User Driven Access Changes

Lifecycle Manager, Part 1

Fundamentals of IdentityIQ Implementation

IdentityIQ 7.0

SailPoint

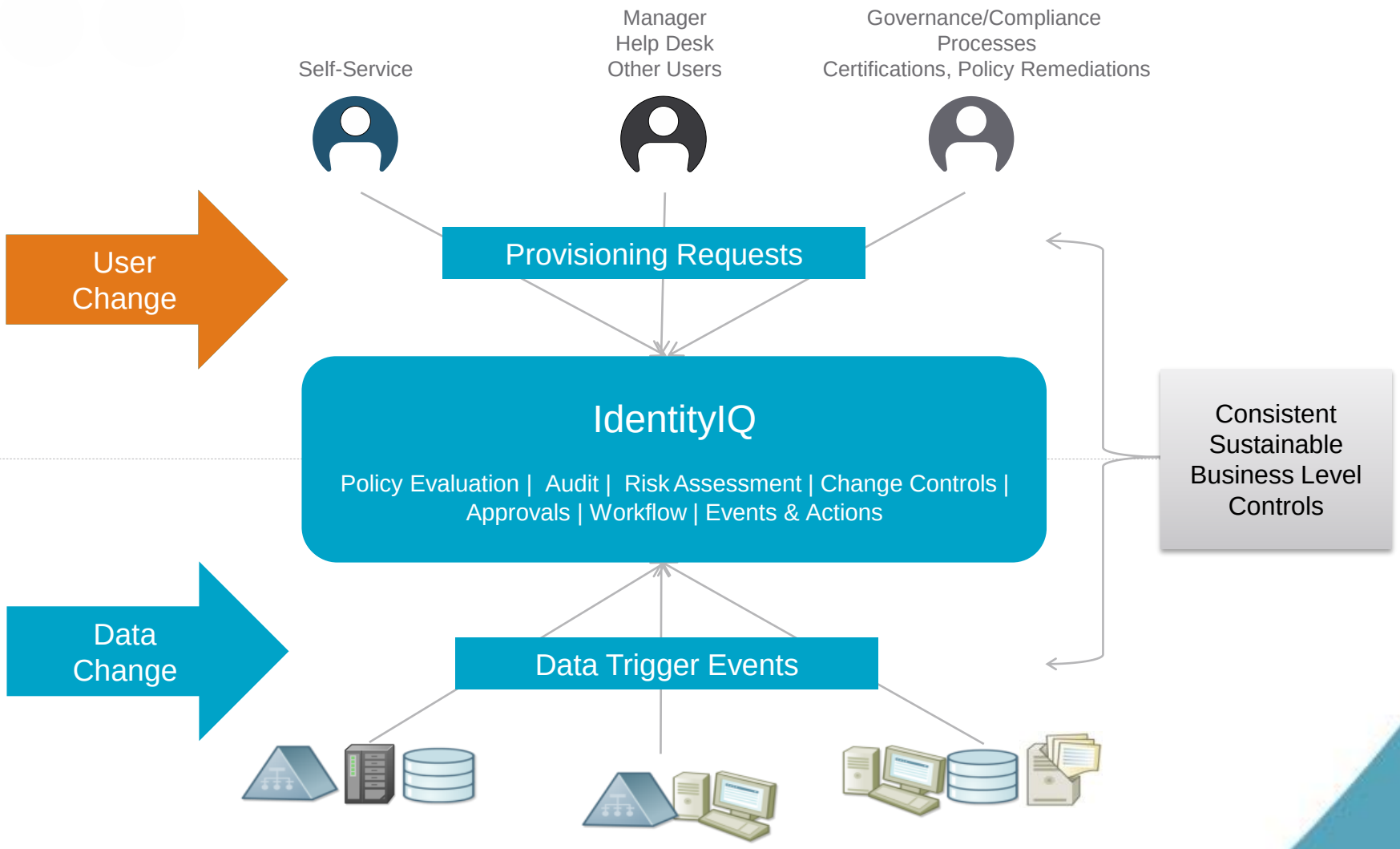
Overview

User Driven Access Changes

- Identity change lifecycle
- Key considerations
- Access request process
  - Requesting entitlements and roles
  - Requesting account, password, and Identity Cube changes
- Configuring access requests
  - Configuring quicklink populations
  - Configuring role and entitlement requests
  - Configuring account requests
- LCM Actions and their associated Business Processes
- Configuring provisioning policies

SailPoint Copyright © SailPoint Technologies, Inc. 2015 All rights reserved.

Identity Change Lifecycle



SailPoint Copyright © SailPoint Technologies, Inc. 2015 All rights reserved.

Key Considerations

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

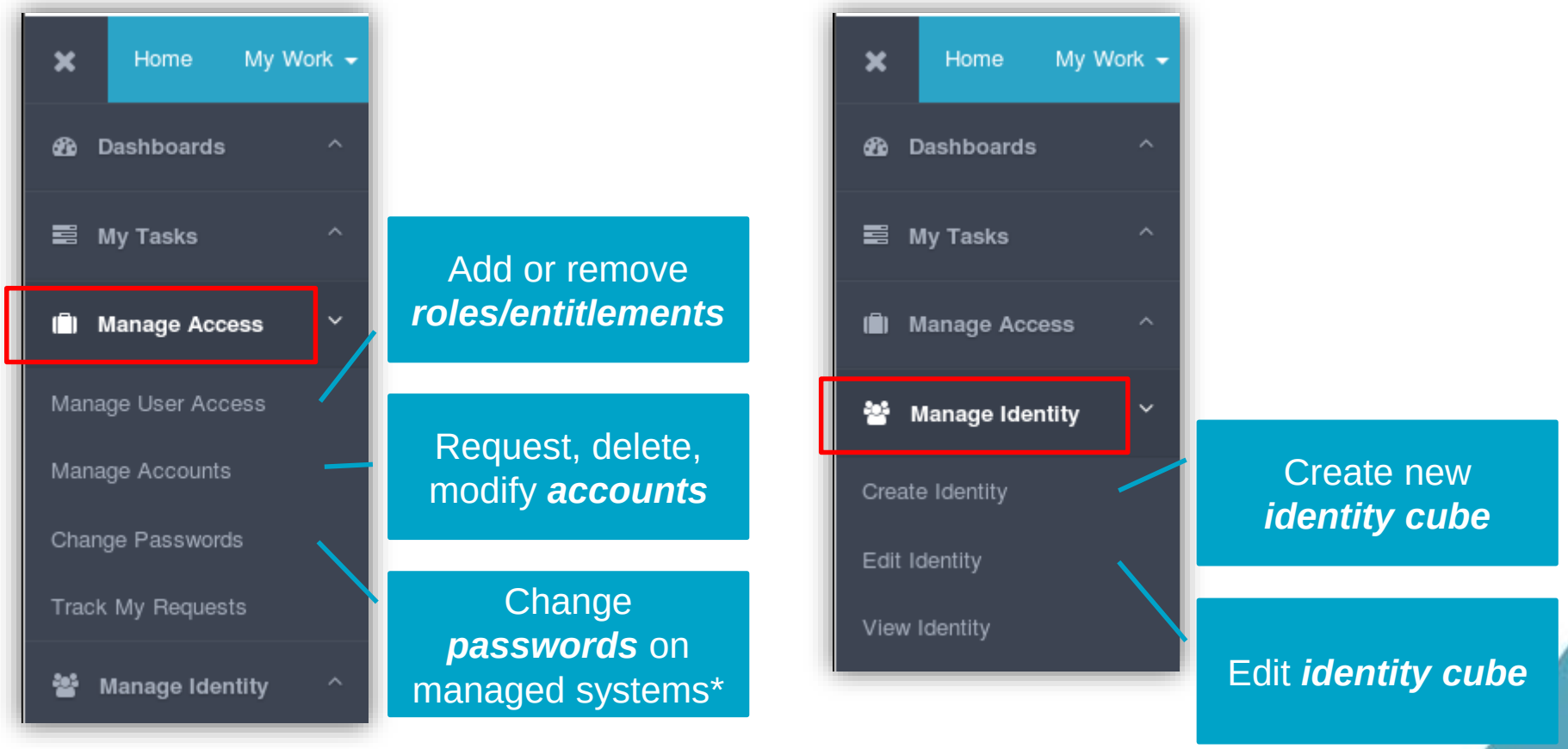
- Data-driven Changes: Lifecycle Events
  - What data changes should be watched as trigger?
  - What workflows should run in response?

