Access Certification

Fundamentals of IdentityIQ Implementation

IdentityIQ 7.0

SailPoint

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

SailPoint Copyright © SailPoint Technologies, Inc. 2016 All rights reserved.

Access Certification

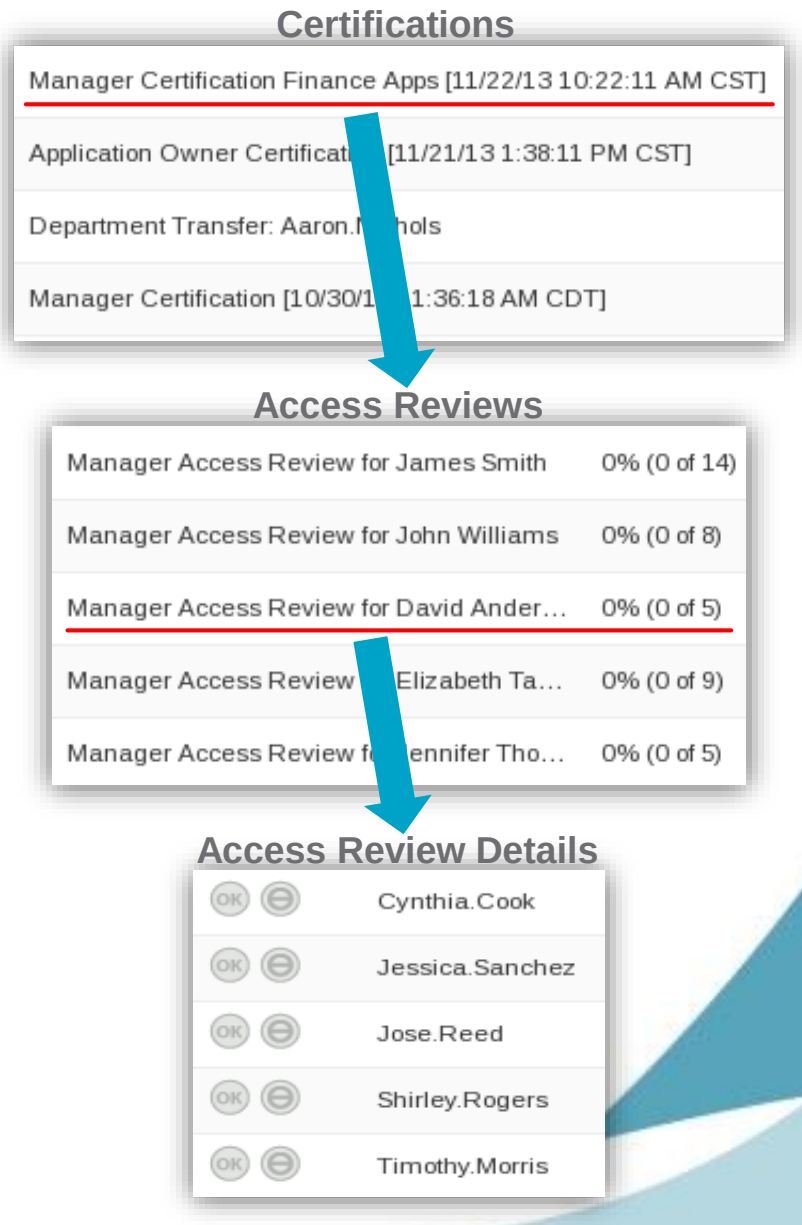
- The process of automating the periodic review and approval of:
  - Identity Access
  - Role Membership
  - Role Composition
  - Account Group Membership
  - Account Group Permissions

SailPoint Copyright © SailPoint Technologies, Inc. 2016 All rights reserved.

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

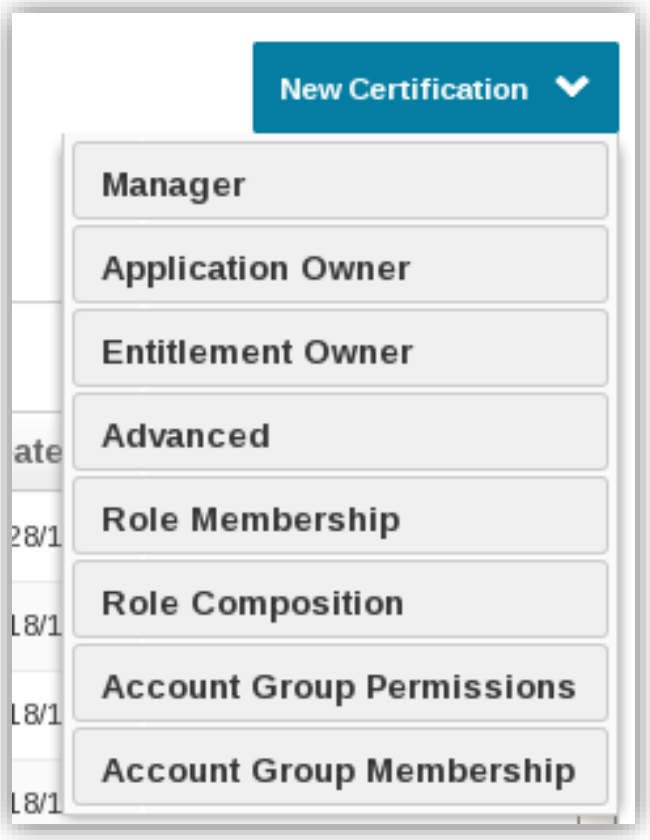


SailPoint Copyright © SailPoint Technologies, Inc. 2016 All rights reserved.

