Roles

Fundamentals of IdentityIQ Implementation

IdentityIQ 7.0

Overview

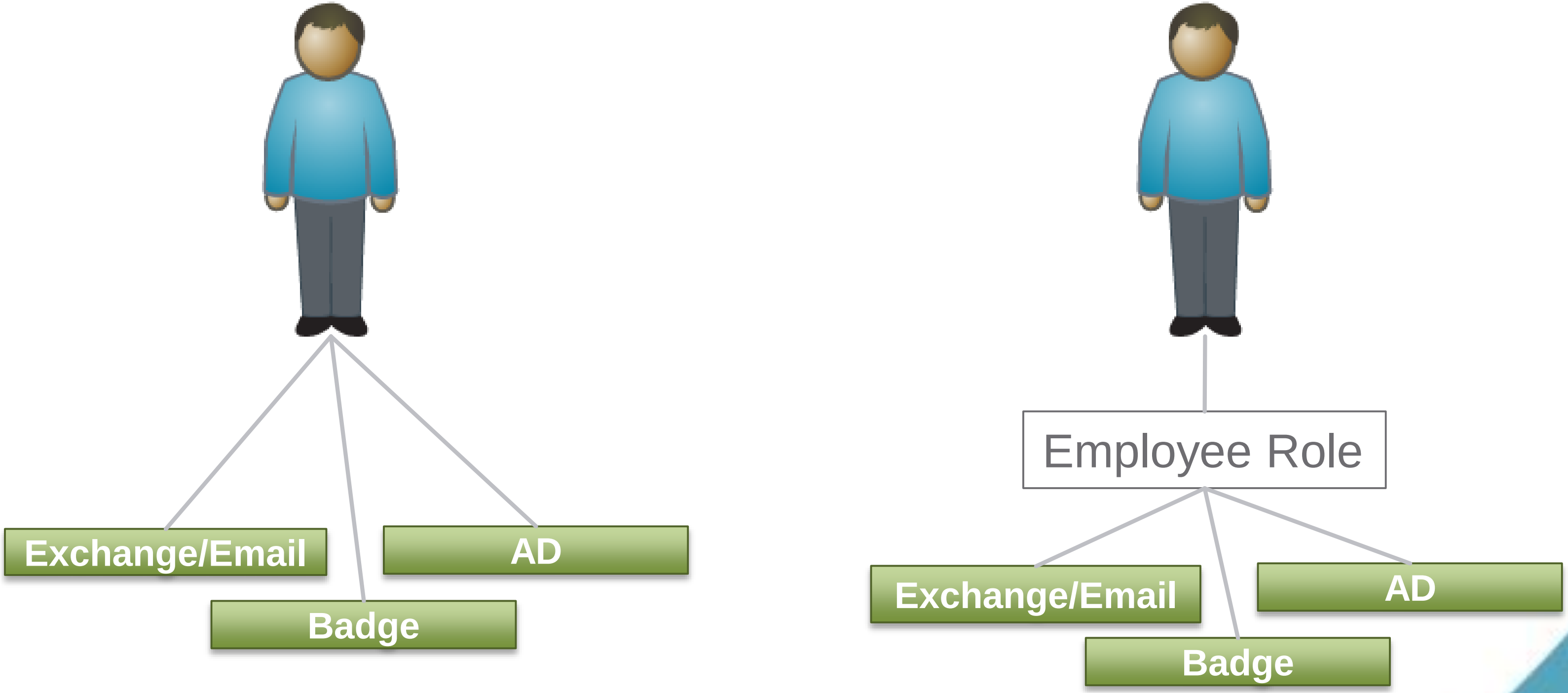
Roles

- Why Roles?
- IdentityIQ Support for Roles
- Acquiring a Role
- Defining Roles
- Extending the Role Model
- Roles versus Logical Applications
- Role Project Pointers

Role

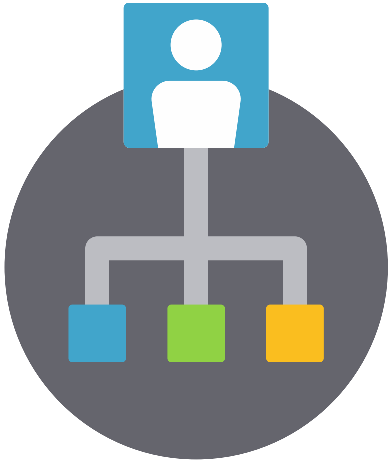
Definition

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



Why Roles?

- Efficiency
  - Encapsulate sets of entitlements
  - Simplify access review process
  - Ease access request process
  - Manage access by expertise
- Control
  - Manage entitlement assignment lifecycle
  - Shared audit process across collection of entitlements
  - Apply shared security model to entitlement collections



A Pragmatic Approach to Roles

Enterprise	Use Case	Targeted
Business roles based on organizational hierarchies Model-based IT roles RBAC strategy	Project scoped Project aligned RBAC not a goal	Bundles of access, groups of identities Focus on targeted groups / areas RBAC not the goal, at least initially

IdentityIQ Support for Roles

IdentityIQ Roles

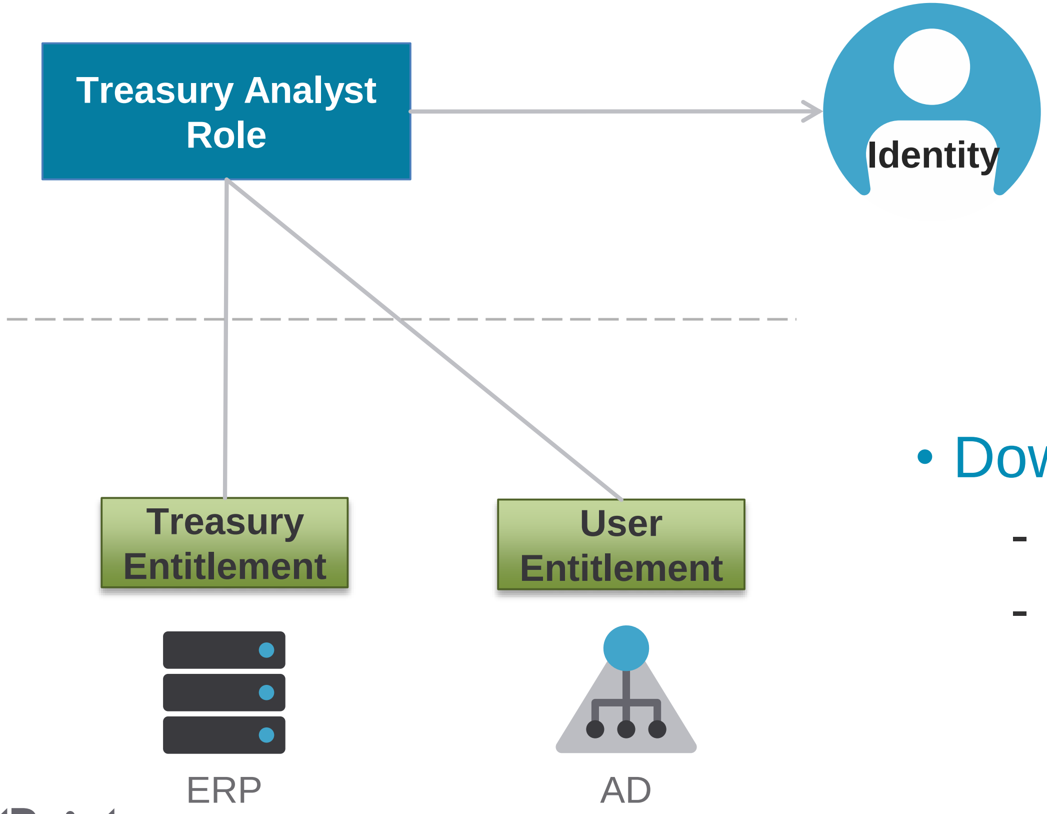
- Support
  - Discovery
  - Auto-assignment (based on rule/logic)
  - Self-service provisioning (through LCM)
  - Meaningful display names and descriptions
  - Extended attributes
  - Role mining
  - Role analytics and statistics
  - Role versioning

- Part of the identity governance framework
  - Access certification
  - Policy enforcement
  - Risk management

Single Tier Role Management Model

Common Role Model

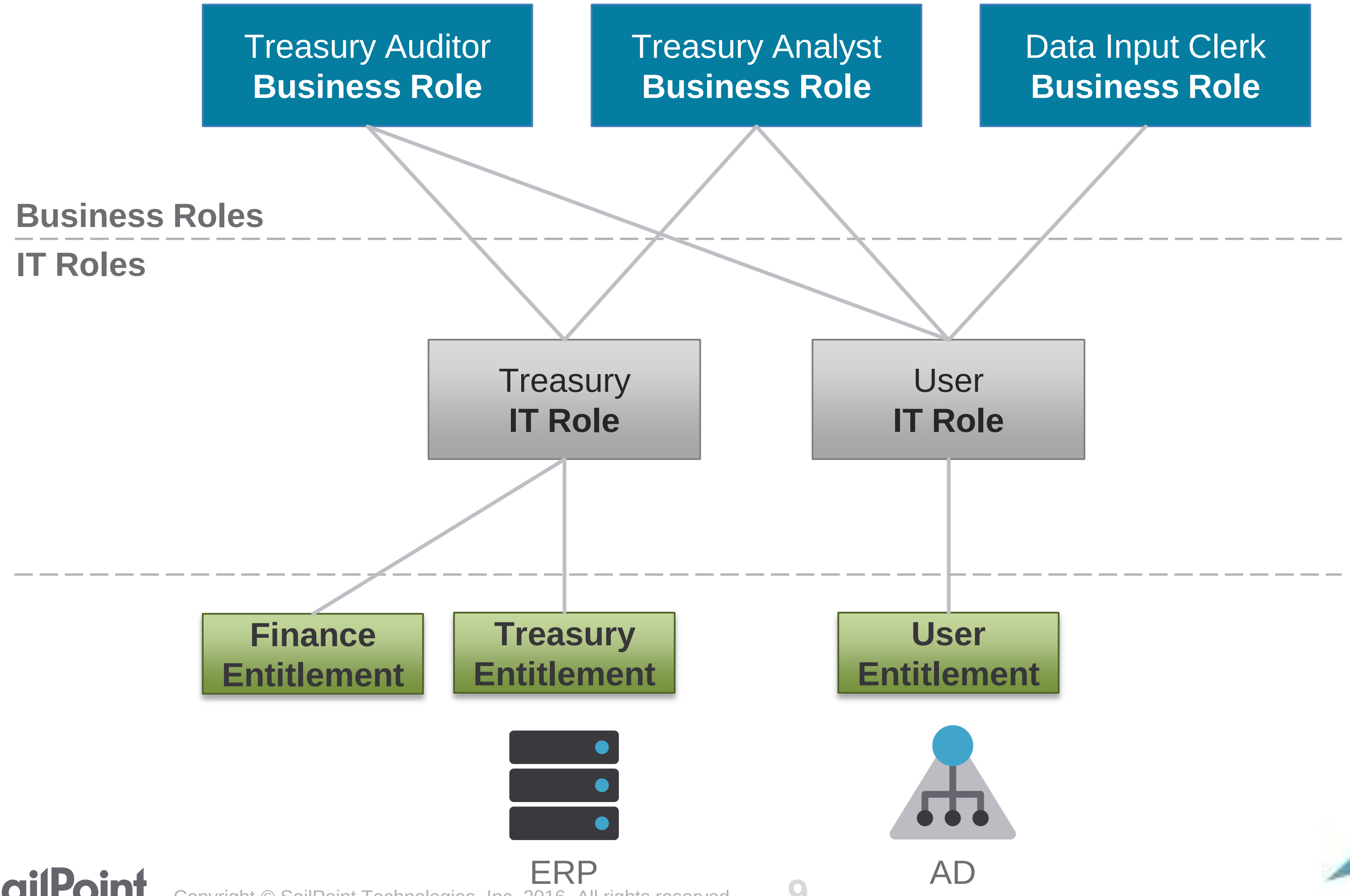
- Combine common groups of entitlements
- Simplify access requests and certifications
- Provide business context



