

Access Certification

Fundamentals of IdentityIQ Implementation
IdentityIQ

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)

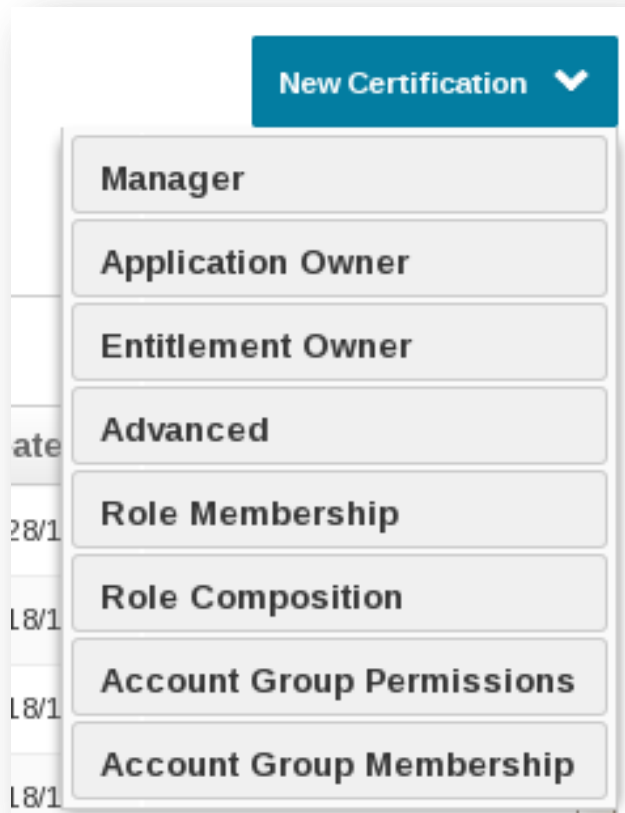
Access Review Details

<input type="radio"/> OK <input type="radio"/> E	Cynthia.Cook
<input type="radio"/> OK <input type="radio"/> E	Jessica.Sanchez
<input type="radio"/> OK <input type="radio"/> E	Jose.Reed
<input type="radio"/> OK <input type="radio"/> E	Shirley.Rogers
<input type="radio"/> OK <input type="radio"/> E	Timothy.Morris