Certification Types

Certification Campaigns

- Setup → Certifications



Targeted Certifications

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

SailPoint Copyright © SailPoint Technologies, Inc. 2016 All rights reserved.

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

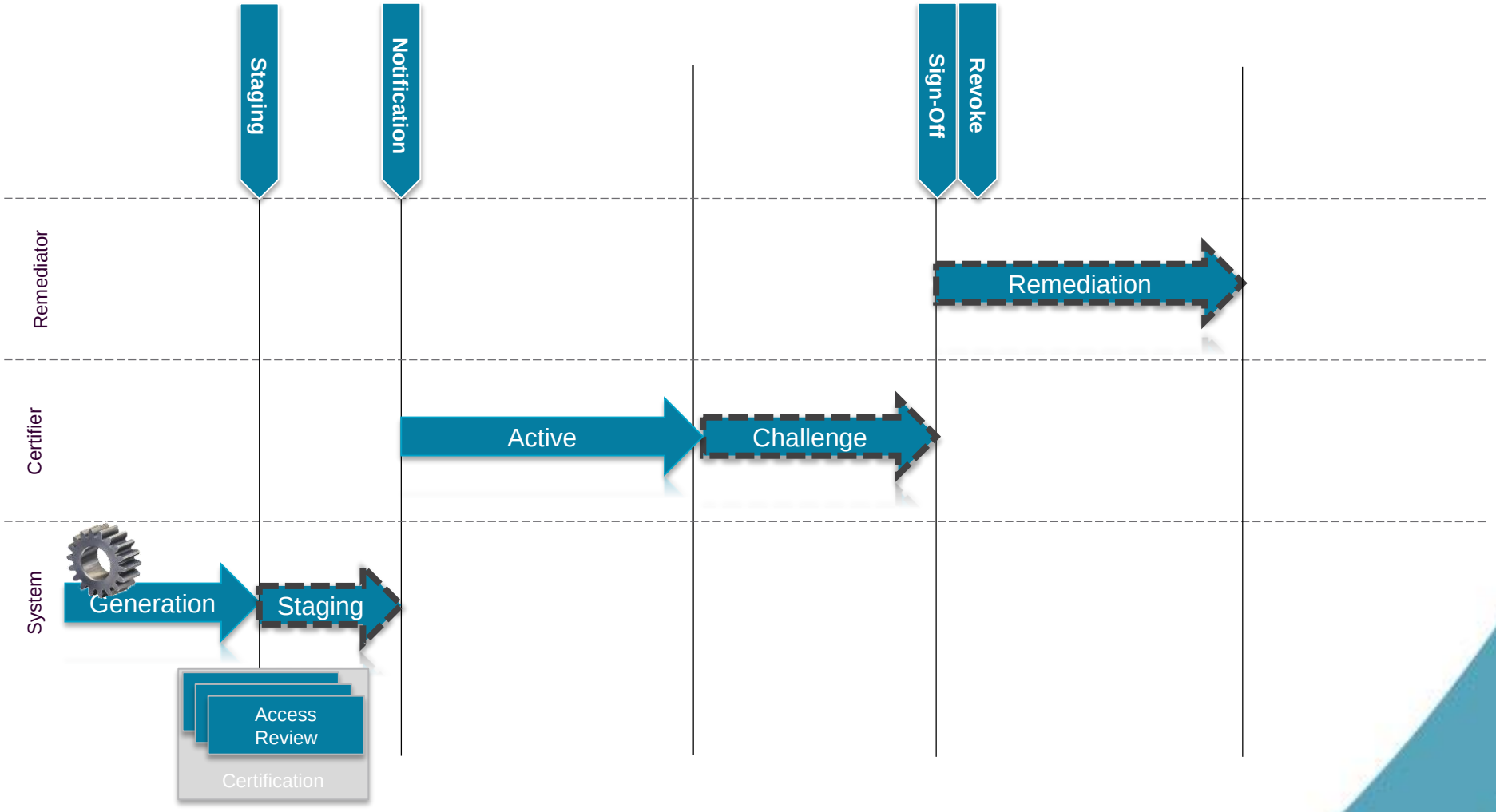
SailPoint Copyright © SailPoint Technologies, Inc. 2016 All rights reserved.

Certification Schedules

Schedule Type	Description
One Time	• Runs a single unscheduled certification • Great for testing/development or full control over schedules
Scheduled (Weekly, Monthly, Quarterly, Annually)	• Runs on a repeatable schedule • Great for production situations whereby certifications must happen at regular intervals
Continuous	• Certification never ends • Individual items are certified based on individual certification schedules (i.e. each entitlement is certified monthly, independently of other items.)

SailPoint Copyright © SailPoint Technologies, Inc. 2016 All rights reserved.

Certification Time Periods



SailPoint Copyright © SailPoint Technologies, Inc. 2016 All rights reserved.

Certification Configuration

SailPoint

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

SailPoint Copyright © SailPoint Technologies, Inc. 2016 All rights reserved.

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

SailPoint Copyright © SailPoint Technologies, Inc. 2016 All rights reserved.