SailPoint Copyright © SailPoint Technologies, Inc. 2015 All rights reserved.

Access Request Process

SailPoint

Access Request Types

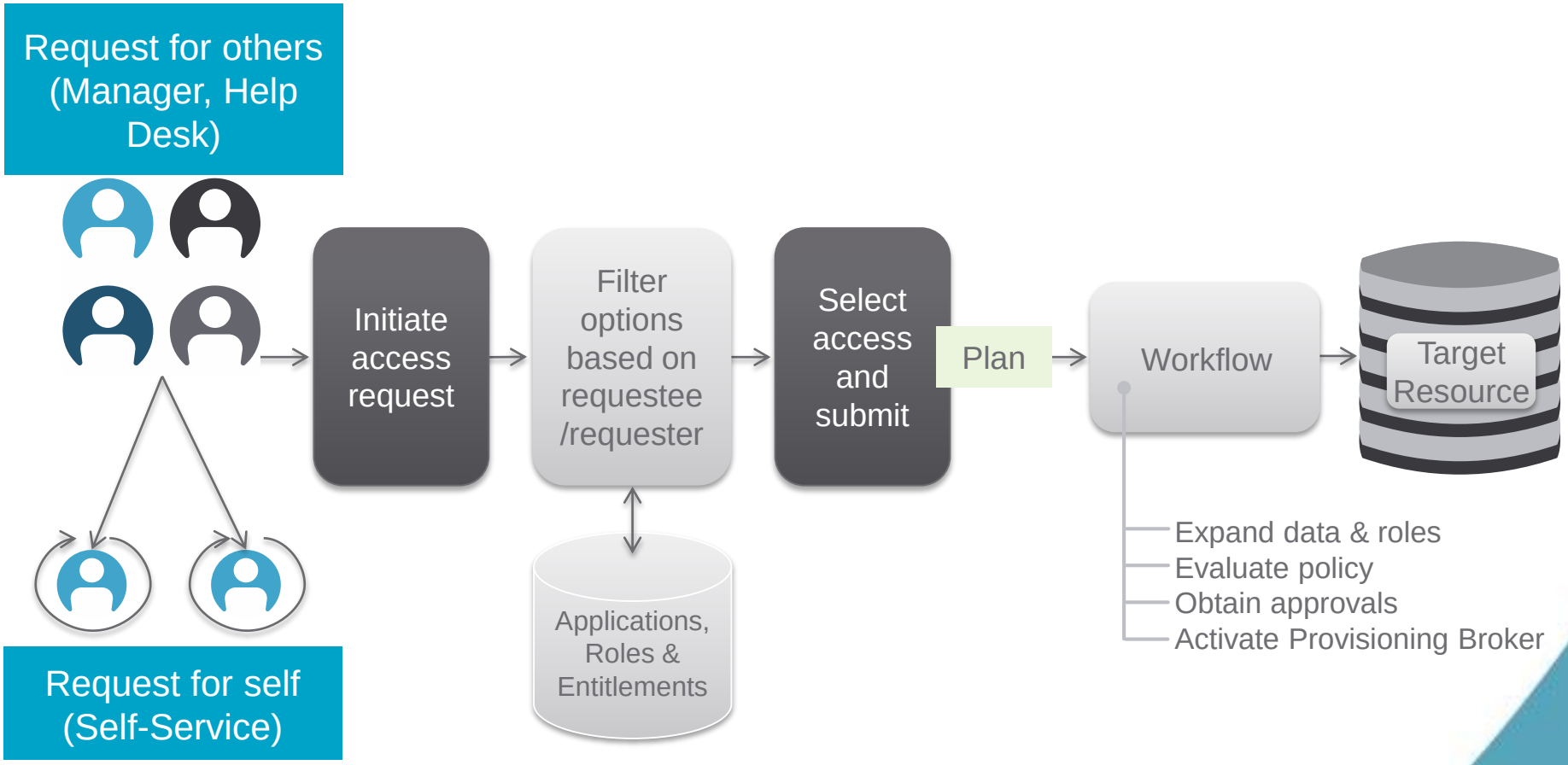


SailPoint Copyright © SailPoint Technologies, Inc. 2015 All rights reserved.

