

# Access Certification

---

Fundamentals of IdentityIQ  
Implementation

IdentityIQ 7.0

# Overview

## Access Certification

- What are Certifications and Access Reviews
- Types of Certifications
- Certification Lifecycle
- Certification Configuration
- Making Certification Decisions
- Certification Completion
- Targeted Identity and Event Based Certifications
- Monitoring Certifications

# Access Certification

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

# 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**

- Provide a snapshot of the 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)

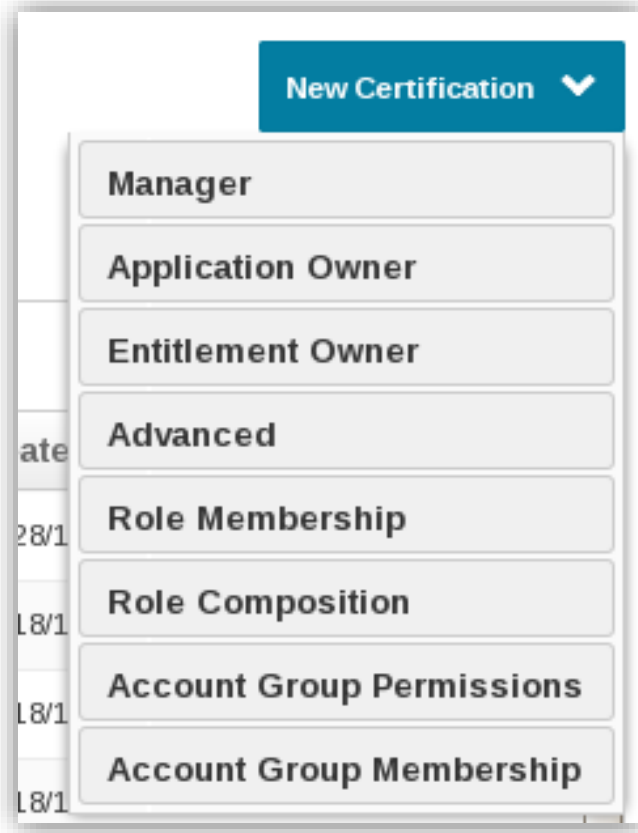
### Access Review Details

OK	⊖	Cynthia.Cook
OK	⊖	Jessica.Sanchez
OK	⊖	Jose.Reed
OK	⊖	Shirley.Rogers
OK	⊖	Timothy.Morris

# Certification Types

## Certification Campaigns

- Setup → Certifications



## Targeted Certifications

- Identity Certifications
  - Identities selected from
    - Identity Search Results
    - Identity Risk Score
    - Policy Violation
- Event-Based Certifications