*or selected reviewer

Certification Contents

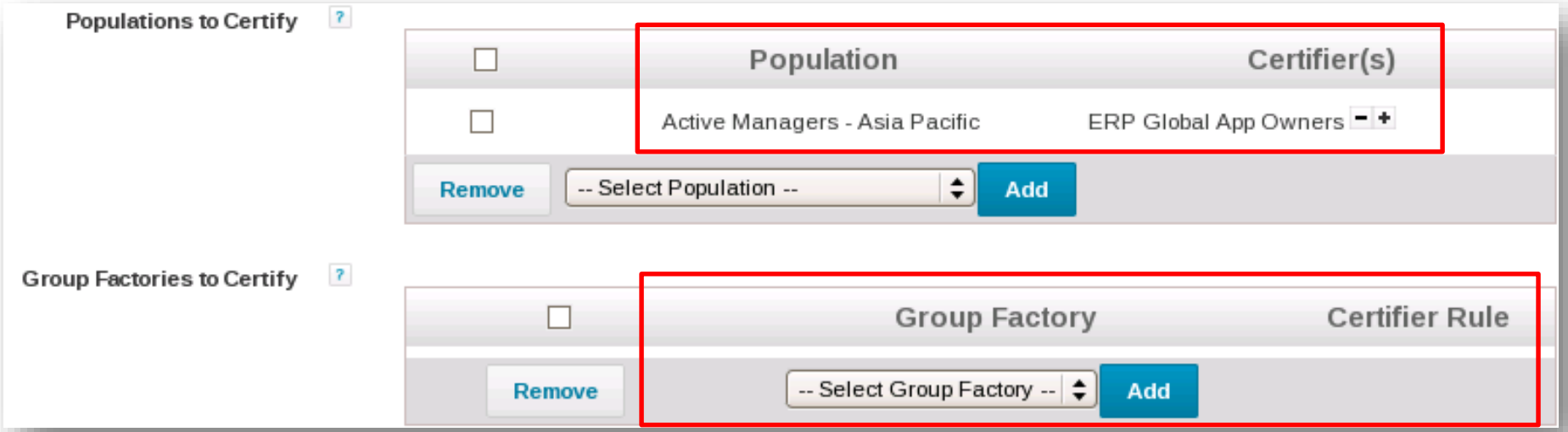
Manager, Application Owner, Entitlement Owner, Advanced

	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	✓	✓		✓

SailPoint Copyright © SailPoint Technologies, Inc. 2016 All rights reserved.

Certification Contents

Advanced Certification



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

SailPoint Copyright © SailPoint Technologies, Inc. 2016 All rights reserved.

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

SailPoint Copyright © SailPoint Technologies, Inc. 2016 All rights reserved.

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

SailPoint Copyright © SailPoint Technologies, Inc. 2016 All rights reserved.

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

SailPoint Copyright © SailPoint Technologies, Inc. 2016 All rights reserved.

Targeted Identity Certifications

Configuration

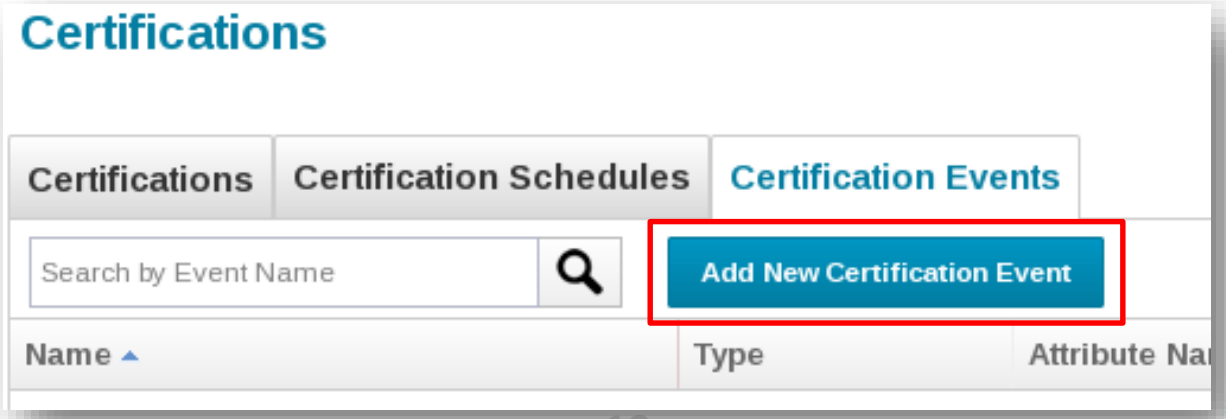
- Identity Based
  - From Advanced Analytics
    - Select from query result to define who to certify
  - From policy violation work item
    - Policy violator is certified
  - From Identity Risk Scores (if risk configured)
    - Select from set of users based on risk score
- Data Based
  - Based on defined data change events
    - Change in identity data defines who to certify

SailPoint Copyright © SailPoint Technologies, Inc. 2016 All rights reserved.