- Downside
  - Potential for duplication
  - Potential for role explosion

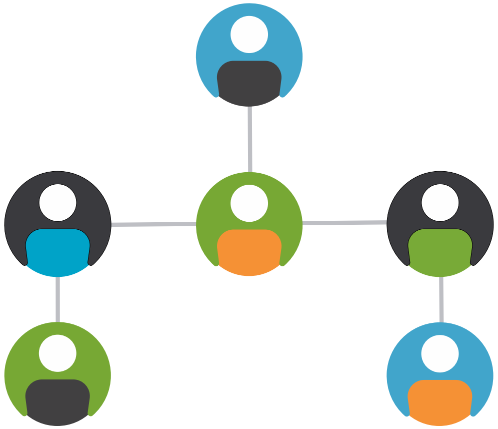
Two Tier Role Management Model

IdentityIQ Default



Two Tier Model

Business Roles

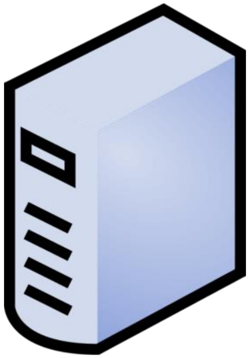


- Represent job functions, titles or responsibilities
- Needs determined by organizational structure or through business analysis
- Include metadata to increase understanding
- Represent the desired state for a user’s access
- Assigned to/requested by users

Two Tier Model

IT Roles

- Model the IT privileges required to perform a specific function within an application or other target system
- Represent the actual state of a user's access
  - Accounts
  - Entitlements
  - Permissions
- Can be used to provision access

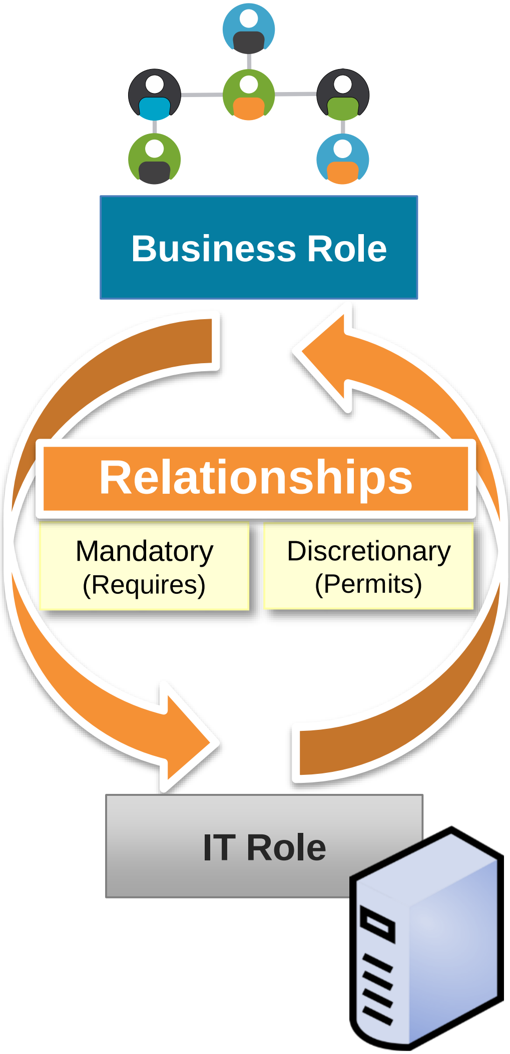


Relating Business and IT Roles

Requires and Permits

Mandatory Relationship: user MUST have

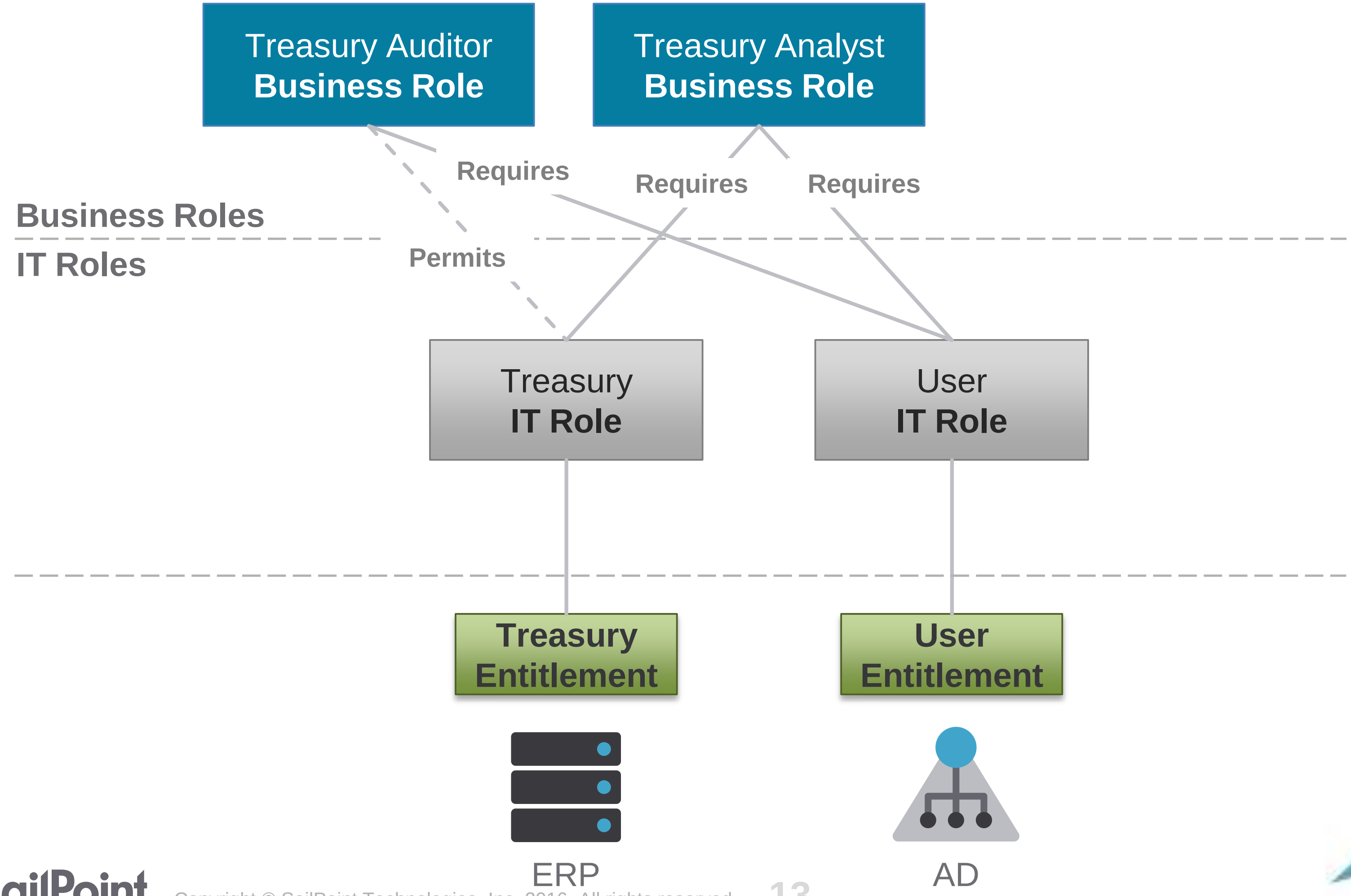
Discretionary relationship: user is ALLOWED to have



Requires/Permits relationship can reduce number of roles and help combat role explosion

