attributes' and 'Searchable Attributes'. Under 'Searchable Attributes', the 'Region' dropdown is set to 'Asia-Pacific'. The 'Is Manager' dropdown is set to 'True'. Other fields like 'Last Name', 'First Name', 'Username', etc., are also present. At the bottom are 'Run Search' and 'Clear Search' buttons.



Intelligence → Advanced Analytics

# Manage Populations

## View Populations

- List populations private to you
- List populations available to all users

**Group Configuration**

Name	Description	Visibility	Owner	Enabled
Active Managers - Asia-Pacific	Current managers located in the Asia-Pacific region.	Private	The Administrator	true
Europe Financials Accounts	All identities who are in the Europe region and who ha...	Private	The Administrator	true
Identities with Privileged Accounts		Public	The Administrator	true

Setup → Groups

# Manage Populations

## View/Edit Population

- Enable or disable populations
- Mark populations as public or private
- View the identities that make up the population

The screenshot shows the 'Edit Population' interface. At the top, it says 'Edit Population' and 'Population'. Below that is a 'Name' field containing 'Active Managers - Asia-Pacific' with a description 'Current managers located in the Asia-Pacific region.' Under 'Private' and 'Enabled', there are checked checkboxes. The 'Scope' field has a dropdown arrow. The 'Owner' field shows 'The Administrator'. Below this is a section titled 'Population Identity Count: 16' with a table of two rows. The table columns are 'User Name ▲', 'First Name', 'Last Name', 'Manager', and 'Last Refresh'. The first row is for Aaron.Nichols (Aaron, Nichols, Randy.Knight, 1/15/15 5:27 PM). The second row is for Andrea.Hudson (Andrea, Hudson, Randy.Knight, 1/15/15 5:28 PM).

User Name ▲	First Name	Last Name	Manager	Last Refresh
Aaron.Nichols	Aaron	Nichols	Randy.Knight	1/15/15 5:27 PM
Andrea.Hudson	Andrea	Hudson	Randy.Knight	1/15/15 5:28 PM

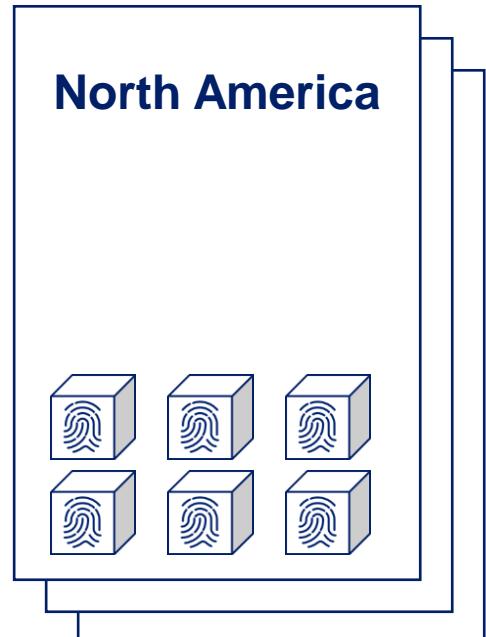
Setup → Groups

# Groups

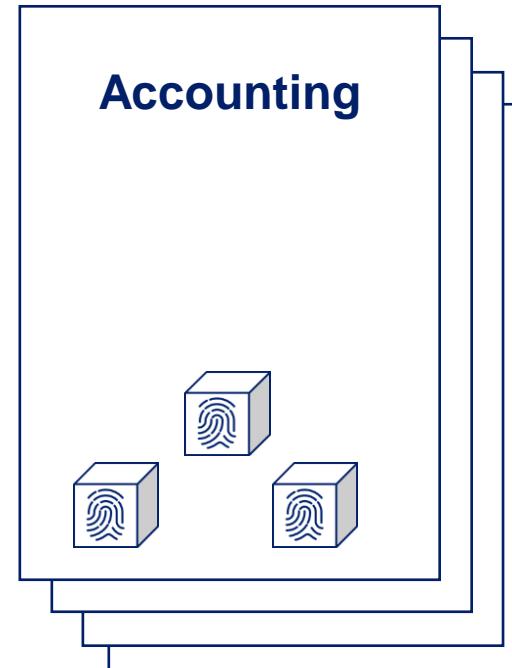
## Definition

- Sets of identities created automatically based on the values of a single identity attribute
- Used to filter identities included in a task, certification, or report

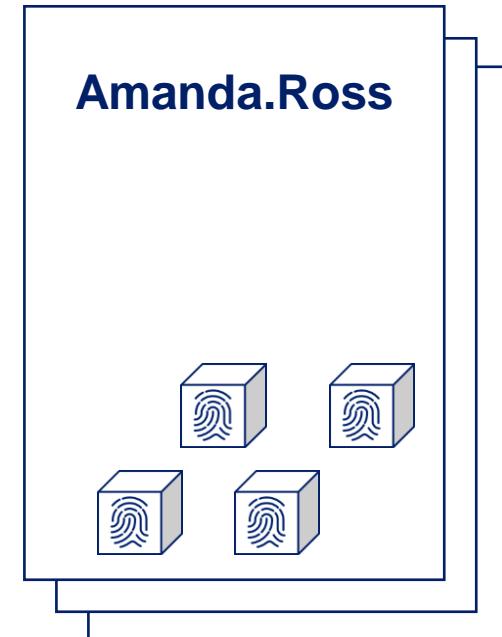
Location



Department



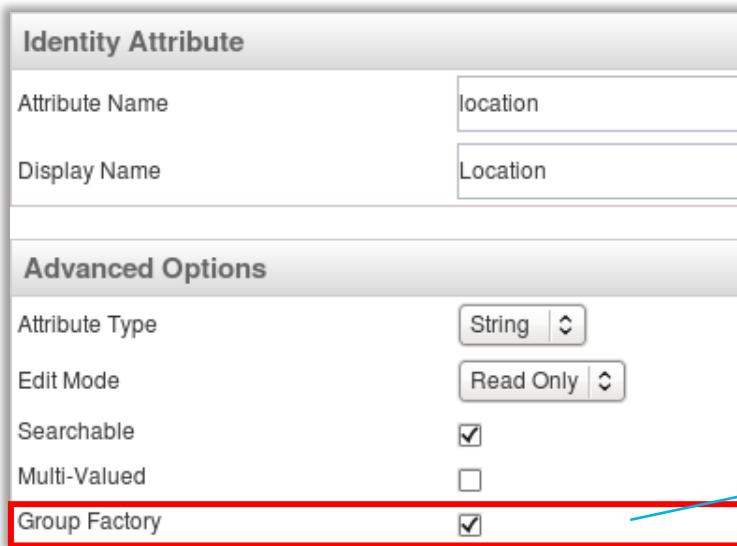
Manager



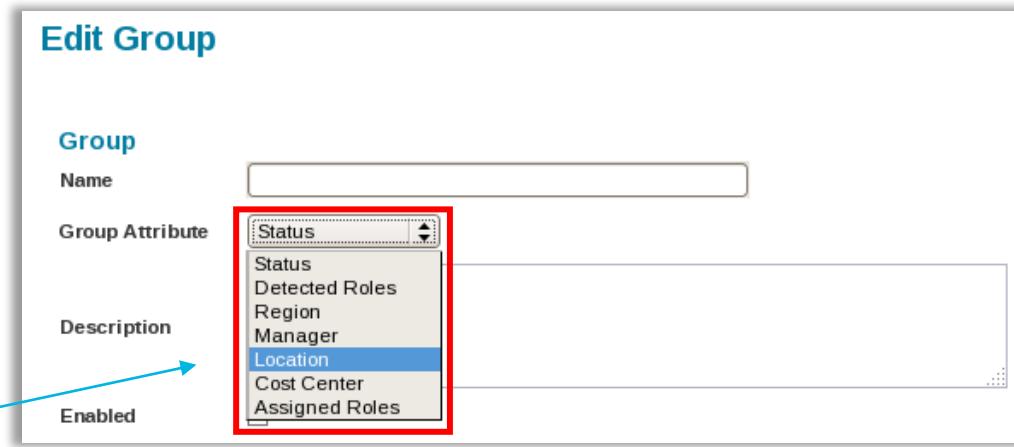
# Creating Groups

## Group Factory

- Identity attributes can be marked as a group factory
- All identity attributes marked as group factory are listed in the Group Attribute menu



The screenshot shows the 'Identity Attribute' configuration screen. It includes fields for 'Attribute Name' (location) and 'Display Name' (Location). Under 'Advanced Options', the 'Attribute Type' is set to 'String', 'Edit Mode' is 'Read Only', 'Searchable' is checked, and 'Multi-Valued' is unchecked. The 'Group Factory' checkbox is checked and highlighted with a red border. A blue arrow points from this checkbox to the 'Group Attribute' dropdown in the 'Edit Group' screen.



The screenshot shows the 'Edit Group' screen. It has fields for 'Name' and 'Group Attribute'. The 'Group Attribute' dropdown is open, showing a list of attributes: Status, Status, Detected Roles, Region, Manager, Location, Cost Center, and Assigned Roles. The 'Location' option is highlighted with a blue selection bar. Below the dropdown, the word 'Enabled' is visible.

Global Settings → Identity Mappings

Setup → Groups → Create New Group

- The term *group factory* can also refer to the collection of sub-groups that share an attribute

# Creating Groups

- Define the group details

The screenshot shows the 'Edit Group' dialog box. The 'Name' field contains 'Location'. The 'Description' field contains 'Group used to group users by Location'. The 'Enabled' checkbox is checked. The 'Scope' dropdown is open. The 'Group Owner Rule' dropdown is set to 'Group Owner - Highest Ranking Member of Sub-Group'. A blue callout box labeled 'Identity Attribute' points to the 'Name' field. Another blue callout box labeled 'Status' points to the 'Enabled' checkbox. A third blue callout box labeled 'Optional owner for each sub-group' points to the 'Group Owner Rule' dropdown.

**Edit Group**

**Group**

Name: Location

Group Attribute: Location

Description: Group used to group users by Location

Enabled:

Scope:

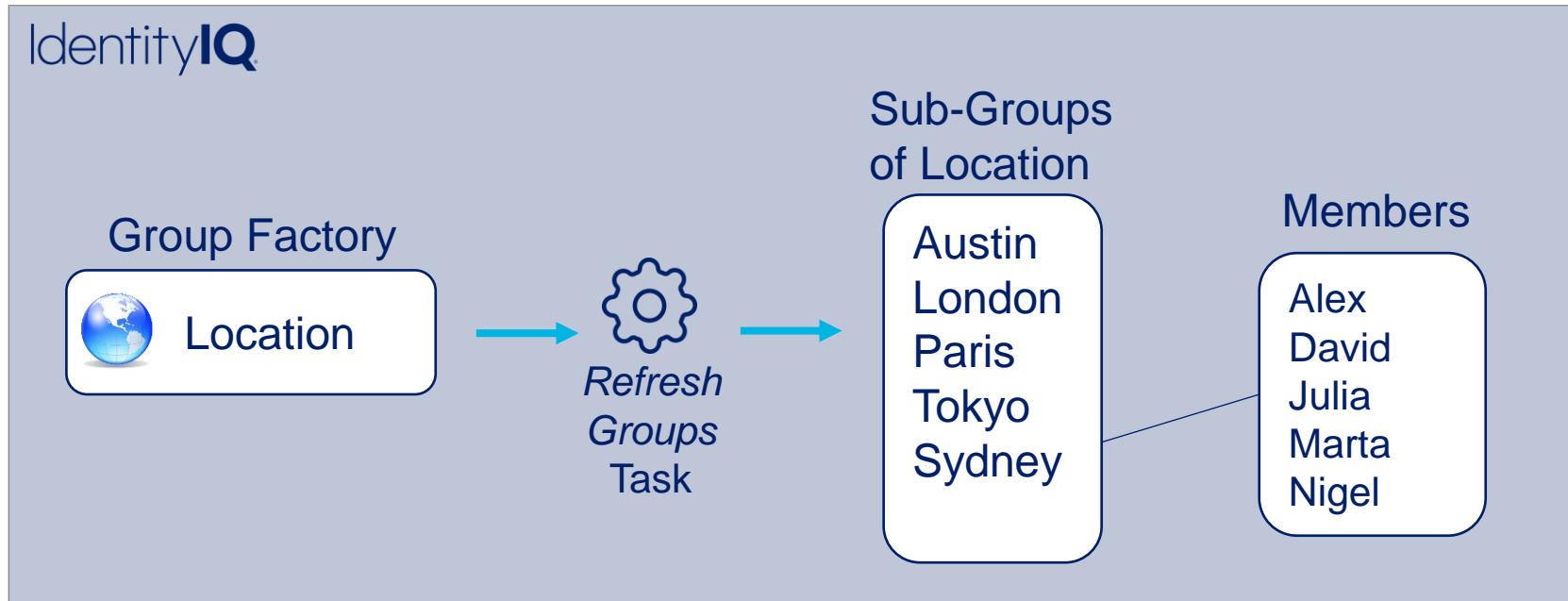
Group Owner Rule: Group Owner - Highest Ranking Member of Sub-Group

Save Cancel

Setup → Groups → Create New Group

# Creating Groups

- Run task: *Refresh Groups*
  - Creates a sub-group for every value for the specified group attribute
    - For example
      - Group Factory: Location
      - Values found for Location = sub-groups created with members
        - Austin, London, Paris, Tokyo, Sydney



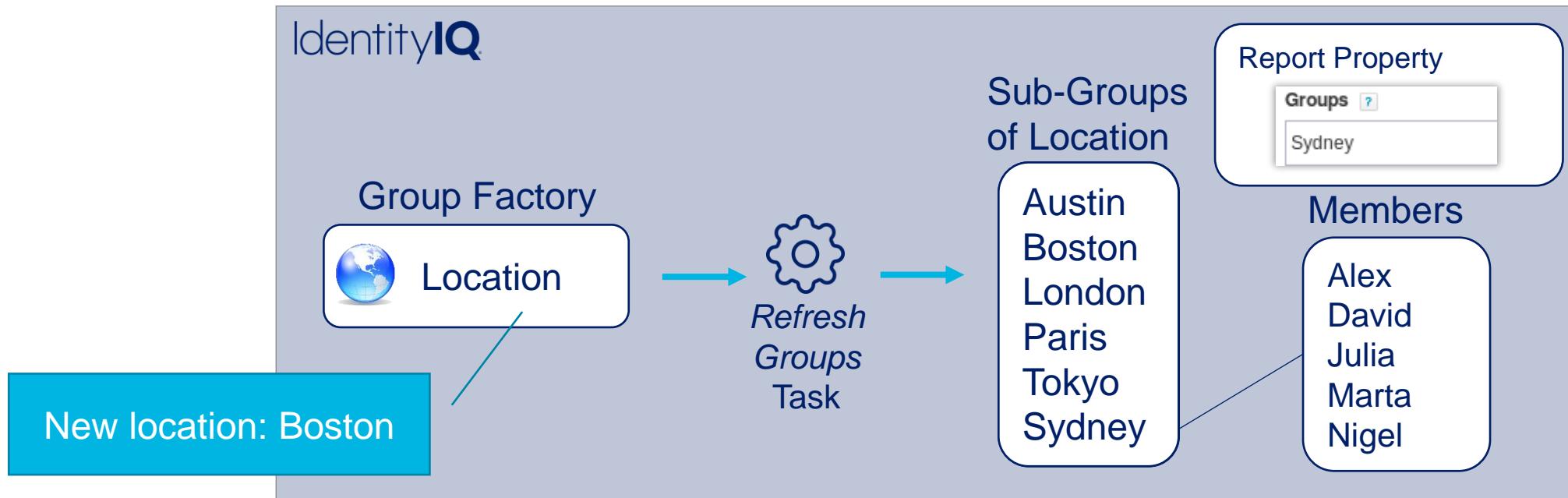
# Manage Groups

## Group Definitions

- List of sub-groups is static
  - Update list with *Refresh Groups* task
    - Run regularly

## Group Membership

- Members are identified when group is used
  - All identities who match group attribute at that point in time are included



# Manage Groups

## View Group

### Edit Group

**Group**

Name: Location

Group Attribute: Location

Description: Group used to group users by Location

Enabled:

Scope:

Group Owner Rule: Group Owner - Highest Ranking Member of Sub-Group

**Sub-Groups**

Name	Member Count	Policy Violations	Composite Score	Owner	Last Updated
Austin	27	2	335	James.Smith	7/20/14 11:34 AM
Brazil	25	2	342	John.Williams	7/20/14 11:34 AM
Brussels	26	1	347	Jerry.Bennett	7/20/14 11:34 AM
London	25	0	500	Amanda.Ross	7/20/14 11:34 AM

Setup → Groups

# Contrasting Populations and Groups

---

Populations

Groups

Commonality: Both store only membership criteria and execute query dynamically at time of use

# Knowledge Check

# Practice Exercises

# Exercise Preview

---

## Section 1, Exercise 4

- Exercise 4: Organize Identities
  - Create populations
  - Create group factories
  - Create and populate workgroups





# Onboarding Additional Applications

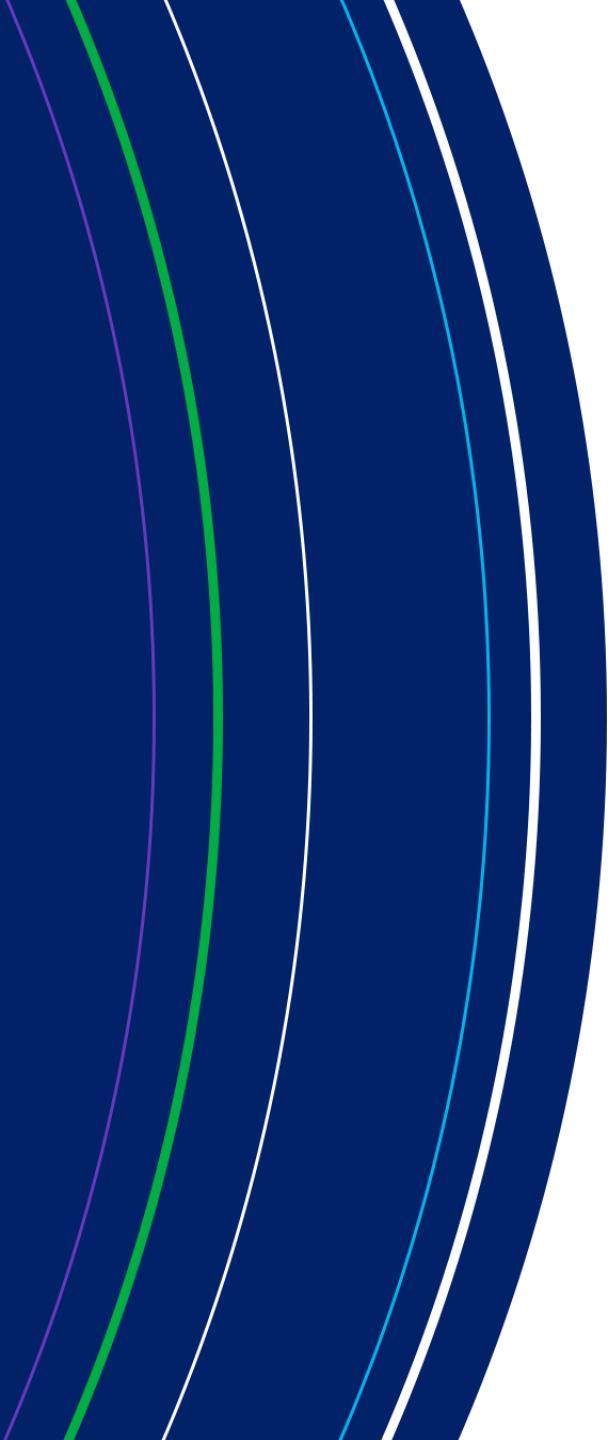
IdentityIQ Essentials

# Overview

---

## Onboarding Additional Applications

- Application and connector planning resources
- Defining non-authoritative applications



# **Planning Resources for Onboarding**

# Planning

---

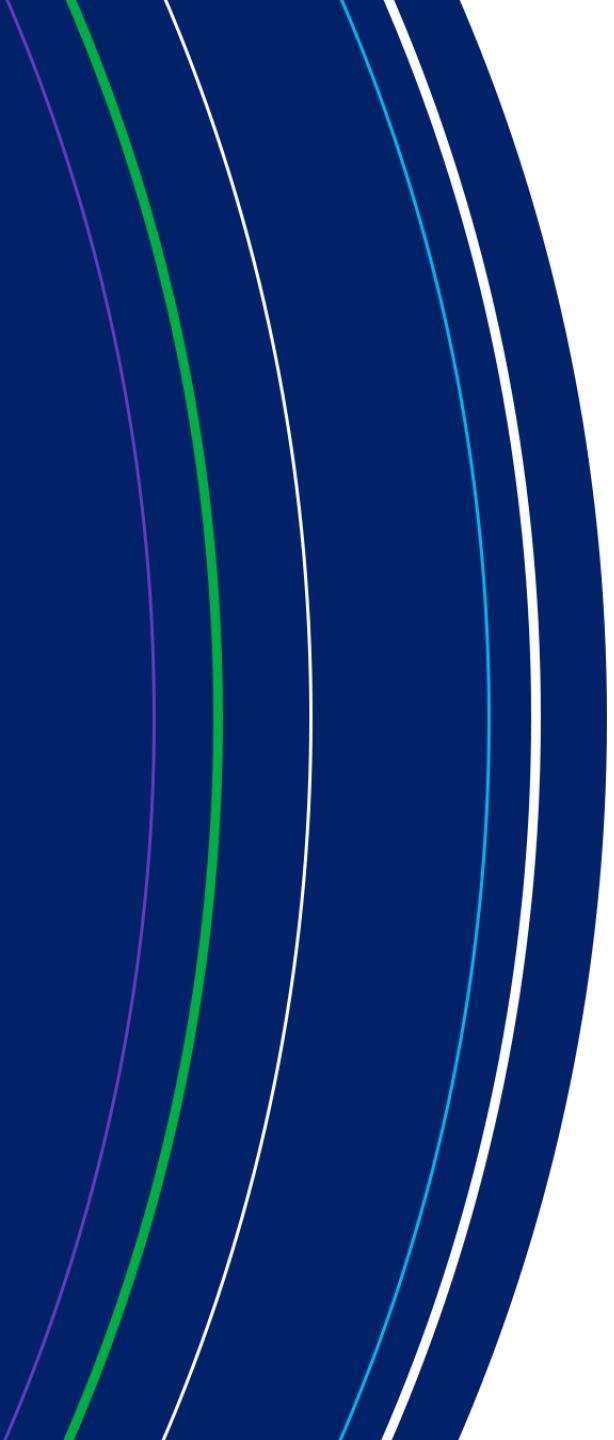
## Prioritizing, Defining, and Connecting

- Applications
  - Prioritize and group in phases
  - Define connectivity
- Accounts
  - Represent users who may sign into that system
- Attributes
  - Additional information associated with account
- Entitlements
  - Specify what actions a user is authorized to perform in a given application (i.e. access payroll)
- Account Groups
  - Specify set of security rights/permissions (i.e. Administrator)
  - Membership in group provides user with group's access rights

# Planning Resources

---

- Product Documentation
  - Installation
  - Administration
  - Direct Connectors Admin and Config Guide
- Services Standard Words (SSW)
  - IdentityIQ Job Titles & Staffing Plan
  - IdentityIQ Pre-Deployment Questionnaire
  - Application Onboarding Questionnaire
  - Go Live Migration Roll Back Plan
  - [https://community.sailpoint.com/t5/Services-Standard-Deployment/tkb-p/SSD\\_KB](https://community.sailpoint.com/t5/Services-Standard-Deployment/tkb-p/SSD_KB)



# **Defining Non-Authoritative Applications**

# Defining Non-Authoritative Applications

---

## Key Configurations

- Account schema and entitlements
- Group schemas
- Classification
- Correlation
- Provisioning (especially birthright)

# Account Schema

## Review

- Specify account attributes to read during aggregation
- Identify key data to IdentityIQ
  - Identity Attribute
  - Display Attribute

Settings   Schema   Provisioning Policies

Object Type: account

Details

Native Object Type	inetOrgPerson	Display Attribute	cn
Identity Attribute	dn	Instance Attribute	
		Remediation Modifiable	Readonly

Attributes

Name	Description
<input type="checkbox"/> businessCategory	business category
<input type="checkbox"/> carLicense	vehicle license or registration plate
<input type="checkbox"/> cn	common name(s) for which the entity is known by
<input type="checkbox"/> departmentNumber	identifies a department within an organization
<input type="checkbox"/> description	descriptive information
<input type="checkbox"/> destinationIndicator	destination indicator
<input type="checkbox"/> displayName	preferred name to be used when displaying entries
<input type="checkbox"/> dn	distinguished name for which the entity is known by
<input type="checkbox"/> employeeNumber	numerically identifies an employee within an organization
<input type="checkbox"/> employeeType	type of employment for a person

Copyright © SailPoint Technologies Holdings, Inc. 2020. All rights reserved.

# Account Schema

## Entitlement Designations

- Identify attribute that lists user entitlements
- **Entitlement → Identity Cube**
  - Include in certifications
  - Include in role mining
- **Managed → Entitlement Catalog**
  - Assign ownership, display name, description
  - Request through LCM
  - Use in policy and risk calculations

Attributes				
	Name	Description	Type	Properties
<input type="checkbox"/>	login		string	<a href="#">Edit</a>
<input type="checkbox"/>	description		string	<a href="#">Edit</a>
<input type="checkbox"/>	first		string	<a href="#">Edit</a>
<input type="checkbox"/>	last		string	<a href="#">Edit</a>
<input type="checkbox"/>	groups		group	<a href="#">Edit</a> Managed, Entitlement, Multi-Valued
<input type="checkbox"/>	status		string	<a href="#">Edit</a>

# Entitlement Catalog / Identity Cube

The diagram illustrates the integration between three components:

- Entitlement Catalog:** A table showing entitlements for the TRAKK application. A red box highlights the last four rows (reject, input, approve) under the "Type" column.
- Identity Cube:** A table showing identity attributes. A red box highlights the "Managed Entitlement Multi-Valued" row under the "Properties" column.
- View Identity Adam.Kennedy:** A detailed view of the identity for user Adam.Kennedy. It shows roles, entitlements, and application accounts. A red box highlights the "capability" entitlement entry in the Entitlements section.

**Entitlement Catalog Data (Red Boxed Rows):**

Application	Attribute	Display Name	Type
TRAKK	capability	super	Entitlement
TRAKK	capability	reject	Entitlement
TRAKK	capability	input	Entitlement
TRAKK	capability	approve	Entitlement
PRISM	groups	User	Group

**Identity Cube Properties Data (Red Boxed Row):**

Name	Description	Type	Properties
id		string	
username		string	
firstname		string	
lastname		string	
email		string	
capability		string	Managed Entitlement Multi-Valued

**View Identity Adam.Kennedy Data (Red Boxed Row):**

Entitlements	
Filter by attribute	Entitlement
capability	input
groupmbr	PayrollAnalysis
memberOf	Domain Users ⓘ
memberOf	Domain Admins ⓘ

# Group Schema

- Represent native account groups from target system
- Groups managed in Entitlement Catalog
- Provides framework for defining what group membership really means
  - Descriptions: Group 920-100 = industry compliance regulatory group
  - Indirect permissions: Group Financials = access to the financial planning file share
- Some connectors support multiple
  - JDBC, SQL Loader, Delimited File, Oracle EBS, etc.

Entitlement Catalog				
Application ▾	Attribute	Display Name	Type	Description
TRAKK	capability	super	Entitlement	
TRAKK	capability	reject	Entitlement	
TRAKK	capability	input	Entitlement	
TRAKK	capability	approve	Entitlement	
LDAP	groups	Users	group	All users at the company
LDAP	groups	Managers	group	All managers at the company

# Group Object Reference

## Account Schema

- Identifies the attribute that holds groups for the account holder
- Used to identify group membership (groups, groupmbr, memberOf)
- Available after Group Object has been defined

## Account Schema

Attributes				
Name	Description	Type	Properties	
<input type="checkbox"/> login		string		<a href="#">Edit</a>
<input type="checkbox"/> description		string		<a href="#">Edit</a>
<input type="checkbox"/> first		string		<a href="#">Edit</a>
<input type="checkbox"/> last		string		<a href="#">Edit</a>
<input type="checkbox"/> groups		group	Managed, Entitlement, Multi-Valued	<a href="#">Edit</a>
<input type="checkbox"/> status		string		<a href="#">Edit</a>

Group Schema	
<b>Object Type:</b>	group
<b>Details</b>	
<b>Native Object Type</b>	group
<b>Identity Attribute</b>	name
<b>Attributes</b>	
<b>Name</b>	
<input type="checkbox"/> name	
<input type="checkbox"/> description	

# Entitlement Requestability

## Rapid Setup Configuration

- Infrastructure Applications
  - High volumes of entitlements, most unknown to users
  - Examples: Active Directory, LDAP, Mainframe, Unix, Database servers
  - Best Practice: Entitlements *not* requestable
- Business Applications
  - Systems supporting business functions
  - Examples
    - HR applications: payroll, benefits, time tracking
    - Commerce applications: finance, accounting
    - Industry-specific business applications
  - Best Practice: Entitlements requestable

### Aggregation

Provide classification and categorization details for this application aggregation

Create Entitlements That Cannot Be Requested 



# Data Classification

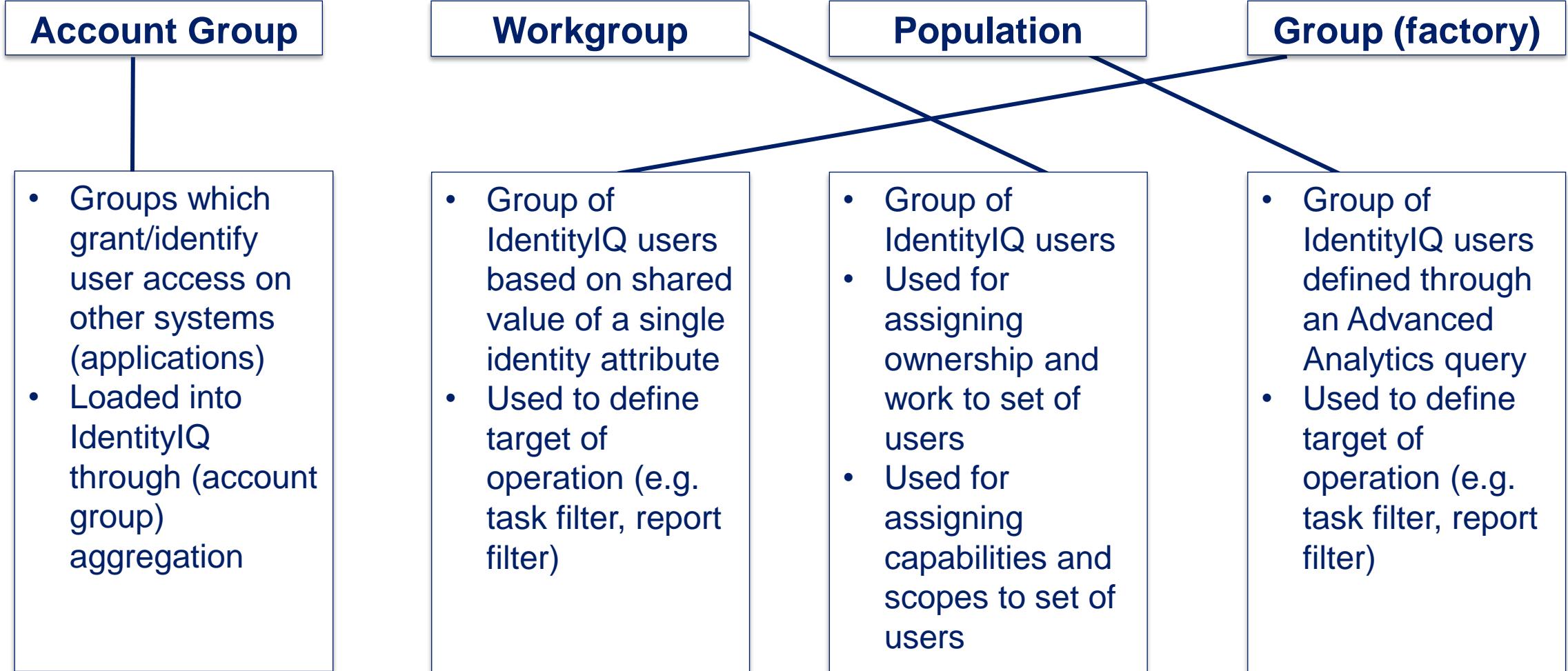
## Rapid Setup Configurations

- Accounts
  - Locked Account
  - Disabled Account
- Identities
  - Service
  - RPA/Bot

The screenshot shows the SailPoint interface for account classification. At the top, there's a 'Disable Account' configuration with a dropdown for 'Status' set to 'Locked' and an 'Equals' operator with the value 'D'. Below it is a 'Service Account' configuration with a note: 'This will change the identity type of the identity to which this account correlates'. It includes fields for 'User Name' (with an 'Starts With' dropdown containing 'SERV') and a 'Locked' checkbox. A 'Lock Account' section is partially visible behind it. At the bottom is an 'RPA Account' configuration with a similar note and an 'Add Filter' button.

# Knowledge Check

# Groups, groups, everywhere...







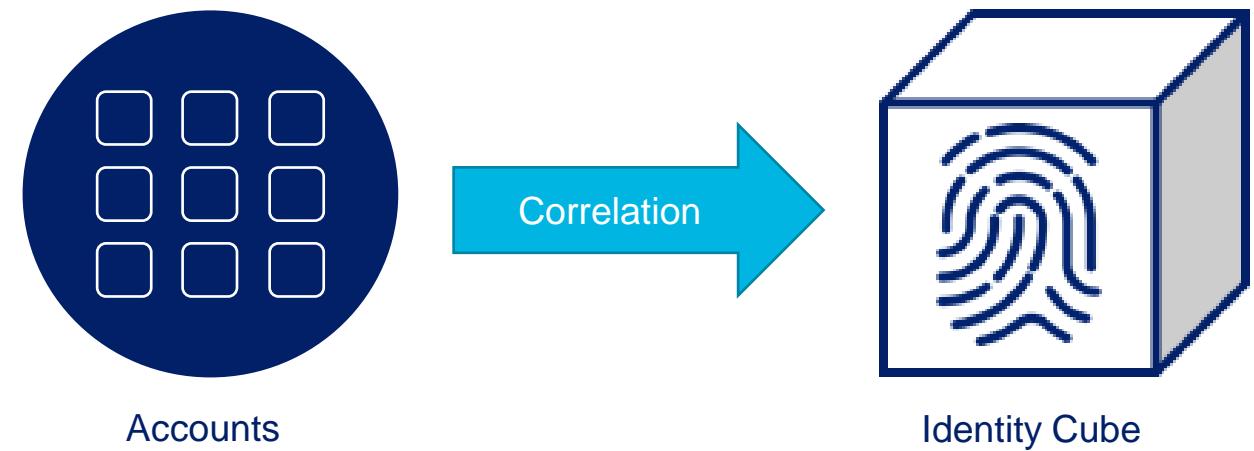
# Account Correlation

IdentityIQ Essentials

# Account Correlation

---

- Matches an account to an authoritative Identity Cube
  - If no correlation, non-authoritative cube is created
- Correlation specification
  - Rapid Setup correlation
  - Correlation Wizard
  - Correlation rule
- Fallback options
  - Default logic
  - Manual
- Order of precedence
  1. Rule
  2. Correlation configuration
  3. Default logic



# Account Correlation

## Rapid Setup

- Provides a simple, easy to configure UI
- Matches one application attribute with one identity attribute
- Allows responsibilities for correlation to be shared

Account Correlation ?

*Changes made here will be reflected for all applications which share this configuration.*

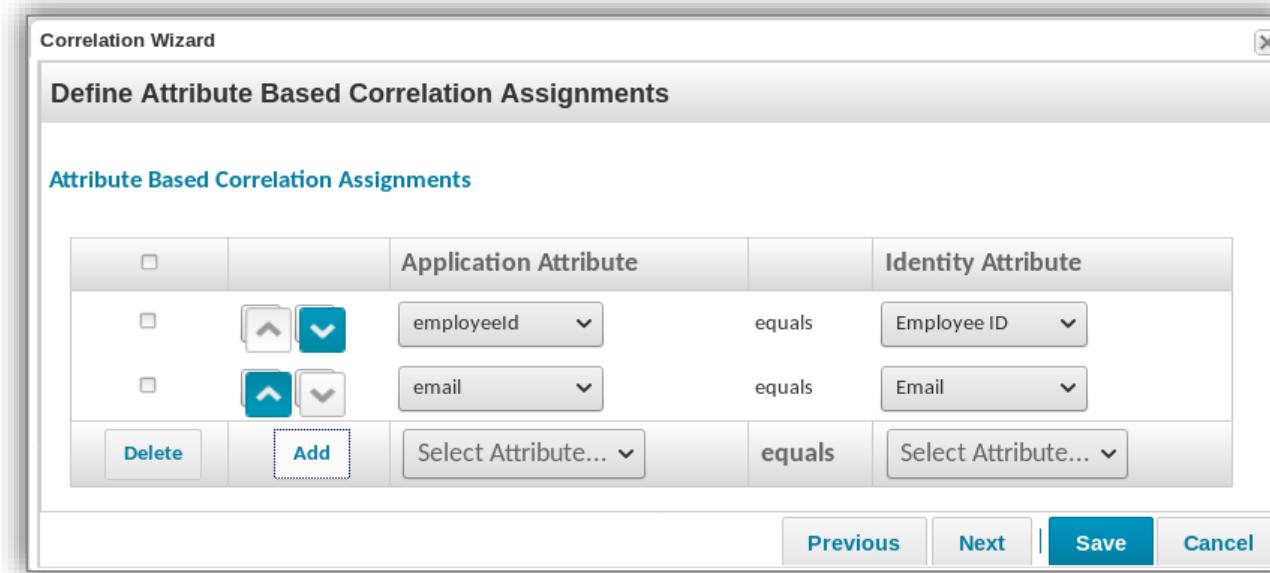
employeeId	Equals	Employee ID
------------	--------	-------------

Applications → Rapid Setup

# Account Correlation

## Correlation Wizard

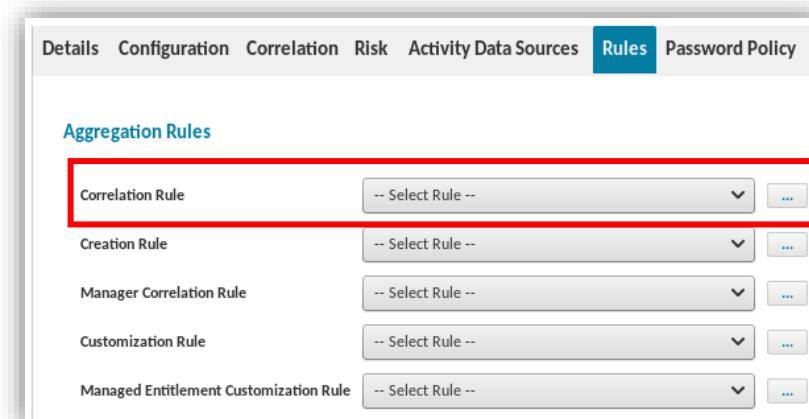
- Provides a set of ordered correlations
- Result is a reusable correlation configuration
- Attribute example – correlate *account attribute email* with *identity attribute Email*
- Condition example – correlate accounts where **serviceAcct = true**



# Account Correlation

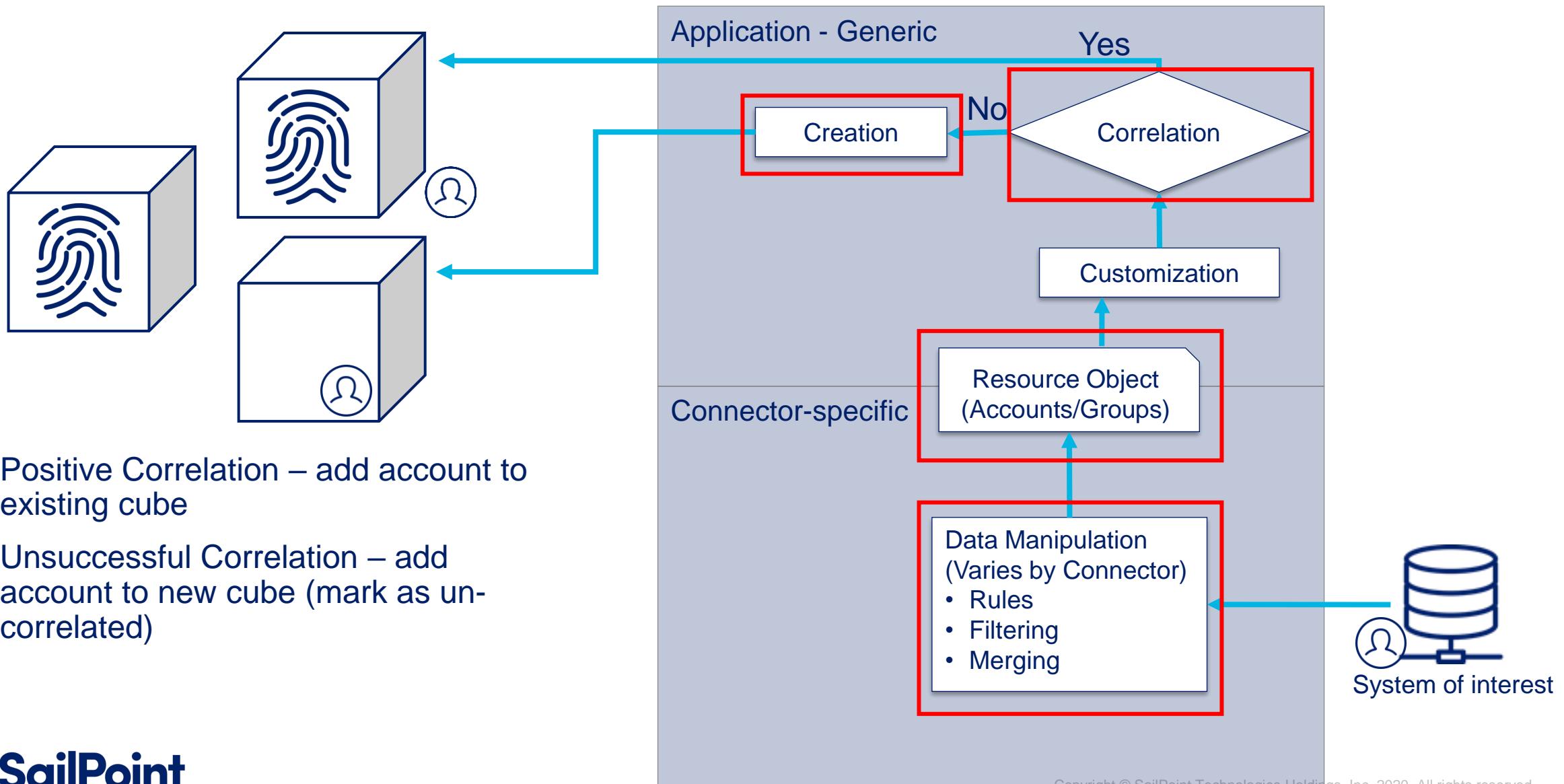
## Correlation Rule

- Used when simple matching isn't enough
- Build and maintain account correlations
- Rule runs for every account, every aggregation



Applications → Application Definition → Rules

# Application/Connector Processing



# Uncorrelated Accounts

## Manual Correlation

- Manually assign accounts to identities
- Correlation permanently retained

List by application

Select identity

Perform merge

Identity Correlation

Use the following tables to manually correlate one or more accounts with an identity. To begin, enter an application name to retrieve the list of all uncorrelated accounts for the given application. Note that some columns in the tables can be edited.

Select Uncorrelated Accounts

Time Tracking	Account ID	Account Name	Create Date	Locked Account	Disabled Account	Privileged Account Type	Privileged Account
Time Tracking	<input type="checkbox"/> ADMIN1	Howard.Rose.Admin	10/11/2019 04:16:48 pm				true

Select Target Identity

Name	First Name	Last Name	Correlated	Manager	Email	Inactive	Last Refresh	Type	
howard	<input type="checkbox"/> Eric.Howard	Eric	Howard	<input checked="" type="checkbox"/>	Maria.White	Eric.Howard@demoexample.com	false	11/11/2019 11:52:23 am	Contractor
howard	<input checked="" type="checkbox"/> Howard.Rose	Howard	Rose	<input checked="" type="checkbox"/>	Jane.Grant	Howard.Rose@demoexample.com	false	11/11/2019 11:52:09 am	Employee
howard	<input type="checkbox"/> Howard.Rose.Admin			<input type="checkbox"/>			false	11/11/2019 11:52:20 am	

Perform Merge

Identities → Identity Correlation

# Incorrect Account Correlation

## Move Account

View Identity Alice.Ford

Attributes Entitlements Application Accounts Policy History Risk Activity User Rights Events

Application Accounts

Application	Account Name
Chat	Alice.Ford
HR Employees	Alice.Ford
LDAP	Alice.Ford
Time Tracking	Alice.Ford

**Move Account** (button highlighted with a red box)

Select Account Owner

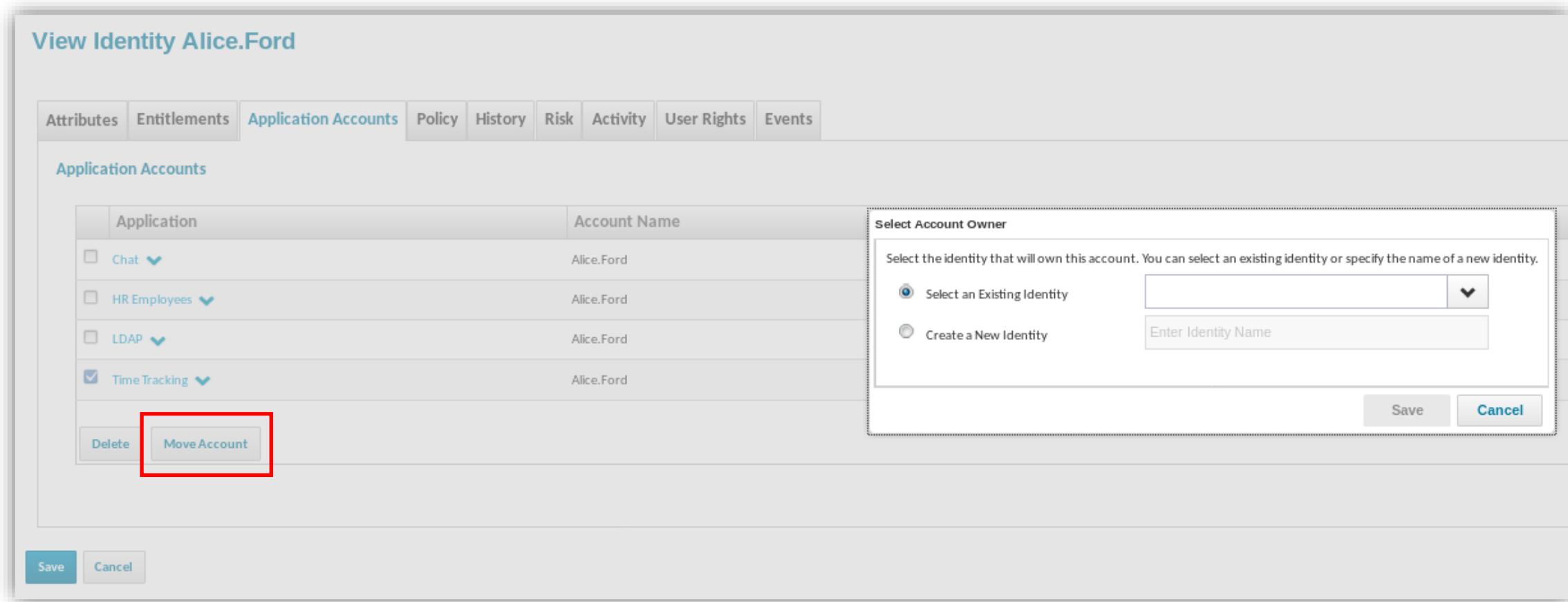
Select the identity that will own this account. You can select an existing identity or specify the name of a new identity.

