

Lifecycle Manager

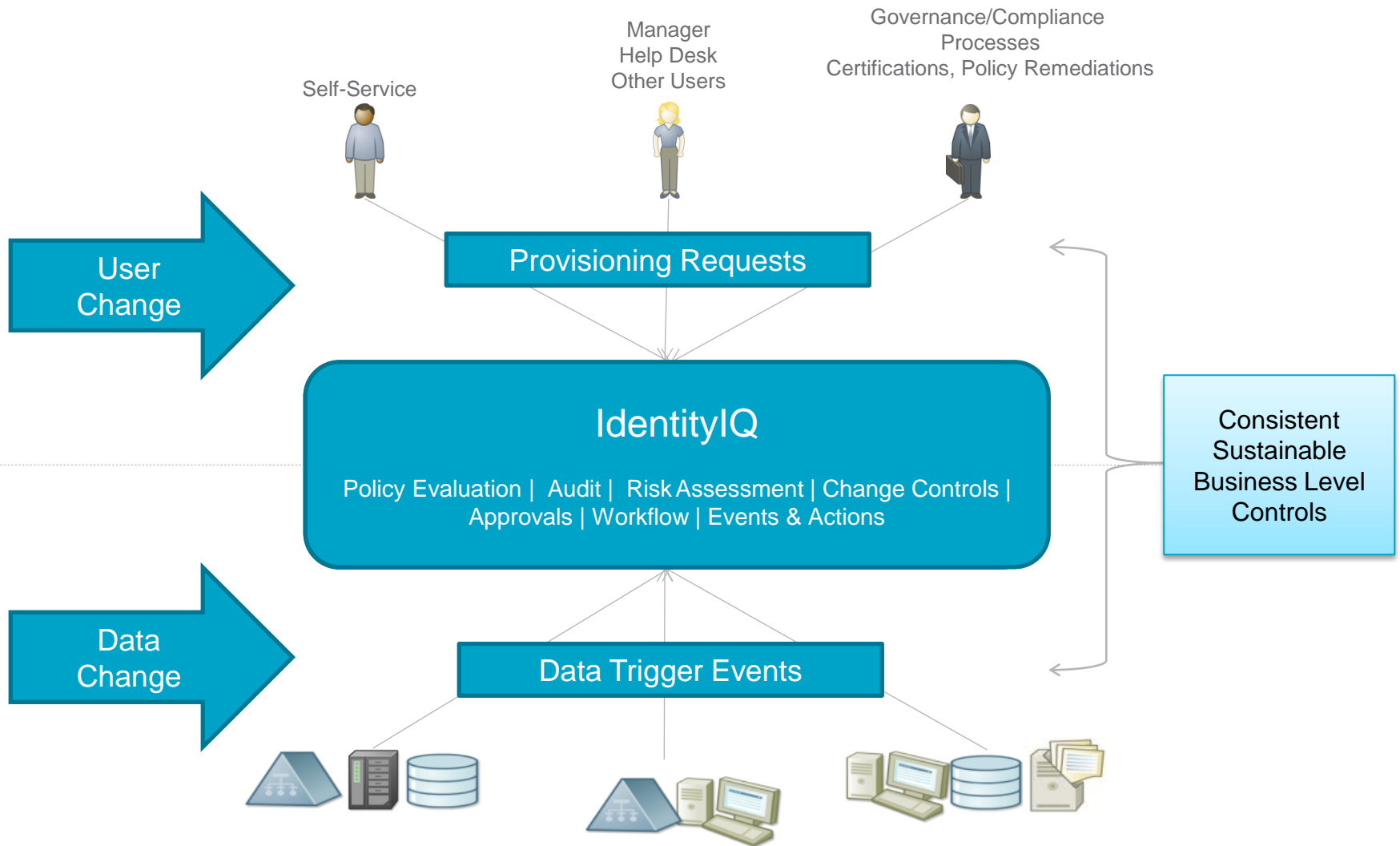
Fundamentals of IdentityIQ Implementation
IdentityIQ

Overview

Lifecycle Manager

- Change Lifecycle
- Key Features and considerations
- Access request process
- Additional Access and Identity Management Options
 - Change passwords
 - Request IdentityIQ identity
- LCM configuration
 - Configuring LCM requests
 - Configuring LCM events
- Additional LCM functionality

Identity & Entitlement Change Lifecycle



Key Features/Considerations

User Change

- Lifecycle Requests

- What do you want people to be able to do?
 - Request Access (Role and Entitlements)
 - Manage Accounts/Passwords
 - Create/Edit/View Identities
- Who should be able to do what?
 - Order for themselves? Self-Service
 - For others? Managers/Help Desk/All Users
- What can be requested?
 - Entitlement Catalog and Role Repository configuration
 - Scoping configuration
 - Rules configuration
- Business Process (Workflow)?
 - What to do for each type of request...

Key Features/Considerations

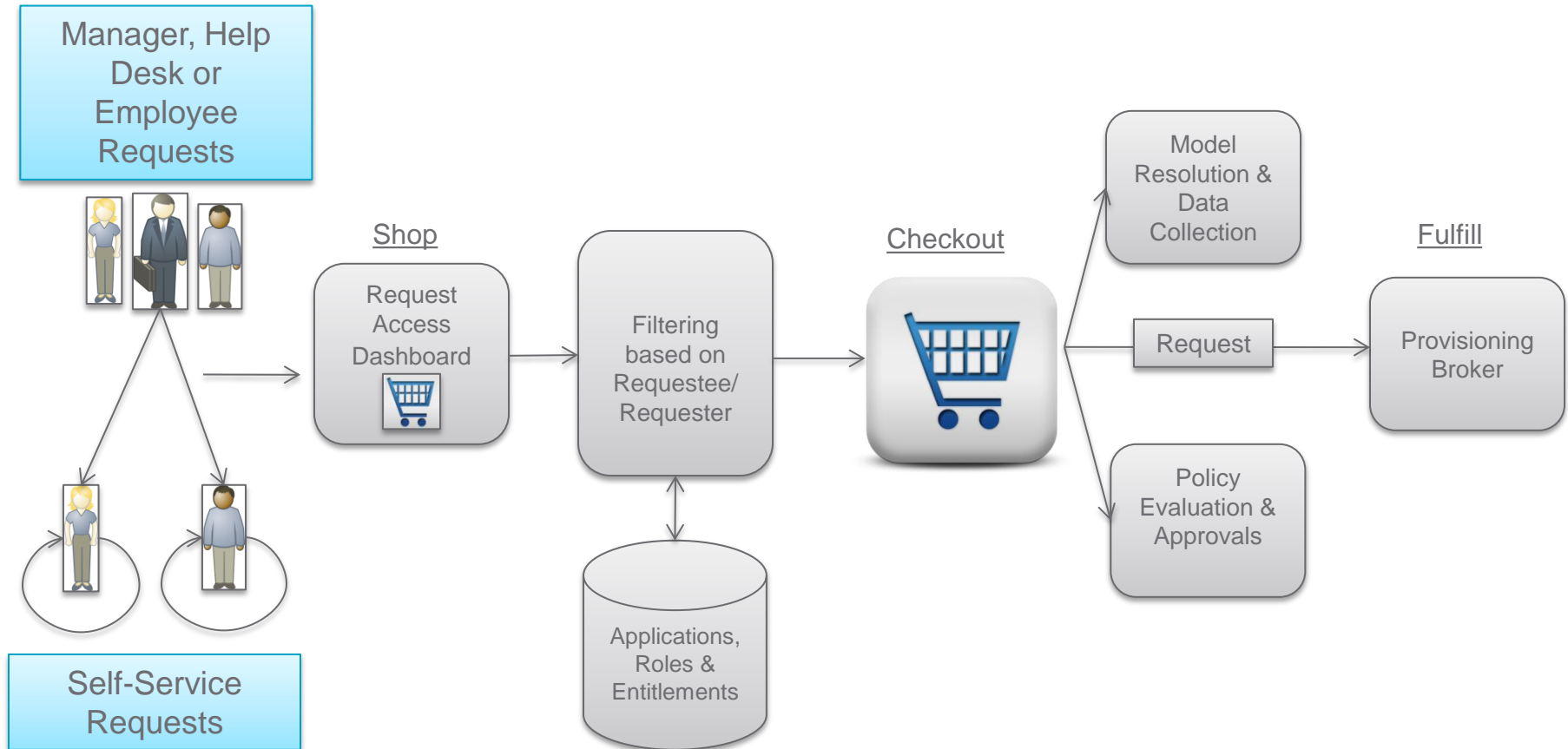
Data Change

- Lifecycle Events

- What changes detected in target systems kickoff workflow?
 - Create/Joiner
 - Attribute Change/Mover or Leaver
 - Rule
 - Native Change (New in 6.0)
- Business Process (Workflows)
 - What to do when each type of event is detected...