Required and Permitted

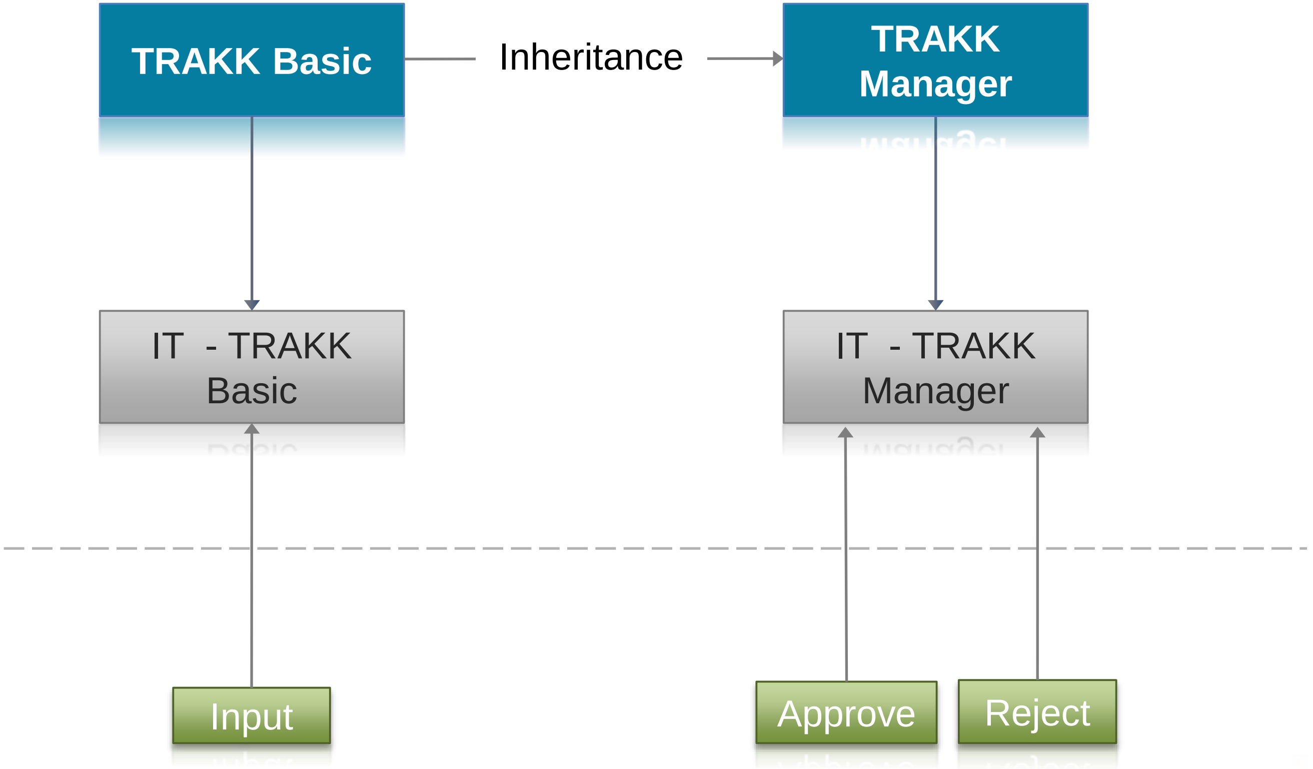
Example



Role Relationships

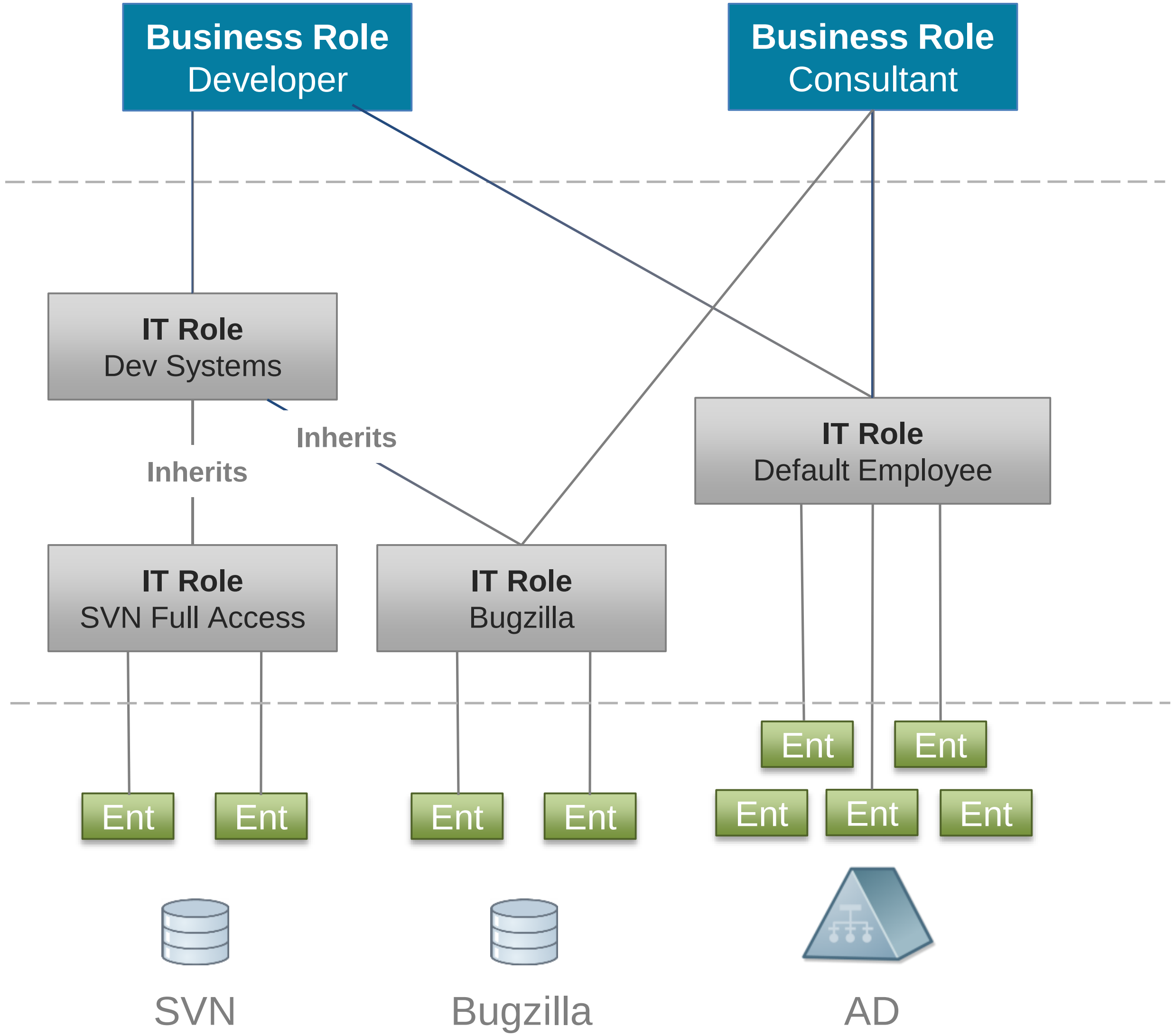
Business Role Inheritance

- Manager Role entitlements are additive
  - Input, Approve, & Reject
- Simpler model



Role Relationships

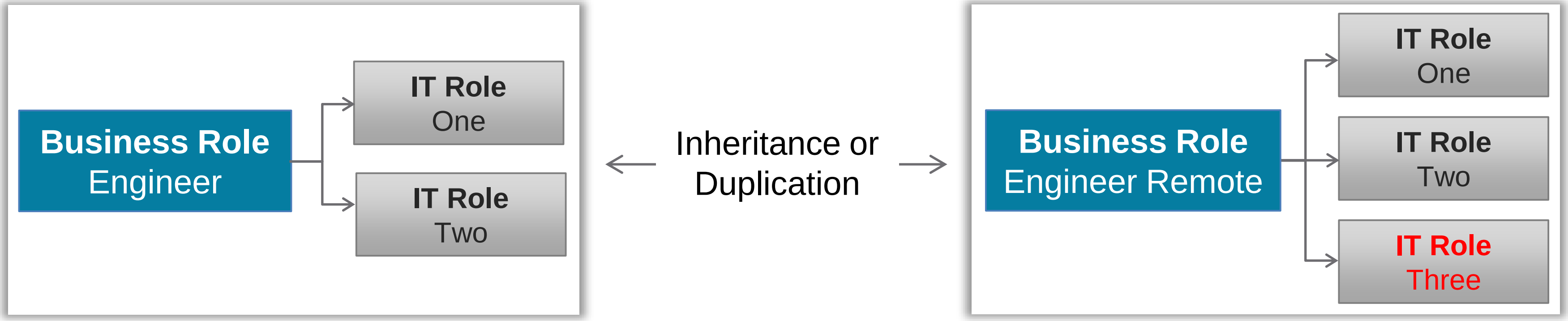
IT Role Inheritance



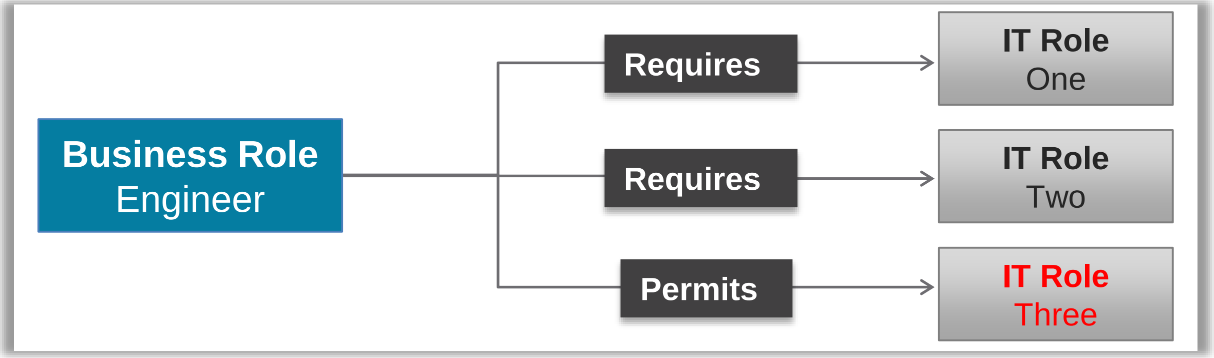
Role Relationships – Requires/Permits

Least Privilege Without Role Explosion

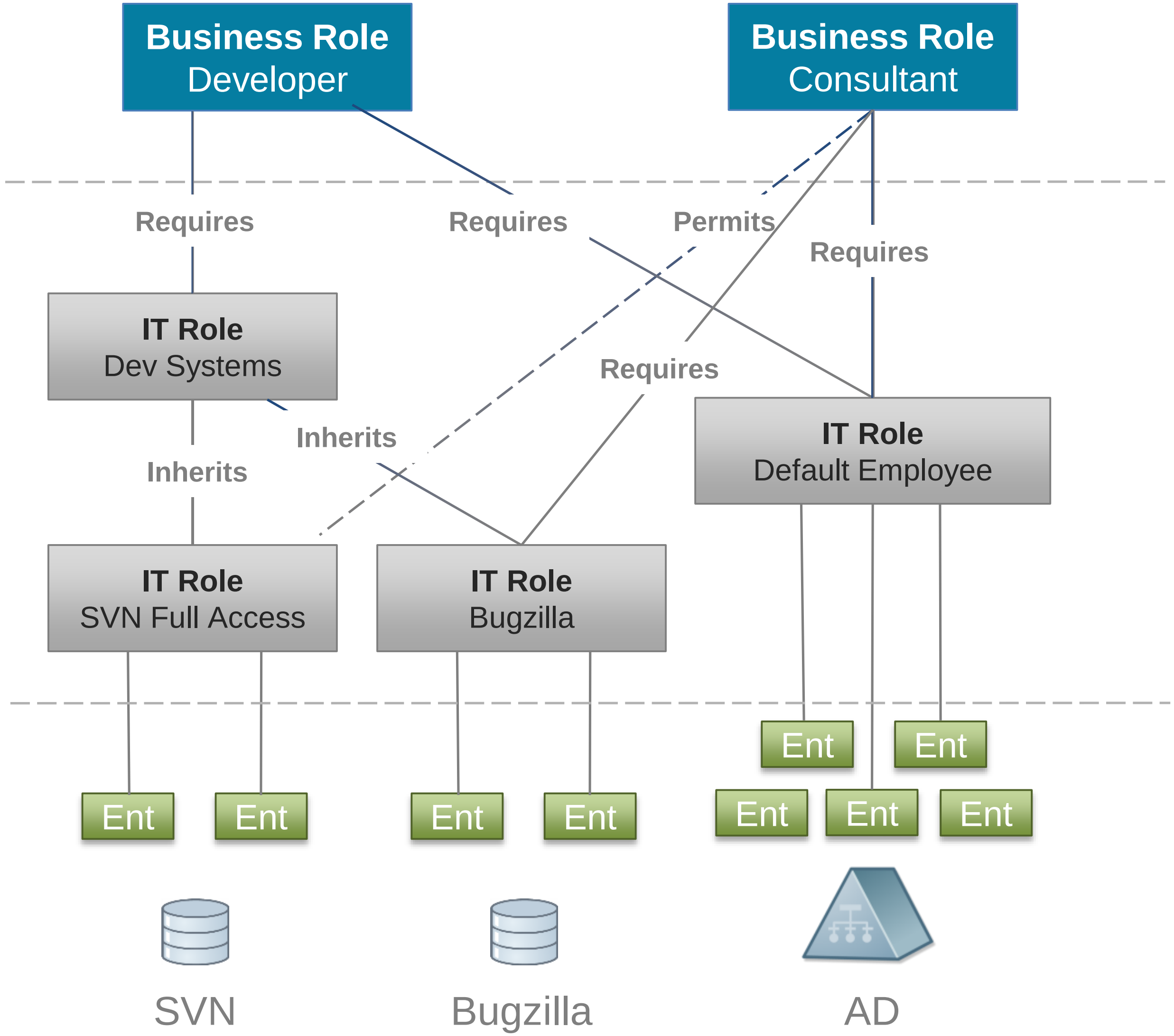
- Functional decomposition can mean more roles…



- Role association relationships minimize role explosion



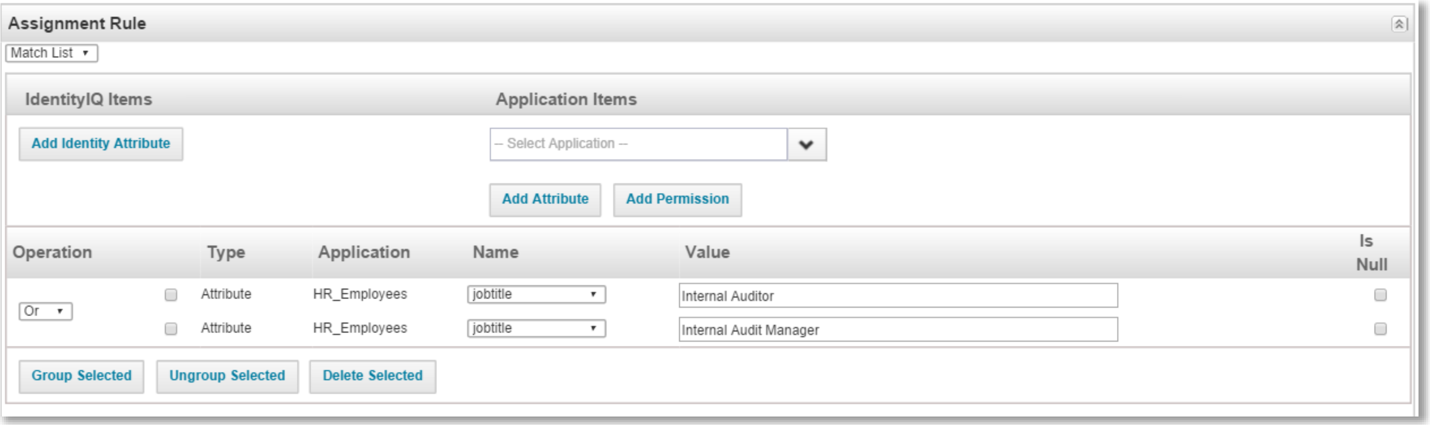
Role Relationships – Requires / Permits



Acquiring a Role

Obtaining Business Roles

- Manually
  - Gear → Lifecycle Manager
  - Identities → Identity Warehouse → Entitlement page (must be enabled)
  - Prompts for permitted entitlements
- Automatically using assignment rules
  - Permitted entitlements must be requested separately



Operation		Type	Application	Name	Value	Is Null
Or	□	Attribute	HR_Employees	jobtitle	Internal Auditor	□
	□	Attribute	HR_Employees	jobtitle	Internal Audit Manager	□

