Application Onboarding Review

Define each item and specify how they are configured

- Aggregation
- Refresh
- Identity Cube
- Application
- Connector
- Group Factory
- Task
- Authoritative Application
- Schema
- Identity Attribute
- Correlation
- Entitlement Catalog
- Identity Cube – Entitlement
- Orphaned account
- Rule

Policies and Risk

Fundamentals of IdentityIQ Implementation

IdentityIQ 7.0

Overview

Policies and Risk

- Policies
  - IdentityIQ Policies Overview
  - Policy Types
  - Defining Policies
  - Discovering Policy Violations
  - Monitoring Policy Violations
- Risk
  - Identity Risk Model
  - Application Risk Model
  - Refreshing Risk Scores
  - Interaction with Risk Scores

Policy Administration

Policy Definition

- IdentityIQ policies define the access business policies of your enterprise
  - Example: Can’t have access to both approve vendor and pay vendor
- Policies are defined specifically for your environment using data from your environment
  - Identity attributes
  - Application attributes
  - Risk scores
  - Roles
  - Entitlements

Policy Usage

Compliance and Provisioning

- Policies in compliance (detective)
  - Detect identities in violation of policy and then appropriate actions can be taken
    - Notifications
    - Remediations
    - Running a workflow to handle a policy violation
  - Violations
    - Stored on the Identity Cube
    - Factor into identity score cards and enable an administrator to identify high-risk employees and act accordingly
- Policies in provisioning (preventative)
  - Identify access that would cause a violation if provisioned and then take action as specified in business process
  - Default is to prompt approver for guidance

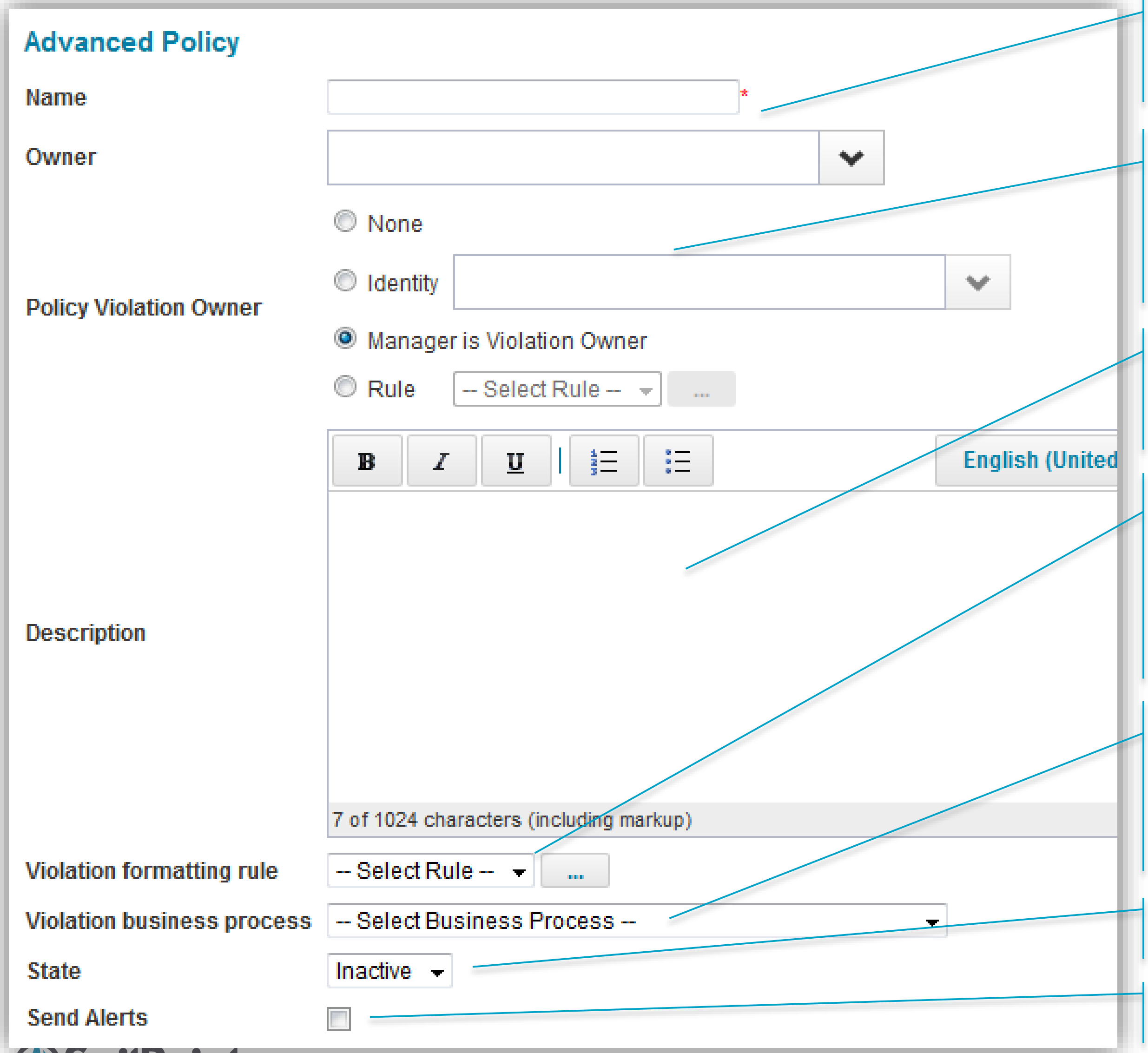
Policy – Examples

- Detect a user with conflicting access (separation of duties)
  - Role SoD
  - Entitlement SoD
- Detect a user who has not logged in to an application in a period of time (dormant account detection.)
  - Compare last login date to today's date
- Detect a non-manager who has access to a manager application
  - Comparing an identity attribute to an application attribute
- Detecting users with more than one account on any given application

Policy Types

Policy Type	Usage
Role SoD	Monitor for identities with roles that conflict
Entitlement SoD	Monitor for identities with entitlements and/or identity attributes that conflict
Activity	Flag identities with monitored activities (prior to use, must aggregate activity data from external monitoring system)
Account	Identify identities who have more than *one* account
Risk	Monitor for identities with risks higher than the threshold
Advanced	Monitor for identities with custom selection criteria: • Match List (Identity or Application Attributes) • Filter • Script • Rule • Population

Defining Policy



Advanced Policy

Name	*
Owner	▾
Policy Violation Owner	○ None ○ Identity ▾ ● Manager is Violation Owner ○ Rule -- Select Rule -- ...
Description	**B** *I* U English (United 7 of 1024 characters (including markup)
Violation formatting rule	-- Select Rule -- ...
Violation business process	-- Select Business Process --
State	Inactive
Send Alerts	□

Policy Name and Owner

Violation Owner
None, Identity, Manager or Rule

Description (multilingual)

Violation Formatting Coded Rule
(defines how to present the resulting violation)

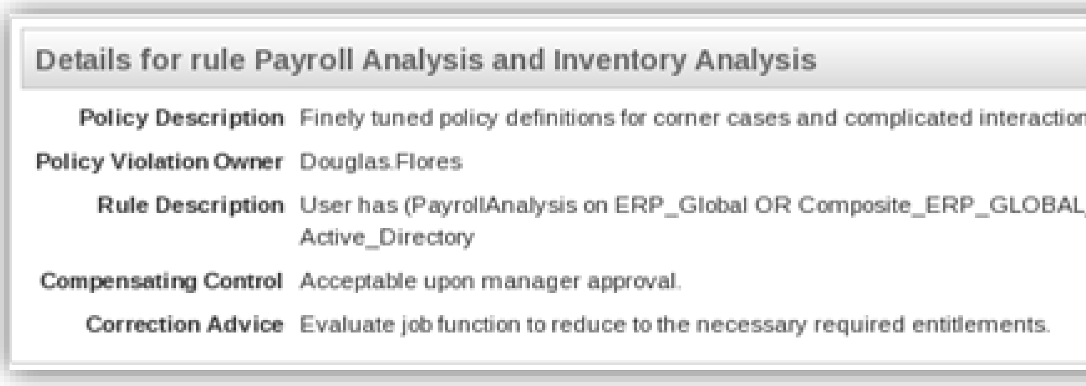
Business Process
(run when violation is detected)

Active/Inactive

Notification Options

Policy Business Rules

- Each policy consists of 1 or more business rules
  - Rules can individually be active or inactive



Details for rule Payroll Analysis and Inventory Analysis

Policy Description	Finely tuned policy definitions for corner cases and complicated interactio
Policy Violation Owner	Douglas.Flores
Rule Description	User has (PayrollAnalysis on ERP_Global OR Composite_ERP_GLOBAL Active_Directory
Compensating Control	Acceptable upon manager approval.
Correction Advice	Evaluate job function to reduce to the necessary required entitlements.

- Most rules have the same standard options

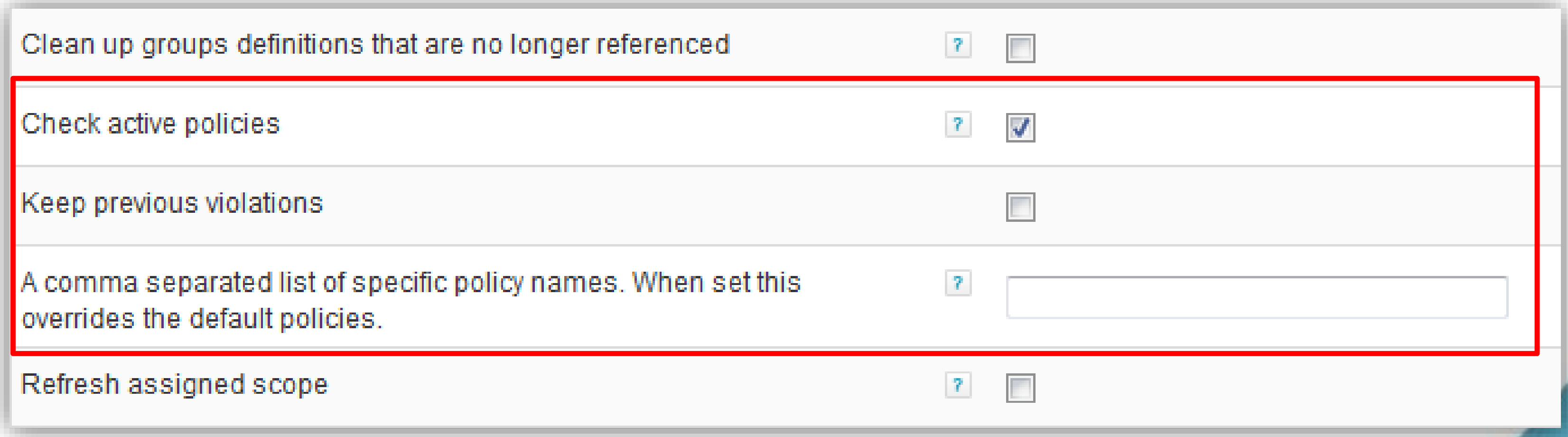
Summary	A brief title for the rule
Description	Short text which describes the rule
State	A flag indicating if the rule is active
Compensating Control	A brief description of conditions which permit exceptions to the rule
Correction Advice	A brief description of the remediation steps