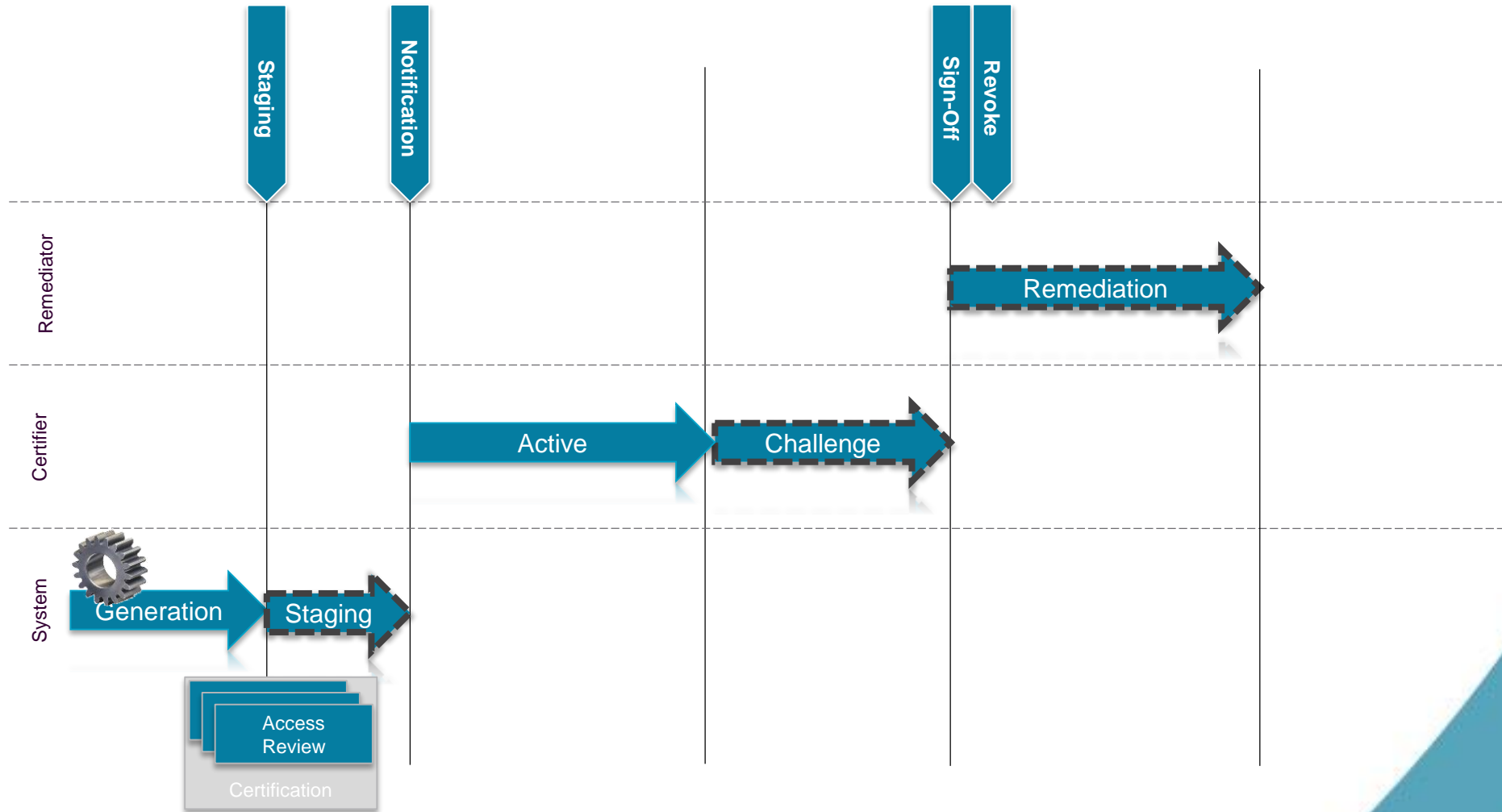
# Overall Certification Process

- Compliance or business analyst defines certification parameters
- IdentityIQ collects data
  - Formats the information into interactive access reviews
  - Routes access reviews to the appropriate reviewers
- Reviewers receive Access Reviews
  - Approve/Revoke access
  - Signs off on completed access review
- IdentityIQ takes action on revoked access
  - Directly revokes access
  - OR
  - Initiates work item

# Certification Schedules

Schedule Type	Description
One Time	<ul style="list-style-type: none"><li>• Runs a single unscheduled certification</li><li>• Great for testing/development or full control over schedules</li></ul>
Scheduled (Weekly, Monthly, Quarterly, Annually)	<ul style="list-style-type: none"><li>• Runs on a repeatable schedule</li><li>• Great for production situations whereby certifications must happen at regular intervals</li></ul>
Continuous	<ul style="list-style-type: none"><li>• Certification never ends</li><li>• Individual items are certified based on individual certification schedules (i.e. each entitlement is certified monthly, independently of other items.)</li></ul>

# Certification Time Periods





# Certification Configuration

# Certification Configuration

## Overview

- Select type of certification
  - What to certify
- Configure parameters unique to certification type
  - Certification contents
- Configure parameters standard to all certifications
  - Schedule, Lifecycle, Notifications, Behavior, etc.
- Configure rules for business specific behavior
- Consider global configurations

# What to Certify

## Who certifies what?

Type	Certifier	Certifies
Manager	Manager	Direct reports
Application Owner	Application Owner	Identities accessing the application(s)
Entitlement Owner	Entitlement Owner	Identities accessing the application(s) (by entitlement)
Advanced	Selected per cert	Population or group
Role Membership	Manager*	Identities who have role
Account Group Membership	Account Group Owner*	Identities who have account group
Role Composition	Role Owner*	Access encapsulated in role
Account Group Composition	Account Group Owner*	Access encapsulated in account group