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

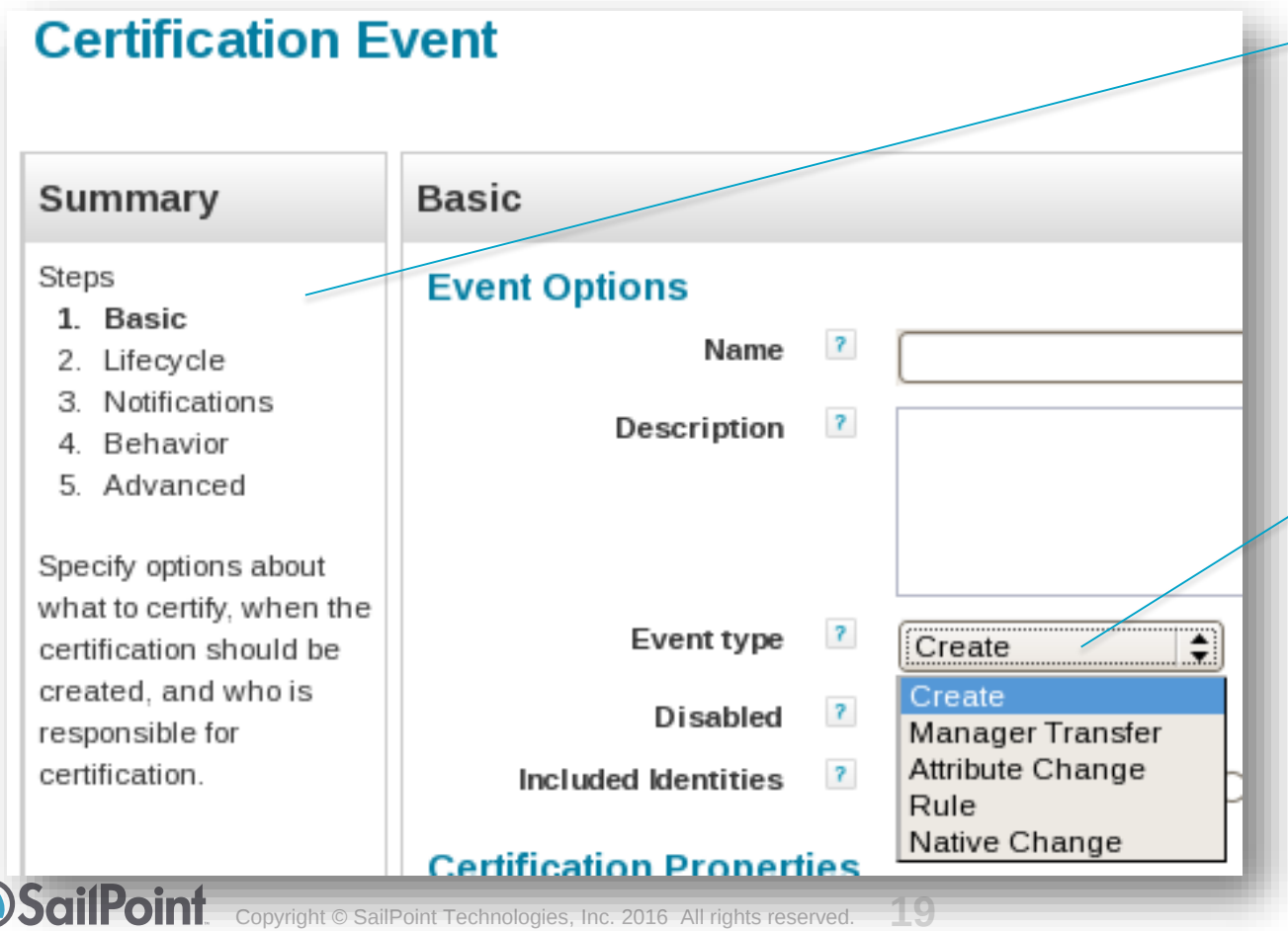


SailPoint
Copyright © SailPoint Technologies, Inc. 2016 All rights reserved.

Targeted Identity Certifications

Configuring Certification Events

- Configure certification to run when event occurs



Configure certification options as usual

Define event type that will invoke a certification

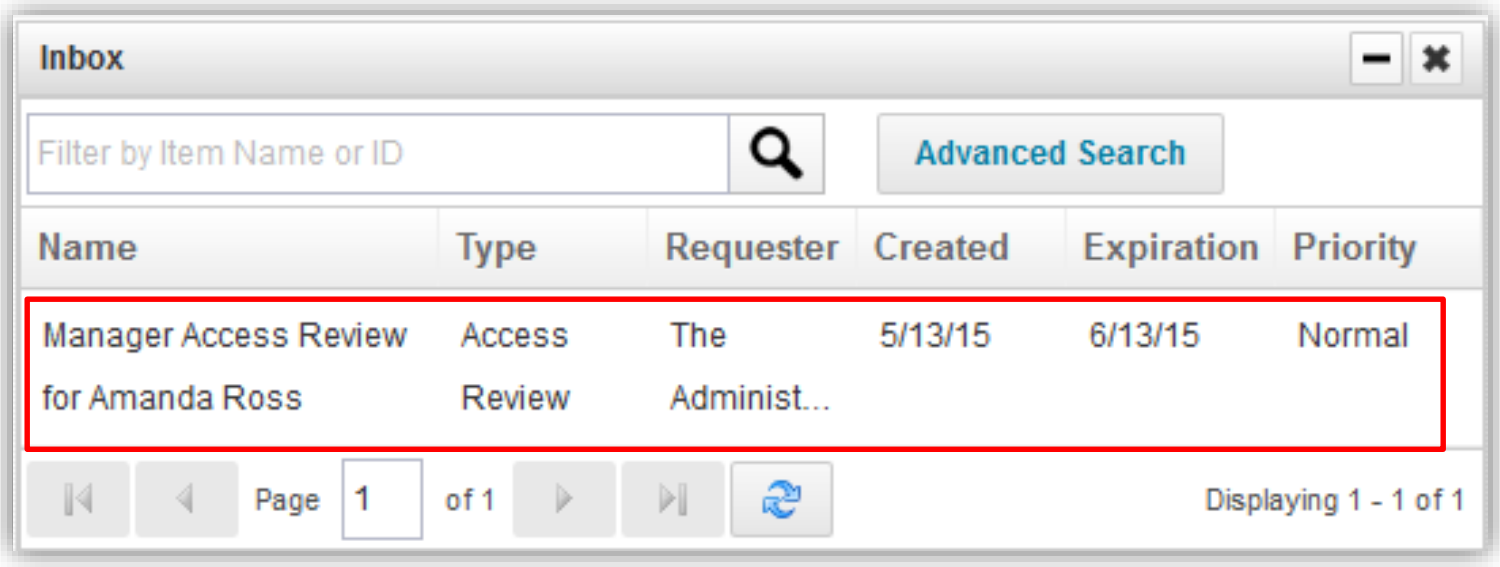
SailPoint Copyright © SailPoint Technologies, Inc. 2016 All rights reserved.