- Can simulate impact prior to activating

Policy Violations

Detection

- Detect during Identity Refresh
  - Select “Check Active Policies” on Identity Refresh task
  - Default operation is to overwrite existing violations
    - Option to “Keep Previous Violations”
  - List policies for selective policy checking



Clean up groups definitions that are no longer referenced	□
Check active policies	☑
Keep previous violations	□
A comma separated list of specific policy names. When set this overrides the default policies.	
Refresh assigned scope	□

Policy Violations

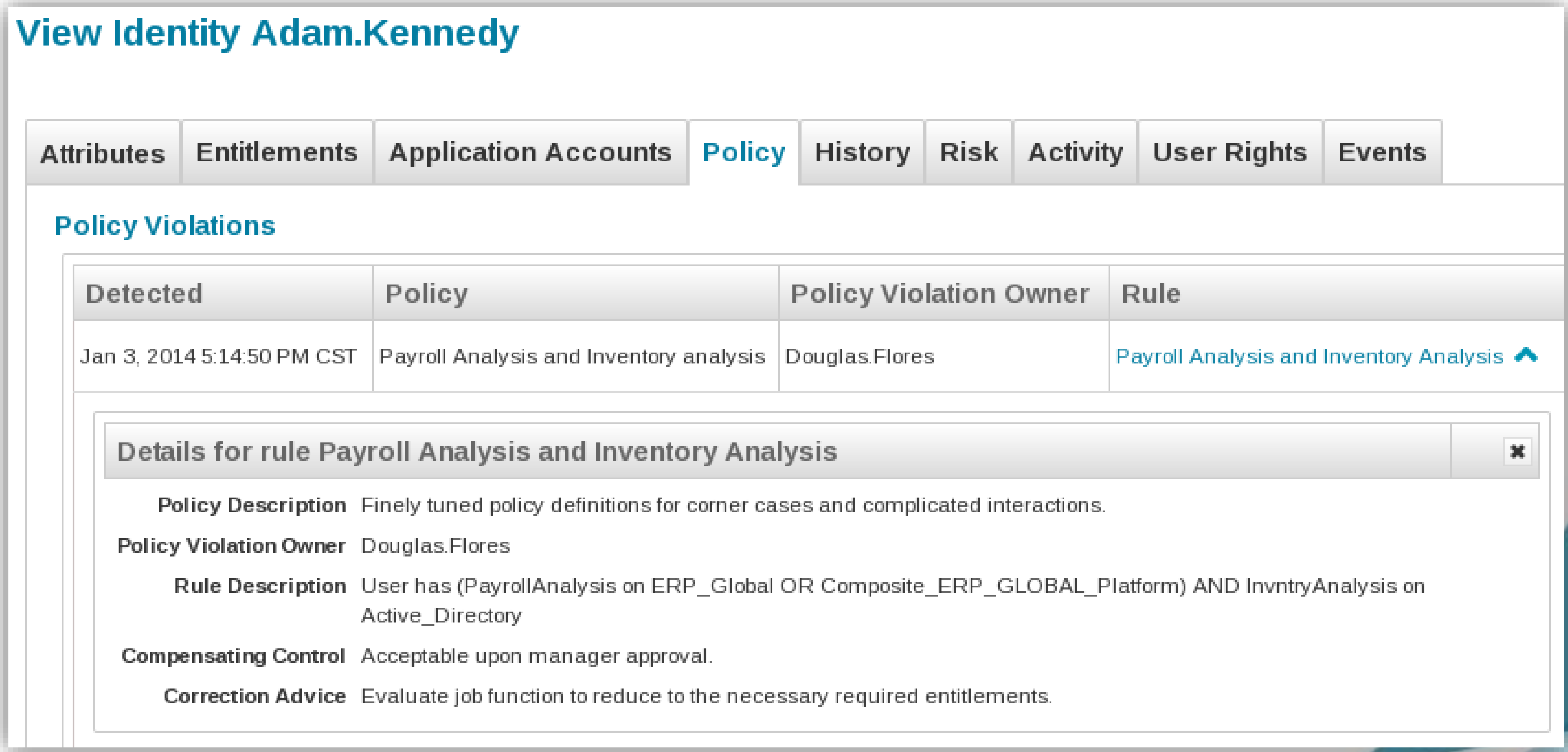
Handling

- Refresh task checks each identity for violations; if found, violations are handled based on the configuration
  - Notifications
  - Ownership
  - Business Process
- Policy Violations can be seen
  - On the Identity Cube
  - On the My Work → Policy Violations tab
  - During Certifications
  - Using Reports
  - Using the API

Policy Violations

Identity Cube

- On the Policy tab of the Identity Cube



View Identity Adam.Kennedy

Policy Violations

Detected	Policy	Policy Violation Owner	Rule
Jan 3, 2014 5:14:50 PM CST	Payroll Analysis and Inventory analysis	Douglas.Flores	Payroll Analysis and Inventory Analysis

Details for rule Payroll Analysis and Inventory Analysis

Policy Description Finely tuned policy definitions for corner cases and complicated interactions.

Policy Violation Owner Douglas.Flores

Rule Description User has (PayrollAnalysis on ERP_Global OR Composite_ERP_GLOBAL_Platform) AND InvntryAnalysis on Active_Directory

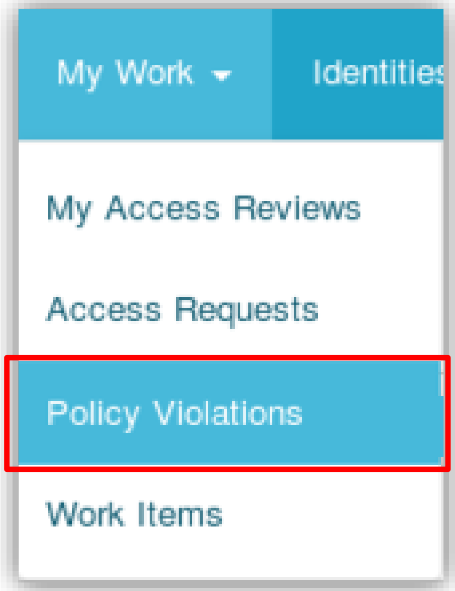
Compensating Control Acceptable upon manager approval.

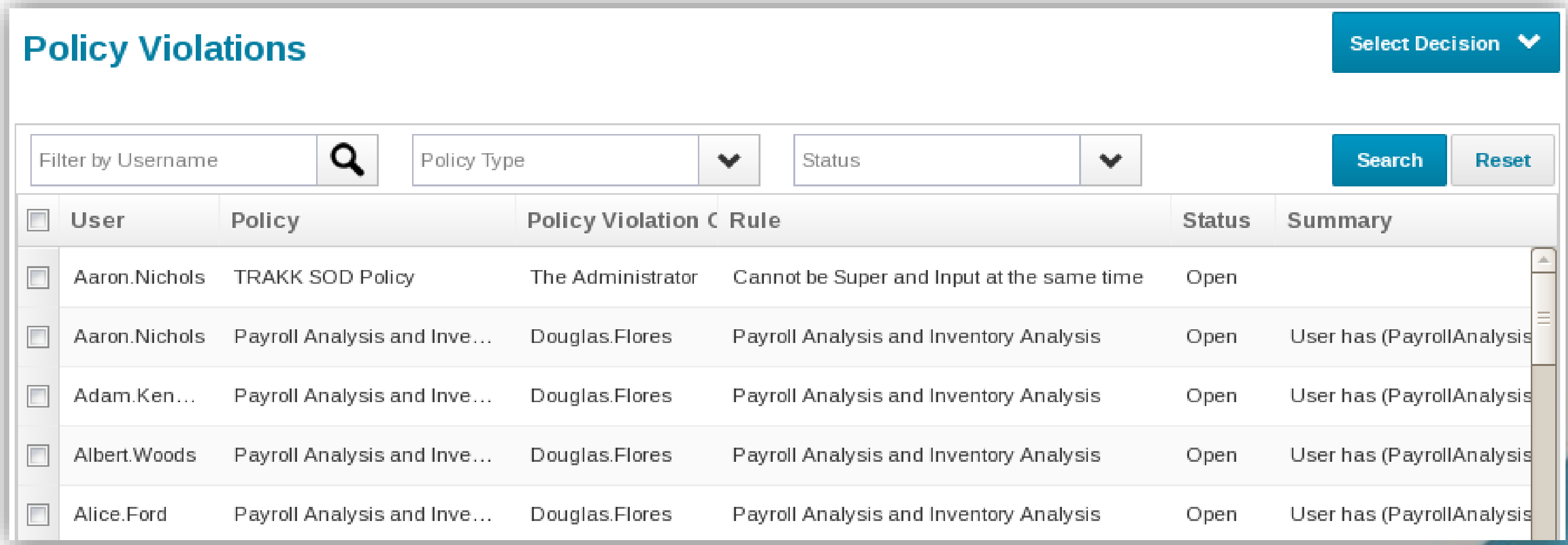
Correction Advice Evaluate job function to reduce to the necessary required entitlements.

Policy Violations

Managing

- My Work→ Policy Violations
- Take action on Policy Violations page
  - Dependent upon capability
    - Most users: List of all violations assigned to user
    - Admins: List of all active violations in the enterprise



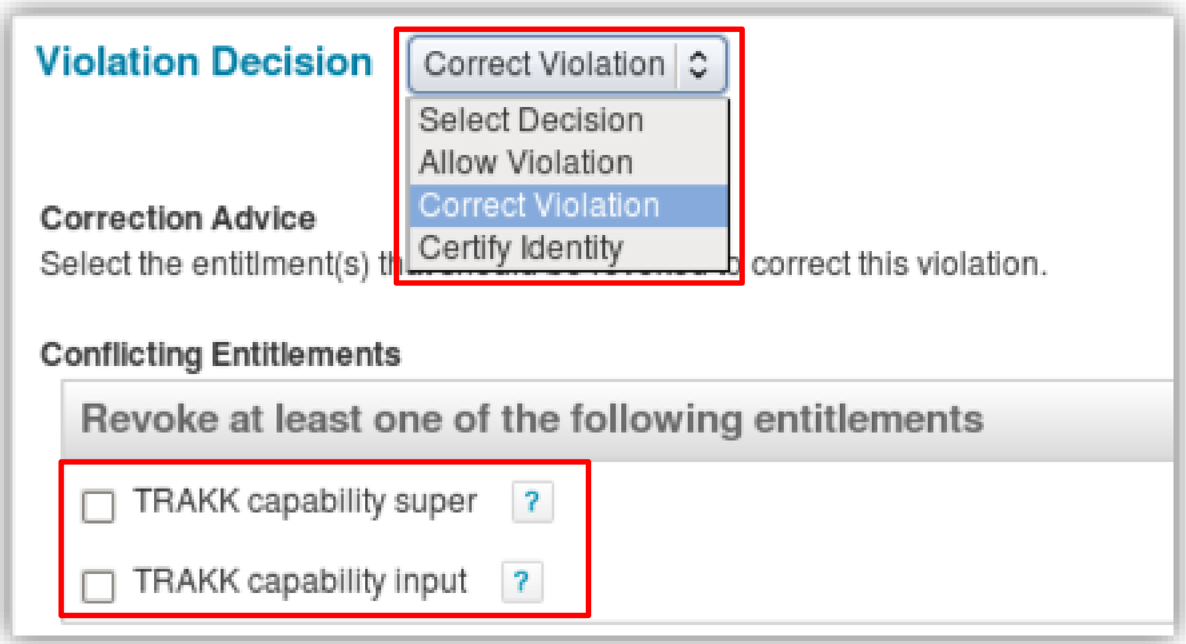


□	User	Policy	Policy Violation O	Rule	Status	Summary
□	Aaron.Nichols	TRAKK SOD Policy	The Administrator	Cannot be Super and Input at the same time	Open	
□	Aaron.Nichols	Payroll Analysis and Inve…	Douglas.Flores	Payroll Analysis and Inventory Analysis	Open	User has (PayrollAnalysis
□	Adam.Ken…	Payroll Analysis and Inve…	Douglas.Flores	Payroll Analysis and Inventory Analysis	Open	User has (PayrollAnalysis
□	Albert.Woods	Payroll Analysis and Inve…	Douglas.Flores	Payroll Analysis and Inventory Analysis	Open	User has (PayrollAnalysis
□	Alice.Ford	Payroll Analysis and Inve…	Douglas.Flores	Payroll Analysis and Inventory Analysis	Open	User has (PayrollAnalysis

Policy Violations

Taking Action

- Actions can include
  - Allowing Exceptions – choose date and add comment
  - Correcting (Role or Entitlement SoD only) – resolve conflicts by revoking
  - Certifying identity – trigger certification of single identity



Violation Decision Correct Violation

- Select Decision
- Allow Violation
- Correct Violation
- Certify Identity

Correction Advice

Select the entitlment(s) th correct this violation.