# Certification Contents

## Manager, Application Owner, Entitlement Owner, Advanced

	Manager	Application Owner	Entitlement Owner	Advanced
Which applications/all applications	✓	✓	✓	✓
Certify Entitlements	✓	✓	✓	✓
Certify Accounts	✓	✓		✓
Include Roles	✓	✓		✓
Include entitlements not encapsulated in roles (Additional Entitlements)	✓	✓		✓
Include policy violations	✓	✓		✓

# Certification Contents

## Advanced Certification

**Populations to Certify** ?

<input type="checkbox"/>	Population	Certifier(s)
<input type="checkbox"/>	Active Managers - Asia Pacific	ERP Global App Owners - +

-- Select Population --

**Group Factories to Certify** ?

<input type="checkbox"/>	Group Factory	Certifier Rule
--------------------------	---------------	----------------

-- Select Group Factory --

**Reminder:** Populations and Groups are used to filter identities to be included in an action (i.e. to be certified)

- Population: Set of users defined by a saved search query
- Group: Set of users defined by a single “group factory” attribute

# Certification Configuration

## Schedule and Behavior

- Schedule
  - Run Once, Scheduled or Continuous
- Duration and types of Phases
  - Staging Period
  - Active Period
  - Challenge Period
  - Revocation Period
  - Automatic Closing (Rule, Revoke, Allow, Exception)
- Email notification parameters
  - Certification Reminders and Escalation
  - Revocation Reminders and Escalation
- Advanced
  - Exclusion, Pre-Delegation, Sign-Off Approver Rules

# Certification Configuration

## Rules (Supplied by Implementation Team)

- 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
- Certification Control
  - Exclusion Rule
  - Pre-Delegation Rule
  - Sign Off Approver Rule

# Certification Configuration

## Global Configuration

- Set default configurations
  - Gear → Compliance Manager
  - Configure Global Settings that apply to all certifications
    - Presentation
    - Lifecycle
    - Behavior
    - Decisions
    - Bulk Actions
    - Certification Contents
    - Email Templates
  - Can be overridden on per-certification basis



# Targeted Identity Certifications

## Configuration

- Identity Based

- From Advanced Analytics
  - Select from query result to define who to certify
- From policy violation work item
  - Policy violator is certified
- From Identity Risk Scores (if risk configured)
  - Select from set of users based on risk score

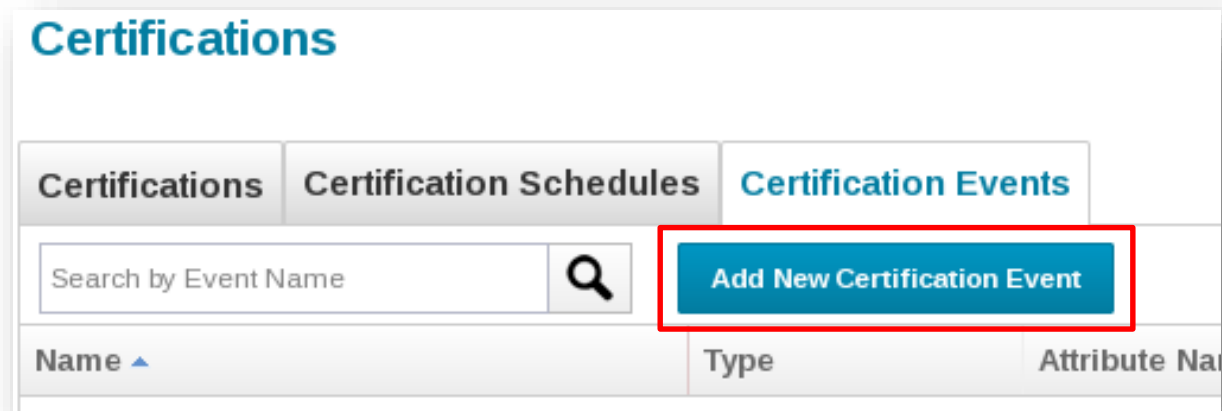
- Data Based

- Based on defined data change events
  - Change in identity data defines who to certify

# Targeted Identity Certifications

## Certification Events

- Data change events
  - New employee
  - Manager change
  - Department change
  - Based on rule evaluation
- Configuration
  - Setup → Certification → Certification Events
    - New Certification Event



The screenshot displays the 'Certifications' management interface. At the top, there are three tabs: 'Certifications', 'Certification Schedules', and 'Certification Events'. The 'Certification Events' tab is currently selected. Below the tabs, there is a search bar labeled 'Search by Event Name' with a magnifying glass icon. To the right of the search bar, a blue button labeled 'Add New Certification Event' is highlighted with a red rectangular border. Below the search bar and button, there is a table with columns labeled 'Name', 'Type', and 'Attribute Na'.