Access Request Process

Lifecycle Access Requests




Managing LifeCycle Requests

- Request for Others
 - Managers, Help Desk Administrators, and all other users based on configuration
- Request for Me
 - Self Service Requests


Dashboard

My Dashboard


Edit Dashboard

COMPLIANCE ACTIVITIES


- Access Reviews (0)
- Policy Violations (5)

ASSIGNED TASKS

- Approvals (0)
- Sign-off Reports (0)
- Work Items (5)

MANAGE ACCESS


- Request Access**
- Manage Accounts
- Change Password
- Track My Requests

MANAGE IDENTITY

- Create Identity
- Edit Identity
- View Identity

For Me
For Others

8

 **SailPoint**


Walkthrough – Requesting Access

- Choose requestees

- Self-Service – defines the requestee as the user making the request
- Driven by LCM configuration
- This example shows a manager making a request and seeing their direct reports in the selection screen

Available Identities

Filter by Identity Name



Advanced Search

<input type="checkbox"/>	Name ▲	First Name	Last Name	Manager
<input type="checkbox"/>	Denise.Hunt	Denise	Hunt	Catherine.Simmons
<input type="checkbox"/>	Irene.Mills	Irene	Mills	Catherine.Simmons
<input type="checkbox"/>	Jeremy.Palmer	Jeremy	Palmer	Catherine.Simmons
<input type="checkbox"/>	Louis.Black	Louis	Black	Catherine.Simmons
<input type="checkbox"/>	Tammy.Daniels	Tammy	Daniels	Catherine.Simmons

Walkthrough – LCM Searching

...for Roles/Entitlements

- Keyword or User-based Search
- See Current Access as well (for removals)
- Shopping paradigm
 - Search, Add To Cart

Select Identity(s) > **Select Access** > Review & Submit



Request Access for [Aaron.Nichols](#) ?

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

Search

Roles (4) | Entitlements (31) | Current Access

[Narrow Results](#) Page 1 of 1 Displaying 1 - 4 of 4

	PRISM Super <ul style="list-style-type: none">Type: BusinessOwner: The Administrator	Risk Score: ● 0	<input type="button" value="Add To Cart"/>
	PRISM User <ul style="list-style-type: none">Type: BusinessOwner: The Administrator	Risk Score: ● 0	<input type="button" value="Add To Cart"/>

Walkthrough – LCM Searching

...by Keyword Search

- Use keywords to search for Roles/Entitlements
- Optional Full Text Search

Select Identity(s) > Select Access > Review & Submit

Request Access for [Aaron.Nichols](#) ?

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

Search

Roles (4) | **Entitlements (31)** | Current Access

[Narrow Results](#)

Page 1 of 1

PRISM Super
• Type: Business
• Owner: The Administrator
• Risk Score: 0

PRISM User
• Type: Business
• Owner: The Administrator
• Risk Score: 0

[Add to Cart](#)

Keyword search uses defined attributes within the Role and Entitlement Models including extended attributes

Role and Entitlement Results are configurable via UIConfig Entry Keys:

- sailpoint.web.lcm.EntitlementsRequestBean_search
- sailpoint.web.lcm.RolesRequestBean_search

Walkthrough – LCM Searching

...by User-based Search

- Affinity-Based Search

- Search by population attribute matching or by identity match
- Available only to those who can request access for others

Select Identity(s) > Select Access > Review & Submit

Request Access for [Aaron.Nichols](#)

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

Search Search

Search Based on What Other Users Have

Roles (3) Entitlements (11) Current Access

Search by Population

To request access owned by a certain population, use the fields below to define a population based on their attributes to review their current access

Manager:

☒ Region:

Benefits Clerk
Coordinates enrollment and maintains group insurance records for medical, life, and other coverage for employees and eligible dependents. Processes enrollment forms and provides assistance and information to employees.
• Type: Business • Risk Score: 50
11% (8/76) [Add To Cart](#)

Benefits Manager
Produces or advises benefits plans for the organization. Implements programs and procedures. Benefits administered may include health, dental, vision, disability or retirement. Arranges and affects new programs with benefits vendors. Oversees programs for conformance with government regulations.
• Type: Business • Risk Score: 80
5% (4/76) [Add To Cart](#)

UIConfig controls available search options

- Entry Key: "lcmSearchIdentityAttributes"
- Configured by implementation team

Walkthrough – Submitting a Request



- Clicking Checkout and Submit starts Business Process (workflow)
- Business Process handles policy checks, approvals, gathering needed information, etc.










Summary of Requests for [Denise.Hunt](#)

Please verify the changes you have requested below. To modify the activation or deactivation date of an individual item, click "Edit Details."

Request Options

Activation: 01/28/14  Deactivation: 

Action	Name	Type	Comments	Risk S	Owner
 Edit Details 	VPN  Activation: 1/28/14 • Attribute: groups • Application: LDAP	Entitlement		 1	Randy.Knight

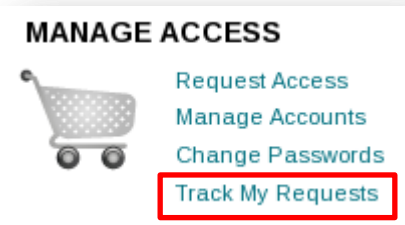
Page 1 of 1  Show 10  items

Displaying 1 - 1 of 1

Submit [Cancel](#) [Make Additional Changes](#)

Walkthrough – Managing Access Requests

- Fully traceable & trackable Access Requests
- Where?
 - Dashboard → Track My Requests
 - Manage → Access Requests
- Choose *View Complete Details*
 - See complete breakdown of Access Request



Access Requests

Filter by Identity		Q	Advanced Search						
Access Request ID	Priority	Type	Requester	Requestee	Request Date	Current Step	Completion Date	Execution Status	
1	Normal	Request Access	Denise.Hunt	Denise.Hunt	1/28/14 7:04 PM	Initialize		Executing	
Request Items View Complete Details									
Operation	Item	Value	Account	Application	Instance	Comments	Approval Status	Provisioning Status	
Add	groups	cn=VPN,ou=groups,dc=training,dc=sailpoint,dc=com	cn=Denise.Hunt,ou=people,dc=training,dc=sailpoint,dc=com	LDAP			Pending	Pending	
Pending Interactions									
Description			Owner	Open Date	Details				
Owner Approval - Account Changes for User: Denise.Hunt			Randy.Knight	1/28/14 7:04 PM	1 Approval Item(s) [Click for Details]				

Walkthrough – Access Request Details

- Details entire request including
 - What was requested
 - Approvals complete/pending
 - Final status of request

Access Request - 1

Access Request ID 1
Type Request Access
Requester Denise.Hunt
Requestee Denise.Hunt
Completion Status Pending
Priority Normal

Current Step Initialize
Request Date 1/28/14 7:04 PM
Completion Date
Verification Date
Execution Status Executing

[Back](#)

