

# 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

# 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 information from your environment

Example:

- 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

- Role SOD Policy
- Entitlement SOD Policy
- Activity Policy
- Account Policy
- Risk Policy
- Advanced Policy

The screenshot displays the 'Policies' page in the SailPoint interface. At the top, there is a navigation bar with tabs: Dashboard, Define, Monitor, Analyze, Manage, and System Setup. Below this, the 'Policies' section is visible. On the right side of the 'Policies' section, there is a 'New Policy' button with a dropdown arrow. A red box highlights this dropdown menu, which contains the following options: Role SOD Policy, Entitlement SOD Policy, Activity Policy, Account Policy, Risk Policy, and Advanced Policy. On the left side of the 'Policies' section, there is a search bar with the placeholder text 'Filter by Policy Name' and a magnifying glass icon. Next to the search bar is an 'Advanced Search' button. Below the search bar is a table with three columns: Name, Type, and Description. The table contains three rows of data:

Name ▲	Type	Description
Last Login more than 180 days ago	Advanced	
More than one account	Account	
TRAKK SOD Policy	EntitlementSOD	



# Defining Policy – All Policies

## Advanced Policy

**Name**

**Owner**  ▼

**Policy Violation Owner**

☐ None



☐ Identity  ▼

☒ Manager is Violation Owner

☐ Rule  ...

**Scope**  ▼

**Description**

**B** **I** **U**   **English (United Kingdom)**

7 of 1024 characters (including markup)

**Violation formatting rule**  ...

**Violation business process**  ▼

**State**  ▼

**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

# Defining Policy

## Role SoD Policy

- SoD Policy is composed of one or more SoD business rules
- An SoD business rule is comprised of the following
  - 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
  - Policy specific options
    - Role Conflicts A list of roles which conflict with each other
    - SoD rule definitions provide a framework for policy enforcement  
Example: Cannot have *Approve Vendor* role and *Pay Vendor* role
- Option to run simulation prior to activating (6.3+)

# Defining Policy

## Entitlement SoD Policy

- SoD Policy is composed of one or more SoD business rules
- An SoD business rule is comprised of the following
  - Standard options
  - Policy specific options
    - Entitlement Conflicts      A list of entitlements which conflict with each other
    - Note: Identity Attributes can also be used for conflict analysis
- Option to run simulation prior to activating

# Defining Policy

## Activity Policy

- Activity Policy consisting of one or more activity business rules
  - Example: Login after hours
- An Activity business rule is comprised of the following
  - Standard options
  - Policy specific options
    - Identity Filters                      A filter of identities to apply this rule to
    - Activity Filters                      A list of activities to detect
- Option to run simulation prior to activating (6.3+)

# Defining Policy

## Account Policy

- Account Policy is composed of a **single** pre-defined rule:  
*Does a user have more than one account on any given application*
- Option to run simulation prior to activating (6.3+)

**Note:** To detect a number of accounts (n or more) you would not use this policy, but define an Advanced Policy

# Defining Policy

## Risk Policy

- Risk Policy is composed of a single business rule:  
*Is an identities risk score over the specified threshold*
- Risk Policy is comprised of one policy attribute
  - Composite score threshold
    - Specify the risk value above which violations will be identified

Example:

All identities with risk score > 500 will be given this violation

- Option to run simulation prior to activating (6.3+)





# Defining Policy

## Advanced Policy

- Advanced policy supports definition of your own policy violation type
- Advanced policy is composed of one or more business rules
- An advanced business rule is comprised of the following
  - Standard options
  - Policy specific options
    - Selection Criteria
      - Match List (Identity or Application Attributes)
      - Filter
      - Script
      - Rule
      - Population
- Option to run simulation prior to activating (6.3+)

# 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		<input type="checkbox"/>
Check active policies		<input checked="" type="checkbox"/>
Keep previous violations		<input type="checkbox"/>
A comma separated list of specific policy names. When set this overrides the default policies.		<input type="text"/>
Refresh assigned scope		<input type="checkbox"/>



# Policy Violation – 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 Manage → 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

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

### Policy Violations

Detected	Policy	Policy Violation Owner	Rule
Jan 3, 2014 5:14:50 PM CST	Payroll Analysis and Inventory analysis	Douglas.Flores	<a href="#">Payroll Analysis and Inventory Analysis</a> ^