Select an Existing Identity

Create a New Identity  Enter Identity Name

Save Cancel

Save Cancel



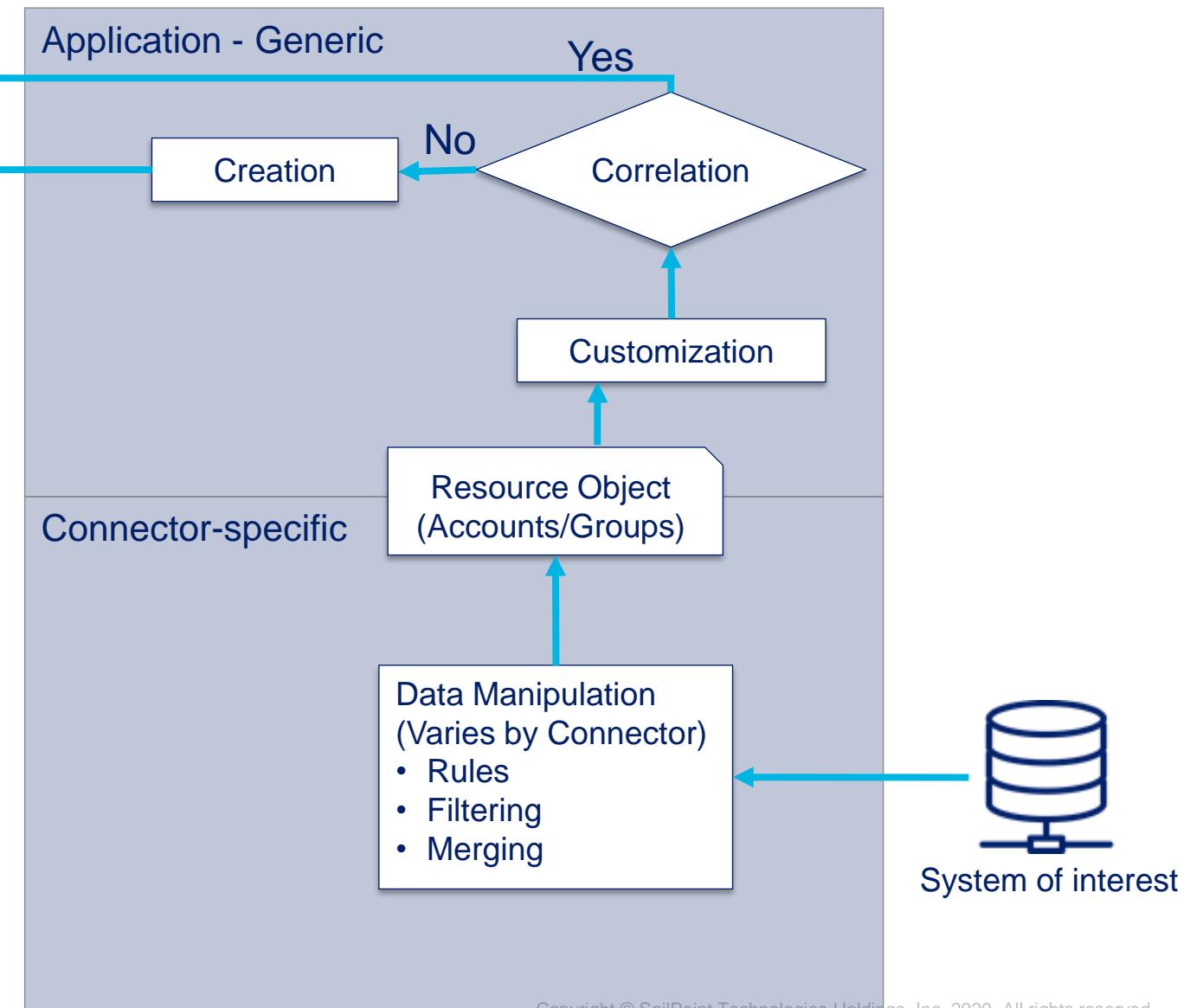
Identity Cube → Application Accounts

# Application/Connector Processing

## Clean Up

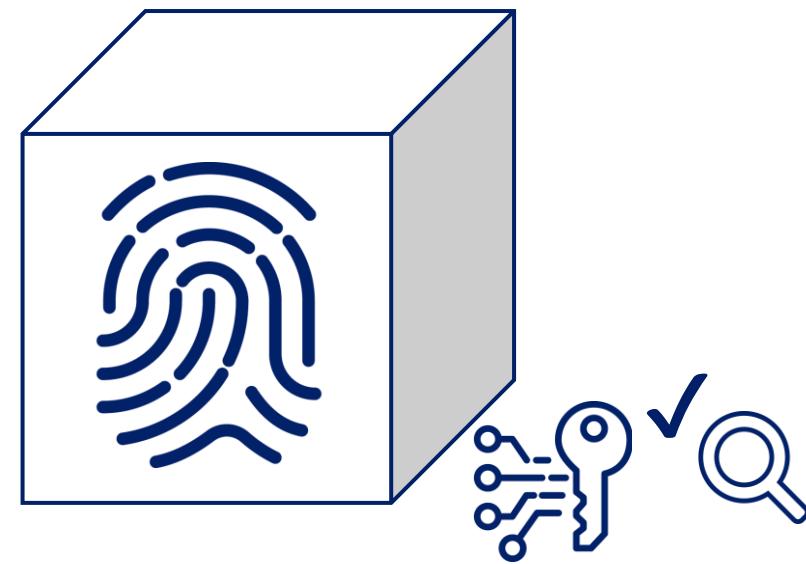


- Resolve Unsuccessful Correlation
  - Fix correlation logic and/or manually correlate
  - Run **Prune Identities** Task



# Identity Refresh Task

- Promote entitlements to a certifiable state



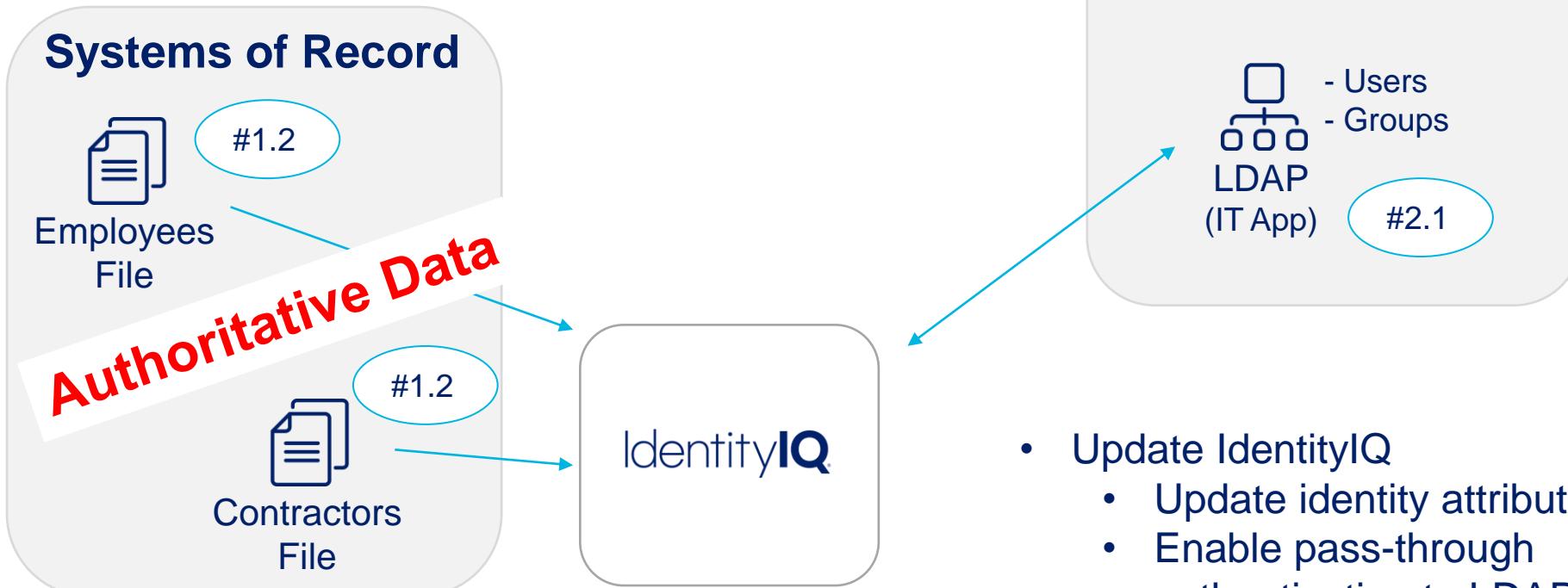
# Knowledge Check

Next Step?

# Practice Exercises

# Exercise Preview

## Section 1, Exercises 5 & 6, Extension Exercise 7



- Update IdentityIQ
  - Update identity attribute email
  - Enable pass-through authentication to LDAP
  - Configure password reset





# IdentityIQ Connectors

IdentityIQ Essentials

# Overview

---

## IdentityIQ Connectors

- Connector Basics
- Connector Details
  - Common Connectors

# Application vs. Connector

- Connector
  - Software component to connect to a business resource and read/write data
  - Provides normalized resource object
- Application
  - Includes configuration details
    - Application name
    - Connector configuration
    - Account attributes
  - Represents a business resource
    - Examples:
      - Human Resource System
      - Active Directory

The screenshot shows a user interface for managing application definitions. At the top, there is a navigation bar with links for Home, My Work, Identities, Applications, and Intelligence. Below the navigation bar is a section titled "Application Definition". This section includes a search bar labeled "Filter by Application Name" with a magnifying glass icon, and a blue button labeled "Add New Application". A table lists eight configured applications with columns for Name, Host, and Type.

Name	Host	Type
Contractor Feed	localhost	DelimitedFile
Financials	localhost	DelimitedFile
HR System - Employees	localhost	DelimitedFile
LDAP	training.sailpoint.com	OpenLDAP - Direct
PAM	localhost	DelimitedFile
PRISM	localhost	JDBC
TRAKK	localhost	JDBC

# Connectors

- Provide for reading data from applications including:
  - Files
  - Databases
  - Directories
  - Mainframes
  - Communication and collaboration tools
  - UNIX
  - ...and more!
- Most provide for writing data to applications

**Edit Application**

**Details**

\*Indicates a required field.

**Name**

**Owner**

**Application Type**

Select One ...  
ACF2 - Full  
ADAM - Direct  
AIX - Direct  
AWS IAM  
Active Directory - Direct  
Airwatch MIM  
Azure Active Directory  
BMC ITSM - Direct  
BMC Remedy - Direct  
Box  
Cloud Gateway  
CyberArk  
DB2 Windows - Direct  
DelimitedFile  
Dropbox  
Duo  
GoToMeeting  
Good Technology MIM  
Google Apps - Direct

# Connector Configuration

---

## Consistent Across Connectors

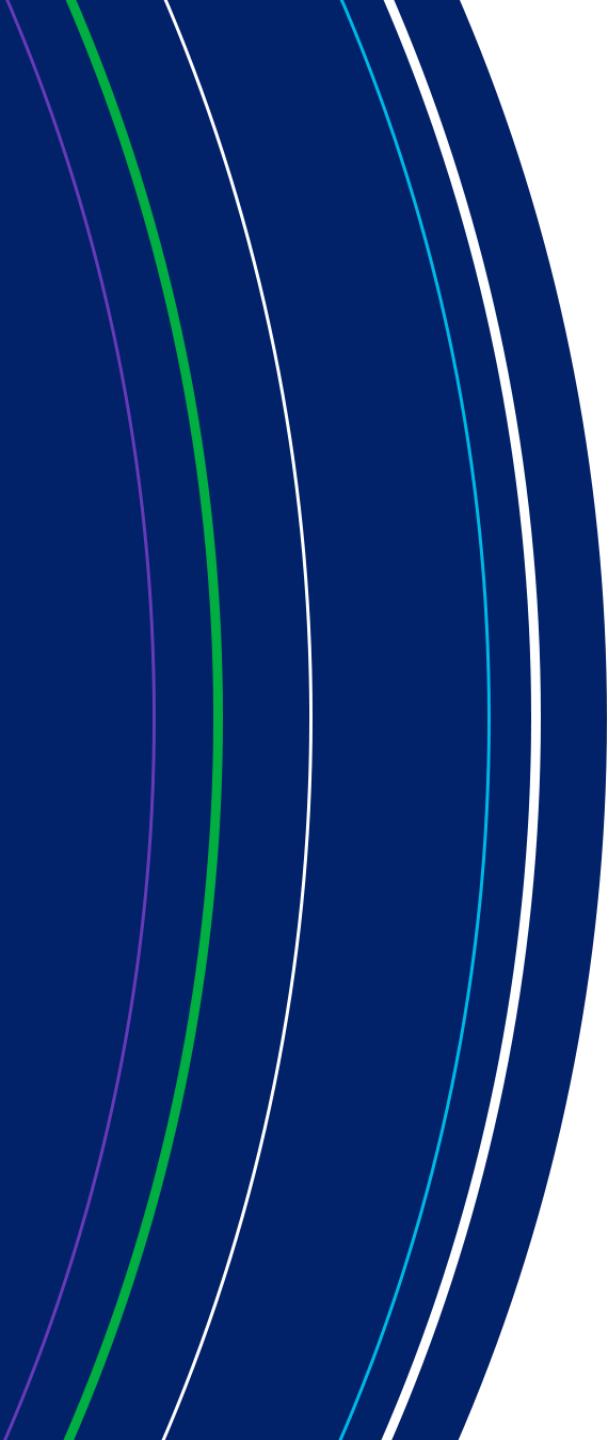
- Account and Group schema
- Resource Object representation
- Application-level rules

## Varies per Connector

- Group schema – one vs. multiple
- Connectivity details
- Connector-specific rules

For more information on connectors, see Compass

- Connector guides (per connector)
- Services deployment documentation



# Common Connectors



# Delimited File

## Usage

- Aggregate (read) accounts and entitlements from a delimited file

## Configuration Details

- Required
  - File name and location
  - Schema
- Optional
  - Filtering
  - Merging
  - Connector-level rules



## Usage

- Aggregate (read) and provision\* (write) to JDBC-enabled databases

## Configuration Details

- Required
  - Database connection details
  - SQL Queries
  - Schema
  - \* JDBC Provisioning Rule
- Optional
  - Merging
  - Connector-level rules

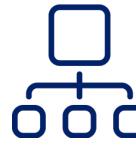


## Usage

- Aggregate and provision to LDAP server
  - Several connectors to connect to a variety of LDAP systems, without customization

## Configuration Details

- Required
  - LDAP connection credentials
  - Search DNs
  - Schema (provided)
- Optional
  - Filtering
  - Multiple groups



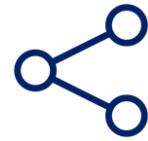
# Active Directory

## Usage

- Aggregate and provision\* to Active Directory

## Configuration Details

- Required
  - Active Directory connection credentials
  - Search DNs
  - Schema (provided)
  - \*IQService
- Optional
  - Filtering
  - Multiple domains or forests



# Web Services

---

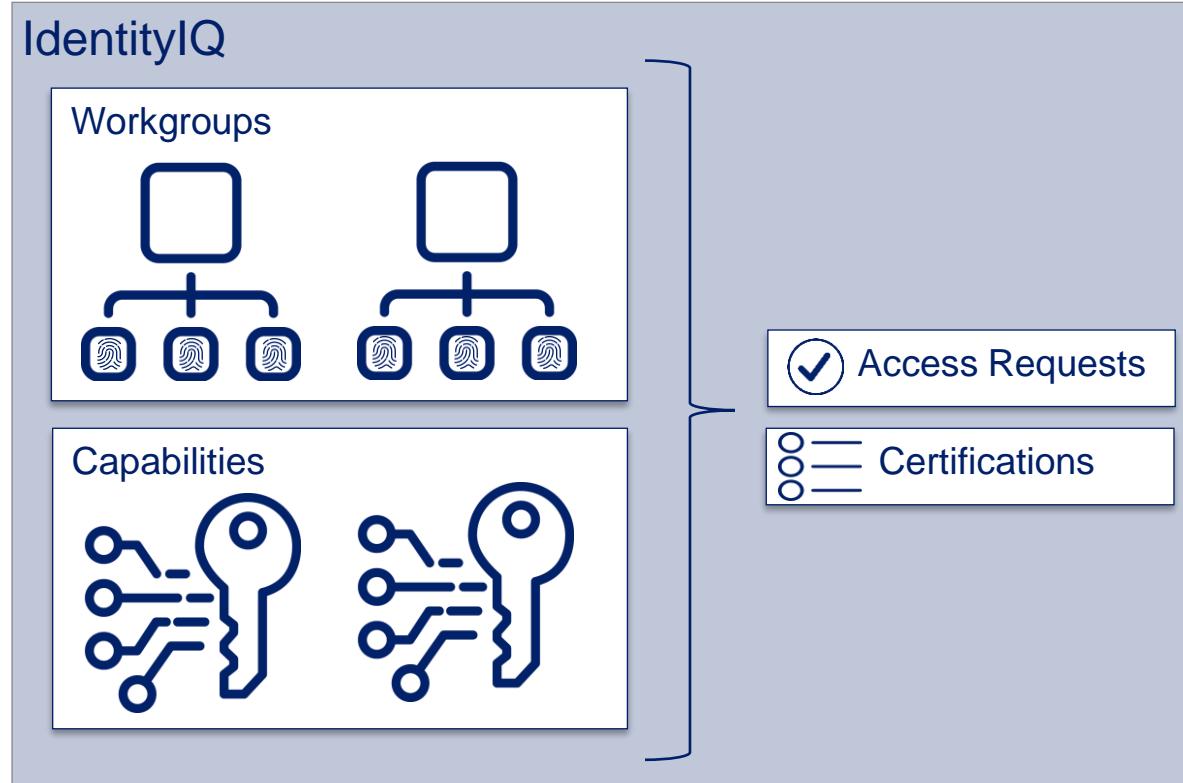
## Usage

- Aggregate and provision to target system using their supported web services

## Configuration Details

- Required
  - URL and connection credentials for target system
- Optional
  - Supported operations (create account, enable/disable account, pass-through authentication, etc.)

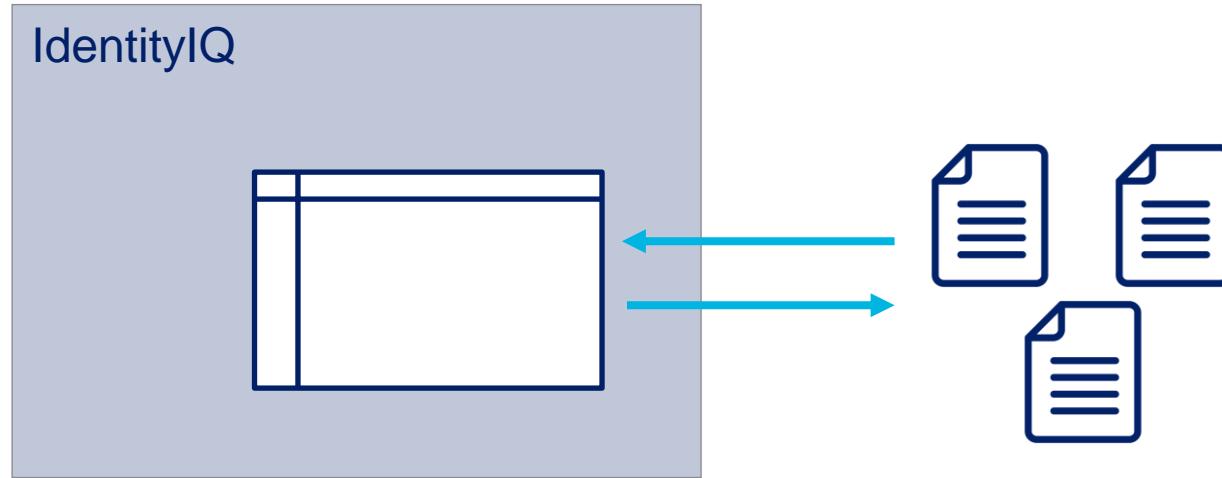
# IdentityIQ Loopback Connector



- Treats Identity Cubes as Accounts
- Treats IdentityIQ Workgroups and Capabilities as Entitlements

# SQL Loader

---



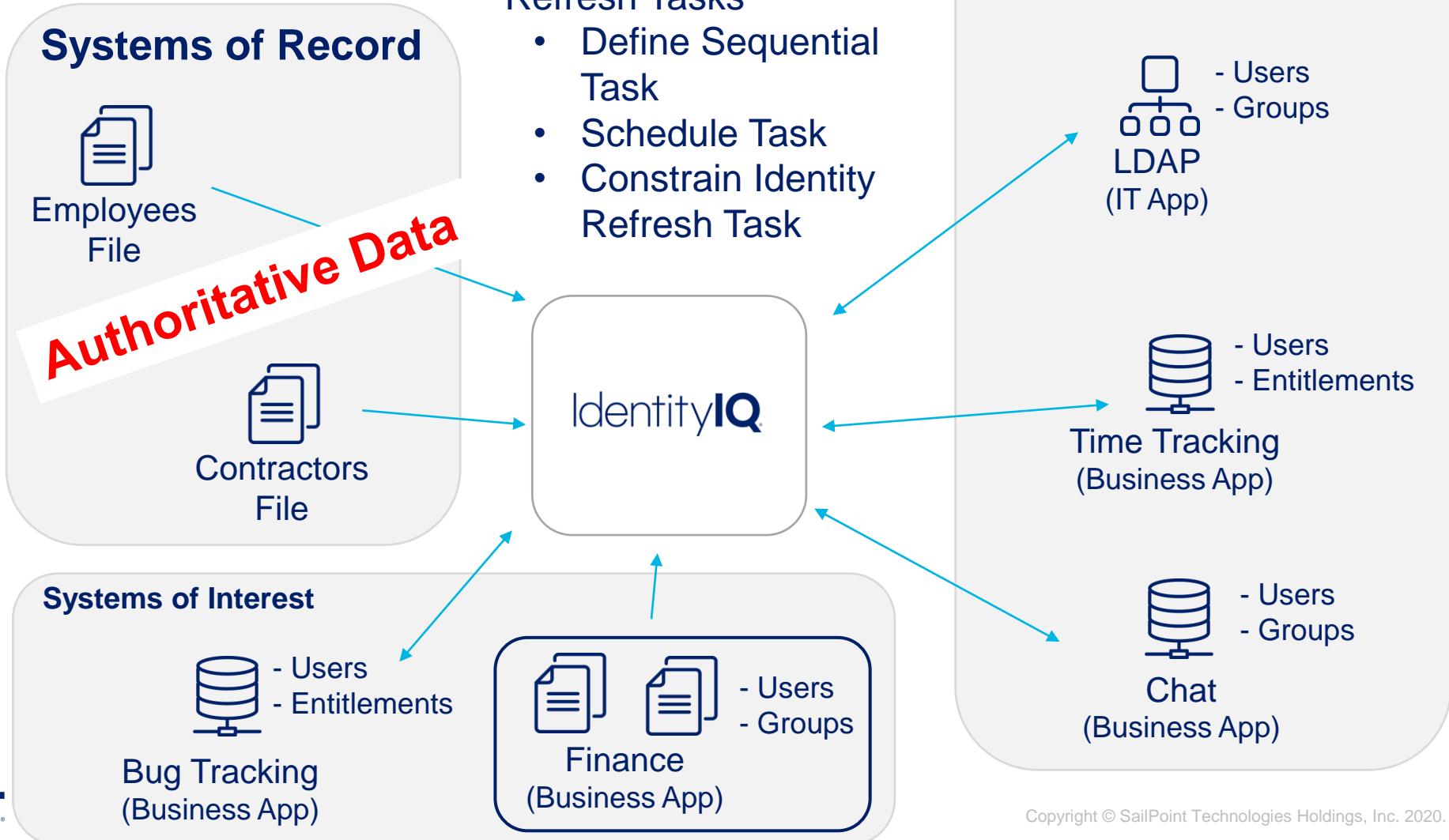
- Treats delimited files as tables in database

# Knowledge Check

# Practice Exercises

# Exercise Preview

## Section 2, Exercises 1 & 2







# Data and System Oversight

IdentityIQ Essentials

# Overview

---

## Data Oversight

- Connector Debug / Preview
- Account, Entitlement, Identity pages
- Querying
- Reporting

# Account and Group Schema Preview

Object Type: account

Details

Native Object Type	Display Attribute
account	User Name
Identity Attribute	Instance Attribute
User ID	
<input type="checkbox"/> Include Permissions	Remediation Modifiable
	Readonly ▾

Attributes

Name	Description	Type	Properties
User ID		string	
User Name			
Permission Group			
Status			
Locked			

[Add New Schema Attribute](#) [Discover Schema Attributes](#) [Delete Schema Attribute](#)

[Preview](#)

**Preview**

User Name	User ID	Permission Group	Status	Locked
James Smith	1a	ACCOUNTING	A	N
Mary Johnson	1a2a	ACCOUNTING,FINANCE	A	N
John Williams	1a2b	FINANCE,HR,IT	A	N
Michelle Perez	1a2b3b4a	IT,HR,ACCOUNTING	A	N
Carl Foster	1b2a3a4a	ACCOUNTING,IT	A	N
Richard Jackson	1a2c3a	AP,AR	A	N
Judy Warren	1b2c3b4a	ACCOUNTING,AP	A	N

Application → Configuration → Schema

# IdentityIQ Console – Connector Debug

## Test and Troubleshoot

Feature	Command
Iteration	Accounts: connectorDebug <Application> <b>iterate account</b> Groups: connectorDebug <Application> <b>iterate group</b>
Connection Test	connectorDebug <Application> <b>test</b>
Pass-through Authentication Test	connectorDebug <Application> <b>auth &lt;username&gt; &lt;password&gt;</b>

# Application, Entitlement & Identity Cube

## Confirm Results

The screenshot displays three interconnected dashboards within the SailPoint Application, Entitlement & Identity Cube:

- Application Dashboard:** Shows account details for Aaron.Nichols. A blue callout box labeled "Application" points to this section.
- Entitlement Catalog Dashboard:** Shows entitlements for LDAP groups. A blue callout box labeled "Entitlements" points to this section.
- Identity Warehouse Dashboard:** Shows identity details for users Aaron.Nichols and Adam.Kennedy. A blue callout box labeled "Identities" points to this section.

**Application Dashboard Data:**

Account ID	Account Name	Status	Last Refresh	Identity Name
cn=Aaron.Nichols,ou=people,dc=trai...	Aaron.Nichols	Active	8/11/19	Aaron.Nichols
cn=Adam.Kennedy,ou=peo...				
cn=Alan.Bradley,ou=pe...				

**Entitlement Catalog Data:**

Application	Attribute	Display Name	Type	Description	Owner	Requestable
LDAP	groups	AccessBugTracking	Group	Access to Bug Tracking application		
LDAP	groups	Contractors	Group	All contractors at the company		
LDAP						
LDAP						

**Identity Warehouse Data:**

User Name	First Name	Last Name	Manager	Assigned Role Sum	Detected Role Sum	Risk Score	Last Refresh	Type
Aaron.Nichols	Aaron	Nichols		0	0	0	7/16/19 8:35 PM	Employee
Adam.Kennedy	Adam	Kennedy	Douglas.Flores	0	0	0	7/16/19 8:35 PM	Employee

# Entitlement Catalog Editing

- Display name
- Descriptions
  - Multi-lingual (optional)
- Owners
- Requestable
- Extended attributes
- UI vs. Export/Import

**Edit Group**

**Standard Properties**   **Object Properties**   **Members**   **Access**   **Classifications**

Application	Active_Directory
Type	Group
Attribute	groupmbr
Value	AccountingGeneral
Display Value	Accounting General
Requestable	<input checked="" type="checkbox"/>
<p style="text-align: right;">B I U       English (United States) ▾</p> <p>Assigned to all members of the Accounting division</p>	
Description	<p>54 of 1024 characters (including markup)</p>
Owner	Mary Johnson
Compliance	
Authorization	None

# Advanced Analytics

## Confirm Results

Identity search

Entitlement search

Account search

Advanced Analytics

Search Type: Identity

Advanced Search

Search Criteria:

- Identity
- Access Review
- Role
- Entitlement
- Activity
- Audit
- Process Metrics
- Access Request
- Syslog
- Account

Last Name

First Name

Username

Display Name

Email

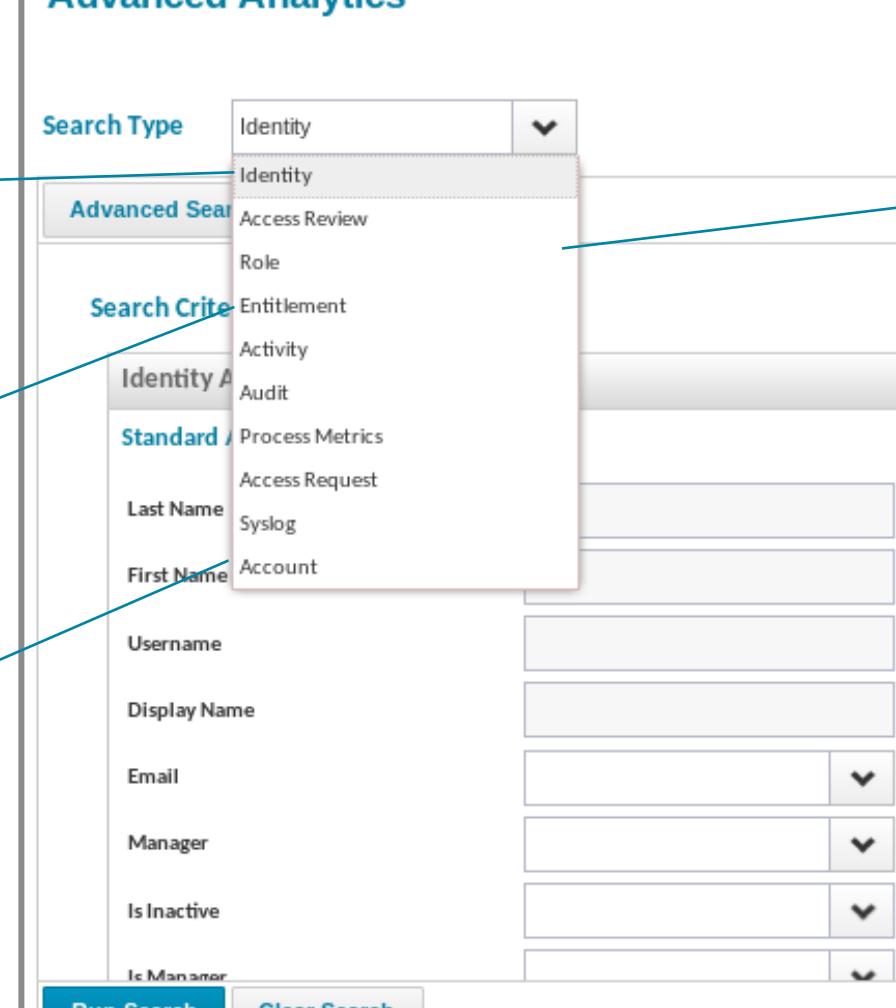
Manager

Is Inactive

Is Manager

Run Search

Clear Search



Types of searches

- Search Results
- View
  - Export
  - Save as report
  - ...and more

# Reports

## Categories

**Application Data**  
• Statistics  
• Configurations

**Identity Data**

The screenshot shows the 'Reports' section of the SailPoint interface. At the top, there are four tabs: 'My Reports', 'Reports' (which is selected and highlighted with a red box), 'Scheduled Reports', and 'Report Results'. Below the tabs is a search bar labeled 'Search by Report Name' with a magnifying glass icon. The main area lists report categories under the heading 'Name':

- + Category: Access Review and Certification Reports (12 Reports)
- + Category: Account Group Reports (2 Reports)
- + Category: Activity Reports (1 Report)
- + Category: Administration Reports (9 Reports)
- + Category: Application Reports (1 Report)
- + Category: Configured Resource Reports (3 Reports)
- + Category: Identity and User Reports (13 Reports)
- + Category: Lifecycle Manager Reports (6 Reports)
- + Category: Policy Enforcement Reports (1 Report)
- + Category: Risk Reports (3 Reports)
- + Category: Role Management Reports (6 Reports)

**Compliance**

**IdentityIQ Admin**

**Request Processes**

**Roles**  
• Definitions  
• Assignments

# Knowledge Check

# Practice Exercises

# Exercise Preview

---

## Section 2, Exercise 3

- Fix Uncorrelated Accounts
  - Identify uncorrelated accounts
  - Manually correlate an account to an Identity Cube
  - Remove empty Identity Cube
- Edit Entitlements
  - Export/import





# System Oversight

IdentityIQ Essentials

# Overview

---

## System Oversight

- Terminology Review
- Task Performance Strategies
- Monitoring Tasks
- Administrator Console
  - Tasks
  - Environment

# Terminology Review

---

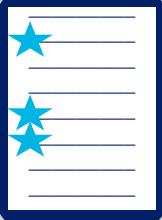
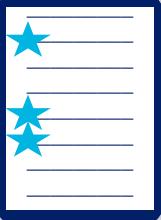
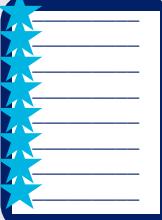
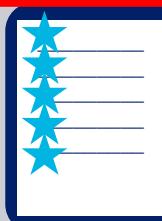
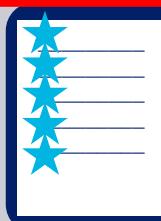
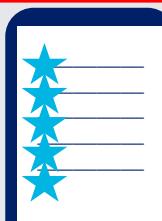
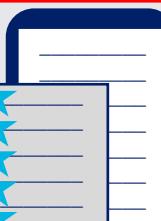
- EL – interactive drag & drop slide (match terms to definitions)

# Tasks

---

- Tasks perform periodic operations such as
  - Aggregation
  - Identity Refresh
  - Running Rules
  - System Maintenance
    - Moving Certifications along and finishing them
    - Checking for remediations
    - Pruning or archiving old objects
  - Running ordered set of tasks (Sequential Task Launcher)
- Performance of regularly scheduled tasks is critical to health of installation
  - Aggregation
  - Refresh
  - Others dependent upon environment

# Aggregation Performance Strategies

	IdentityIQ	Application
IdentityIQ-based Optimization (default) <ul style="list-style-type: none"><li>• Every account read</li><li>• Only those with changes are processed</li><li>• Task option <i>Disable optimization of unchanged accounts</i> = false</li></ul>		
Process All <ul style="list-style-type: none"><li>• Every account read and processed</li><li>• Task option <i>Disable optimization of unchanged accounts</i> = true</li></ul>		
Custom Delta Processing <ul style="list-style-type: none"><li>• Manage own change (i.e. write changed accounts to a flat file and process flat file)</li><li>• Task option <i>Detect deleted accounts</i> = false</li></ul>		
Connector-based Delta Aggregation* <ul style="list-style-type: none"><li>• Read and process only accounts with changes that have taken place after benchmark<ul style="list-style-type: none"><li>• lastModData, DirSync, usnChanged, etc.</li></ul></li><li>• Task option <i>Enable Delta Aggregation</i> = true</li></ul>		

\*Not supported by all connectors

# Aggregation Performance Strategies

---

## Partitioning

- Connector level
  - Supported connectors
    - LDAP, AD, JDBC, Delimited File, PeopleSoft, SAP, etc.
  - Limit partitions to less than 250
- All at application level
  - Specify loss limit
- More information
  - Compass→IdentityIQ Whitepapers→Partitioning Best Practices

# Identity Refresh Performance Strategies

---

- Split Refresh into different tasks
  - Attribute Refresh/Role/Entitlement Processing/Provisioning multiple times a day
  - Policy Checking/Risk Scoring at less frequent intervals
- Refresh only Identities that have changed
  - Delta refresh – aggregation marks cubes with changes for refresh processing
  - Controllable with task options
    - Filters, time stamp
- Divide and Conquer
  - Multi-threading
    - Runs on multiple threads on a single server
  - Partitioning
    - Runs on multiple threads on multiple servers
    - Specify loss limit

# IdentityIQ Maintenance Tasks

## Required for IdentityIQ Functionality

- Five tasks are pre-scheduled

Task	Purpose	Default Schedule
Perform maintenance	Keeps core processes working (certification phases, background processes, etc.)	Every 5 minutes
Check expired mitigations daily	Scans for policy & certification exceptions that have expired	Daily
Check sunset requests for notifications daily	Controls timing of email notifications and sunset reminders of expiring items	Daily
Check expired work items daily	Scans for incomplete work items that have expired	Daily
Perform Identity Request Maintenance	Checks for provisioning completeness	Daily

# Monitoring Tasks

The screenshot shows the SailPoint Administrator Console interface. On the left, a sidebar titled "Task Result" displays details for a completed task named "Aggregate Employees". The task was a "Perform maintenance" operation using the "System" type, which was successful. It started at 7/7/19 10:20 AM and completed at 7/7/19 10:19 AM. The host was "training.sailpoint.com". The average runtime was 10 seconds, and the run time was 11 seconds, which is 10% more than the average. The status is marked as "Success". Below this, there is a table titled "Aggregate Employees Attributes" showing the following data:

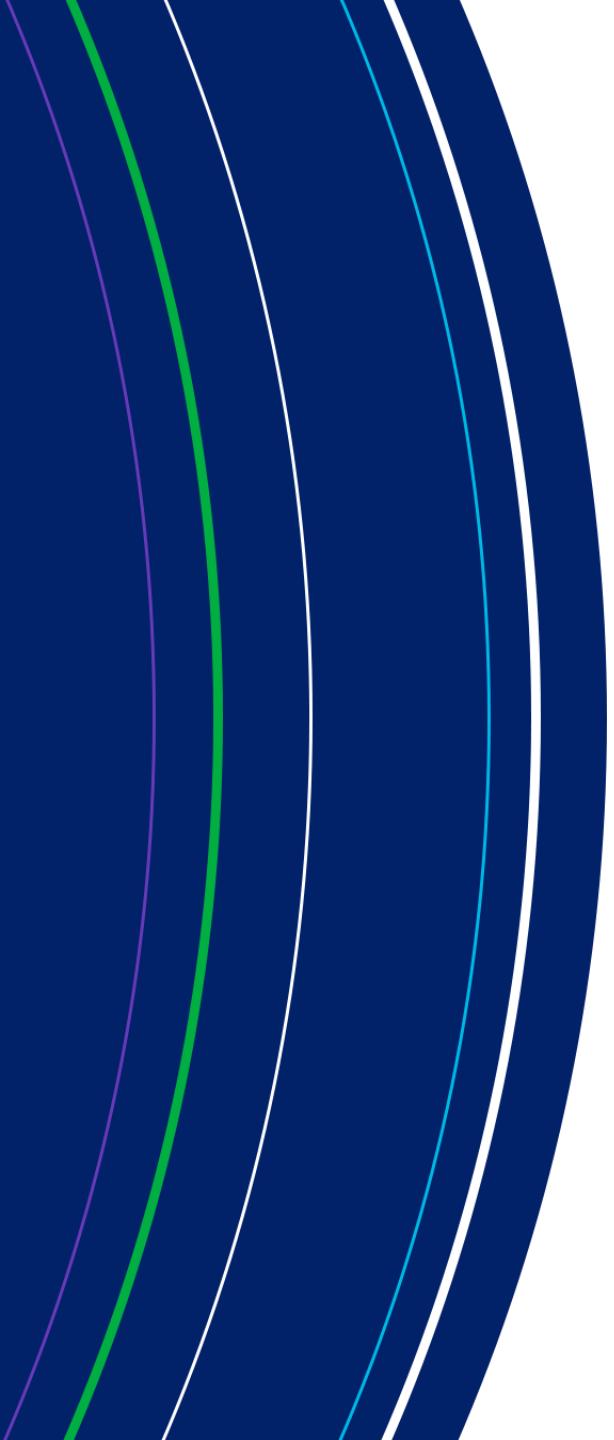
Attribute	Value
Applications scanned	HR Employees
Accounts scanned	162
Identities updated	162

At the top of the main content area, there are three tabs: "Active" (1), "Scheduled" (5), and "Completed" (17). The "Completed" tab is selected, showing a list of completed tasks. The first task listed is "Perform maintenance" (System type, Success, 10:20 AM - 10:19 AM, host training.sailpoint.com, runtime 10 seconds). The second task listed is "Aggregate Employees" (AccountAggregation type, Success, 10:19 AM - 10:19 AM, host spadmin, runtime 11 seconds, 10% more than average).

**Gear → Administrator Console → Tasks**

**Setup → Tasks → Task Results**

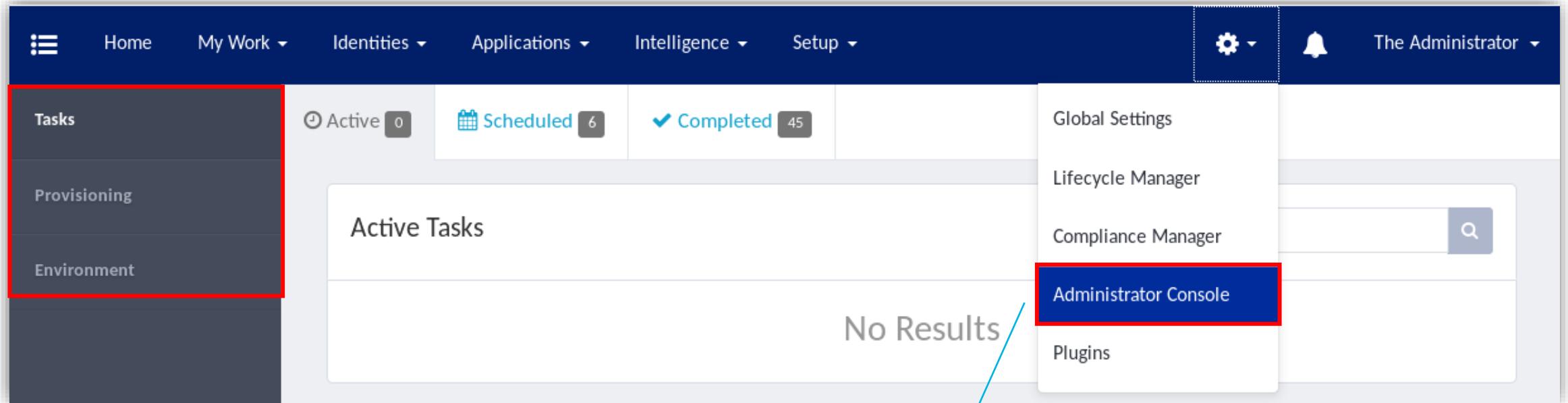
**Task Notifications**



# **Administrator Console Tasks & Environment**

# Administrator Console

## Manage Tasks, Provisioning and Environment



Requires System Administrator or  
FullAccessAdminConsole capabilities

# Tasks Page

- View or terminate running tasks
- Dump a stack trace

- View, postpone, or delete scheduled tasks

- View completed tasks, including run statistics

The screenshot shows the SailPoint Tasks Page interface. At the top, there are three navigation tabs: "Active" (9), "Scheduled" (6), and "Completed" (68). Below the tabs is a section titled "Active Tasks" containing a table with the following columns: Name, Type, Start Date, Owner, Host, Current Runtime, Average Runtime, and Actions. Two rows of data are visible:

Name	Type	Start Date	Owner	Host	Current Runtime	Average Runtime	Actions
Aggregate Authoritative Apps and Refresh	Generic	12/26/17 5:36 PM	spadmin	training.sailpoint.com	26 seconds	32 seconds	<span>X</span> <span>&lt;/&gt;</span>
Refresh Identity Cube	Identity	12/26/17 5:36 PM	spadmin	training.sailpoint.com	10 seconds	13 seconds	<span>X</span> <span>&lt;/&gt;</span>

# Environment Page

- Statistics on the state of your environments
- Configure globally, or per host

- Status of applications

- Status of installed modules and extensions

The screenshot shows the SailPoint Environment Page interface. At the top, there are three main navigation tabs: 'Hosts' (selected), 'Applications' (highlighted with a blue border), and 'SailPoint Modules & Extensions'. Below the tabs is a 'Hosts' section with a table. The table has columns: Host Name, Status, Last Heartbeat, CPU, Memory Percentage, Request Threads, and Host Actions. A single row is visible for 'training.sailpoint.com', which is marked as 'Up' with a green arrow icon. The 'Host Actions' column for this row contains two icons: a gear (highlighted with a red box) and a delete (X). The bottom left of the table area shows 'Show 10'. The bottom center of the page displays 'Showing 1-1 of 1'. The entire interface has a light gray background with blue and white text.

Host Name	Status	Last Heartbeat	CPU	Memory Percentage	Request Threads	Host Actions
training.sailpoint.com	Up	6/4/19 3:04 PM	0.255%	66.4%	0	

# Environment Page

## Applications

Application Name	Type	Status
Bug Tracking	JDBC	0 ↑ 0 ↓
Chat	JDBC	0 ↑ 0 ↓
Extended Form	DelimitedFile	0 ↑ 0 ↓
Finance	DelimitedFile	0 ↑ 0 ↓

# Knowledge Check

# Practice Exercises

# Exercise Preview

---

## Section 3, Exercise 1

- Explore Task Management Options
  - Delta Refresh
  - Run Rule task
  - Standard maintenance tasks
  - Aggregation and application maintenance windows
  - Monitor tasks with the Administrator Console





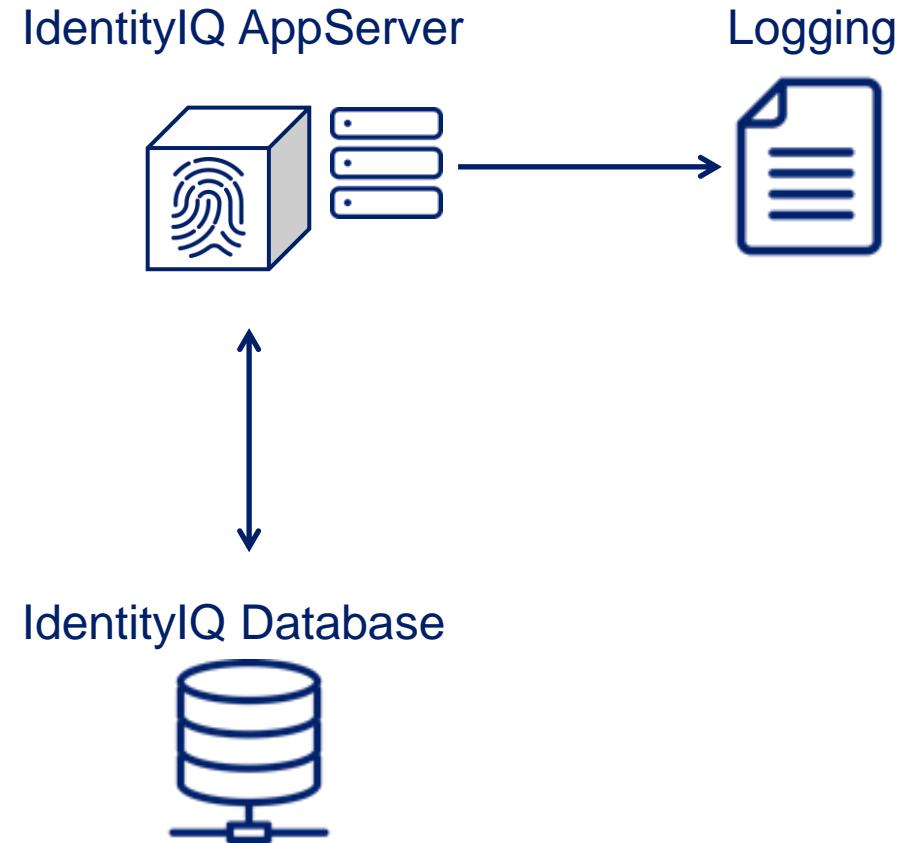
# Logging

IdentityIQ Essentials

# Logging

## Options

- Standard Out print statements  
(Not recommended for production)
- Java application logging (log4j)
- Email redirection
- Audit configuration
- Syslog logging configuration



# Standard Out Logging

---

- Standard Out
  - Usage: `System.out.println("I'm logging this message.");`
- Configuration
  - App server configuration determines where to send this information
- Best practices
  - Only use for testing – useful for quick debugging
  - Do not use in production
  - Not as useful as log4J since these messages are always printed no matter what

# Logging

---

## Print vs. Log4j

- `System.out.println("I'm logging this message all the time.");`
- `log.debug("I'm logging this message when debug logging is turned on.");`

# Java Application Logging

## Log4j File Settings

Logging levels

RootLogger configuration

Class logging configurations

```
### set default log levels and appenderRef
### valid log levels in increasing order of severity are:
###   trace, debug, info, warn, error, fatal, off
### trace is required to get method entry and exit logging

rootLogger.level=warn
rootLogger.appenderRefs = rolling, stdout
rootLogger.appenderRef.rolling.ref = roll
rootLogger.appenderRef.stdout.ref = stdout

logger.aggregator.name=sailpoint.api.Aggregator
logger.aggregator.level=debug

#logger.cacheTracker.name=sailpoint.api.CacheTracker
#logger.cacheTracker.level=trace

#logger.certificationer.name=sailpoint.api.Certificationer
#logger.certificationer.level=info
```

<install dir>/WEB-INF/classes/log4j2.properties

# Java Application Logging

## Log4j Log Levels

```
logger.aggregator.name=sailpoint.api.Aggregator  
logger.aggregator.level=debug
```

log4j2.properties

Set log level

```
2019-06-14T11:33:21,562 INFO QuartzScheduler_Worker-4 sailpoint.api.Aggregator:1665 - Creating: Grace.Stanley  
2019-06-14T11:33:21,568 DEBUG QuartzScheduler_Worker-4 sailpoint.api.Aggregator:1672 - Iterating over the next account.  
2019-06-14T11:33:21,571 DEBUG QuartzScheduler_Worker-4 sailpoint.api.Aggregator:1672 - Processing object Cori.Garrett  
2019-06-14T11:33:21,587 INFO QuartzScheduler_Worker-4 sailpoint.api.Aggregator:4359 - Committing : Grace.Stanley  
2019-06-14T11:33:21,594 INFO QuartzScheduler_Worker-4 sailpoint.api.Aggregator:1665 - *** Aggregating: 1c2d  
2019-06-14T11:33:21,600 INFO QuartzScheduler_Worker-4 sailpoint.api.Aggregator:1665 - Creating: Cori.Garrett  
2019-06-14T11:33:21,606 DEBUG QuartzScheduler_Worker-4 sailpoint.api.Aggregator:1672 - Iterating over the next account.  
2019-06-14T11:33:21,610 DEBUG QuartzScheduler_Worker-4 sailpoint.api.Aggregator:1672 - Processing object Tyler.Petrick  
2019-06-14T11:33:21,624 INFO QuartzScheduler_Worker-4 sailpoint.api.Aggregator:4359 - Committing : Cori.Garrett
```

<custom dir>/iiq\_training\_rolling.log

# Java Application Logging

---

## Log4j Example

- Inside of rule

```
log.error("This is an error message");
log.warn("This is a warn message");
log.info("This is an info message");
log.debug("This is a debug message");
log.trace("This is a trace message");
```

- What gets printed into log file if log level is set to “info”?