Options

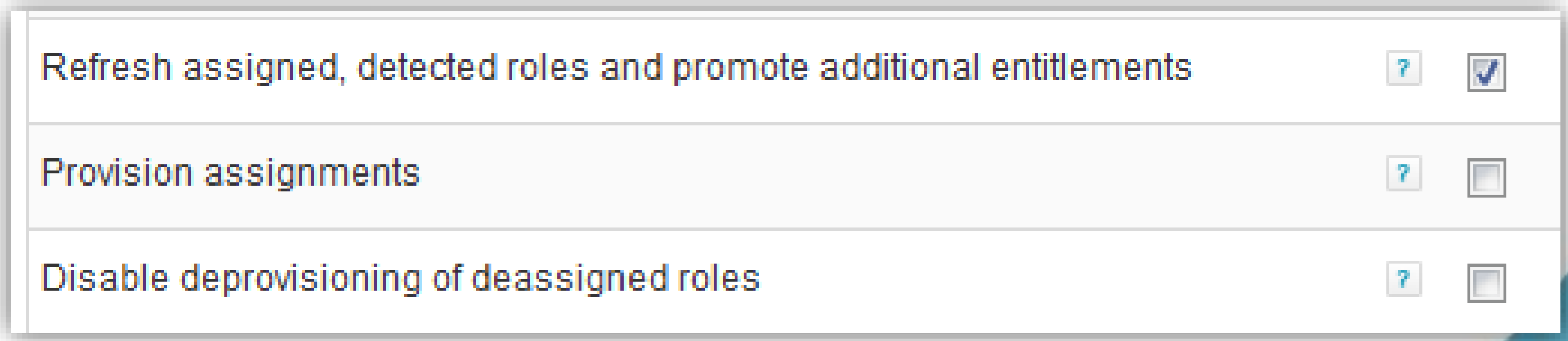
- Match Lists
- Filters
- Populations
- Scripts/rules (code snippets)

Obtaining IT Roles

- Detected from environment on Identity Refresh
  - ‘Refresh Assigned and Detected Roles’ option selected
  - Detection is defined through an Entitlement Profile
- Result of indirect request
  - LCM Access Request for a business role
  - Business role assignment rule
  - During an Access Review (provisioning missing roles)
  - **Exception**: can request *permitted* roles directly

Assigning and Detecting Roles

- Monitor → Tasks
- Run “Identity Refresh” Task
  - “Refresh assigned, detected roles…” selected
  - Detection is defined through an IT Role Profile
- Optionally choose
  - “Provision assignments”
  - “Disable deprovisioning…”



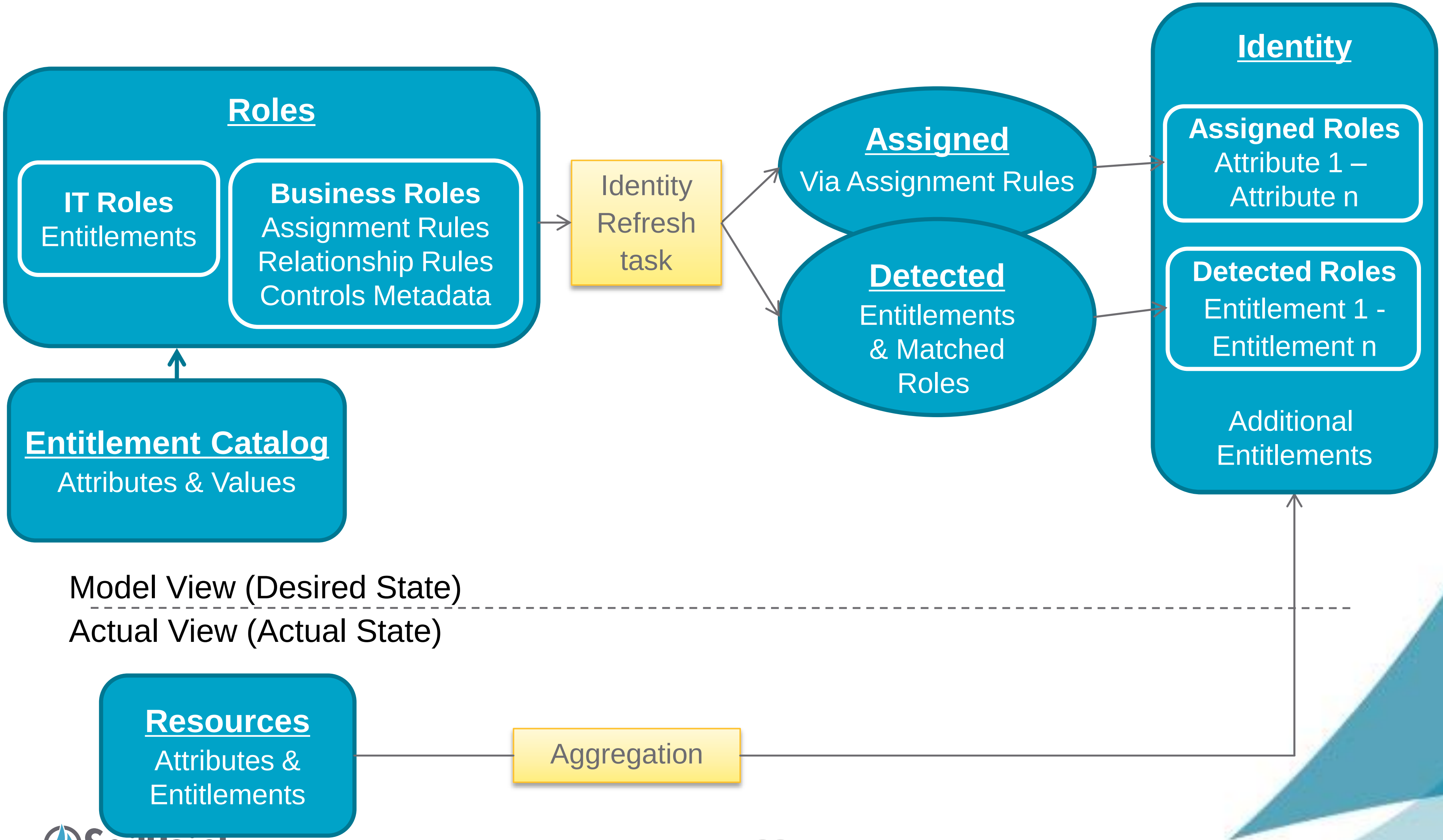
Refresh assigned, detected roles and promote additional entitlements ? ☑

Provision assignments ? □

Disable deprovisioning of deassigned roles ? □

Assigned vs Detected Roles

Automatic Assignment



Roles

IT Roles
Entitlements

Business Roles
Assignment Rules
Relationship Rules
Controls Metadata

Identity Refresh task

Assigned
Via Assignment Rules

Detected
Entitlements & Matched Roles

Identity

Assigned Roles
Attribute 1 – Attribute n

Detected Roles
Entitlement 1 - Entitlement n

Additional Entitlements

Entitlement Catalog
Attributes & Values

Model View (Desired State)

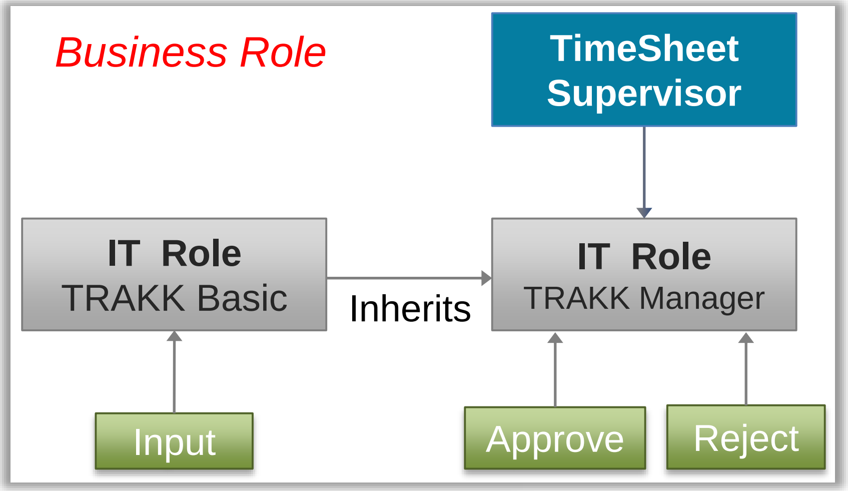
Actual View (Actual State)