Request Items

Operation	Item	Value	Account	Application	Instance	Comments	Approval Status	Provisioning Status
Add	groups	cn=VPN,ou=groups	cn=Denise.Hu...	LDAP			Pending	Pending

Page 1 of 1
Show 5 items
Displaying 1 - 1 of 1

Interactions

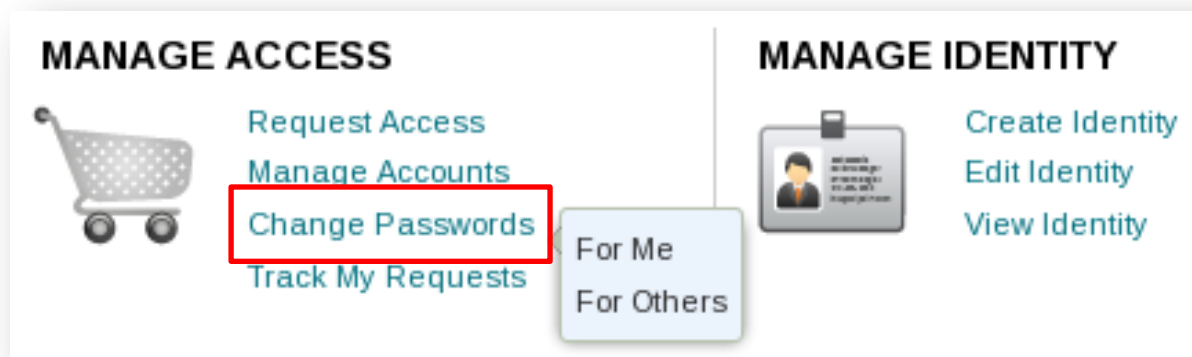
Description	Owner	Open Date	Completion Date	Comments	Status	Details
Owner Approval - Acco...	Randy.Knight	01/28/14 07:04:48 pm			Open	1 Approval Item(s) [Click for Details]

Page 1 of 1
Show 5 items
Displaying 1 - 1 of 1

Additional Access and Identity Management Options

Changing Passwords

- Generate or specify a password
 - Application password policy is enforced
 - Whose password a user can manage is configurable
 - Self
 - Direct reports
 - Others



Changing Passwords

Synchronize Password and Multiple Application Policies

- IdentityIQ detects and enforces strictest combination of policy criteria
- Applications with conflicting policies are identified and cannot be synchronized

Select method for password change:

☒ Synchronize passwords for selected accounts

New Password:



Password Constraints

Password must have at least 1 digit(s)
Password must have at least 8 character(s)
Password must have at least 1 uppercase

Confirm Password:

<input checked="" type="checkbox"/> Account ID	Application	Status	Last Refresh
<input checked="" type="checkbox"/> Adam.Kennedy	LDAP	Active	1/2/14 6:24 PM
<input checked="" type="checkbox"/> Adam Kennedy	PeopleSoft	Active	1/29/14 9:53 AM

Page 1 of 1 show 10 items

Displaying 1 - 2 of 2

2 items selected

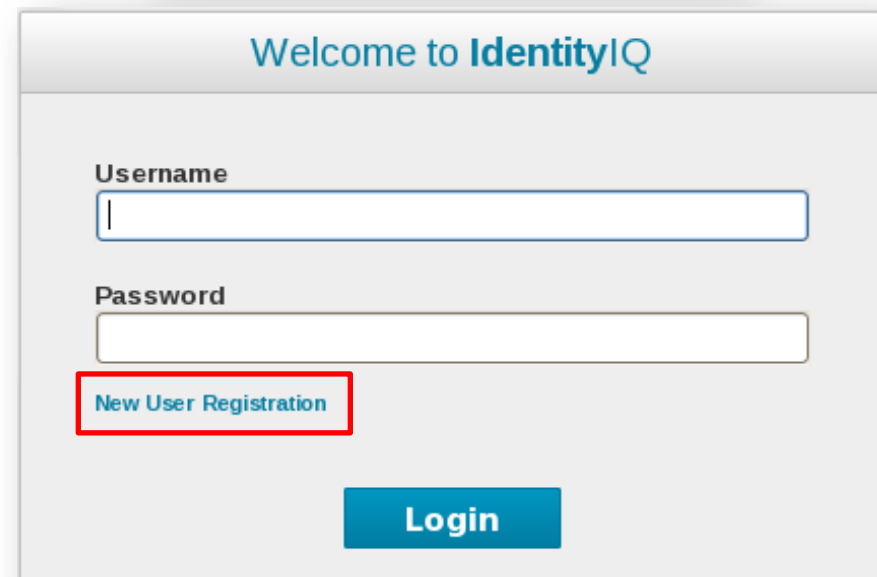
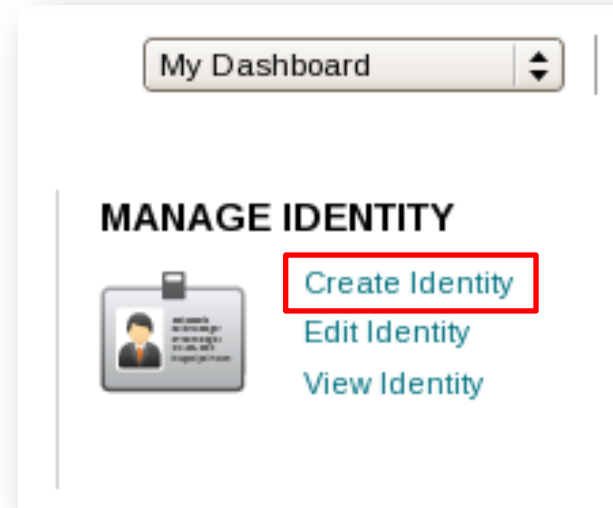
Submit

Cancel

Requesting IdentityIQ Identities

Two Cases

- User has IdentityIQ identity
 - Requesting identity from within IdentityIQ
- User has no IdentityIQ identity (Self-service Registration)
 - Requesting new identity for themselves
 - Must be enabled (default = off)
 - Access registration form from
 - Login page
 - External link (6.2)



Lifecycle Manager Configuration

LCM Configuration Process Overview

- Install LCM
 - In the console
 - >import init-lcm.xml
- Configure LCM requests
 - Who can request what for whom
- Configure LCM events
- Configure associated items outside of LCM
 - Requestable Items
 - Entitlement Catalog
 - Roles
 - Provisioning Policies
 - Business Processes (Workflows)

LCM Configuration

(Performed by Implementation Team)

- Three main configuration areas
 - Lifecycle Actions
 - Who can request what and for whom
 - Business Processes
 - Define which LCM actions run which Business Processes (workflows)
 - Additional Options
 - Options related to Role/Entitlement/Account requests and other general options

Lifecycle Manager Configuration

Lifecycle Actions

Business Processes

Additional Options

Configuring LCM Requests

LifeCycle Actions Configuration

- Who can make requests or manage?
 - Four groups of users
 - Self-Service
 - Manager
 - Help Desk Personnel
 - All Users
 - Defaults
 - Self-Service – Make requests for self
 - Manager – Make requests for direct or indirect reports
 - Help Desk Personnel – Make request on anyone's behalf
 - All Users – Can make no requests
 - Configuration for each set of users defines
 - What actions can be performed
 - For whom
 - On what objects (applications, roles, entitlements)

* indicates that a population of users must be specified to make

Self Service ?

Lifecycle Actions	
Request Access	<input type="checkbox"/>
Manage Accounts	<input type="checkbox"/>
Manage Passwords	<input type="checkbox"/>
Edit Identity	<input type="checkbox"/>
View Identity	<input type="checkbox"/>

Managers ?

Lifecycle Actions	
Request Access	<input type="checkbox"/>
Manage Accounts	<input type="checkbox"/>
Manage Passwords	<input type="checkbox"/>
Edit Identity	<input type="checkbox"/>
Create Identity	<input type="checkbox"/>
View Identity	<input type="checkbox"/>

Help Desk Personnel ?