Certification Types

Certification Campaigns

- Monitor → Certifications



Targeted Certifications

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

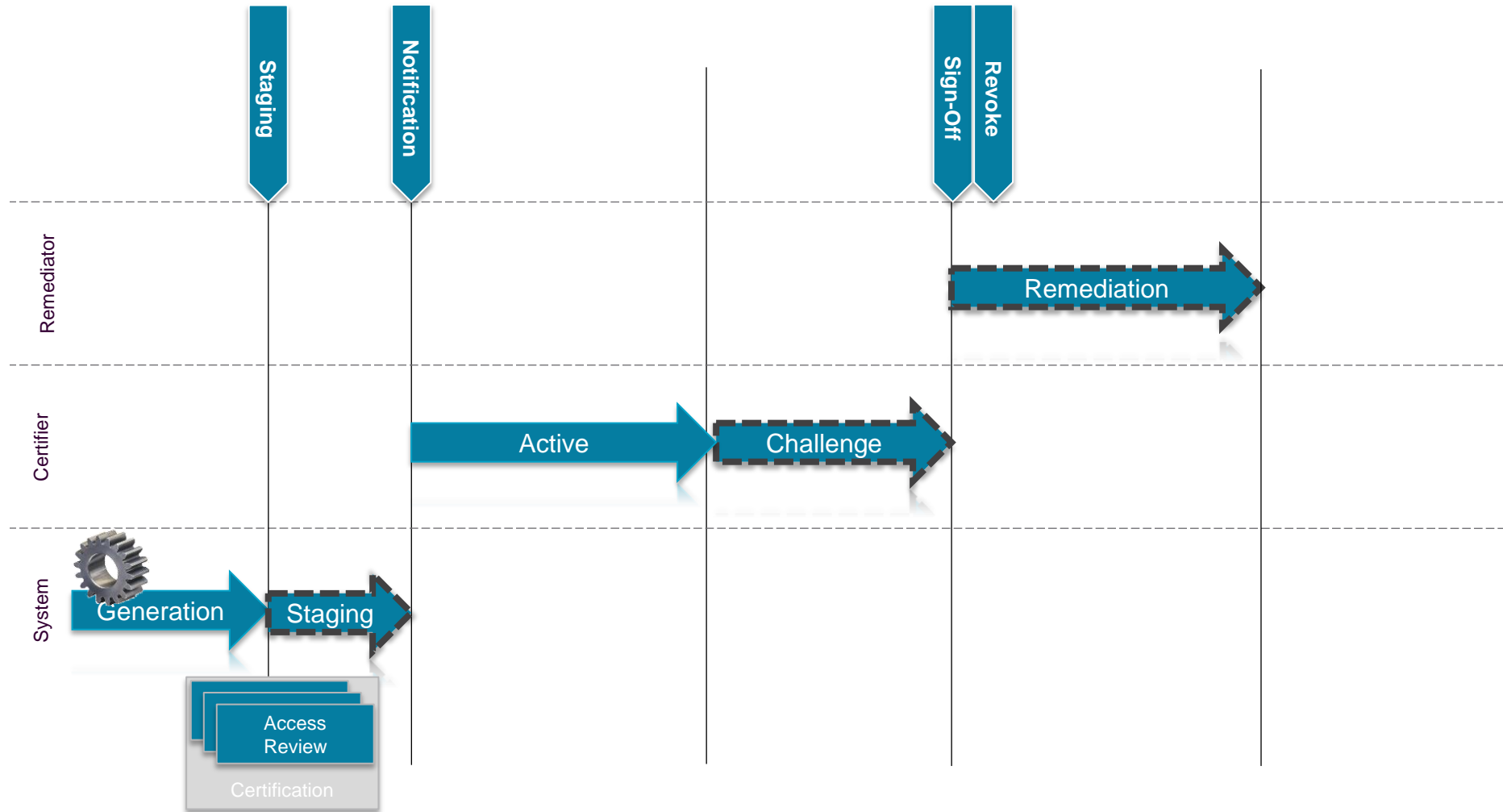
Overall Certification Process

- Compliance or business analyst defines certification parameters
- IdentityIQ collects data
 - Formats the information into interactive access reviews
 - Annotated with descriptive business language
 - Highlighted changes, anomalies and violations
 - Can require Electronic Signature sign-off (default is disabled)
 - Routes it to the appropriate reviewers
- Reviewers receive Access Reviews
 - Approve access for identities, roles and/or account groups
 - Take corrective actions (such as revoking entitlements that violate policy)
 - Forward, reassign, or delegate all or part of an access review to another user
 - Signs off on completed access review
- IdentityIQ takes action on revoked access
 - Directly revokes access
 - Initiates work item
 - Whatever is configured