Certification Completion

SailPoint

Managing Access Reviews

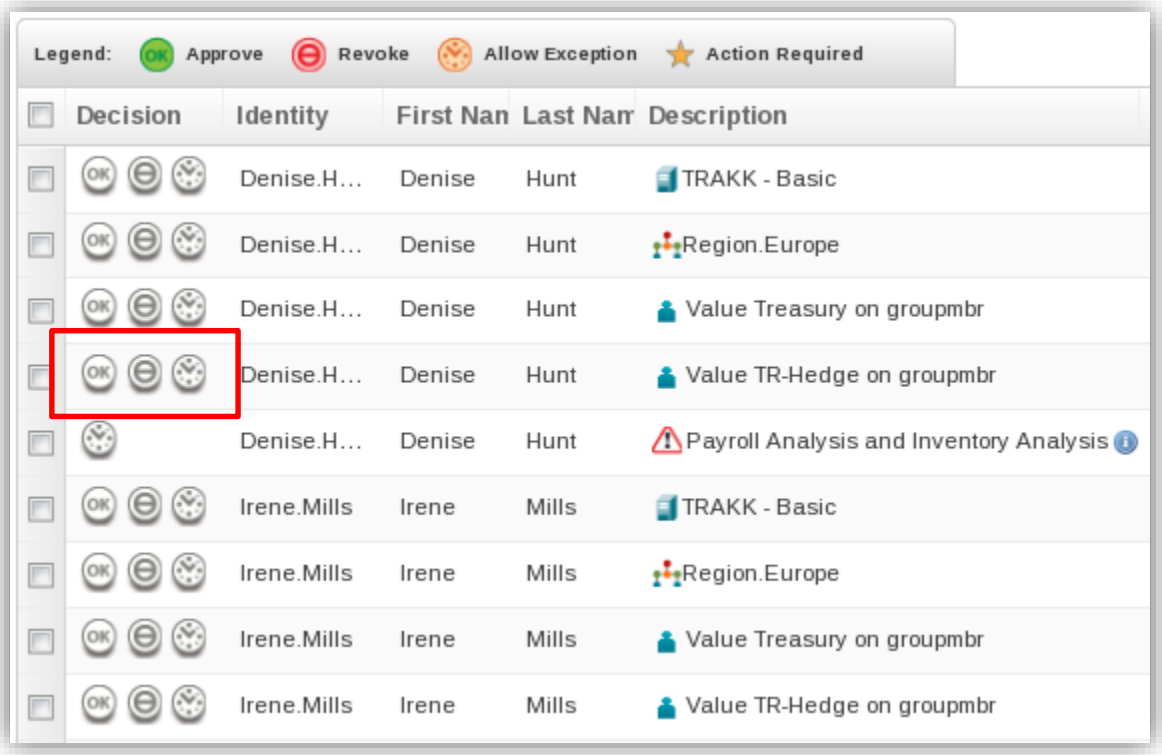
- Inbox or My Work → My Access Reviews



SailPoint Copyright © SailPoint Technologies, Inc. 2016 All rights reserved.

Managing Access Reviews

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



SailPoint
Copyright © SailPoint Technologies, Inc. 2016 All rights reserved.

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

SailPoint Copyright © SailPoint Technologies, Inc. 2016 All rights reserved.

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
Workitem is sent to the delegate(s)	*New child access review* 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

SailPoint Copyright © SailPoint Technologies, Inc. 2016 All rights reserved.