# Java Application Logging

## Enabling Class Logging

Enabled class

Disabled classes

```
### set default log levels and appenderRef  
### valid log levels in increasing order of severity are:  
###      trace, debug, info, warn, error, fatal, off  
### trace is required to get method entry and exit logging
```

```
logger|aggregator| name=sailpoint.api.Aggregator  
logger|aggregator| level=debug
```

```
#logger.cacheTracker.name=sailpoint.api.CacheTracker  
#logger.cacheTracker.level=trace
```

```
#logger.certificationer.name=sailpoint.api.Certificationer  
#logger.certificationer.level=info
```

<install dir>/WEB-INF/classes/log4j2.properties

# Java Application Logging

## Activating New Settings

The screenshot shows the SailPoint Identity IQ interface with the 'Logging' configuration page open. The top navigation bar includes 'Home', 'My Work', 'Identities', 'Applications', 'Intelligence', 'Setup', and a gear icon. The left sidebar lists 'About', 'Object', 'Memory', 'Caches', 'Beans', 'Threads', 'Call Timings', and 'Logging'. The main content area displays the 'Logging' configuration with a 'Server File Path' input field containing the path '/opt/apache-tomcat-9.0.16/webapps/identityiq/WEB-INF/classes/log4j2.properties'. Below it is a red-bordered 'Reload Logging Configuration' button. A blue callout box points to this button with the text 'Reload changes every 20 seconds'. Another blue callout box points to the 'Logging' item in the sidebar with the text 'Force reload'. On the far left, a code snippet from 'log4j2.properties' is shown, with the 'monitorInterval=20' line highlighted by a red box.

```
#####
## Global log4j2 properties
#####
name=identityiq_default
status=warn
monitorInterval=20
packages=sailpoint.api.logging
```

log4j2.properties

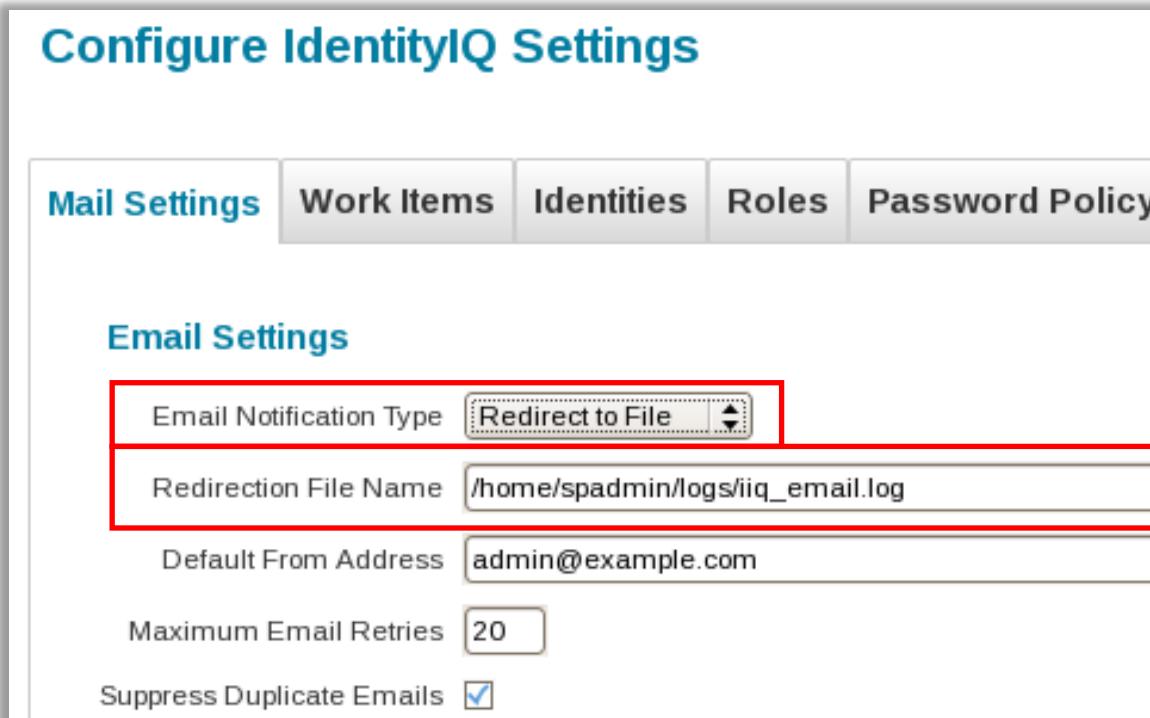
Reload changes  
every 20 seconds

Force reload

Debug Pages → Logging

# Email Logging

- Can redirect emails to file for testing, debugging, and troubleshooting
  - Send to log file
  - Send to single email recipient



# Auditing

## Configure

**Audit Configuration**

General Actions   Identity Attribute Changes   Class Actions   SCIM Resource Actions

**General Actions**

Action	Enabled
Login	<input type="checkbox"/>
Logout	<input type="checkbox"/>
Login Failure	<input checked="" type="checkbox"/>
Session Timeout	<input type="checkbox"/>
Import File	<input checked="" type="checkbox"/>
Run Task	<input type="checkbox"/>
Email Sent	<input checked="" type="checkbox"/>
Email Failure	<input checked="" type="checkbox"/>
Delegate Certification Item	<input checked="" type="checkbox"/>
Delegation Completion	<input checked="" type="checkbox"/>
Delegation Revocation	<input checked="" type="checkbox"/>

Gear → Global Settings → Audit Configuration

## View

Search Type: Audit

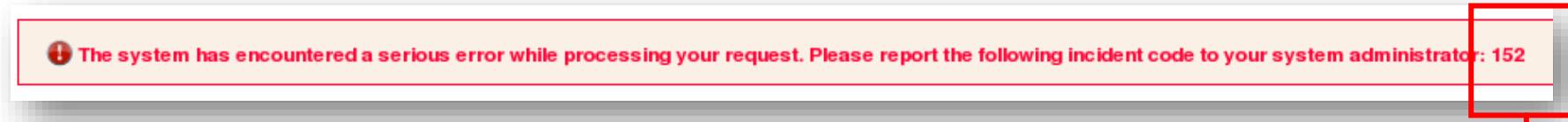
Search Results - 26 Results Returned

Action	Client Host	Date	Server Host	Source	Target
ServerUpDown		July 2, 2019 6:41 PM	training.sailpoint.c...	training.sailpoint.c...	ServerUp
import		July 2, 2019 6:40 PM	training.sailpoint.c...	The Administrator	init-acceleratorpac...
...		July 2, 2019 6:40 PM	training.sailpoint.c...	The Administrator	init-acceleratorpac...

Intelligence → Advanced Analytics → Audit Search

# Syslog – Incident Codes

- When errors occur, an incident code may display in the UI



- Enter incident code to retrieve details
  - Intelligence → Advanced Analytics → Syslog Search

The screenshot shows the "Search Criteria" and "Fields to Display" sections of the Syslog search interface. The "Incident Code" field in the search criteria is highlighted with a red box and contains the value "152". The "Server" dropdown in the search criteria and the "Server" checkbox in the "Fields to Display" section are also highlighted with red boxes. Both the "Server" dropdown and the "Server" checkbox are checked.

**Search Type:** Syslog

**Search Criteria:**

**Syslog Attributes:**

Incident Code	152	Server
Level		Username
Classname		Message

**Filter by: Date**

Start Date  End Date

**Fields to Display:**

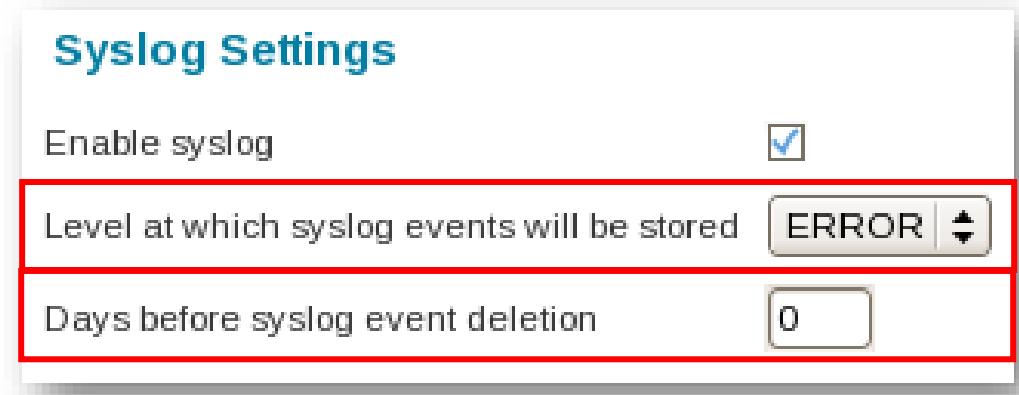
**Syslog Display Fields:**

<input type="checkbox"/> Classname
<input checked="" type="checkbox"/> Date
<input checked="" type="checkbox"/> Incident Code
<input checked="" type="checkbox"/> Level
<input type="checkbox"/> Line
<input checked="" type="checkbox"/> Message
<input checked="" type="checkbox"/> Server

# Syslog Log

## Configuration

- Default = enabled, with no event deletion
- Set “Days before syslog event deletion” (best practice)
  - Typically set to 30 days
- Gear → Global Settings → IdentityIQ Configuration → Miscellaneous



# Knowledge Check

Next Step?

# Practice Exercises

# Exercise Preview

---

## Section 3, Exercise 2

- Explore Logging Options
  - Enable/disable logging
  - View results





# Troubleshooting Tools and Resources

IdentityIQ Implementation and Administration: Essentials

# Overview

---

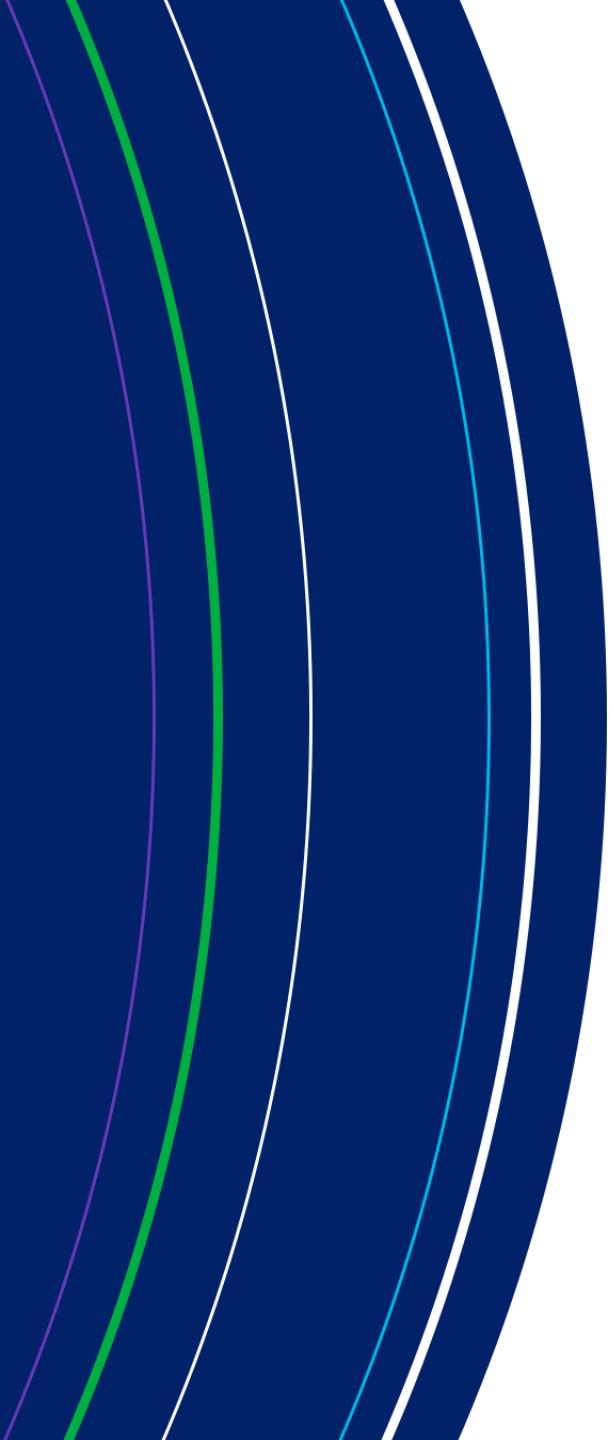
## Troubleshooting Tools and Resources

- Factors in successful troubleshooting
- IdentityIQ Console
- IdentityIQ Debug Pages

# Factors in Successful Troubleshooting

---

- Detail-Oriented
  - Small inconsistencies can cause large headaches
  - Take detailed notes, follow documentation steps carefully
- System Familiarity
  - Build your IdentityIQ knowledge
  - Training and time spent with the product
- Methodical Testing
  - Repeatable testing leads to success
  - Change one variable at a time
- Environmental Awareness
  - Components in play: database, application server, JVM, network, other systems
  - It might not be related to IdentityIQ



# **IdentityIQ Console and Debug Pages**

# IdentityIQ Console

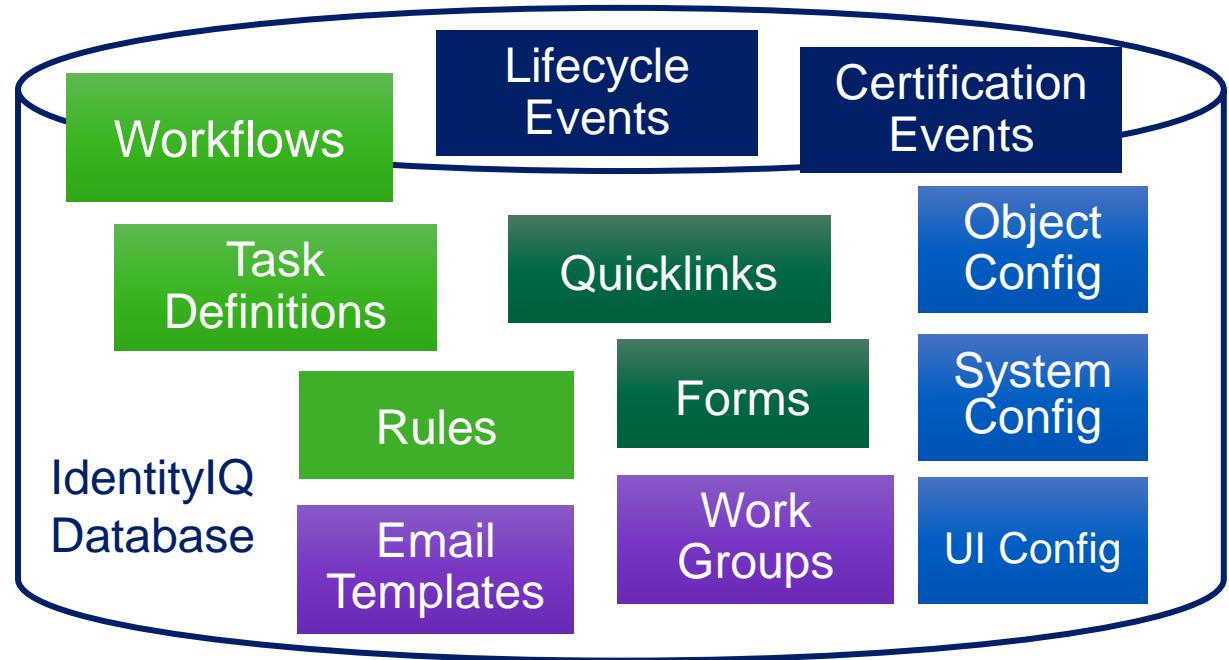
---

- Command-line interface
- Authentication required
  - Exception: **spadmin** with the **admin** password
- Connects directly to database
  - Can be used to troubleshoot connectivity problems
- Many commands available through both browser interface and console
  - Test connections
  - Import objects
- Some commands are only available via console
  - SQL query interface
  - Export

# Console

## Managing Objects

- Act upon sets of objects
  - List
  - Count
  - Delete



# Console

## Retrieving Objects

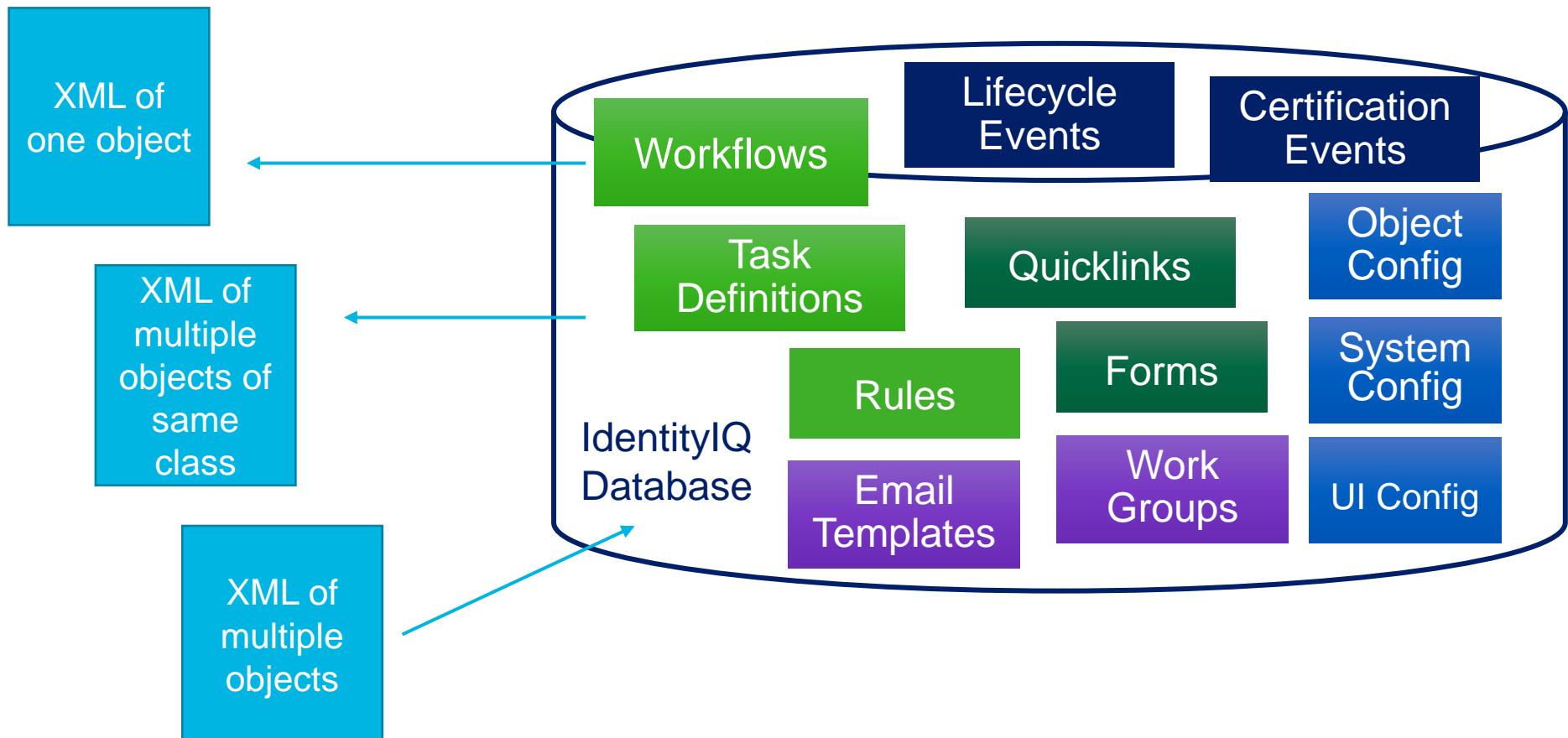
- View XML representation
  - Get

```
<?xml version='1.0' encoding='UTF-8'?>
<!DOCTYPE TaskDefinition PUBLIC "sailpoint.dtd" "sailpoint.dtd">
<TaskDefinition created="1581899628883" formPath="/monitor/tasks/accountAggregationTask.xhtml"
id="7f000001705018c081705090c1530533" modified="1582019248229" name="Aggregate Chat"
resultAction="Delete" subType="task_item_type_acct_aggregation" type="AccountAggregation">
  <Attributes>
    <Map>
      <entry key="TaskDefinition.runLengthAverage" value="20"/>
      <entry key="TaskDefinition.runLengthTotal" value="62"/>
      <entry key="TaskDefinition.runs" value="3"/>
      <entry key="TaskSchedule.host"/>
      <entry key="applications" value="Chat"/>
      <entry key="checkDeleted" value="true"/>
      <entry key="checkHistory" value="false"/>
      <entry key="checkPolicies" value="false"/>
      <entry key="correlateEntitlements" value="false"/>
      <entry key="correlateOnly" value="false"/>
      <entry key="correlateScope" value="false"/>
      <entry key="deltaAggregation" value="false"/>
      <entry key="enablePartitioning" value="false"/>
      <entry key="haltOnMaxError" value="false"/>
      <entry key="noAutoCreateApplications" value="false"/>
      <entry key="noAutoCreateScopes" value="false"/>
      <entry key="noNeedsRefresh" value="false"/>
      <entry key="noOptimizeReaggregation" value="true"/>
      <entry key="promoteManagedAttributes" value="true"/>
      <entry key="refreshScorecard" value="false"/>
      <entry key="sequential" value="false"/>
      <entry key="taskCompletionEmailNotify" value="Disabled"/>
      <entry key="taskCompletionEmailRecipients"/>
      <entry key="taskCompletionEmailTemplate"/>
    </Map>
  </Attributes>
  <Description>Task template for application account scanning.</Description>
  <Owner>
    <Reference class="sailpoint.object.Identity" id="7f00000170451164817045e1c6de0109" name="sp
  </Owner>
  <Parent>
    <Reference class="sailpoint.object.TaskDefinition" id="7f00000170451164817045e1dd3501bf" na
  </Parent>
</TaskDefinition>
```

# Console

## Importing/Exporting Objects

- Checkout
- Export
- Import



# Console

## Data Export Best Practice

```
<?xml version='1.0' encoding='UTF-8'?>
<!DOCTYPE AuditEvent PUBLIC "sailpoint.dtd" "sailpoint.dtd">
<AuditEvent action="loginFailure" clientHost="0:0:0:0:0:0:0:1" created="1581722848004"
id="7f000001704514b9817046074aff004f" modified="1582025795342"
serverHost="training.sailpoint.com" source="foo"/>
```

- Unique to Instance
- Id
  - Created Date
  - Modified Date

- Remove information unique to IdentityIQ instance
  - Export and checkout “clean” option
  - Import “noid” option

# Console

## Other Useful Commands

Category	Command	Purpose
Aggregation	connectorDebug	Iterate over application accounts or groups without loading them
Rules	rule <rulename>	Runs a rule
Tasks	list taskdefinition	Lists all tasks <b>and reports</b> in the system
	tasks	Lists all scheduled tasks
	run <taskname>	Runs a task
General	about	Lists info about system
	source	Load and execute command file into console

# IdentityIQ Debug Pages

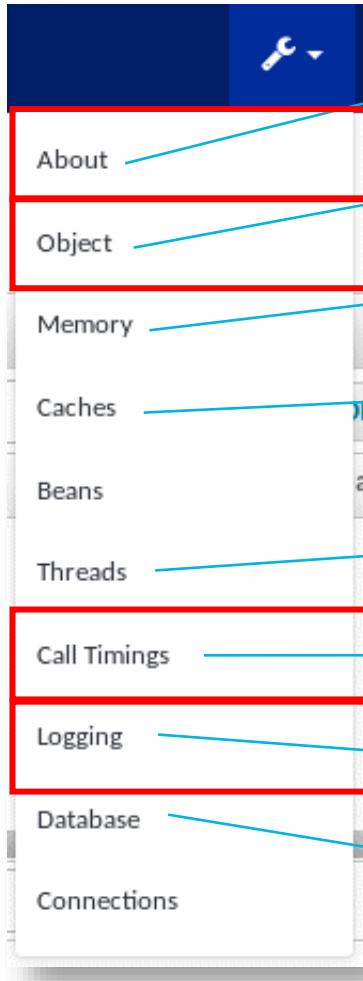
---

## Advanced Configuration and Debugging

- Only available to users with System Administrator capability
- Hidden context root for debugging options
  - Example: `http://localhost:8080/identityiq/debug/`
- Provides Many Features
  - Viewing and editing of XML objects
  - Creating and deleting objects
  - Access to Configuration
    - System Configuration
    - UI Configuration
  - Memory Usage
  - Garbage Collection Methods

# Debug Pages

## System Information



About IIQ Environment

Object Viewer (Default Page)

Display Current Memory Usage

Reset Cache

Troubleshoot Threads

Call Timings

Reload Log4J Configuration

DB Settings/# of Connections  
Used

# Debug Page – Default View

## Object Viewer

Object Type to Search for

Object to Search for

Manipulate Configuration Objects UIConfig System Config Identity / Mapping

Run Rules

Create and Delete Objects

### Debug Pages

#### Object Browser

Identity	Name	Created	Modified
ff808014369706c01436970c71a011c	Carl.Foster	1/6/14 3:23 PM	1/20/14 12:17 PM
ff808014369706c01436970ce8c0172	Carlos.Perkins	1/6/14 3:23 PM	1/20/14 12:16 PM
ff808014369706c01436970b9d2008e	Carmen.Hansen	1/6/14 3:23 PM	1/20/14 12:16 PM
ff808014369706c01436970bfb200cc	Carol.Adams	1/6/14 3:23 PM	1/20/14 12:17 PM
ff808014369706c01436970c5bd010a	Carolyn.Perry	1/6/14 3:23 PM	1/20/14 12:16 PM

# Knowledge Check

Next Step?

# Practice Exercises

# Exercise Preview

---

## Section 3, Exercise 3

- Explore IdentityIQ Debug, Console, and Logging
  - Explore Debug Pages
    - About, Logging, and Call Timings
    - Object Browser
    - Create a copy of an object
    - Run a rule
  - Explore IdentityIQ Console
    - Explore help
    - Explore commands
    - Run a rule
    - Import/export objects





# Introduction to Policies

IdentityIQ Essentials

# Policy Definition

---

- IdentityIQ policies define the access-related business policies of your enterprise

**Example:** Can't have access to both approve vendor and pay vendor

- Detect users who are currently in violation of policies
- Prevent users from violating policies
- Defined using data from business environment
  - Identity attributes
  - Application attributes
  - Risk scores
  - Roles
  - Entitlements

# Policy Examples

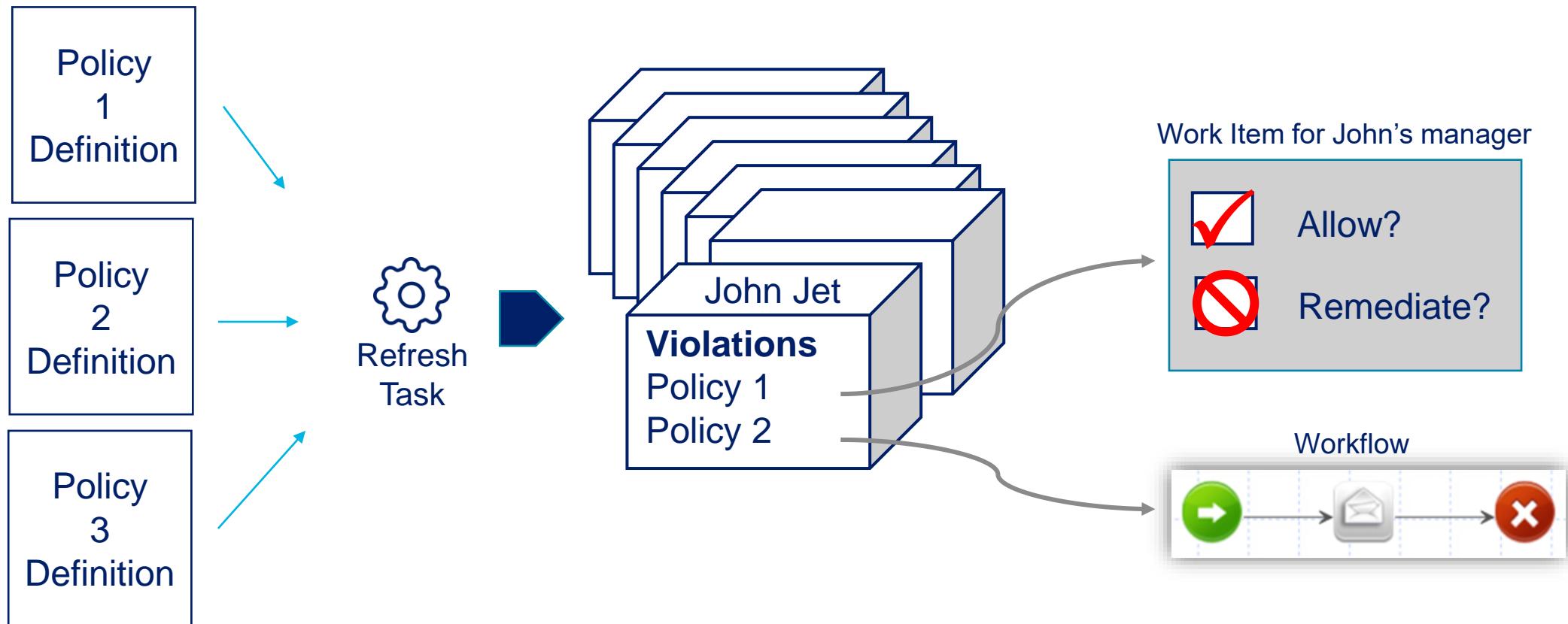
---

- Mutually exclusive access
- Incorrect responsibilities
- More than one account



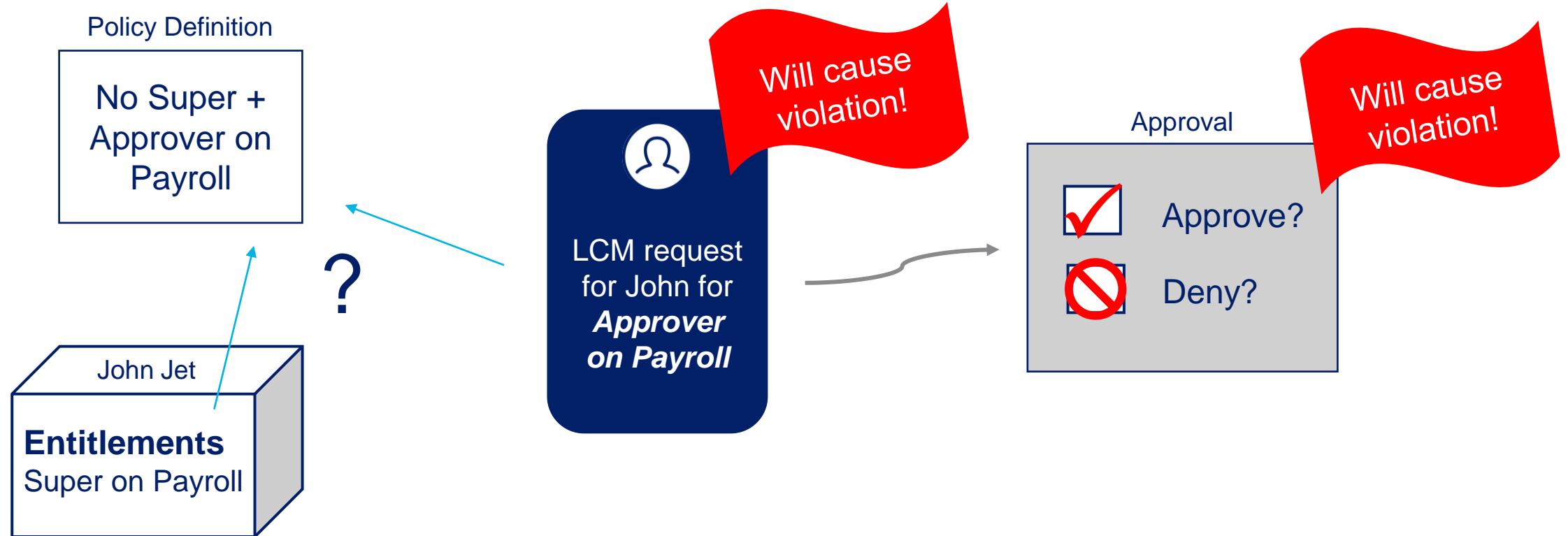
# Policy Usage

## Compliance – Detective



# Policy Usage

## Provisioning – Preventive



# Detection

## Identity Refresh Task

Clean up groups definitions that are no longer referenced	 <input type="checkbox"/>	Enable policy checking
Check active policies	 <input checked="" type="checkbox"/>	
Keep previous violations	<input type="checkbox"/>	Optionally keep previous violations
A comma separated list of specific policy names. When set this overrides the default policies.	 <input type="text"/>	
Refresh assigned scope	 <input type="checkbox"/>	Selective policy checking

# Knowledge Check

# Practice Exercises

# Exercise Preview

---

## Section 3, Exercise 4

- Define Policies
  - Define entitlement separation of duties (SoD) policy
  - Detect users in violation of policy





# Introduction to Certifications

IdentityIQ Essentials

# Certifications

---

## Purpose and Responsibilities

- Purpose
  - Keep user access compliant
    - Legal requirements
    - Industry standards or regulations
    - Business rules
  - Provide oversight and visibility
- Responsibilities
  - Implementers and system administrators
    - Responsible for knowing how these features work
    - Possibly responsible for providing rules
    - Unlikely to be responsible for ongoing configuration and monitoring
  - Often companies have dedicated compliance teams/business administrators

# Access Certification

---

- The process of automating the periodic review and approval of:
  - Identity Access
  - Role Membership
  - Account Group Membership
  - Role Composition
  - Account Group Permissions



Targeted  
Manager  
Application Owner  
Entitlement Owner  
Advanced

# Certifications/Access Reviews

## Definitions

- Certifications
  - Define the certification campaign
    - What is reviewed
    - When
    - By whom
  - Comprised of one or more access reviews that share the same parameters
- Access Reviews
  - Gather users' access data at time of generation
  - Provide that collection of data to be certified
  - Routed to the reviewer to take action
- Access Review Details
  - Present the entities to be certified

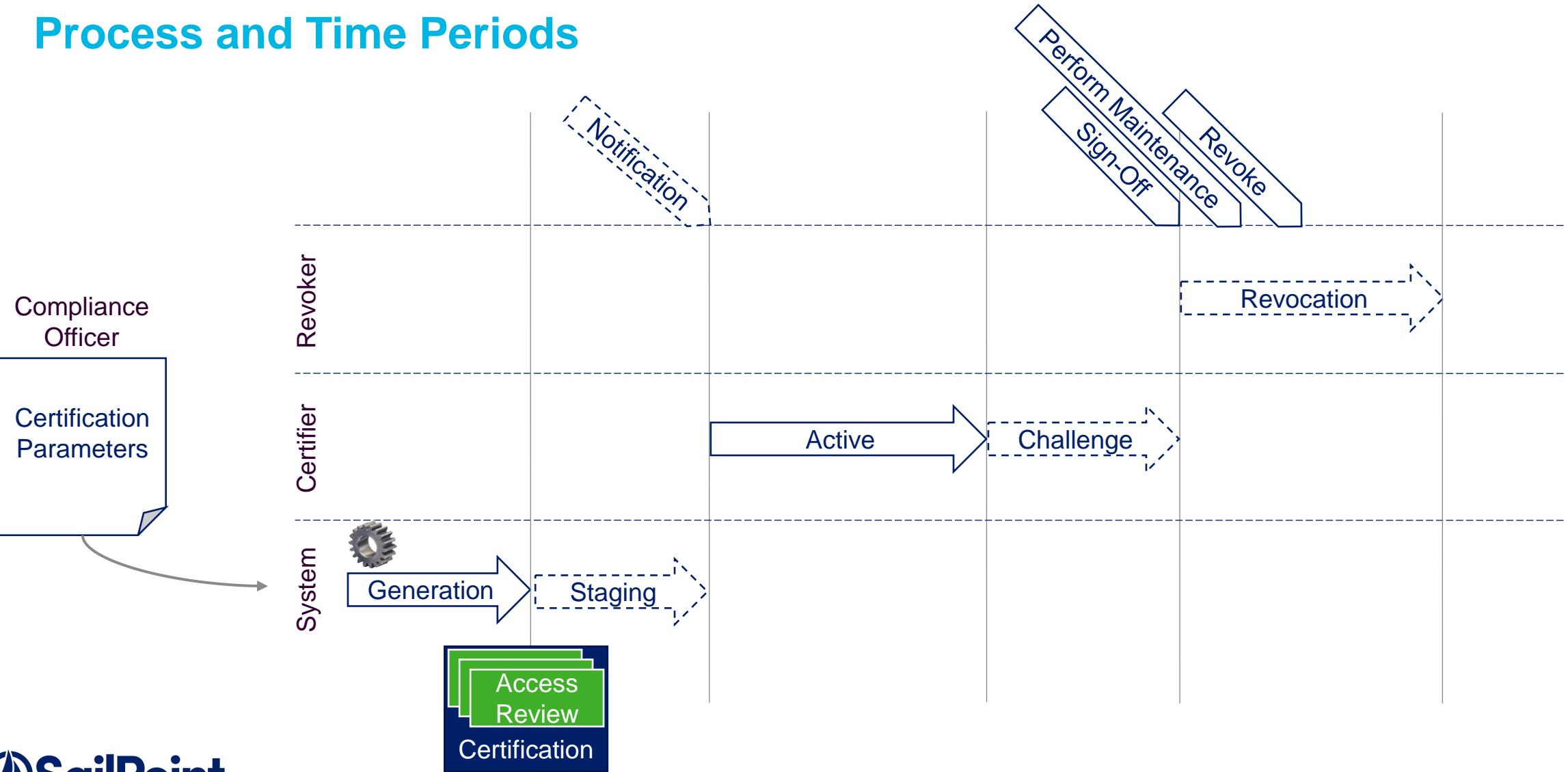
Certifications	
Manager Certification Finance Apps	[11/22/13 10:22:11 AM CST]
Application Owner Certification	[11/21/13 1:38:11 PM CST]
Department Transfer: Aaron.Michols	
Manager Certification [10/30/13]	1:36:18 AM CDT

Access Reviews	
Manager Access Review for James Smith	0% (0 of 14)
Manager Access Review for John Williams	0% (0 of 8)
Manager Access Review for David Ander...	0% (0 of 5)
Manager Access Review for Elizabeth Ta...	0% (0 of 9)
Manager Access Review for Jennifer Tho...	0% (0 of 5)

Access Review Details			
Deborah	Collins	Role	Region.Americas
Gary	Stewart	Role	Region.Americas
Jason	Parker	Role	Region.Americas
Kimberly	Evans	Role	Region.Americas
Matthew	Edwards	Role	Region.Americas

# Certification Lifecycle

## Process and Time Periods



# Certification Configuration

---

## Rules (Supplied by Implementation Team)

- Certification Control
  - Exclusion Rule
  - Pre-Delegation Rule
  - Sign Off Approver Rule
- Time Period Rules
  - Active Period Enter Rule
  - Challenge Period Enter Rule
  - Revocation Period Enter Rule
  - End Period Rule
  - Closing Rule
- Escalation
  - Escalation Rule for Expirations and Revocations

# Trigger Certifications

---

- Multiple options for triggering certifications

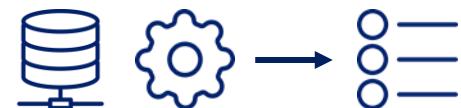
- Manual creation



- Scheduled, recurring



- Data changed, triggering Certification Event



# AI Recommendations in Certifications

Application Owner Access Review for Procurement\_System

Open 420 Review 2

Bulk Decisions ▾ Columns ▾ Group By Filter ▾ Recommendations

Type	Display Name	Description	Application	Account Name	Identity	Department	MGR Department	Decision
Role	RACF Security Administrator - IT	Evaluates and researches current and new security controls and implementations within RACF. Supports... Read more	Procurement_System	Martin Matthews	Information Technology	Information Technology	<span>Approve</span> <span>Revoke</span>	
Entitlement	ACME05 on Groups	Reporting activities	Procurement_System	10375	Aaron Townsend		<span>Approve</span> <span>Revoke</span>	
Entitlement	CICS00 on Groups	CICS region designation, allow IT to designate	Procurement_System	10375	Aaron Townsend		<span>Approve</span> <span>Revoke</span>	
Entitlement	CICS00 on Groups	CICS region designation, allow IT to designate	Procurement_System	1a2a3a4a	Joseph Thompson	Information Technology	<span>Approve</span> <span>Revoke</span>	
Entitlement	CICS01 on Groups	CICS region designation, allow IT to designate	Procurement_System	1a2a3a4a	Joseph Thompson	Information Technology	<span>Approve</span> <span>Revoke</span>	
Entitlement	CICS10 on Groups	CICS region designation, allow IT to designate	Procurement_System	1a2a3a4a	Joseph Thompson	Information Technology	<span>Approve</span> <span>Revoke</span>	

**Not Recommended**

Only 50.00% of identities of similar users have this access.

Approve Revoke

Approve Revoke

# Certification Demonstration

# Knowledge Check

# Practice Exercises

# Exercise Preview

---

## Section 3, Exercise 5

- Certify Access
  - Generate targeted certification
  - Perform access review





# Introduction to Roles

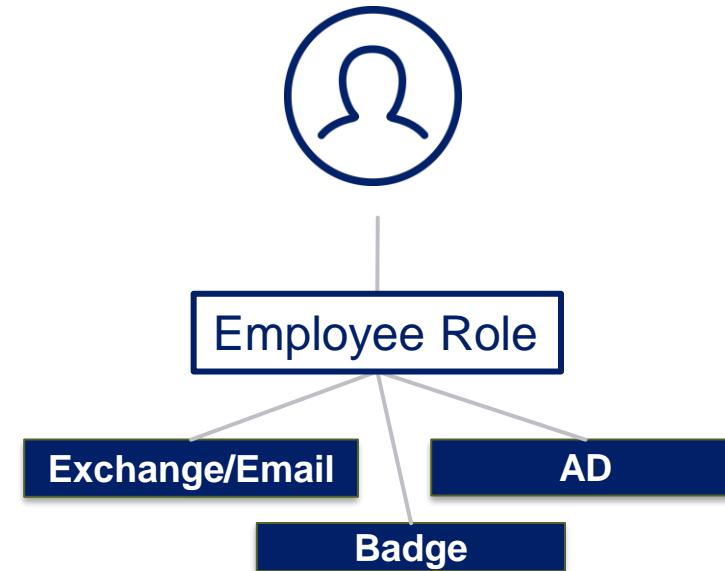
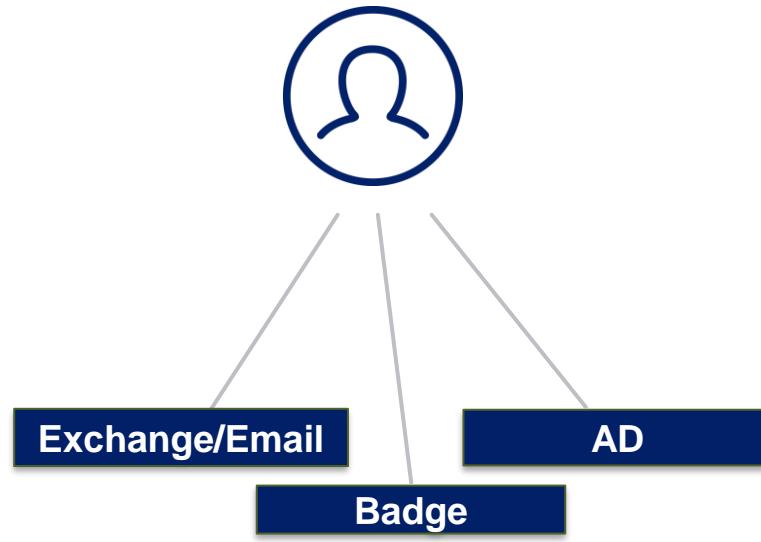
IdentityIQ Essentials

# Role

---

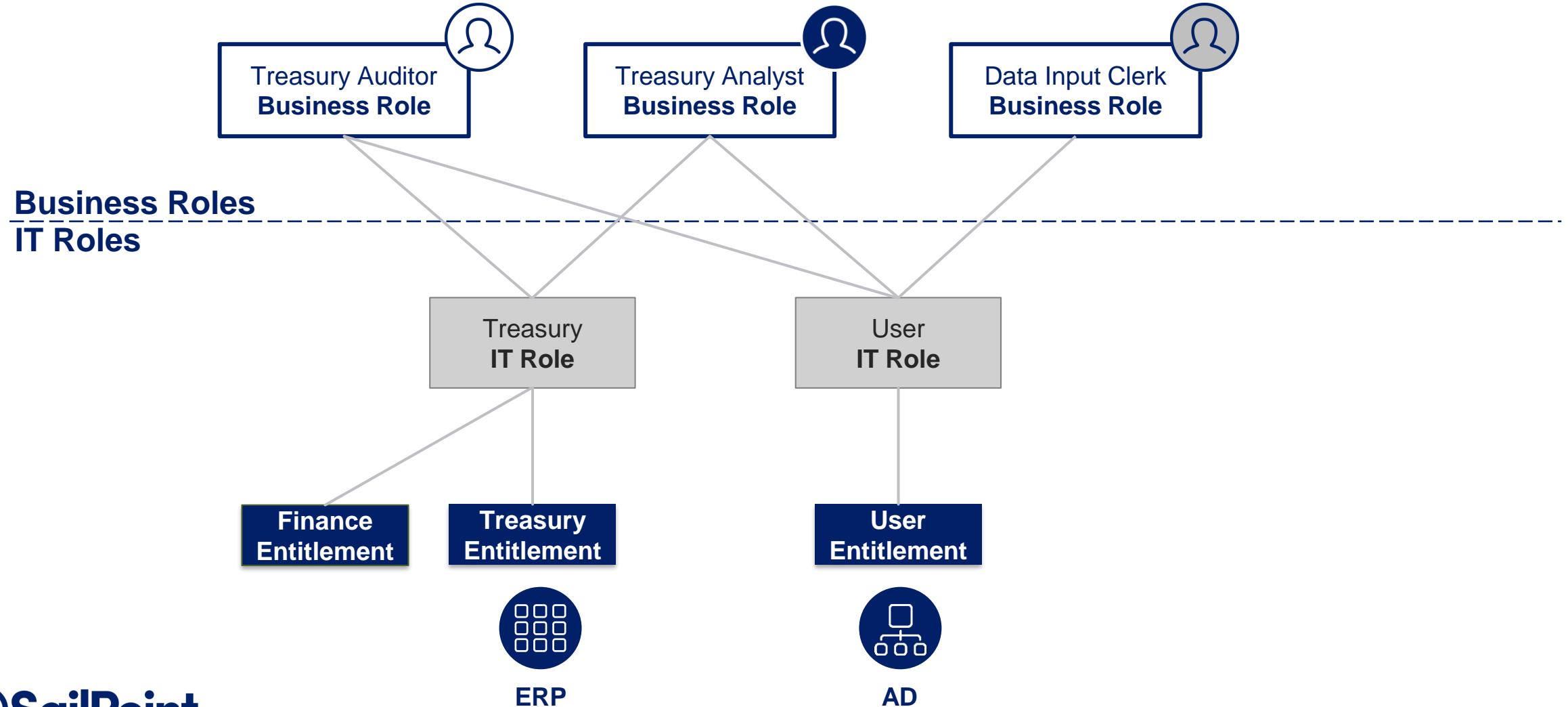
## Definition (Review)

- An object that encapsulates sets of access
  - Regulate and provision access to resources based on roles of each user