Certification Schedules

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

Certification Time Periods

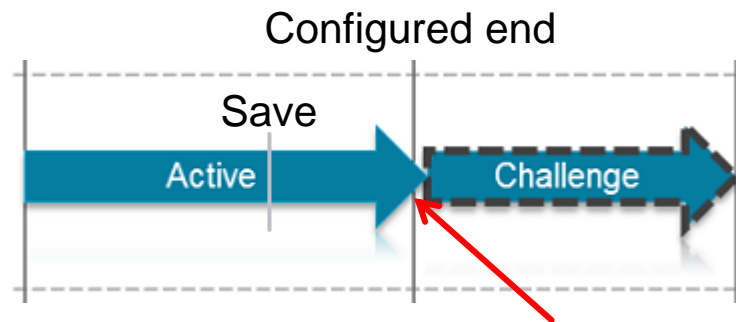


Certification Time Periods

Interaction between Challenge Period and Revoke Immediately

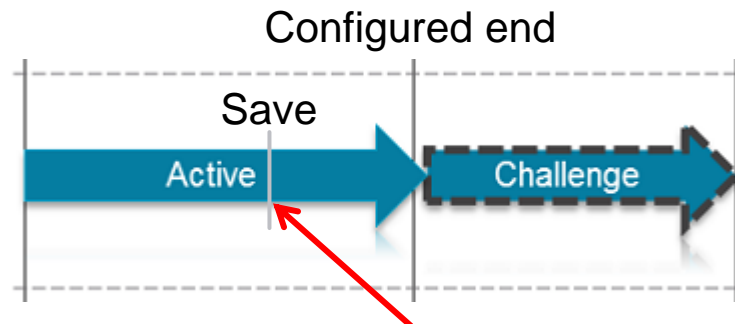
- Default Challenge Period behavior

- Challenge period starts at the end of the configured active period



- With Process Revokes Immediately option

- Challenge period starts immediately upon **save** of a revoke decision



Certification Time Periods

Challenge Period Interaction

- When a challenge occurs
 - The certifier sees an Action Required flag in the access review
 - The certifier right clicks on the challenged entitlement to handle the challenge
 - The certifier accepts or rejects the challenge and provides a comment

Certification Configuration

Overview

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

Certification Configuration – What to Certify

Manager Certification

- Certify that direct reports have correct access
- Configuration
 - Which specific managers/all managers
 - Which applications/all applications
 - Certify Entitlements or Accounts
 - Can certify if a user has an account on a system versus the specific entitlements a user possesses
 - For Entitlements
 - Include Additional Entitlements
 - Include Roles
 - Certify Accounts with no Entitlements (Y/N)
 - Policy Violations

Certification Configuration – What to Certify

Application Owner Certification

- Certify that identities accessing the application have the proper access to the application
- Configuration
 - Which applications/all applications
 - Certify Entitlements or Accounts
 - Can certify if a user has an account on a system versus the specific entitlements a user possesses
 - For Entitlements
 - Include Additional Entitlements
 - Include Roles
 - Certify Accounts with no Entitlements (Y/N)
 - Policy Violations

Certification Configuration – What to Certify

Entitlement Owner Certification


- Certify that identities accessing entitlements are correct
- Configuration
 - Which applications/all applications
 - Include un-owned Entitlements
 - If yes, who will review un-owned Entitlements
 - Default: Application owner
 - Can define another user






Q: Where is entitlement ownership defined?


Certification Configuration – What to Certify




Advanced Certification

- Certify that identities included in a population or group have the correct access
- Configuration
 - User group(s) to certify
 - Population
 - Select pre-defined population of users to certify
 - Select certifiers from a pick list
 - Group Factory
 - Select pre-defined group of users to certify
 - Rules used to assign certifiers

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 -- 	

Certification Configuration – What to Certify

Role Membership and Role Composition Certification

- Role Membership Certification
 - Request that the owner of a role certify the members of each role
- Role Composition Certification
 - Request that the owner of a role certify the composition (makeup) of the role
- Which roles to certify
 - Choose specific ones
 - By Type (IT/Business/etc.)
 - All Roles

Certification Configuration – What to Certify

Account Group Permissions and Membership Certifications

- Account Group Membership Certification
 - Request that the owner of an account group certify the Membership of the Account Group
- Account Group Permissions Certification
 - Request that the owner of an account group certify the actual entitlements/permissions granted to the Account Group
- Which applications to certify
 - Choose or All Applications

