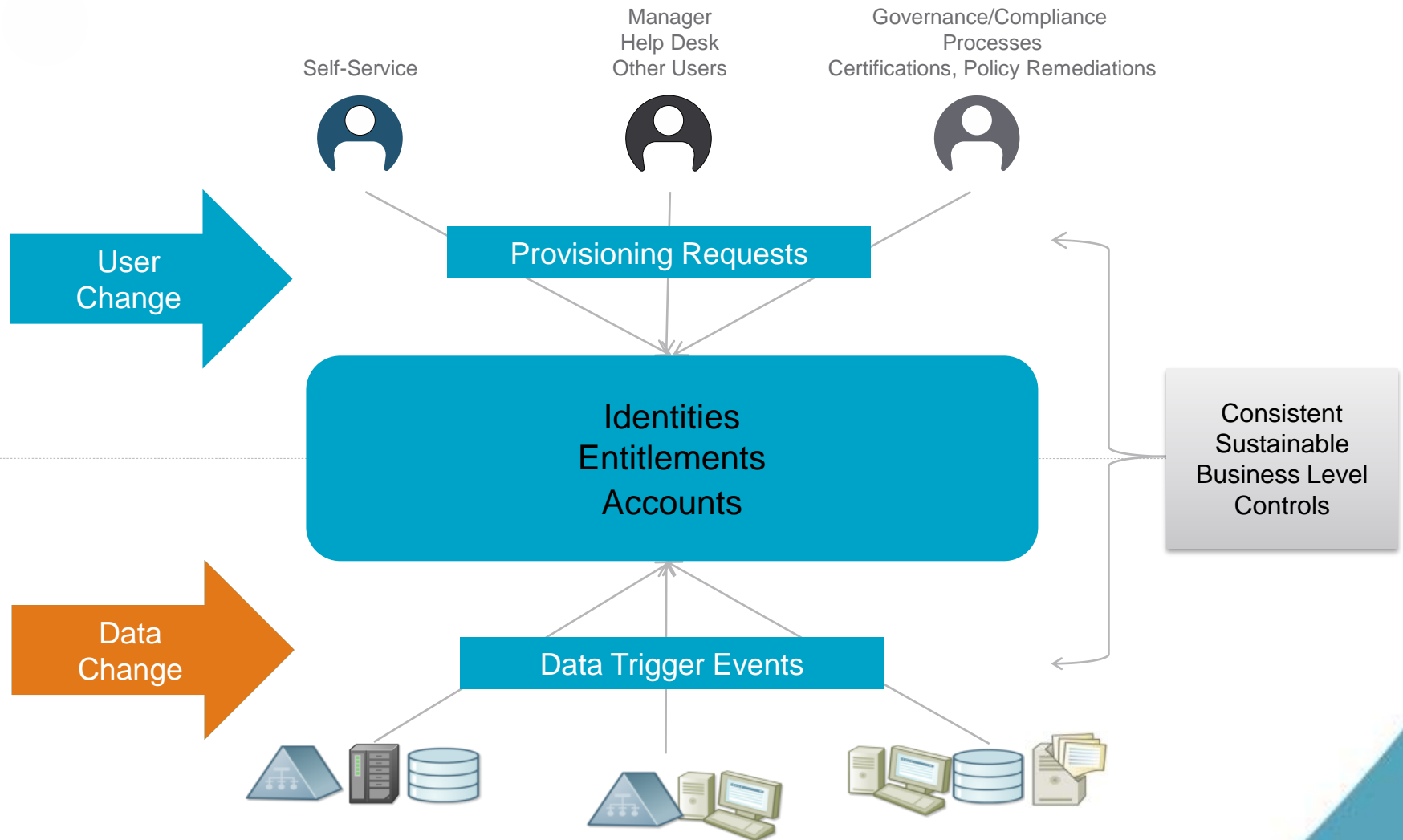# Additional LCM Functionality Overview

- Lifecycle Events
  - Date driven changes
  - Native change detection
- Account Group Provisioning
  - Create account groups
  - Update account groups
- Attribute synchronization
- Password interception
- Batch requests

Lifecycle Events

Identity Change Lifecycle
Review

Self-Service

Manager
Help Desk
Other Users

Governance/Compliance
Processes
Certifications, Policy Remediations

User Change

Provisioning Requests

Identities
Entitlements
Accounts

Consistent
Sustainable
Business Level
Controls

Data Change

Data Trigger Events

Key Features
Review

- User-driven Changes: LifeCycle Requests
    - Who can make what kinds of requests for whom?
    - What workflow should run to fulfill the request?