Conflicting Entitlements

Revoke at least one of the following entitlements

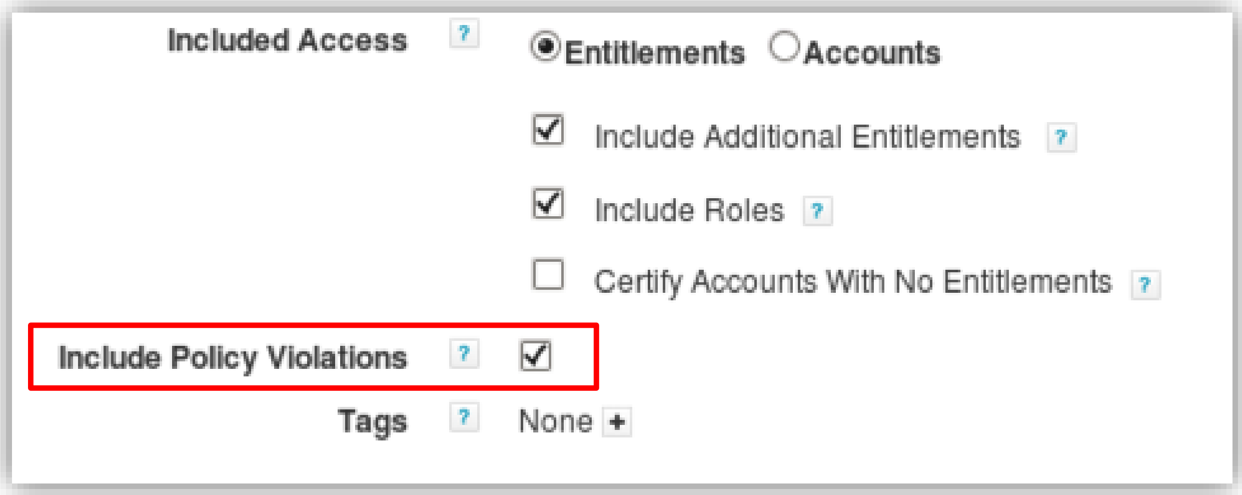
□ TRAKK capability super ?

□ TRAKK capability input ?

Policy Violations

Certifications

- Actions may be taken on policy violations during an Access Review
  - Configure Certification to include Policy Violations



Included Access ? ● Entitlements ○ Accounts

☑ Include Additional Entitlements ?

☑ Include Roles ?

□ Certify Accounts With No Entitlements ?

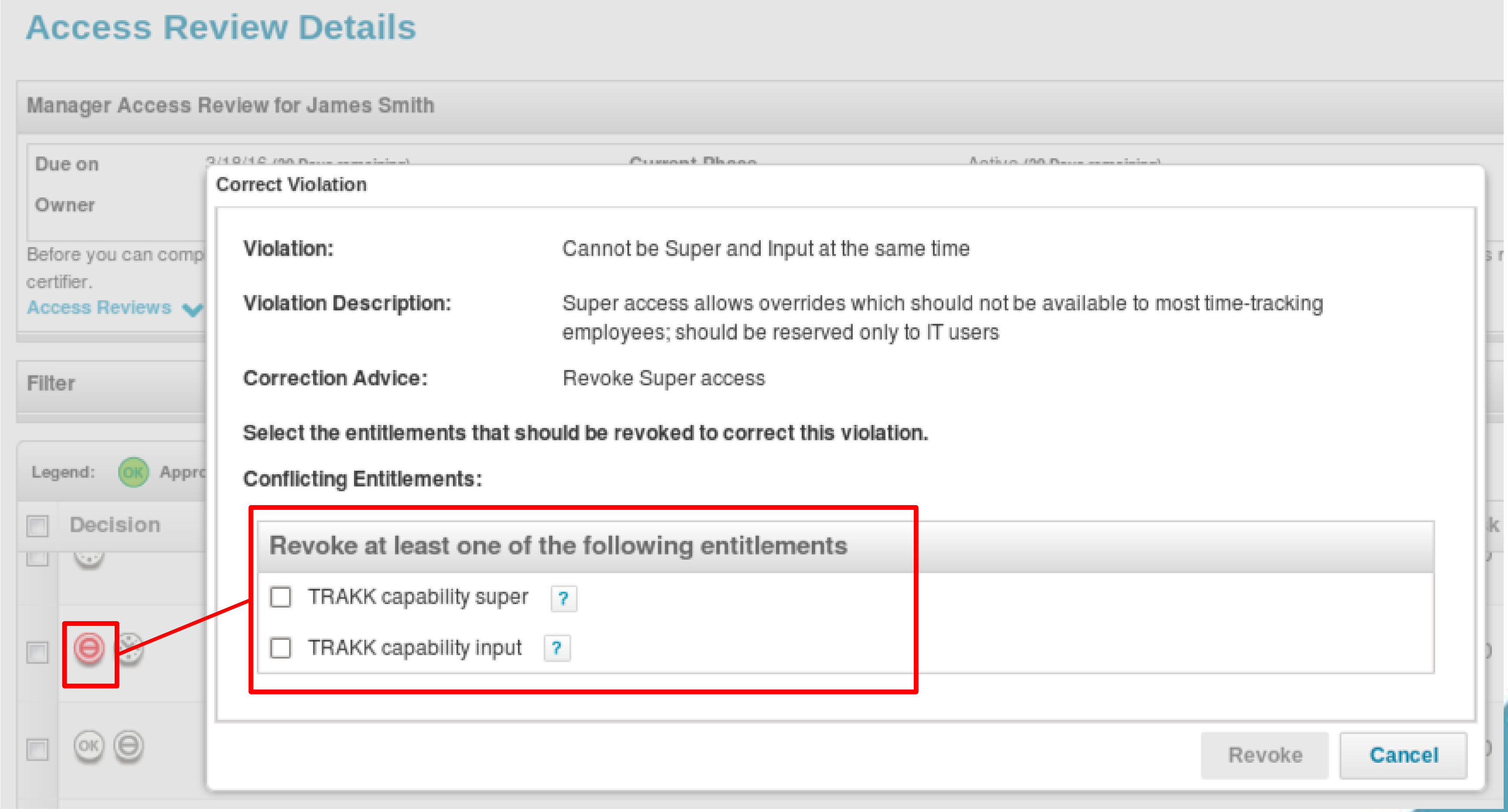
Include Policy Violations ? ☑

Tags ? None +

  - During Access Reviews, certifiers can allow exceptions or revoke conflicting items

Policy Violations

Handling in Certification



Access Review Details

Manager Access Review for James Smith

Due on

Owner

Before you can comp

certifier.

Access Reviews

Filter

Legend: OK Appro

□ Decision

Correct Violation

Violation: Cannot be Super and Input at the same time

Violation Description: Super access allows overrides which should not be available to most time-tracking employees; should be reserved only to IT users

Correction Advice: Revoke Super access

Select the entitlements that should be revoked to correct this violation.

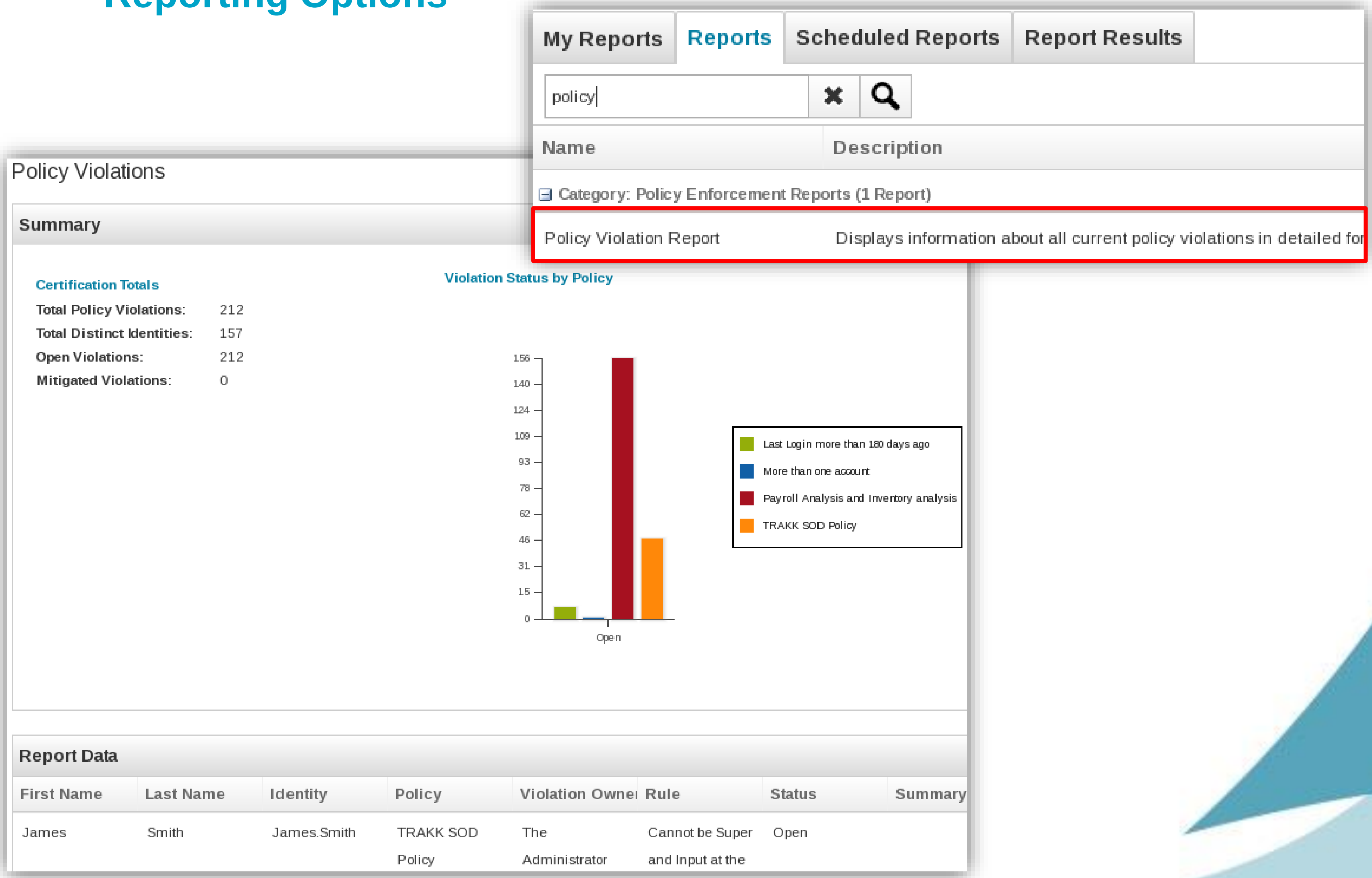
Conflicting Entitlements:

Revoke at least one of the following entitlements

- □ TRAKK capability super ?
- □ TRAKK capability input ?