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

Coded 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

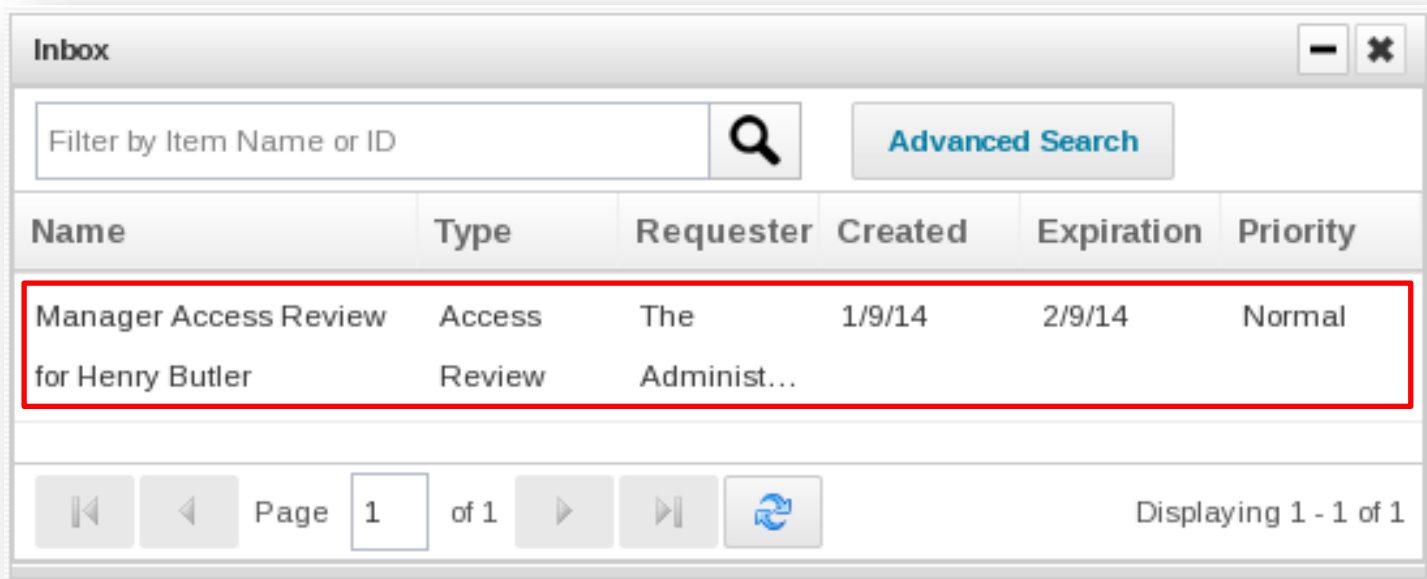
Certification Configuration

Global Configuration

- Set default configurations
 - System Setup → Certification Configuration
 - 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

Managing Access Reviews

- [Inbox or Manage](#) → [My Access Reviews](#)










































The screenshot shows a web application window titled "Inbox". It features a search bar with the placeholder text "Filter by Item Name or ID" and a magnifying glass icon. To the right of the search bar is a button labeled "Advanced Search". Below the search bar is a table with the following columns: Name, Type, Requester, Created, Expiration, and Priority. The table contains one row of data, which is highlighted with a red border. The data in the row is: Name: "Manager Access Review for Henry Butler", Type: "Access Review", Requester: "The Administ...", Created: "1/9/14", Expiration: "2/9/14", and Priority: "Normal". At the bottom of the window, there is a pagination bar with navigation buttons (back, first, previous, next, last, refresh) and the text "Page 1 of 1" and "Displaying 1 - 1 of 1".

Name	Type	Requester	Created	Expiration	Priority
Manager Access Review for Henry Butler	Access Review	The Administ...	1/9/14	2/9/14	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

- 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
- Decisions
 - 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
 - Pass decision to another user
 - Delegate, Reassign or Forward (see next slides for details)

Access Reviews – Certifier Decisions

Delegate

- Unique to certifications
- Delegate whole entity (default) or single line item (option)
 - Delegated item/entity remains part of the original access review
 - *Workitem* is sent to the delegate
 - Delegate makes decisions on the item(s)
 - Decisions are merged back onto the original access review
- Access review owner
 - Retains responsibility for all decisions
 - Can revoke delegation at any time and make new decisions
 - Can be required to review the decisions made by a delegate before the items are considered complete (configuration option)
- Examples
 - Automatic: Use rule to delegate (pre-delegate)
 - Manual: Perform delegation from within access review details

Access Reviews – Certifier Decisions

Reassign

- Unique to certifications
- Reassign whole entity, single line item, or bulk
 - Items are removed from the original access review
 - *New child access review* created and assigned to new owner
 - Child access review allows for same actions as parent (i.e. delegate, reassign, forward, etc.)
 - Child access review owner assumes responsibility for decisions
- Parent access review owner
 - Can revoke reassignment at any time and make new decisions
 - Cannot sign off until the reassignment is completed and signed off (default)
 - Can be configured to retain no responsibility

Access Reviews – Certifier Decisions

Forward

- Applies to any work item in IdentityIQ
- Forward entire access review
 - Retains all previously made decisions, reassignments or delegations
 - Passes all responsibility from the original owner to a new user
 - Forwarding owner has no access to the work item
 - Forwarded item cannot be recalled or edited in any way by original owner
- Typical Uses:
 - Out of Office
 - Executives
 - “Service” Identities

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
- **Without Electronic Signature enabled**
 - Sign off serves as loose contract that assigns final responsibility to the access review owner
- **With Electronic Signature enabled**
 - Formal meaning assigned and permanently recorded