- Data-driven Changes: Lifecycle Events
    - What data changes should be watched as trigger?
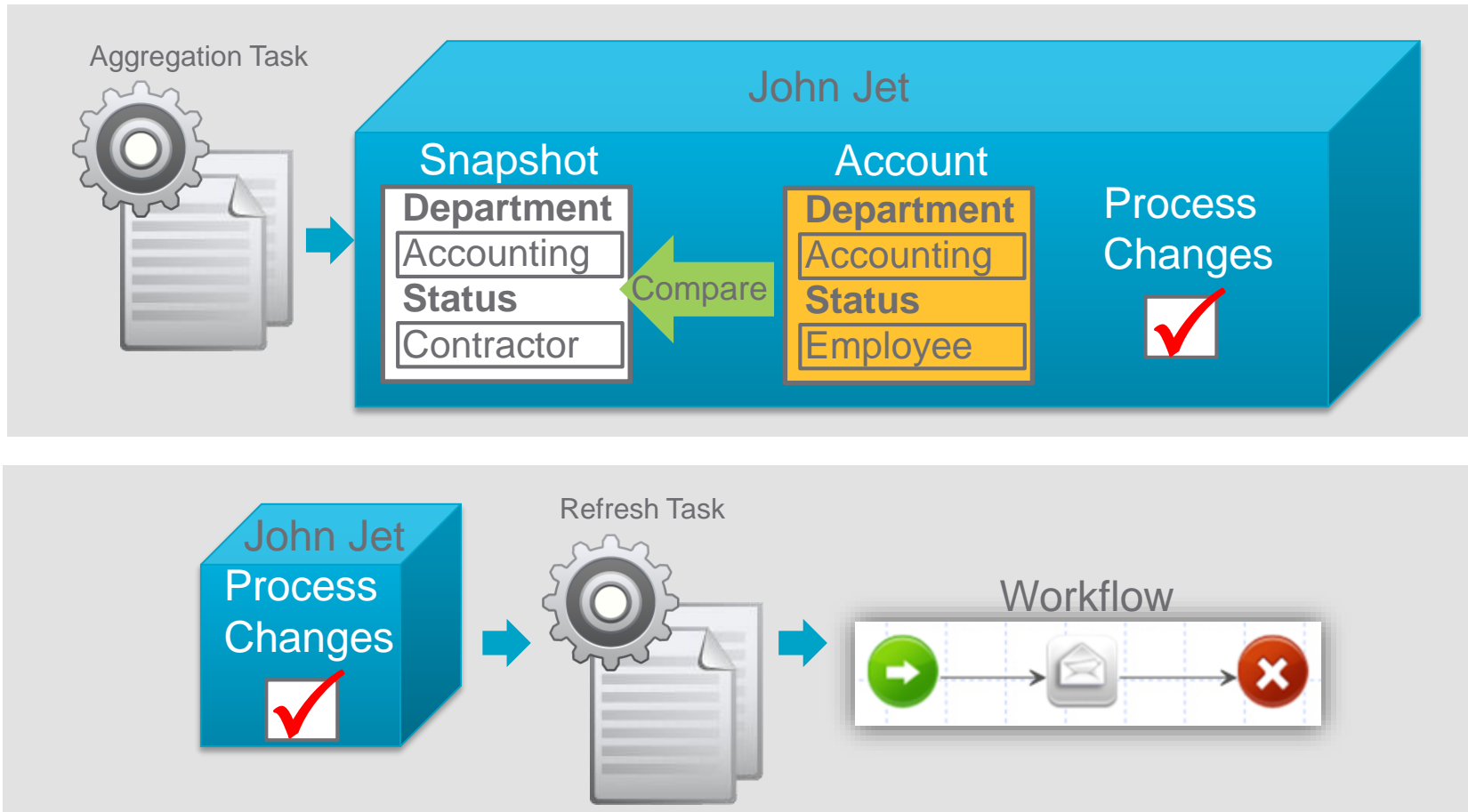   - What workflows should run in response?
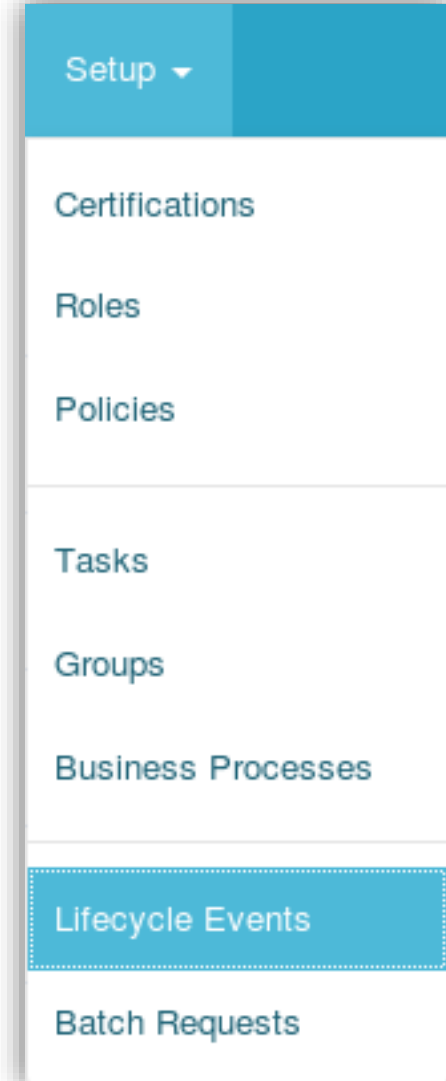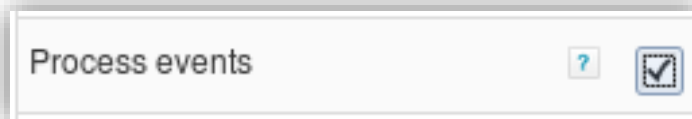
Lifecycle Event
Overview