#### 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

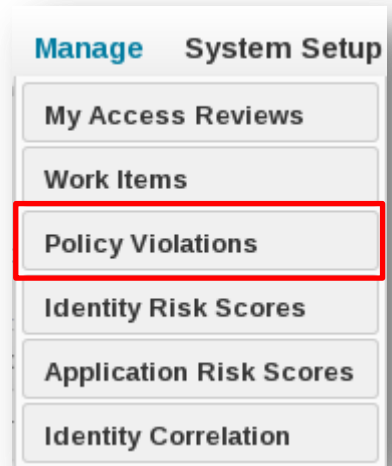
**Rule Description** User has (PayrollAnalysis on ERP\_Global OR Composite\_ERP\_GLOBAL\_Platform) AND InvntryAnalysis on Active\_Directory

**Compensating Control** Acceptable upon manager approval.

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

# Policy Violations – Managing

- **Manage → Policy Violations**
  - Take action on Policy Violations page
  - Dependent upon capability
    - List of all active violations in your enterprise
    - Default user: list of all active violations assigned to the default user



Policy Violations						Select Decision ▼
Filter by Username		Q	Policy Type	▼	Status	▼
<input type="checkbox"/>	User	Policy	Policy Violation C	Rule	Status	Summary
<input type="checkbox"/>	Aaron.Nichols	TRAKK SOD Policy	The Administrator	Cannot be Super and Input at the same time	Open	
<input type="checkbox"/>	Aaron.Nichols	Payroll Analysis and Inve...	Douglas.Flores	Payroll Analysis and Inventory Analysis	Open	User has (PayrollAnalysis
<input type="checkbox"/>	Adam.Ken...	Payroll Analysis and Inve...	Douglas.Flores	Payroll Analysis and Inventory Analysis	Open	User has (PayrollAnalysis
<input type="checkbox"/>	Albert.Woods	Payroll Analysis and Inve...	Douglas.Flores	Payroll Analysis and Inventory Analysis	Open	User has (PayrollAnalysis
<input type="checkbox"/>	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 entitlement(s) that should be revoked to correct this violation.

**Conflicting Entitlements**

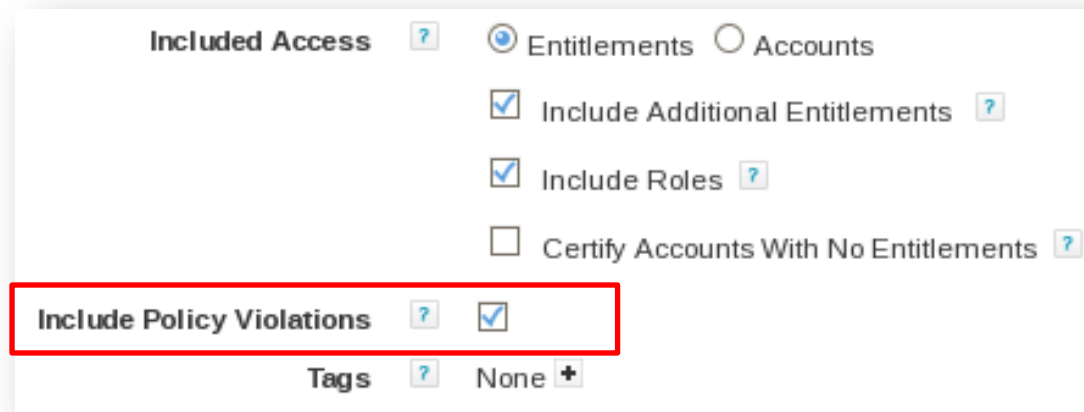
Revoke at least one of the following entitlements

☐ TRAKK capability super ?

☐ TRAKK capability input ?

# Policy Violations – Certifications

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



The screenshot displays a configuration window for access reviews. At the top, there is a section labeled 'Included Access' with a help icon (?). Below this, there are two radio buttons: 'Entitlements' (selected) and 'Accounts'. Under the 'Entitlements' section, there are three checkboxes: 'Include Additional Entitlements' (checked), 'Include Roles' (checked), and 'Certify Accounts With No Entitlements' (unchecked). At the bottom of the configuration area, there is a checkbox labeled 'Include Policy Violations' which is checked and highlighted with a red rectangular border. Below this, there is a 'Tags' section with a help icon (?) and a dropdown menu currently set to 'None' with a plus icon (+).