*Applications

Access Request Process

Default Process

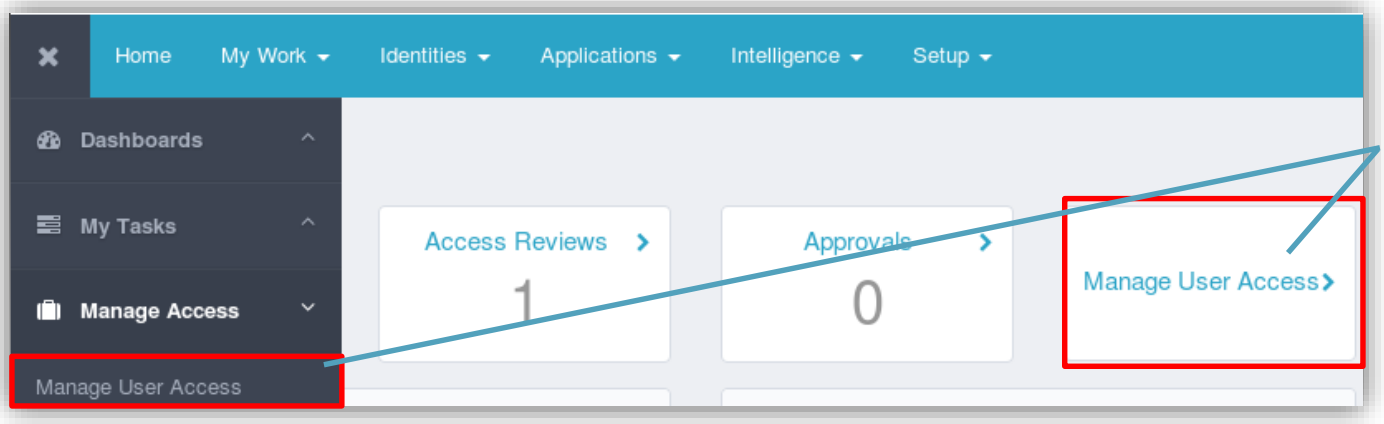


SailPoint Copyright © SailPoint Technologies, Inc. 2015 All rights reserved.

Entitlement/Role Access Change Requests

SailPoint

Submitting a Role/Entitlement Request

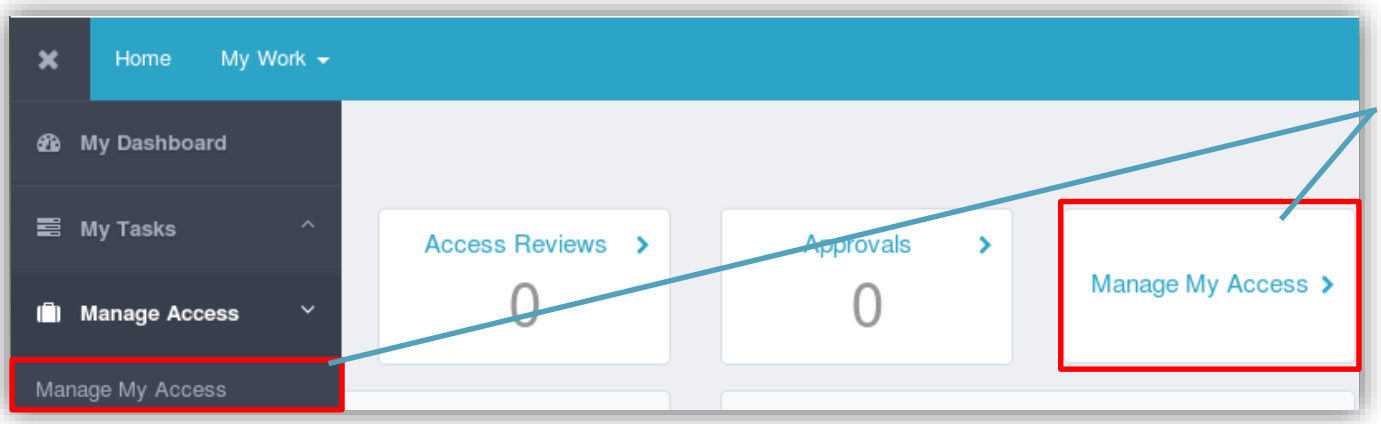


Quicklink Menu

Quicklink Card

All users who can manage access for other identities

(Managers, Help Desk, etc.)



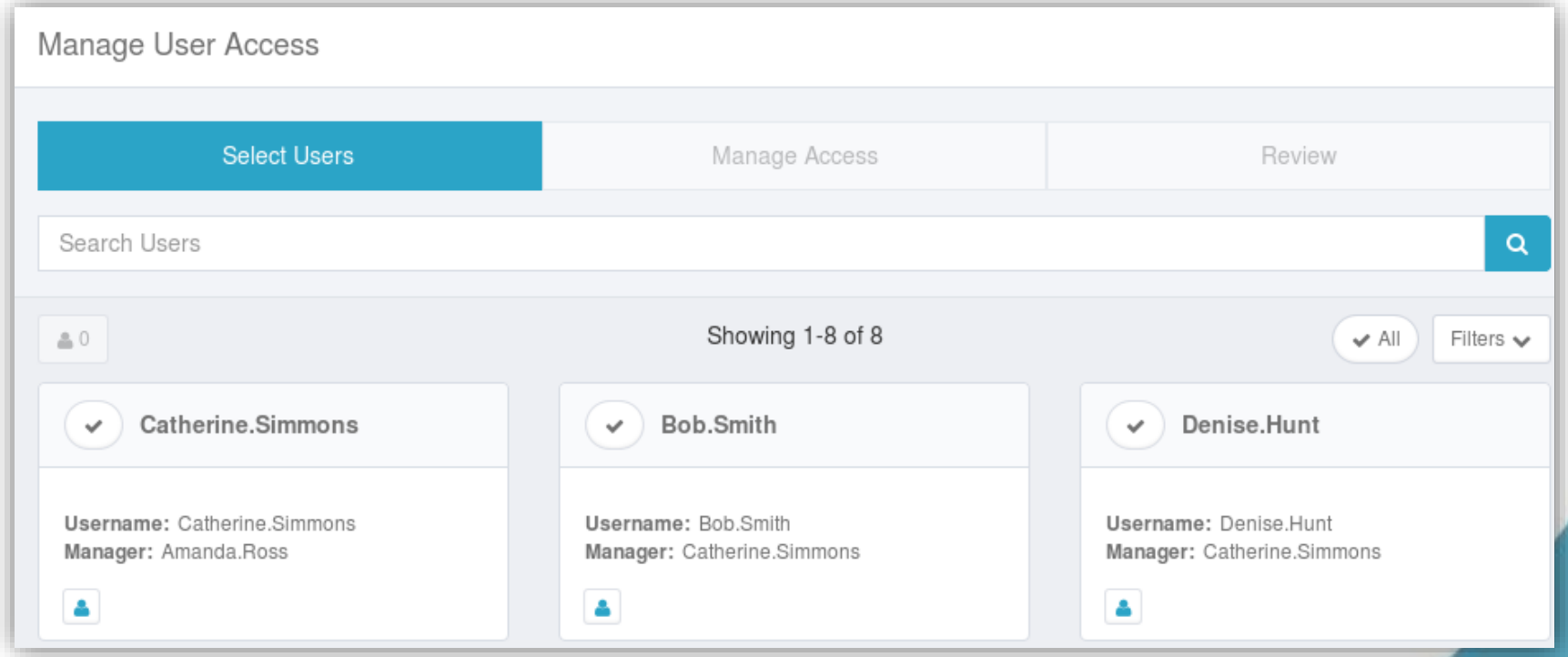
All users who can manage access only for themselves

SailPoint Copyright © SailPoint Technologies, Inc. 2015 All rights reserved.