Lifecycle Actions	
Request Access	<input type="checkbox"/>
Manage Accounts	<input type="checkbox"/>
Manage Passwords	<input type="checkbox"/>
Edit Identity	<input type="checkbox"/>
Create Identity	<input type="checkbox"/>
View Identity	<input type="checkbox"/>

All Users ?

Lifecycle Actions	
Request Access	<input type="checkbox"/>
Manage Accounts	<input type="checkbox"/>
Manage Passwords	<input type="checkbox"/>
Edit Identity	<input type="checkbox"/>
Create Identity	<input type="checkbox"/>
View Identity	<input type="checkbox"/>

Lifecycle Actions

Manager's Configuration

Lifecycle Actions

Business Processes

Managers ?

Lifecycle Actions

Request Access ? ☒

Request Access Options

Request Roles ? ☒

Request Roles Options

Allow requestor to see population statistics in Advanced Search for each role ? ☒

Request Entitlements ? ☒

Request Entitlements Options

Allow requesting additional accounts ? ☐

Allow requestor to see population statistics in Advanced Search for each entitlement ? ☒

Manage Accounts ? ☒

Manage Accounts Options

Allow managing existing accounts ? ☒

Allow requesting new accounts ? ☐

Allow requesting additional accounts ? ☐

Manage Passwords ? ☒

Edit Identity ? ☒

Create Identity ? ☒

View Identity ? ☒

Lifecycle Actions

Manager's Configuration (continued)

- Population request authority for managers is defined to allow managers to request items for their reports

Population Managers request authority*

☐ Make requests on anyone's behalf

☒ Define a population that this group of users can make requests for

Match Any ?

Share attributes with the requester ? ☐

Report to the requester ? ☒

☐ Directly

☒ Directly or indirectly

 ? Maximum Hierarchical Depth

Match custom criteria ? ☐

☐ ? Ignore IdentityIQ Scopes when selecting the population of Identities that this group of users can make requests for

LifeCycle Actions

Manager's Configuration (continued)

- Object Request Authority

- Defines objects available based on requestor and requestees
 - Roles
 - Applications
 - Managed Entitlement
- Rule Hooks
 - Provided rule options
 - Objects owned by the Requestor
 - Objects in Requestee's Assigned Scope
 - Objects in Requestee's Assigned Scope or Requestor's Controlled Scope
 - Objects in Requestor's Controlled Scopes
 - Can create own rules

Object request authority			
Roles ?	Objects in Requestor's Authorized Scopes	▼	...
Applications ?	Objects in Requestor's Authorized Scopes	▼	...
Managed Entitlements ?	All Objects	▼	...

What Can be Requested

Entitlements

- Controlled through Entitlement Catalog
- Requestable
 - Whether or not an entitlement may be requested through LCM
 - Available only when LCM is installed
 - Default = Requestable
- Owner
 - Drives entitlement approval process
- Description
 - Displayed in LCM

Edit Entitlement

Standard Properties

Members

Application Financials
Type Entitlement
Attribute groupmbr
Value AcctsPayable

Display Value

Requestable ☒

B **I** **U** |  

Description

0 of 1024 characters (including markup)

Owner

Scope

What Can be Requested

Roles

- Business Roles and Permitted IT Roles
 - Defined in Role Definition
 - Owner
 - Drives entitlement approval process
 - Description
 - Displayed in LCM
 - Default = Requestable

Request Roles Options

Choose which of the following role types are requestable for each type of request roles request. Any options unselected will be unavailable to any user attempting to make that type of request.

Role Type	My Actions	Others
Assignable Role	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Permitted Role	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

LCM Configuration – Business Processes

- Specify business process that performs action

The screenshot displays the 'Lifecycle Manager Configuration' interface. It features three tabs: 'Lifecycle Actions', 'Business Processes', and 'Additional Options'. The 'Business Processes' tab is active, showing a table with two columns: 'Action' and 'Business Process'.

Action	Business Process
Request Access	LCM Provisioning
Manage Accounts	LCM Provisioning
Manage Passwords	LCM Manage Passwords
Edit Identity	LCM Create and Update
Create Identity	LCM Create and Update
Self-service Registration	LCM Registration

A red box highlights the 'Request Access', 'Manage Accounts', 'Manage Passwords', 'Edit Identity', 'Create Identity', and 'Self-service Registration' actions in the table. A red line connects the 'Self-service Registration' action to a 'New User Registration' link in a 'Welcome to IdentityIQ' login screen. The login screen also includes fields for 'Username' and 'Password', and a 'Login' button.

Below the table, there are two sections: 'MANAGE ACCESS' and 'MANAGE IDENTITY'. The 'MANAGE ACCESS' section includes a shopping cart icon and the following links: 'Request Access', 'Manage Accounts', 'Change Passwords', and 'Track My Requests'. The 'MANAGE IDENTITY' section includes a user card icon and the following links: 'Create Identity', 'Edit Identity', and 'View Identity'.

LCM Configuration – Provisioning Policies

- Policy which gets evaluated if information is needed as part of the LCM request
- Typical usage
 - When roles or entitlements require an account to be created
 - Used for “Manage Accounts” requests when adding new accounts
- Three types
 - Identity
 - Role
 - Account (Create/Update/Delete)
- Provisioning policies support the creation of the necessary data or forms to support the creation/update or deletion of accounts

Provisioning Policy Configuration

- Identity Provisioning Policy
 - System Setup → Identity Provisioning Policies
 - Support for Create Identity and Edit Identity
 - Support for Self-service Registration
- Role Provisioning Policy
 - Define → Roles → <role> → Edit Role → Provisioning Policy
 - Support for Create
- Account Provisioning Policy
 - Define → Applications → Provisioning Policies
 - Support for Create, Update, and Delete Account

Provisioning Policy

- Calculate fields or prompt for input

Add Field		Remove Field	
<input type="checkbox"/> Name	Type		
<input type="checkbox"/> User DN	string		
<input type="checkbox"/> Password	secret		
<input type="checkbox"/> CN	string		
<input type="checkbox"/> SN	string		
<input type="checkbox"/> User Type	string		

Edit Provisioning Policy Fields

Field Properties

Name:

Display Name:

Help Text:

Type:

Multi-Valued: ☐

Read Only: ☒ Value ☐ Rule ☐ Script

Hidden: ☒ Value ☐ Rule ☐ Script

Owner: ☒ Requester ☐ Rule ☐ Script ☐ App Owner

Required: ☒

Review Required: ☐

Refresh Form on Change: ☐

Display Only: ☐

Authoritative: ☐

Value Properties

Value: ☐ Value ☐ Rule ☒ Script ☐ Dependent

Allowed Values: ☒ None ☐ Value ☐ Rule ☐ Script

Validation: ☒ None ☐ Rule ☐ Script

Overview of Additional LCM Options

LCM Additional Options

Controlling LCM Behavior – Highlights

Options	Control Search	Enable Features	Control Availability	Set Counts
General	✓	✓		✓
Request Roles	✓		✓	
Request Entitlements	✓		✓	✓
Create Identity		✓		✓
Manage Accounts		✓	✓	
Manage Password		✓		
Password Validation Rule		✓		
Batch Request Approver		✓		

General Options

Maximum size of bulk requests processed interactively 5

Filter searches by **Contains**

- ☐ Allow requesters to set request priorities
- ☒ Enable Account Group Management
- ☐ Enable Full Text Search
- ☒ Allow searching by Population when requesting access
- ☒ Allow searching by identity when requesting access
- ☐ Allow opt-in to viewing request access search result details
- ☐ Show external service request details

Maximum number of results returned in a Request Access search

Request Roles Options

Choose which role types are requestable for each type

Role Type	My Actions
Assignable Role	<input checked="" type="checkbox"/>
Permitted Role	<input checked="" type="checkbox"/>

☐ When searching for roles based on population, only return roles

Request Entitlements Options

☐ When searching for entitlements based on population, only return

Entitlement Search Results must return less than this number of id

Entitlement Search Results must return less than this number of en

Applications that support additional account requests

☐ All Applications

Create Identity Options

- ☒ Require password on all identity creation requests.
- ☒ Enable self-service registration.