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

# Policy Violations – Handling in Certification

## Access Review Details

Previous Identity

Decisions

Recent Changes

Approve All Revoke All

Legend: Approve Revoke

### Policy Violations

Decision

Policy



TRAKK SC

Payroll An

Inventory analysis

Douglas Flores

Inventory Analysis

Composite\_ERP\_GLOBA

AND InvntryAnalysis on

Active\_Directory

Page 1 of 1 Show 15 items

Displaying 1 - 2

### Additional Entitlements

Decision

Application

Account Name

Attribute

Entitlements



LDAP

Aaron.Nichols

groups

Managers

### Correct Violation

**Violation:** Cannot be Super and Input at the same time

**Violation Description:**

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 ?

Revoke

Cancel

# Policy Violation – Reporting Options

My Reports

Reports

Scheduled Reports

Report Results

×

🔍

Name

Description

Category: Policy Enforcement Reports (1 Report)

Policy Violation Report

Displays information about all current policy violations in detailed for

Policy Violations

Summary

Certification Totals

Total Policy Violations: 212

Total Distinct Identities: 157

Open Violations: 212

Mitigated Violations: 0

Violation Status by Policy

Policy	Open Violations
Last Login more than 180 days ago	~10
More than one account	~1
Payroll Analysis and Inventory analysis	156
TRAKK SOD Policy	~45

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

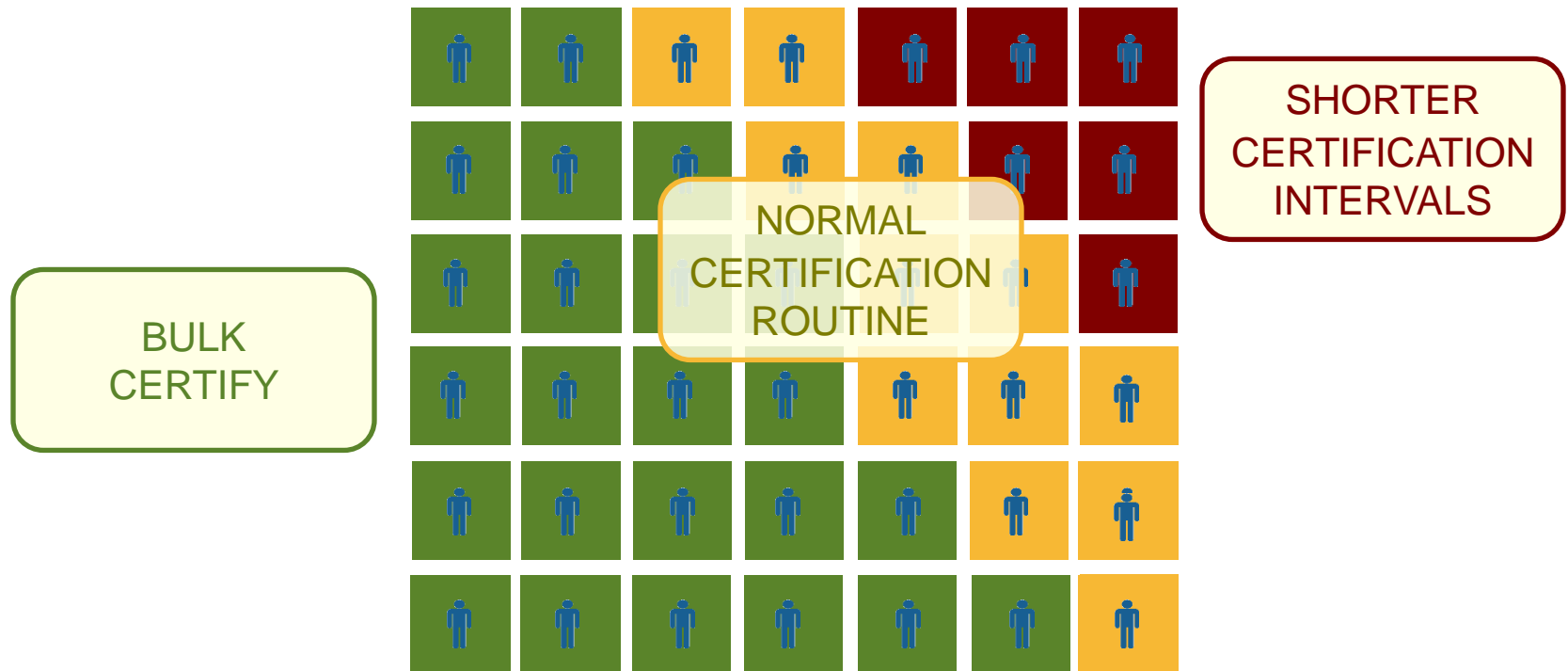
- Read-only privileges
- No changes since review
- No policy violations
- No access to high risk apps
- Risk score <300