Submitting a Request

Select Users

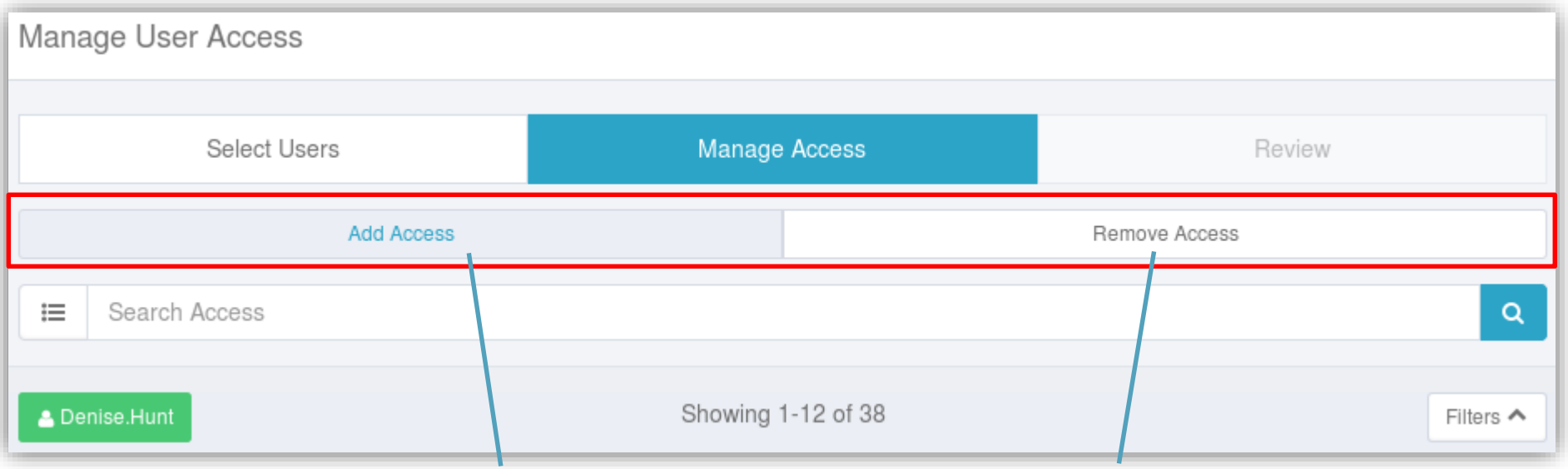
- Self and/or others
- Driven by quicklink population configuration
- Filter identities on identity attributes, roles, applications



SailPoint Copyright © SailPoint Technologies, Inc. 2015 All rights reserved.

Submitting a Request

Manage Access Options



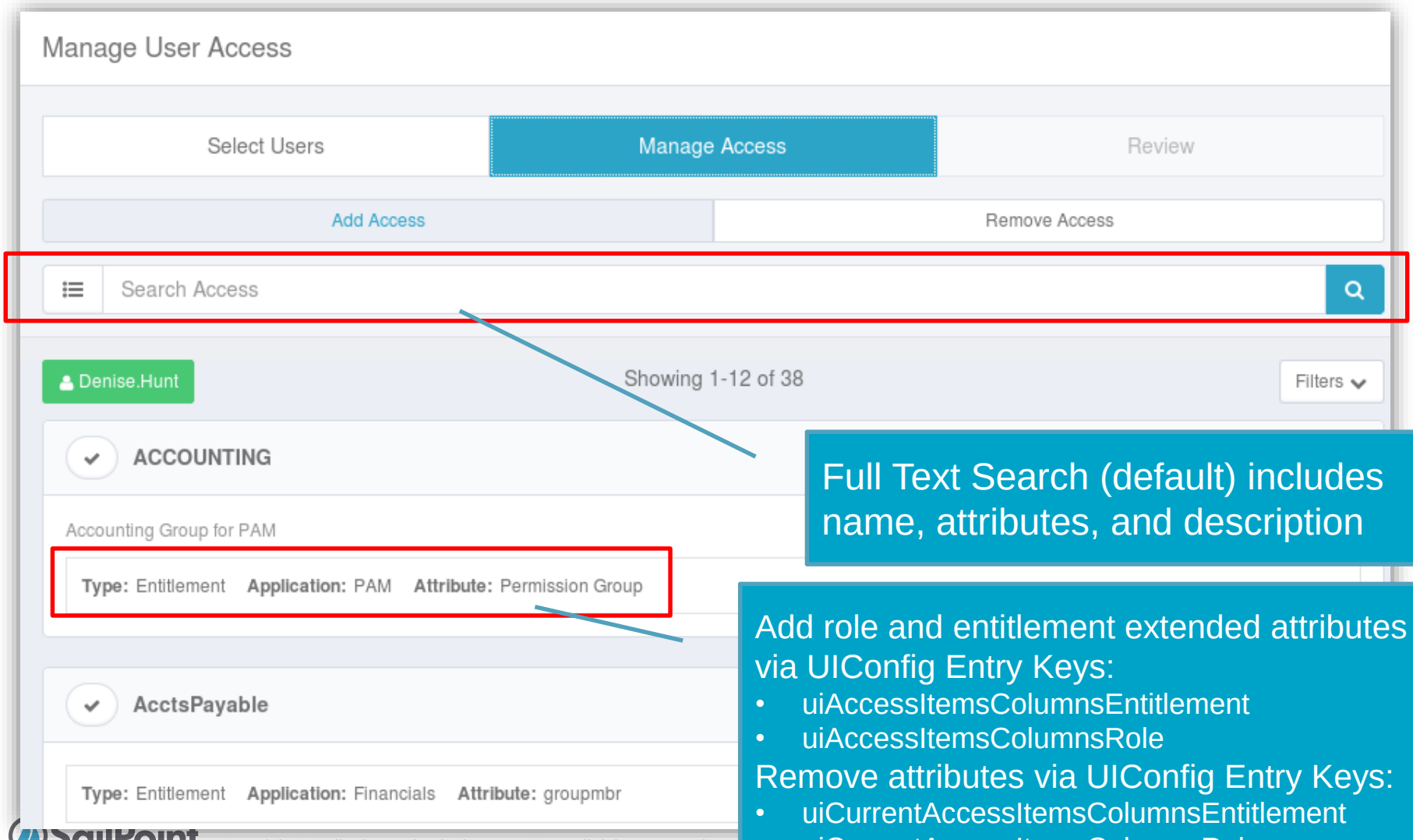
- Select from allowed roles and entitlements
- Listed roles and entitlements controlled by configuration

- List user's current roles and entitlements
- Delete role or entitlement

SailPoint Copyright © SailPoint Technologies, Inc. 2015 All rights reserved.