# Targeted Identity Certifications

## Configuring Certification Events

- Configure certification to run when event occurs

### Certification Event

#### Summary

##### Steps

1. **Basic**
2. Lifecycle
3. Notifications
4. Behavior
5. Advanced

Specify options about what to certify, when the certification should be created, and who is responsible for certification.

#### Basic

##### Event Options

Name

Description

Event type

Disabled

Included Identities

Create

Create  
Manager Transfer  
Attribute Change  
Rule  
Native Change

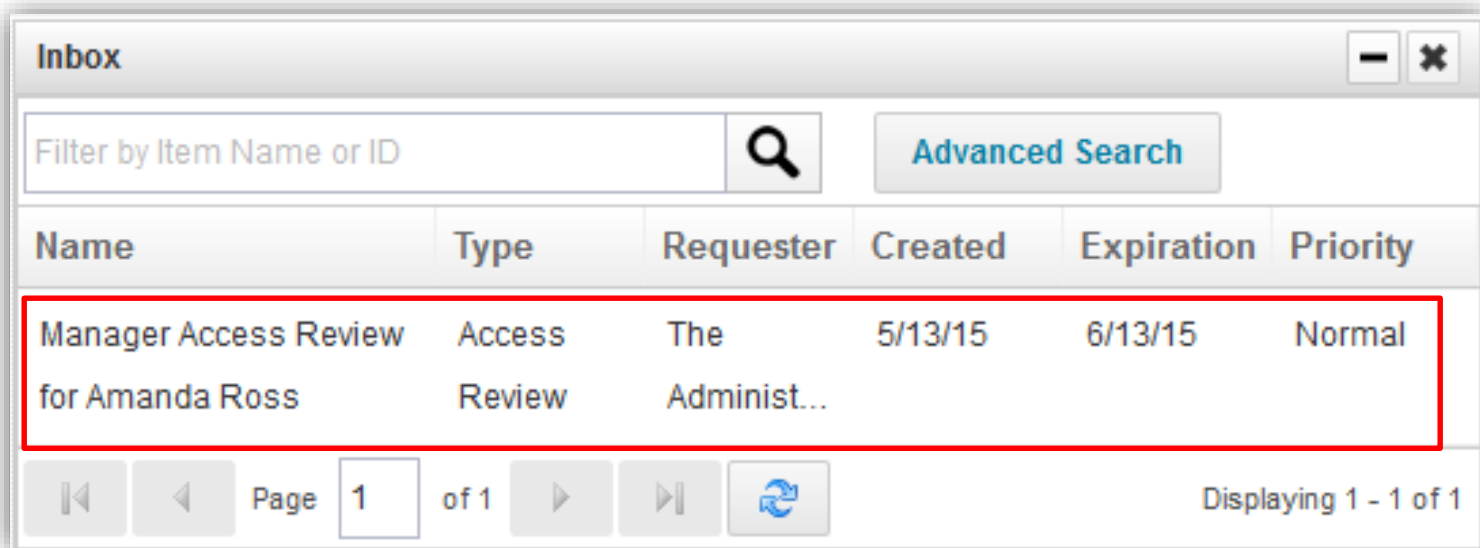
Configure certification options as usual

Define event type that will invoke a certification

# Certification Completion

# Managing Access Reviews

- Inbox or My Work → My Access Reviews



Name	Type	Requester	Created	Expiration	Priority
Manager Access Review for Amanda Ross	Access Review	The Administ...	5/13/15	6/13/15	Normal

# Managing Access Reviews

- Click on Access Review Work Item
- View – Worksheet or Identity
- Make Decisions and Sign Off