Aggregation Task

John Jet

Snapshot

Department
Accounting
Status
Contractor

Compare

Account

Department
Accounting
Status
Employee

Process
Changes
✓

John Jet

Process
Changes
✓

Refresh Task

Workflow

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

  Process events [?] ☑

  - When editing attributes directly through GUI
    - Mark attributes as "editable" – useful for testing

Setup ▾

Certifications

Roles

Policies

Tasks

Groups

Business Processes

Lifecycle Events

Batch Requests

LifeCycle Event
Configuration

Lifecycle Events

Lifecycle Events

Filter by Lifecycle Event Name	🔍	**Add New Lifecycle Event**

Name ▲	Type	Attribute Name	Owner	Disabled
Department Transfer	Attribute Change	De...		
Joiner	Create			
Leaver	Attribute Change	Ina...		
Manager transfer	Manager Transfer	De...		
Reinstate	Attribute Change	Ina...		

Lifecycle Event Options

Name*	?	Joiner
Description	?	Process a new employee.
Event type	?	Create
Disabled	?	☑
Included Identities	?	All

Behavior

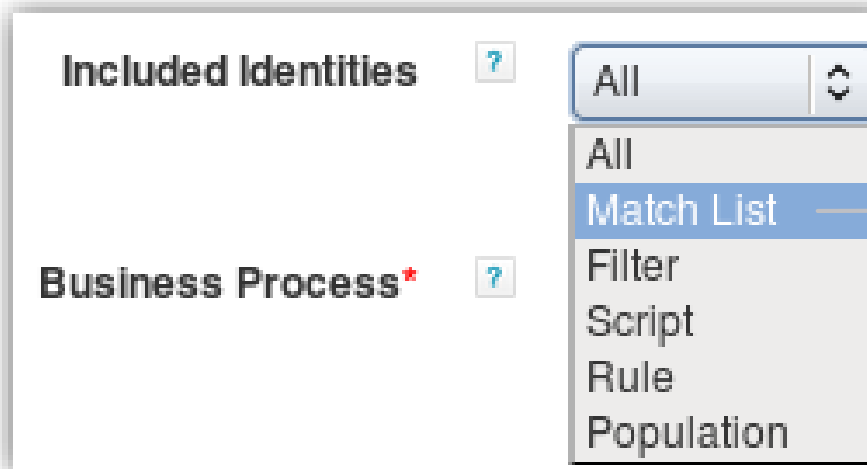|		
Business Process*	?	Lifecycle Event - Joiner

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 a list of identities to include

Included Identities [?]   All [⌄]

All
Match List ——— Identity Attributes
Filter   Application Account Attributes
Business Process* [?]
Script
Rule
Population

Native Change Detection

Native Change Detection
Overview

- ## Native-change detection
  - Detect account changes that occur natively on an application

- ## Response Options
  - Automatically start a certification (LCM not required)
    - Setup→Certifications→Certification Events→Add New Certification Event
  - Lifecycle Event
    - Provided workflows
      - Manager approval for all native changes
      - Email manager for all native changes
    - Custom workflow

- ## Best Practices
  - Aggregate all accounts without native change detection, then turn on native change detection
  - Process changes regularly

Native Change Detection
Configuration

- Configure native change detection per application
- Create a Native Change Lifecycle Event

Application

Native Change Detection [?] ☑

Native Change Operations [?] ☑ Create
☑ Modify
☑ Delete

Attributes to detect [?] ⦿ Entitlements ○ User Defined

Lifecycle Event Options

Name* [?] Native Change Detec...