Submitting a Request

Searching by Keyword



Full Text Search (default) includes name, attributes, and description

Add role and entitlement extended attributes via UIConfig Entry Keys:

- uiAccessItemsColumnsEntitlement
- uiAccessItemsColumnsRole

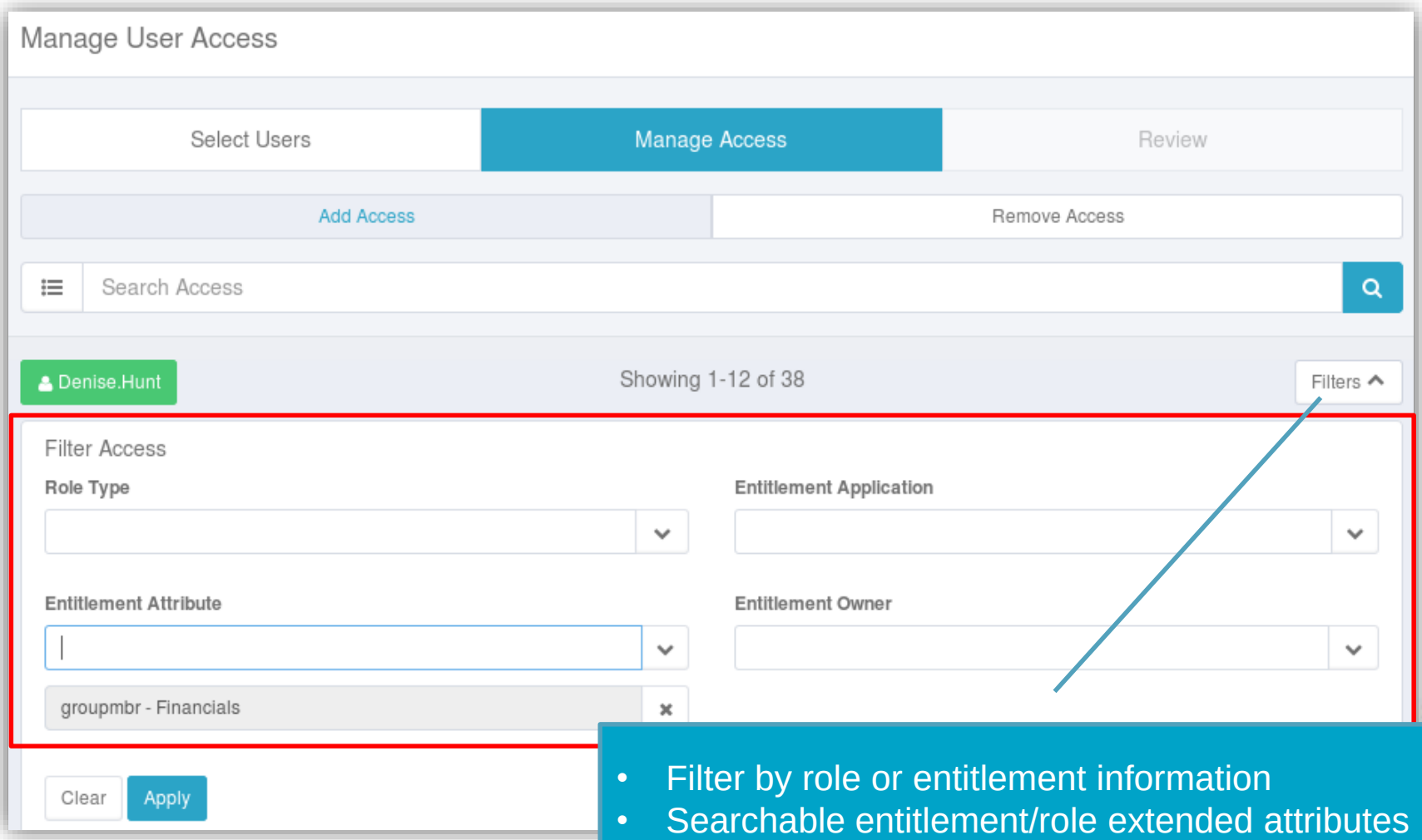
Remove attributes via UIConfig Entry Keys:

- uiCurrentAccessItemsColumnsEntitlement
- uiCurrentAccessItemsColumnsRole

SailPoint Copyright © SailPoint Technologies, Inc. 2015 All rights reserved.