Access Certification – Certification End

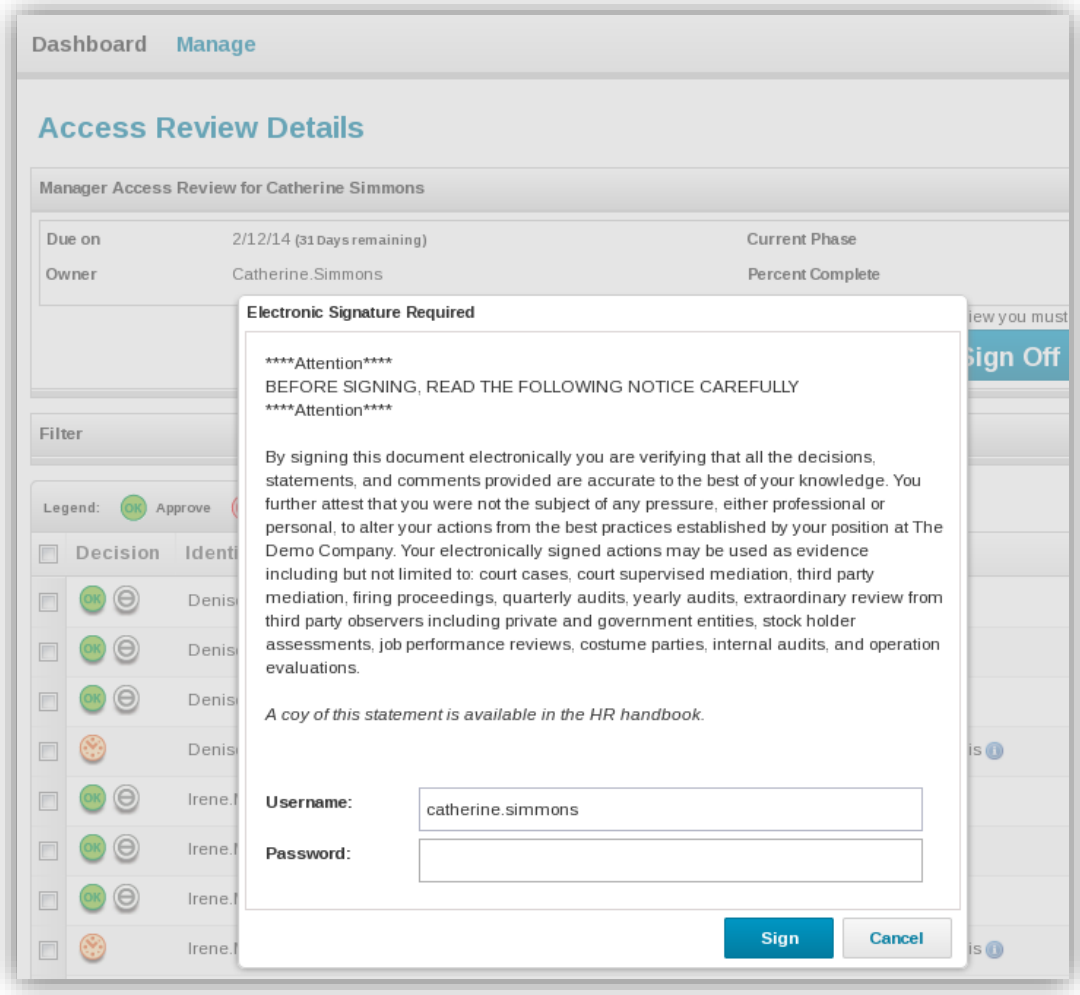
Users

- 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

SailPoint Copyright © SailPoint Technologies, Inc. 2016 All rights reserved.

Access Certification – Certification End

Electronic Signatures (6.1)



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

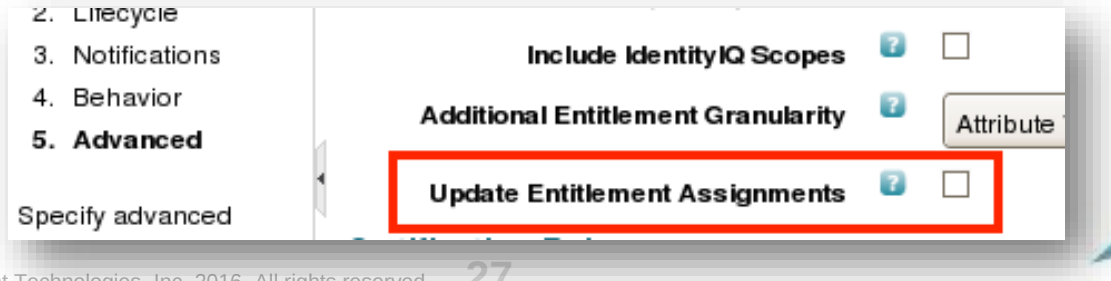
SailPoint Copyright © SailPoint Technologies, Inc. 2016 All rights reserved.

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



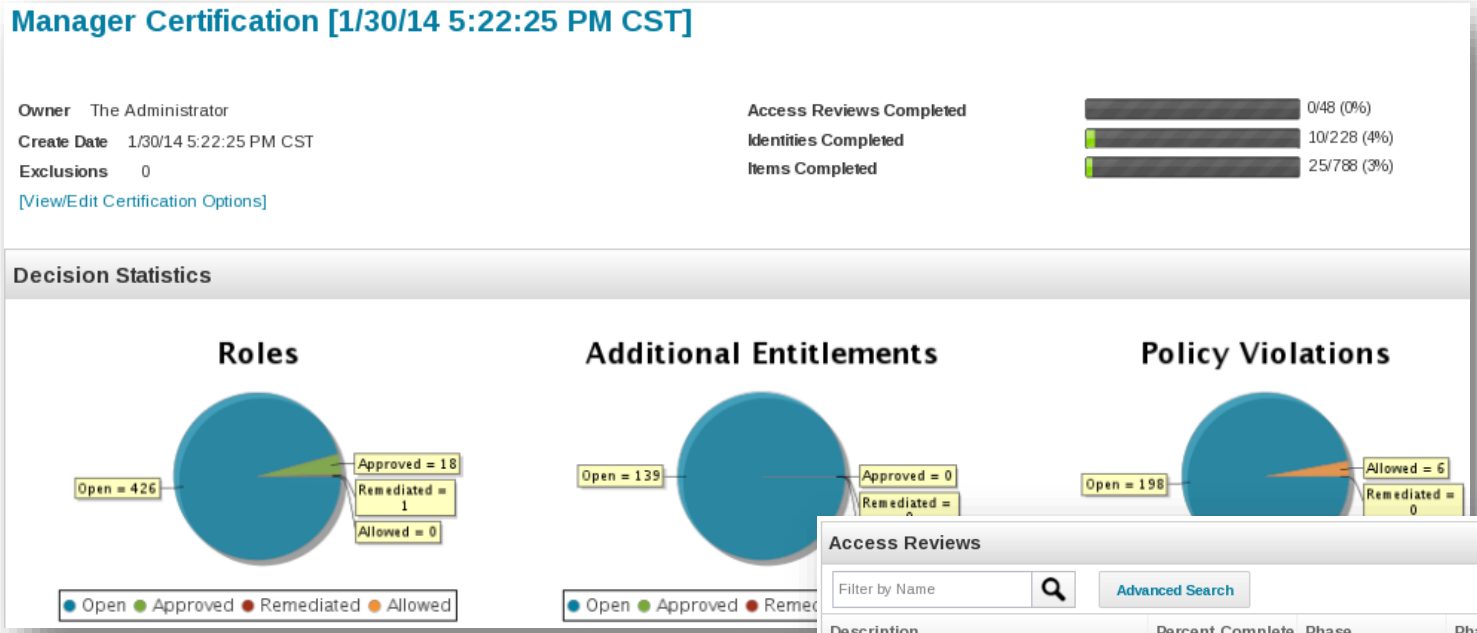
SailPoint Copyright © SailPoint Technologies, Inc. 2016 All rights reserved.