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

Event type [?] Native Change ⬍

Disabled [?] ☐

Included Identities [?] All ⬍

Behavior

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: OK Approve ⊖ Reject

Search: Filter by Decision ⌄

	Decision	Application	Account Name	Operation	Attribute	Value(s)	Completion Comments
☐	OK ⊖	LDAP	Allen.Burton	Add	groups	Managers ?	⊕

Account Group Provisioning

Account Group Provisioning
Overview

IdentityIQ

Application

Define Group
VPN

Workflow

New Group

Group
VPN

SailPoint

Account Group Provisioning

Configuration

Lifecycle Manager

Configure	Business Processes	Identi...

General Options

Filter searches by [Starts With ◇]

☐ Allow requesters to set request prioriti...

☑ Enable Account Group Management

1 Enable group provisioning

Application

Details	**Configuration**	Correlation	Accounts
Settings	Schema	**Provisioning Policies**	

Object Type: group

Type	Name
Create	group create
Update	edit group

2 Configure group Create and Update

Entitlement Catalog

[ldap | ✖ | 🔍] [Advanced Search]   [Import] [Export] [**Add New Entitlement**]

Application ▾	Attribute	Display Name	Type	Description	Owner	Requestable
LDAP	groups	Users	group	All users at the		✅

Click to edit

3 Create New

Attribute Synchronization

SailPoint

Attribute Synchronization

Overview

- Attribute synchronization
  - Automatically synchronizes changes to identity attributes with downstream systems
- Identity Attributes
  - Allow source mappings and target mappings
- Configuration
  - Identity Mappings
  - Identity Refresh Task

Attribute Synchronization

Configuration

- Add target mappings for attributes to synchronize
    - System Setup → Identity Mappings
- Options
    - Transformation rule
    - Push change to all accounts if user has more than one