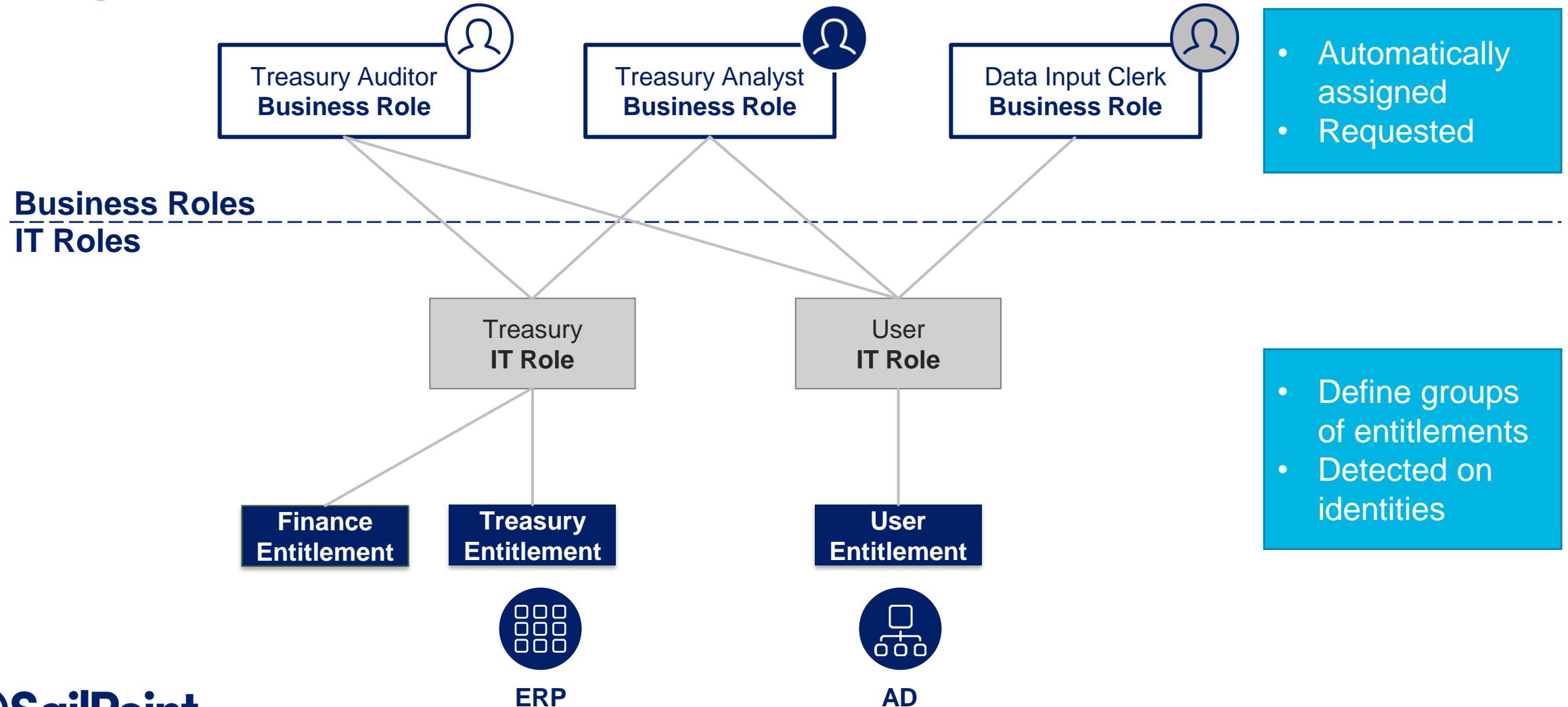
# IdentityIQ Two Tier Role Model

## IdentityIQ Default

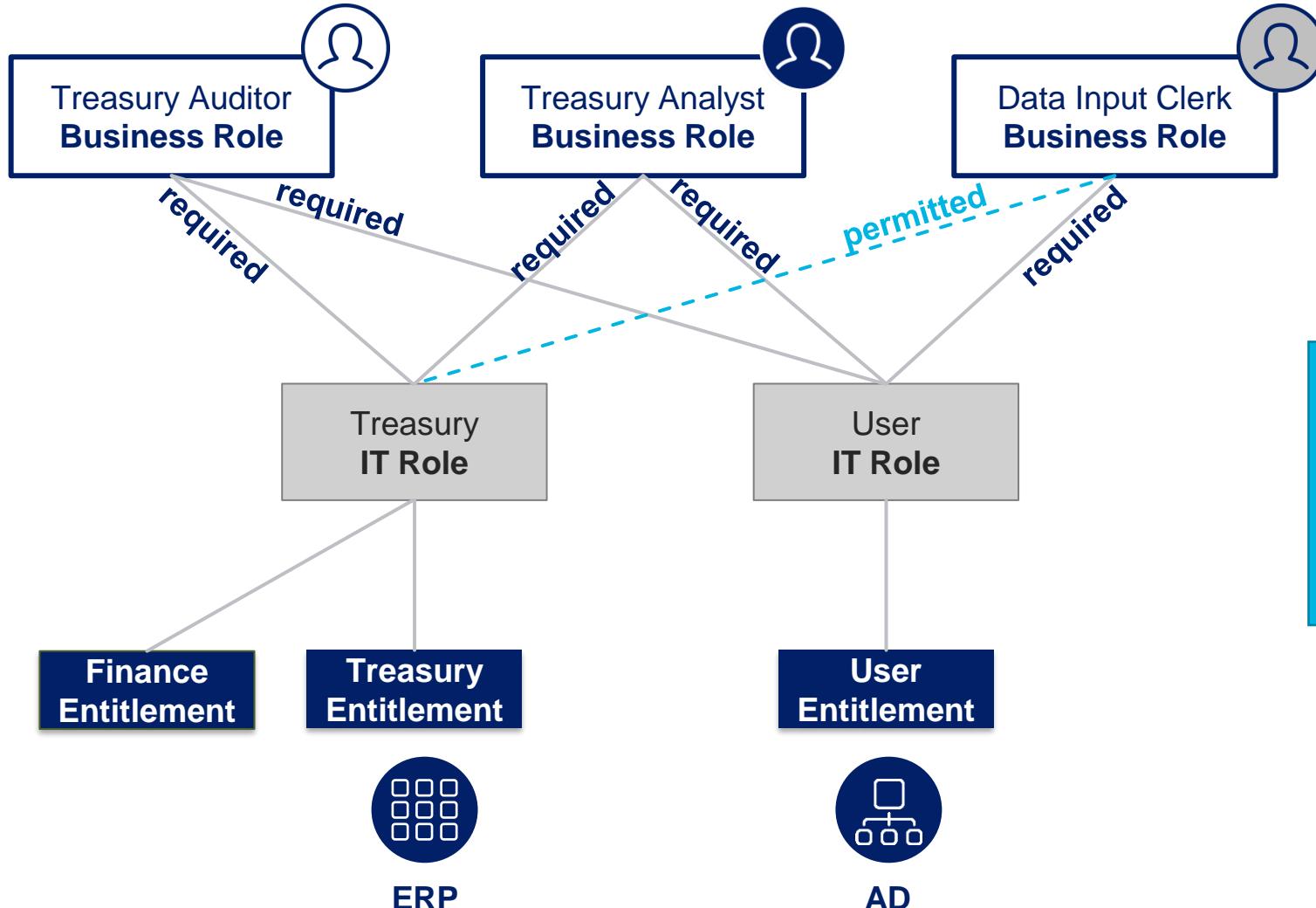


# IdentityIQ Two Tier Role Model

## Usage



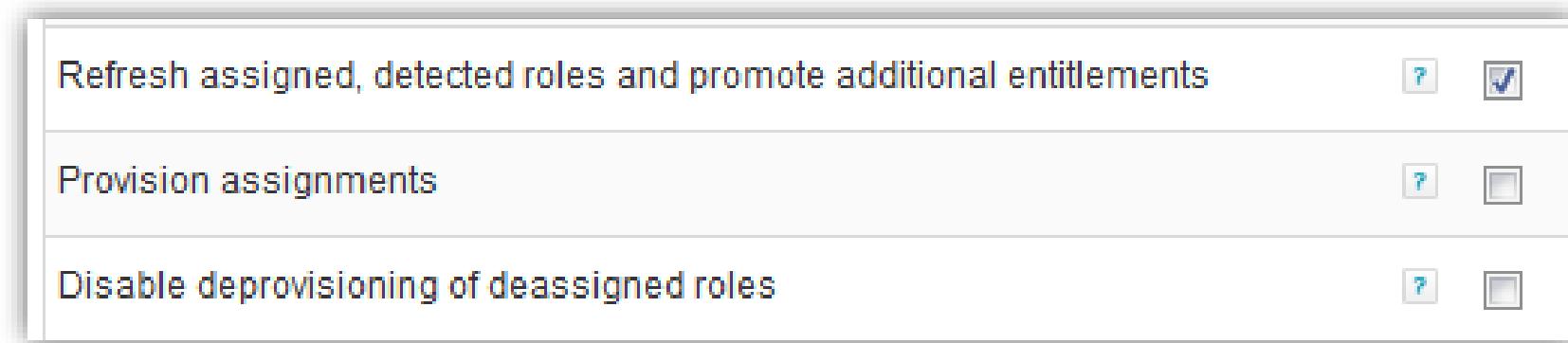
# Required and Permitted Relationships



# Assigning and Detecting Roles

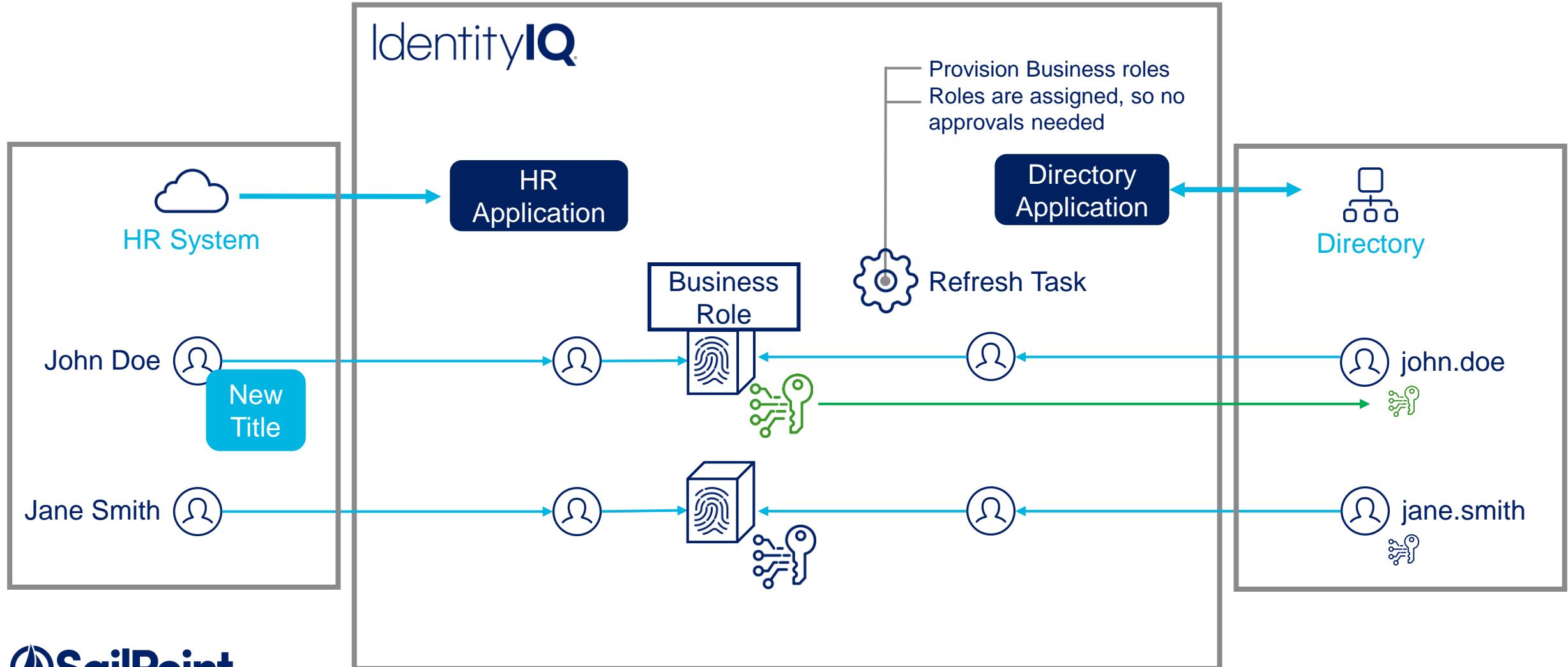
## Identity Refresh Task

- “Refresh assigned, detected roles...”
  - Processes assignment rule defined in business role
  - Detection defined through an IT Role Profile
- Optionally choose
  - “Provision assignments”
  - “Disable deprovisioning...”



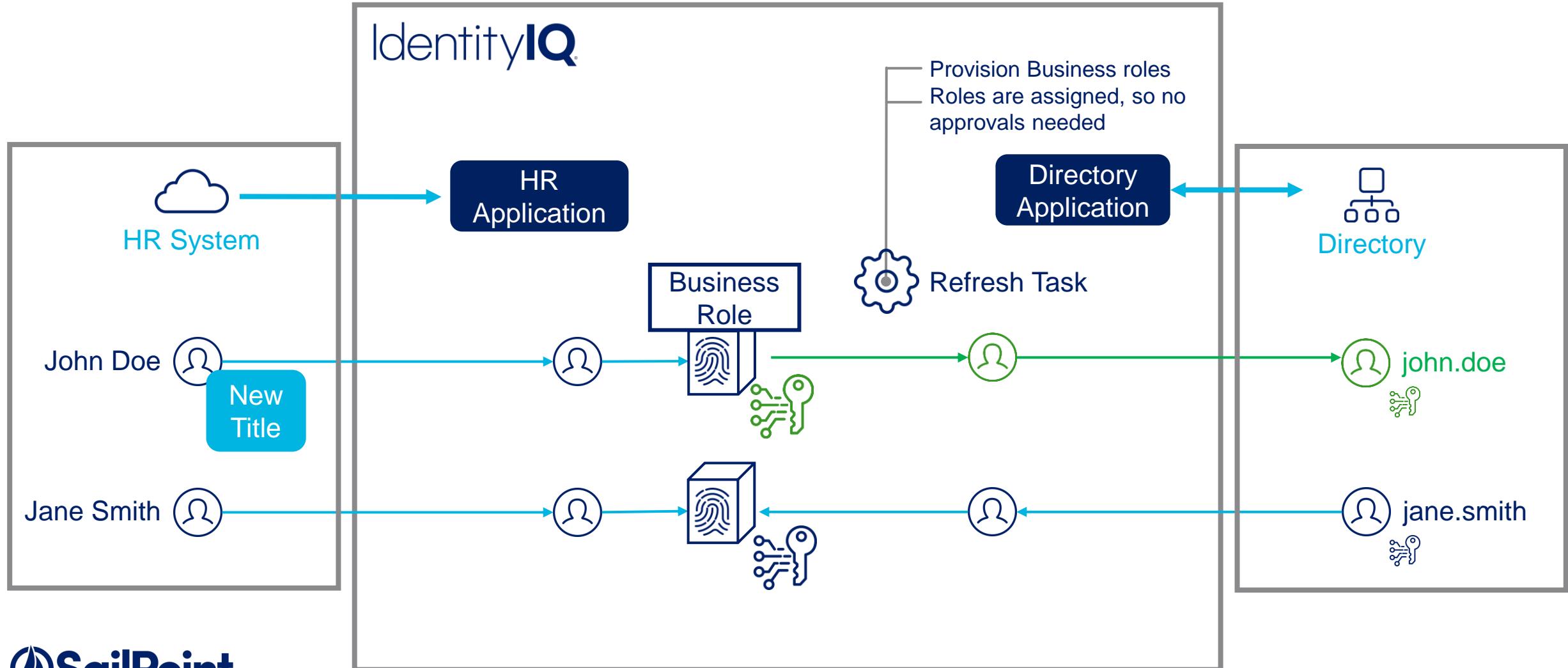
# Automated Role Provisioning

## Illustration



# Automated Role Provisioning

## Account Provisioning

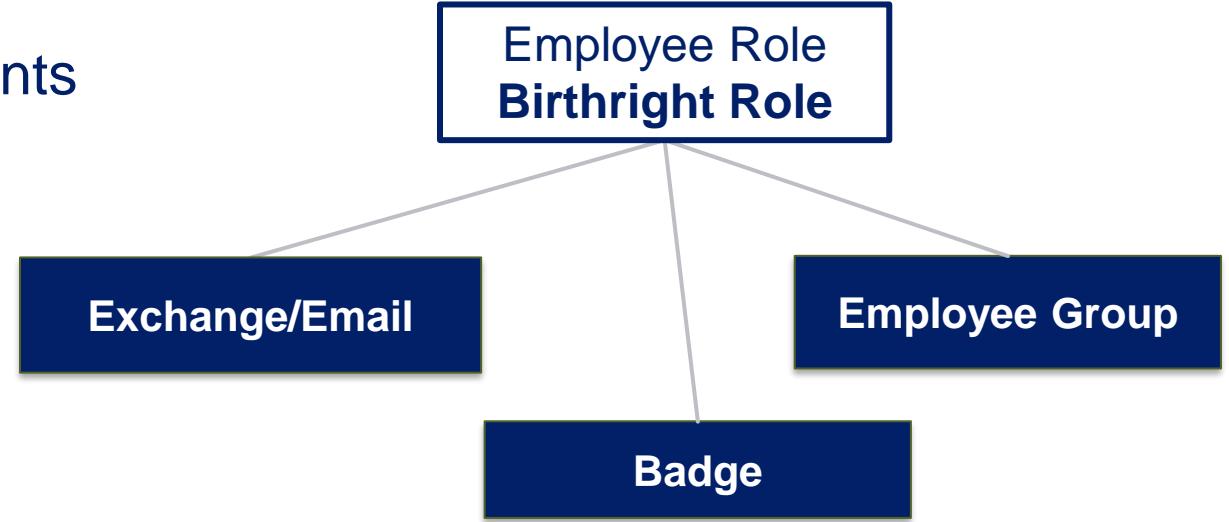


# Birthright Roles

---

## Rapid Setup

- Only assigned during joiner lifecycle events
- Not requestable
- Single tier role model



# Birthright versus Business Roles

---

## Birthright Roles

- Baseline access, assigned to new personnel
- Only assigned during joiner lifecycle events
- Not requestable
- Single tier

## Business Roles

- Access for teams, departments, projects, etc.
- Assigned by Identity Refresh task, “Refresh assigned, detected roles...”
- Requestable
- Two-tier: required and permitted relationship with IT roles

# Role Extension Options

---

## Beyond the Default Role Model

- Extended attributes
  - Support business-specific governance or provisioning requirements
- Different role types
  - Address business-specific requirements
  - Manage IdentityIQ capabilities

# Knowledge Check

# Practice Exercises

# Exercise Preview

---

## Section 3, Exercise 6

- Explore Business, IT, and Birthright Roles
  - Import Business and IT Roles
  - Assign and Detect Roles
  - Review Provisioning Activity
  - Create Birthright roles





# Provisioning Overview

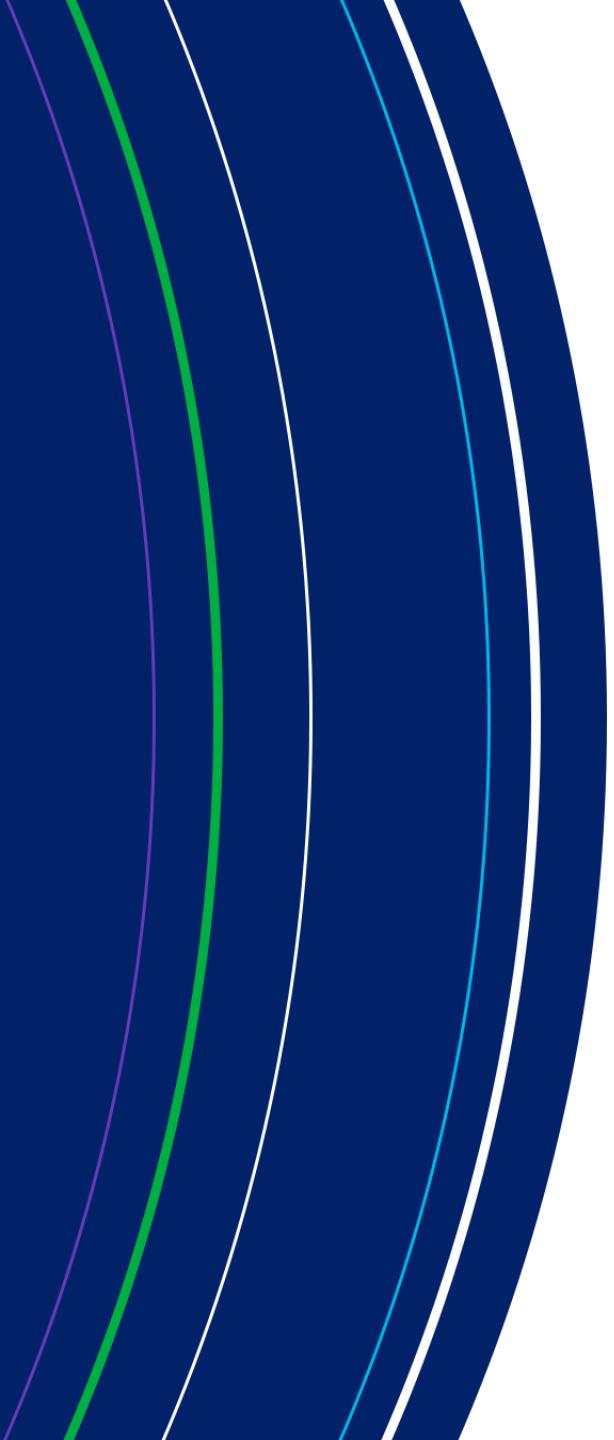
IdentityIQ Essentials

# Overview

---

## Provisioning Overview

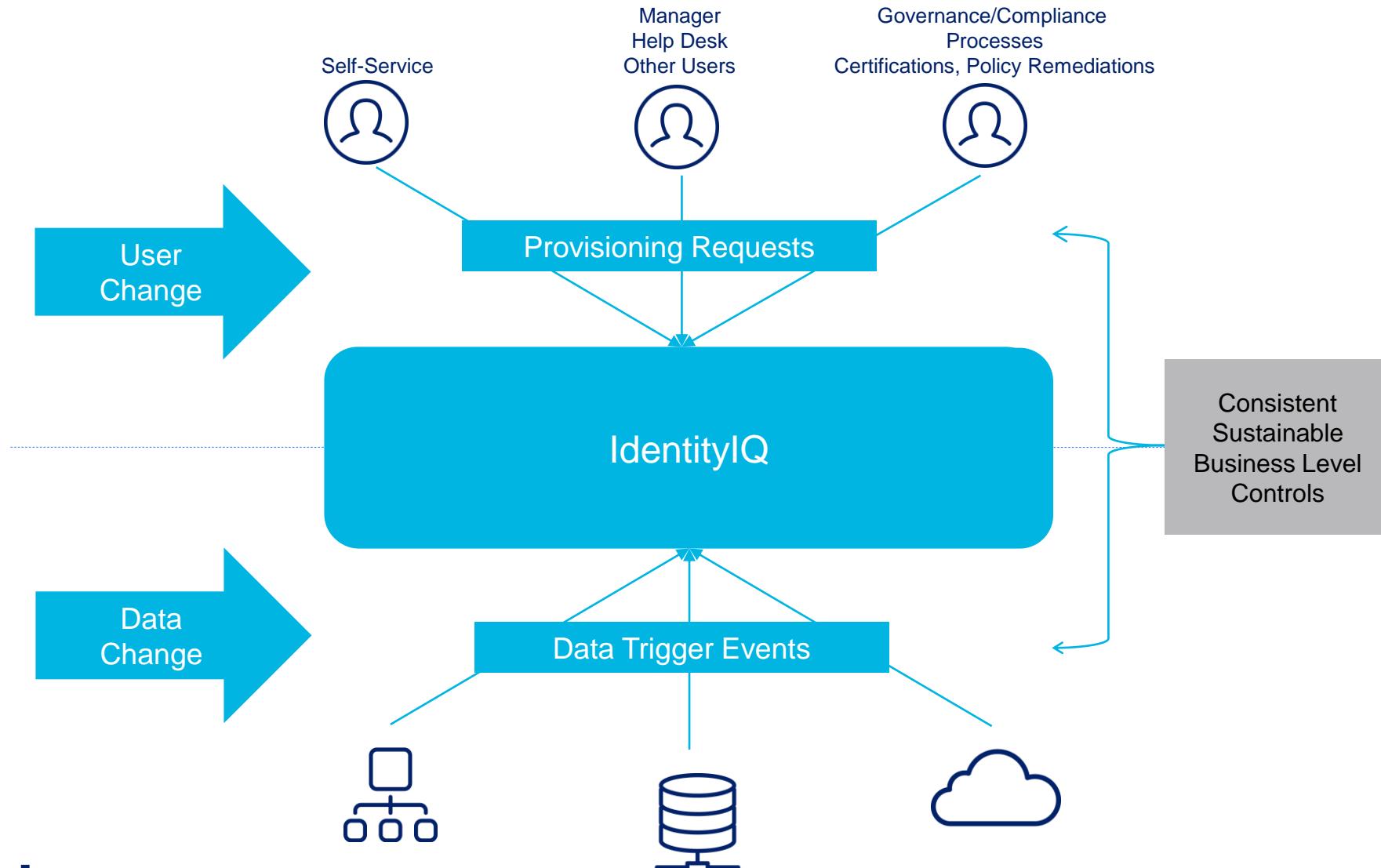
- Provisioning overview
  - What causes provisioning to occur?
  - How does IdentityIQ process provisioning requests?
  - What are the available provisioning channels?
- Provisioning configuration
  - Provisioning policies
  - Provisioning dependencies on accounts or entitlements



# Provisioning Overview

# Provisioning: Adding, modifying, or deleting user or access data

# Identity Change Lifecycle



# Manage the Fulfillment

---

## Supported Write Channels

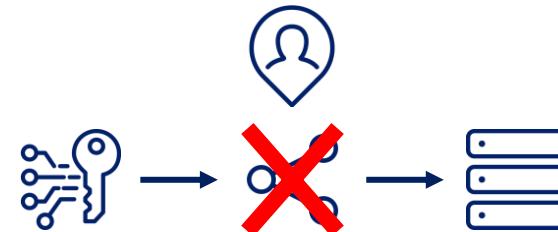
- Multiple channels available
  - Automated with direct connectors
  - Semi-automated with 3<sup>rd</sup> party integration
  - Manual with user-assigned work items



# Provisioning Channel

## Controlling Provisioning

- Most connectors can read and write
- Force provisioning via manual work item
  - Ex: JDBC connectivity not fully implemented (missing JDBC Provisioning Rule)



Object Editor - Application : Chat

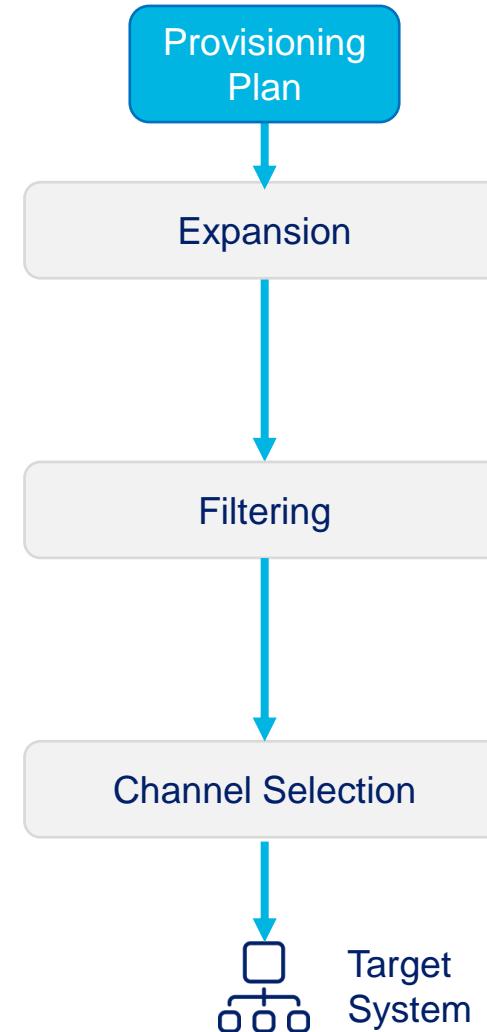
```
<?xml version='1.0' encoding='UTF-8'?>
<!DOCTYPE Application PUBLIC "sailpoint.dtd" "sailpoint.dtd">
<Application connector="sailpoint.connector.JDBCConnector" created="1559341038837" featuresString="DISCOVER_SCHEMA, PROVISIONING, SYNC_PROVISIONING">
<Attributes>
<Map>
<entry key="SQL" value="select * from users;"/>
<entry key="acceleratorPackEnabled" value="TRUE"/>
<entry key="accountCorrelationAttrExpression" value="displayName#IIQCorrelated#login#IIQCorrelated#EQUALS"/>
<entry key="accountCreateConditionalRule"/>
<entry key="accountCreateEntitlements"/>
<entry key="accountDisableAttrExpression" value="status#IIODisabled#I#IIODisabled#EQUALS"/>
```

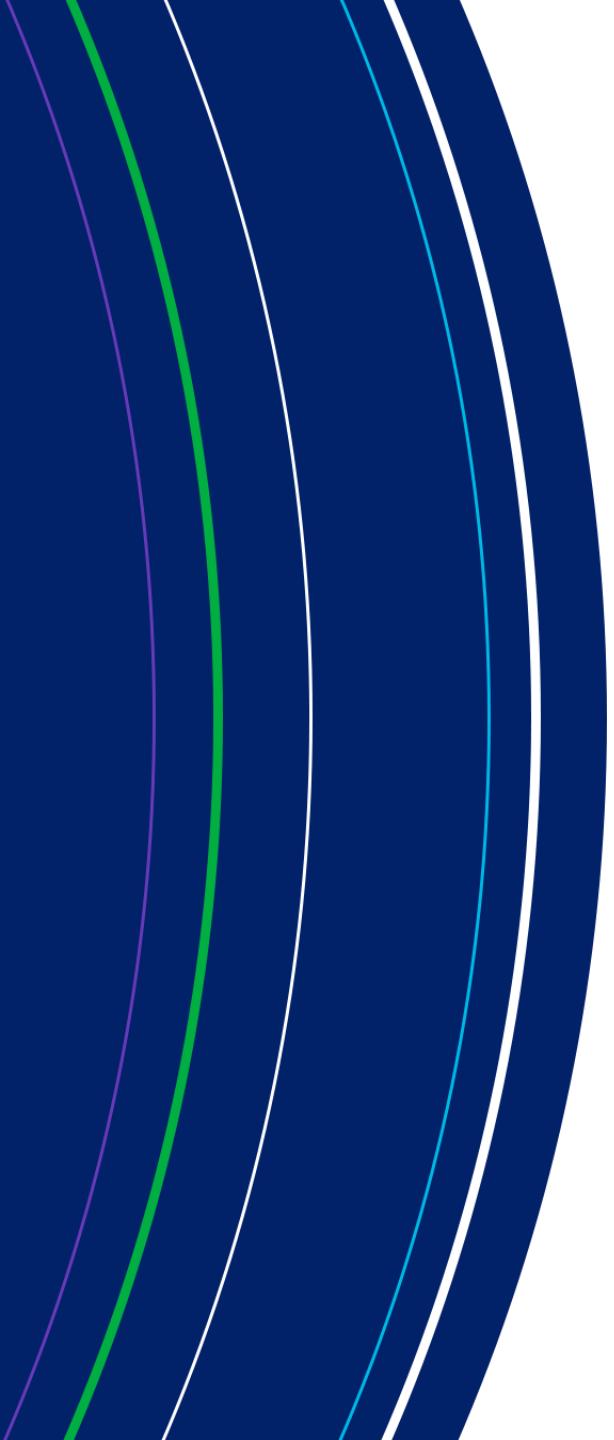
Debug Pages → Application

# Provisioning Process

## Provisioning Engine Features

- Expansion
  - Understanding plan requirements
    - Roles → entitlements
    - Account creation
- Filtering
  - Understanding existing identity access
- Channel Selection
  - Determining provisioning pathway





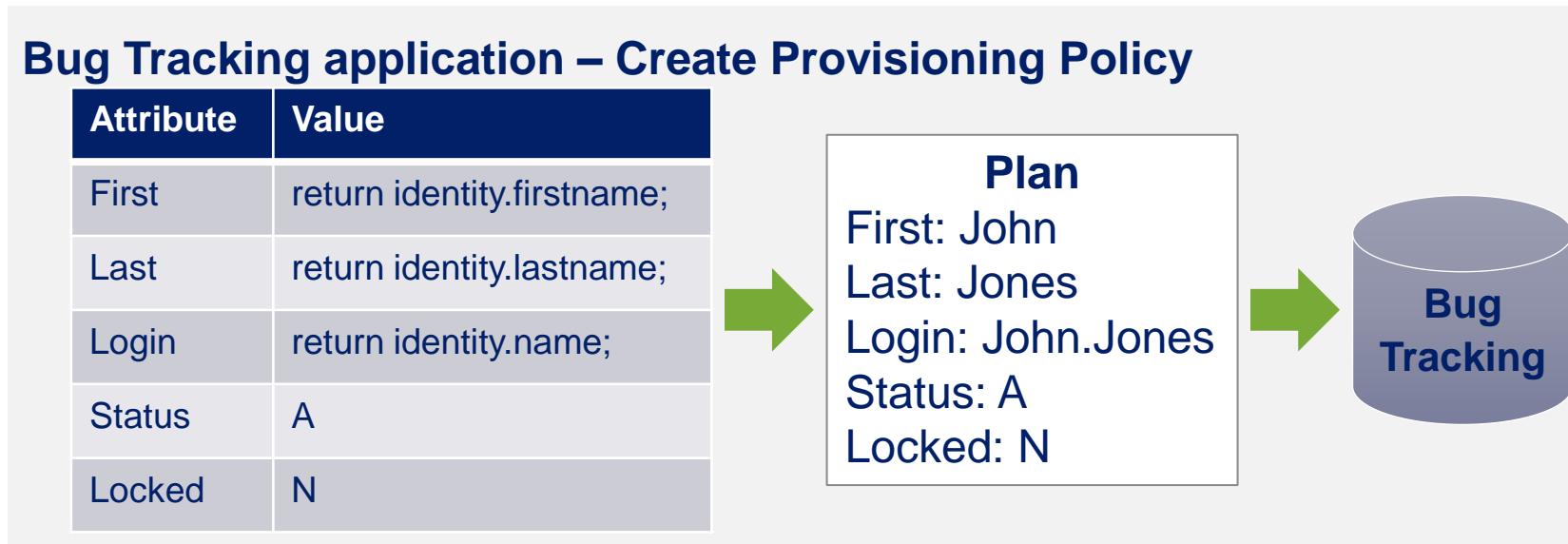
# Prepping for Provisioning

# Provisioning Policies

## Overview

- Provide values to **create**, **update**, and **delete** accounts on connected applications
  - Values can be provided manually by user
  - Values can be provided by IdentityIQ (auto-calculated or static)

Example: Create an account on “Bug Tracking” application



# Provisioning Policies

## Configuration: Application Policies

- Support
  - Account *create*
    - Most important policy
    - Often predefined with connector
  - Account *update, delete, enable, disable, unlock, and password change*
  - Group *create and update*  
(if groups are supported by connector)
- *Create* often predefined

### Edit Application PRISM

Details	Configuration	Correlation	Acc
Settings	Schema	Provisioning Policies	
A list of provisioning policies associated with this application			
<b>Object Type: account</b>			
Type	Name		
Create	PRISM		
Update	PRISM		
Delete			
Enable Account			
Disable Account			
Unlock Account			
Change Password			

# Provisioning Policies

## Form Editor

The screenshot shows the SailPoint Form Editor interface. At the top, there's a navigation bar with icons for Home, Search, User Management, Provisioning, Policies, and Help. Below the navigation, the main title is "Provisioning Policies". Underneath that, the section "Form Editor" is highlighted in blue.

The main area displays a form configuration. On the left, there's a table titled "Section 1" with six rows: "First Name", "Last Name", "Login ID", "Status", and "Account Locked". To the right of the table is a "Edit Options" panel. A red box highlights the "Edit Options" button for the "Login ID" row. A blue arrow points from the "Value Settings" section below to the "Edit Options" panel, indicating a relationship between them.

The "Value Settings" section contains a "Dynamic" checkbox and a "Value" section. The "Value" section is also highlighted with a red box and contains a "Script" dropdown and a text area with the code "return identity.name;".

The "Edit Options" panel is divided into sections: "Settings", "Name" (containing "Field 3"), "Display Name" (containing "Login ID"), "Help Text" (empty), "Type" (set to "String"), "Type Settings" (dropdown), and "Value Settings" (dropdown). A large red box surrounds the entire "Edit Options" panel. At the bottom right of the "Edit Options" panel is a blue "Apply" button.

# JDBC Provisioning

## Provisioning Policy

The screenshot shows the 'Time Tracking' form definition. It includes sections for 'Add Section' and 'Preview Form'. On the left, there's a table with columns for 'Section 1' and several fields: First Name, Last Name, Username, Status, Locked, and Employee ID. The 'First Name' field is highlighted with a red box. To the right is the 'Edit Options' panel with tabs for 'Settings', 'Display Name', 'Help Text', 'Type', 'Type Settings', and 'Value Settings'. Buttons for 'Apply' and 'Save' are at the bottom.

## Provisioning Rule

The screenshot shows the 'Rule Editor' for a JDBC provisioning rule named 'Time Tracking - Provision'. The 'Rule Type' is set to 'JDBCProvision' and the 'Return Type' is 'ProvisioningResult'. The 'Arguments' section lists 'log', 'context', 'application', and 'schema'. The 'Returns' section lists 'result'. The main area contains Java code for a 'CREATE' operation:

```
// CREATE Operation
//
System.out.println("Account Request Operation = Create");

PreparedStatement statement = connection.prepareStatement("insert into
users (id,firstname,lastname,capability,status,locked,username) values (?,?,?,?,?,?)");
statement.setString(1, (String) account.getNativeIdentity());
statement.setString(2, getAttributeRequestValue(account, "firstname"));
statement.setString(3, getAttributeRequestValue(account, "lastname"));
statement.setString(5, getAttributeRequestValue(account, "status"));
statement.setString(6, getAttributeRequestValue(account, "locked"));
statement.setString(7, getAttributeRequestValue(account, "username"));

//
// Grab the role from the request. If it's a single role, it'll be a string, add it to
// the statement, other wise if it's a List, convert to CSV and add it to the
//
AttributeRequest attrReq = account.getAttributeRequest("capability");
if (attrReq != null) {
    if (attrReq.getValue() instanceof String) {
        statement.setString(4, (String) attrReq.getValue());
    } else if (attrReq.getValue() instanceof List) {
        String listOfRoles = Util.listToCsv((List) attrReq.getValue());
        statement.setString(4, listOfRoles);
    }
} else {
    statement.setString(4, "");
}
```

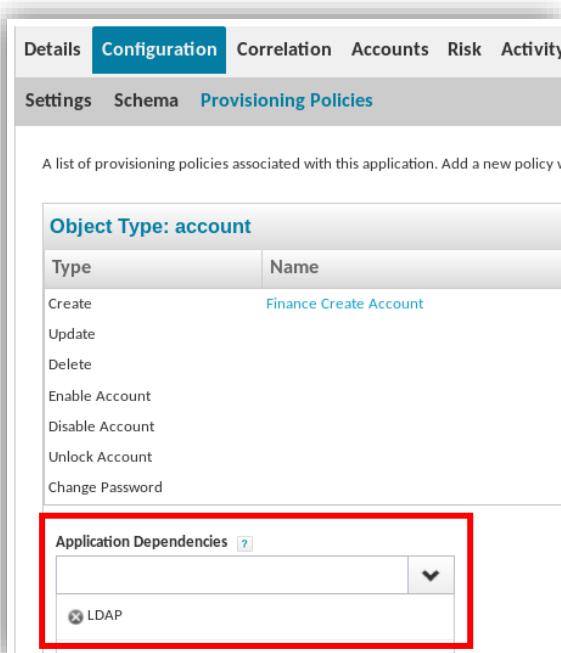
**Description**  
A Provisioning rule for the Time Tracking application. Handles Account Creates/Deletes/Modifies /Unlocks/Enables/Disables

Buttons at the bottom include 'Save', 'Save As...', and 'Cancel'.

# Provisioning Dependencies

## Dependency on Account

- Dependencies on direct-connected applications only
- Pull account attribute values from master application attributes



Application → Configuration → Provisioning Policies

The screenshot shows the 'Value Settings' dialog for a provisioning policy. It has sections for 'Value' (set to 'Dependent'), 'Application' (set to 'LDAP'), 'Attribute' (set to 'dn'), 'Allowed Values' (set to 'None'), and 'Validation' (set to 'None').

Finance Account Create Policy → Field → Value Settings

# Knowledge Check

# Practice Exercises

# Exercise Preview

---

## Section 4, Exercise 1

- Exercise 1: Configure applications to support provisioning actions
  - Define provisioning policies
  - Set provisioning rules for JDBC applications
  - Configure Account Dependency





# Monitoring Provisioning

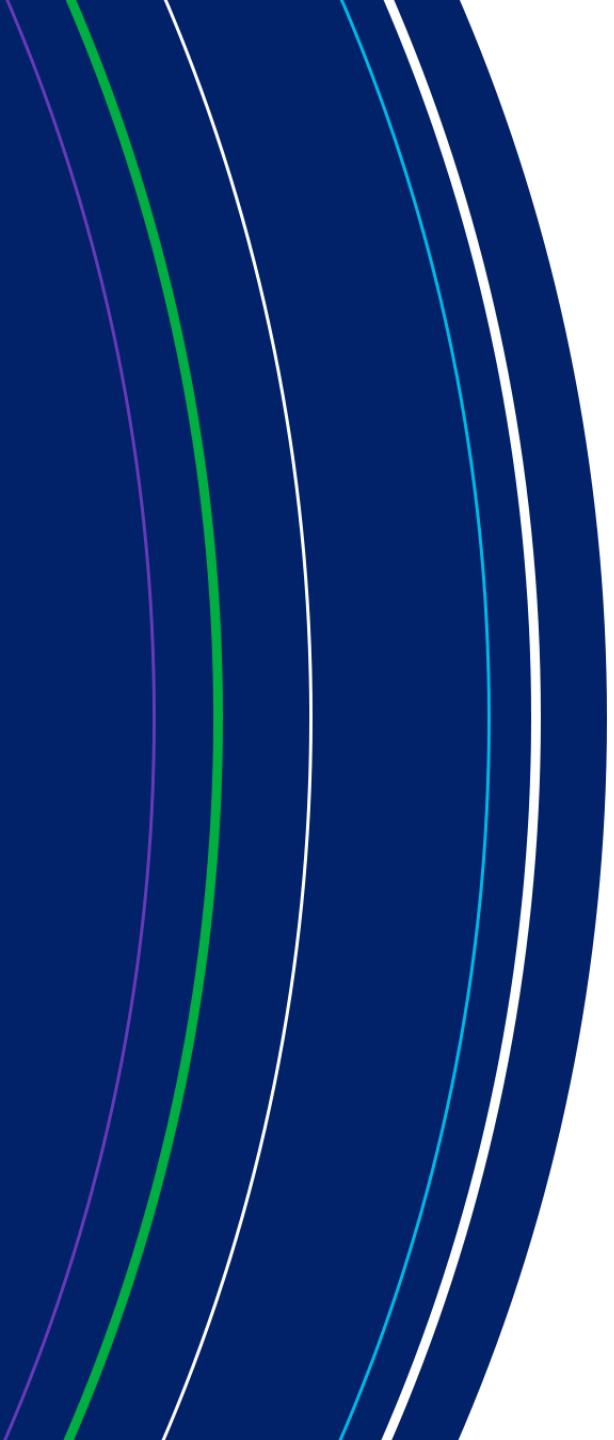
IdentityIQ Essentials

# Overview

---

## Monitoring Provisioning

- Administrator Console, Provisioning
- Workflows
  - WorkflowCase
  - WorkItem



# **Administrator Console Provisioning**

# Provisioning Transactions Page

- Override to convert automated transaction to manual workitem
- Retry to force next attempt for retry-enabled applications

Provisioning Transactions											Showing 1-10 of 80
ID	Event	Application	Identity	Account	Source	Type	Channel	Date	Status	Actions	
80	Modify	LDAP	Luis.Castillo	Luis.Castillo	LCM	Auto	LDAP	4/4/17 1:49 PM	Pending	<span>Info</span> <span>Retry</span>	
79	Create	TRAKK	Donald.John	Donald.John	LCM	Manual	Work Item	4/3/17 9:24 AM	Success	<span>Info</span>	
78	Create	TRAKK	Donald.John	Donald.John	LCM	Auto	TRAKK	3/31/17 12:46 PM	Failed	<span>Info</span> <span>Override</span>	

Gear → Administrator Console → Provisioning

# Provisioning Transactions Page

## Configuration

**Provisioning Transaction Log Settings**

Enable Provisioning Transaction Log

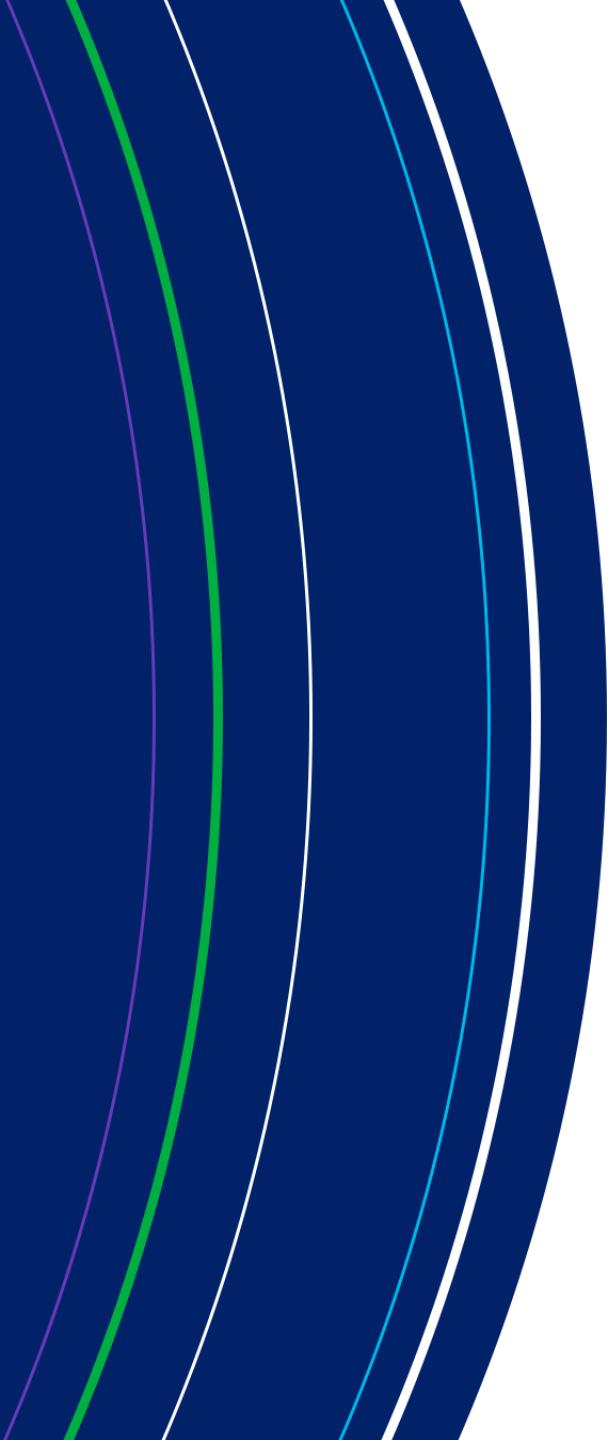
Maximum Log Level

Days before provisioning transaction event deletion

Global Settings → IdentityIQ Configuration → Miscellaneous

- Set log level (Success, Retry, or Failure)
- Default setting = Failure

- Set to non-zero
- Default is no purge



# Workflow Monitoring

# Workflow Execution

## WorkflowCase Object

- Created when action in IdentityIQ triggers a workflow
- Contains details for a running workflow process
  - Launcher, type of workflow, copy of the workflow, current step being processed, info about target objective, etc.
- Exists only until workflow completes



# Workflow Status

### Task Result

**Details**

Name	Update Identity Tammy.Daniels AccessRequest	Started By	Catherine.Simmons
Type	LCM	Started	2/21/14 2:32:26 PM
Description	Workflow Case	Completed	
Status	pending...		