Access Certification – Certification End

Electronic Signatures (6.1)

- Available for

- Certification Sign-off
- Access Sign-off
- Report Sign-off

- Process

- Meaning of sign-off displayed
- Authenticator enters credentials
- After sign-off
 - Signature and meaning embedded into signed object
 - Object cannot be edited or deleted

The screenshot displays the 'Access Review Details' page for Catherine Simmons. A modal titled 'Electronic Signature Required' is open, containing a notice about the legal implications of electronic signing. Below the notice are input fields for 'Username' (pre-filled with 'catherine.simmons') and 'Password'. At the bottom of the modal are 'Sign' and 'Cancel' buttons. The background interface includes a 'Manager Access Review for Catherine Simmons' section with 'Due on' (2/12/14) and 'Owner' (Catherine Simmons) information, and a table of review items with status icons (green for 'Approve', orange for 'Deny').

Dashboard Manage

Access Review Details

Manager Access Review for Catherine Simmons

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

Filter

Legend: OK Approve X Deny

Decision	Ident
OK ⊖	Denis
OK ⊖	Denis
OK ⊖	Denis
X ⊖	Denis
OK ⊖	Irene.T
OK ⊖	Irene.T
OK ⊖	Irene.T
X ⊖	Irene.T

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 coy of this statement is available in the HR handbook.

Username:

Password:

Sign Cancel

Configuring Electronic Signatures

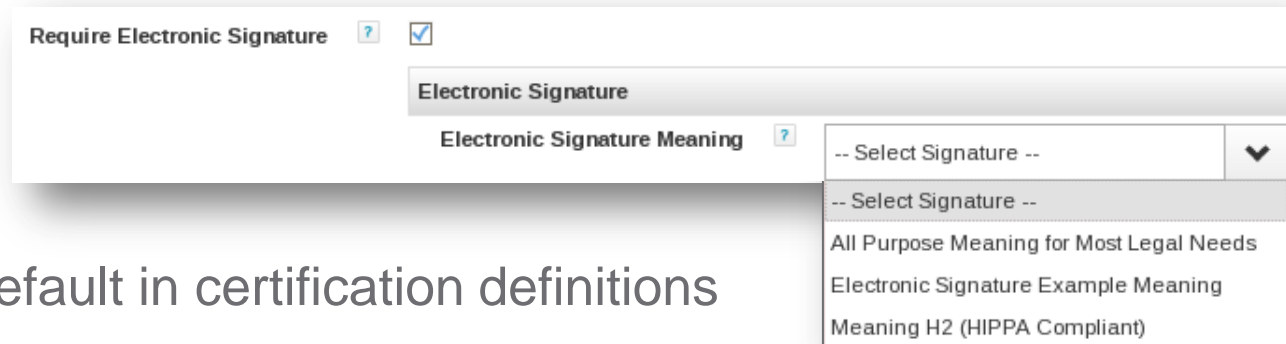
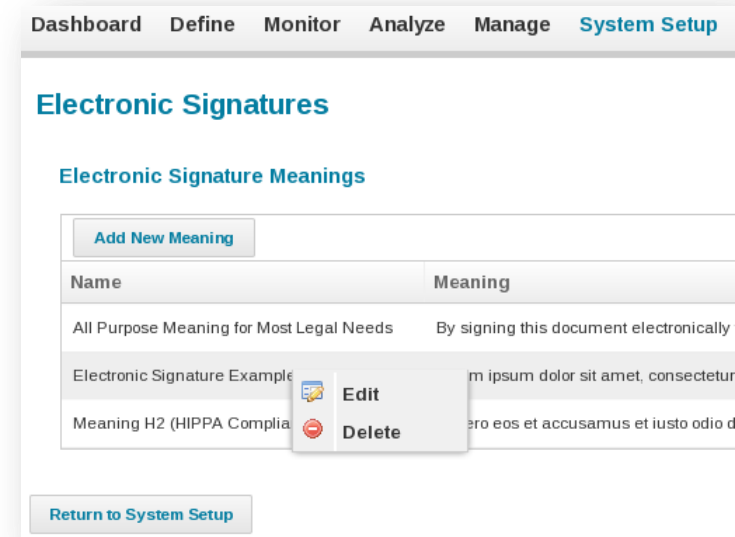
Certifications