Prevent pruning of new identities for this many days 30

Manage Accounts Options

☐ Show Enable/Unlock decision buttons regardless of whether the

Choose which actions are enabled for each type of manage accounts

Action	My Actions	Support
Delete	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Disable	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Enable	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Unlock	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Applications that support account only requests

☐ All Applications

Manage Password Options

- ☒ Enable password auto-generation when requesting for others

Password Validation Rule

Password Validation Rule **-- Select Rule --**

Batch Request Approver

- ☐ Require batch request approval

LCM Additional Options – Call Outs

■ Full text search

General Options

Maximum size of bulk requests processed interactively

Filter searches by

☐ Allow requesters to set request priorities

☒ Enable Account Group Management

☐ Enable Full Text Search

☒ Allow searching by Population when requesting access

☒ Allow searching by Identity when requesting access

☐ Allow opt-in to viewing request access search result details

☐ Show external service request details

■ Self-registration

Create Identity Options

☒ Require password on all identity creation requests.

☐ Enable self-service registration.

Prevent pruning of new identities for this many days

Lifecycle Actions | Business Processes | Additional Options

General Options

Maximum size of bulk requests processed interactively

Filter searches by

☐ Allow requesters to set request priorities

☒ Enable Account Group Management

☐ Enable Full Text Search

☒ Allow searching by Population when requesting access

☒ Allow searching by Identity when requesting access

☐ Allow opt-in to viewing request access search result details

☐ Show external service request details

Maximum number of results returned in a Request Access search

Request Roles Options

Choose which of the following role types are requestable for each type of request

Role Type	My Actions
Assignable Role	<input checked="" type="checkbox"/>
Permitted Role	<input checked="" type="checkbox"/>

☐ When searching for roles based on population, only return roles that are requestable

Request Entitlements Options

☐ When searching for entitlements based on population, only return entitlements that are requestable

Entitlement Search Results must return less than this number of identities

Entitlement Search Results must return less than this number of request details

Applications that support additional account requests

☐ All Applications

Create Identity Options

☒ Require password on all identity creation requests.

☐ Enable self-service registration.

Prevent pruning of new identities for this many days

Manage Accounts Options

☐ Show Enable/Unlock decision buttons regardless of whether the user is an administrator

Choose which actions are enabled for each type of manage accounts

Action	My Actions	System Actions
Delete	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Disable	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Enable	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Unlock	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Applications that support account only requests

☐ All Applications

Manage Password Options

☒ Enable password auto-generation when requesting for others

Password Validation Rule

Password Validation Rule

Batch Request Approver

☐ Require batch request approval

LCM Full Text Search (6.0)

■ Benefits

- Faster searching
 - Particularly helpful for large environments (i.e. 50 million entitlements)
- Search by entitlement descriptions and more
 - Default search fields
 - Entitlements: displayName, description, and application.name
 - Roles: name, displayName, and description
 - Extend indexed searching to additional fields

■ Two steps to enable

- Set LCM option *Enable Full Text Search*
 - System Setup → Lifecycle Manager Configuration → Additional Options
- Run task
 - Full Text Index Refresh

LCM Full Text Search Engine

Index Details

- Full Text Index Refresh task details
 - Builds full-text indexes for roles and entitlements
 - Schedule for regular updates
- Index File Location
 - Two Directories store the index
 - Entitlement Catalog Index
 - [IdentityIQ installation directory]\WEB-INF\BundleIndex
 - Role Index
 - [IdentityIQ installation directory]\WEB-INF\ManagedAttributeIndex
 - Can write to a different location
 - set indexPath in your FullTextIndex XML object
 - File is written to the host where the task runs
 - Needs to be shared to UI Tier servers
 - Write to known location shared across all servers

How to Extend Full Text Search

- **FullTextIndex object**
 - One each for Managed Attributes and Bundles
 - Can be used to configure what is indexed by engine
- **Add FullTextField objects to your FullTextIndex**
 - **Field Options**
 - **Analyzed** (use this option to include field in full text search)
 - Field broken up and indexed for full text search with substring matching
 - **Indexed**
 - Enables field to be used in advanced filters on access request page
 - **Stored**
 - Enables the field to return in the search results
 - **Ignored**
 - Field is not used in full text searching or filtering

```
<FullTextField name='application.securityLevel' analyzed='true' indexed='true'/>
```

FullTextIndex XML Object

```
<?xml version='1.0' encoding='UTF-8'?>
<!DOCTYPE FullTextIndex PUBLIC "sailpoint.dtd" "sailpoint.dtd">
<FullTextIndex created="1346076712810" id="4028818239686c4f0139686c9f6900e7" name="Bundle">
  <Attributes>
    <Map>
      <entry key="fields">
        <value>
          <List>
            <FullTextField analyzed="true" indexed="true" name="name"/>
            <FullTextField analyzed="true" indexed="true" name="displayableName"/>
            <FullTextField analyzed="true" name="description"/>
            <FullTextField indexed="true" name="assignedScope.path"/>
            <FullTextField indexed="true" name="type"/>
            <FullTextField name="defaultDescription" stored="true"/>
            <FullTextField ignored="true" name="disabled"/>
            <FullTextField name="riskScoreWeight" stored="true"/>
            <FullTextField indexed="true" name="owner.id"/>
            <FullTextField name="owner.name"/>
            <FullTextField name="owner.displayName" stored="true"/>
            <FullTextField name="division" analyzed="true" indexed="true">
          </List>
        </value>
      </entry>
      <entry key="indexPath" value="/home/spadmin/tomcat/webapps/identityiq"/>
    </Map>
  </Attributes>
</FullTextIndex>
```


LCM – Enabling Self-service Registration

- Enabling
 - System Setup → Lifecycle Manager Configuration → Additional Options
 - Set Enable self-service registration
 - Once enabled, it runs out-of-the-box
- `spadmin` is default approver

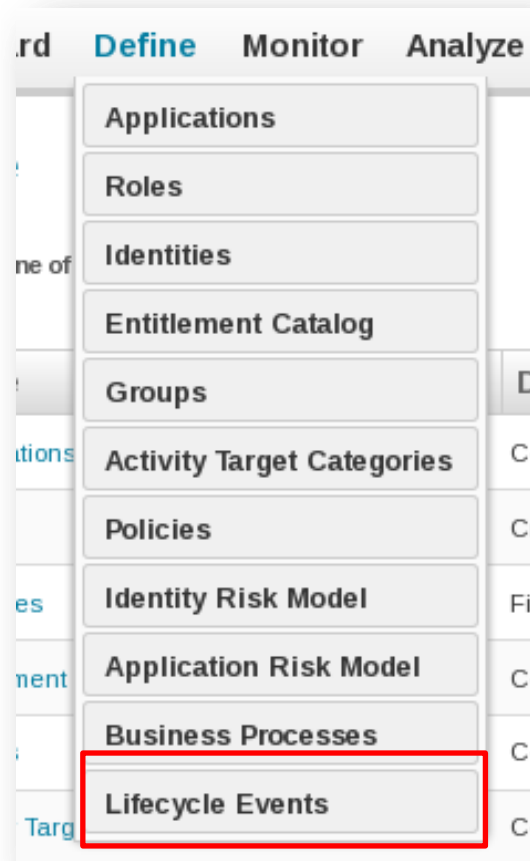
LCM – Modifying Self-Service Registration

- Many workflow process variables for controlling the approval and notification process
 - For example, override default approver
 - Set **securityOfficerName** to approver
- Workflow details
 - System Setup → Lifecycle Manager Configuration → Business Processes
 - Default workflow: LCM Registration
- Extension options
 - Extend Provisioning Policy
 - System Setup → Identity Provisioning Policies
 - Extend or replace workflow

Configuring LCM Events

LCM Event Configuration

- Define → Lifecycle Events
- Configure which events begin which process



LifeCycle Events

- Identity events trigger Business Processes (workflows)

Lifecycle Events

Lifecycle Events

Filter by Lifecycle Event Name



Add New Lifecycle Event

Name ▴	Type	Attribute Name	Owner	Disabled
Department Transfer	Attribute Change	Department	The Administrator	No
Joiner	Create			Yes
Leaver	Attribute Change	Inactive		
Manager transfer	Manager Transfer			
Reinstate	Attribute Change	Inactive		

Lifecycle Event

Lifecycle Event Options

Name ? Joiner

Description ? Process a new employee.