Policy Violations

Reporting Options



My Reports | Reports | Scheduled Reports | Report Results

policy

Name	Description
⊟ Category: Policy Enforcement Reports (1 Report)	
Policy Violation Report	Displays information about all current policy violations in detailed fo

Policy Violations

Summary

Certification Totals

Total Policy Violations:	212
Total Distinct Identities:	157
Open Violations:	212
Mitigated Violations:	0

Violation Status by Policy

🟩 Last Login more than 180 days ago
🟦 More than one account
🟥 Payroll Analysis and Inventory analysis
🟧 TRAKK SOD Policy

Report Data

First Name	Last Name	Identity	Policy	Violation Owner	Rule	Status	Summary
James	Smith	James.Smith	TRAKK SOD Policy	The Administrator	Cannot be Super and Input at the	Open	

Risk Administration

Overview

- Risk Scoring Overview
- Risk Scoring Configuration
  - Identity Risk Score Configuration
  - Application Risk Score Configuration
- Monitoring Risk

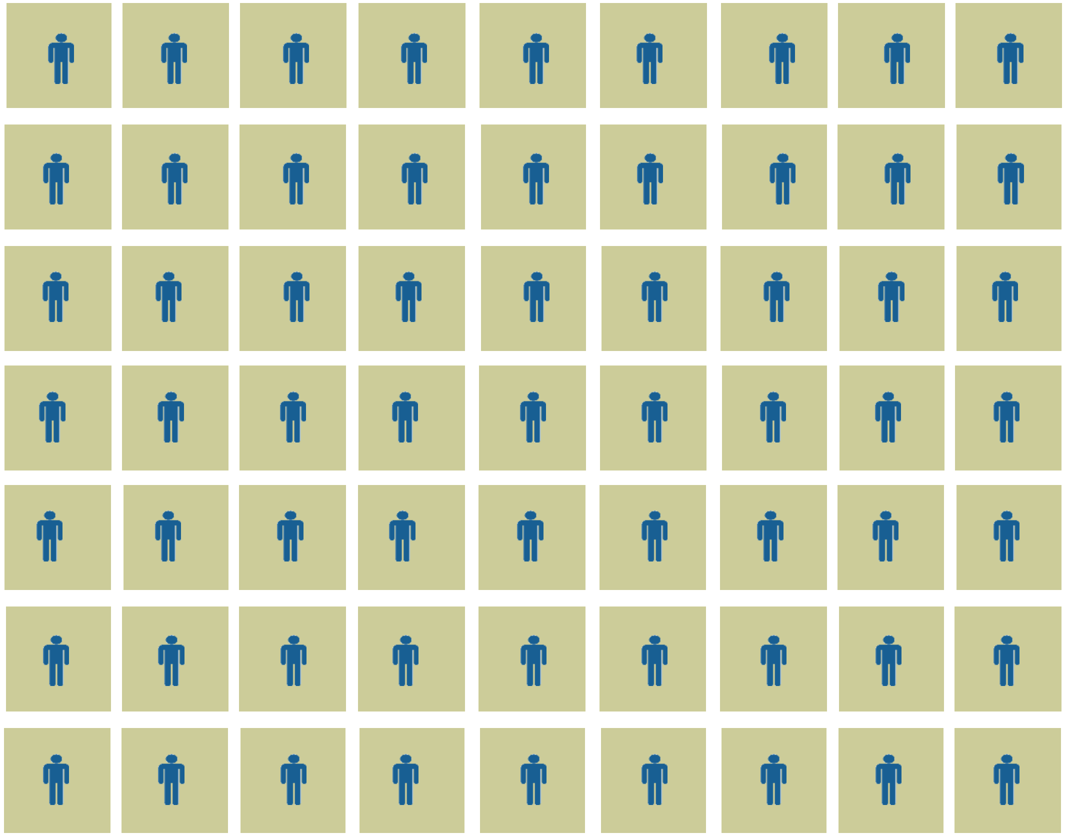
Risk

Definition and Purpose

- What is risk scoring?
  - Process of applying a risk scoring methodology to identities and applications to assign a numeric risk value
- Why risk score?
  - Allow companies to flag identities or applications that pose the greatest security threat to their enterprise
- IdentityIQ provides two types of risk scoring
  - Identity
  - Application

Risk Scoring Overview

Without risk scoring, all users must be scrutinized…



Risk Scoring Overview

But with risk scoring, enterprises can focus on the users “of interest.”

Low Risk Profile

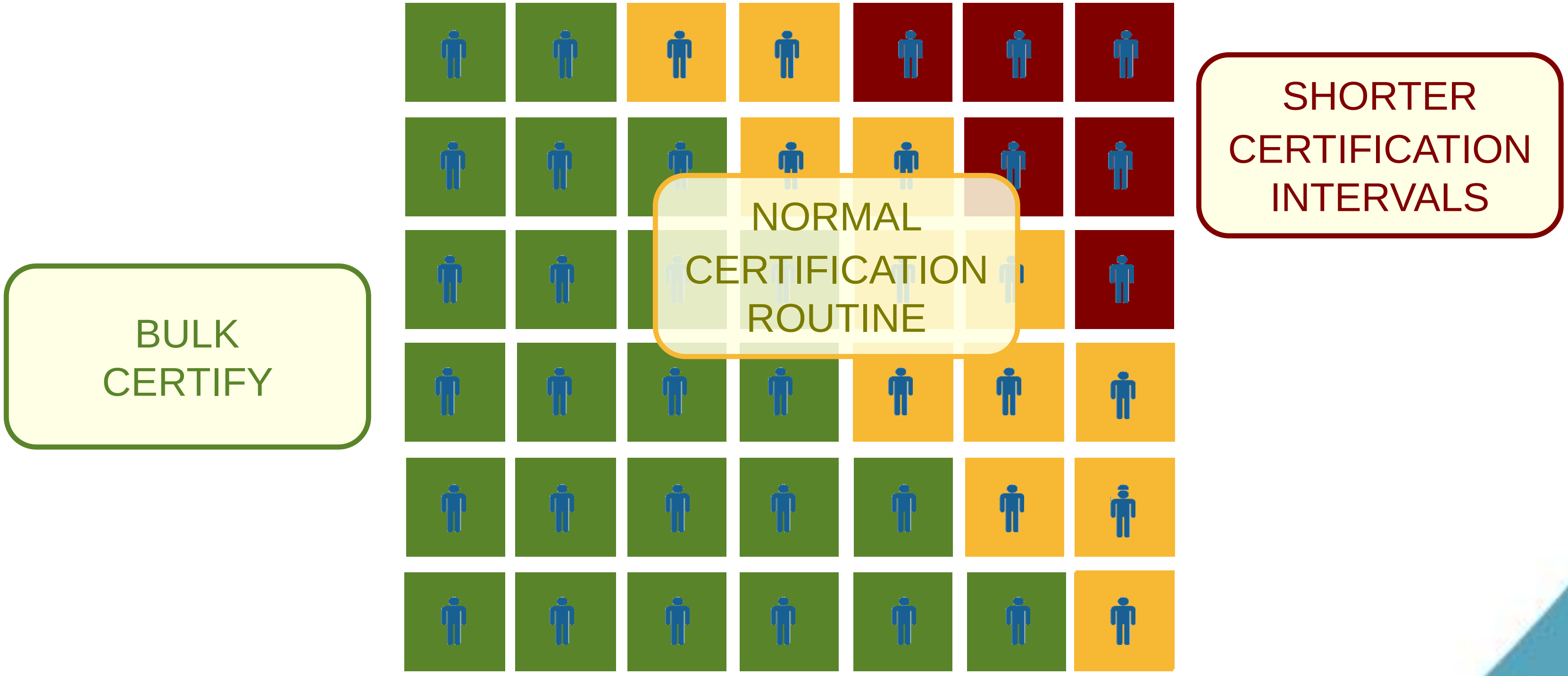
- Read-only privileges
- No policy violations
- No access to high risk apps
- Risk score <300

Medium Risk Profile

- Mitigated policy violations
- Previously approved high-risk application access
- 301< Risk score <600

High Risk Profile

- Privileged user accounts
- Active policy violations
- Aged certification status
- Pending remediations
- High risk application access (not previously approved)
- Risk score >601