Submitting a Request

Filtering Search Results

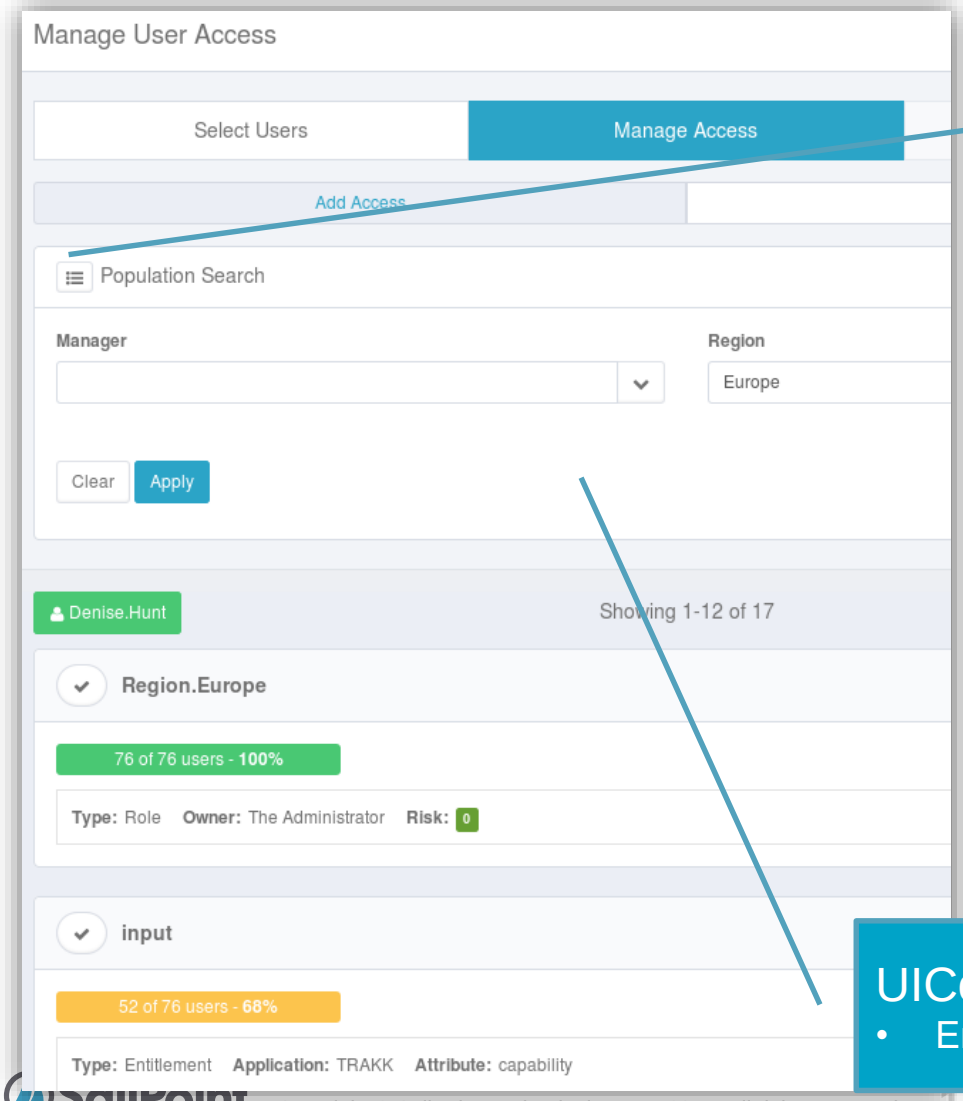


- Filter by role or entitlement information
- Searchable entitlement/role extended attributes automatically added to search parameters

SailPoint Copyright © SailPoint Technologies, Inc. 2015 All r

Submitting a Request

Searching by Affinity



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

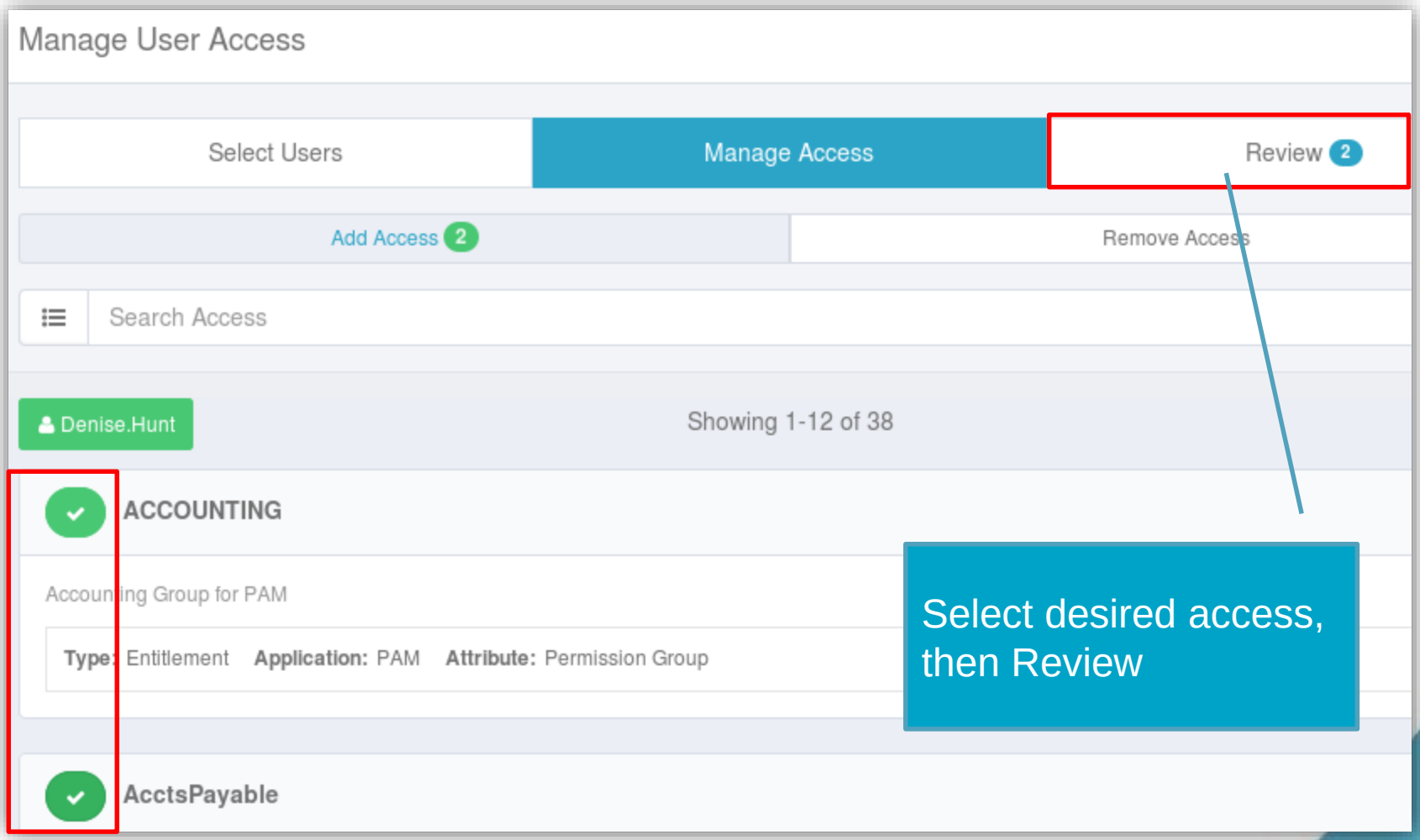
UIConfig controls available search options

- Entry Key: “lcmSearchIdentityAttributes”

SailPoint Copyright © SailPoint Technologies, Inc. 2015 All rights reserved.