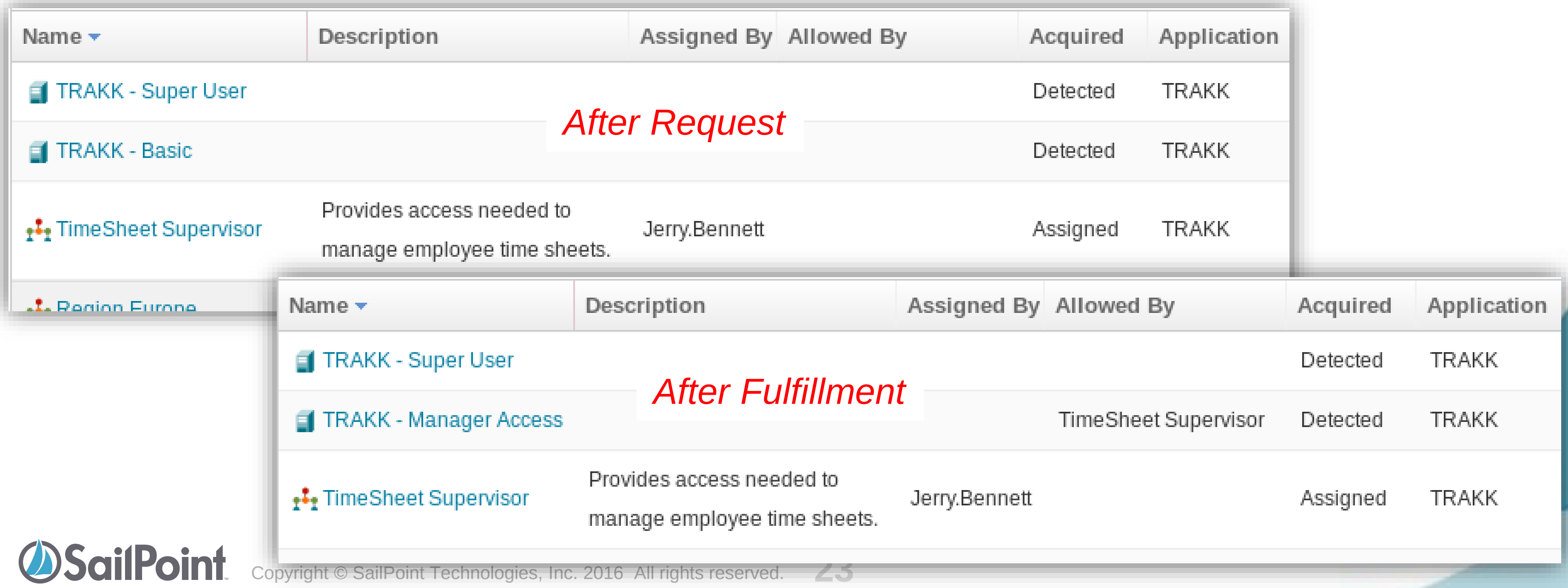
Resources
Attributes & Entitlements

Aggregation

Assigned vs Detected Roles

Manual Assignment





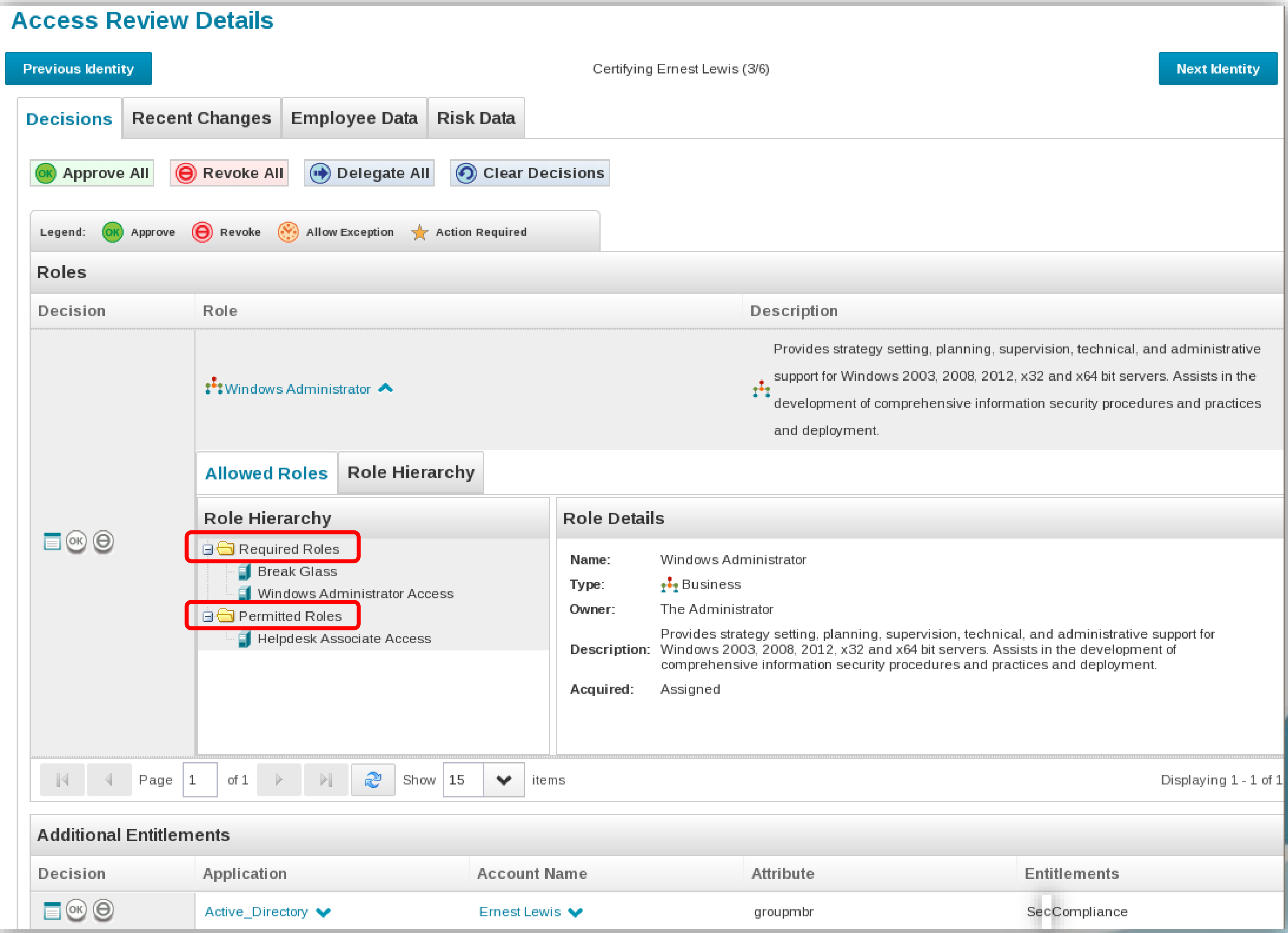
After Request

Name	Description	Assigned By	Allowed By	Acquired	Application
TRAKK - Super User				Detected	TRAKK
TRAKK - Basic				Detected	TRAKK
TimeSheet Supervisor	Provides access needed to manage employee time sheets.	Jerry.Bennett		Assigned	TRAKK
Region Europe					

After Fulfillment

Name	Description	Assigned By	Allowed By	Acquired	Application
TRAKK - Super User				Detected	TRAKK
TRAKK - Manager Access			TimeSheet Supervisor	Detected	TRAKK
TimeSheet Supervisor	Provides access needed to manage employee time sheets.	Jerry.Bennett		Assigned	TRAKK

Certification – Assigned vs Detected Roles



Access Review Details

Certifying Ernest Lewis (3/6)

Legend: OK Approve ⊖ Revoke Allow Exception ★ Action Required

Roles

Decision	Role	Description
OK ⊖	Windows Administrator	Provides strategy setting, planning, supervision, technical, and administrative support for Windows 2003, 2008, 2012, x32 and x64 bit servers. Assists in the development of comprehensive information security procedures and practices and deployment.

Role Hierarchy

- Required Roles
  - Break Glass
  - Windows Administrator Access
- Permitted Roles
  - Helpdesk Associate Access

Role Details

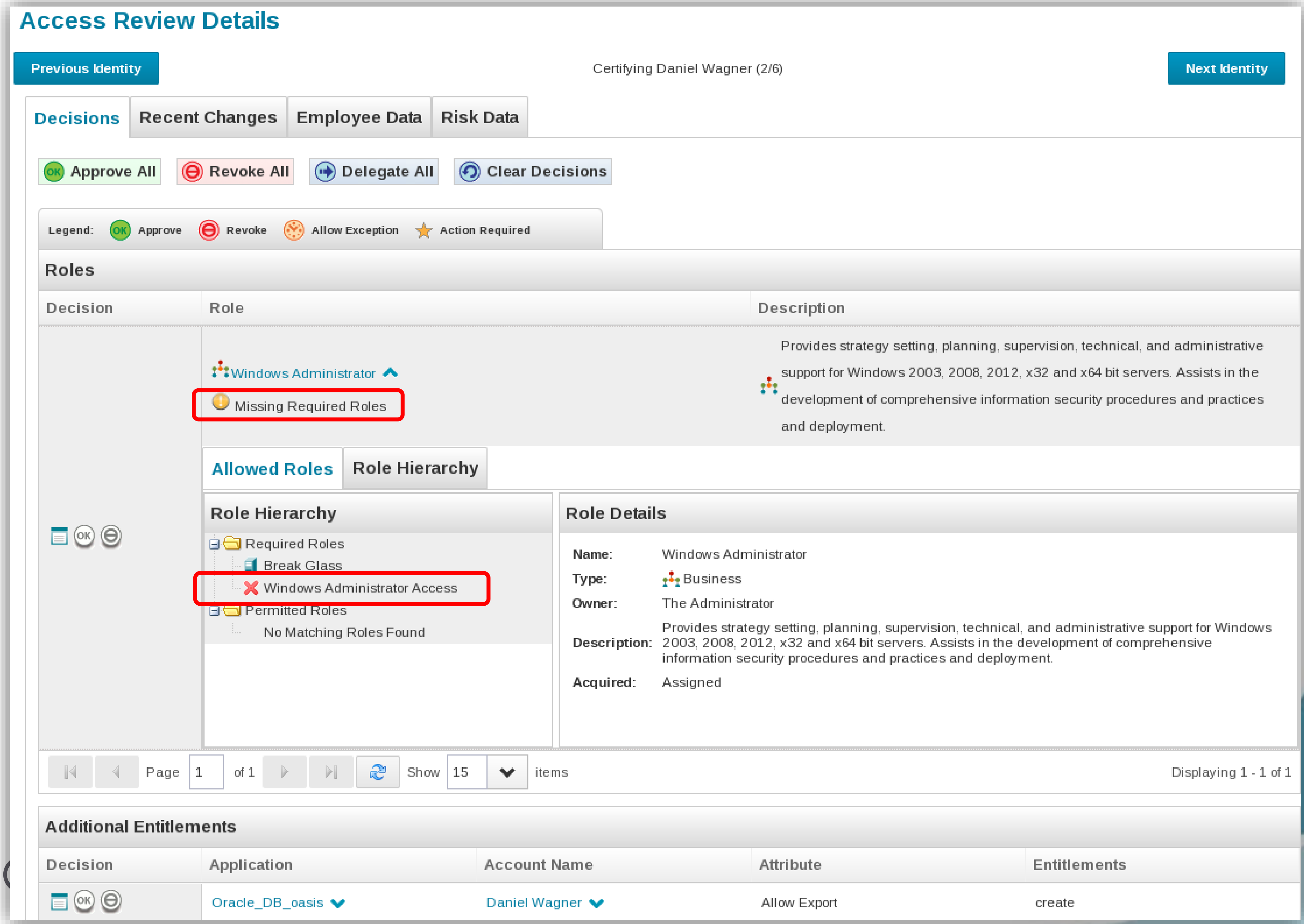
Name:	Windows Administrator
Type:	Business
Owner:	The Administrator
Description:	Provides strategy setting, planning, supervision, technical, and administrative support for Windows 2003, 2008, 2012, x32 and x64 bit servers. Assists in the development of comprehensive information security procedures and practices and deployment.
Acquired:	Assigned

Page 1 of 1 Show 15 items Displaying 1 - 1 of 1

Additional Entitlements

Decision	Application	Account Name	Attribute	Entitlements
OK ⊖	Active_Directory	Ernest Lewis	groupmbr	SecCompliance

Certification – Assigned vs Detected Roles



Access Review Details

Previous Identity | Certifying Daniel Wagner (2/6) | Next Identity

Decisions | Recent Changes | Employee Data | Risk Data

Approve All | Revoke All | Delegate All | Clear Decisions

Legend: Approve | Revoke | Allow Exception | Action Required

Roles

Decision	Role	Description
	Windows Administrator Missing Required Roles	Provides strategy setting, planning, supervision, technical, and administrative support for Windows 2003, 2008, 2012, x32 and x64 bit servers. Assists in the development of comprehensive information security procedures and practices and deployment.

Allowed Roles | Role Hierarchy

Role Hierarchy

- Required Roles
  - Break Glass
  - Windows Administrator Access
- Permitted Roles
  - No Matching Roles Found

Role Details

Name:	Windows Administrator
Type:	Business
Owner:	The Administrator
Description:	Provides strategy setting, planning, supervision, technical, and administrative support for Windows 2003, 2008, 2012, x32 and x64 bit servers. Assists in the development of comprehensive information security procedures and practices and deployment.
Acquired:	Assigned

Page 1 of 1 | Show 15 items | Displaying 1 - 1 of 1

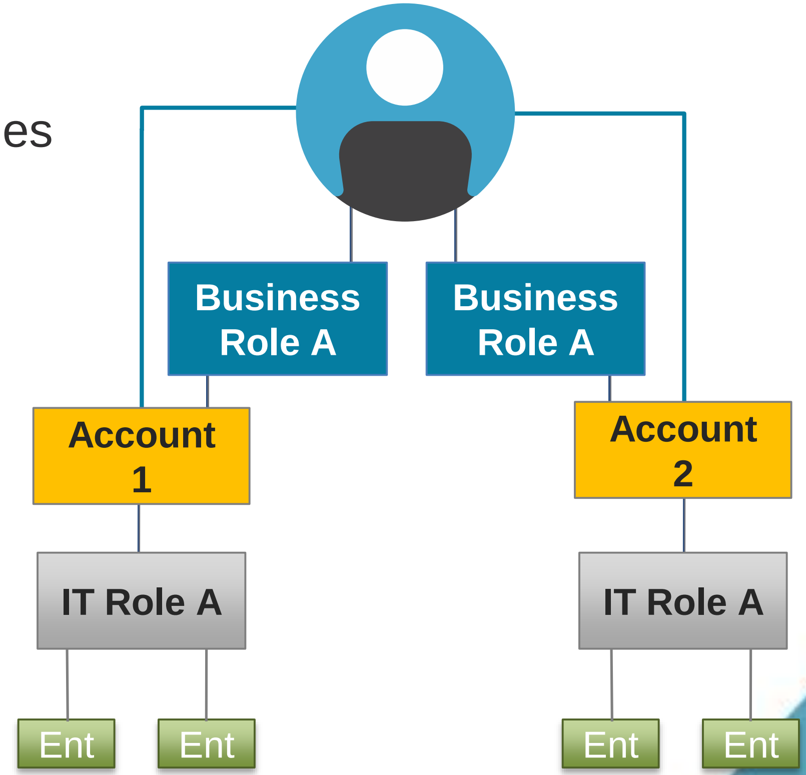
Additional Entitlements

Decision	Application	Account Name	Attribute	Entitlements
	Oracle_DB_oasis	Daniel Wagner	Allow Export	create

Role Multi-Account Support

Acquiring Roles at the Account Level

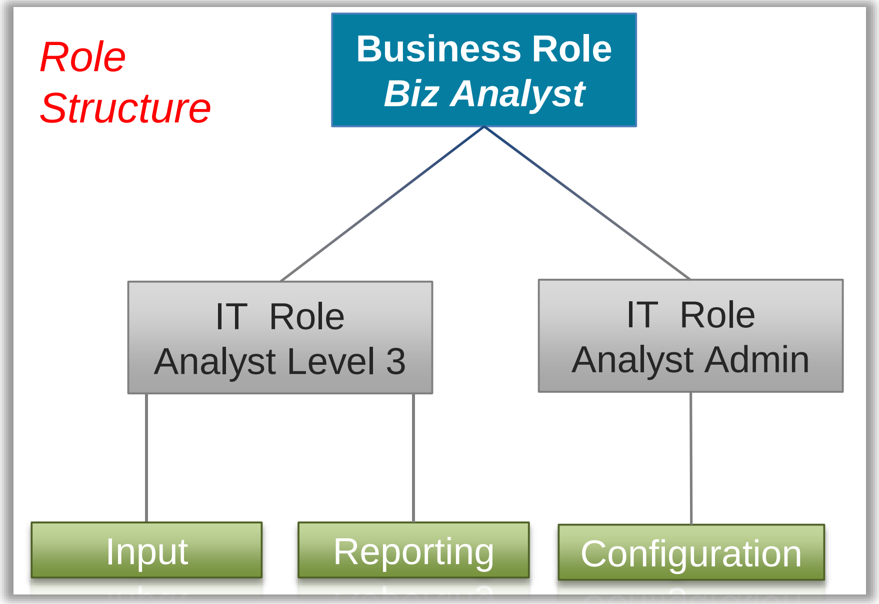
- Situation: Identities with multiple accounts on an application
- Assign same business role to multiple accounts on same identity
  - Account selected
    - Automatically based on rules
    - Manually through LCM
    - Through work items