- Create Meanings

- Named, preconfigured messages describing meaning of the sign off
- System Setup → Electronic Signatures

- Configure Usage

- Can require for all certifications
 - System Setup → Certification Configuration

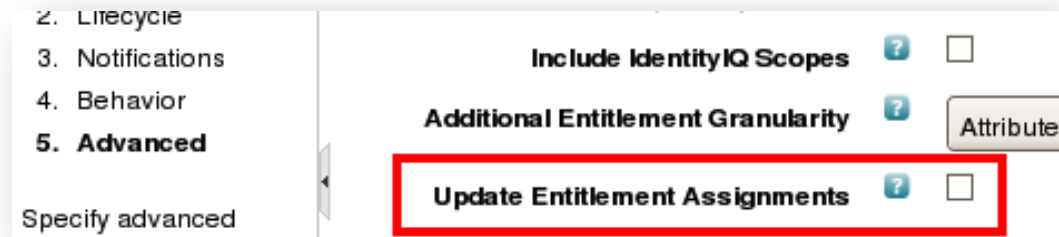


- Can override default in certification definitions

Access Certification – Certification End

PerformMaintenance Task

- PerformMaintenance task runs periodically
 - Checks for certification completion and sign-off
 - On sign-off, it performs the following
 - Revokes are processed
 - For configured connectors or integrations
 - Revoke changes are made
 - Trouble Tickets created (Remedy, ServiceNow)
 - Where no connector or integration exists
 - IdentityIQ Workitems created with details on how to perform the remediation.
 - Certification Decisions
 - Are factored into risk score
 - Entitlement assignment may be updated based on configuration



The screenshot shows a configuration window with a sidebar on the left and a main content area on the right. The sidebar contains a list of options: 2. Lifecycle, 3. Notifications, 4. Behavior, 5. Advanced (which is selected), and Specify advanced. The main content area has three sections, each with a title, a help icon (question mark), and a checkbox. The first section is 'Include IdentityIQ Scopes' with an unchecked checkbox. The second section is 'Additional Entitlement Granularity' with a help icon and an 'Attribute' button. The third section is 'Update Entitlement Assignments' with a help icon and a checked checkbox. This third section is highlighted with a red rectangular border.

2. Lifecycle	
3. Notifications	
4. Behavior	
5. Advanced	
Specify advanced	

Include IdentityIQ Scopes	?	<input type="checkbox"/>
Additional Entitlement Granularity	?	Attribute
Update Entitlement Assignments	?	<input checked="" type="checkbox"/>

Targeted Identity Certifications

Targeted Identity Certifications

Certifications from Advanced Analytics

- Analyze → Advanced Analytics
- Select and Certify

The screenshot displays the 'Advanced Analytics' interface. At the top, there are four tabs: 'Identity Search' (active), 'Access Review Search', 'Role Search', and 'Account Group Search'. Below the tabs, it says 'Search Results - 3 Results Returned'. There are three buttons: 'Result Options' with a dropdown arrow, 'Refine Search', and 'Schedule Certification' (highlighted with a red box). Below these buttons is a table with a header row 'Username' and three data rows: 'Clarence.Harper', 'Norma.Armstrong', and 'Tina.Ruiz'. The checkboxes in the first column of the table are highlighted with a red box.

	Username ▲
<input type="checkbox"/>	Clarence.Harper
<input type="checkbox"/>	Norma.Armstrong
<input type="checkbox"/>	Tina.Ruiz

Targeted Identity Certifications

Certifications from Risk Scoring

- Manage → Identity Risk Scores
- Select and Certify

<input type="checkbox"/>	Cynthia.Cook	Cynthia	Cook	575
<input checked="" type="checkbox"/>	Daniel.Lewis	Daniel	Lewis	575
<input type="checkbox"/>	Douglas.Flores	Douglas	Flores	338
<input checked="" type="checkbox"/>	Earl.Sims	Earl	Sims	575
<input checked="" type="checkbox"/>	Edward.Baker	Edward	Baker	575
<input type="checkbox"/>	Emily.Kelley	Emily	Kelley	575
<input type="checkbox"/>	Evelyn.Ellis	Evelyn	Ellis	575