Event type ? Create

Disabled ? ☒

Included Identities ? ☒ All ☐ Match List ☐ Filter ☐ Sc

Behavior

Business Process ? Lifecycle Event - Joiner

LifeCycle Events

- LifeCycle event can be created based on:
 - Attribute Change
 - Manager Change
 - Create
 - Native Change
 - Rule (Rule type = IdentityTrigger)
- Lifecycle events occur
 - During Identity Refresh - check “Process Events” during identity refresh
 - When editing the Attributes directly through GUI (mark attributes as “editable”) – Useful for testing

Lifecycle Events – Multiple instances

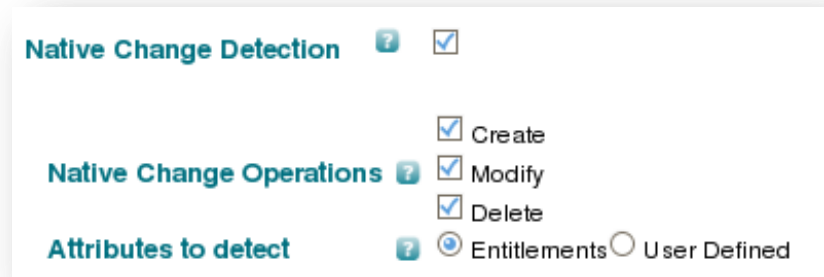
- Multiple events can be created for same “type” of event
 - Example:
 - Joiner events – One for Contractors, one for Employees
 - Configured based on an Included Identities list
 - Attribute-Based
 - Identity Attributes
 - Application Account Attributes
 - Filter
 - Script
 - Rule
 - Populations

Native Change Detection – Overview


- Native-change detection
 - Detects access changes that occur natively on an application
 - Runs a Business Process in response to the changes
- Best Practices
 - Aggregate all accounts without native change detection
 - Turn on native change detection
- Built In Workflows
 - Lifecycle Event - Manager Approval for all native changes
 - Creates work item for manager
 - Asks whether to keep or revoke native changes
 - Provisions based on decision
 - Lifecycle Event - Email manager for all native changes
 - Will send email to manager to notify them of any native changes
- Custom Workflow


Native Change Detection – Configuration


- Turn on native change detection per Application
- Create a Native Change Lifecycle Event



This screenshot shows the configuration for Native Change Detection. It includes a toggle for 'Native Change Detection' which is checked. Below it, 'Native Change Operations' are configured with checkboxes for 'Create', 'Modify', and 'Delete', all of which are checked. The 'Attributes to detect' section has radio buttons for 'Entitlements' (selected) and 'User Defined'.

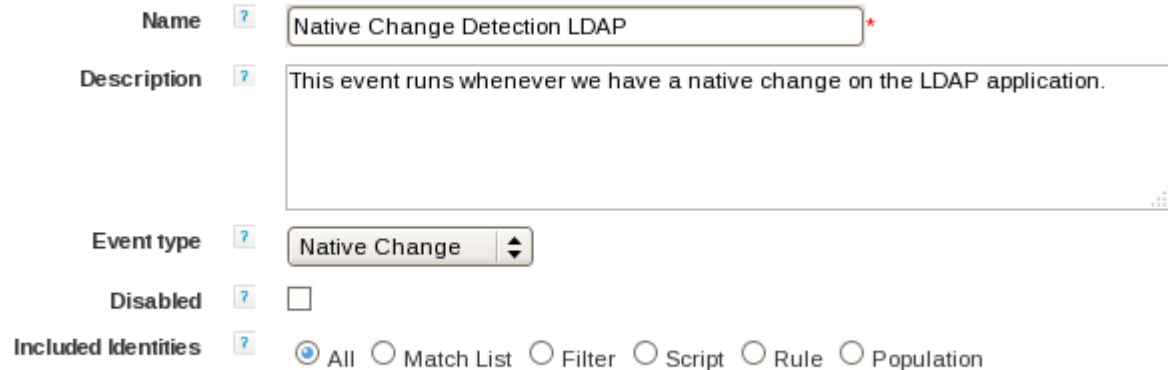
Native Change Detection  ☒

Native Change Operations  ☒ Create ☒ Modify ☒ Delete


Attributes to detect  ☒ Entitlements ☐ User Defined


Lifecycle Event


Lifecycle Event Options





This screenshot shows the configuration for a Lifecycle Event. The 'Name' field is 'Native Change Detection LDAP'. The 'Description' field contains the text 'This event runs whenever we have a native change on the LDAP application.' The 'Event type' dropdown is set to 'Native Change'. The 'Disabled' checkbox is unchecked. The 'Included identities' section has radio buttons for 'All' (selected), 'Match List', 'Filter', 'Script', 'Rule', and 'Population'.

Name  Native Change Detection LDAP *

Description  This event runs whenever we have a native change on the LDAP application.

Event type  Native Change

Disabled  ☐

Included identities  ☒ All ☐ Match List ☐ Filter ☐ Script ☐ Rule ☐ Population

Behavior



This screenshot shows the 'Business Process' configuration, which is set to 'Lifecycle Event - Manager Approval for all native changes'.

Business Process  Lifecycle Event - Manager Approval for all native changes

Native Change Detection – Operation

- Run Identity Refresh with “Process Events” checked



Summary


Work Item ID 174
Requester Scheduler
Owner Sara.Berry
Description Native Account Changes for User: Allen.Burton - Manager Approval
Created Jan 30, 2014 12:56:55 PM
Priority Normal
History None





Details

Detected Native Change(s)


The following Modify native change(s) were detected during the last aggregation scan.
To accept a native change, click the Approve icon in the decision column.
Otherwise, click the Reject icon for any items you want reverted.
Once all decisions have been made click complete, any approved items will be kept and any rejected items will be reversed.

Legend:  Approve  Reject

Search: **Filter by Decision** 

<input type="checkbox"/>	Decision	Application	Account Name	Operation	Attribute	Value(s)	Completion	Comments
<input type="checkbox"/>	 	LDAP	Allen.Burton	Add	groups	Managers 		

50

 SailPoint

Additional LCM Functionality

Additional LCM Functionality Overview

- Extending the dashboard
 - Quicklinks
- Attribute synchronization
- Password interception
- Batch requests

Extending the Dashboard

Quick Links (6.0)

- Dashboard quick links allow for the extension of the standard LCM operations
 - Launch workflows
 - Link to specific areas of the UI
 - Link externally
- Configuration supports
 - Granular access control (i.e. who sees the quick link) (6.2)
 - Categories to allow for grouping
 - Counting and displaying counts for objects
 - Calculating and passing values into workflows
 - Custom icons

COMPLIANCE ACTIVITIES



Access Reviews (1)
Policy Violations (0)

ASSIGNED TASKS



Approvals (0)
Sign-off Reports (0)
Work Items (1)

MANAGE ACCESS



Request Access
Manage Accounts
Change
Passwords
Track My Requests

MANAGE IDENTITY



Create Identity
Edit Identity
View Identity

ADMIN TOOLS



Edit Email
Template
Debug

Extending the Dashboard

Quick Link Objects

- Quick link configuration
 - QuickLink object (6.2)
 - SystemConfig object
- User access control
 - DynamicScope object (6.2)
 - IdentitySelector
 - Inclusion/exclusion list
 - Default DynamicScope object = Everyone
 - LCM populations
- Category definitions
 - SystemConfig object