Legend: Approve Revoke Allow Exception Action Required

<input type="checkbox"/>	Decision	Identity	First Name	Last Name	Description
<input type="checkbox"/>		Denise.H...	Denise	Hunt	TRAKK - Basic
<input type="checkbox"/>		Denise.H...	Denise	Hunt	Region.Europe
<input type="checkbox"/>		Denise.H...	Denise	Hunt	Value Treasury on groupmbr
<input type="checkbox"/>		Denise.H...	Denise	Hunt	Value TR-Hedge on groupmbr
<input type="checkbox"/>		Denise.H...	Denise	Hunt	Payroll Analysis and Inventory Analysis
<input type="checkbox"/>		Irene.Mills	Irene	Mills	TRAKK - Basic
<input type="checkbox"/>		Irene.Mills	Irene	Mills	Region.Europe
<input type="checkbox"/>		Irene.Mills	Irene	Mills	Value Treasury on groupmbr
<input type="checkbox"/>		Irene.Mills	Irene	Mills	Value TR-Hedge on groupmbr

# Access Reviews

## Certifier Decisions

Decision	Action	Result
Approve	Approve item	No action taken
Revoke	Remove entitlement/role from user	Remediations will be sent out to remove access from user
Allow Exception	Allow user to keep entitlement/role for period of time	No action taken; will mark item as an exception until time period expires

- Decisions can be made per entitlement per identity or account group or in bulk on many items at once
  - Bulk decisions not advised by auditors
  - Can be disabled per certification or globally

# Access Reviews

## Sharing Decision Making Responsibility

Delegate	Reassign	Forward
Unique to access reviews	Unique to access reviews	Applies to all work items
Delegate whole entity or single line item	Reassign whole entity, single line item, or bulk	Entire access review sent to new owner
<i>Workitem</i> is sent to the delegate(s)	<i>New child access review</i> created and assigned to new owner(s)	Retains previously made decisions, reassigns or delegations
Can be recalled	Can be recalled	No option to recall
Access review owner retains responsibility for all decisions	Child access review owner assumes responsibility for decisions	Passes all responsibility to the new owner



# Access Certification – Certification End Users

- Certification ends
  - When challenge period is over (if enabled)
  - Sign off occurs
- Sign off is performed by the access review owner when
  - All certified entities (Identity, Account Group, Roles) reach completed state
  - All subordinate access review are completed
    - Subordinate access reviews are manager/subordinate manager access reviews or reassigned or delegated access reviews
  - Electronic signature can optionally be enabled

# Access Certification – Certification End

## Electronic Signatures (6.1)

The screenshot shows the 'Access Review Details' page for Catherine Simmons. A modal titled 'Electronic Signature Required' is open, displaying a notice and a sign-off form.

**Access Review Details**

Manager Access Review for Catherine Simmons

Due on	2/12/14 (31 Days remaining)	Current Phase
Owner	Catherine Simmons	Percent Complete

**Electronic Signature Required**

\*\*\*\*Attention\*\*\*\*  
BEFORE SIGNING, READ THE FOLLOWING NOTICE CAREFULLY  
\*\*\*\*Attention\*\*\*\*

By signing this document electronically you are verifying that all the decisions, statements, and comments provided are accurate to the best of your knowledge. You further attest that you were not the subject of any pressure, either professional or personal, to alter your actions from the best practices established by your position at The Demo Company. Your electronically signed actions may be used as evidence including but not limited to: court cases, court supervised mediation, third party mediation, firing proceedings, quarterly audits, yearly audits, extraordinary review from third party observers including private and government entities, stock holder assessments, job performance reviews, costume parties, internal audits, and operation evaluations.

*A copy of this statement is available in the HR handbook.*

Username:

Password:

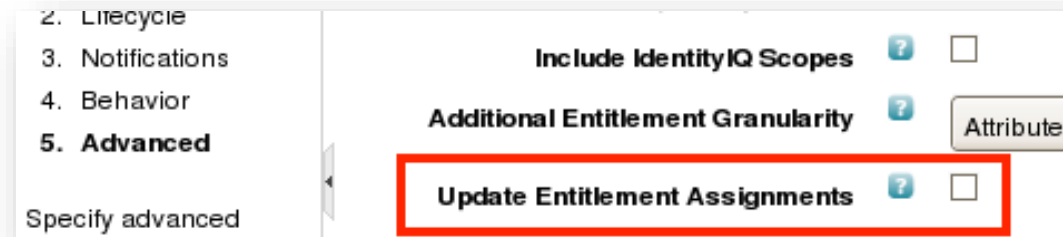
**Sign** **Cancel**

- Available for
  - Certification Sign-off
  - Access Sign-off
  - Report Sign-off
- Process
  - Reauthenticate
  - Formal meaning assigned
  - Make objects immutable