Page 1 of 4

[Schedule Certifications](#) 28 items selected

Targeted Identity Certifications

Certification from Policy Violation

- From policy violation trigger one-off certification of identity

Policy Violations

Identity Bobby.Stephens

Status Open

Policy TRAKK SOD Policy

Policy Description

Policy Violation Owner Lori.Ferguson

Rule Cannot be Super and Input at the same time

Score Weight 300

Violation Decision

Select Decision

Select Decision

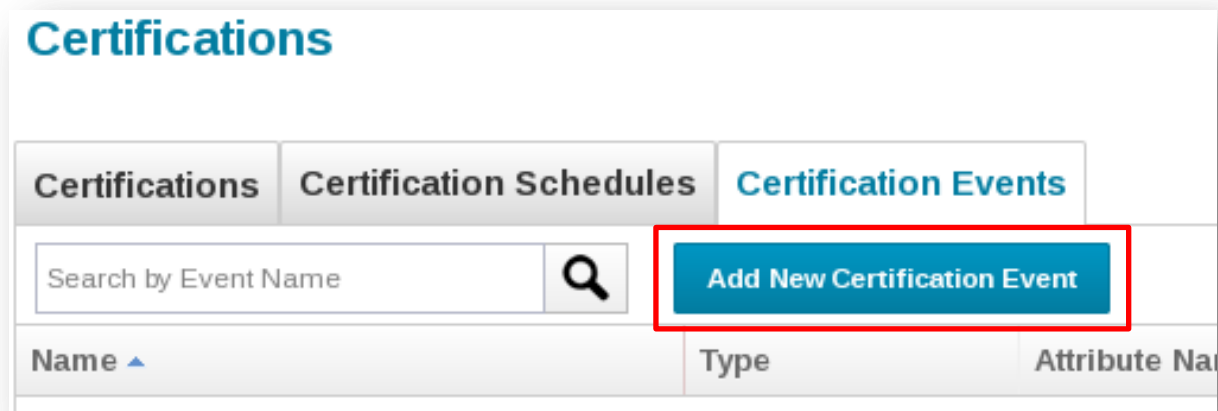
Allow Violation

Correct Violation

Certify Identity

Certification Events

- Perform targeted certification based on changes to an identity
 - New employee
 - Manager change
 - Department change
 - Based on rule evaluation
- Configuration
 - Monitor → Certification → Certification Events
 - New Certification Event



The screenshot displays the 'Certifications' section of the SailPoint interface. It features 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, a table header is visible with columns for 'Name', 'Type', and 'Attribute Na'.

Certification Events

Configuring

- Configure certification to run when event occurs

Certification Event

Summary	Basic
Steps <ol style="list-style-type: none">1. Basic2. Lifecycle3. Notifications4. Behavior5. Advanced <p>Specify options about what to certify, when the certification should be created, and who is responsible for certification.</p>	<h4>Event Options</h4> <p>Name <small>?</small> <input type="text"/></p> <p>Description <small>?</small> <input type="text"/></p> <p>Event type <small>?</small> <input type="text" value="Create"/></p> <p>Disabled <small>?</small> <input type="checkbox"/></p> <p>Included Identities <small>?</small> <input type="text"/></p> <h4>Certification Properties</h4>

Configure certification options as usual

Define event type that will invoke a certification

Certification Monitoring

Certifications – Monitoring Progress

- Monitor → 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

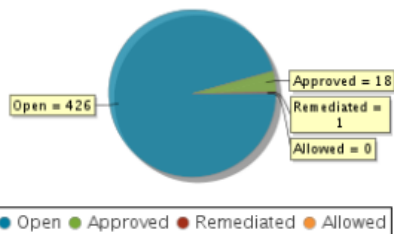
10/228 (4%)

Items Completed

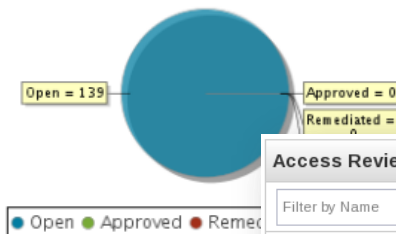
25/788 (3%)

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

- Analyze → 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
 Category: Access Review and Certification Reports (11 Reports)
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