[Return to Tasks](#)

**Current Workflow Step:** Approve

### Interactions

Owner	Type	Request	Status	Started	Completed
Randy.Knight	Approval	Owner Approval - Account Changes for User: Tammy.Daniels	Open	2/21/14 2:32:28 PM	

### Debug Pages

#### Object Browser

WorkflowCase

Filter by Name or ID  Configuration Objects

Id	Name	Created	Modified
ff80808143db395f0143e482d258033e	Native Change Detection LDAP: Allen.Bu...	1/30/14 12:56 PM	1/30/14 12:56 PM
ff8080814451375f0144562626d10071	Update Identity Denise.Hunt AccessReq...	2/21/14 2:32 PM	2/21/14 2:32 PM
ff8080814451375f0144562612790061	Update Identity Irene.Mills AccessRequest	2/21/14 2:32 PM	2/21/14 2:32 PM
ff8080814451375f014456261def0069	Update Identity Jeremy.Palmer AccessR...	2/21/14 2:32 PM	2/21/14 2:32 PM
ff8080814451375f0144562604460059	Update Identity Louis.Black AccessRequest	2/21/14 2:32 PM	2/21/14 2:32 PM
ff8080814451375f01445626313a0079	Update Identity Tammy.Daniels AccessR...	2/21/14 2:32 PM	2/21/14 2:32 PM
ff8080814451375f014465fa6e4100d7	Update Identity Tammy.Daniels Accounts...	2/24/14 4:18 PM	2/24/14 4:18 PM

# Workflow Execution

---

## WorkItem

- Created by a workflow (or IdentityIQ) to obtain input from a person
- Exists until the input is acquired
- Examples
  - Approvals
  - Policy violations
  - Request for manual provisioning
  - Access review delegations
  - Request for data

# Knowledge Check





# Rapid Setup Lifecycle Events

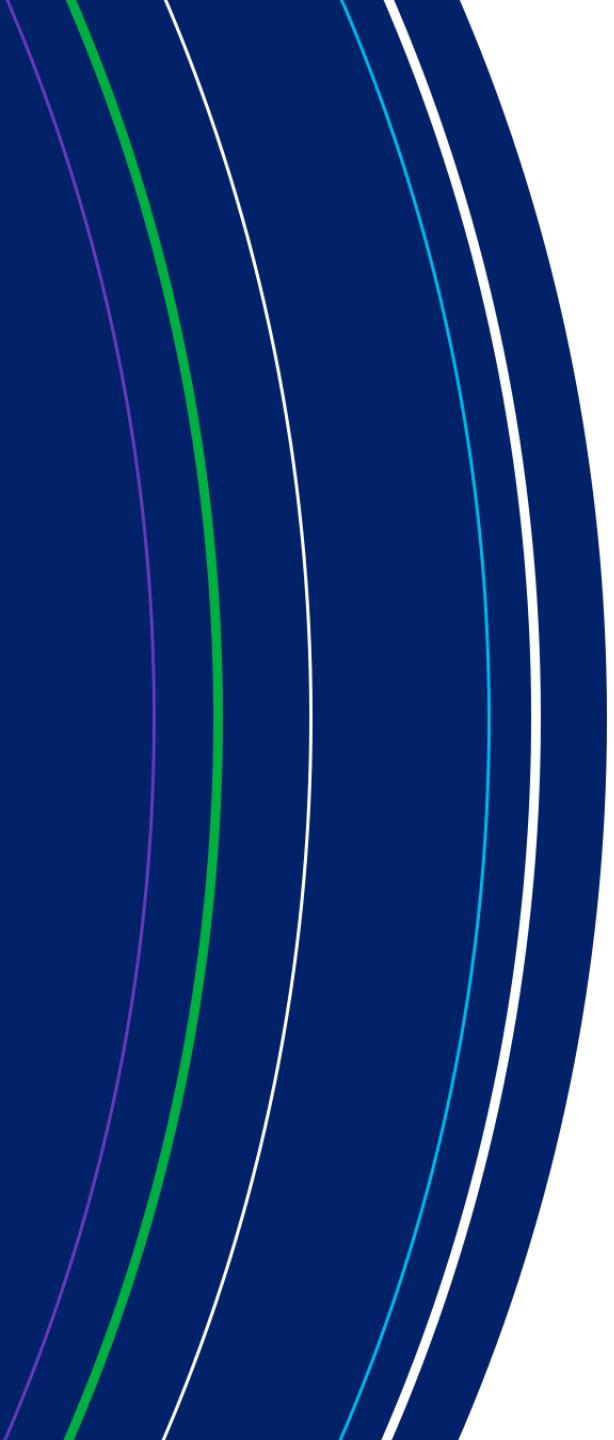
IdentityIQ Essentials

# Overview

---

## Lifecycle Events

- Lifecycle Event overview
- Rapid Setup Lifecycle Events
  - Joiner, Mover, Leaver



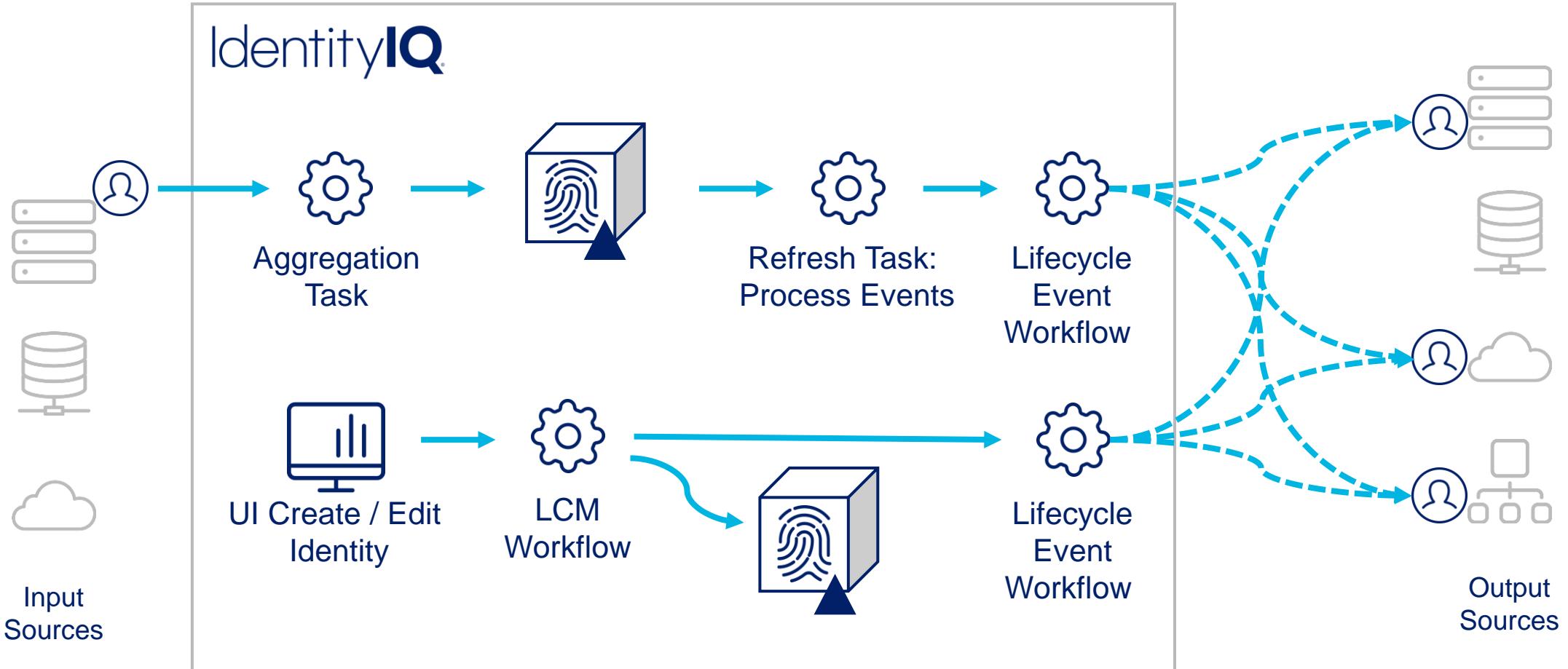
# **Lifecycle Event Overview**

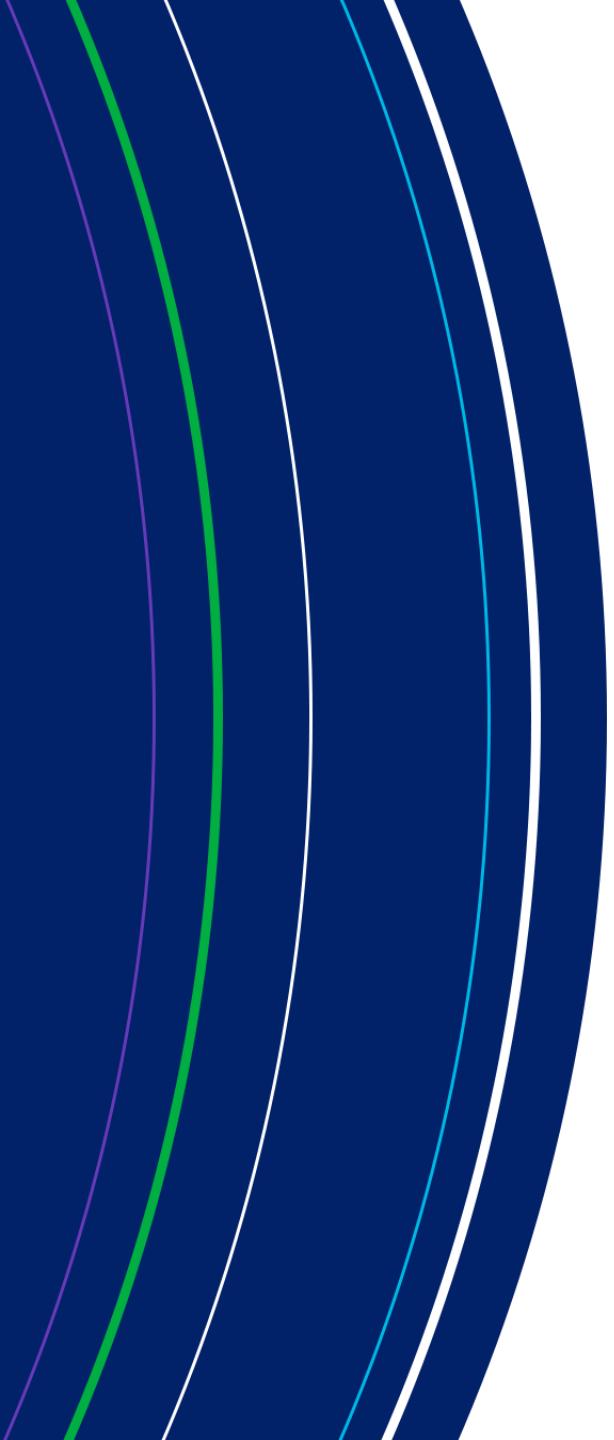
# Lifecycle Events Overview

---

- What are Lifecycle Events?
  - Activities that happen in the normal course of a person's employment
    - Joining the company (joiners)
    - Changing departments/managers (movers)
    - Leaving the company (leavers)

# Lifecycle Event Process





# **Rapid Setup Lifecycle Events**

# Rapid Setup Lifecycle Events

---

## Supported Options

- Joiner
  - Birthright role assignment
  - Application-specific account-creation
- Mover
  - Certification
  - Reprocess joiner
- Leaver
  - Disable, delete, move account
  - Remove entitlements
  - Scramble password
  - Immediate or time-delayed

# Rapid Setup Lifecycle Events

---

## Configuration Actions

- Define supporting objects
  - Birthright roles
  - Others: populations, workgroups, email templates, etc.
- Set up per-application actions
- Configure global settings
  - Event criteria
  - Global event actions

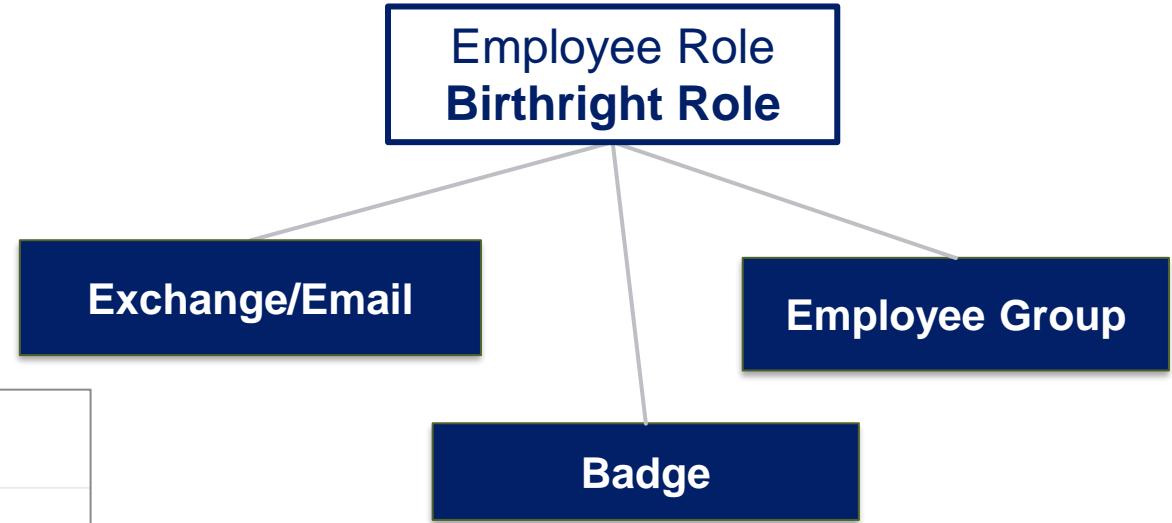
# Rapid Setup Joiner Event

## Rapid Setup Birthright Roles

- Assigned during joiner lifecycle events

Rapid Setup Configuration

Joiner	Mover	Leaver	Identity Operations	Miscellaneous
Role Types to Treat as Rapid Setup Birthright Roles				
<input type="text"/> rapidSetupBirthright <input type="button" value="X"/>				



Global Settings → Rapid Setup Configuration → Miscellaneous

# Rapid Setup Joiner Event

---

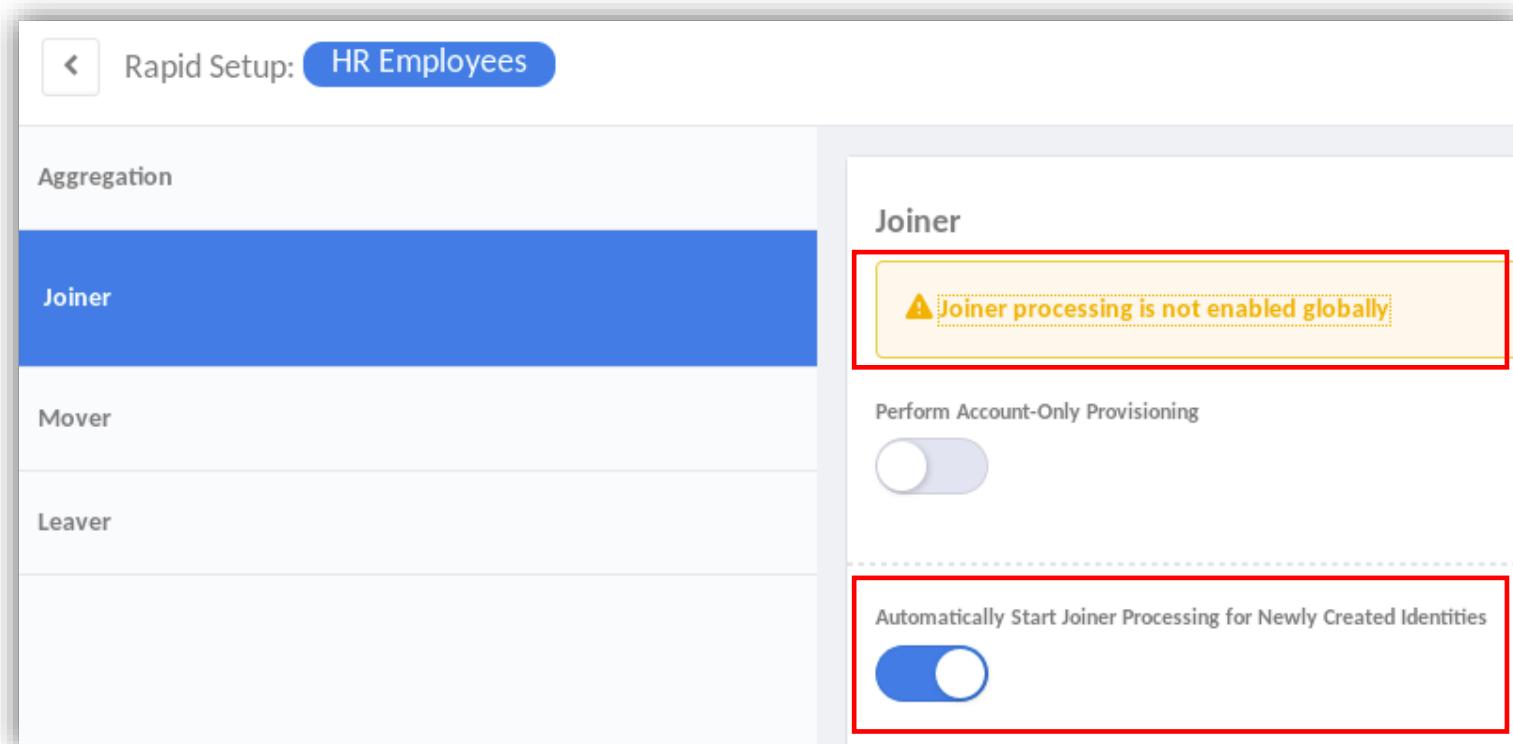
## Other Supporting Objects

- Populations – filtering option
- Workgroups
  - Granting access
  - Assigning responsibility
  - Sending notifications
- Email templates

# Rapid Setup Joiner Event

## Define Joiner Eligibility

- Specify which applications are sources for Joiner identities
- Usually authoritative applications



# Rapid Setup Joiner Event

## Application-specific Logic

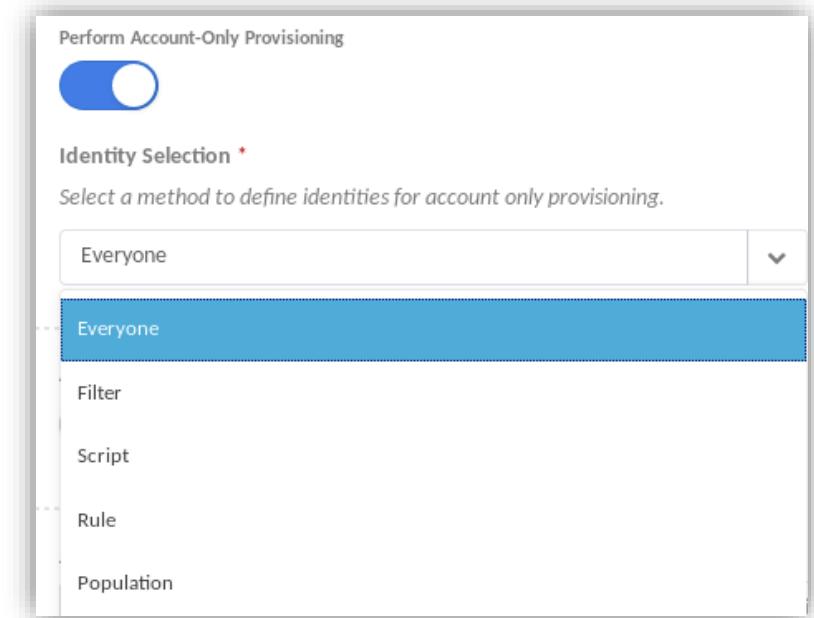
- Account-only provisioning
  - Identity Selection
    - Everyone
    - Selected Users
- App-specific instructions and password instructions in joiner emails

Joiner Email Instructions

This string is expanded and added to the end of the Joiner Completed Notification email sent to the manager.

Joiner Email Password Instructions

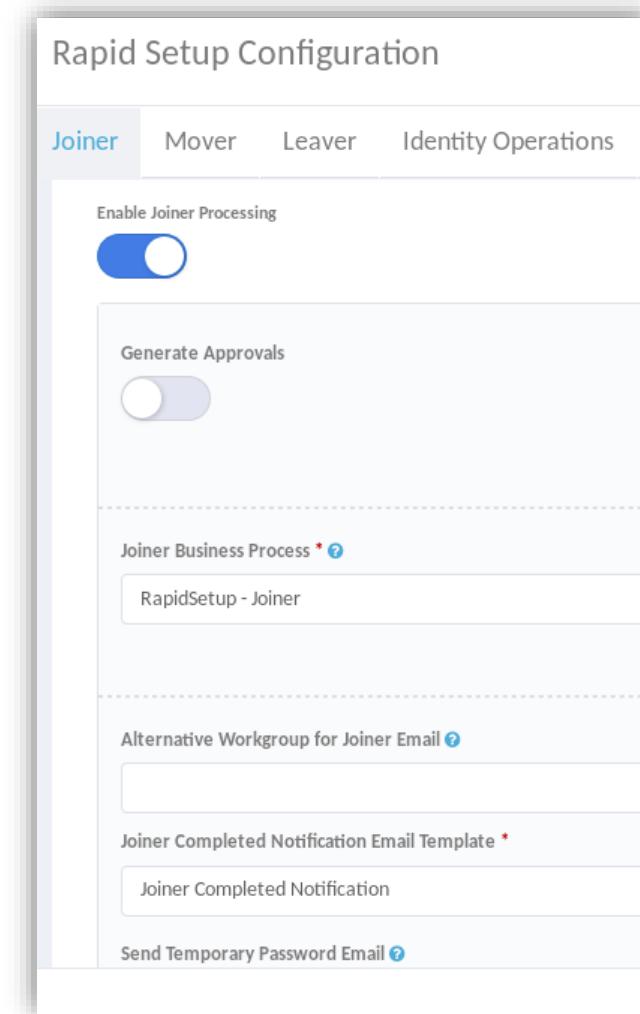
If defined, this string will be expanded in the Joiner Temporary Password Notification email to the manager. Th



# Rapid Setup Joiner Event

## Global Joiner Configurations

- Enable Joiner feature
- Approval requirements
- Business process
- Email notification
  - Workgroup vs. manager
  - Email templates
  - Password email
- Post Joiner Rule

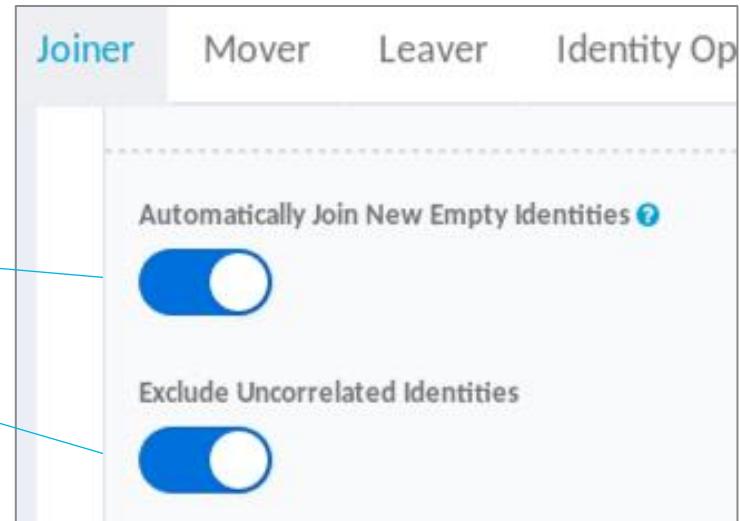


Global Settings → Rapid Setup Configuration

# Rapid Setup Joiner Event

## Global Trigger Controls

- Identity-source configurations
  - Trigger for IdentityIQ-created identities
  - Exclude uncorrelated identities (override)
- Trigger Filter
  - Limit joiners within aggregated identities



This screenshot displays the 'Trigger Filter' configuration. It uses an 'OR' logic operator. There are two rows of conditions. Each row consists of a 'Type' dropdown, a 'String' dropdown, an 'Equals' dropdown, and a value input field ('Employee' or 'Contractor'). Below the filter rows are buttons for '+ Add Row' and '+ Add Group'.

Global Settings → Rapid Setup Configuration → Joiner

# Rapid Setup Mover Event

## Define Mover Criteria

- Trigger Filter define criteria
  - Manager, department, job title changed (any or all)
  - Flag attribute set
  - Targeted: Region = Americas + job title change

Trigger Filter \* ⓘ

AND OR

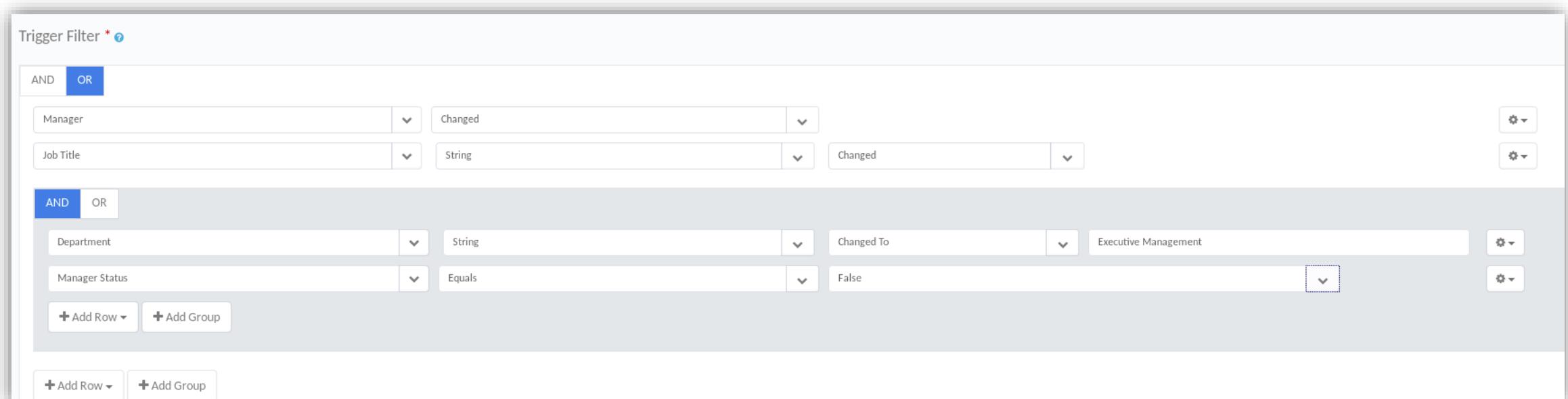
Manager	Changed
Job Title	String
Changed	

AND OR

Department	String	Changed To	Executive Management
Manager Status	Equals	False	

+ Add Row ▾ + Add Group

+ Add Row ▾ + Add Group



# Rapid Setup Mover Event

## Triggered Actions

- Generate access review for identity's manager
- Re-process joiner logic
- Other controls
  - Business process
  - Post mover rule

### Global

- Birthright roles
- Approvals

### Per Application

- Account-only provisioning

### Global Options

- Enable
- Staged certification
- Include birthright roles
- Certification owner
- Backup certifier
- Previous manager as additional certifier

### Per Application Options

- Include entitlements in access review
- Include target permissions in access review

# Rapid Setup Leaver Event

## Define Leaver Criteria

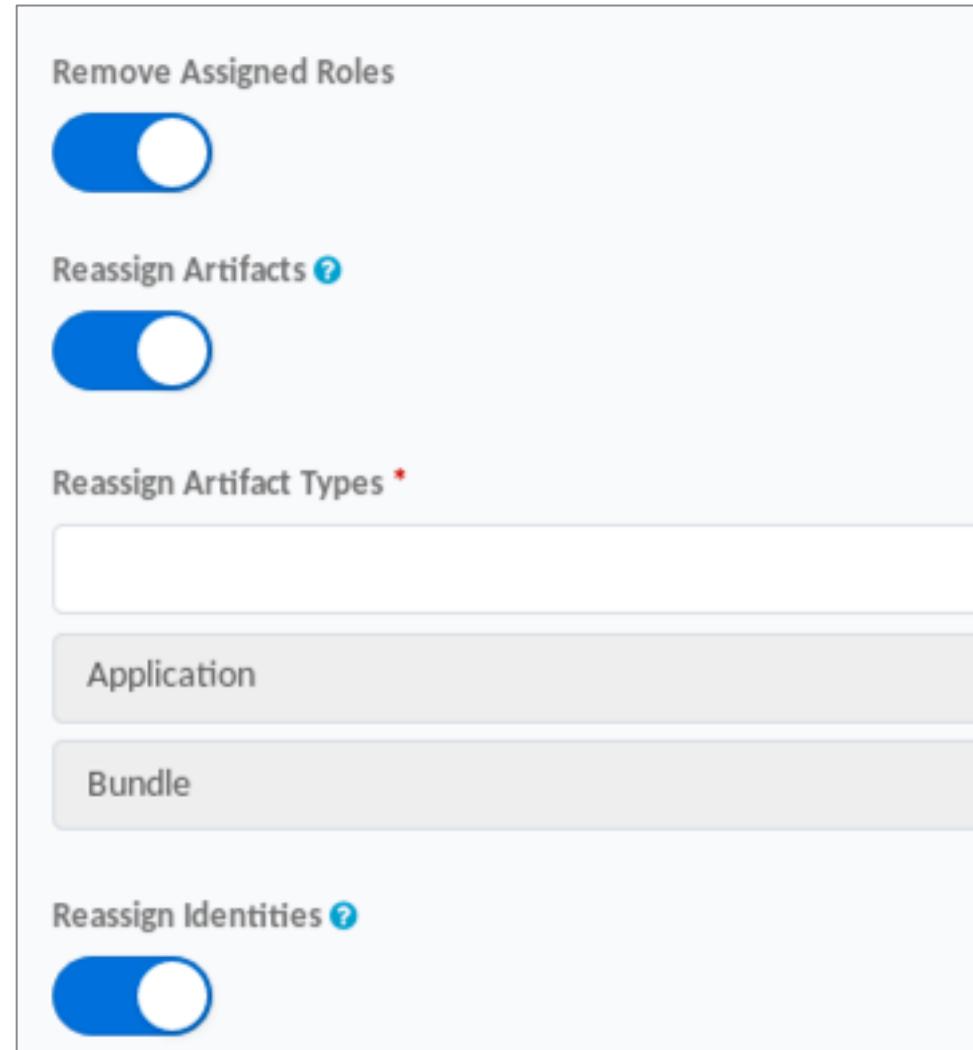
- Trigger Filters define criteria
  - Inactive attribute changes from False to True
  - Flag attribute set

The screenshot shows the 'Leaver' tab selected in the top navigation bar, which includes tabs for 'Mover', 'Leaver' (selected), 'Identity Operations', and 'Miscellaneous'. Below the tabs, there is a section titled 'Trigger Filter \*' with a question mark icon. The filter is set to 'AND'. It consists of two dropdown menus: 'Inactive' and 'Changed To', both currently set to 'True'. At the bottom of the filter section are two buttons: '+ Add Row' and '+ Add Group'.

# Rapid Setup Leaver Event

## Global Configuration

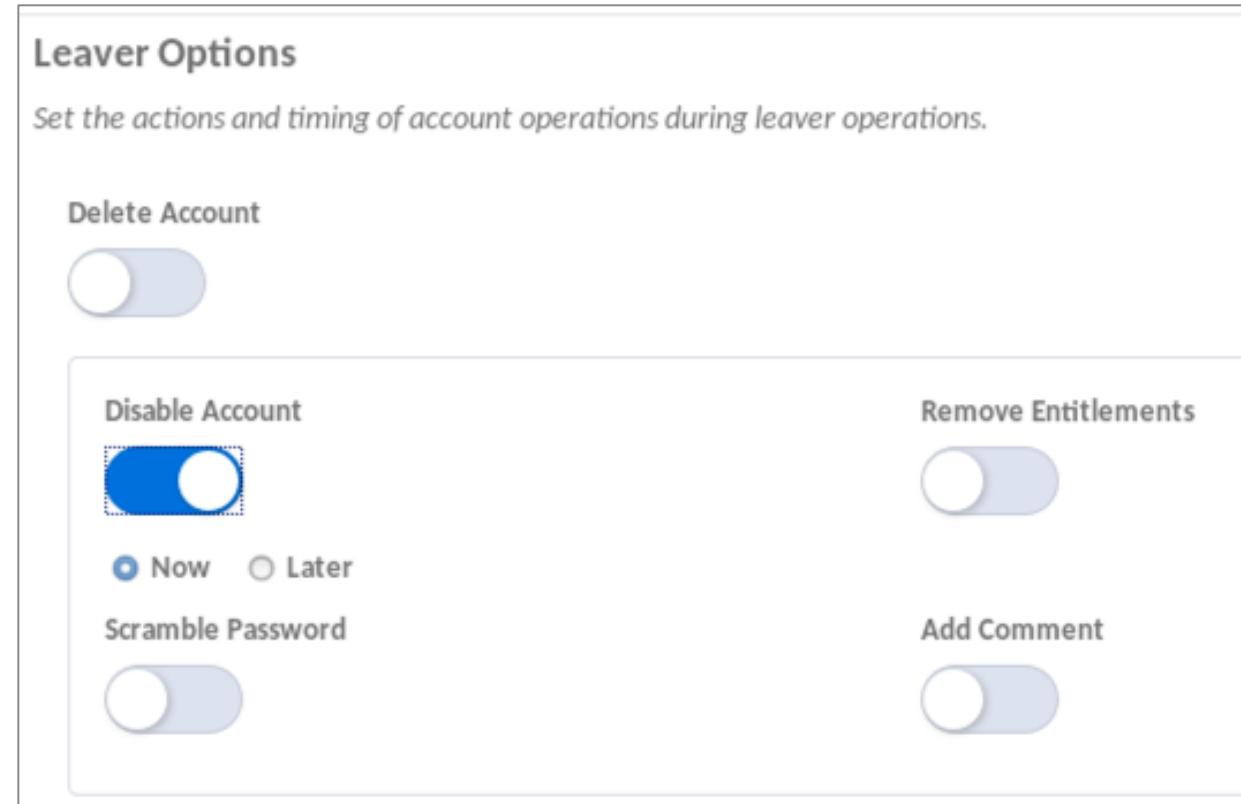
- IdentityIQ-internal actions
  - Remove assigned roles
  - Reassign owned artifacts
    - Which ones, to whom
  - Reassign RPA/Service Identities
- Approvals
- Notification
  - Manager or workgroup
  - Email templates
- Logic Controls
  - Business process
  - Post leaver rule



# Rapid Setup Leaver Event

## Per Application Configuration

- Delete account
- Disable account
- Scramble password
- Remove entitlements
  - Keep certain entitlements
- Add comments
- Active Directory only: Move OU
- Immediate or delayed (# of days)



# Rapid Setup Leaver: Scramble Password

## Password Policies (Best Practice)

- Enforce application's password policy
    - Set constraints to match application password constraints
  - Zero to multiple policies per application
  - Apply to specific users or all
- 
- More information
    - Product Documentation:  
***IdentityIQ Administration Guide***

### Password Policy

#### Configure Password Policy

Password Policy Name*	<input type="text" value="LDAP Password Policy"/>
Password Policy Description	<input type="text"/>
Minimum number of characters	<input type="text" value="12"/>
Maximum number of characters	<input type="text"/>
Minimum number of letters	<input type="text"/>
Minimum number of character type constraints to meet	<input type="text"/>
Minimum number of digits	<input type="text" value="1"/>
Minimum uppercase letters	<input type="text" value="1"/>
Minimum lowercase letters	<input type="text"/>
Minimum special characters	<input type="text" value="1"/>
Number of repeated characters allowed	<input type="text"/>
Password history length	<input type="text"/>
Triviality check against old password	<input type="checkbox"/>
Minimum number of characters by position	<input type="text"/>
Validate passwords against the password dictionary	<input type="checkbox"/>
Validate passwords against the identity's list of attributes	<input type="checkbox"/>
Validate passwords against the account's display name	<input type="checkbox"/>
Validate passwords against account ID	<input type="checkbox"/>
Validate passwords against the identity's account attributes	<input type="checkbox"/>

\*Indicates a required field.

#### Configure Password Filter

Identity Filter

# Knowledge Check

# Practice Exercises

# Exercise Preview

---

## Section 4, Exercises 2, 3

- Exercise 2: Define and Test Joiner Lifecycle Event
  - Configure Joiner event
  - Test Joiner event
- Exercise 3: Define and Test Mover Lifecycle Event
  - Configure Mover event
  - Test Mover event





# Lifecycle Event Configurations

IdentityIQ Essentials

# Overview

---

## Lifecycle Events

- Other Lifecycle Event configurations
- Viewing Lifecycle Events

# Lifecycle Events

## Standard IdentityIQ Feature

Lifecycle Events	
Lifecycle Events	
Name	Type
Joiner	Create
Leaver	Attribute Change
Manager transfer	Manager Transfer
RapidSetup Joiner	RapidSetup
RapidSetup Leaver	RapidSetup
RapidSetup Mover	RapidSetup
Reinstate	Attribute Change

Setup → Lifecycle Events

# Lifecycle Events

## Custom

**Lifecycle Event Options**

**Name\*** Department Transfer from IT

**Description** IT privileges must be carefully governed so extra processing is required when users leave the IT department but stay in the organization

**Event type** Attribute Change

**Attribute** Department

**Previous Value Filter** IT

**New Value Filter**

**Disabled**

**Included Identities** All

**Business Process\*** IT Department Transfer

\* Indicates a required field.

**Custom**

**Name and description**

**What is being monitored**

**Targeted Identities**

**Workflow to process event**

# Implementation Steps

## Included Identities Filter

The screenshot shows the 'Included Identities' configuration screen. On the left, a sidebar menu lists 'Match List' as the selected option. The main area is divided into three tabs: 'IdentityIQ Items', 'Application Items', and 'Additional Items'. Under 'IdentityIQ Items', there is an 'Add Identity Attribute' button and a dropdown menu labeled '-- Select Application --'. Under 'Additional Items', there are 'Add Role Attribute' and 'Add Entitlement Attribute' buttons. Below these tabs is a table with columns: Operation, Type, Source, Name, and Value. A row in the table shows 'Or' as the operation, 'Attribute' as the type, 'IdentityIQ' as the source, 'Location' as the name, and 'Headquarters' as the value. At the bottom of the table are buttons for 'Group Selected', 'Ungroup Selected', and 'Delete Selected'.

Setup → Lifecycle Events → Add New Lifecycle Event

# Lifecycle Events

## Rapid Setup

**Lifecycle Events**

**Lifecycle Events**

Filter by Lifecycle Event Name

Add New Lifecycle Event

Name	Type
Joiner	Create
Leaver	Attribute Change
Manager transfer	Manager Transfer
RapidSetup Joiner	RapidSetup
RapidSetup Leaver	RapidSetup
RapidSetup Mover	RapidSetup
Reinstate	Attribute Change

Setup → Lifecycle Events

**Lifecycle Event**

**Lifecycle Event Options**

Name\*  RapidSetup Joiner

Description  An ACTIVE Joiner for an new or existing Identity was detected in IdentityIQ.

Event type  RapidSetup

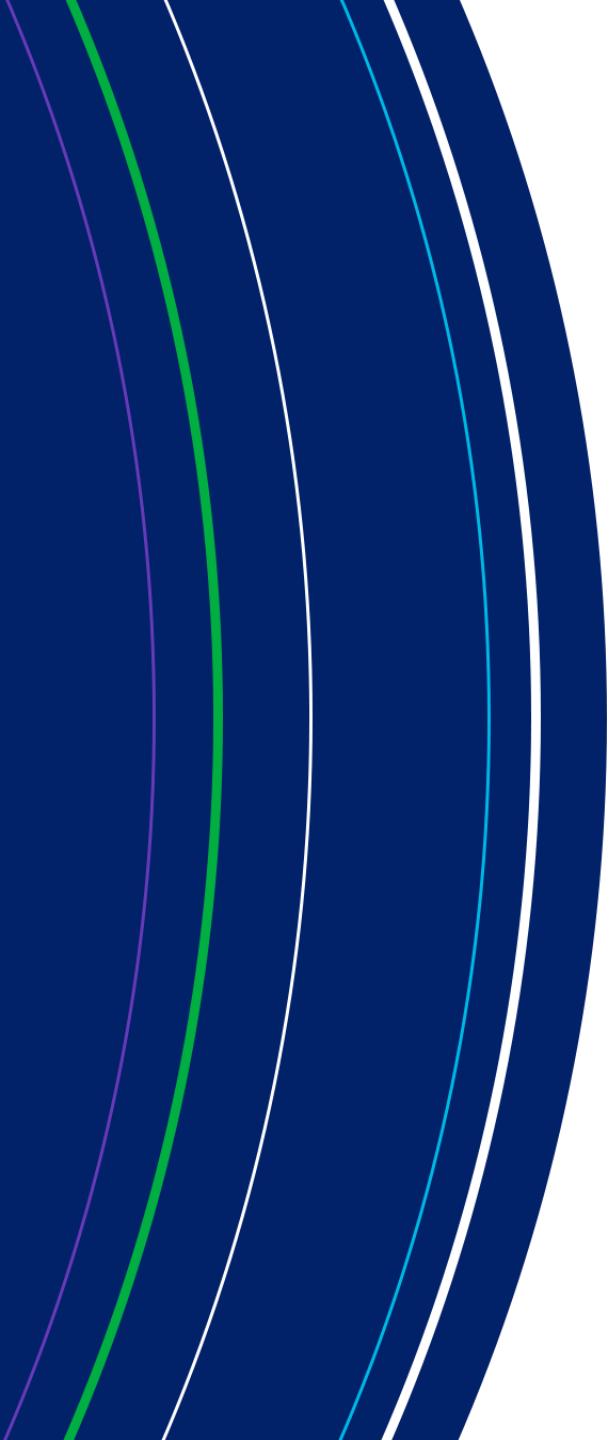
RapidSetup Process\*  Joiner

Disabled

Included Identities  All

\* Indicates a required field.

Rapid Setup Lifecycle Events



# **Monitoring Lifecycle Events**

# Monitoring Lifecycle Events

## Track My Requests

The screenshot shows the SailPoint interface with a dark blue header and sidebar. The sidebar on the left has a dropdown menu labeled 'Manage Access' with options: 'Manage User Access', 'Manage Accounts', 'Manage Passwords', and 'Track My Requests', which is highlighted with a red border. The main content area has a title 'Lifecycle: Caroline.Martin' and a subtitle 'Requested by RequestHandler on 5/31/19 | Request ID: 4'. A 'Details >' button is in the top right. Below this, there's a green bar with the text '✓ Request completed on 5/31/19'. Underneath are three rows, each with an 'Add Role' entry and a 'Complete' button:

Add Role	Action
Employees Birthright Role	Complete
Global Birthright Role	Complete
Asia-Pacific Birthright Role	Complete

- Dependent upon workflow
- Rapid Setup workflows provide tracking

# Monitoring Lifecycle Events

## Advanced Analytics - Audit

Advanced Analytics

Search Type   

Audit Search Criteria ?

**Audit Attributes**

Action	<input type="text" value="identityLifecycleEvent"/> <span style="border: 2px solid red; padding: 2px;"> </span>	Source	<input type="text"/>
Application	<input type="text"/>	Instance	<input type="text"/>
Attribute Name	<input type="text"/>	Attribute Value	<input type="text"/>
Target	<input type="text"/>		

Filter by: Date

Start Date

**Run Search** **Clear Search**

**Fields to Display** ?

**Audit Fields**

- Account Name
- Action
- Application
- Attribute Name

**Search Results - 2 Results Returned**

Action	Date	Source	Target
identityLifecycleEvent	August 28, 2014 6:22 PM	Ryan.Russell	Identity:Alice.Ford
identityLifecycleEvent	September 5, 2014 1:52 PM	Refresh Identity Cubes with Process ...	Identity:D'Arcy.O'Mahoney

# Monitoring Lifecycle Events

## Identity Events

**View Identity Caroline.Martin**

Attributes	Entitlements	Application Accounts	Policy	History	Risk	Activity	User Rights	Events
<b>Past Identity Events</b>								
Date	Event	Source	Cause		Summary			
Jul 24, 2020 2:21:52 PM	RapidSetup Leaver	Task: Refresh with Process Events	RapidSetup trigger matched for leaver		Rapid Setup Leaver processed a lifecycle event. Launched workflow 'RapidSetup Leaver: Caroline.Martin'			
Jul 23, 2020 2:37:31 PM	RapidSetup Joiner	Task: Refresh with Process Events	RapidSetup trigger matched for joiner		Rapid Setup Joiner processed a lifecycle event. Launched workflow 'RapidSetup Joiner: Caroline.Martin'			

# Knowledge Check





# Lifecycle Manager Requests

IdentityIQ Implementation and Administration: Essentials

# Overview

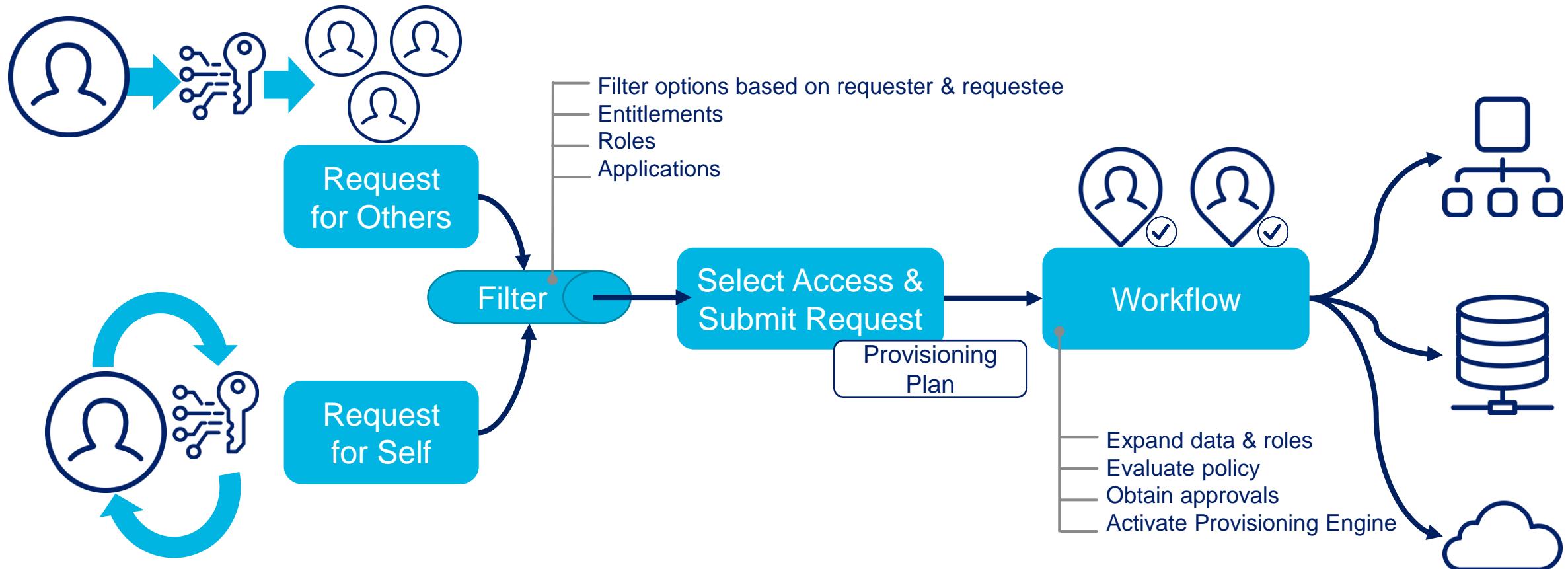
---

## Lifecycle Manager Requests

- Request Process Overview
- Supported Request Types
- Quicklink Populations

# Process Overview

## Access Request



# Lifecycle Manager

The screenshot shows the SailPoint Lifecycle Manager interface. On the left, there is a sidebar titled "Quicklink Menu" containing the following items:

- My Tasks
- Manage Access (highlighted with a red box)
- Manage Identity (highlighted with a red box)
- Rapid Application Onboarding
- Smart Setup
- Break Glass Operations
- Administrative Tasks

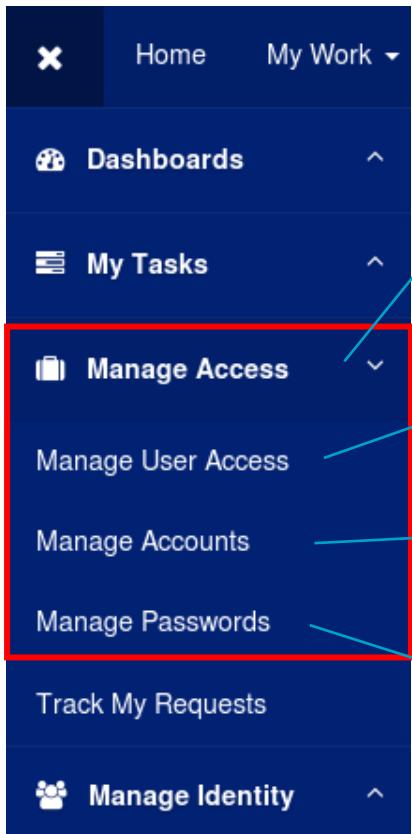
The main area is titled "Quicklink Cards" and contains the following cards:

- Access Reviews (0)
- Approvals (0)
- Manage User Access (highlighted with a red box)
- Track My Requests
- Manage Accounts
- Request Violations (0)
- Forms (0)
- View Identity (highlighted with a red box)
- Latest Violation Work Items (Both)
- Direct Reports

Quicklink Menu

# Access Request Types

## Quicklinks

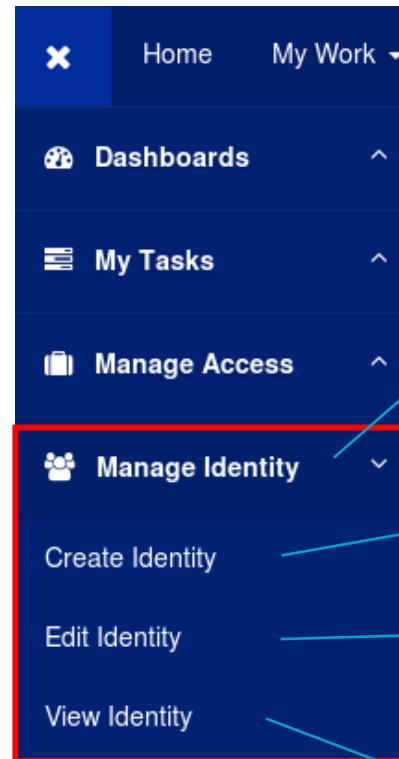


Quicklink Category

Add or remove  
*roles/entitlements*

Request, delete,  
modify **accounts**

Change  
**passwords** on  
managed systems  
or IdentityIQ



Quicklink Category

Create new  
**Identity Cube**

Edit **Identity Cube**

View **identity**  
attributes

# Key Considerations

---

## User-driven Changes: Lifecycle Requests

- Lifecycle Requests
  - **Who** submits the request? (requester)
  - **What** is the request? (requested)
  - **Which** identity is the target of the access change? (requestee)
- Responses
  - **How** is the request fulfilled? (business process)

**Who** can request **what** for **whom**?

What **workflow** should run to fulfill the request?

# Lifecycle Manager Workflows

## Default Workflows

The screenshot illustrates the configuration of default workflows in the Lifecycle Manager. On the left, the 'Business Processes' tab is selected in the 'Lifecycle Manager' interface. A table lists various actions and their associated business processes:

Action	Business Process
Request Access	LCM Provisioning
Manage Accounts	LCM Provisioning
User Unlock Account	LCM Provisioning
Manage Passwords	LCM Manage Passwords
Edit Identity	LCM Create and Update
Create Identity	LCM Create and Update
Self-service Registration	LCM Registration

Red boxes highlight the 'Manage Accounts', 'Manage Passwords', 'Edit Identity', and 'Create Identity' rows. Red arrows point from these highlighted rows to two separate vertical menus on the right:

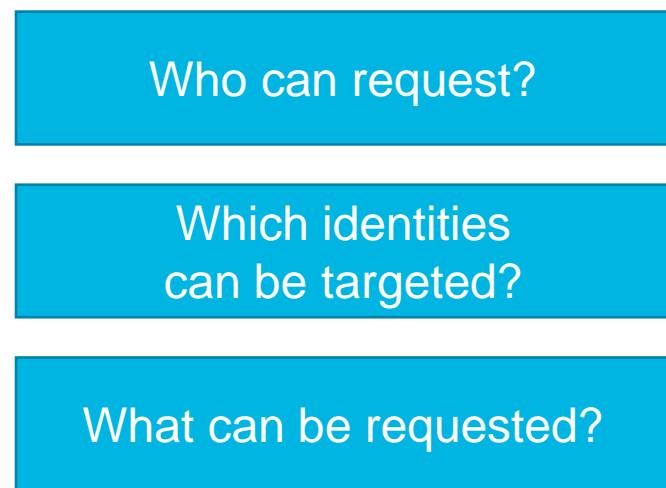
- Manage Access**:
  - Manage User Access
  - Manage Accounts
  - Manage Passwords
  - Track My Requests
- Manage Identity**:
  - Create Identity
  - Edit Identity
  - View Identity

Below the table, the text "Default Workflows" is displayed.

# Quicklink Populations

## Definition

- Flexible method to control who has access to a Quicklink
- Provide for answering the three questions:



Quicklink Populations

Configuration Quicklinks

Details

Name\*

Description

**Membership**

Membership Rule

Included Identities

Excluded Identities

**Who can members request for?**

Everyone  Specific Users

Ignore Scoping

**What can members request?**

Roles  Applications  Entitlements

Save

Global Settings → Quicklink Populations

# Lifecycle Manager Quicklink Populations

---

## Members and Requestees

- Default LCM Quicklink Populations

	Help Desk	Manager	Self-Service
Who can request?	Users with <i>Help Desk Personnel</i> capability	Users with <i>Manager Status = true</i>	All identities
Which identities can be targeted?	All identities	Direct and indirect reports	Themelves

- Custom Quicklink Populations
  - Members based on attribute match, filter, script, rule, or population
  - Requestees are either everyone or specific users
- Access is cumulative

# Who Can Request?

## Quicklink Population Members

The screenshot shows the 'Quicklink Populations' configuration page. On the left, a sidebar lists populations: Everyone, Help Desk, Manager (selected), and Self Service. The main area has tabs for 'Configuration' and 'Quicklinks'. Under 'Configuration', the 'Details' section shows 'Name\*' as 'Manager' and 'Description' as empty. A red box highlights the 'Membership' tab. In the 'Membership Rule' section, a dropdown menu is open with options: Match List (selected), None, All, Match List, Filter, Script, Rule, and Population. Another red box highlights the 'Match List' option in the dropdown. Below this, there are sections for 'Items' and 'Application Items', both currently empty. Buttons for 'Add Attribute' and 'Add Permission' are visible. At the bottom, a table defines a membership rule: 'Or' (selected), 'Attribute' 'IdentityIQ', 'Type' 'Manager Status', and 'Value' 'true'. A red box highlights the entire row of the table.