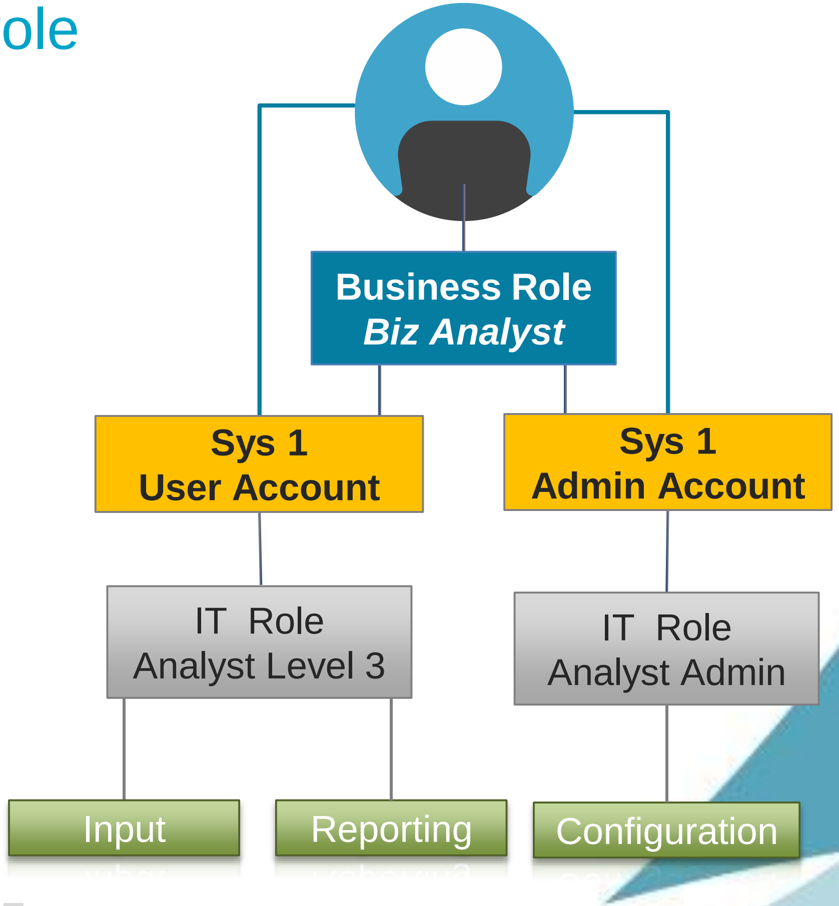


Role Multi-Account Support

Acquiring Roles at the Account Level (continued)

- Situation: Identities with multiple accounts on an application
- Target IT Roles to different accounts then their associated business role
  - Account selected
    - Manually through LCM

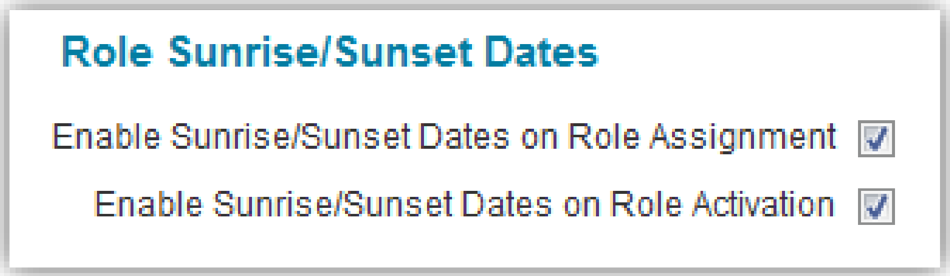




Future Role Acquisition

Sunrise/Sunset of Roles

- Global Configuration
    - Assignment configuration applies to both roles and entitlements
    - Default is enabled

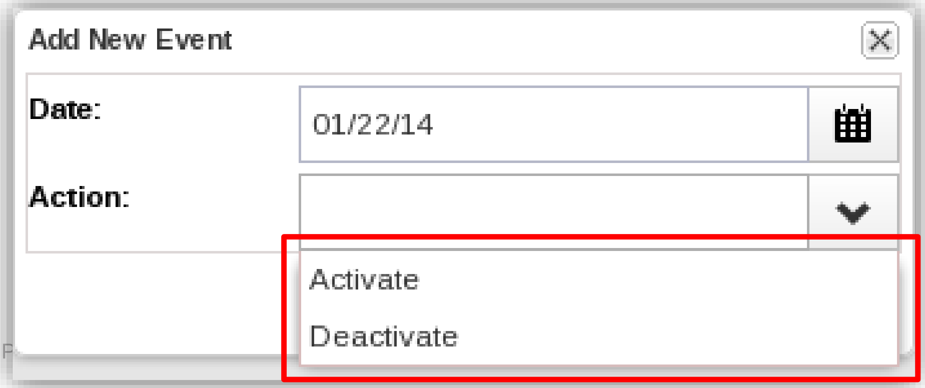


Role Sunrise/Sunset Dates

Enable Sunrise/Sunset Dates on Role Assignment ☑

Enable Sunrise/Sunset Dates on Role Activation ☑

- Role Activation – Sunrise/Sunset Dates for Roles
    - Define → Roles → Edit → Scheduled Events → Add Event
    - Used for roles that have limited time usage or delayed activation



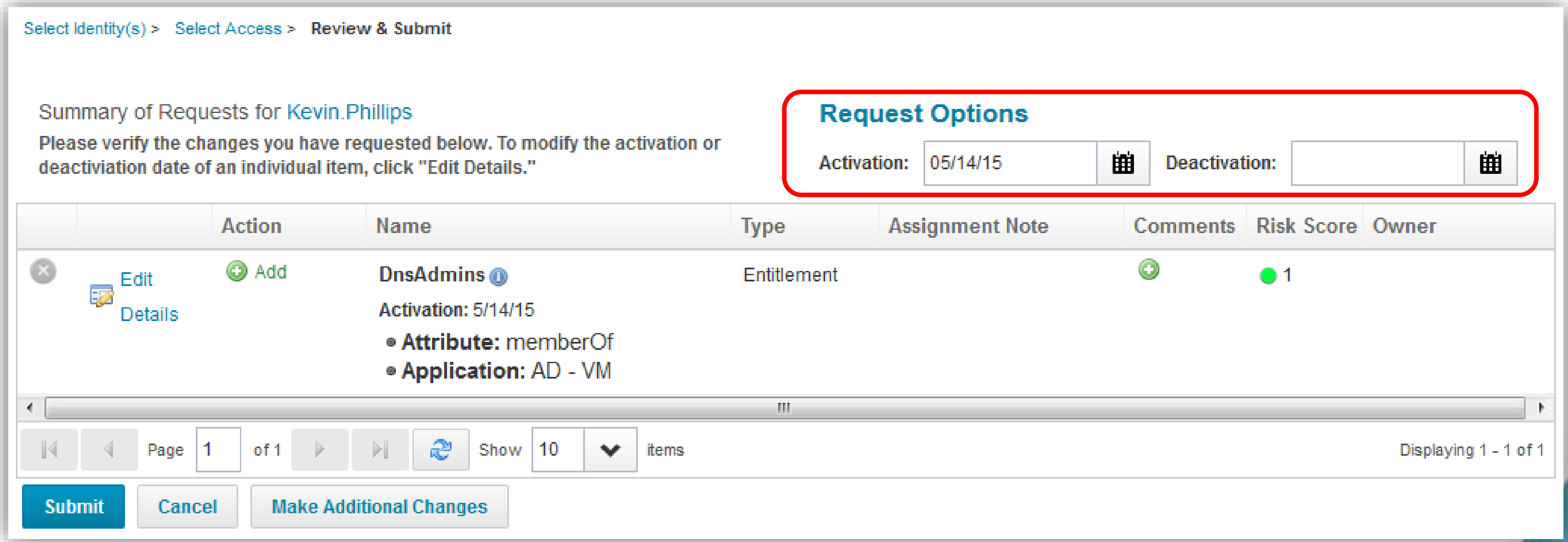
Add New Event

Date: 01/22/14

Action:

Future Role Acquisition

Sunrise/Sunset of Roles



Select Identity(s) > Select Access > **Review & Submit**

Summary of Requests for Kevin.Phillips

Please verify the changes you have requested below. To modify the activation or deactiviation date of an individual item, click "Edit Details."

Request Options

Activation: 05/14/15 Deactivation:

		Action	Name	Type	Assignment Note	Comments	Risk Score	Owner
✕	Edit Details	Add	**DnsAdmins** Activation: 5/14/15 ● **Attribute:** memberOf ● **Application:** AD - VM	Entitlement		⊕	● 1	

Page 1 of 1 Show 10 items Displaying 1 - 1 of 1

Acquiring Role Updates

Propagate Role Changes

- Enforce additions to a role
  - Identity Refresh Task
    - Provision Role Assignments option
  - Propagate Role Changes Task
- Enforce removals from a role
  - Propagate Role Changes Task

- Configuring Propagate Role Changes
  - Enable role change capture
  - Create Propagate Role Changes task
  - Schedule task

Defining Roles

Analyzing and Building Roles

Tools

Entitlement Analysis

IT Role Mining

Business Role Mining

Creating Roles from Certifications

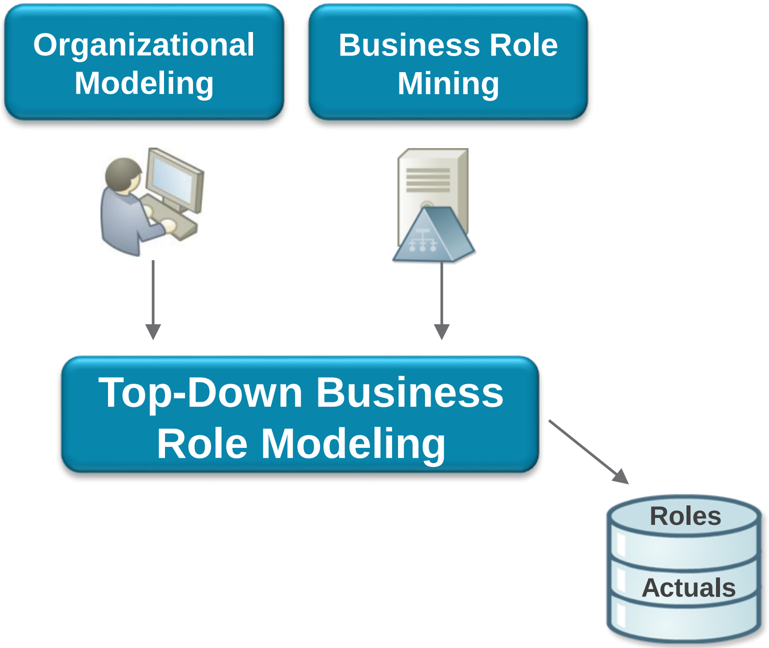
Export to CSV

Pencil and Paper (or Excel)