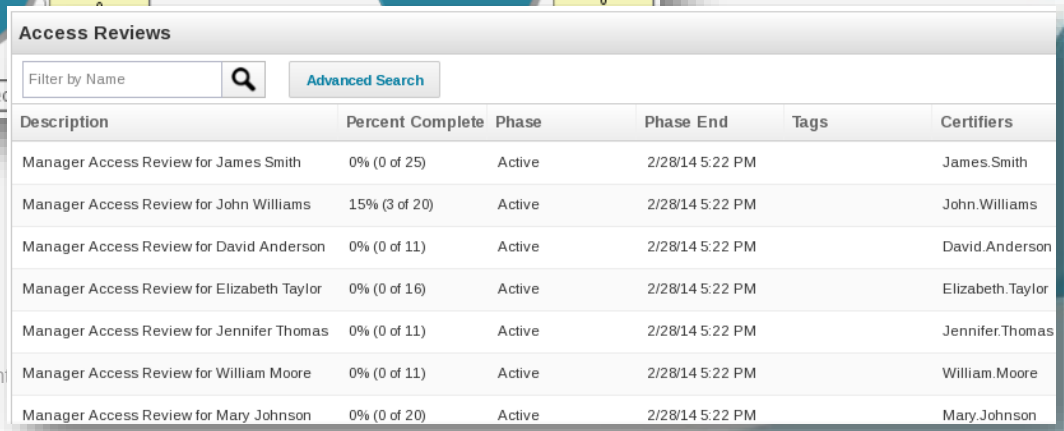
Certification Monitoring

SailPoint

Certifications – Monitoring Progress

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

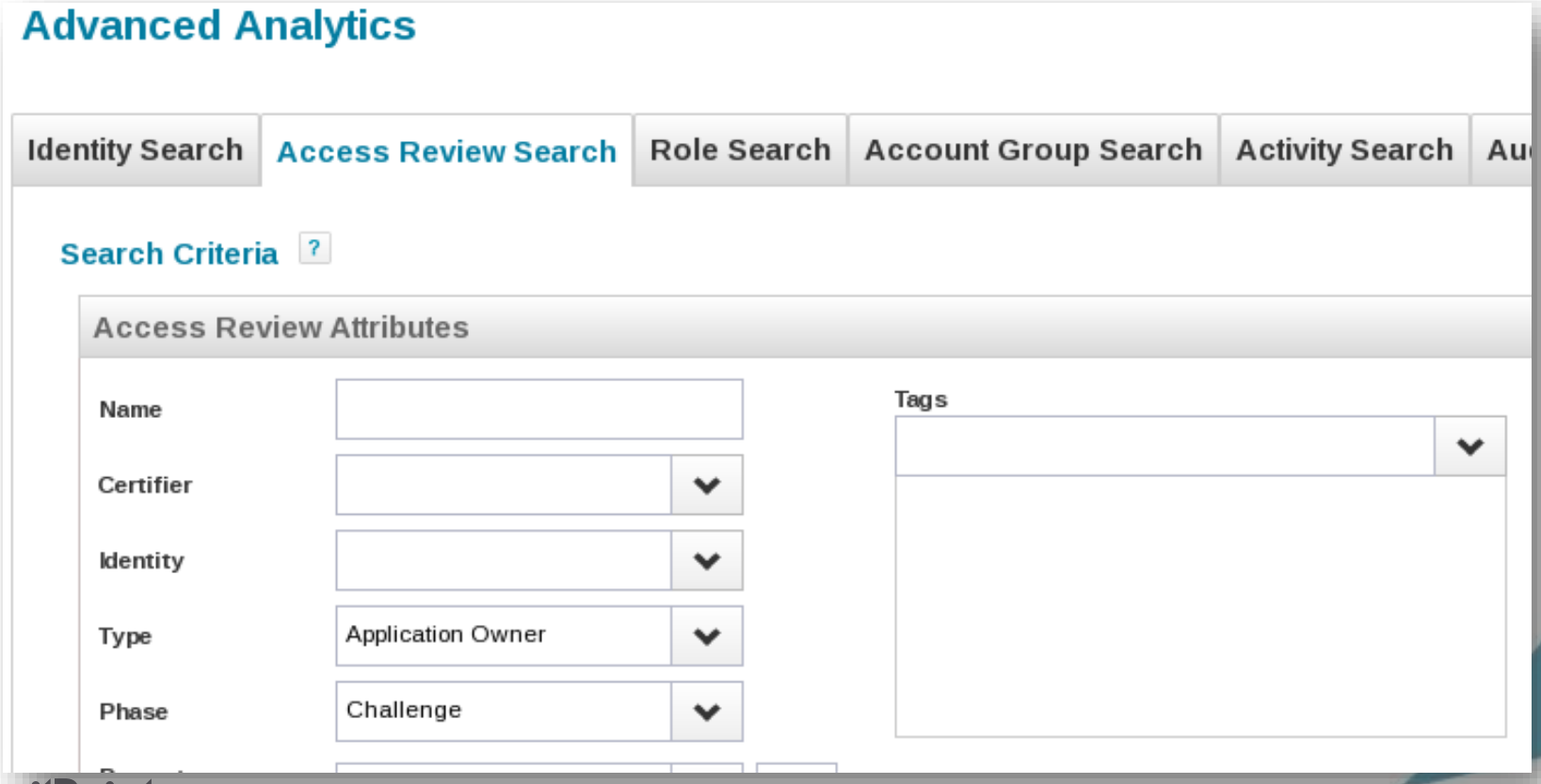




SailPoint Copyright © SailPoint Technologies, Inc. 2016 All right

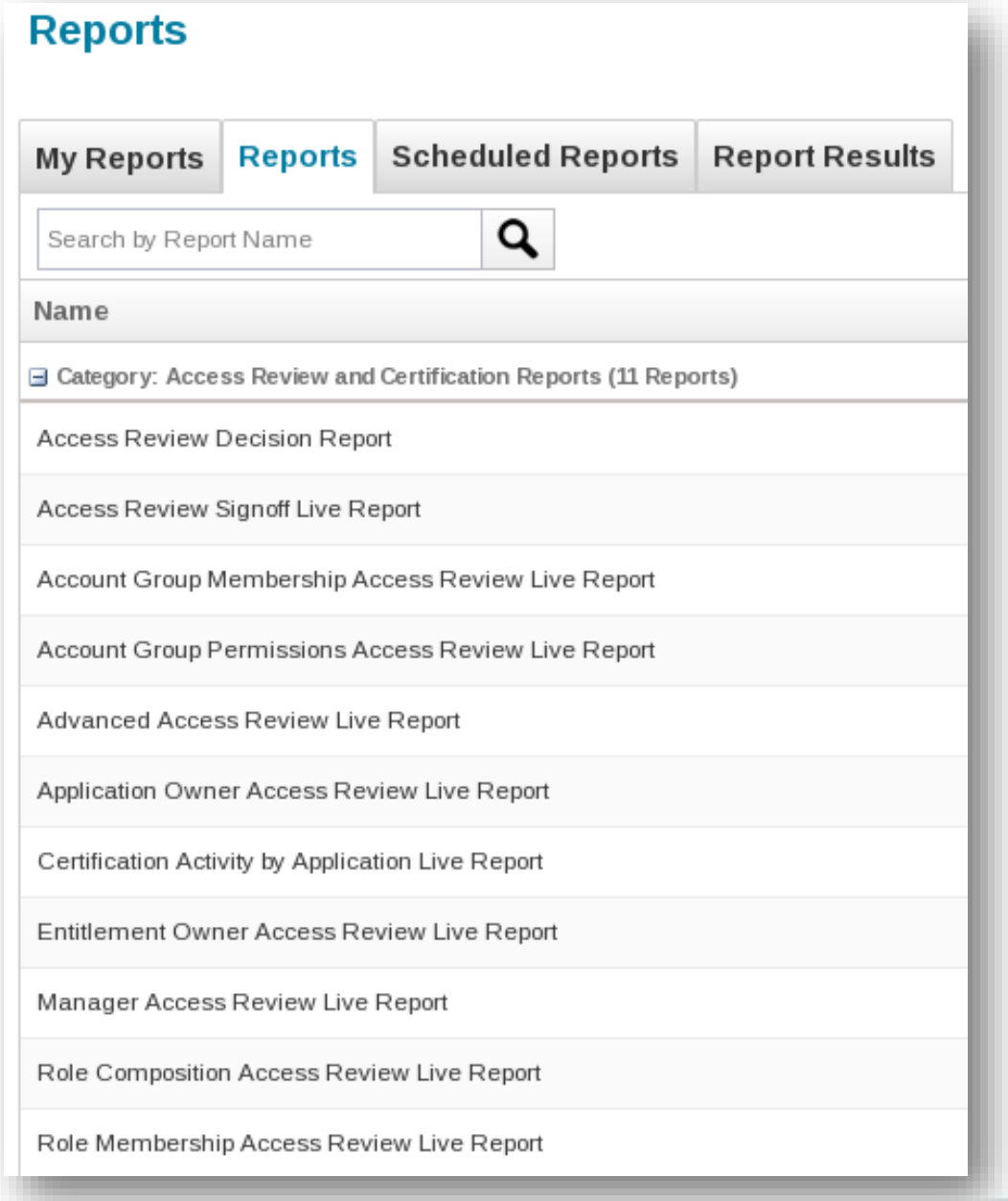
Certifications – Analytics

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



SailPoint Copyright © SailPoint Technologies, Inc. 2016 All rights reserved.

Certifications – Reporting



SailPoint Copyright ©

Questions?

SailPoint

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

SailPoint Copyright © SailPoint Technologies, Inc. 2016 All rights reserved.