Submitting a Request

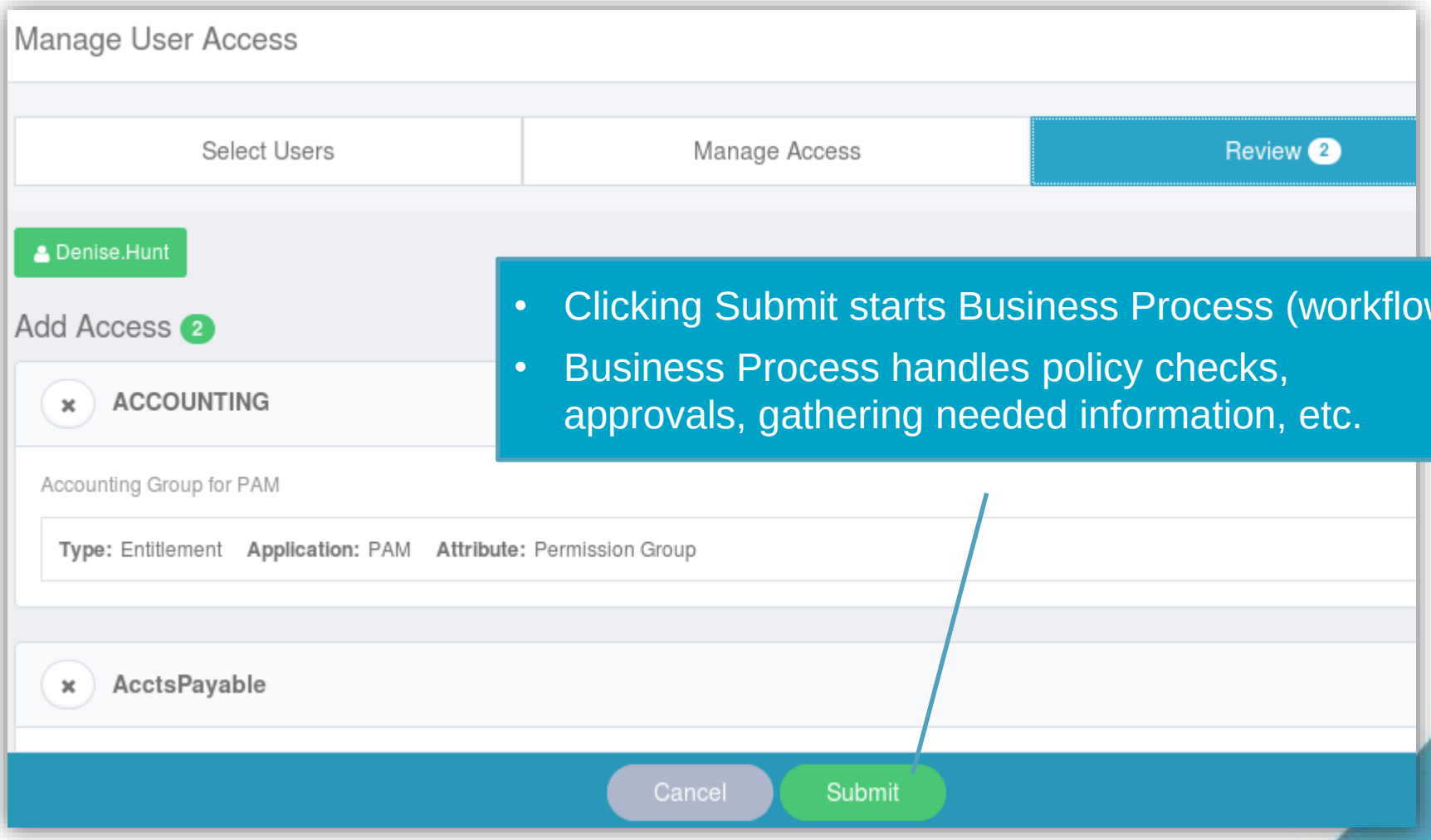
Selecting Access



SailPoint Copyright © SailPoint Technologies, Inc. 2015 All rights reserved.

Submitting a Request

Review and Submit



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

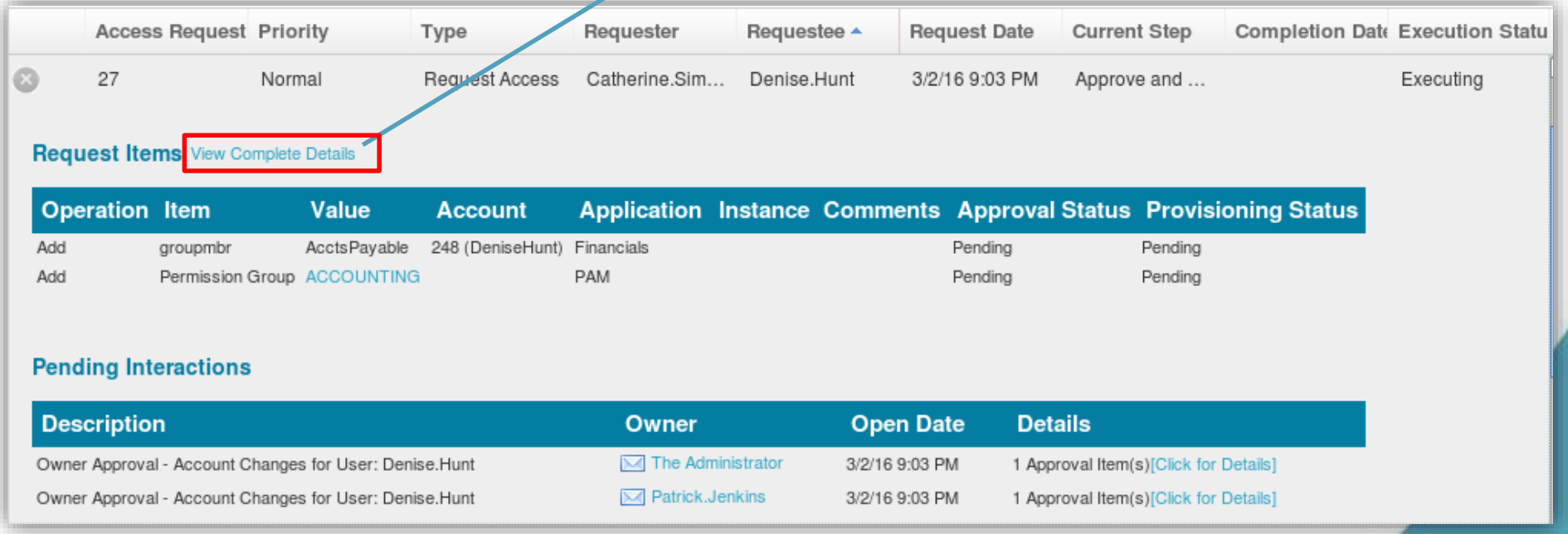
SailPoint Copyright © SailPoint Technologies, Inc. 2015 All rights reserved.