Attribute Synchronization
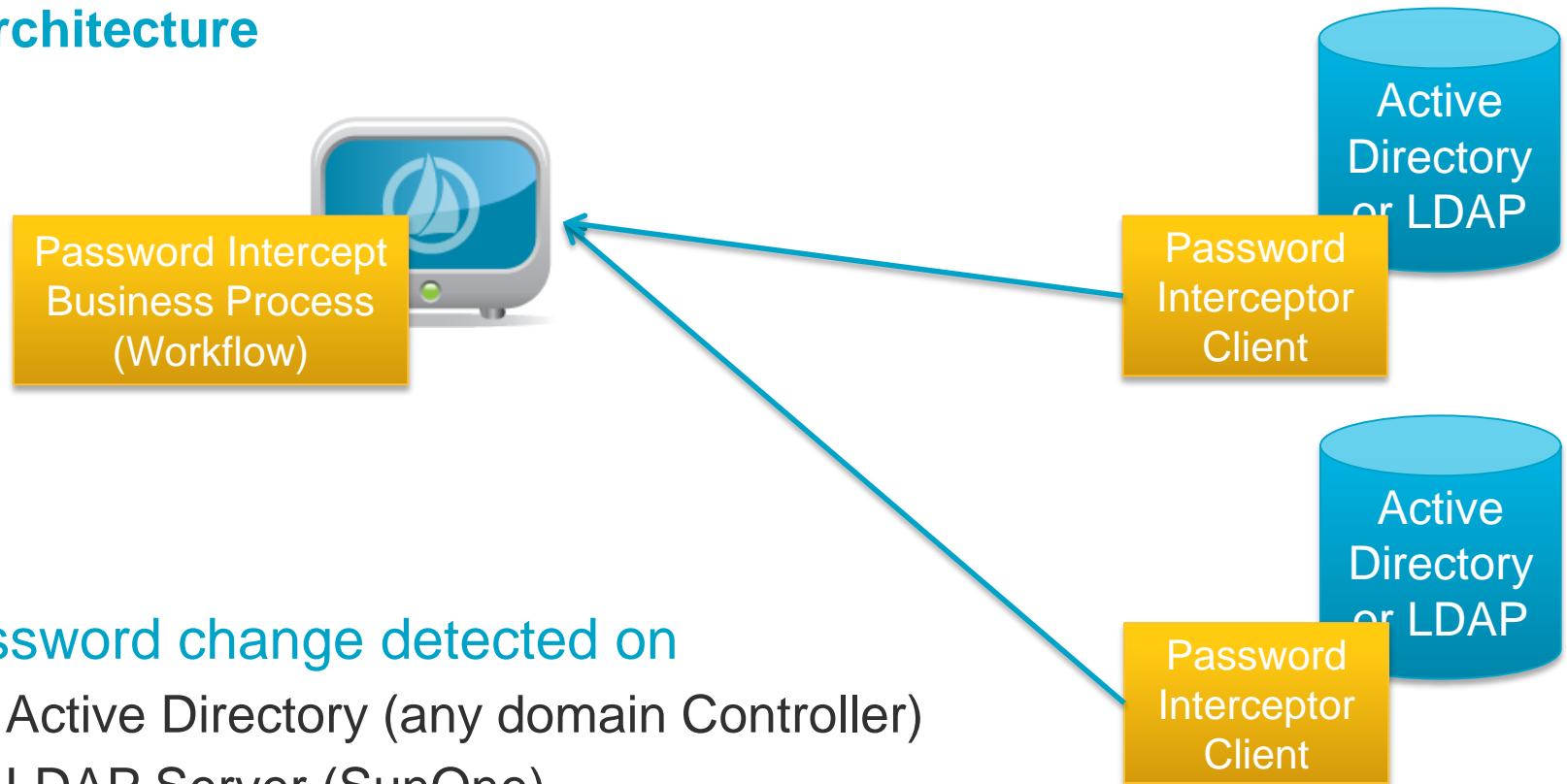## Operation

- Edit identity
  - LCM: Manage Identity → Edit Identity
  - Immediately invoke provisioning to target mapping(s)
- Aggregate changed identity attribute
  - Synchronize with Identity Refresh Task

Enable manual account selection	?	☐
Synchronize attributes	?	☑
Refresh the identity risk scorecards	?	☐

Password Interception

Password Interception

Architecture

Password Intercept Business Process (Workflow)

Password Interceptor Client

Active Directory or LDAP

Password Interceptor Client

Active Directory or LDAP

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

Password Interception
Configuration

- Install interceptor client
  - Instructions: Direct Connectors Admin & Config guide
- Configure Password Intercept business process
  - Global Settings→IdentityIQ Configuration→Miscellaneous
  - Options
    - Sync to all applications that support password updates (default)
   - Specify target applications

Identity Batch Processing

Identity 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

Setup ▾

Certifications

Roles

Policies

Tasks

Groups

Business Processes

Lifecycle Events
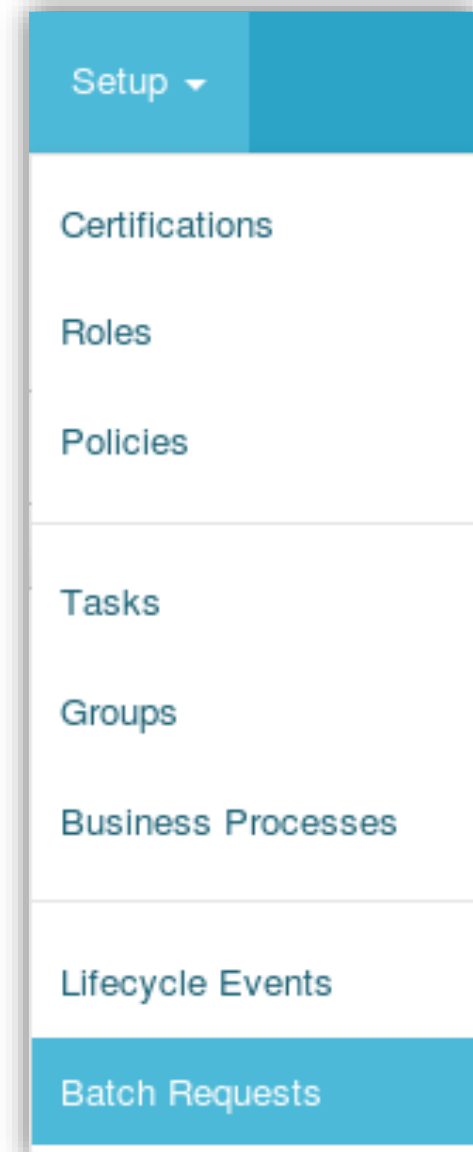
Batch Requests

Batch Request

Data Format Examples

- Examples:

```
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
    - *Users Guide*

Questions?

SailPoint

Exercise Preview

Section 4, Exercises 4 & 5

- Exercise 4: Turn on Group Provisioning and Create New Group in LDAP
- Exercise 5: Provision VPN Access Using Lifecycle Manager