## Medium Risk Profile

- Changes or new accounts
- Mitigated policy violations
- Previously approved high-risk application access
- 301 < Risk score < 600

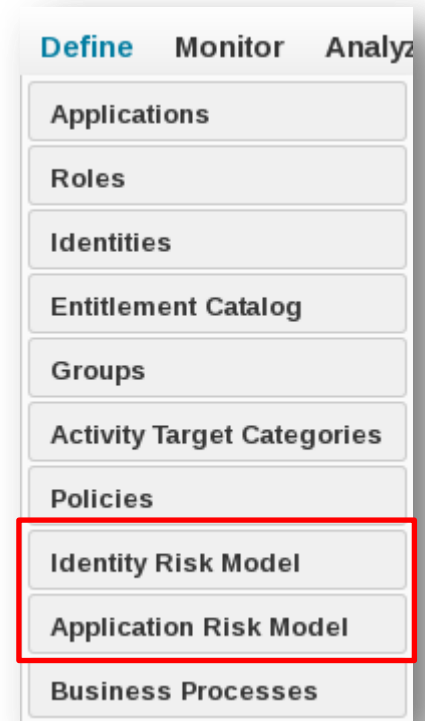
## High Risk Profile

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



# Risk Scoring Configuration

- Risk scoring configuration
  - Defines parameters used by the IdentityIQ risk scoring algorithm to calculate risk scores for identities and applications within an organization
- Risk Model access
  - Define→Identity Risk Model
  - Define→Application Risk Model



# Identity Risk Score Configuration

# Risk Scoring Details

- Identity Risk scoring is based on



Roles/Entitlements



Violations



Certification Age

# Identity Risk – Baseline Risk

- Assign risk value per role, entitlement, policy violation

## Risk Scoring Configuration

The Baseline Access Risk score is a measure of inherent user access risk. A user's Baseline Access Risk score is expressed as a percentage of the total risk score.

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

**Baseline Access Risk**Composite Scoring

### 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 each role.
Entitlement Baseline Access Risk	A user's Entitlement Baseline Access Risk (BAR) score depends on the additional entitlements assigned to the user or more of the following permissions on one or more applications: create, read, update, delete.
Policy Violation Baseline Access Risk	A user's Policy Baseline Access Risk (BAR) score is based on policy violations that are detected for the user. The score is calculated by taking the sum of the risks associated with every policy or rule that is violated.

## Baseline Risk Configuration

## Configure Risk score per Role, Entitlement and Policy Violation



# Identity Risk – Composite Scoring

- Determine overall scoring weights per category

Baseline Access Risk

Composite Scoring

### Composite Scoring

Category	Percentage Contribution
Role Compensated Score	<div><div></div><div></div></div> 25 %
Entitlement Compensated Score	<div><div></div><div></div></div> 25 %
Policy Violation Compensated Score	<div><div></div><div></div></div> 25 %
Certification Age	<div><div></div><div></div></div> 25 %

Composite Scoring Configuration

Configure Overall Percentage Contribution from Each Risk Component

# Identity Risk – Composite Scoring

## Compensated Score

Baseline Access Risk

Composite Scoring

For each Composite Scoring category...

### Composite Scoring

Category

Role Compensated Score

Entitlement Compensated Score

Policy Violation Compensated Score

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



# Application Risk Scoring

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





The screenshot shows the 'Application Risk Scoring Configuration' page in the SailPoint interface. The navigation bar at the top includes 'Dashboard', 'Define', 'Monitor', 'Analyze', 'Manage', and 'System Settings'. The 'Define' tab is active. The page title is 'Application Risk Scoring Configuration'. Below the title, there are two tabs: 'Component Scores' and 'Composite Score'. The 'Component Scores' tab is selected. Under this tab, there is a section titled 'Service Account'. It contains four configuration items: 'Disabled' with a checkbox, 'Attribute Name' with a text input field containing 'service', 'Attribute Value' with a text input field containing 'true', and 'Sensitivity' with a text input field containing '5'. Each item has a small question mark icon next to its label.