# Access Certification – Certification End

## PerformMaintenance Task

- PerformMaintenance task runs periodically
  - Checks for certification completion and sign-off
  - On sign-off, launches RemediationManager to process revokes
    - Direct updates, tickets in service desk system, IdentityIQ WorkItem
- Certification Decisions
  - Are factored into risk score
  - Entitlement assignment may be updated based on configuration



# Certification Monitoring

# Certifications – Monitoring Progress

- Setup → Certifications
- Oversee progress as certification progresses
- Can modify in-flight certification

## Manager Certification [1/30/14 5:22:25 PM CST]

Owner The Administrator

Create Date 1/30/14 5:22:25 PM CST

Exclusions 0

[\[View/Edit Certification Options\]](#)

Access Reviews Completed

0/48 (0%)

Identities Completed

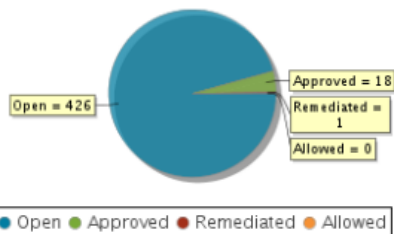
10/228 (4%)

Items Completed

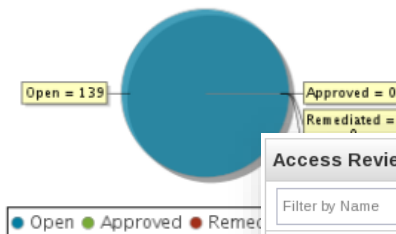
25/788 (3%)

### Decision Statistics

#### Roles



#### Additional Entitlements



#### Policy Violations



### Access Reviews

Filter by Name



[Advanced Search](#)

Description	Percent Complete	Phase	Phase End	Tags	Certifiers
Manager Access Review for James Smith	0% (0 of 25)	Active	2/28/14 5:22 PM		James.Smith
Manager Access Review for John Williams	15% (3 of 20)	Active	2/28/14 5:22 PM		John.Williams
Manager Access Review for David Anderson	0% (0 of 11)	Active	2/28/14 5:22 PM		David.Anderson
Manager Access Review for Elizabeth Taylor	0% (0 of 16)	Active	2/28/14 5:22 PM		Elizabeth.Taylor
Manager Access Review for Jennifer Thomas	0% (0 of 11)	Active	2/28/14 5:22 PM		Jennifer.Thomas
Manager Access Review for William Moore	0% (0 of 11)	Active	2/28/14 5:22 PM		William.Moore
Manager Access Review for Mary Johnson	0% (0 of 20)	Active	2/28/14 5:22 PM		Mary.Johnson

# Certifications – Analytics

- Intelligence → Advanced Analytics → Access Review Search
- Search for access reviews based on criteria

## Advanced Analytics

Identity Search

Access Review Search

Role Search

Account Group Search

Activity Search

Au

Search Criteria ?

Access Review Attributes

Name	<input type="text"/>	
Certifier	<input type="text"/>	▼
Identity	<input type="text"/>	▼
Type	Application Owner	▼
Phase	Challenge	▼

Tags

▼

# Certifications – Reporting

## Reports

My Reports

Reports

Scheduled Reports

Report Results

Name
<div><div></div>Category: Access Review and Certification Reports (11 Reports)</div>
Access Review Decision Report
Access Review Signoff Live Report
Account Group Membership Access Review Live Report
Account Group Permissions Access Review Live Report
Advanced Access Review Live Report
Application Owner Access Review Live Report
Certification Activity by Application Live Report
Entitlement Owner Access Review Live Report
Manager Access Review Live Report
Role Composition Access Review Live Report
Role Membership Access Review Live Report

# Questions?

---



# Exercise Preview

## Section 2, Exercises 6, 7, 8

- Continue to identify and correct issues with user's access
  - Exercise 6: Certification of PAM Application and Account Groups
  - Exercise 7: Manager Certification with Rules
  - Exercise 8: Certification by Populations and Groups