BULK CERTIFY

NORMAL CERTIFICATION ROUTINE

SHORTER CERTIFICATION INTERVALS

Identity Risk Score Configuration

Risk Scoring Details

- Identity Risk scoring is based on

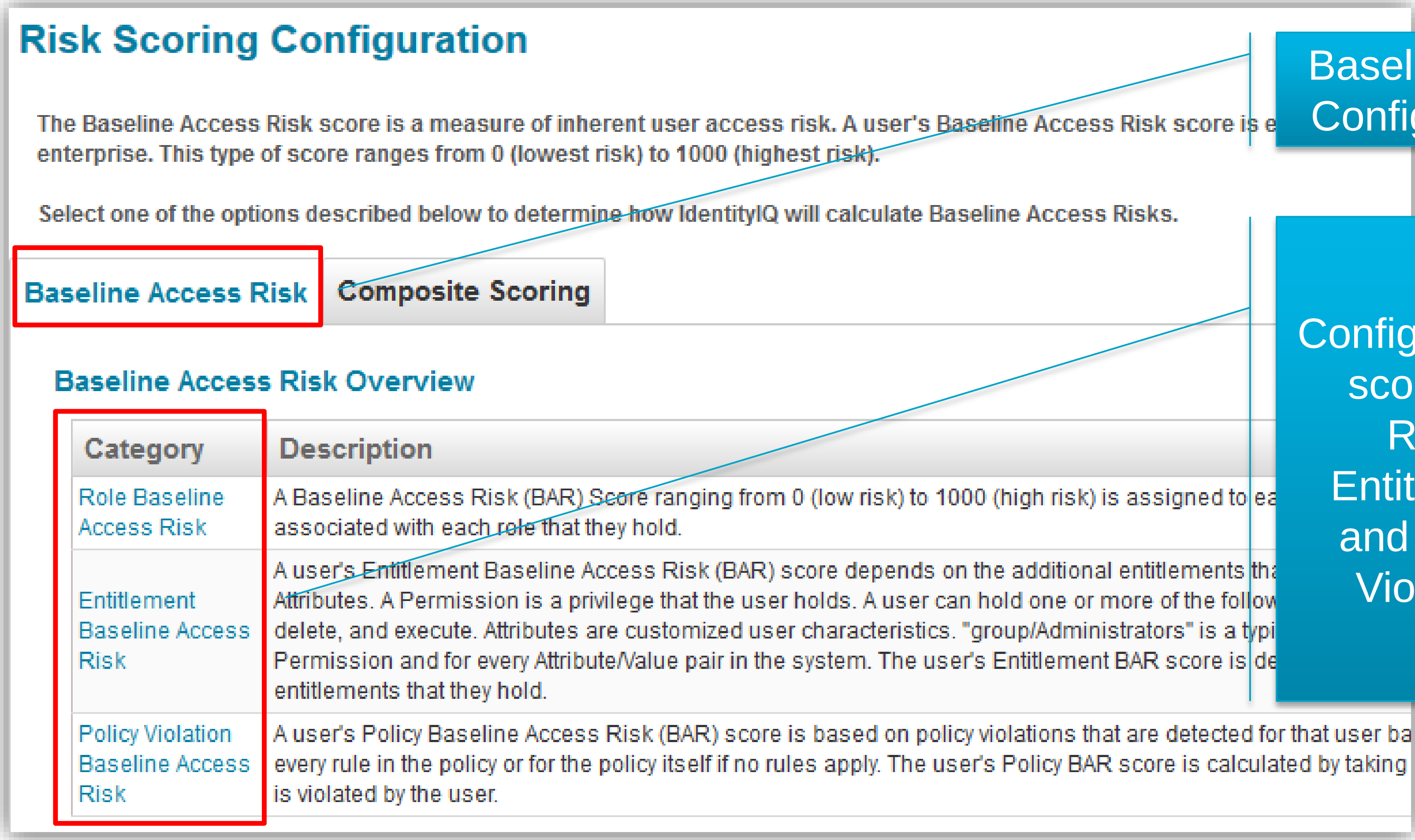
Roles/Entitlements

Violations

Certification Age

Identity Risk

1. Define Baseline Risk



Risk Scoring Configuration

The Baseline Access Risk score is a measure of inherent user access risk. A user's Baseline Access Risk score is e
enterprise. This type of score ranges from 0 (lowest risk) to 1000 (highest risk).

Select one of the options described below to determine how IdentityIQ will calculate Baseline Access Risks.

Baseline Access Risk Overview

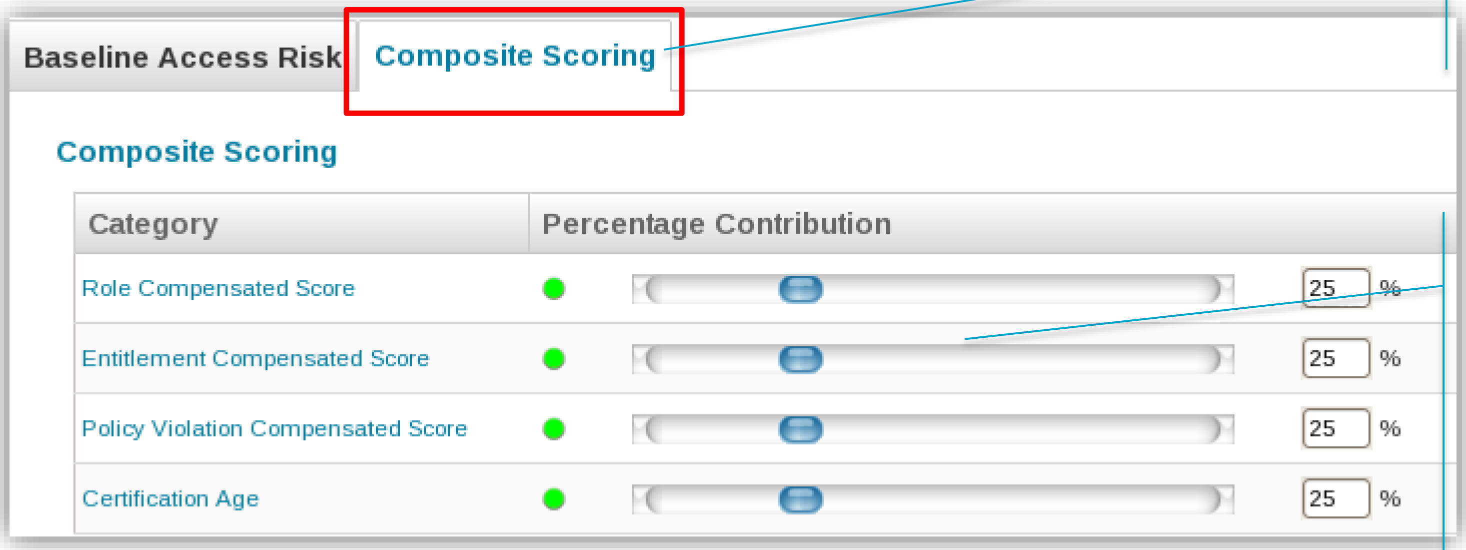
Category	Description
Role Baseline Access Risk	A Baseline Access Risk (BAR) Score ranging from 0 (low risk) to 1000 (high risk) is assigned to ea associated with each role that they hold.
Entitlement Baseline Access Risk	A user's Entitlement Baseline Access Risk (BAR) score depends on the additional entitlements tha Attributes. A Permission is a privilege that the user holds. A user can hold one or more of the follow delete, and execute. Attributes are customized user characteristics. "group/Administrators" is a typi Permission and for every Attribute/Value pair in the system. The user's Entitlement BAR score is de entitlements that they hold.
Policy Violation Baseline Access Risk	A user's Policy Baseline Access Risk (BAR) score is based on policy violations that are detected for that user ba every rule in the policy or for the policy itself if no rules apply. The user's Policy BAR score is calculated by taking is violated by the user.

Baseline Risk Configuration

Configure Risk score per Role, Entitlement and Policy Violation

Identity Risk

2. Define Composite Scoring



Composite Scoring

Category		Percentage Contribution	
Role Compensated Score	●	25	%
Entitlement Compensated Score	●	25	%
Policy Violation Compensated Score	●	25	%
Certification Age	●	25	%

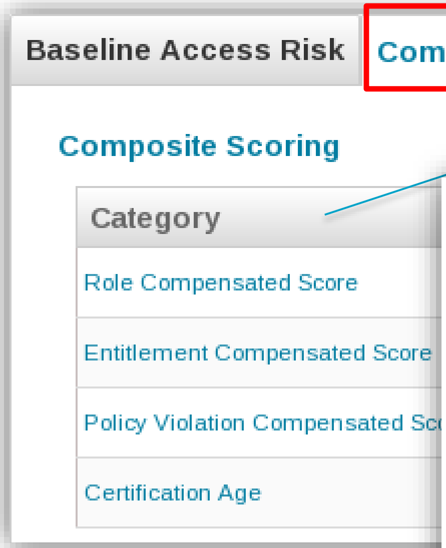
Composite Scoring Configuration

Configure percentage contribution from each risk component

Identity Risk

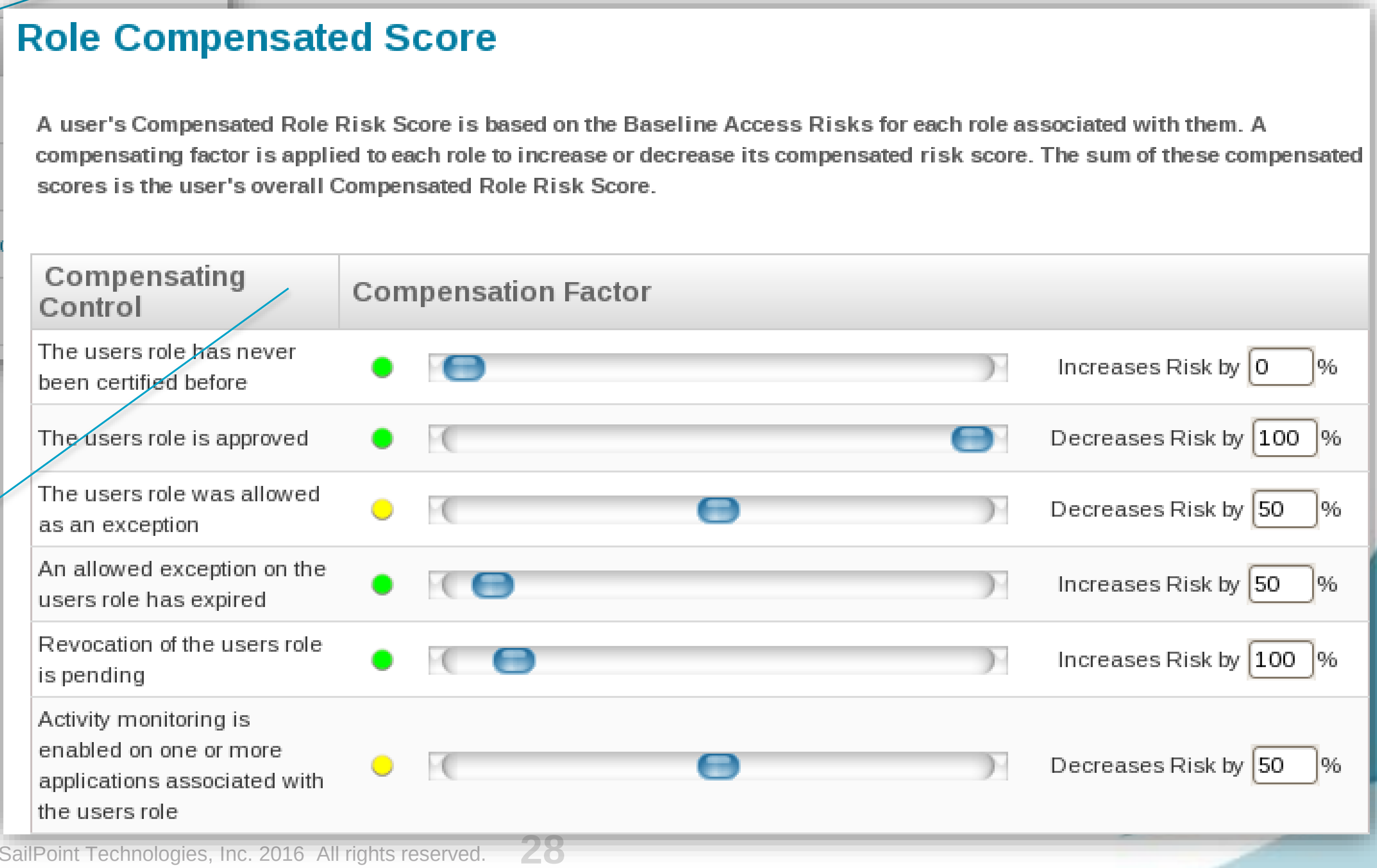
3. Define Compensated Scores

For each Composite Scoring category…



Composite Scoring

Category
Role Compensated Score
Entitlement Compensated Score
Policy Violation Compensated Sc
Certification Age



Role Compensated Score

A user's Compensated Role Risk Score is based on the Baseline Access Risks for each role associated with them. A compensating factor is applied to each role to increase or decrease its compensated risk score. The sum of these compensated scores is the user's overall Compensated Role Risk Score.