## Criteria Options

- Identity attribute values
- IdentityIQ controls: workgroups, capabilities
- Account-level data
- Populations
- Rules, Scripts
- Inclusion, Exclusion lists

# For Which Users?

## Target Identities / Requestees

**Who can members request for?**

Everyone  Specific Users

Share attributes with the requester [?](#)

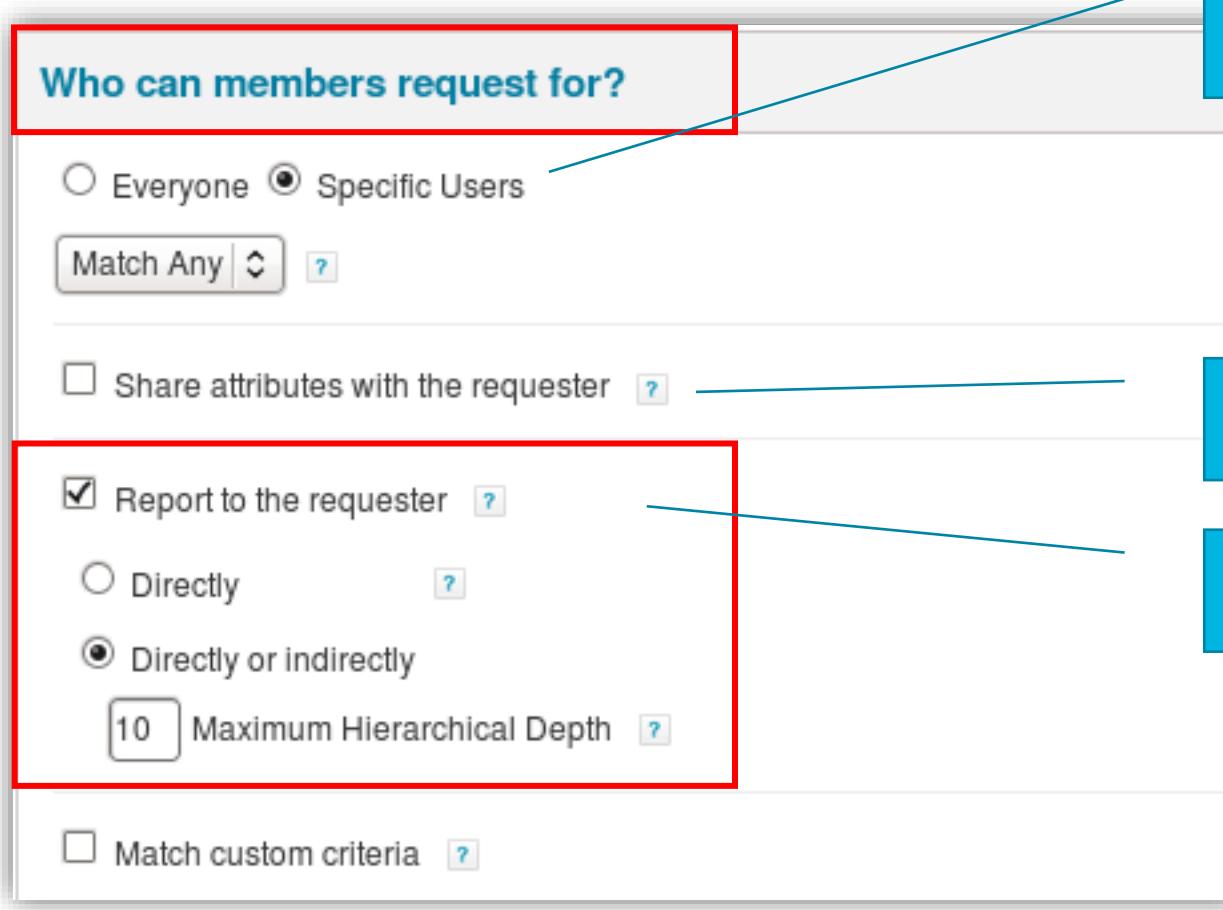
Report to the requester [?](#)

Directly [?](#)

Directly or indirectly

10 Maximum Hierarchical Depth [?](#)

Match custom criteria [?](#)



- Allow population to request for all or as filtered

- Allow population to request for others where they share specified attributes

- Allow managers to request for subordinates

# What can they request?

## Quicklink Access

The screenshot shows the SailPoint interface with the 'Quicklinks' configuration page open. The left sidebar has two main sections: 'Manage Identity' and 'Manage Access'. Red arrows point from the 'Create Identity', 'Edit Identity', and 'View Identity' items under 'Manage Identity', and from the 'Manage User Access', 'Manage Accounts', and 'Manage Passwords' items under 'Manage Access' towards the central configuration area. The central area has tabs for 'Configuration' and 'Quicklinks', with 'Quicklinks' selected and highlighted by a red box. Below the tabs is a descriptive message: 'Click the checkbox to enable a Quicklink. Use Configure to control specific Quicklink settings.' A table lists various quicklinks, each with an 'Enabled' checkbox, a 'Name' column, a 'Description' column, a 'Category' column, and a 'Configure' link.

Enabled	Name ▾	Description	Category	Options
<input type="checkbox"/>	Access Reviews	The number of access reviews that require attention.	Tasks	<a href="#">Configure</a>
<input type="checkbox"/>	Approvals	Opens the Manage Work Items page displaying approvals that require attention.	Tasks	<a href="#">Configure</a>
<input checked="" type="checkbox"/>	Create Identity	Create a new identity.	Manage	<a href="#">Configure</a>
<input checked="" type="checkbox"/>	Edit Identity	Edit identity attributes.	Manage	<a href="#">Configure</a>
<input type="checkbox"/>	Forms		Tasks	<a href="#">Configure</a>
<input checked="" type="checkbox"/>	Manage Accounts	Take action on any assigned accounts.	Access	<a href="#">Configure</a>
<input checked="" type="checkbox"/>	Manage Passwords	Issue requests to auto-generate or manually set account passwords.	Access	<a href="#">Configure</a>
<input type="checkbox"/>	Mobile Violation Reviews	The number of policy violation activities that require attention.	Tasks	<a href="#">Configure</a>
<input type="checkbox"/>	Policy Violations	The number of policy violation activities that require attention.	Tasks	<a href="#">Configure</a>
<input checked="" type="checkbox"/>	Request Access	Requests the addition or removal of roles or entitlements.	Access	<a href="#">Configure</a>

# Specifically, what can they request?

## Object Filtering Rules

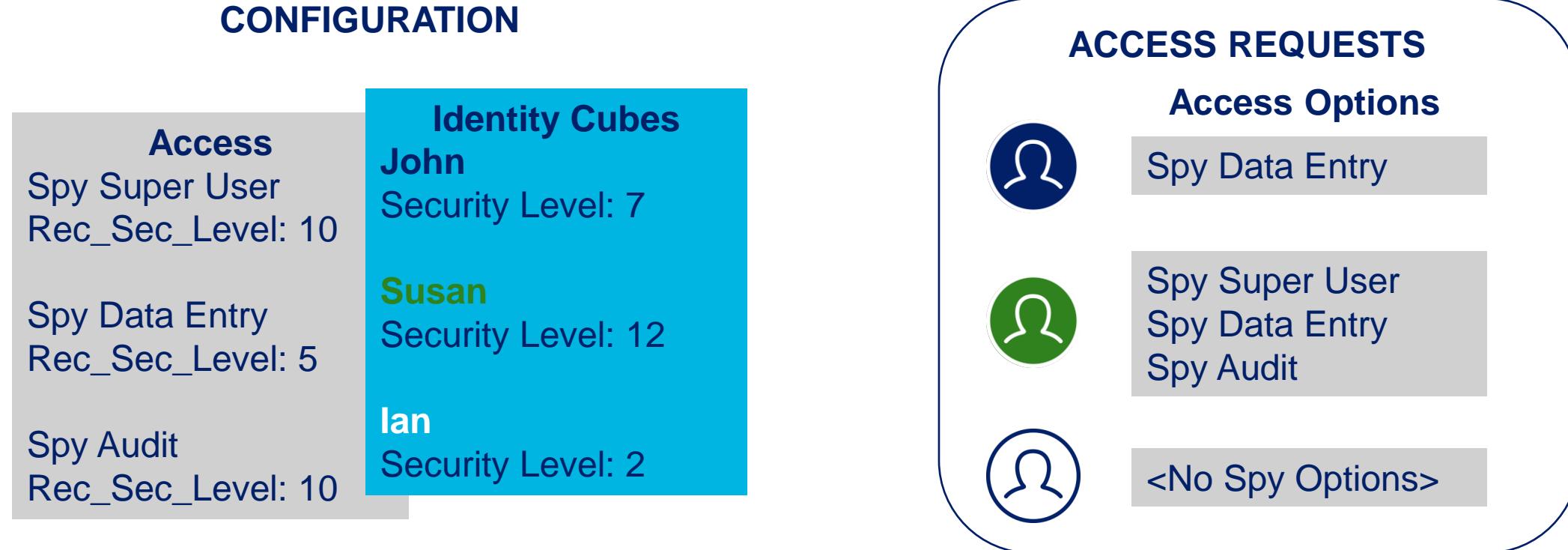
What can members request?

Roles	Applications	Entitlements
Objects in Requestor's Authorized Scopes	Objects in Requestor's Authorized Scopes	All Objects
<a href="#">Edit Rule</a>	<a href="#">Edit Rule</a>	<a href="#">Edit Rule</a>

- Availability based on requester and/or requestee
- Configured through rules
  - Multiple rule options provided
  - Can create own rules
- Separate rule set for revocation filters

# What can members request?

## Example: Controlling Access with Rules and Extended Attributes



### Rule

```
import sailpoint.object.Filter;  
return Filter.le("rec_sec_lev",requestee.getAttribute("security_lev"));
```

# Knowledge Check





# Manage User Access

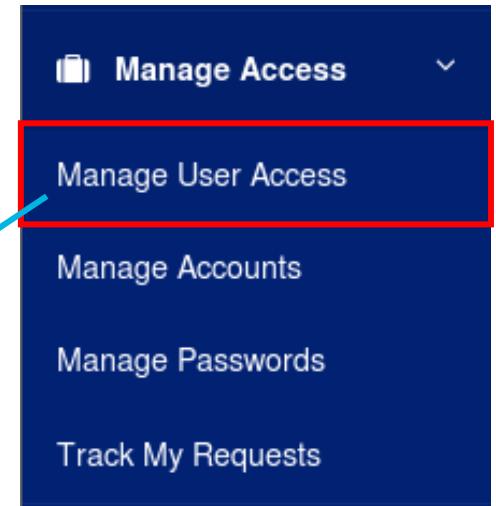
IdentityIQ Essentials

# Access Request Overview

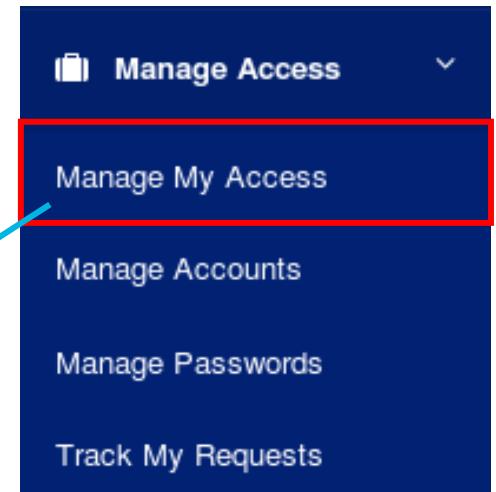
## Manage User Access Quicklink

- **Role** requests
- **Entitlement** requests

Request for self  
and others



Request only  
for self



# Manage User Access Quicklink Configuration

## Quicklink Population Example

Configuration Quicklinks

Click the checkbox to enable a Quicklink. Use Configure to control specific Quicklink settings.

Enabled	Name ▾	Description	Tasks	Configure
<input type="checkbox"/>	Access Reviews	The number of access reviews that require attention.		
<input type="checkbox"/>	Approvals	Opens the Manage Work Items page displaying approva		
<input checked="" type="checkbox"/>	Create Identity	Create a new identity.		
<input checked="" type="checkbox"/>	Edit Identity	Edit identity attributes.		
<input type="checkbox"/>	Forms			
<input checked="" type="checkbox"/>	Manage Accounts	Take action on any assigned accounts.		
<input checked="" type="checkbox"/>	Manage Passwords	Issue requests to auto-generate or manually set account		
<input type="checkbox"/>	Mobile Violation Reviews	The number of policy violation activities that require attention.		
<input type="checkbox"/>	Policy Violations	The number of policy violation activities that require attention.	Access	 Configure
<input checked="" type="checkbox"/>	Request Access	Requests the addition or removal of roles or entitlements.		 Configure

### Request Access Options

For Self  
 For Others

Single  Bulk

Request Roles   
 Allow requesting additional accounts   
 Allow requester to see population statistics in Advanced Search for each role 

Request Entitlements   
 Allow requesting additional accounts   
 Allow requester to see population statistics in Advanced Search for each entitlement 

Allow remove requests for roles   
 Allow remove requests for entitlements 

**Save** **Cancel**

Point Technologies Holdings, Inc. 2020. All rights reserved.

# Entitlement Catalog

## Which entitlements can be requested?

- Requestability indicator
- Standard default: all requestable
- Alternatives
  - Rapid Setup configurable
  - Rules to auto set
    - ManagedAttributePromotion
    - GroupAggregationRefresh

- Visible in LCM

The screenshot shows the 'Edit Group' interface. Under the 'Standard Properties' tab, the 'Requestable' checkbox is checked. The 'Description' field contains the text: 'Provides access to view and run reports on accounting system data across all modules'. The 'Owner' field is set to 'Mary Johnson'.

Applications → Entitlement Catalog

# Role Type Filtering

## Request Roles Options

Choose which of the following role types are requestable for each type of request roles request. Any options

Role Type	My Actions	Others
Assignable Role	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Permitted Role	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Gear → Lifecycle Manager

Example:

- My Actions: Only Permitted Roles allowed for self-service
- For Others: Assignable Roles are allowed

# LCM Quicklinks Demonstration

# Manage User Access

## Requesting for Others

Manage User Access Help

- 1 Select Users**  
Find and select users for whom you want to manage access.
- 2 Manage Access**  
Add access for the users you've selected.
- 3 Review and Submit**  
Look over your selections and confirm.

Search Users Filters

Users Selected: None All

Showing 1-6 of 6

<input checked="" type="checkbox"/> Catherine.Simmons  Username: Catherine.Simmons Manager: Amanda.Ross  	<input checked="" type="checkbox"/> Denise.Hunt  Username: Denise.Hunt Manager: Catherine.Simmons  	<input checked="" type="checkbox"/> Irene.Mills  Username: Irene.Mills Manager: Catherine.Simmons  
--	--	--

# Access Request Configuration Options

The screenshot shows a three-step configuration process:

- 1 Select Users**: Find and select users for whom you want to manage access.
- 2 Manage Access**: Add access for the users you've selected. This step is highlighted with a red box around the "Add Access" and "Remove Access" buttons.
- 3 Review and Submit**: Look over your selections and confirm.

Below the steps, there is a search bar with "Search By Keywords" and "Search Access" fields, a magnifying glass icon, and a "Filters" dropdown. The "Manage Access" section shows "Users Selected: Denise.Hunt" and "Showing 1-12 of 16". A specific row for "ACCOUNTING" is selected, showing "Accounting Group for Finance Application" with "Type: Entitlement Application: Finance Attribute: Permission Group".

Listed roles and entitlements controlled by Quicklink configuration

Add Access Page UIConfig Entry Keys:  
• uiAccessItemsColumnsEntitlement  
• uiAccessItemsColumnsRole

Remove Access Page UIConfig Entry Keys:  
• uiCurrentAccessItemsColumnsEntitlement  
• uiCurrentAccessItemsColumnsRole

# Search Configuration

## Searching by Keyword

1 Select Users  
Find and select users for whom you want to manage access.

2 Manage Access  
Add access for the users you've selected.

3 Review and Submit  
Look over your selections and confirm.

Add Access      Remove Access

Search By Keywords ▾      Search Access      🔍      Filters ▾

Users Selected: Denise.Hunt      Showing 1-12 of 16

ACCOUNTING  
Accounting Group for Finance Application  
Type: Entitlement   Application: Finance   Attribute: Permission Group

Previous      Next

Full Text Search (default) includes name, attributes, and description

# Searching Configuration

## Searching by Affinity

- Search by *identity match* or by *population attribute matching*
- Request access from search results
- Available only to those who can request access for others
- Quicklink configuration

Request Entitlements [?](#)

Allow requesting additional accounts [?](#)

Allow requester to see population statistics in Advanced Search for each entitlement [?](#)

The screenshot shows a two-step process for managing user access:

- 1 Select Users:** Find and select users for whom you want to manage access.
- 2 Manage Access:** Add access for the users you've selected.

In the 'Select Users' step, there is a 'Filter Population' dropdown. Below it, there are 'Manager' and 'Region' dropdowns. The 'Manager' dropdown is set to 'Denise.Hunt'. The 'Region' dropdown is set to 'Europe'. There are 'Clear' and 'Apply' buttons below the dropdowns. The 'Apply' button is highlighted with a red box. The status bar at the bottom indicates 'Showing 1-2 of 2'.

Users Selected: Denise.Hunt

Showing 1-2 of 2

Type: Entitlement Application: LDAP Attribute: groups

- UIConfig controls available search options
  - Entry Key: "IcmSearchIdentityAttributes"

# Searching Configuration

## Filtering Search Results

The screenshot shows the 'Manage Access' step of a configuration wizard. The interface is divided into three main sections: 'Select Users' (Step 1), 'Manage Access' (Step 2, currently active), and 'Review and Submit' (Step 3). In the 'Manage Access' section, there are tabs for 'Add Access' and 'Remove Access'. Below these are search fields for 'Search By Keywords' and 'Search Access', followed by a search icon and a 'Filters' button, which is highlighted with a red box. The 'Filter Access' section contains various dropdown menus for filtering access based on Role Type, Entitlement Application, Entitlement Attribute, Entitlement Owner, Entitlement Birthright Entitlement, Entitlement Manual Override, Entitlement 1st Level Business Approvers, Entitlement 2nd Level Business Approvers, Entitlement Logical Business Application Name, and Entitlement Privileged Entitlement. At the bottom of this section are 'Clear' and 'Apply' buttons. The overall background is light gray, and the steps are indicated by large blue arrows.

- *Searchable entitlement/role extended attributes automatically added to search parameters*

# Submitting the Request

## Review and Submit

1 Select Users  
Find and select users for whom you want to manage access.

2 Manage Access  
Add access for the users you've selected.

3 Review and Submit  
Look over your selections and confirm.

Users Selected: Denise.Hunt

Add Access 2

**ACCOUNTING**  
Accounting Group for Finance Application  
Type: Entitlement Application: Finance Attribute: Permission Group

**AP**  
Accounts Payable Group for Finance Application  
Type: Entitlement Application: Finance Attribute: Permission Group

Normal

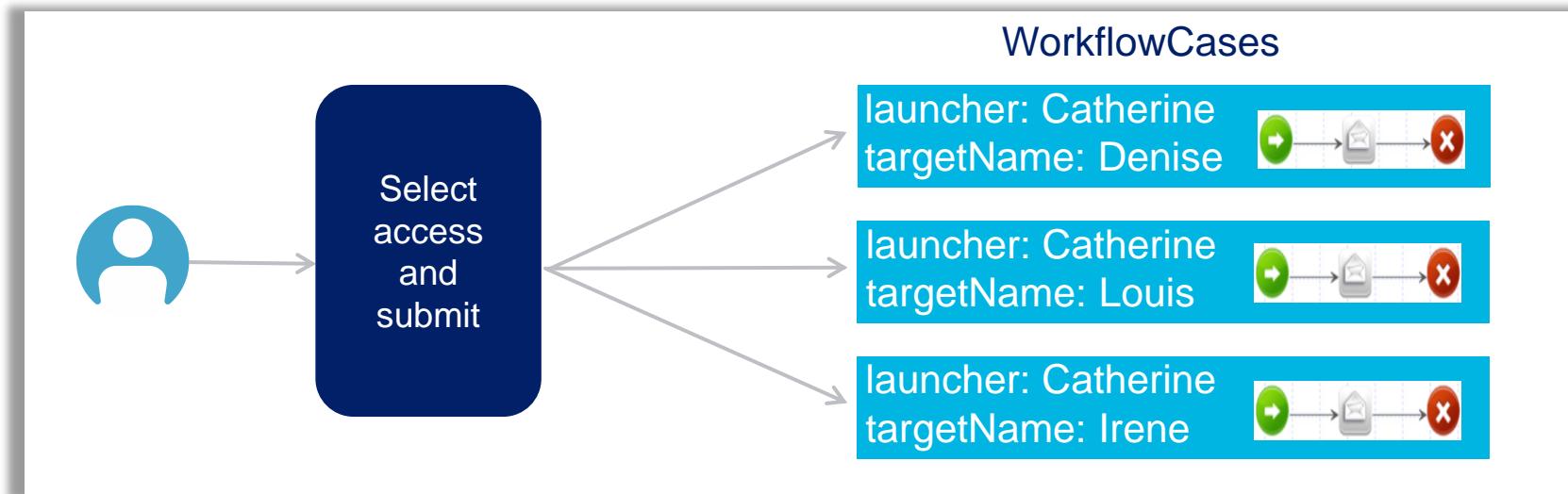
Previous Cancel Submit

- Submit starts Business Process
- Business Process handles policy checks, approvals, gathering needed information, etc.

# Workflow Execution

## WorkflowCase Per Target User

**Example:** Catherine Simmons submits request for 3 employees



# Approval Process

---

## Default and Configuration

Method	Default Approver	Configuration
Standard IdentityIQ workflow (LCM Provisioning)	Object owner	<ul style="list-style-type: none"><li>• Set variables on the provisioning workflows</li><li>• Set rules (if necessary) on the provisioning workflows</li></ul>
Custom Workflow	Dependent upon design	Dependent upon design

# Track My Requests

## Review Request

The diagram illustrates the 'Track My Requests' feature. On the left, a vertical navigation menu is shown with the following items:

- Manage Access
- Manage User Access
- Manage Accounts
- Manage Passwords
- Track My Requests**

A green arrow points from the 'Track My Requests' menu item to the main content area. The main content area displays a request titled 'Request Access: Denise.Hunt'.

Request Details:

- Requested by Catherine.Simmons on 7/5/19 | Request ID: 1
- Status: Request pending
- Add Entitlement: ACCOUNTING on Finance (Waiting on: Operations)
- Add Entitlement: FINANCE on Finance (Waiting)
- Add Entitlement: approve on Time Tracking (Waiting)

Actions:

- Cancel Request

A red box highlights the 'Details >' button in the top right corner of the request details page. A blue box on the bottom right lists additional features:

- Approval status
- Provisioning status
- Error messages
- ...and more

# Knowledge Check





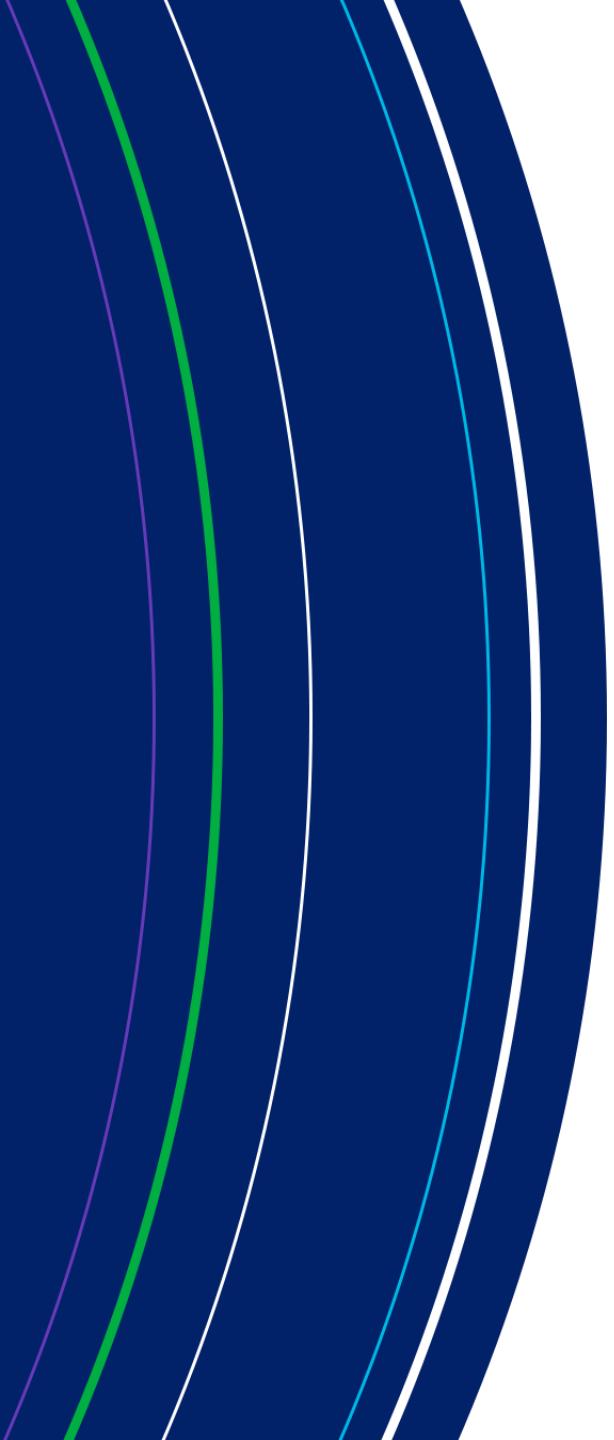
# Additional Access Request Options

# Overview

---

## Additional Access Request Options

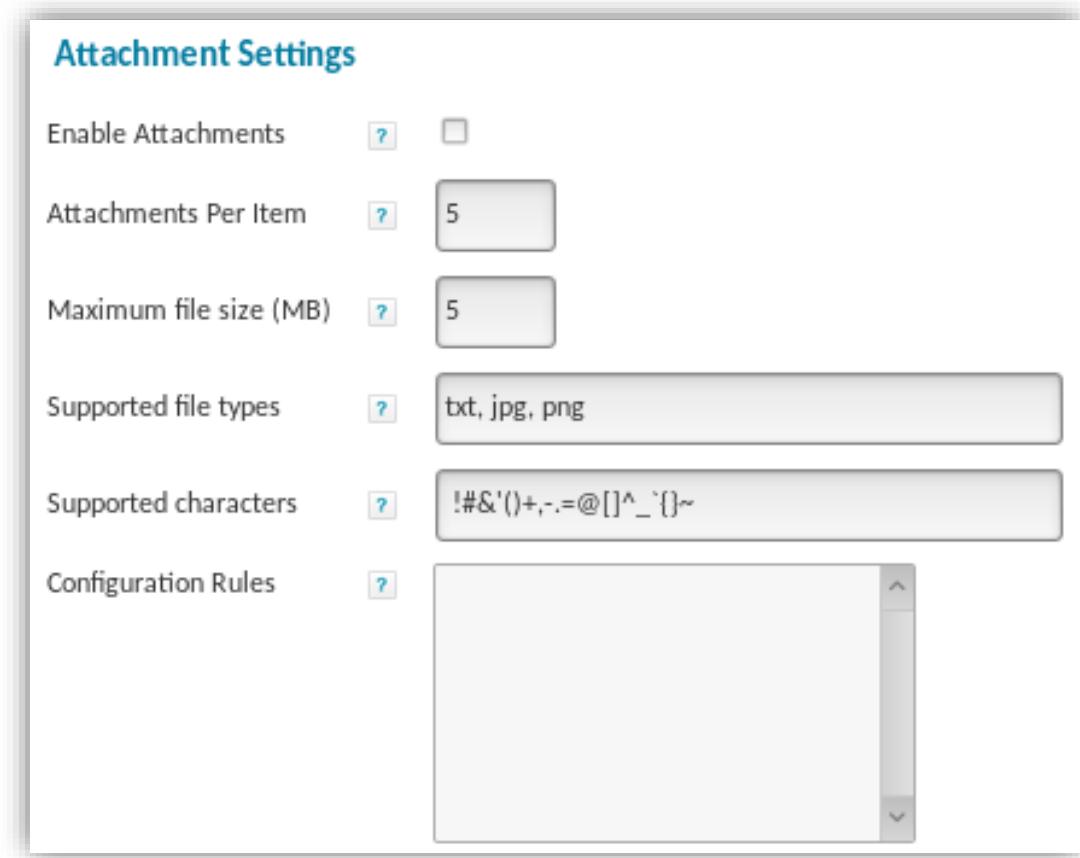
- Attachments on access requests
- Future-dated provisioning actions
- Recommendation Engine advice



# **Attachments on Access Requests**

# Attachments on Access Requests

- Who can access attachments?
  - Requester
  - Requestee
  - Approver
  - System administrator
- Configuration options
  - Constrain file types
  - Require attachment with rule
- Limits
  - Maximum size: 20 MB
  - Single user request
  - 10 attachments per request



Global Settings → IdentityIQ Configuration → Miscellaneous

# Attachments on Access Requests

1 Select Users  
Find and select users for whom you want to manage access.

2 Manage Access  
Add access for the users you've selected.

3 Review and Submit  
Look over your selections and confirm.

Add Access 1

x manager

Type: Entitlement Application: Bug Tracking Attribute: capability

Access Request

1st Level Application Business Approvers Approval - Account Changes for User: Jeremy.Palmer | 1 Request  
Requested on: Jun 26, 2019 1:27:29 PM Requested by: Catherine.Simmons Work Item ID: 22 Assigned to: Finance Administration

Approve All Deny All

Add: ACCOUNTING

Accounting Group for Finance Application  
Application: Finance Attribute: Permission Group

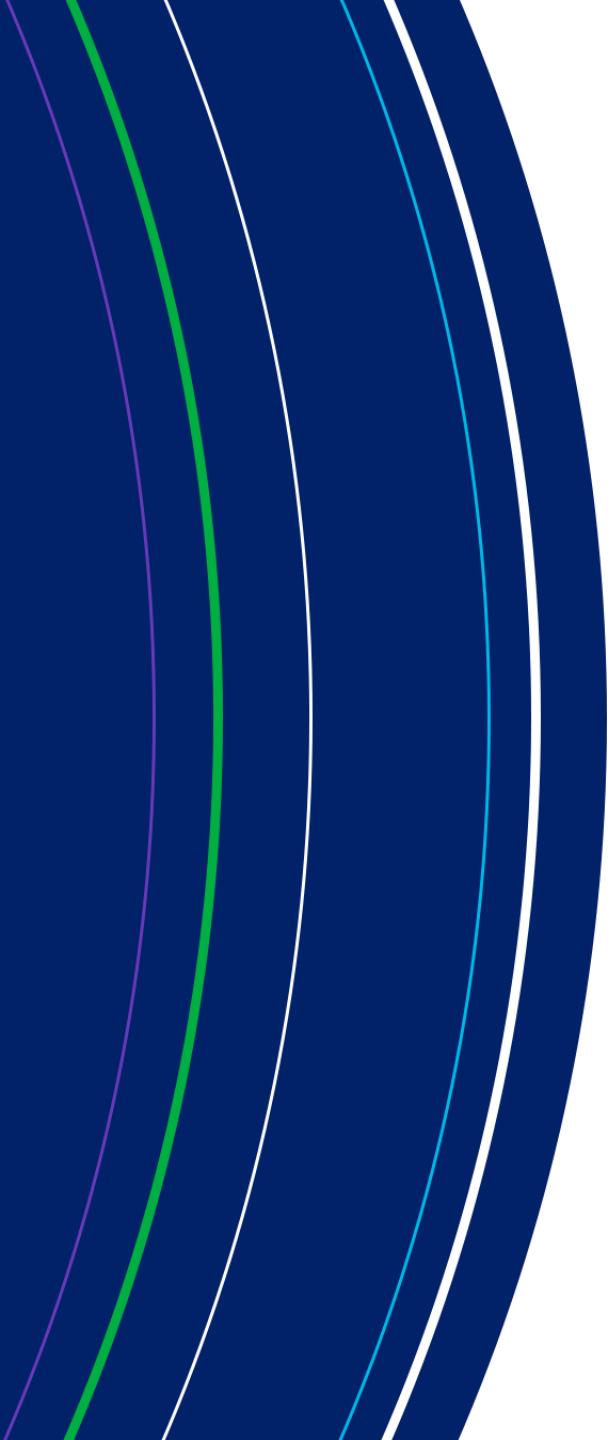
Approval

Attach a File

Drag and drop file here  
Or click to upload a file

Attached to This Item

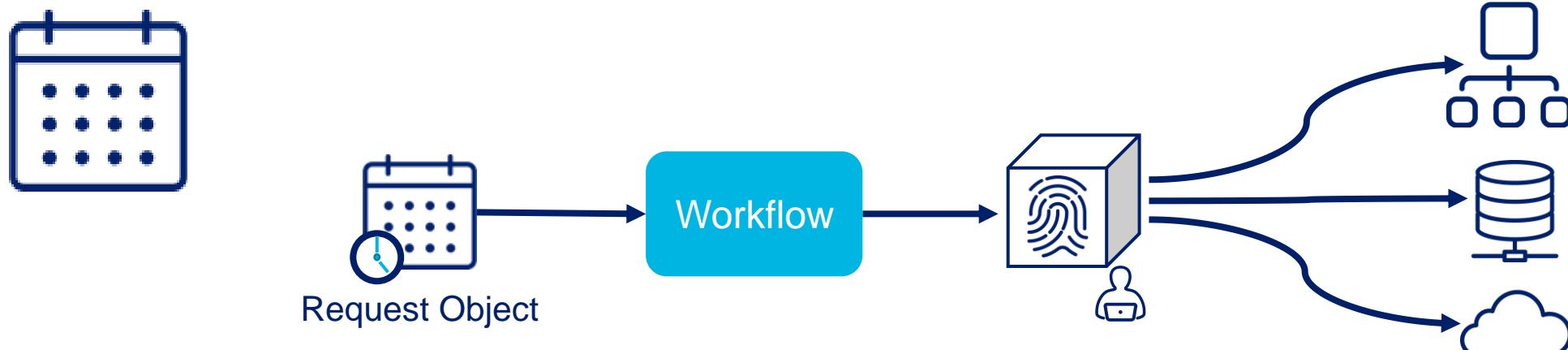
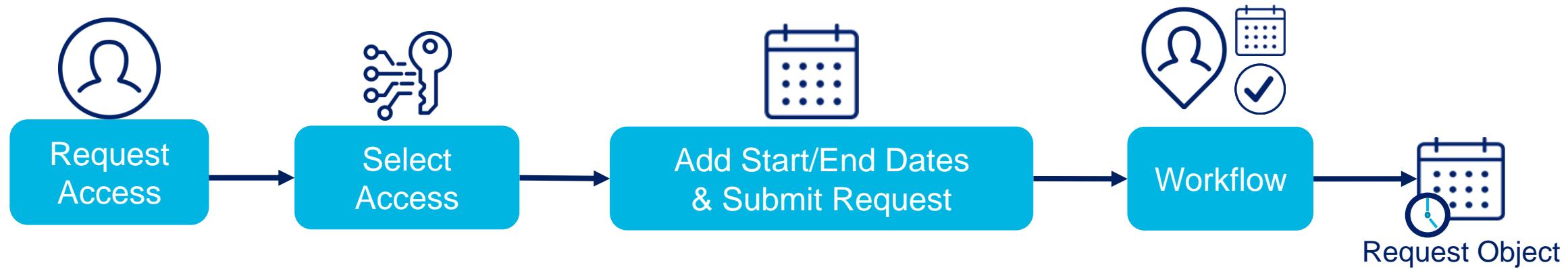
No Attachments



# **Future-dated Provisioning Actions**

# Role and Entitlement Assignment

## Sunrise and Sunset Dates



# Role and Entitlement Assignment

## Sunrise/Sunset Configuration

The screenshot shows the 'Role and Entitlement Assignment' process with three steps:

- 1 Select Users**: Find and select users for whom you want to manage access. It shows 'Users Selected: Jeremy.Palmer'.
- 2 Manage Access**: Add access for the users you've selected. It shows 'Add Access 1' and a selected item 'ACCOUNTING'. Below it, it says 'Accounting Group for Finance Application' and 'Type: Entitlement Application: Finance Attribute: Permission Group'.
- 3 Review and Submit**: Look over your selections and confirm. This step is highlighted with a red box around the 'Enable Sunrise/Sunset Dates' checkbox.

A modal window titled 'Set Sunrise/Sunset dates for this request' is open, containing fields for 'Start Date' (04/30/2016) and 'End Date' (07/01/2016), with 'Save' and 'Cancel' buttons.

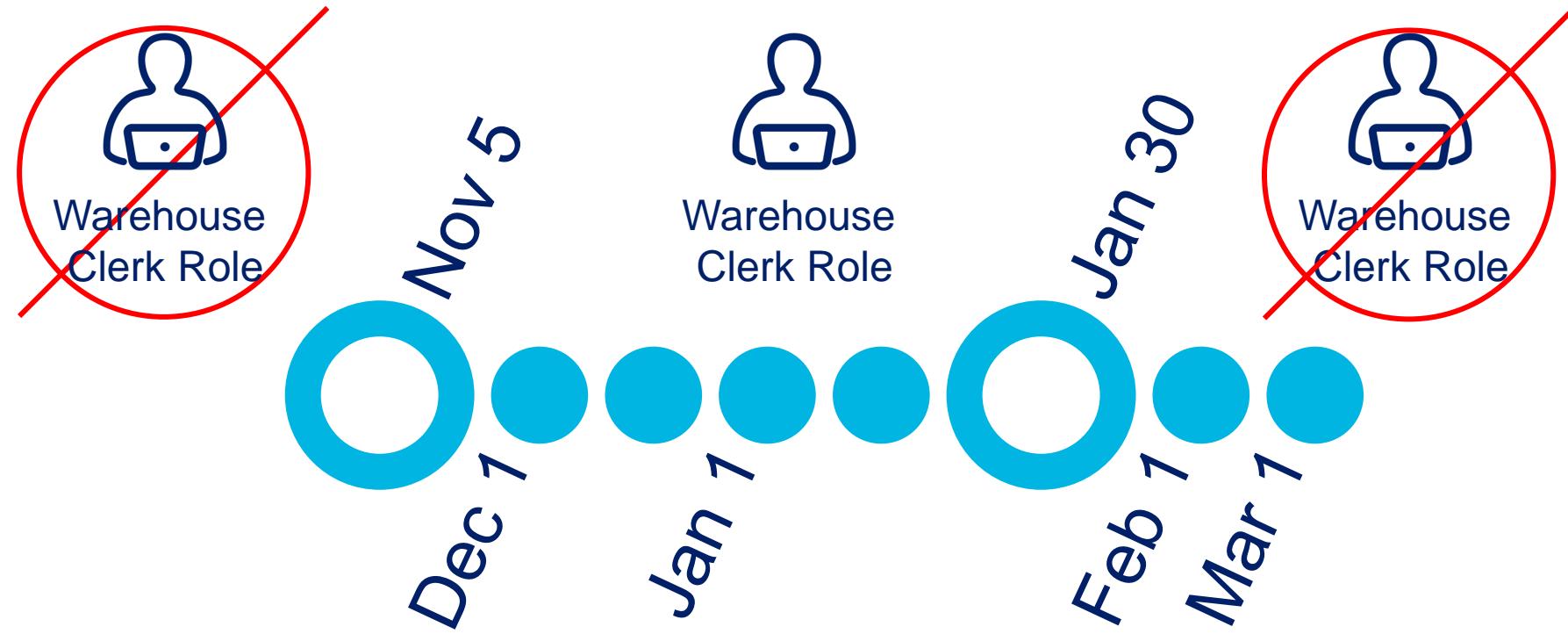
**Role Sunrise/Sunset Dates**

Enable Sunrise/Sunset Dates on Role Assignment

Enable Sunrise/Sunset Dates on Role Activation

# Role Activation

## Sunrise and Sunset Dates



# Role Activation

## Sunrise/Sunset Configuration

**Role Sunrise/Sunset Dates**

Enable Sunrise/Sunset Dates on Role Assignment

Enable Sunrise/Sunset Dates on Role Activation

Global Settings → IdentityIQ Configuration → Roles

**Scheduled Events**

Add Event   Delete Event

No Scheduled Events

Assignment Rule

**Add New Event**

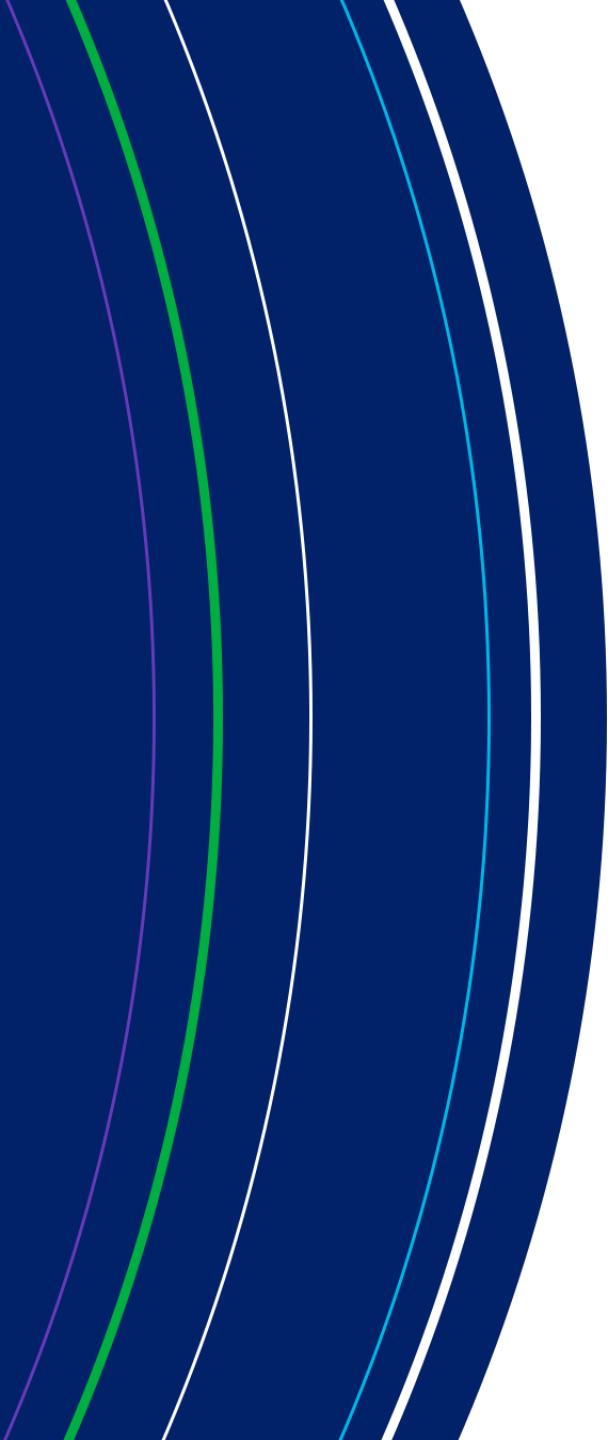
Date: 03/25/17

Action:

Activate

Deactivate

Setup → Roles → Edit Role → Scheduled Events → Add Event



# **Recommendation Engine Advice**

# Approving a Request

## IdentityAI Guidance for Approvers

The screenshot shows the 'Approvals' interface with 24 items. The top navigation includes 'Sort By', 'Filter', 'Collapse All', and a search bar. A 'Recommendations' section is visible. The main content displays two requests under 'Owner Approval - Account Changes for User: Amy Cox | 2 Requests'.  
Request 1: Add: DataComm\_AD (CN=DataComm\_AD,OU=demoGroups,OU=DemoData,DC=test,DC=sailpoint,DC=com). Application: ADDirectDemodata Attribute: memberOf.  
Request 2: Add (new account requested): DataArchive\_AD (CN=DataArchive\_AD,OU=demoGroups,OU=DemoData,DC=test,DC=sailpoint,DC=com). Application: ADDirectDemodata Attribute: memberOf.  
For each request, there are 'Approve' and 'Deny' buttons. The 'Deny' button for the second request is highlighted with a red box.

# Knowledge Check

# Practice Exercises

# Exercise Preview

---

## Section 4, Exercise 4, 5 and Extension Exercise 7

- Exercise 4: Configure access requests
  - Update entitlements: description, requestable
  - Allow attachments on access requests
  - Configure Request Access options
- Exercise 5: Test access requests
  - Retry Provisioning
  - Access Request with Attachments
  - Preventive Policy and Multi-Step Approvals
  - Request Permitted IT Roles





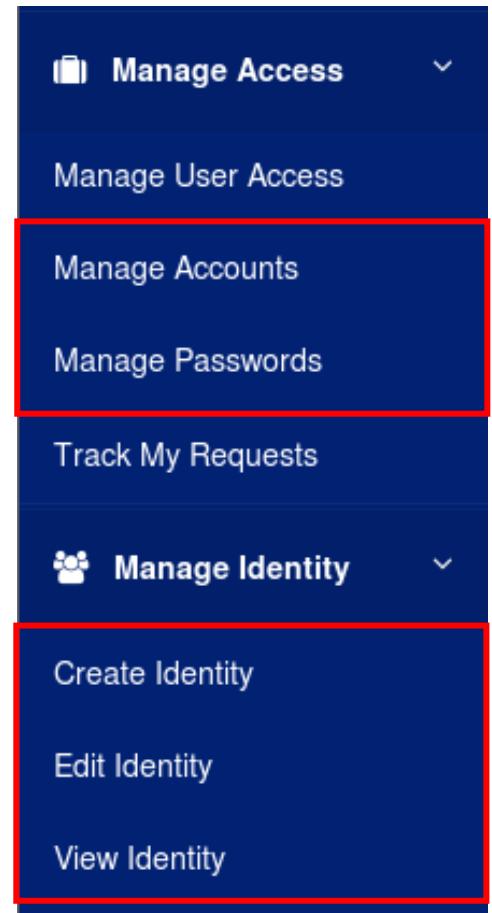
# Other Lifecycle Manager Requests

IdentityIQ Implementation and Administration: Essentials

# Remaining LCM Quicklinks

---

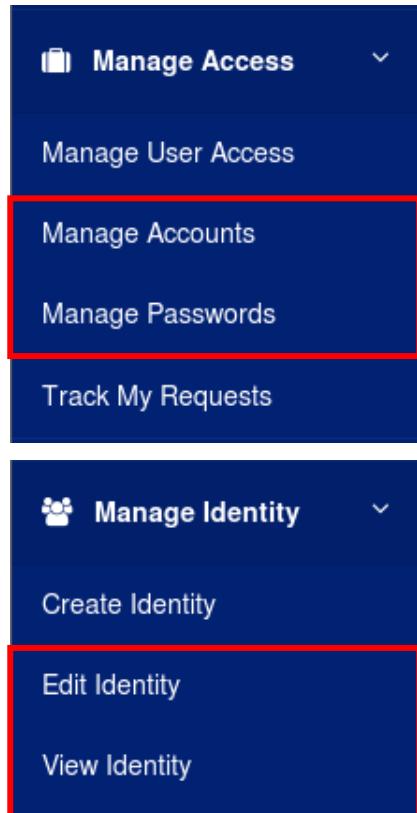
- Act on connected applications
  - Manage Accounts
  - Manage Passwords
- Act on IdentityIQ
  - Create Identity
  - Edit Identity
  - View Identity
- All can act on only one requestee at a time



# Submitting Single User Requests

## Request for Others

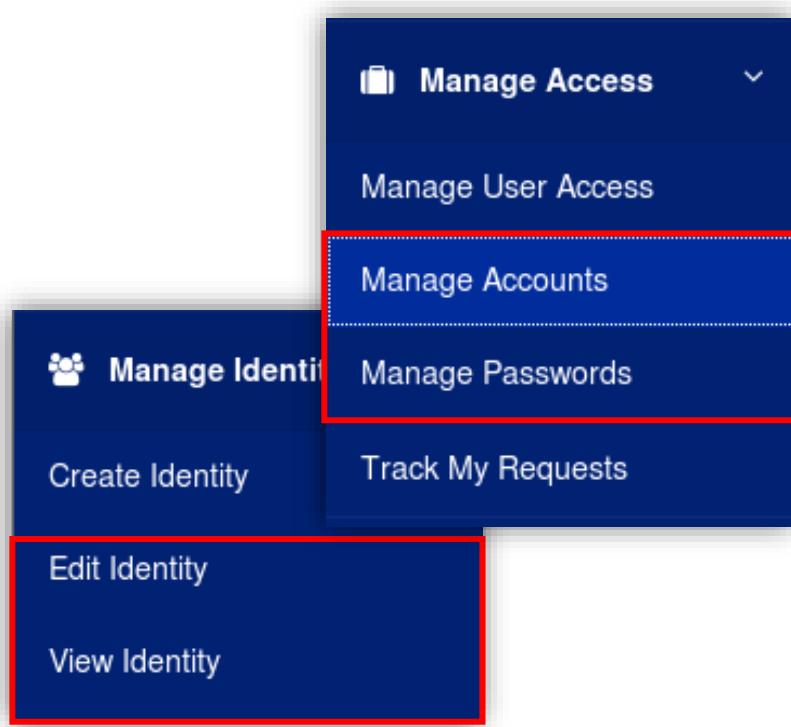
- Card for each identity for which requester can perform action



Manage Accounts	
Showing 1-12 of 237	
The Administrator	Username: spadmin
<button>Manage</button>	<button>Manage</button>
Aaron.Nichols	Username: Aaron.Nichols
<button>Manage</button>	<button>Manage</button>
Adam.Kennedy	Username: Adam.Kennedy
<button>Manage</button>	<button>Manager: Douglas.Flores</button>
Alan.Bradley	Username: Alan.Bradley
<button>Manage</button>	<button>Manager: Eugene.Hawkins</button>
Albert.Woods	Username: Albert.Woods
<button>Manage</button>	<button>Manager: Patrick.Jenkins</button>
Alice.Ford	Username: Alice.Ford
<button>Manage</button>	<button>Manager: Stephanie.Coleman</button>
Allen.Burton	Username: Allen.Burton
<button>Manage</button>	<button>Manager: Sara.Berry</button>
Amanda.Ross	Username: Amanda.Ross
<button>Manage</button>	<button>Manager: Jerry.Bennett</button>

# Identity Details Menu

## Quicklinks with Secondary Menu



Select Quicklink



A screenshot of the 'Identity Details' menu. At the top is a profile icon and the name 'Walter.Henderson'. Below the name are several menu items: 'Edit Identity' (in blue), 'Forwarding', 'Attributes', 'Access', and 'Accounts'. The 'Accounts' item is highlighted with a blue background and a right-pointing arrow. Below 'Accounts' are 'Passwords' and 'Change Password'.