QuickLinks at a glance

■ QuickLinks

- name – Unique name
- messageKey – UI display or message key name
- Category – Section where it should display in the UI
- action
 - “workflow”
 - using a from-outcome from faces-config.xml (example: editApplication)
 - external
- enabled
- hidden

■ Additional items

- countScript
 - Script to return item count
- displayCount
 - true/false
- workflowName
 - if action = “workflow”, workflow to execute
- workflowSuccess
 - if action = “workflow” and workflow launches okay, display this message

QuickLink to Launch a Workflow

```
<QuickLink action="workflow" category="Custom" enabled="true" messageKey="Run A Process" name="RunAProcess">
```

```
<Attributes>
```

```
<Map>
```

```
<entry key="identityName">
```

```
<value>
```

```
<Script>
```

```
<Source>
```

```
return currentUser.getName();
```

```
</Source>
```

```
</Script>
```

```
</value>
```

```
</entry>
```

```
<entry key="workflowName" value="A Form"/>
```

```
<entry key="workflowSuccess" value="A Form Executed Successfully"/>
```

```
</Map>
```

```
</Attributes>
```

```
<DynamicScopes>
```

```
<Reference class="sailpoint.object.DynamicScope" name="SystemAdministrator"/>
```

```
</DynamicScopes>
```

```
</QuickLink>
```

This quicklink
launches a workflow

Entry keys can be
used to inject
workflow variables

Name of workflow to
execute

Reference to DynamicScope
object controlling who can access

Value to display when
workflow is executed (can be
localized using message key)

Dynamic Scoping

Limiting Access by Capability

- Define Dynamic Scopes

```
<DynamicScope name="Compliance Officers">  
  <Selector>  
    <IdentitySelector>  
      <MatchExpression>  
        <MatchTerm name="capabilities" value="ComplianceOfficer"/>  
      </MatchExpression>  
    </IdentitySelector>  
  </Selector>  
</DynamicScope>
```

Attribute Synchronization – Overview

- **Attribute synchronization**
 - Automatically syncs changes to identity attributes with downstream systems
- **Identity Attributes**
 - Allow source mappings and target mappings (v6.0+)
- **Configuration**
 - Identity Mappings
 - Identity Refresh Task

Attribute Synchronization – Configuration

- System Setup → Identity Mappings
 - Application and Attribute to “target” with any changes
 - Optional Transformation Rule
 - Configuration option to push change to all accounts if user has more than one
 - Default, we create a workitem and ask the user to choose or ask the user immediately if they are making a change via UI

The screenshot displays the 'Source Mappings' and 'Target Mappings' sections of the SailPoint Identity Manager configuration interface. The 'Source Mappings' section lists two sources: '1. Email from the HR System' and '2. Email from the Contractor F'. Below this list are buttons for 'Add Source' and 'Delete Source'. The 'Target Mappings' section is currently empty, with buttons for 'Add Target' and 'Delete Target'. The 'Add Target' button is highlighted with a red box. A modal dialog titled 'Add a target to the email attribute' is open, showing configuration options for a new target. The dialog includes fields for 'Application' (set to 'LDAP'), 'Attribute' (set to 'mail'), 'Transformation Rule' (set to '- Select Rule -'), and a checked checkbox for 'Provision All Accounts'. The 'Add' button at the bottom right of the dialog is also highlighted with a red box.

Source Mappings

1. Email from the HR System
2. Email from the Contractor F

Target Mappings

Add a target to the email attribute

Application ? LDAP

Attribute ? mail

Transformation Rule ? - Select Rule -

Provision All Accounts ? ☒

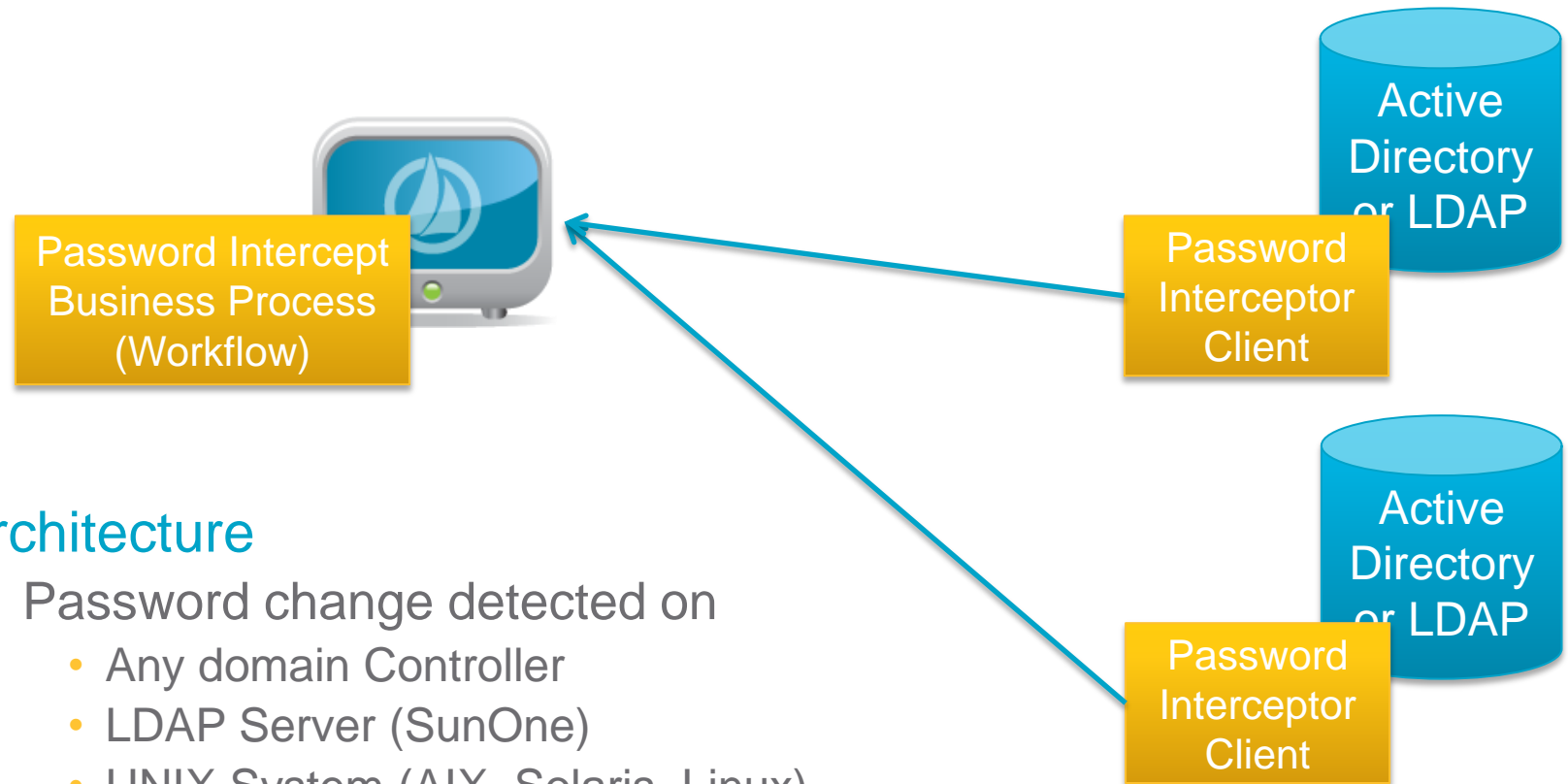
Save Cancel Add Cancel

Attribute Synchronization – Operation

- Edit identity
 - Define → Identity or LCM → Edit Identity
 - Either method will immediately invoke provisioning to target mapping(s)
- Identity Attribute change due to aggregation
 - Identity Refresh Task is required to Synchronize Attributes (check option shown here)