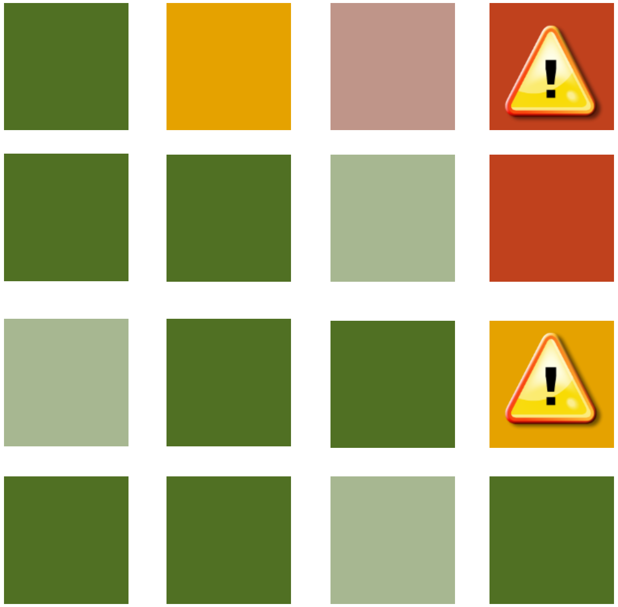
Compensating Control	Compensation Factor
The users role has never been certified before	● Increases Risk by 0 %
The users role is approved	● Decreases Risk by 100 %
The users role was allowed as an exception	● Decreases Risk by 50 %
An allowed exception on the users role has expired	● Increases Risk by 50 %
Revocation of the users role is pending	● Increases Risk by 100 %
Activity monitoring is enabled on one or more applications associated with the users role	● Decreases Risk by 50 %

…set percentage contribution for Compensation Factors

Application Risk Score Configuration

Risk Scoring Details

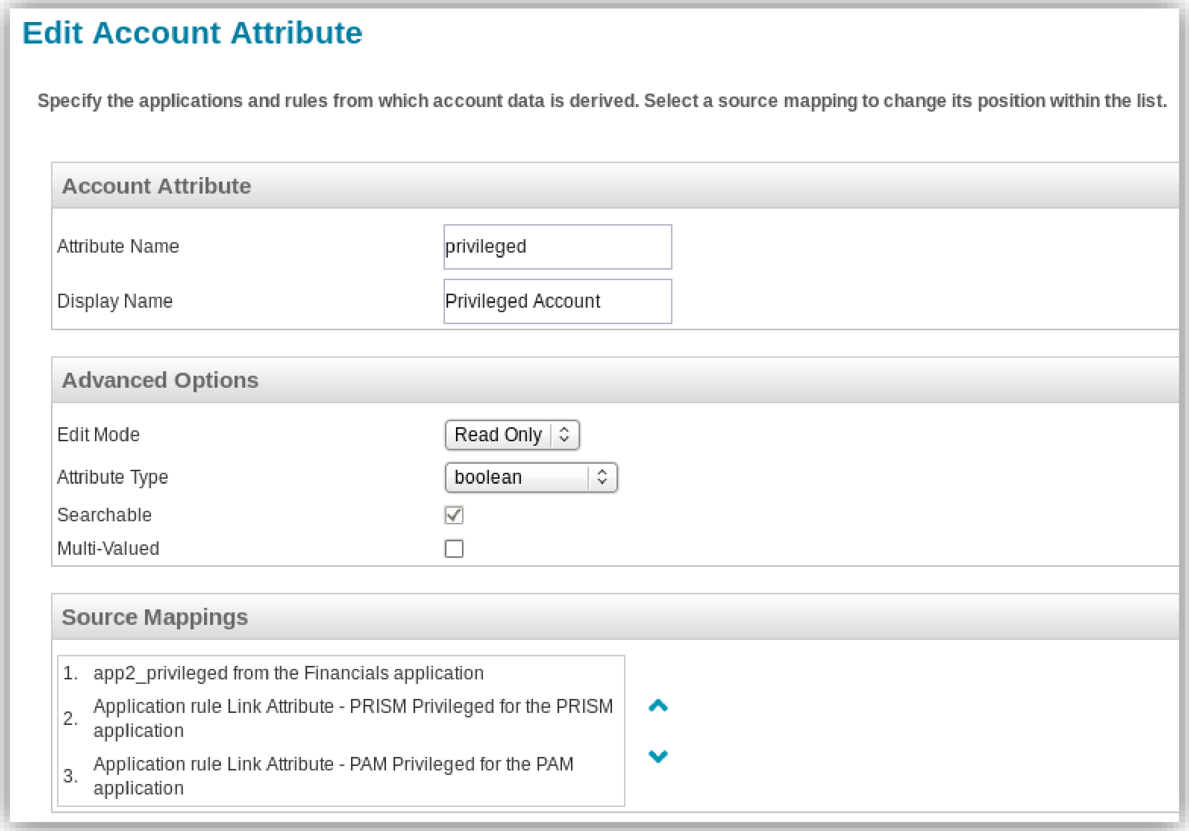
- Application Risk scoring is based on
  - % of Service, Privileged, Inactive and Dormant Accounts
  - % of accounts owned by risky identities
  - % of accounts owned by identities with policy violations



Account Attributes

Define Service, Privileged, Inactive, Dormant Accounts

- Designate data source of attributes for each application
- Normalize data across applications



Edit Account Attribute

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

Account Attribute

Attribute Name	privileged
Display Name	Privileged Account

Advanced Options

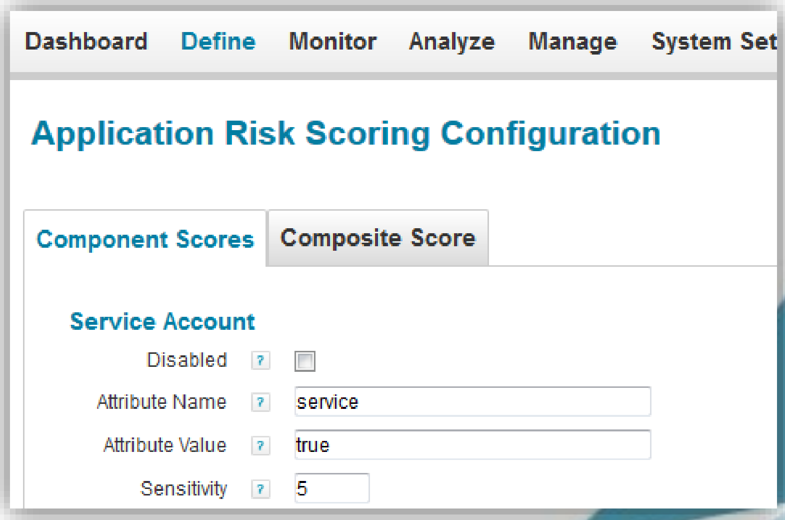
Edit Mode	Read Only
Attribute Type	boolean
Searchable	☑
Multi-Valued	☐

Source Mappings

1. app2_privileged from the Financials application
2. Application rule Link Attribute - PRISM Privileged for the PRISM application
3. Application rule Link Attribute - PAM Privileged for the PAM application

Application Risk Scoring

1. Determine scoring for each component
   - Configure attributes for identifying service, inactive, dormant and privileged accounts
   - Determine thresholds for risky and violator accounts
   - Determine sensitivity for each individual component
2. Determine overall % contribution *Composite Score*
   - Service, inactive, dormant and privileged accounts
   - Risky accounts
   - Violator accounts



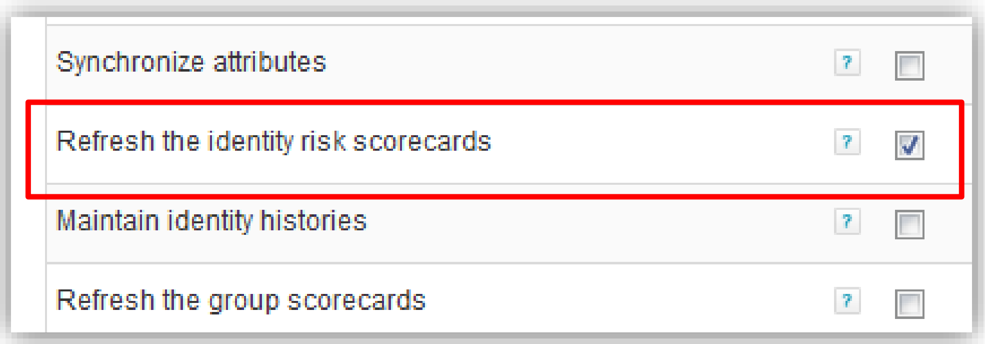
Application Risk Scoring Configuration

Service Account

Disabled	□
Attribute Name	service
Attribute Value	true
Sensitivity	5

Calculating Risk Scores

- Identity Risk Scoring
  - Identity Refresh Task, check “Refresh the identity risk scorecards”
  - Preconfigured task: Refresh Risk Scores