# Calculating Risk Scores

## ■ Identity Risk Scoring

### ■ Tasks

- Refresh Risk Scores
- Any Identity Refresh Task with “Refresh the Identity risk scorecards” checked

Synchronize attributes		<input type="checkbox"/>
Refresh the identity risk scorecards		<input checked="" type="checkbox"/>
Maintain identity histories		<input type="checkbox"/>
Refresh the group scorecards		<input type="checkbox"/>

## ■ Application Risk Scoring

- Task: Refresh Application Scores
- Always update identity scores first – application scores are dependent on the identity risk scores

# Where to Monitor Risk Scores

- Identity Risk tab (breakdown of score calculation)

## View Identity Aaron.Nichols

Attributes	Entitlements	Application Accounts	Policy	History	Risk	Activity	User Rights	Events
Scorecard					Risk Score 838 <span></span>			
Score Category			Base Score		Compensated Score			
Role Compensated Score			<span></span> 0		<span></span> 0			
Entitlement Compensated Score			<span></span> 754		<span></span> 754			
Policy Violation Compensated Score			<span></span> 600		<span></span> 600			
Certification Age			<span></span> 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 (breakdown of score calculation)

Attributes

Schema

Correlation

Accounts

Risk

Activity Data Sources

Rules

Provisioning Policies

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%
violationAccount	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

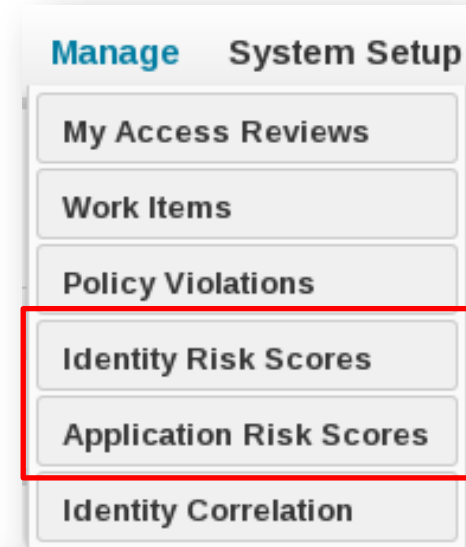
## ■ Manage Tab

### ■ Identity Risk Scores

- Sort scores by risk score
- See scores by risk band (low/med/high)
- Perform Certifications
- See Score Breakdown

### ■ Application Risk Scores

- Sort application risk scores



<div><div><div>● Low</div><div>● Medium</div><div>● High</div></div></div>								
35/235 Identities (15%)								
<input type="checkbox"/>	Name	First Name	Last Name	Composite Score	Role	Entitlement	Policy	Certification
<input type="checkbox"/>	Aaron.Nichols	Aaron	Nichols	● 838	● 0	● 754	● 600	● 1000
<input type="checkbox"/>	Amanda.Ross	Amanda	Ross	● 838	● 0	● 752	● 600	● 1000
<input type="checkbox"/>	Andrea.Hudson	Andrea	Hudson	● 838	● 0	● 752	● 600	● 1000
<input type="checkbox"/>	Barbara.Wilson	Barbara	Wilson	● 838	● 0	● 752	● 600	● 1000

# Lifecycle Manager and Risk

- Preview risk values when requesting access





Request Access for [Amanda.Ross](#) ?

**Keyword Search** | [User-based Search](#)

trakk Search

**Roles (0)** **Entitlements (4)** **Current Access**

Narrow Results Page 1 of 1 Displaying 1 - 4 of 4

 <b>input</b> <ul style="list-style-type: none"><li>Application: TRAKK</li><li>Owner:</li></ul>	<ul style="list-style-type: none"><li>Attribute: capability</li><li>Risk: ● 1</li></ul>	<span>Add To Cart</span>
 <b>reject</b> <ul style="list-style-type: none"><li>Application: TRAKK</li><li>Owner:</li></ul>	<ul style="list-style-type: none"><li>Attribute: capability</li><li>Risk: ● 1</li></ul>	<span>Add To Cart</span>
 <b>approve</b> <ul style="list-style-type: none"><li>Application: TRAKK</li><li>Owner:</li></ul>	<ul style="list-style-type: none"><li>Attribute: capability</li><li>Risk: ● 200</li></ul>	<span>Add To Cart</span>
 <b>super</b> <ul style="list-style-type: none"><li>Application: TRAKK</li><li>Owner:</li></ul>	<ul style="list-style-type: none"><li>Attribute: capability</li><li>Risk: ● 550</li></ul>	<span>Add To Cart</span>

# Advanced Analytics and Risk

- 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 ▼

# Risk Scoring – Reporting

- Report on risky identities, applications, or accounts


## Reports

My Reports

Reports

Scheduled Reports

Report Results



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.

# 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

# Risk – Process

- Process
  - Define parameters for risk scoring
  - Refresh identities or applications to update risk scores
  - Risk scores
    - Displayed on identity cubes
    - Displayed when requesting access
    - Available to business processes