Perform selected or alternative action

# Configuring Identity Details Menu

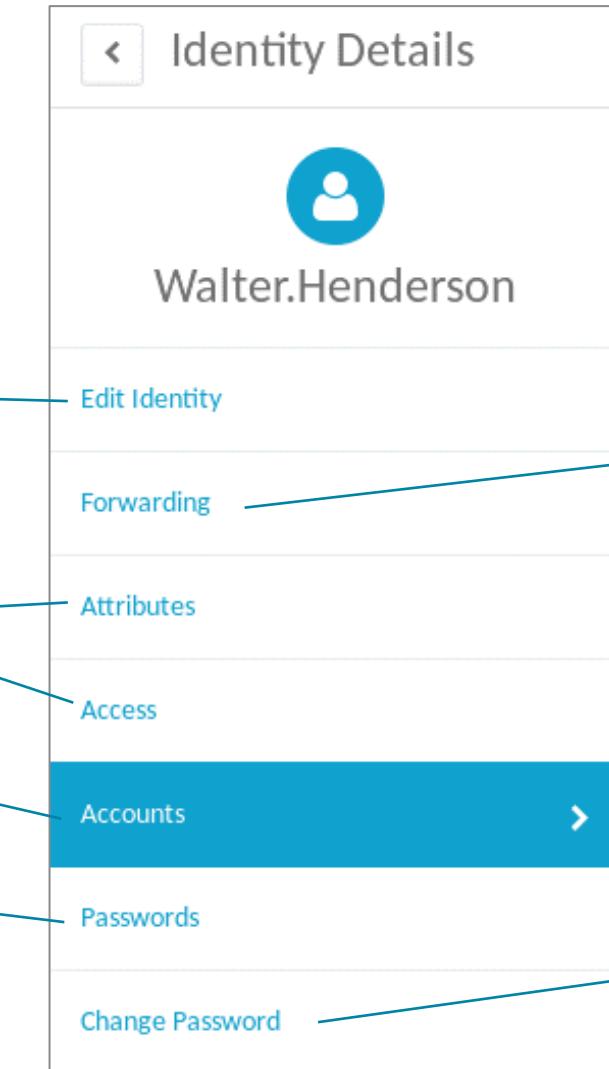
Controlled by Corresponding Quicklink Population

Edit Identity

View Identity

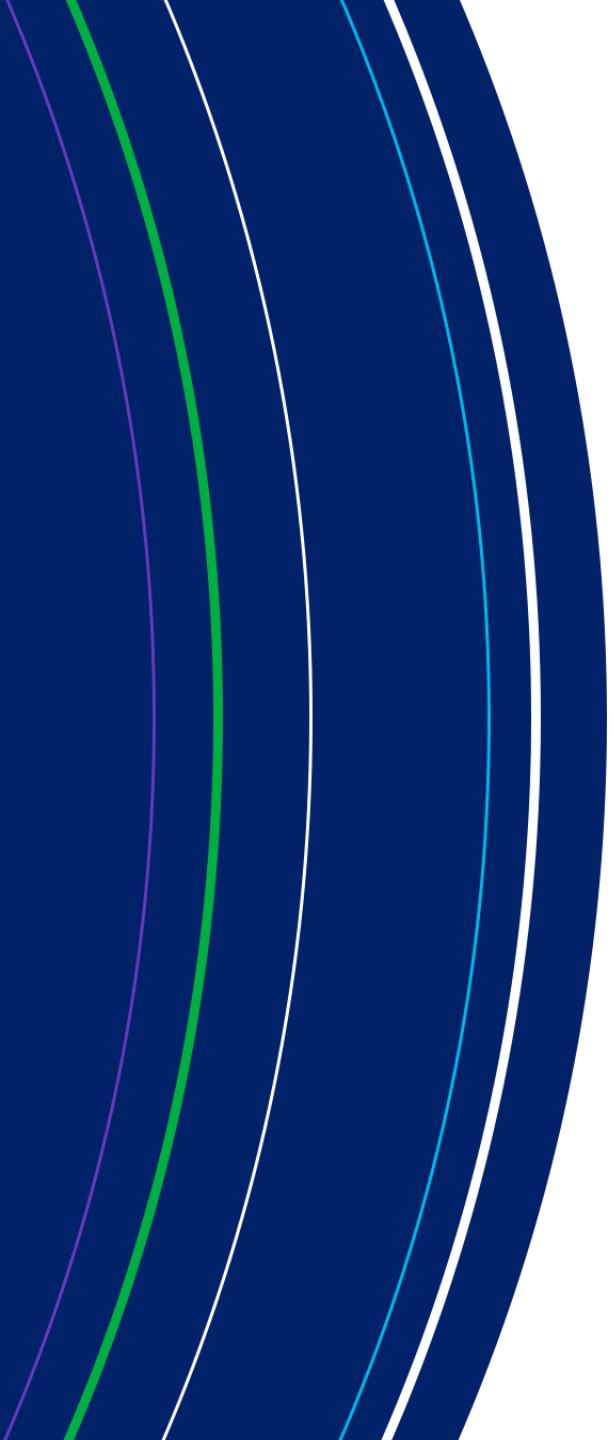
Manage Accounts

Manage Passwords



Add SP Right  
`SetIdentityForwarding`  
to capability and  
assign capability to  
user

Assign *Password Administrator*  
capability to user



# **Configuring Manage Accounts Quicklink**

# Manage Accounts Quicklink

- Manage Access
- Manage User Access
- Manage Accounts**
- Manage Passwords
- Track My Requests

- Manage existing application accounts
  - Enable, Disable, Unlock, Delete
- Request a new account
  - One account or additional account
    - Configurable per application

### Identity Details

Walter.Henderson

- [Edit Identity](#)
- [Forwarding](#)
- [Attributes](#)
- [Access](#)
- [Accounts](#)
- [Passwords](#)
- [Change Password](#)

#### Accounts 4

Showing 1-4 of 4

Application	Account ID	Status	Last Refresh	Action Status	Actions
HR System - Employees	Walter.Henderson	Active	3/31/17 1:39 PM		
TRAKK	Walter.Henderson	Active	4/12/17 9:12 AM		
PRISM	whenderson	Active	4/12/17 9:12 AM	Completed Unlock	
LDAP	Walter.Henderson	Active	4/12/17 9:12 AM		

Show 10 ▾

# Manage Accounts Quicklink

## Configuration Options

The screenshot shows two interface components related to account management:

- Manage Accounts Options Dialog:** A modal window titled "Manage Accounts Options". It contains three sections:
  - For Self
  - For Others
  - Single  
  - Allow managing existing accounts [?](#)
  - Allow requesting new accounts [?](#)
  - Allow requesting additional accounts [?](#)

At the bottom are "Save" and "Cancel" buttons.
- Configuration Page:** A table showing configuration options for quicklinks. The "Quicklinks" tab is selected. A note says: "Click the checkbox to enable a Quicklink. Use Configure to control specific Quicklink settings." The table has columns: Enabled, Name ▾, Description, Manage, and Configure.

Enabled	Name ▾	Description	Manage	Configure
<input type="checkbox"/>	Access Reviews	The number of access reviews that require attention.		
<input type="checkbox"/>	Approvals	Opens the Manage Work Items page displaying approvals that require attention.		
<input checked="" type="checkbox"/>	Create Identity	Create a new identity.		
<input checked="" type="checkbox"/>	Edit Identity	Edit identity attributes.	Manage	<a href="#">Configure</a>
<input type="checkbox"/>	Forms		Tasks	<a href="#">Configure</a>
<input checked="" type="checkbox"/>	Manage Accounts	Take action on any assigned accounts.	Access	<a href="#">Configure</a>
<input checked="" type="checkbox"/>	Manage Passwords	Issue requests to auto-generate or manually set account passwords.	Access	<a href="#">Configure</a>

A red box highlights the "Manage Accounts" row in the table, and another red box highlights the "Configure" link in the same row. A third red box highlights the "For Others" checkbox in the dialog.

# LCM Configuration

## Supporting Account Only Requests

The screenshot illustrates the configuration of account provisioning in the Lifecycle Manager (LCM) application. It shows two main components: a user profile page and the LCM configuration interface.

**User Profile Page:** On the left, a user profile for "Bruce.Willis" is displayed. The "Accounts" tab is selected. A modal window titled "Request Account" is open, showing a dropdown menu for "Application". The "LDAP" option is selected and highlighted with a red box. The "PRISM" option is also listed below it.

**Lifecycle Manager Configuration:** On the right, the "Lifecycle Manager" interface is shown. The "Configure" tab is active. Under "Applications that support account only requests", the "LDAP" and "PRISM" applications are listed, each preceded by a crossed-out radio button icon. A red box highlights this list. At the bottom of this section is a checkbox labeled "All Applications".

**Configuration Summary:** To the right of the configuration interface, a bulleted list provides a summary of the configuration:

- Quicklink option
  - Allow requesting new accounts

# LCM Configuration

## Supporting Requests for Additional Account

The screenshot shows the SailPoint LCM Configuration interface. On the left, there's a sidebar with options: Identity Details, Edit Identity, Forwarding, Attributes, Access, and Accounts (which is selected). A modal window titled "Request Account" is open, showing a summary for "Aaron.Nichols". It includes a "Summary of Request for Aaron.Nichols" section and a "Request Account" button. Below this, there's an "Application" dropdown menu where "LDAP" is selected. A red box highlights the "Request Account" button and the "LDAP" option in the dropdown. A red arrow points from the "LDAP" option in the dropdown to a tooltip. The tooltip is titled "Applications that support additional account requests" and lists "LDAP" with a crossed-out icon. At the bottom of the tooltip are "Submit" and "Cancel" buttons. The main interface also has a "Status" and "Actions" panel on the right.

- Quicklink option
  - Allow requesting additional accounts

# LCM Configuration

## Supporting Account Operations

- Quicklink option
  - Allow managing existing accounts

The screenshot shows the LCM Configuration interface. On the left, there's a sidebar with navigation links: Edit Identity, Forwarding, Attributes, Access, Accounts (which is selected and highlighted in blue), and Passwords. The main area displays account details for 'Walter.Henderson'. A red arrow points from the 'Accounts' link in the sidebar to the 'Accounts' section in the main view.

**Accounts 4**

Application	Account ID
HR System - Employees	Walter.Henderson
TRAKK	Walter.Henderson
PRISM	whenderson
LDAP	Walter.Henderson

**Manage Accounts Options**

Show Enable/Unlock decision buttons regardless of whether the account is disabled or unlocked.

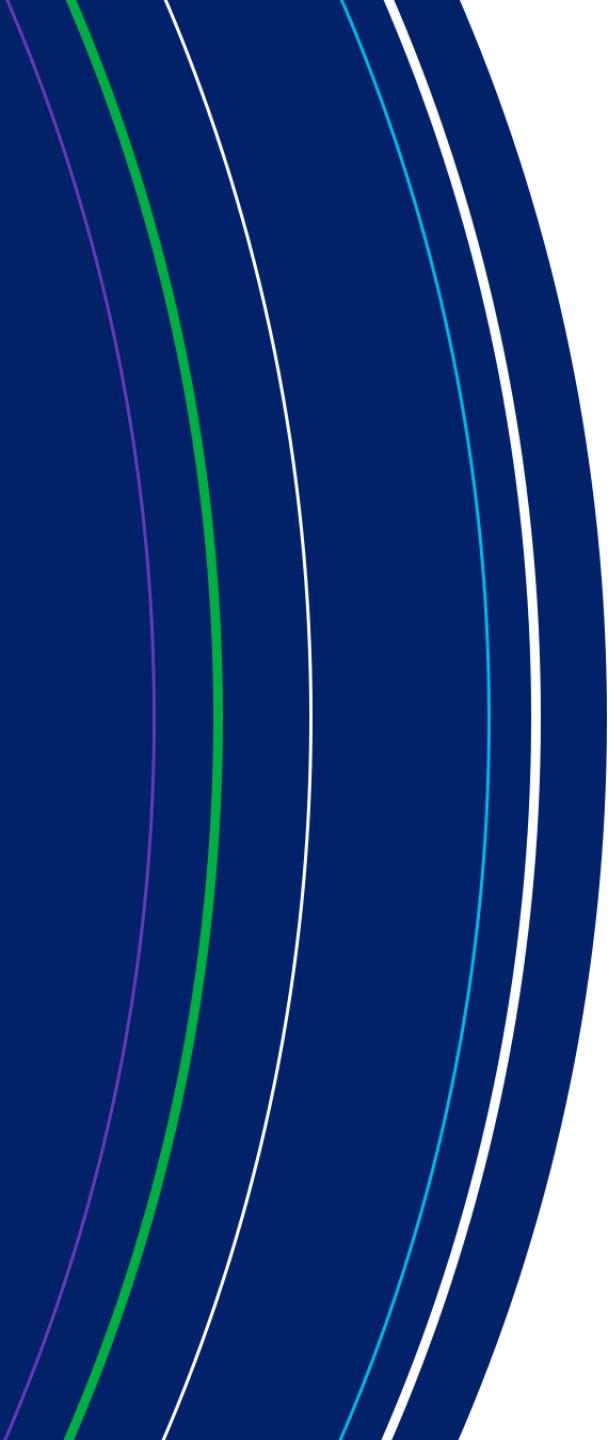
Choose which actions are enabled for each type of manage accounts request. Any options unselected wi

Action	My Actions	Subordinate
Delete	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Disable	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Enable	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Unlock	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Actions for individual accounts:

- For HR System - Employees: Active,  (disabled),  (locked),  (completed),  (unlock).
- For TRAKK: Active,  (disabled),  (locked),  (completed),  (unlock).
- For PRISM: Active,  (disabled),  (locked),  (completed),  (unlock).
- For LDAP: Active,  (disabled),  (locked),  (completed),  (unlock).

A red box highlights the 'Delete' and 'Disable' buttons for the PRISM account.

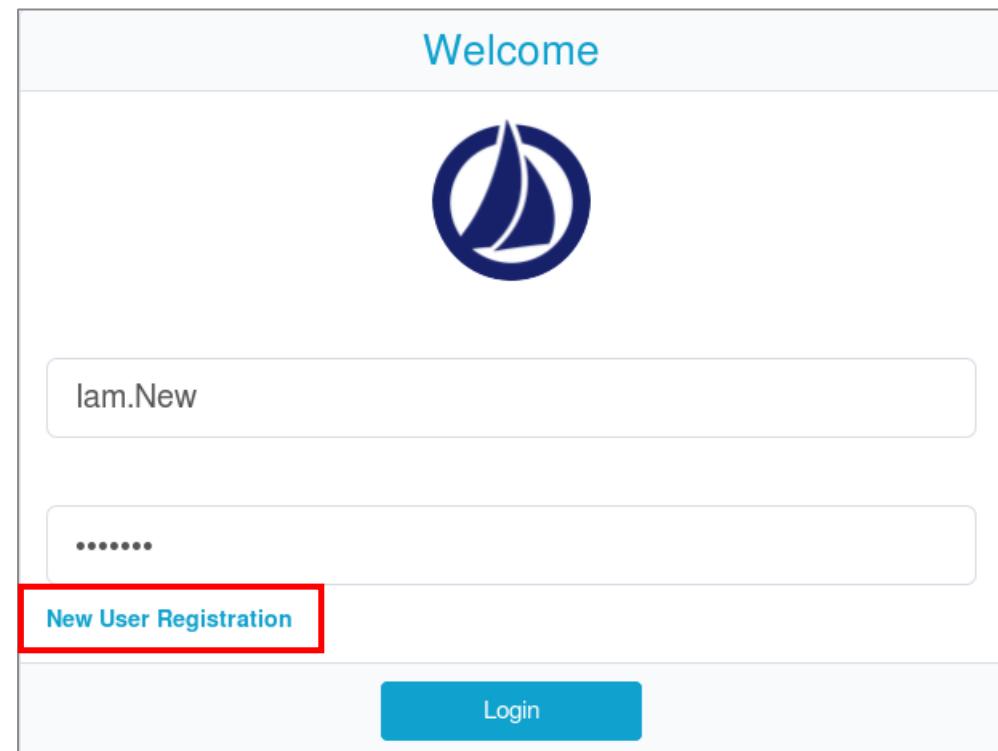
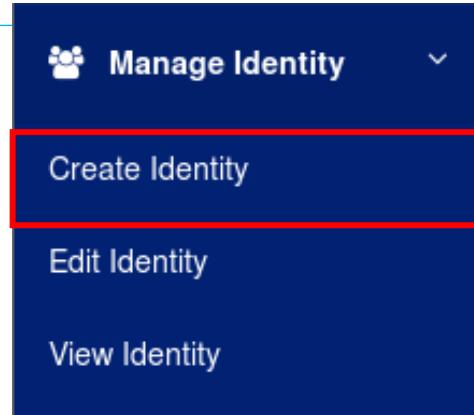


# **Configuring Manage Identity Quicklinks**

# Create Identity Options

## Two Manual Methods

- *Create Identity* Quicklink
  - Requester has IdentityIQ identity
  - Default or custom form presented to requester
- *New User Registration* link
  - Requester has no IdentityIQ identity
  - Lifecycle Manager Create Identity option
    - Enable self-service registration
    - Default = disabled
  - Default or custom form presented to requester



# Edit Identity

Manage Identity

Create Identity

**Edit Identity**

View Identity

Identity Details

Amanda.Ross

Edit Identity

The screenshot shows a user profile for 'Amanda.Ross' with a blue circular icon. Below the profile is a teal button labeled 'Edit Identity'. To the right of the profile, there is a modal window titled 'Edit Identity' with a red box highlighting the 'Department' field, which contains 'Regional Operations'.

## Edit Identity Attribute

Specify the applications and rules from which identity data is derived. Select a source mapping to change its position within the list.

### Identity Attribute

Attribute Name

department

Display Name

Department

### Advanced Options

Attribute Type

String

Edit Mode

Permanent

Searchable



Multi-Valued



Group Factory



Value Change Rule



Value Change Workflow



### Edit Identity Options

For Self

For Others

Single

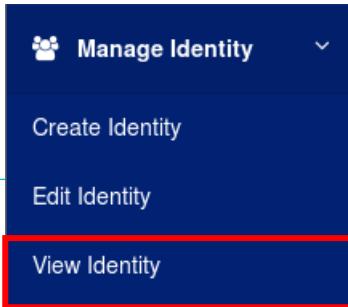
Save

Cancel

### Options

- Read Only (default)
- Temporary
- Permanent

# View Identity



The screenshot shows the 'Identity Details' page for 'Alan.Bradley'. The 'Attributes' section is highlighted with a blue background. A blue arrow points from the text 'UIConfig entry: identityViewAttributes' to the 'Attributes' section.

Attributes	
User Name	Alan.Bradley
First Name	Alan
Last Name	Bradley
Email	Alan.Bradley@demoexample.com
Manager	Eugene.Hawkins
Type	Contractor
Department	Engineering
Location	Singapore
Employee ID	1c2a3c4c
Region	Asia-Pacific
Cost Center	R02e, L04e

UIConfig entry:  
identityViewAttributes

The screenshot shows the 'View Identity Options' dialog box with the following settings:

- For Self
- For Others
- Single

**Save** **Cancel**

# Identity Provisioning Policies

Identity Create

Add Section      Preview Form

+	Section 1	<span style="color: blue;">+</span>	<span style="color: green;">-</span>	<span style="color: red;">X</span>	E
+	Instructions	<span style="color: blue;">+</span>	<span style="color: green;">-</span>	<span style="color: red;">X</span>	
+	Identity Attributes	<span style="color: blue;">+</span>	<span style="color: green;">-</span>	<span style="color: red;">X</span>	
+	Row 1	<span style="color: blue;">+</span>	<span style="color: green;">-</span>	<span style="color: red;">X</span>	
	First Name				
	Last Name				
+	Row 2				
	Password				
	Password Confirmation				
+	Row 3				
	Username				
	Display Name				
+	Row 4				
	Location				
	Region				
+	Manager				
+	Type				
+	Job Title				
+	Implicit Joiner				

**Identity Attributes**

First Name *	Joe	Last Name *	Smith
Password *	*****	Password Confirmation *	*****
Set initial password			
Username	Joe.Smith		
Location *	Austin	Region *	Americas
Manager	Adam.Kennedy		
Type *	<input checked="" type="radio"/> contractor <input type="radio"/> employee		
Job Title *	AR Accounting Manager		

# Knowledge Check

Next Step?

# Practice Exercises

# Exercise Preview

---

## Section 4, Exercise 6

- Explore Provisioning Policy for Creating Identities
  - Import Provisioning Policy
  - Create Identity
  - Investigate Policy Form





# Automated Provisioning

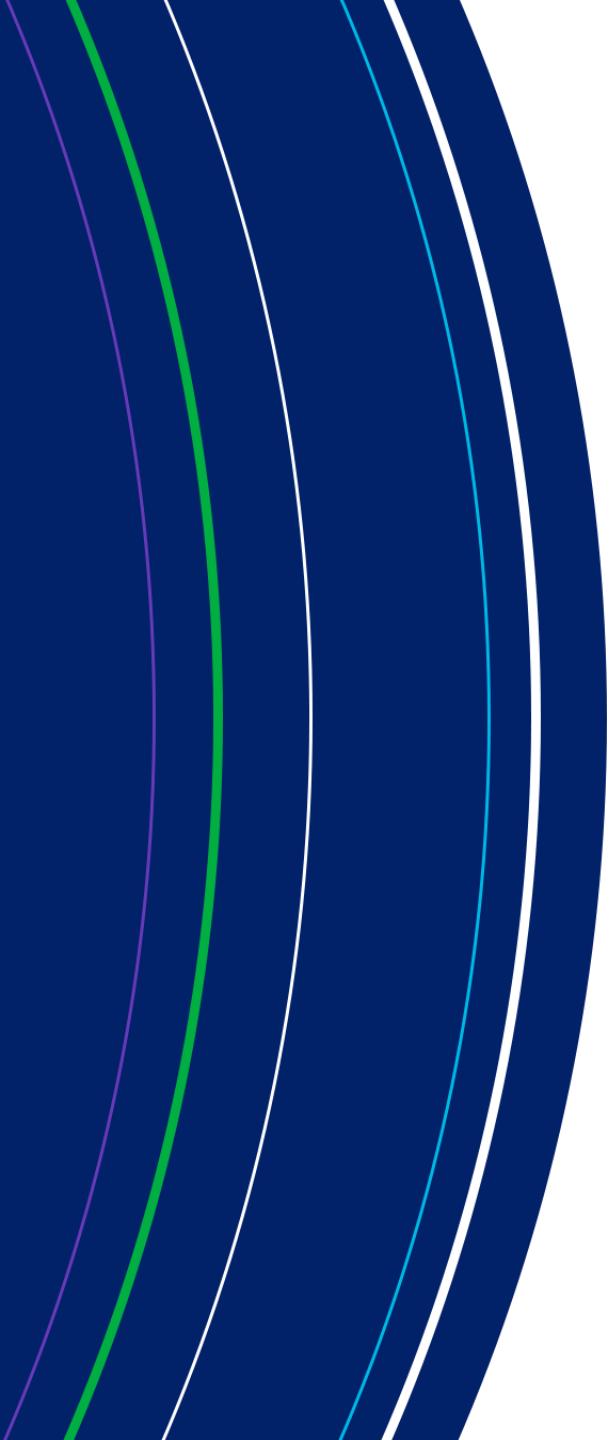
IdentityIQ Essentials

# Overview

---

## Automated Provisioning

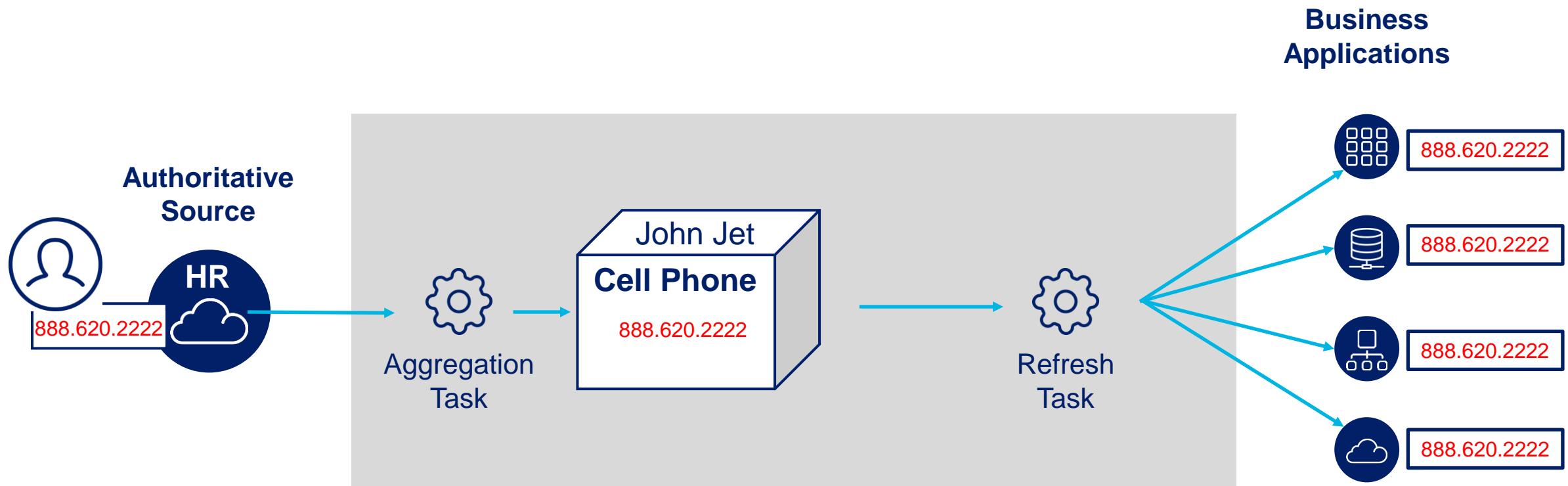
- Attribute Synchronization
- Password Interception
- Native Changes



# **Attribute Synchronization**

# Attribute Synchronization

## Process Overview



# Attribute Synchronization

## Configuration

- Add target mappings to identity attribute definitions

The screenshot shows the SailPoint Identity Mappings configuration interface. On the left, there's a sidebar with 'Source Mappings' (containing two items: 'Email from the HR System' and 'Email from the Contractor F...') and 'Target Mappings' (with 'Add Target' and 'Delete Target' buttons). The main area is titled 'Add a target to the email attribute' and contains fields for 'Application' (set to 'LDAP'), 'Attribute' (set to 'mail'), 'Transformation Rule' (set to '- Select Rule -'), and 'Provision All Accounts' (checkbox checked). At the bottom are 'Add' and 'Cancel' buttons. Three callout boxes on the right provide context: one for the application and attribute, one for transformation rules, and one for account provisioning.

Global Settings → Identity Mappings → Email

Application and attribute to synchronize to

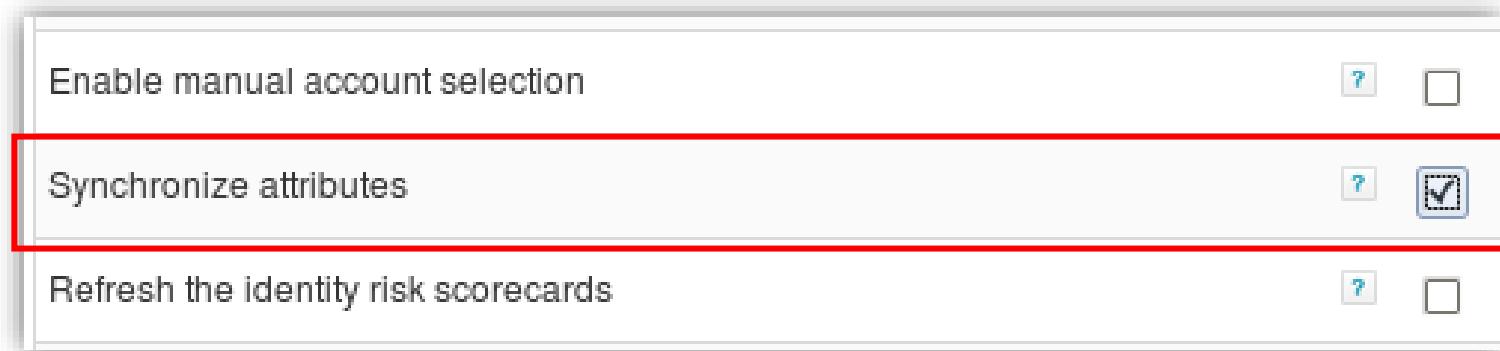
BeanShell rule for data transformation

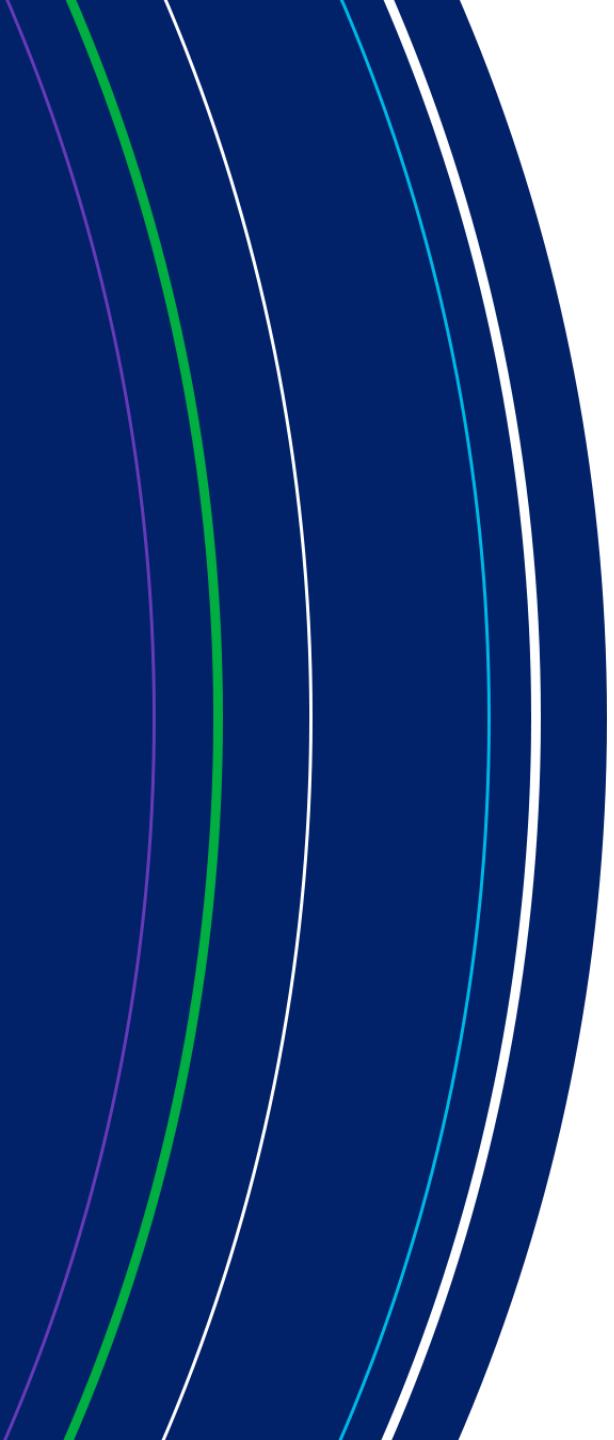
Instructions for handling multiple accounts

# Attribute Synchronization

## Operation

- Edit identity
  - LCM: Manage Identity → Edit Identity
  - Immediately invoke provisioning to target mapping(s)
- Aggregate changed identity attribute
  - **Identity Refresh Task with Synchronize attributes**

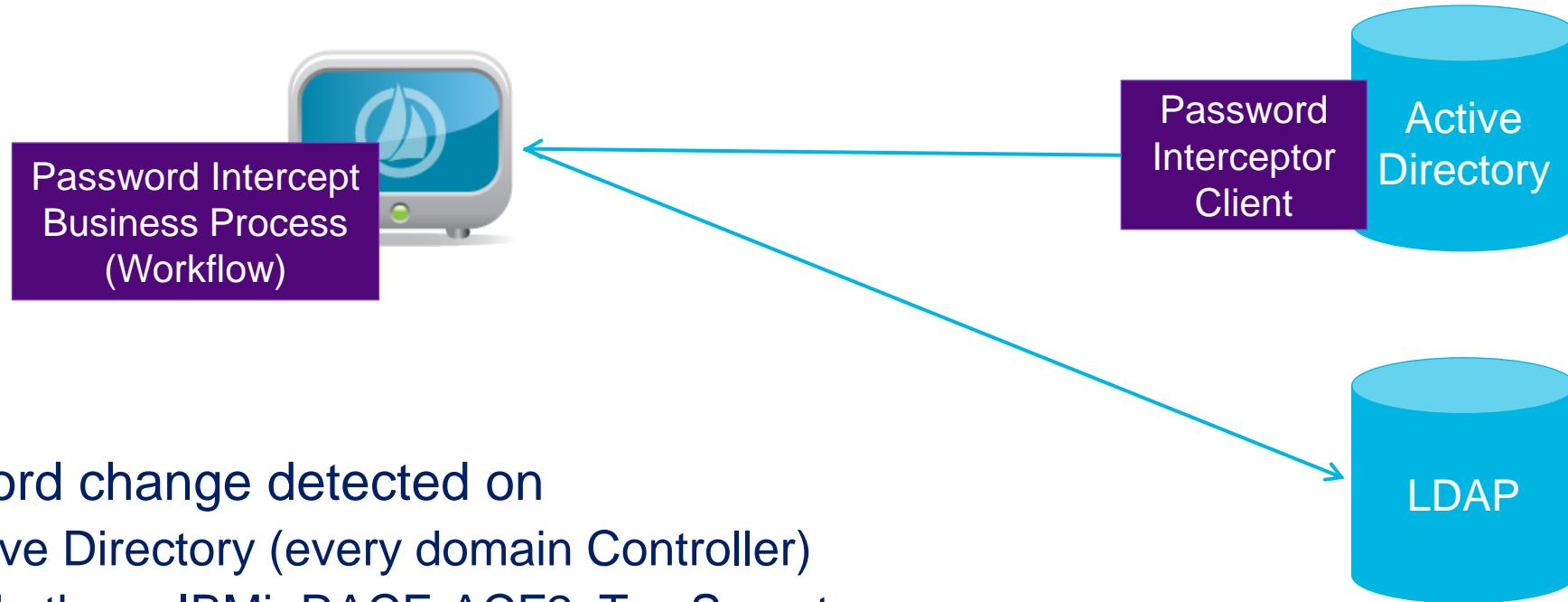




# **Password Interception**

# Password Interception

## Architecture



- Password change detected on
  - Active Directory (every domain Controller)
  - And others: IBMi, RACF, ACF2, Top Secret
- Password Interceptor Client sends password change to IdentityIQ
- IdentityIQ runs configurable Business Process (Workflow)

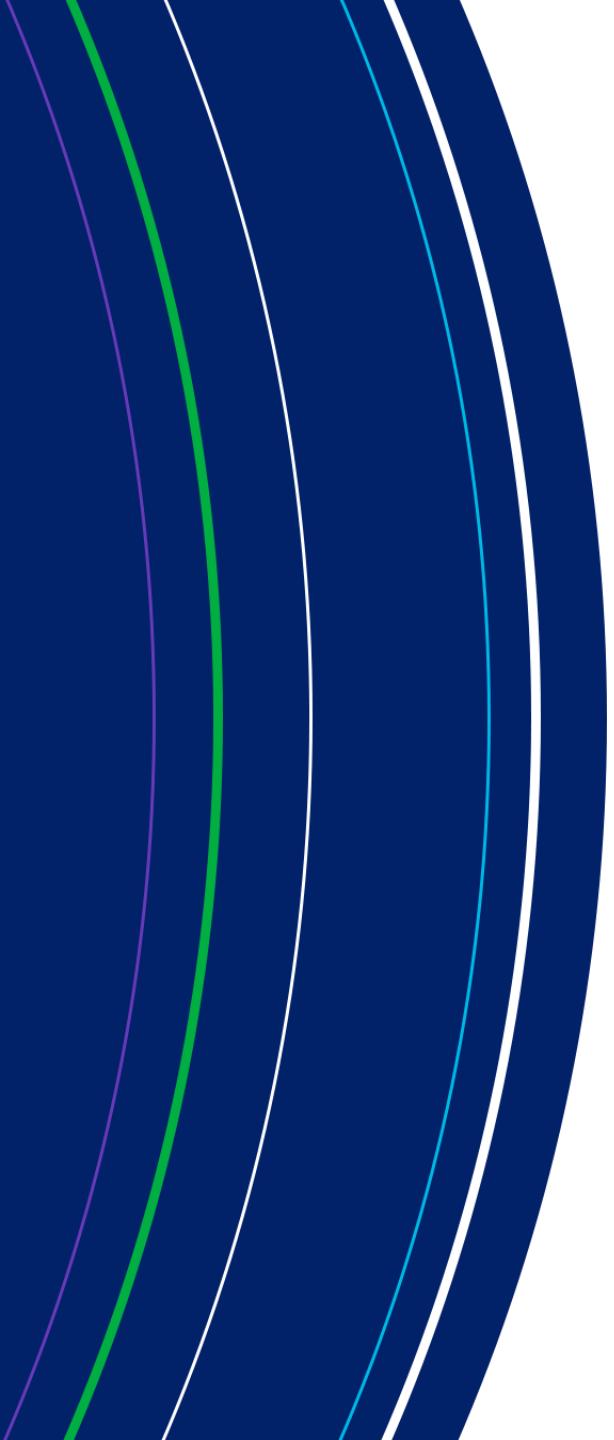
# Password Interception

## Configuration

- Install interceptor client
  - Instructions: Password Interceptor Installation and Configuration guide
- Configure Password Intercept business process
  - Options
    - Sync to all applications that support password updates (default)
    - Specify target applications



Global Settings → IdentityIQ Configuration → Miscellaneous



# Native Changes

# Native Change

---

## Definition

- A data change that is discovered at the application account level, during an aggregation process
  - Undesired, unexpected
  - Not following normal process

# Native Change Detection Events

---

## Response Options

- Automatically start a certification
  - Setup→Certifications→Certification Events→Add New Certification Event
- Lifecycle Event
  - Provided workflows
    - Lifecycle Event - Email manager for all native changes
    - Lifecycle Event - Manager approval for all native changes
  - Custom workflow

# Native Change Detection

## Configuration

- Configure native change detection per application
- Create a Native Change Lifecycle Event

The screenshot displays the configuration interface for Native Change Detection, divided into two main sections: Application and Behavior.

**Application Tab:**

- Native Change Detection:** A checkbox labeled "Native Change Detection" is checked and highlighted with a red box.
- Native Change Operations:** A group of checkboxes for "Create", "Modify", and "Delete" are checked and highlighted with a red box.
- Attributes to detect:** A section where "Entitlements" is selected (radio button highlighted with a red box) over "User Defined".

**Behavior Tab:**

**Lifecycle Event Options:**

- Name:** "Native Change Detection" (highlighted with a red box)
- Description:** "This event runs whenever we have a native change"
- Event type:** "Native Change" (highlighted with a red box)
- Disabled:** An unchecked checkbox.
- Included Identities:** "All" (highlighted with a red box)
- Business Process:** "Lifecycle Event - Manager Approval for all native changes" (highlighted with a red box)

\* Indicates a required field.

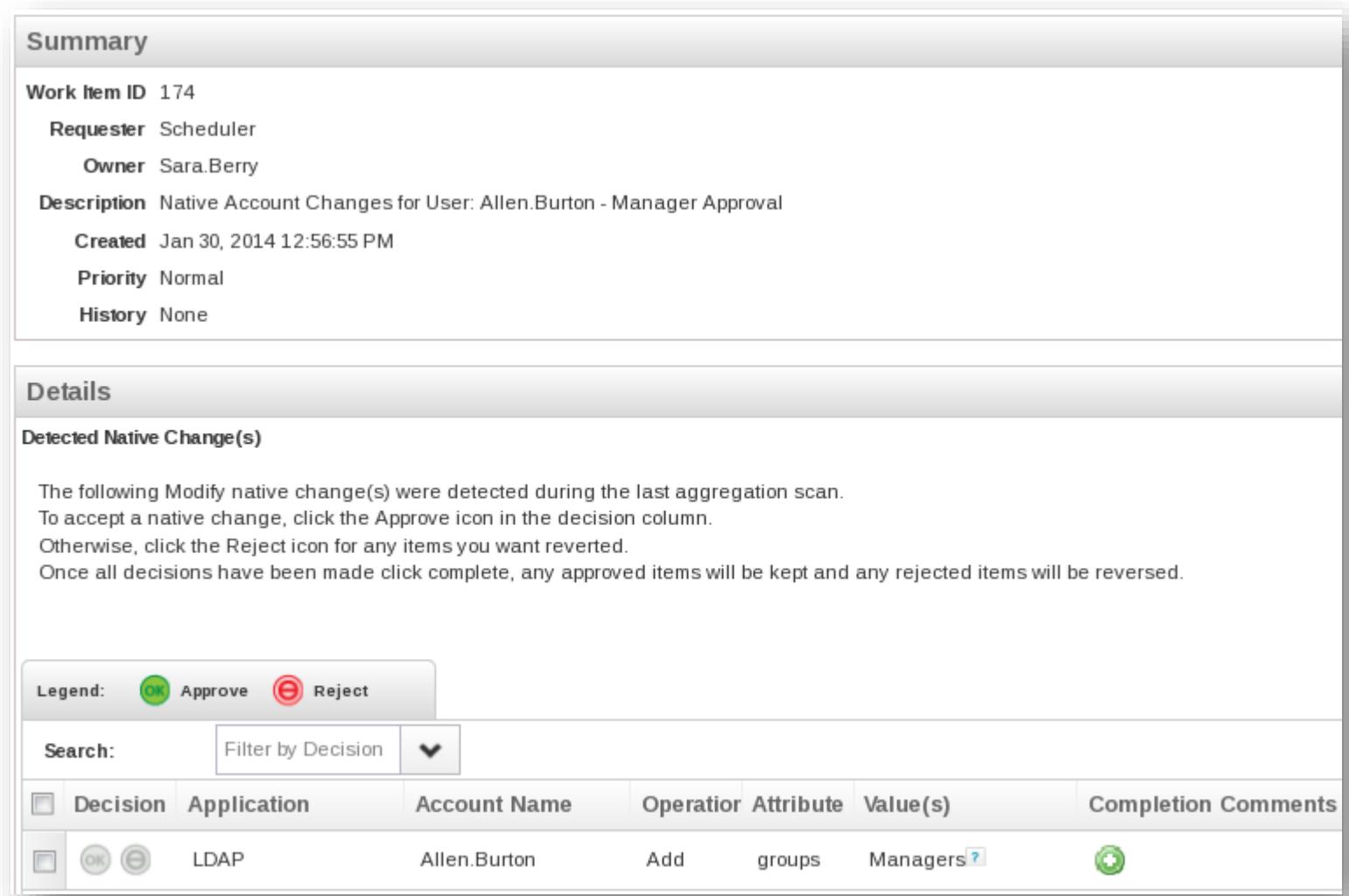
# Native Change Detection

## Operation

- Run aggregation task to mark changed cubes

Process Changes  


- Run Identity Refresh with “Process Events” checked
  - Runs workflow



The screenshot shows the SailPoint interface for managing native changes. The top section is the 'Summary' page for Work Item ID 174, created by Scheduler on Jan 30, 2014. It includes fields for Owner (Sara.Berry), Description (Native Account Changes for User: Allen.Burton - Manager Approval), Priority (Normal), and History (None). Below is the 'Details' page, which lists 'Detected Native Change(s)'. A legend indicates that green 'OK' icons represent approved changes and red 'Reject' icons represent rejected changes. A message states: "The following Modify native change(s) were detected during the last aggregation scan. To accept a native change, click the Approve icon in the decision column. Otherwise, click the Reject icon for any items you want reverted. Once all decisions have been made click complete, any approved items will be kept and any rejected items will be reversed." A table at the bottom shows a single detected change for user Allen.Burton, application LDAP, operation Add, attribute groups, value Managers, and status Approved.

Decision	Application	Account Name	Operator	Attribute	Value(s)	Completion	Comments
<input type="checkbox"/>  	LDAP	Allen.Burton	Add	groups	Managers 		

# Lifecycle Event: Native Change Detection

---

## Best Practices

- Aggregate all accounts without native change detection, then activate
- Process changes regularly
- Avoid monitoring native change for applications where native changes are expected

# Knowledge Check

# Practice Exercises

# Exercise Preview

---

## Section 4, Exercise 8

- Define and Test Attribute Synchronization
  - Configure Attribute Synchronization
  - Test Attribute Synchronization





# Other Provisioning Requests

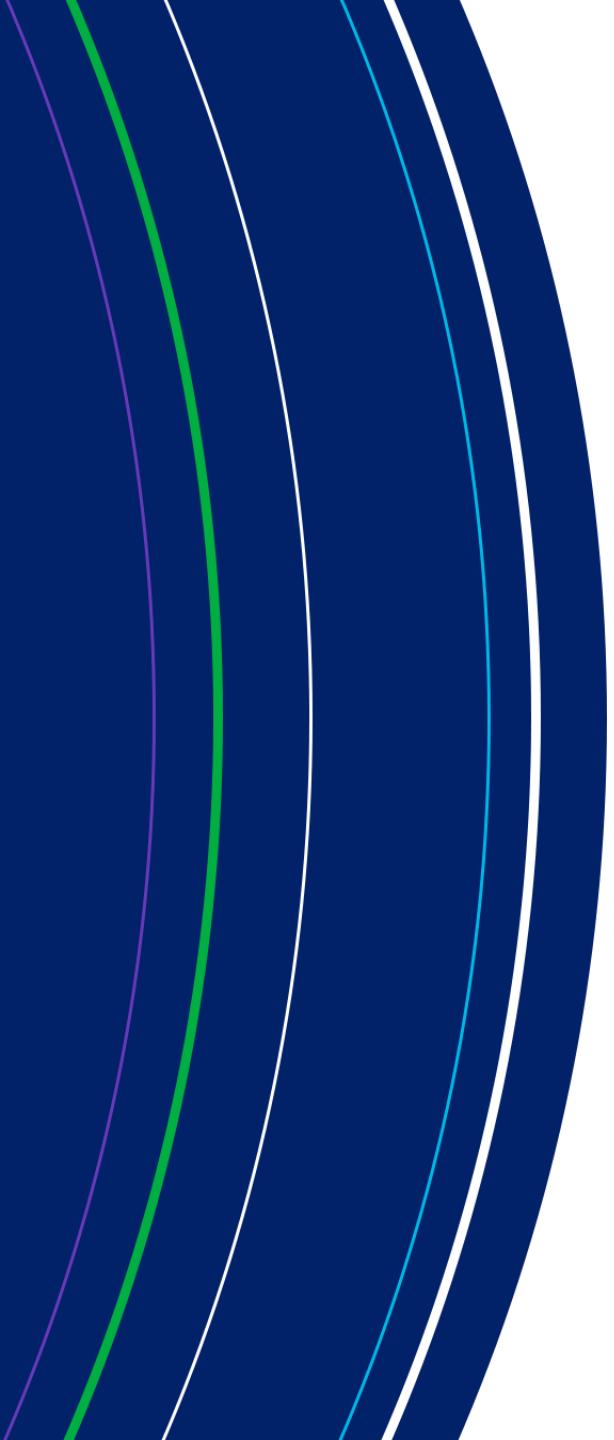
IdentityIQ Essentials

# Overview

---

## Other Provisioning Requests

- Account Group Provisioning
- Batch Requests
- Rapid Setup Identity Termination

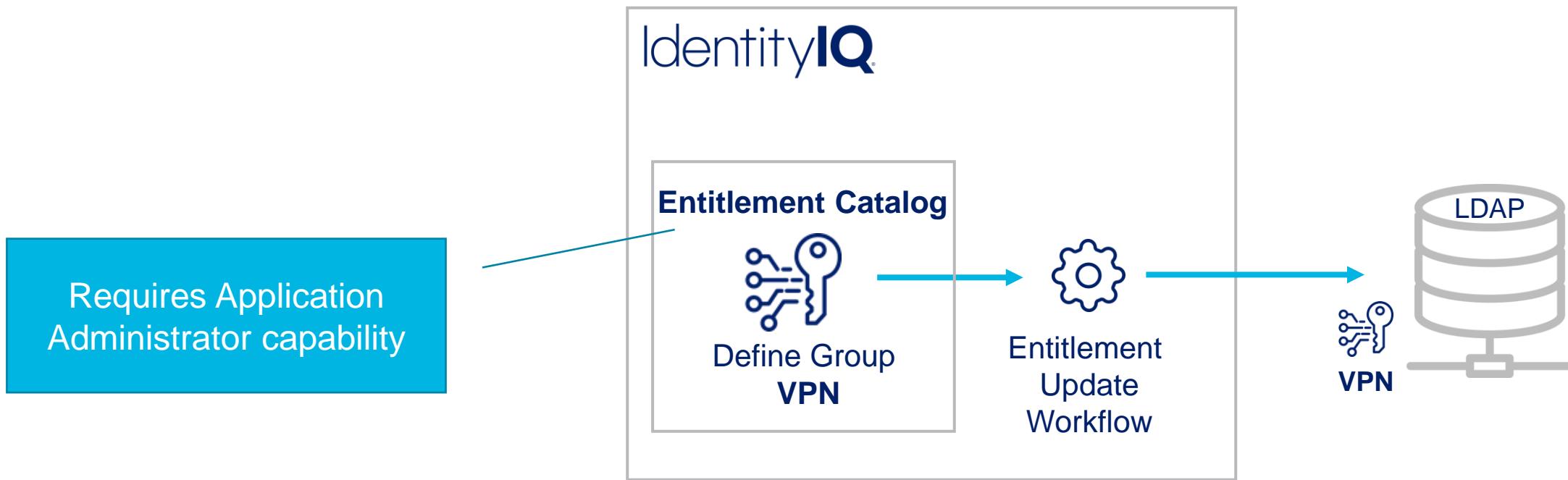


# **Account Group Provisioning**

# Account Group Provisioning

## Overview

- Create new groups
- Update group definitions



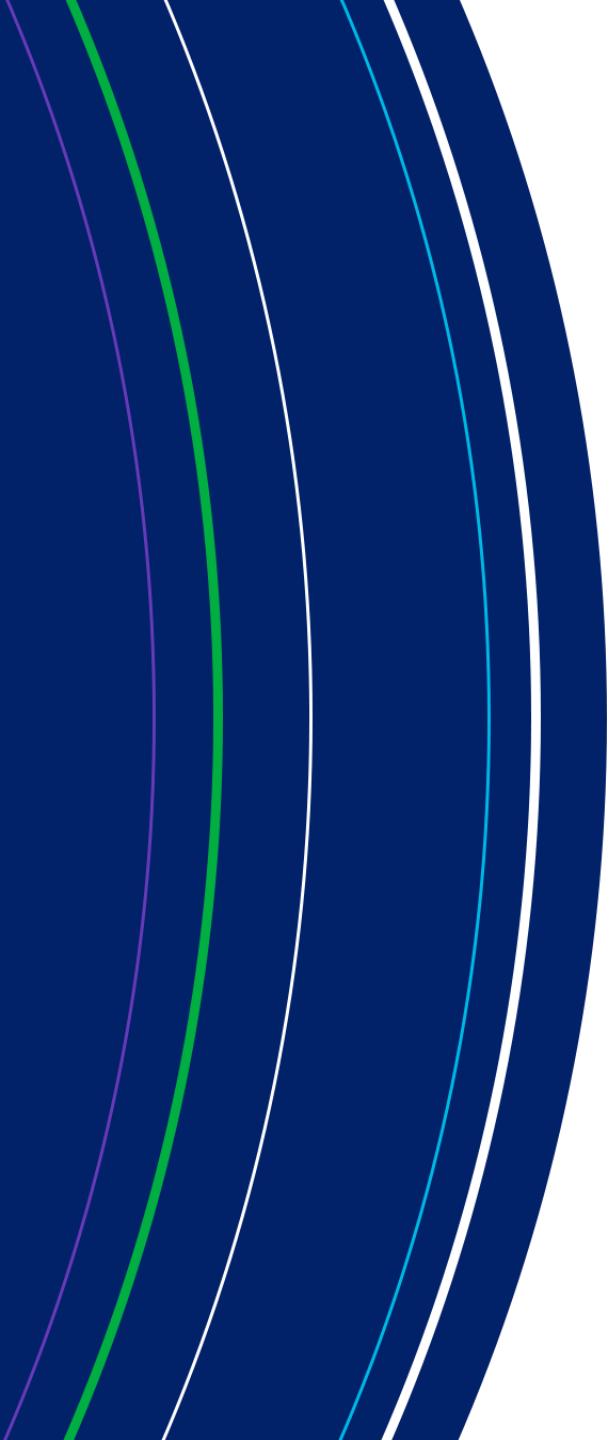
# Account Group Provisioning

## Configuration

The screenshot shows two panels. The left panel is titled 'Lifecycle Manager' with tabs for 'Configure', 'Business Processes', and 'Identiti'. Under 'Configure', there's a 'General Options' section with a 'Starts With' filter and checkboxes for 'Allow requesters to set request priorities' (unchecked) and 'Enable Account Group Management' (checked). A blue callout box labeled '1' points to the 'Enable Account Group Management' checkbox with the text 'Enable group provisioning'. The right panel is titled 'Application' with tabs for 'Details', 'Configuration', 'Correlation', 'Accounts', 'Settings', 'Schema', and 'Provisioning Policies'. The 'Provisioning Policies' tab is highlighted with a red border. It shows 'Object Type: group' with 'Type' and 'Name' columns. Under 'Create', it says 'group create'. Under 'Update', it says 'edit group'. A blue callout box labeled '2' points to the 'group create' entry with the text 'Configure group Create and Update'.