Refresh role metadata for each identity	?	<input type="checkbox"/>
Synchronize attributes	?	<input type="checkbox"/>
Refresh the identity risk scorecards	?	<input type="checkbox"/>

Password Interception



■ Architecture

- Password change detected on
 - Any domain Controller
 - LDAP Server (SunOne)
 - UNIX System (AIX, Solaris, Linux)
- Using configuration, Password Interceptor Client sends password change to IdentityIQ
- IdentityIQ runs configurable Business Process (Workflow)

Password Interception – Configuration

- Password Interception Support
 - Active Directory
 - LDAP (SunONE)
- Configuration
 - Follow instructions from install guide to setup AD or LDAP Password Interception Client
 - Configure Password Intercept Business Process
 - System Setup → IdentityIQ Configuration → Miscellaneous
 - Out-of-the-Box Process is provided

Business Processes

Entitlement Update	?	Entitlement Update	▲▼
Password Intercept	?	Password Intercept	▲▼

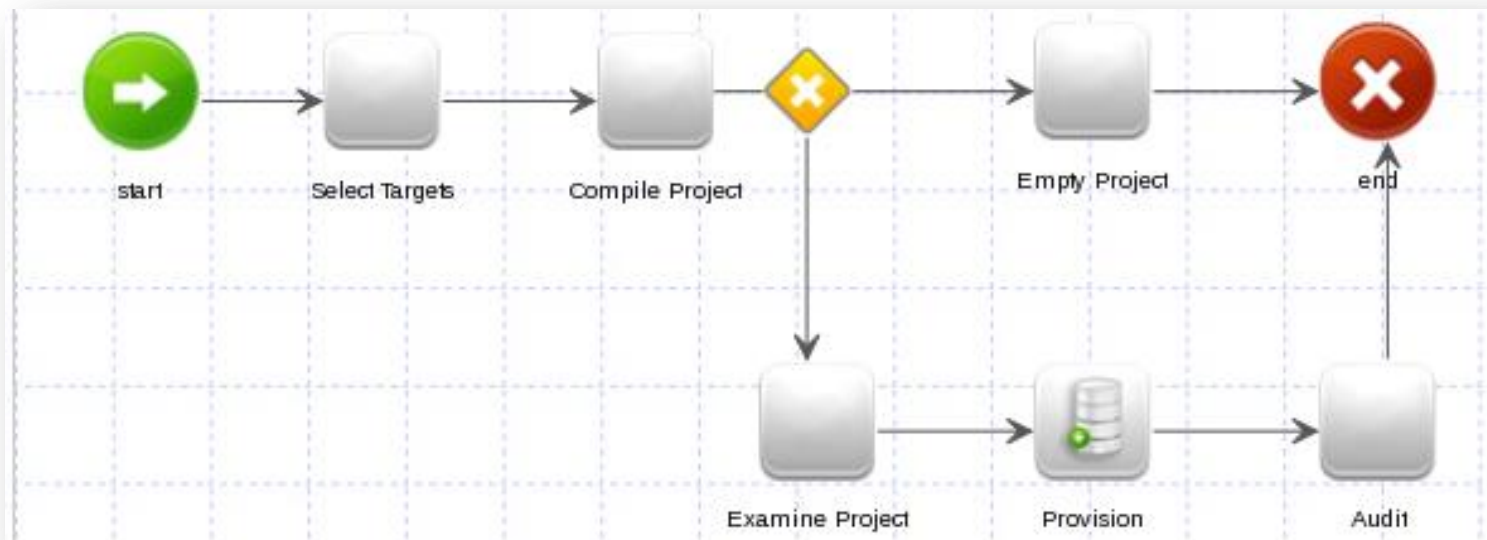
Password Interception – Workflow

■ Customization

- Determine which applications to sync passwords to: All or List of Applications
- Create a custom workflow

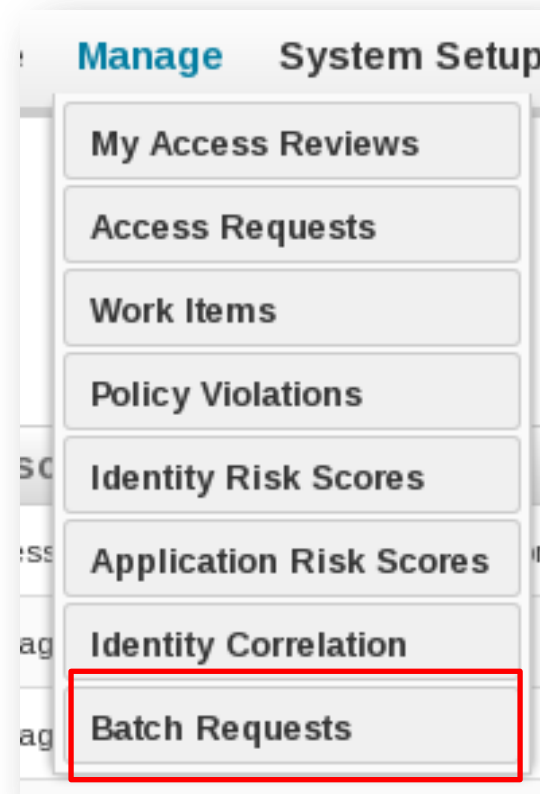
■ Out of the Box Workflow

- Input Variables
 - targetApplications - (CSV or List(String) of Application names)
 - Hardcode in initializer
 - Calculate application names in workflow step (script, call, etc)
 - applicationName – Which application detected the password change
 - syncAll – (true/false) – Whether to sync all password attributes for all supported applications



Batch Request

- **Batch request management**
 - Allows mass change requests to be processed via a file upload
- **Operations Supported**
 - Create/Modify Identity
 - Create/Delete Account
 - Enable/Disable Account
 - Unlock Account
 - Add/Remove Role
 - Add/Remove Entitlement
 - Change Password



Batch Request – Configuration

Create Batch Request

Choose batch file: ?

(Please refer to online help for batch file formatting details.)

Error handling: ?

- ☒ Ignore errors
☐ Stop on errors

Policy option: ?

- ☒ Disable policy checking
☐ Fail on any policy violation

Schedule to run: ?

- ☒ Run now
☐ Run later

Manual input: ?

- ☒ Skip requests that generate provisioning forms
☐ Create provisioning forms

Work items: ?

- ☒ Skip requests that create work items
☐ Create work items

Handle create identity as modify if identity exists: ?

☒

Generate identity requests: ?

☐

Batch Request – Primary Approver

- Approver for batch requests
 - System Setup → LCM Configuration → Additional Options

Batch Request Approver

☒ Require batch request approval

Identity responsible for approving batch requests:

The Administrator



Batch Request – Examples

- Example:

operation, name, location, email, department

CreateIdentity, Alex Smith, Austin, asmith@adept.com, Accounting

CreateIdentity, Bob Smith, Austin, asmith@adept.com, Engineering

CreateIdentity, Mark Smith, Austin, asmith@adept.com, Accounting

CreateIdentity, John Smith, Austin, johnsmith@adept.com, Finance

operation, name, location, email, department

ModifyIdentity, Alex Smith, Austin, asmith@adept.com, Accounting

ModifyIdentity, Bob Smith, Austin, asmith@adept.com, Engineering

ModifyIdentity, Mark Smith, Austin, asmith@adept.com, Accounting

ModifyIdentity, John Smith, Austin, johnsmith@adept.com, Finance

- Documentation

- For full documentation of how to use Batch Requests refer to the *Users Guide*

Questions?

Exercise Preview

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

- Exercise 1: Enabling Lifecycle Manager
- Exercise 2: Turn on Group Provisioning and Create New Group in LDAP
- Exercise 3: Provision VPN Access Using Lifecycle Manager
- Exercise 4: Create and Manage Identities in IdentityIQ
- Exercise 5: Account Management with Lifecycle Manager