SailPoint

Role Definition and Mining

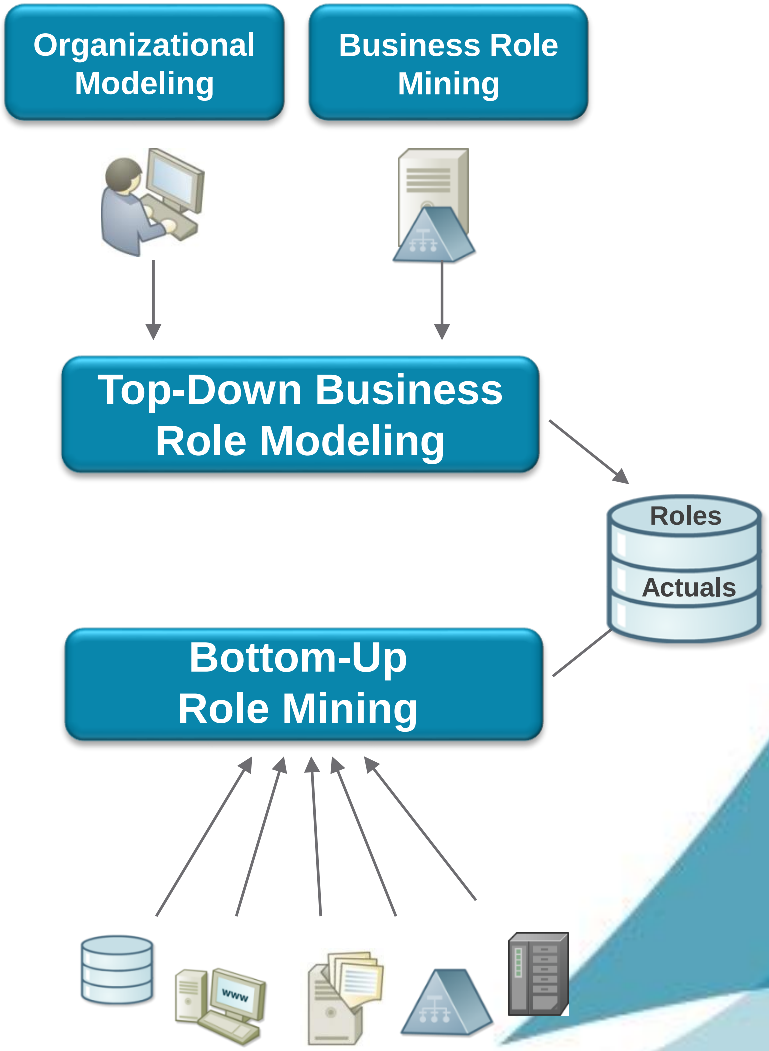
- Top-Down Business Role Modeling
  - Capture via business analysis and organizational modeling
  - Leverage
    - Automated analysis of identity data
    - Role membership certification



Role Definition and Mining

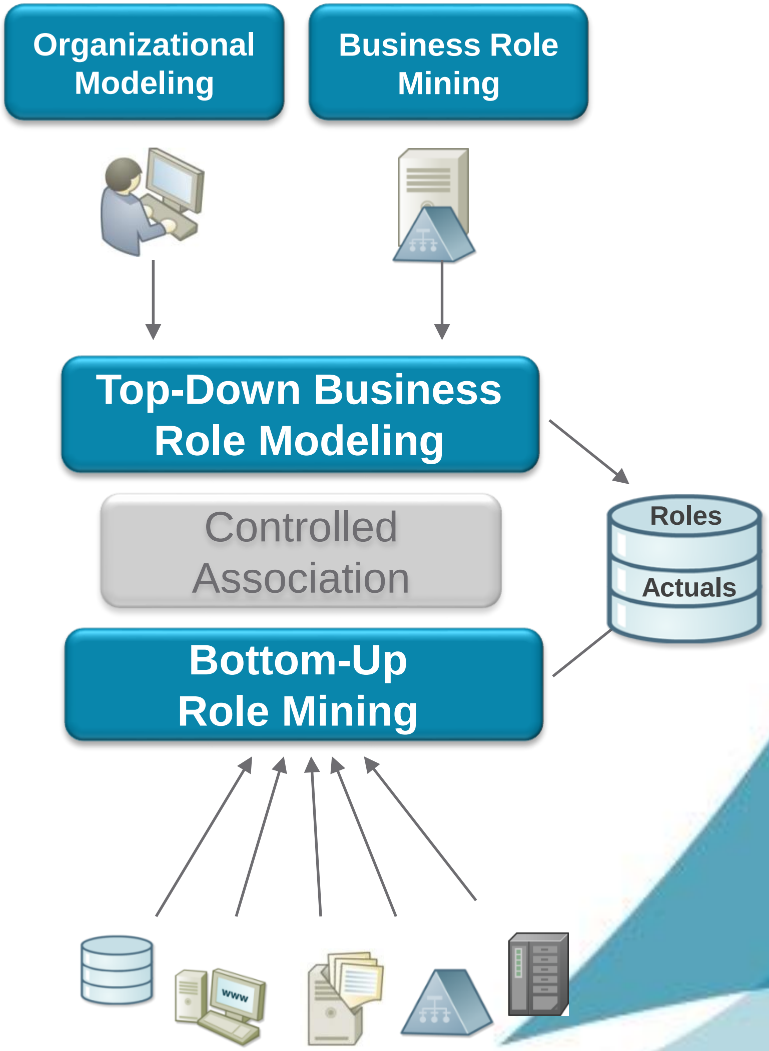
- Top-Down Business Role Modeling
  - Capture via business analysis and organizational modeling
  - Leverage
    - Automated analysis of identity data
    - Role membership certification

- Bottom-Up IT Role Mining
  - Driven by algorithmic analysis and analytics-focused mining processes
  - Leverage
    - Actual data from the central repository
    - Role composition certification and analysis and “review” of those actuals



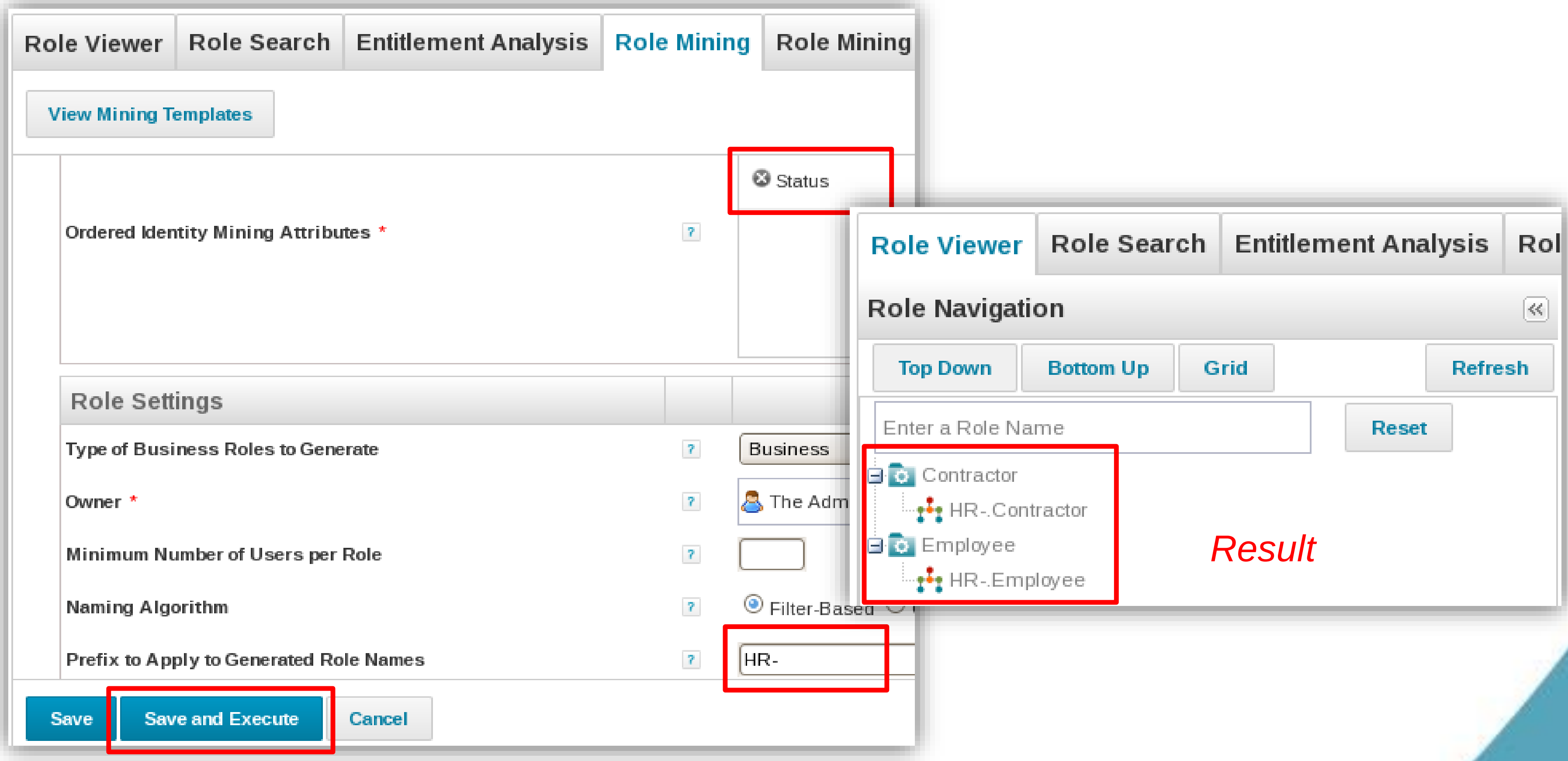
Role Definition and Mining

- Top-Down Business Role Modeling
  - Capture via business analysis and organizational modeling
  - Leverage
    - Automated analysis of identity data
    - Role membership certification
- Bottom-Up IT Role Mining
  - Driven by algorithmic analysis and analytics-focused mining processes
  - Leverage
    - Actual data from the central repository
    - Role composition certification and analysis and "review" of those actuals
- Controlled Association
  - Join business & IT roles using *required* and *permitted*



Tools

Business Role Mining



Ordered Identity Mining Attributes * ? — ⊗ Status

Role Settings

Type of Business Roles to Generate ? — Business

Owner * ? — The Adm

Minimum Number of Users per Role ?