## Usage

The screenshot shows the 'Entitlement Catalog' interface with a search bar containing 'ldap', an 'Advanced Search' button, and buttons for 'Import', 'Export', and 'Add New Entitlement'. Below the search bar is a table header with columns: Application, Attribute, Display Name, Type, Description, Owner, and Requestable. A blue callout box labeled 'Click to edit' points to the 'Edit' icon in the 'Type' column of a row. Another blue callout box labeled 'Create New' points to the 'Add New Entitlement' button.



# Batch Requests

# Identity Batch Request

- Support mass identity change requests via file upload
- Supplemental to aggregation or access request processes



# Identity Batch Request

- Batch request management
  - Process mass identity changes via a file upload
- Operations Supported
  - Create/Modify Identity
  - Create/Delete Account
  - Enable/Disable Account
  - Unlock Account
  - Add/Remove Role
  - Add/Remove Entitlement
  - Change Password

**Required Capabilities:**  
System Administrator or  
Batch Request Administrator

Setup ▾

Certifications

Roles

Policies

Alerts

Tasks

Groups

Business Processes

Lifecycle Events

Batch Requests

Setup → Batch Requests

# Batch Request Data Format

---

## Example 1

operation, name, location, email, department

CreateIdentity, Alex Smith, Austin, asmith@adept.com, Accounting

CreateIdentity, Bob Smith, Austin, bsmith@adept.com, Engineering

CreateIdentity, Mark Smith, Austin, msmith@adept.com, Accounting

CreateIdentity, John Smith, Austin, jsmith@adept.com, Finance

## Example 2

operation, name, location, email, department

ModifyIdentity, Rojit Patel, Austin, rpatel@adept.com, Accounting

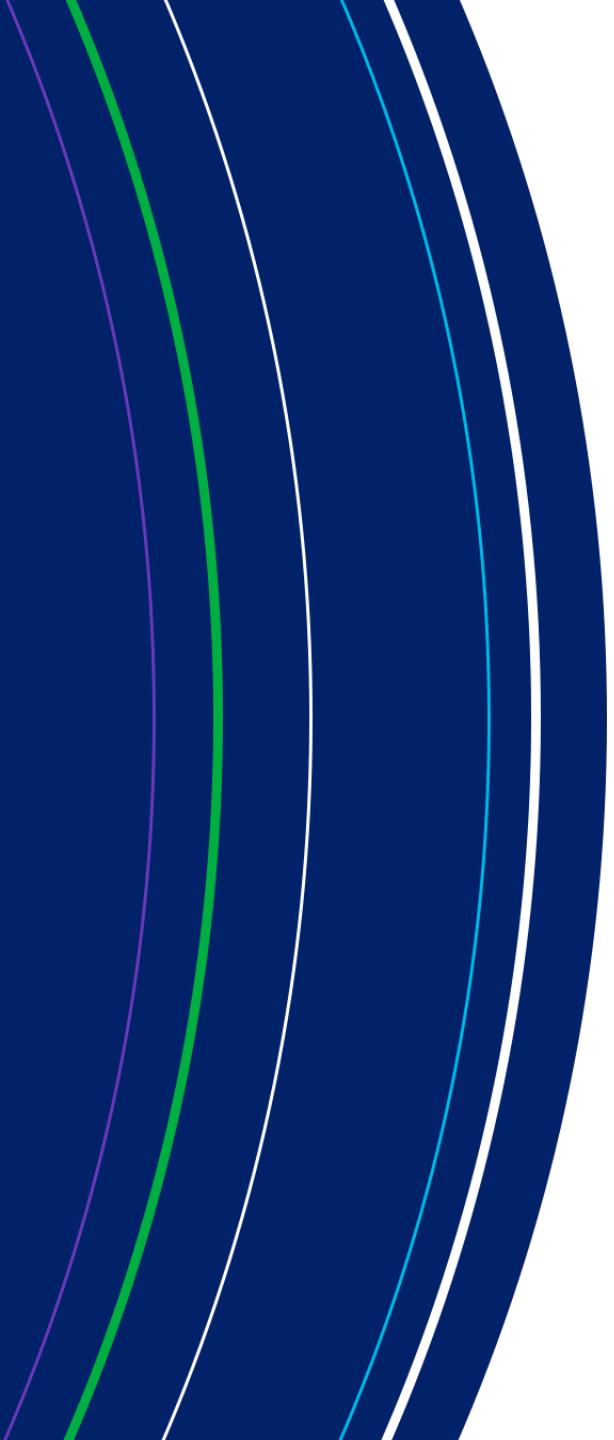
ModifyIdentity, Cindi Yu, Austin, cyu@adept.com, Engineering

ModifyIdentity, Jessie Johnson, Austin, jjohnson@adept.com, Accounting

ModifyIdentity, Ewin James, Austin, ejames@adept.com, Finance

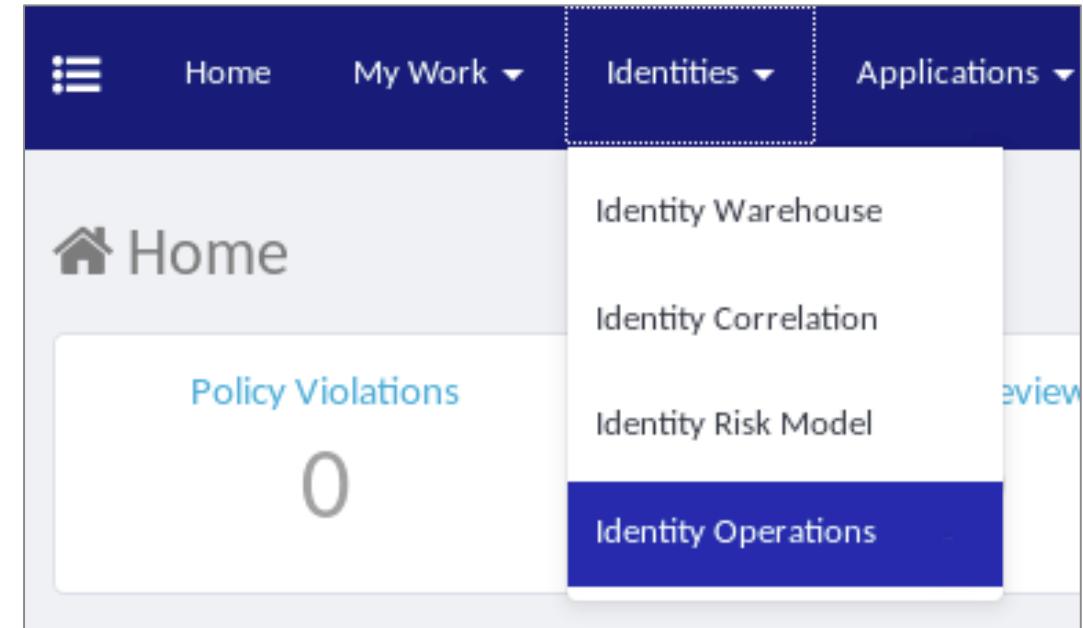
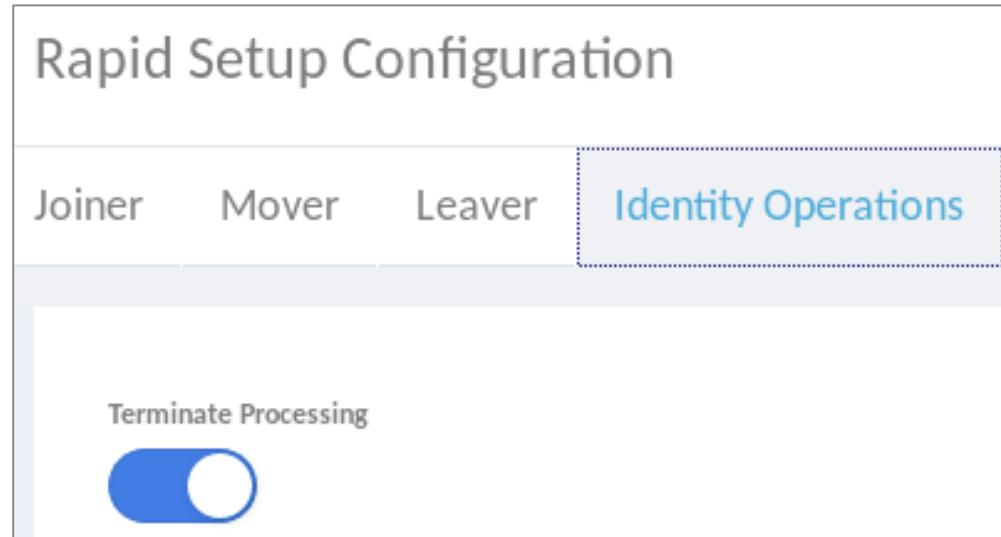
## Documentation

- *Users Guide*



# Identity Termination

# Rapid Setup Identity Termination



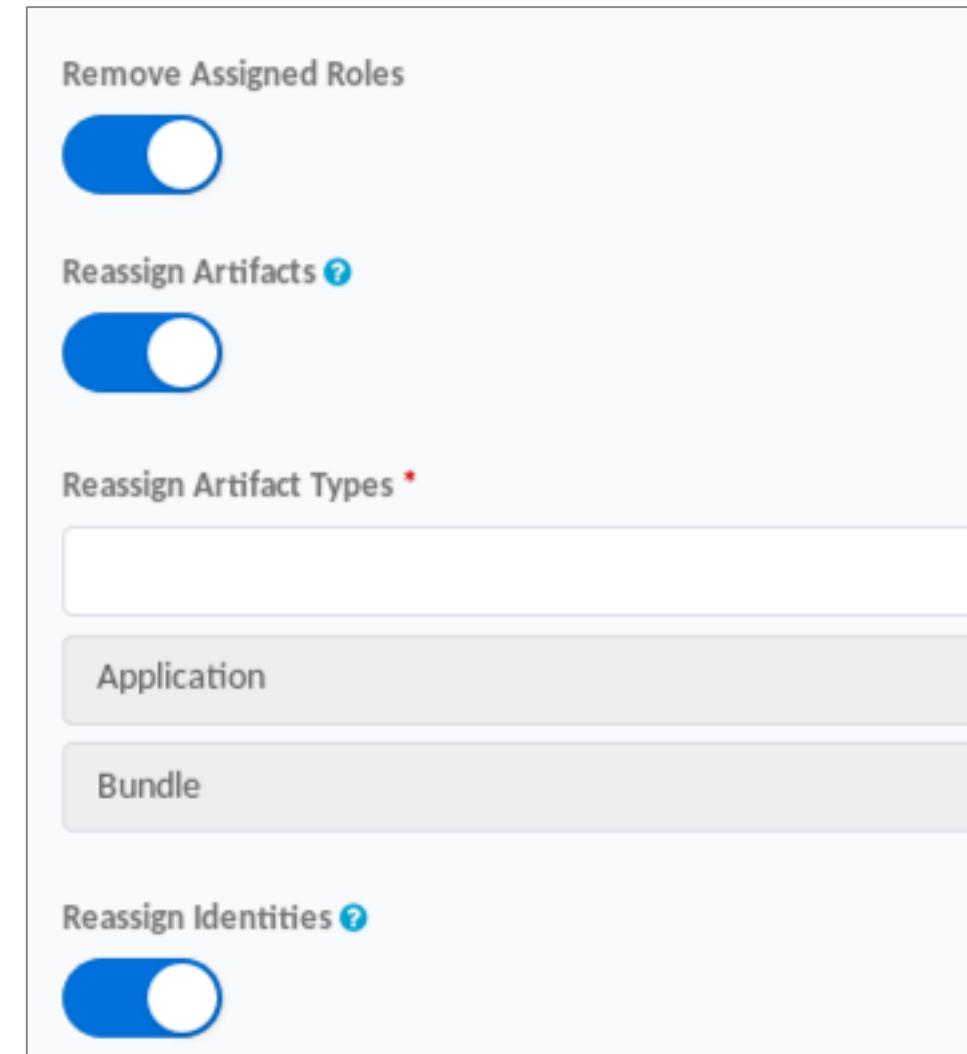
## Required Capabilities:

- System Administrator
- Rapid Setup Identity Operations Administrator

# Rapid Setup Identity Termination

## Global Configuration

- IdentityIQ-internal actions
  - Remove assigned roles
  - Reassign owned artifacts
    - Which ones, to whom
  - Reassign RPA/Service Identities
- Approvals
- Notification
  - Manager or workgroup
  - Email templates
- Logic Controls
  - Business process
  - Post leaver rule

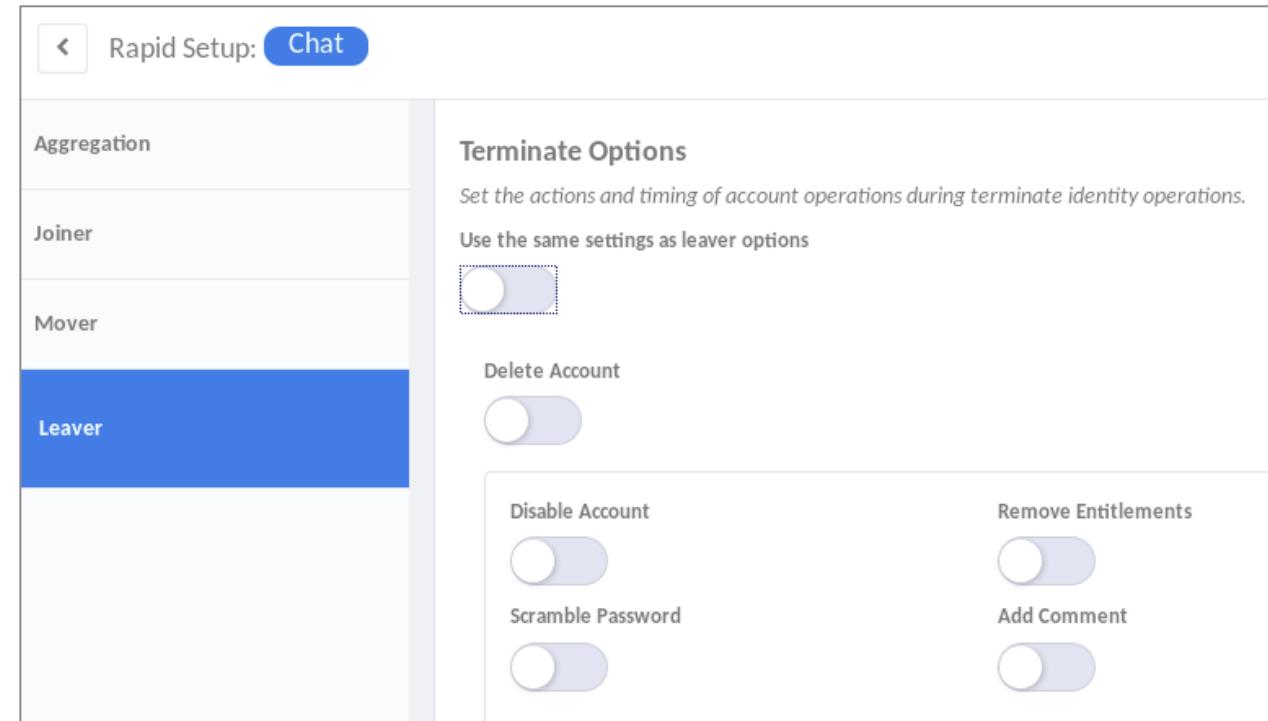


Global Settings → Rapid Setup Configuration → Identity Operations

# Rapid Setup Identity Termination

## Per Application Configuration

- Delete account
- Disable account
- Scramble password
- Remove entitlements
  - Keep certain entitlements
- Add comments
- Active Directory only: Move OU
- Immediate or delayed (# of days)



Applications → Rapid Setup → [Application] → Leaver

# Rapid Setup Identity Termination

## Termination Process

Identity Operations

1 Select Identity Find and select an identity

2 Choose Operation Select an operation to perform

3 Review and Submit Look over your selections and confirm

Identity Operations

1 Select Identity Find and select an identity

2 Choose Operation Select an operation to perform

3 Review and Submit Look over your selections and confirm

Identity Operations

1 Select Identity Find and select an identity

2 Choose Operation Select an operation to perform

3 Review and Submit Look over your selections and confirm

Identity Selected: Heather.Wallace

Heather.Wallace

Username: Heather.Wallace  
Manager: Patrick.Jenkins

Identity Selected: Heather.Wallace

Choose an op

Terminate

Reason \*

Breach of contract

Review and confirm your selections

⚠ Terminate

Full Name : Heather.Wallace  
Manager : Patrick.Jenkins  
Email Address :  
Reason : Breach of contract

Previous Cancel Submit

The image displays three sequential screenshots of a web-based application for terminating identities. The first screenshot shows the 'Select Identity' step, where 'Heather.Wallace' is selected from a list. The second screenshot shows the 'Choose Operation' step, specifically the 'Terminate' option, with a reason 'Breach of contract' chosen. The third screenshot shows the 'Review and Submit' step, displaying the full details of the termination request: Full Name (Heather.Wallace), Manager (Patrick.Jenkins), Email Address (not provided), and Reason (Breach of contract). At the bottom of each step, there are navigation buttons: 'Previous', 'Cancel', and 'Submit'.

# Knowledge Check

# Practice Exercises

# Exercise Preview

---

## Section 4, Exercise 9

- Define and Test Leaver Processes
  - Configure Rapid Setup Leaver process
  - Execute Leaver process
  - Configure Rapid Setup Identity Termination
  - Execute immediate termination





# System Architecture and Deployment

IdentityIQ Essentials

# Overview

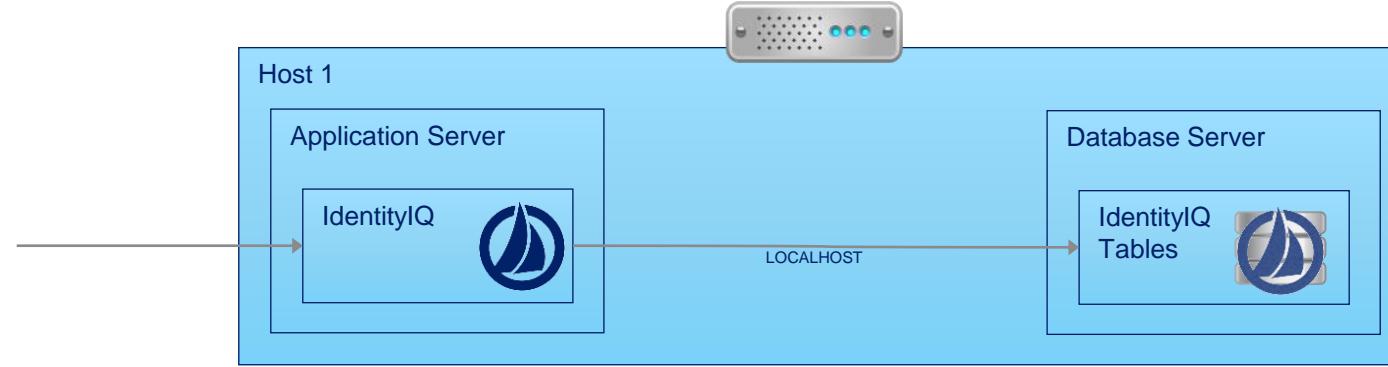
---

## System Architecture and Deployment

- Server Architectures
- Deployment Options

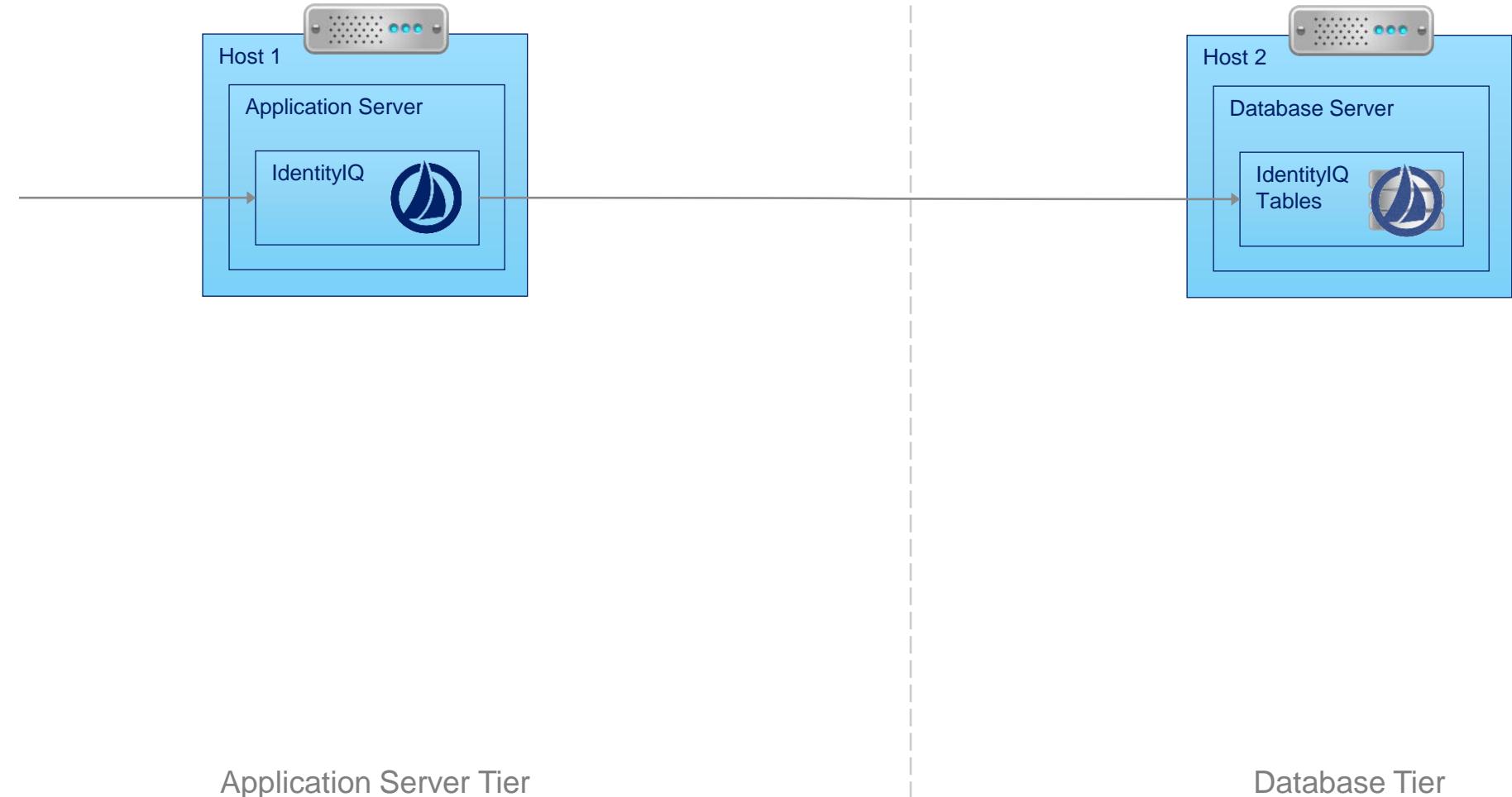
# Architecture

## Simplest Model



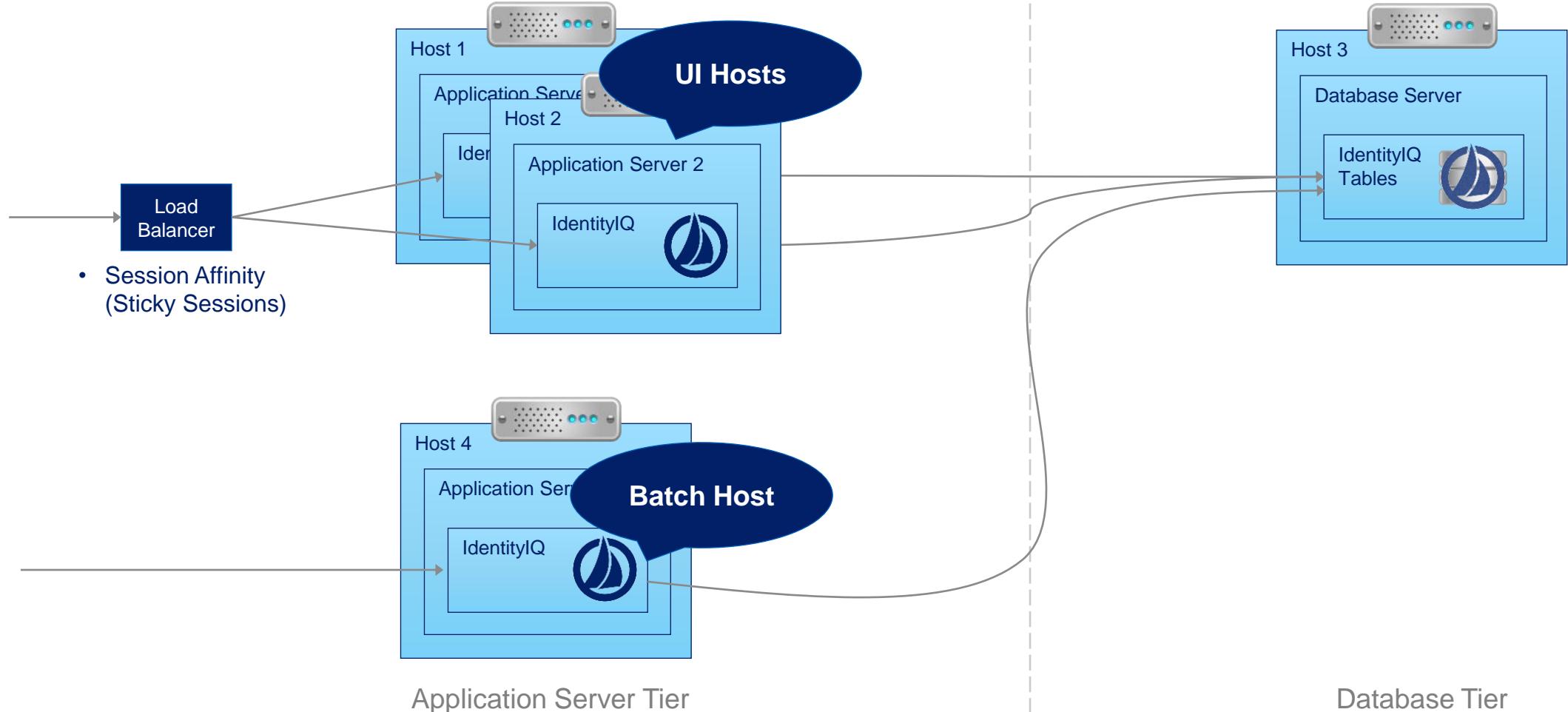
# Architecture

## Processing and Storage Segregation



# Architecture

## Application Server Availability / Redundancy



# Multi-host Deployments

## UI versus Batch Hosts

	Batch hosts	UI hosts
What's processed?	<ul style="list-style-type: none"><li>• Tasks/reports</li><li>• Workflows</li><li>• Certification generation</li><li>• Etcetera</li></ul>	<ul style="list-style-type: none"><li>• Access Requests</li><li>• Access Reviews (certifications)</li><li>• Dynamic Analytics</li><li>• Etcetera</li></ul>
What designates host type?	Named in task and request service definitions	Pointed to by load balancer

```
<ServiceDefinition created="1388105905701" hosts="HostA,HostB"  
id="ff80808143318eba0143318f362500f8" name="Request">
```

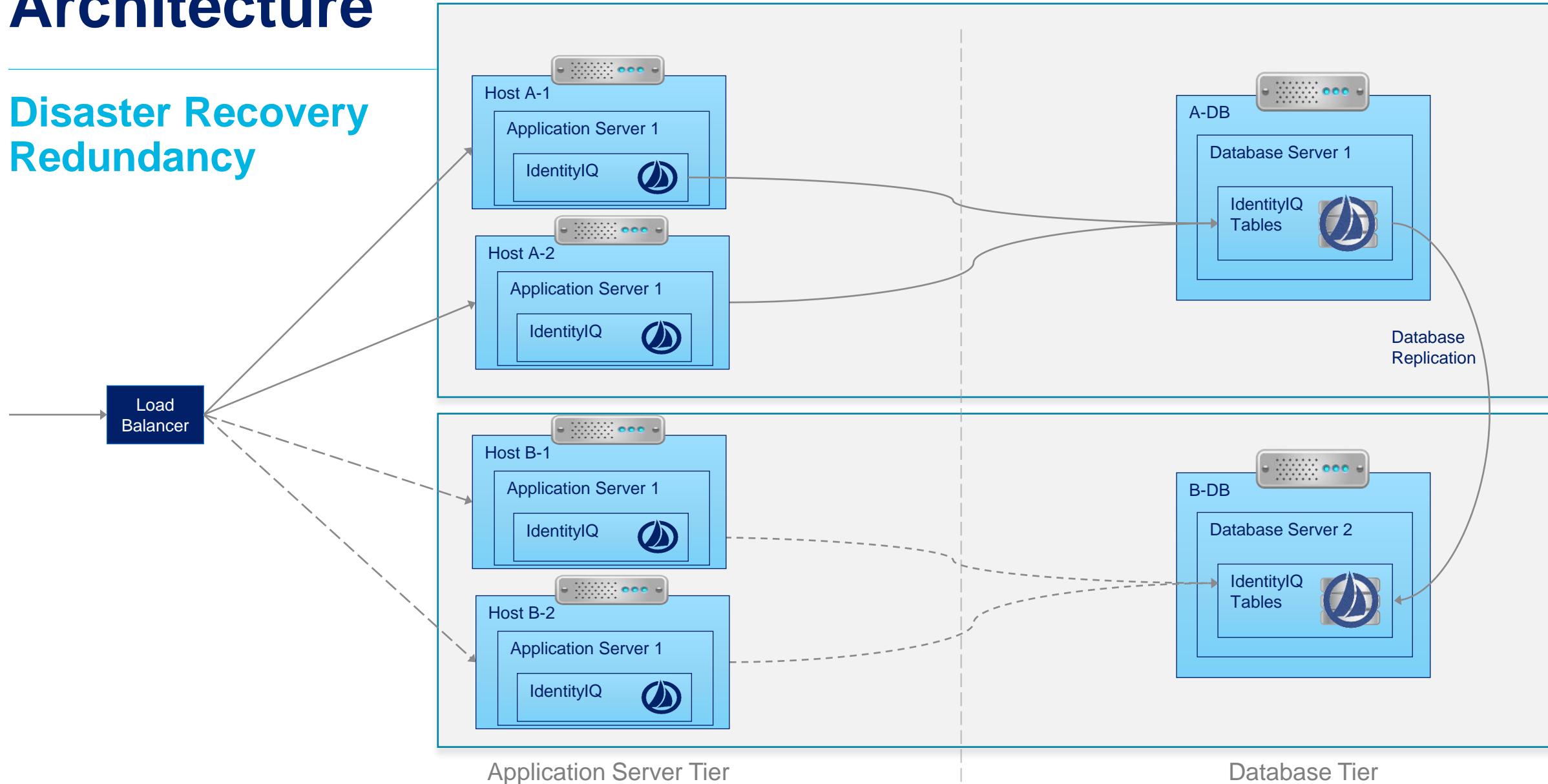
```
<ServiceDefinition created="1388105905677" hosts="HostA,HostB"  
id="ff80808143318eba0143318f360d00f7" name="Task">
```

Batch hosts

For more details see Compass article: *Background Processing in IdentityIQ: The TaskScheduler and RequestScheduler*

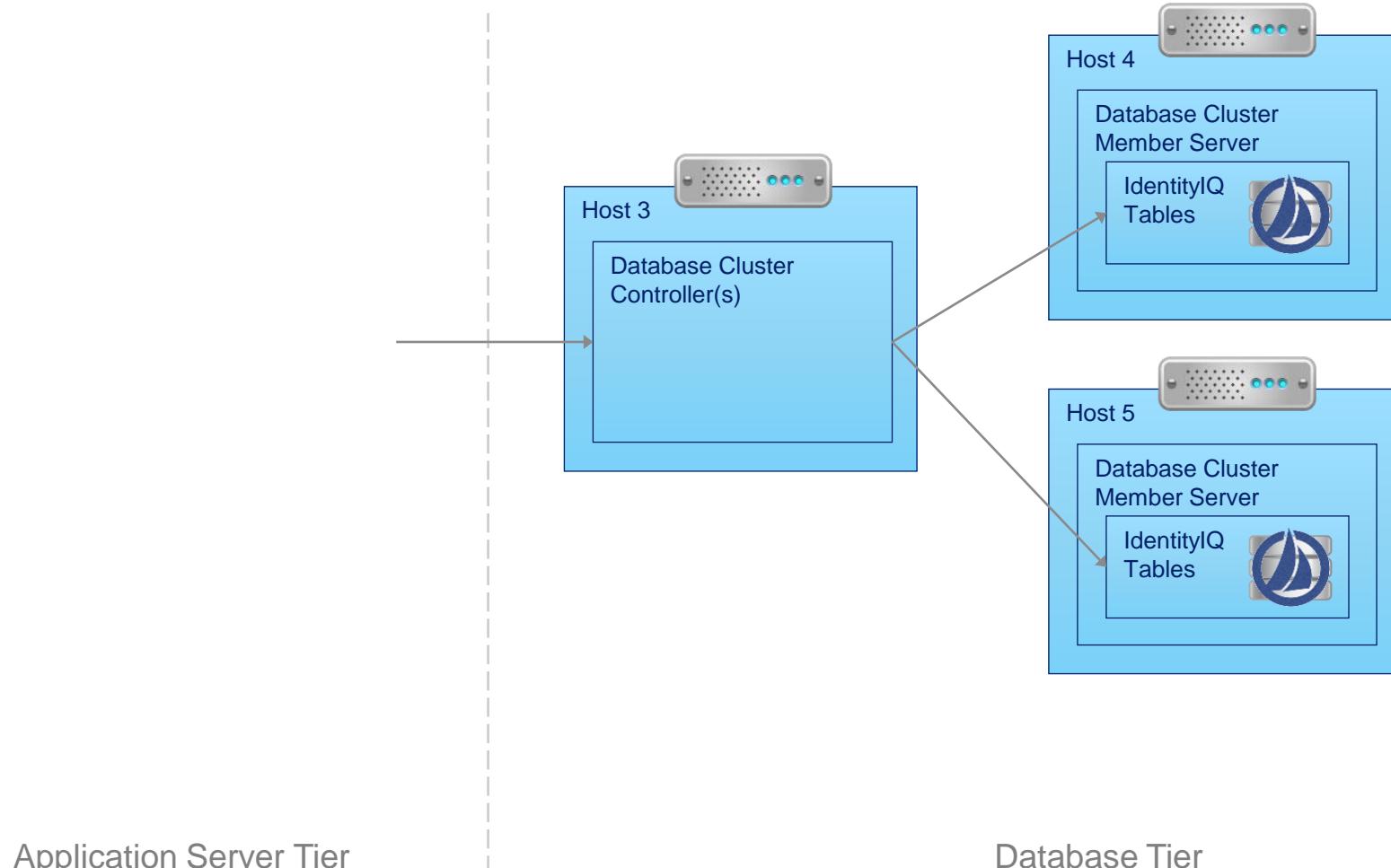
# Architecture

## Disaster Recovery Redundancy



# Other Architectures

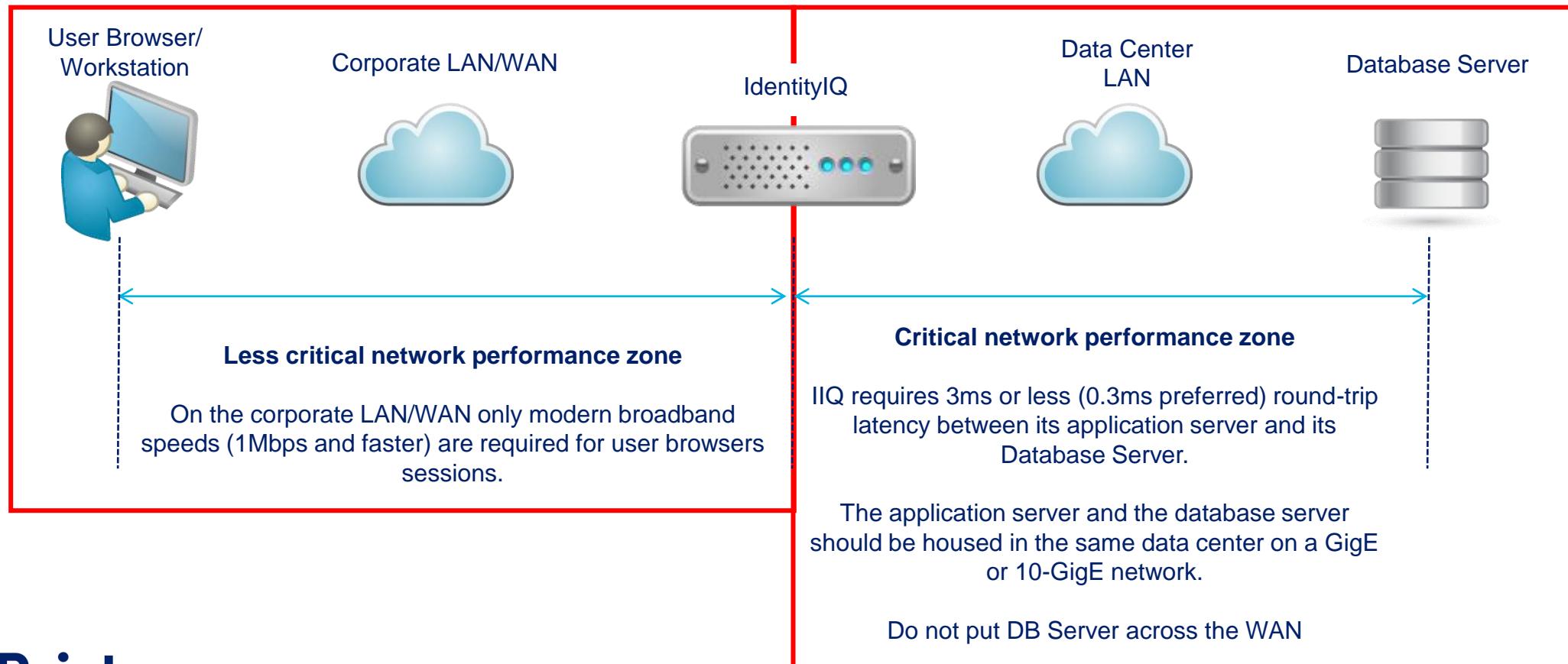
## Database Clustering



# Deployment Database Considerations

## Network

- Latency between the Application tier to the Database tier is extremely important for IdentityIQ



# Deployment Options

---

## Data Center

- Delivered from your own data center
- Managed by your own team

## Public Cloud

- Hosted on a cloud platform
- Managed by your own team

## Cloud Managed Service

- Delivered and administered by a trusted provider

# Cloud Managed Service

---

## Typical Service Offerings

- IdentityIQ
  - Upgrading
  - Patching
- Monitoring and support of infrastructure
  - Operating system
  - Application server
  - Database

# Knowledge Check





# Deployment Process Management

IdentityIQ Essentials

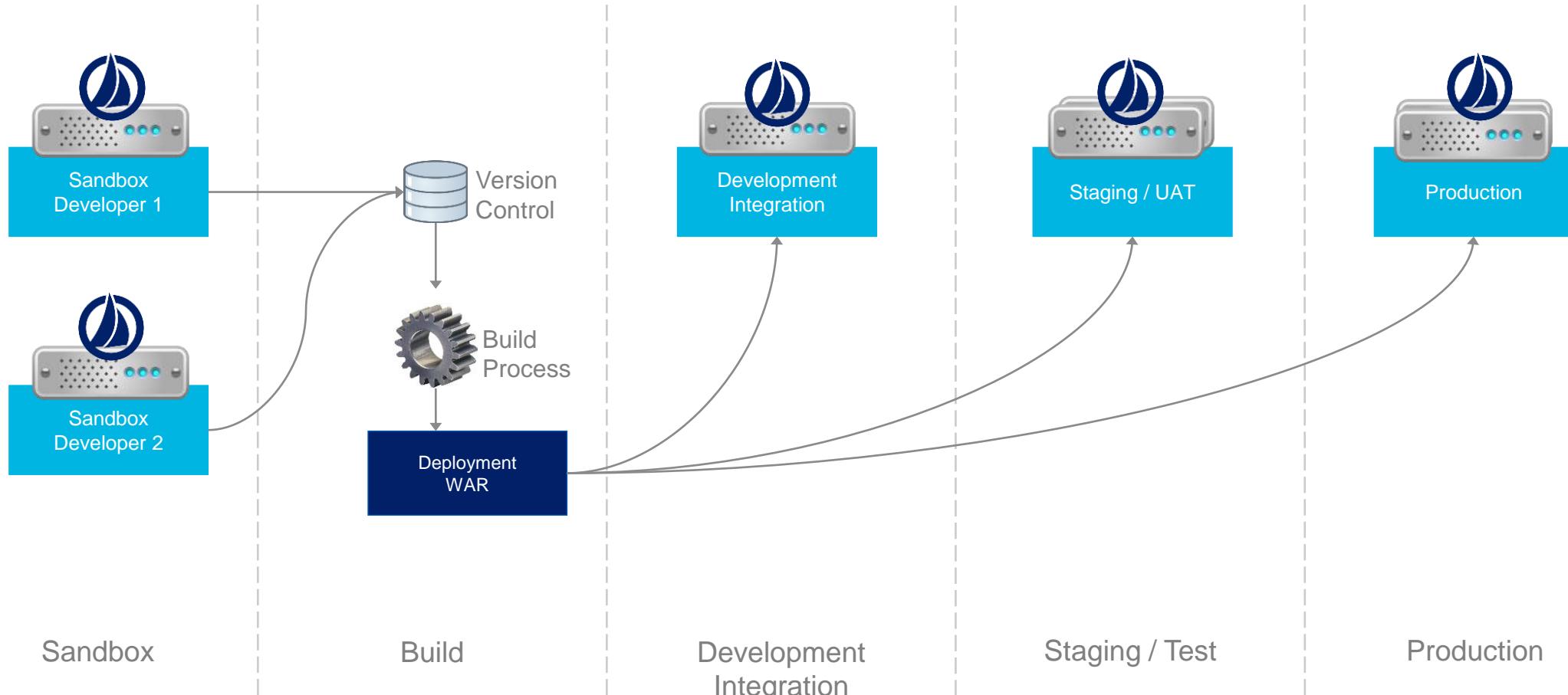
# Deployment Strategy

---

- Sandbox – Developer Environment
  - Individual IdentityIQ system per developer
  - Typically limited memory, disk space and running in a VM
  - Load small amount of representative data
- Development – Unit Test Environment
  - System for multiple developers to test code together
  - Load small amount of representative data
- Staging –Test Environment
  - User acceptance, functional testing, etc.
  - Similar to production
  - Can be used for performance and stress testing
- Production Environment
  - Incorporates redundancy and failover

# Deployment Strategy

## Environment Management



# Build Process

---

## Services Standard Build (SSB)

- Created and used by SailPoint Professional Services
- Automates packaging and deployment of custom objects and code
  - Supports token replacement – useful for dissimilar environments
- Build configuration for Apache Ant build tool
- Utilize directly or as a model for creating a build process
- Available on Compass

# Knowledge Check





# Getting Help

IdentityIQ Essentials

# Compass – A Valuable Resource

---

- Compass is the SailPoint collaborative customer and partner community for sharing product knowledge and experience
  - <https://community.sailpoint.com>
- Compass includes
  - Discussion forums
  - Product releases for download
  - Technical whitepapers
  - Support cases
  - Redirect to Identity University for self-paced training materials, schedules and registration for open enrollment courses
    - <https://university.sailpoint.com>

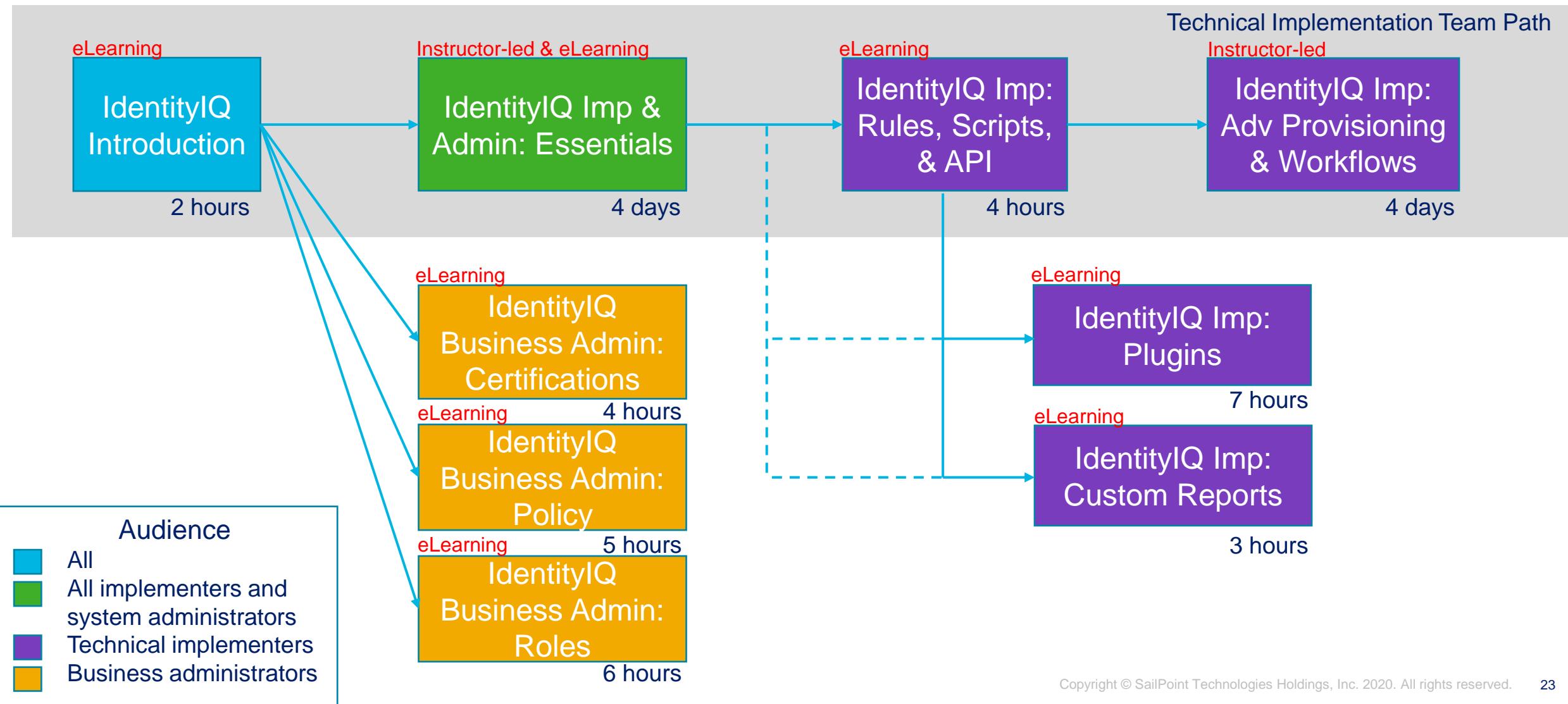
# When Compass isn't Enough

---

## Options

- SailPoint support
  - Assistance with product issues
- SailPoint Expert Services
  - Augment your technical team
- Customer Success Manager / Partner Success Manager
  - Your SailPoint advocate

# Continuing Education



# New Training Validation Certifications

## SailPoint Associate and SailPoint Professional