Synchronize attributes ? □

Refresh the identity risk scorecards ? ☑

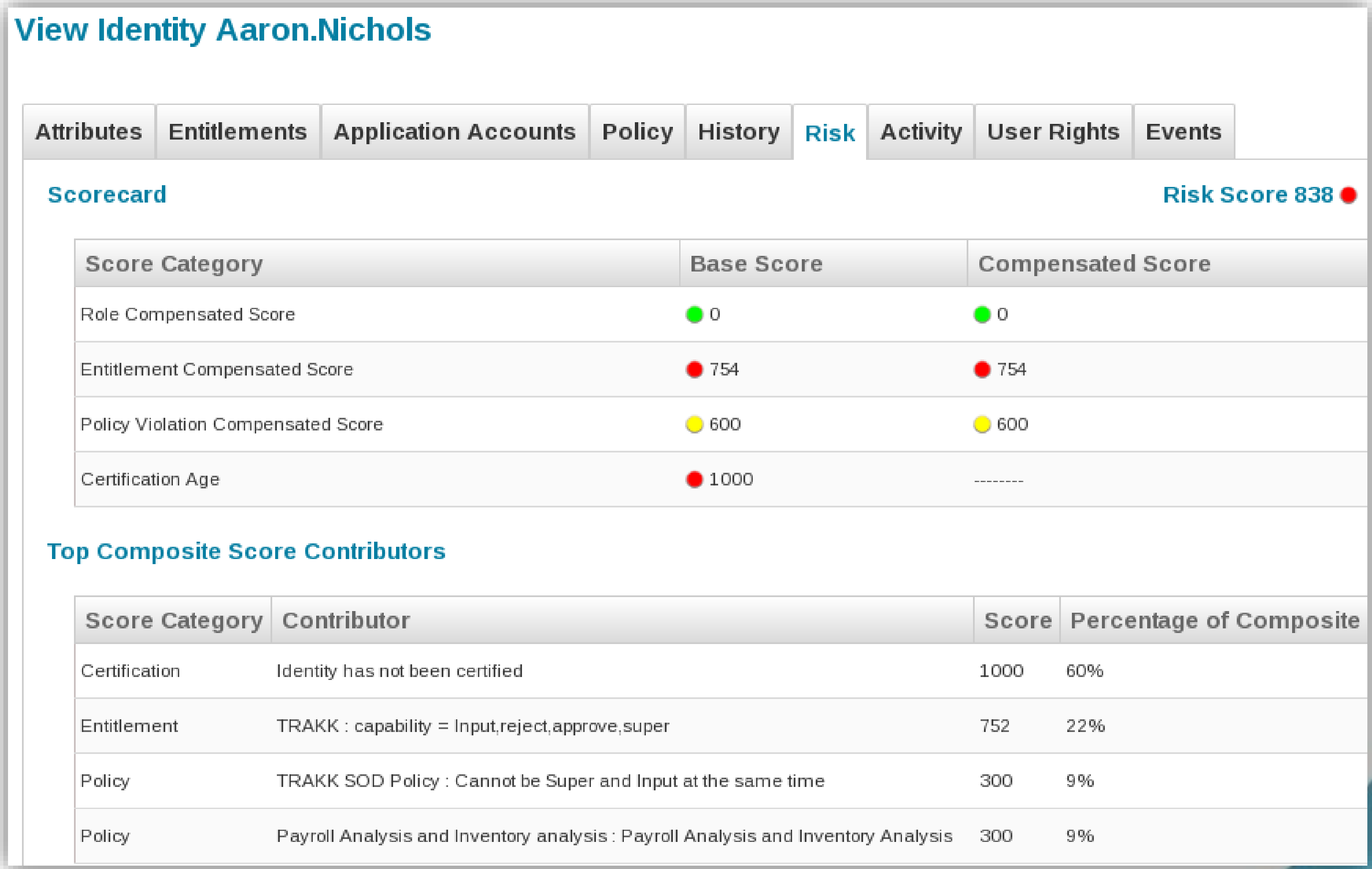
Maintain identity histories ? □

Refresh the group scorecards ? □

- Application Risk Scoring
  - Preconfigured task: Refresh Application Scores
  - Must update identity scores first
    - Application scores are dependent on the identity risk scores

Where to Monitor Risk Scores

Identity Risk Tab



Scorecard

Risk Score 838 ●

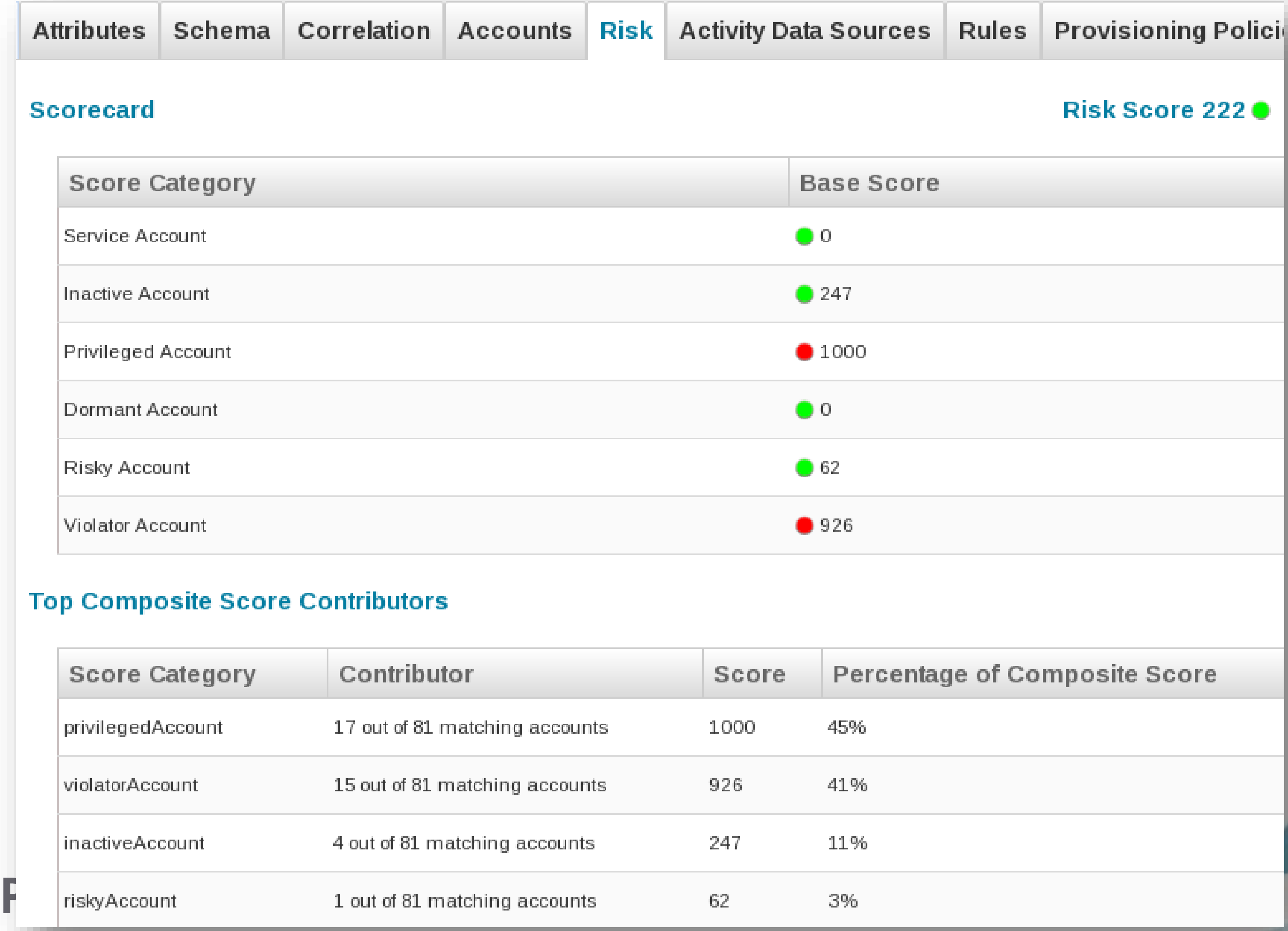
Score Category	Base Score	Compensated Score
Role Compensated Score	● 0	● 0
Entitlement Compensated Score	● 754	● 754
Policy Violation Compensated Score	● 600	● 600
Certification Age	● 1000	--------

Top Composite Score Contributors

Score Category	Contributor	Score	Percentage of Composite
Certification	Identity has not been certified	1000	60%
Entitlement	TRAKK : capability = Input,reject,approve,super	752	22%
Policy	TRAKK SOD Policy : Cannot be Super and Input at the same time	300	9%
Policy	Payroll Analysis and Inventory analysis : Payroll Analysis and Inventory Analysis	300	9%

Where to Monitor Risk Scores

Application Risk Tab



Scorecard

Risk Score 222 🟢

Score Category	Base Score
Service Account	🟢 0
Inactive Account	🟢 247
Privileged Account	🔴 1000
Dormant Account	🟢 0
Risky Account	🟢 62
Violator Account	🔴 926

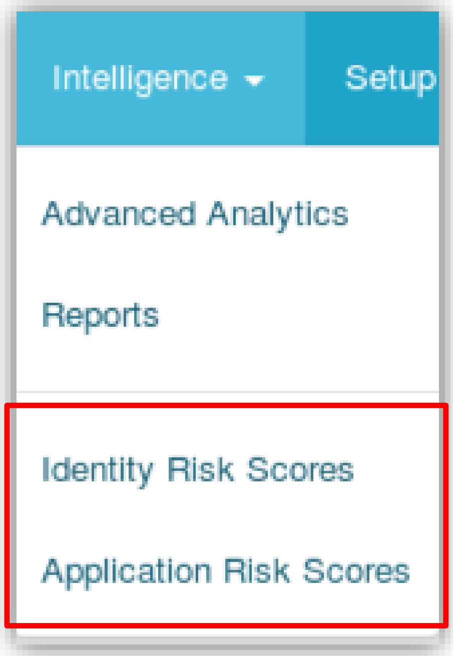
Top Composite Score Contributors

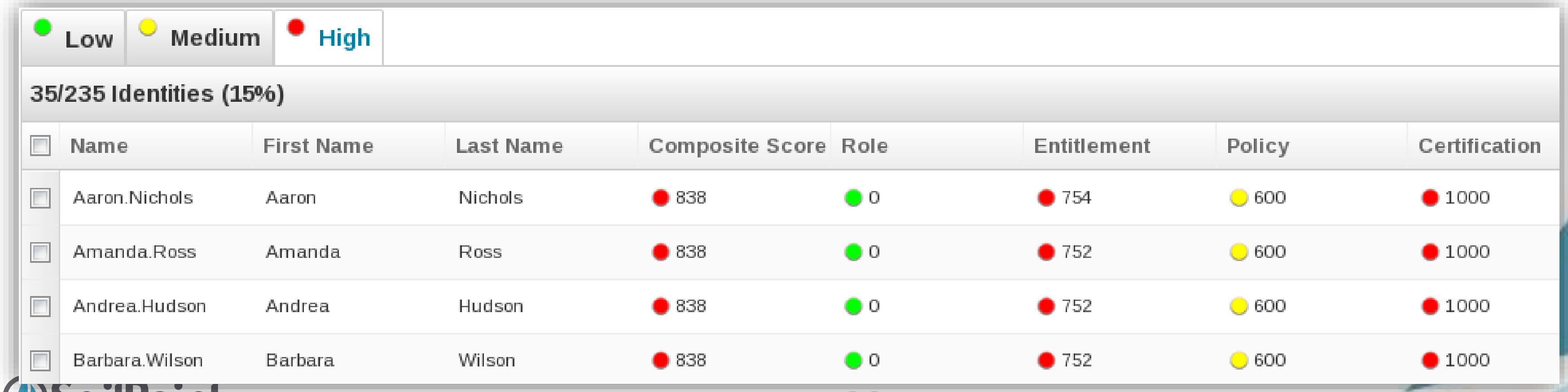
Score Category	Contributor	Score	Percentage of Composite Score
privilegedAccount	17 out of 81 matching accounts	1000	45%
violatorAccount	15 out of 81 matching accounts	926	41%
inactiveAccount	4 out of 81 matching accounts	247	11%
riskyAccount	1 out of 81 matching accounts	62	3%

Where to Monitor Risk Scores

Manage Link

- Identity Risk Scores
  - Sort scores by risk score
  - See scores by risk band (low/med/high)
  - Perform Certifications
- Application Risk Scores
  - Sort application risk scores