Naming Algorithm ? — ● Filter-Based

Prefix to Apply to Generated Role Names ? — HR-

Role Navigation

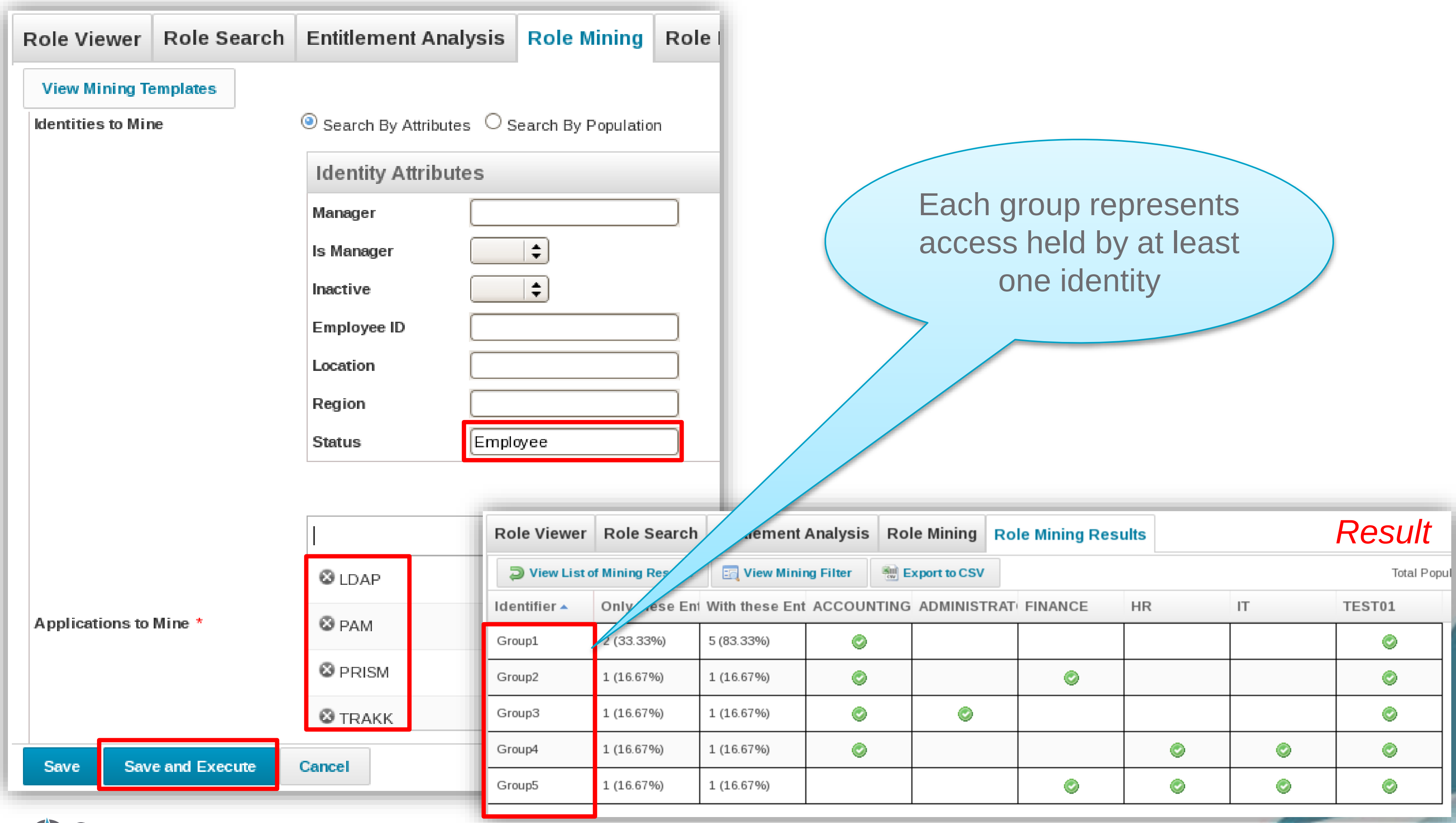
Enter a Role Name

⊟ Contractor
- HR-.Contractor

⊟ Employee
- HR-.Employee

Tools

IT Role Mining



Identities to Mine

● Search By Attributes ○ Search By Population

Identity Attributes

Manager	
Is Manager	
Inactive	
Employee ID	
Location	
Region	
Status	Employee

Applications to Mine *

- LDAP
- PAM
- PRISM
- TRAKK

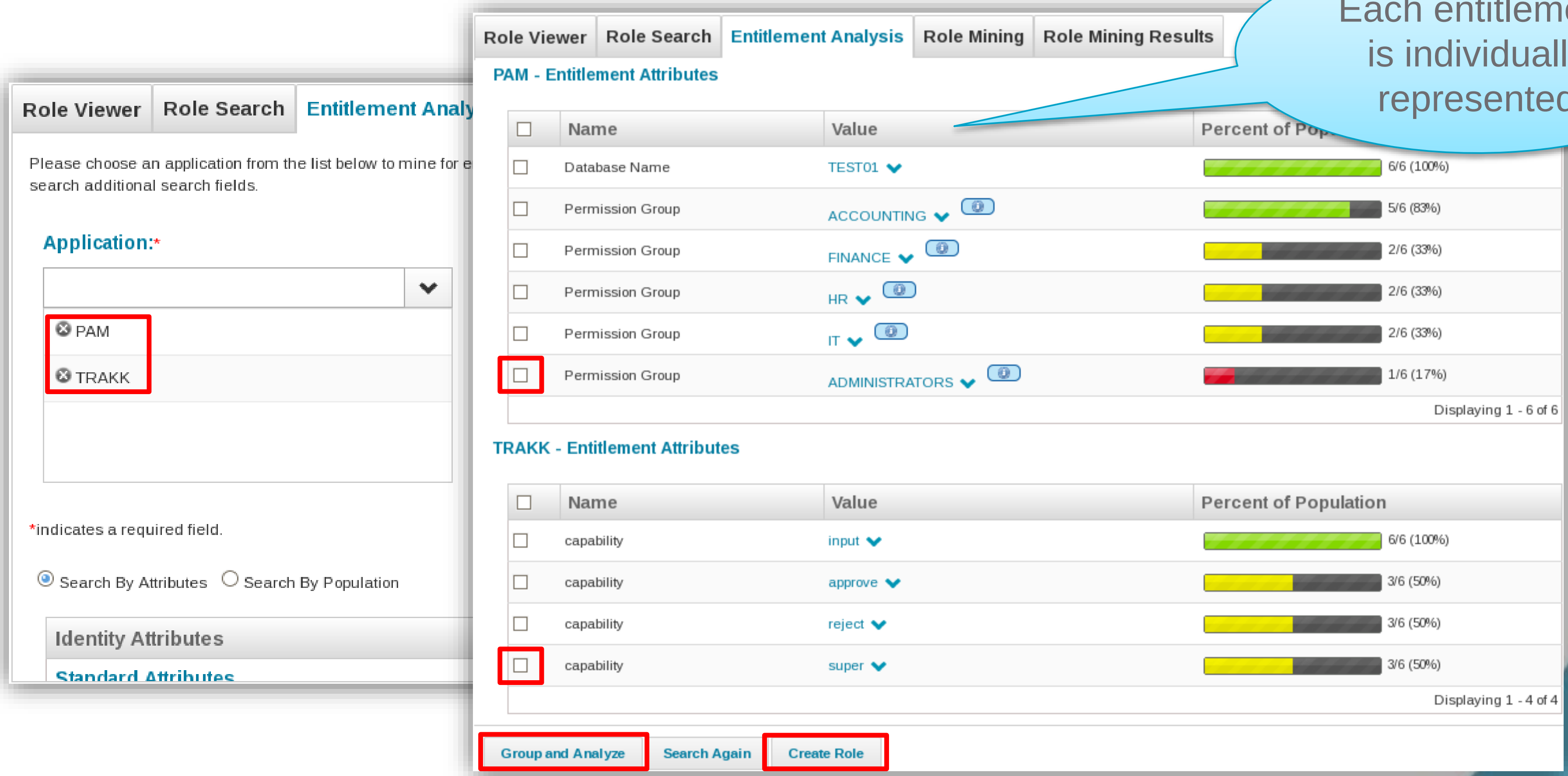
Each group represents access held by at least one identity

Result

Identifier	Only ese Ent	With these Ent	ACCOUNTING	ADMINISTRAT	FINANCE	HR	IT	TEST01
Group1	2 (33.33%)	5 (83.33%)	✓					✓
Group2	1 (16.67%)	1 (16.67%)	✓		✓			✓
Group3	1 (16.67%)	1 (16.67%)	✓	✓				✓
Group4	1 (16.67%)	1 (16.67%)	✓			✓	✓	✓
Group5	1 (16.67%)	1 (16.67%)			✓	✓	✓	✓

Tools

IT Role Entitlement Analysis



Role Viewer | Role Search | Entitlement Analy

Please choose an application from the list below to mine for e search additional search fields.

Application:*

⊗ PAM

⊗ TRAKK

*indicates a required field.

● Search By Attributes ○ Search By Population

Identity Attributes

Standard Attributes

Role Viewer | Role Search | Entitlement Analysis | Role Mining | Role Mining Results

PAM - Entitlement Attributes

□	Name	Value	Percent of Pop
□	Database Name	TEST01	6/6 (100%)
□	Permission Group	ACCOUNTING	5/6 (83%)
□	Permission Group	FINANCE	2/6 (33%)
□	Permission Group	HR	2/6 (33%)
□	Permission Group	IT	2/6 (33%)
□	Permission Group	ADMINISTRATORS	1/6 (17%)

Displaying 1 - 6 of 6

TRAKK - Entitlement Attributes

□	Name	Value	Percent of Population
□	capability	input	6/6 (100%)
□	capability	approve	3/6 (50%)
□	capability	reject	3/6 (50%)
□	capability	super	3/6 (50%)

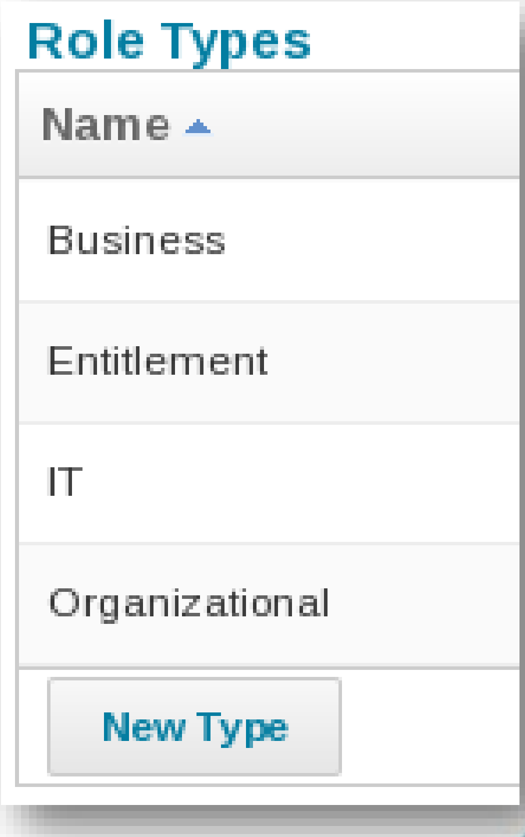
Displaying 1 - 4 of 4

Each entitlement is individually represented

Extending the Role Model

Standard Role Types

- Business Roles
  - Assignable
  - Requestable
- IT Roles
  - Detection
  - Provisioning
- Organizational Roles
  - Containment
- Entitlement (Legacy)
  - Backwards compatibility (pre-6.0)



Role Types

Name ▲
Business
Entitlement
IT
Organizational

Standard Role Types

Behavior

Type	Business	IT	Organizational
Allow Inheritance of other roles	Yes	Yes	Yes
Allow other roles inheriting this role	Yes	Yes	Yes
Auto Detection with Profiles	No	Yes	No
Entitlement Profiles	No	Yes	No
Automatic Assignment with Rule	Yes	No	No
Assignment Rule	Yes	No	No
Manual Assignment	Yes	No	No
Permitted Roles List	Yes	No	No
Allow being on permitted roles list	No	Yes	No
Required Roles list	Yes	No	No
Allow being on a Required Roles list	No	Yes	No
Allow granting of IdentityIQ rights	No	No	No

Extensible Role Model

Extension Examples

- Single tier role model
- Hybrid role model
    - Request IT roles
    - Request business roles
- New Icons
- Create new types
    - Roles for IdentityIQ Capabilities
    - Dedicated birthright provisioning roles
        - Non requestable
        - Non assignable

(System Setup → Role Configuration)

Extensible Role Model

Custom Role Types (Examples)

Type	Business	IT	Birthright	IdentityIQ Cap
Allow Inheritance of other roles	Yes	Yes	Yes	Yes
Allow other roles inheriting this role	Yes	Yes	Yes	Yes
Auto Detection with Profiles	No	Yes	No	No
Entitlement Profiles	No	Yes	No	No
Automatic Assignment with Rule	Yes	No	No	Yes
Assignment Rule	Yes	No	No	Yes
Manual Assignment	Yes	No	No	Yes
Permitted Roles List	Yes	No	No	No
Allow being on permitted roles list	No	Yes	No	No
Required Roles list	Yes	No	Yes	No
Allow being on a Required Roles list	No	Yes	No	No
Allow granting of IdentityIQ rights	No	No	No	Yes

SailPoint

Roles vs. Logical Applications

Roles or Logical Applications?

	Roles	Logical App
User perspective	Users think about access holistically	Users think about access in terms of an account
Governance	Supported	Supported
Provisioning	Leverages environment	• Manually through work items • Automated through custom rules
Scalability	100,000+	Less than 100

Role Project Pointers

Role Project Pointers

- General
  - Look for groupings of user types
  - Prevent role proliferation
  - Enforce least privilege
  - Define roles that are reusable
- High turnover or high use roles are a good way to start
  - Bank tellers, seasonal employees, employee vs. contractor
  - Don’t attempt to “boil the ocean”
- Know your scope
  - Simplify certifications? Access requests?
  - Involve SME’s who know the business

Role Project Pointers

- Build in Roles when the IdM Program is Mature
  - Because data is cleaner
- Every business approaches roles differently
- Roles are a program; not a project
  - Too big, too fast is how role projects fail
  - Roles have a lifecycle and should evolve
  - Start small and familiar
  - Can give key managers capability to create roles as needed; this still requires approvals
- Before inventing your own, consider the default IdentityIQ role model

Questions?

Exercise Preview

Section 3, Exercises 1, 2, 3

- Exercise 1: Defining a Role Model
- Exercise 2: Assign and Detect Business Roles
- Exercise 3: Using Roles to Provision Access to the PRISM Application