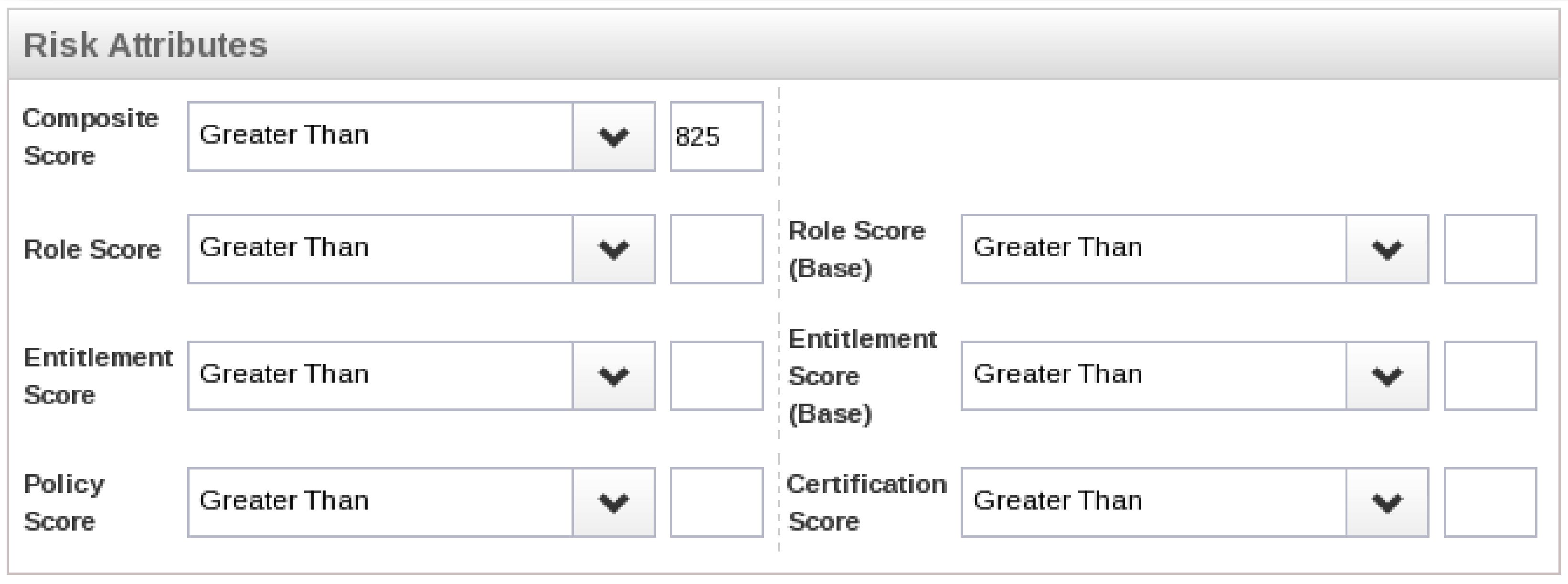
35/235 Identities (15%)

□	Name	First Name	Last Name	Composite Score	Role	Entitlement	Policy	Certification
□	Aaron.Nichols	Aaron	Nichols	🔴 838	🟢 0	🔴 754	🟡 600	🔴 1000
□	Amanda.Ross	Amanda	Ross	🔴 838	🟢 0	🔴 752	🟡 600	🔴 1000
□	Andrea.Hudson	Andrea	Hudson	🔴 838	🟢 0	🔴 752	🟡 600	🔴 1000
□	Barbara.Wilson	Barbara	Wilson	🔴 838	🟢 0	🔴 752	🟡 600	🔴 1000

Where to Monitor Risk Scores

Advanced Analytics

- Risk scores are a searchable value in Analytics
- Can use risk scores to define high risk populations for more aggressive certification actions
- Risk Scores are also available via the API



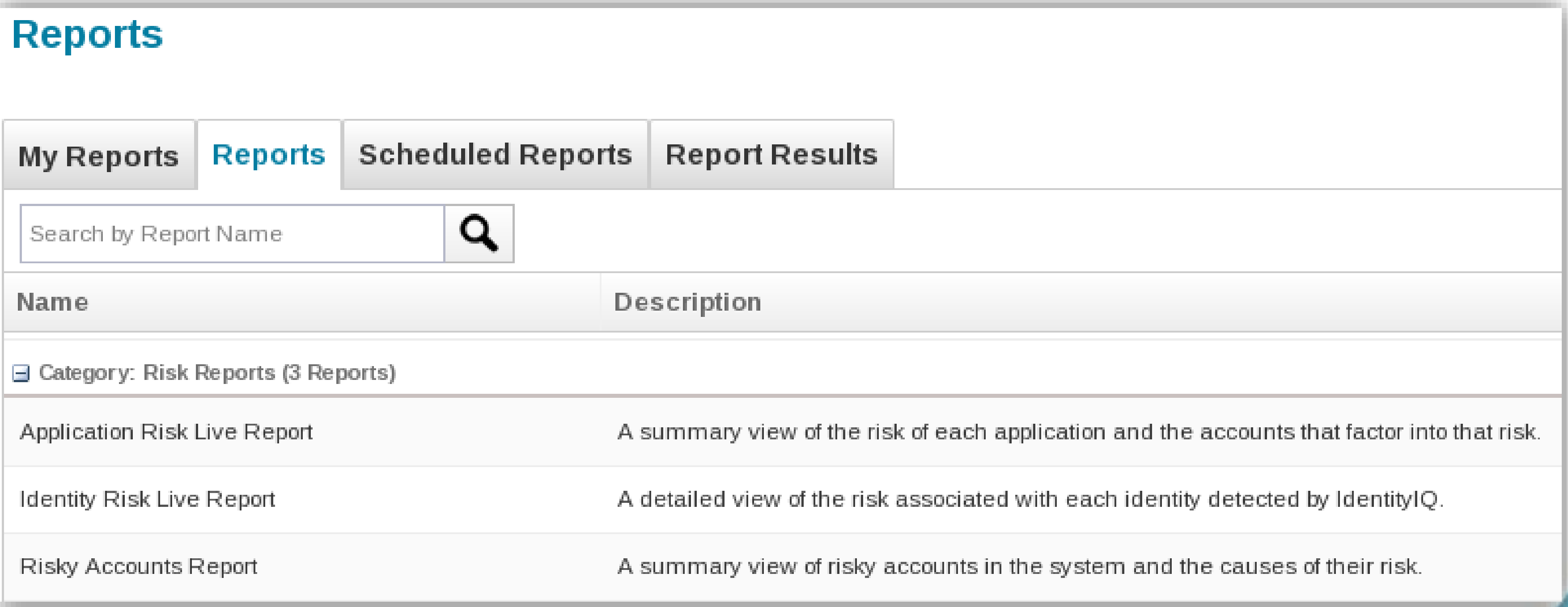
Risk Attributes

Composite Score	Greater Than	825			
Role Score	Greater Than		Role Score (Base)	Greater Than	
Entitlement Score	Greater Than		Entitlement Score (Base)	Greater Than	
Policy Score	Greater Than		Certification Score	Greater Than	

Where to View Risk Scores

Reporting

- Report on risky identities, applications, or accounts



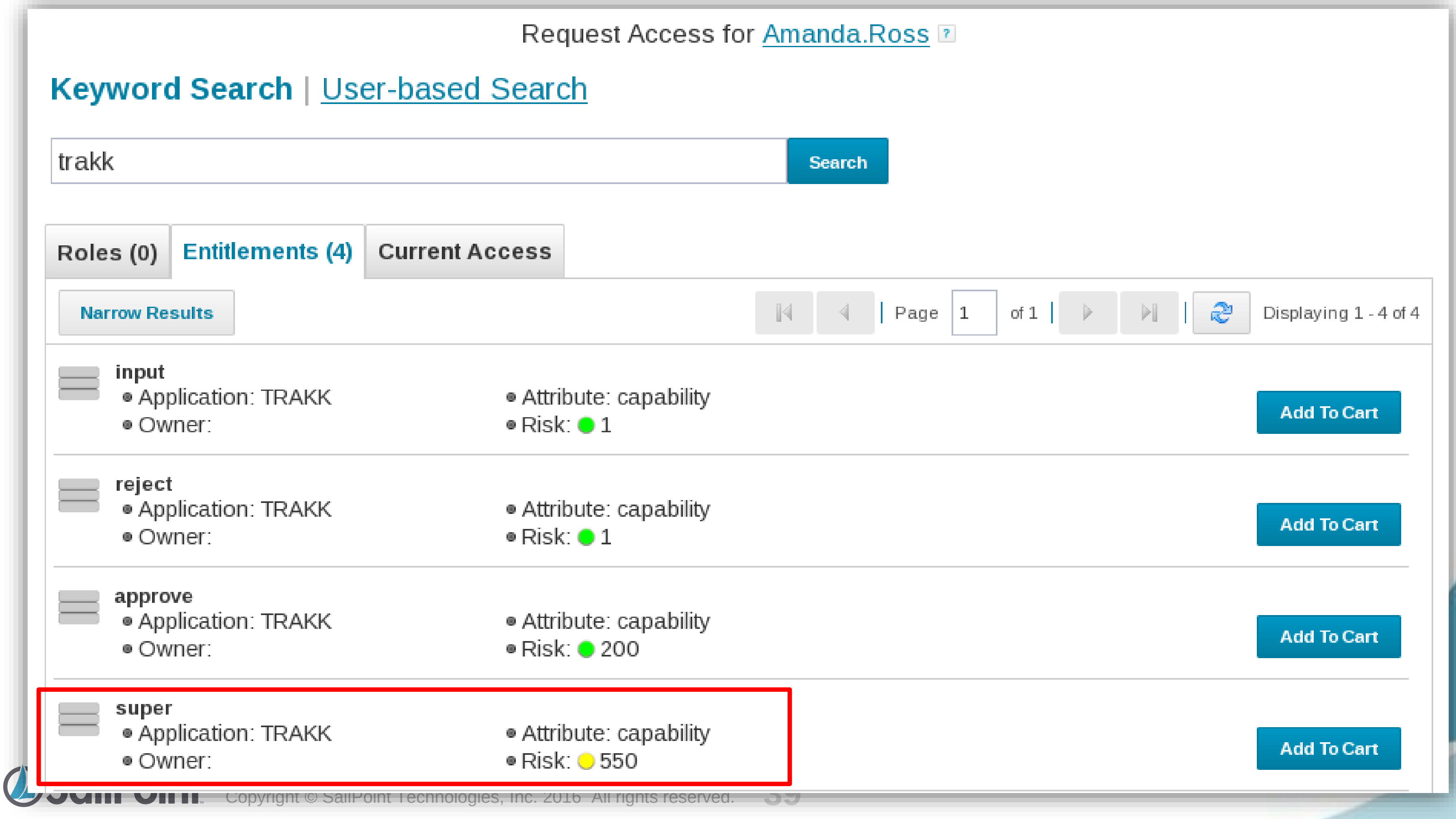
Reports

Name	Description
⊟ Category: Risk Reports (3 Reports)	
Application Risk Live Report	A summary view of the risk of each application and the accounts that factor into that risk.
Identity Risk Live Report	A detailed view of the risk associated with each identity detected by IdentityIQ.
Risky Accounts Report	A summary view of risky accounts in the system and the causes of their risk.

Risk Score Preview

Lifecycle Manager

- Preview risk values when requesting access



Request Access for Amanda.Ross

Keyword Search | User-based Search

trakk

input
- Application: TRAKK
- Owner:
- Attribute: capability
- Risk: 🟢 1

reject
- Application: TRAKK
- Owner:
- Attribute: capability
- Risk: 🟢 1

approve
- Application: TRAKK
- Owner:
- Attribute: capability
- Risk: 🟢 200

super
- Application: TRAKK
- Owner:
- Attribute: capability
- Risk: 🟡 550

Questions?

Exercise Preview

Section 2, Exercises 1, 2, 3, 4, 5

- Making sense of our users and their access
  - Exercise 1: Handling Uncorrelated Identities and Accounts
  - Exercise 2: Configuring Account Attributes
  - Exercise 3: Creating Groups and Populations
- Identity and correct issues with user’s access
  - Exercise 4: Create Policies
  - Exercise 5: Defining Identity Risk Scoring (optional)