Submitting a Request

Track My Requests

- See all access requested by you and for you
- Cancel requests

See complete breakdown of Access Request



Access Request	Priority	Type	Requester	Requestee	Request Date	Current Step	Completion Dat	Execution Statu
27	Normal	Request Access	Catherine.Sim...	Denise.Hunt	3/2/16 9:03 PM	Approve and ...		Executing

Request Items View Complete Details

Operation	Item	Value	Account	Application	Instance	Comments	Approval Status	Provisioning Status
Add	groupmbr	AcctsPayable	248 (DeniseHunt)	Financials			Pending	Pending
Add	Permission Group	ACCOUNTING		PAM			Pending	Pending

Pending Interactions

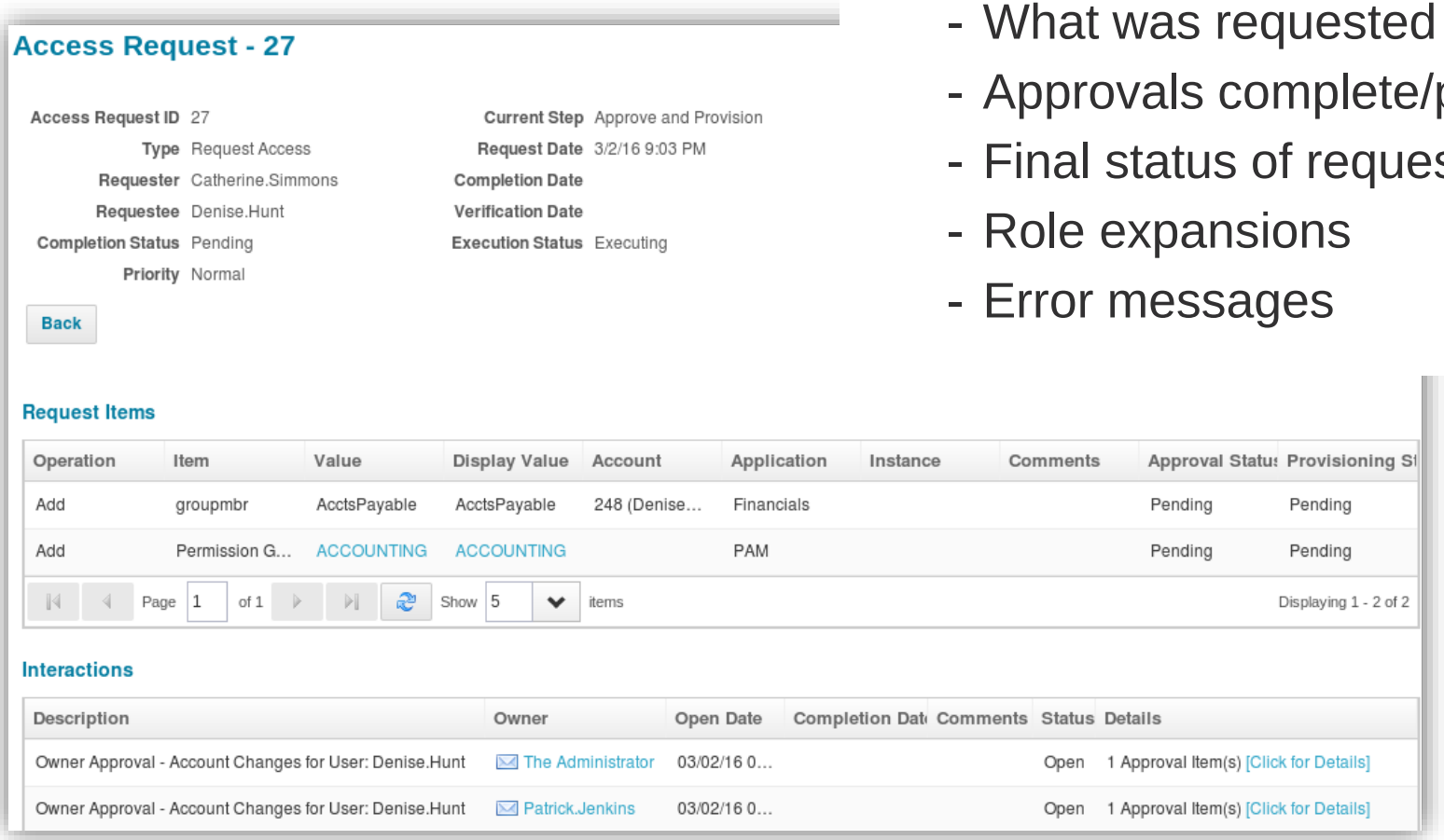
Description	Owner	Open Date	Details
Owner Approval - Account Changes for User: Denise.Hunt	The Administrator	3/2/16 9:03 PM	1 Approval Item(s)[Click for Details]
Owner Approval - Account Changes for User: Denise.Hunt	Patrick.Jenkins	3/2/16 9:03 PM	1 Approval Item(s)[Click for Details]

SailPoint Copyright © SailPoint Technologies, Inc. 2015 All rights reserved.

Submitting a Request

Access Request Details

- Details entire request including
  - What was requested
  - Approvals complete/pending
  - Final status of request
  - Role expansions
  - Error messages



Access Request - 27

Access Request ID	27	**Current Step**	Approve and Provision
Type	Request Access	**Request Date**	3/2/16 9:03 PM
Requester	Catherine.Simmons	**Completion Date**	
Requestee	Denise.Hunt	**Verification Date**	
Completion Status	Pending	**Execution Status**	Executing
Priority	Normal		

Back

Request Items

Operation	Item	Value	Display Value	Account	Application	Instance	Comments	Approval Statu	Provisioning St
Add	groupmbr	AcctsPayable	AcctsPayable	248 (Denise...	Financials			Pending	Pending
Add	Permission G...	ACCOUNTING	ACCOUNTING		PAM			Pending	Pending

Page 1 of 1 Show 5 items Displaying 1 - 2 of 2

Interactions

Description	Owner	Open Date	Completion Dat	Comments	Status	Details
Owner Approval - Account Changes for User: Denise.Hunt	The Administrator	03/02/16 0...			Open	1 Approval Item(s) [Click for Details]
Owner Approval - Account Changes for User: Denise.Hunt	Patrick.Jenkins	03/02/16 0...			Open	1 Approval Item(s) [Click for Details]

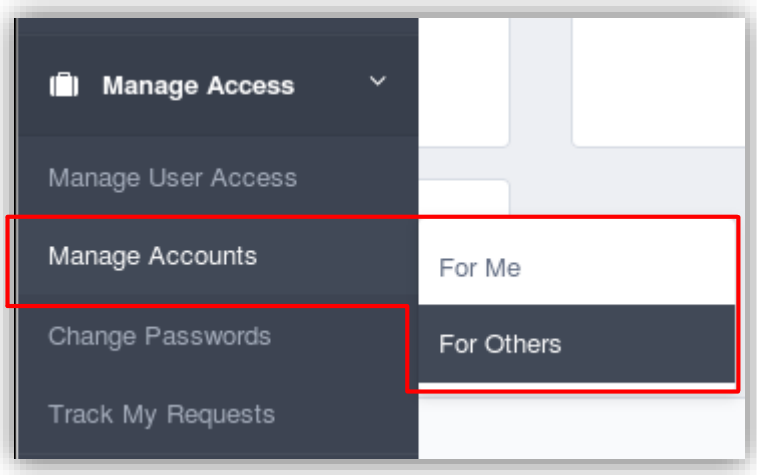
SailPoint Copyright © SailPoint Technologies, Inc. 2015 All rights reserved.

Account, Password, and Identity Cube Access Change Requests

SailPoint

Managing Accounts

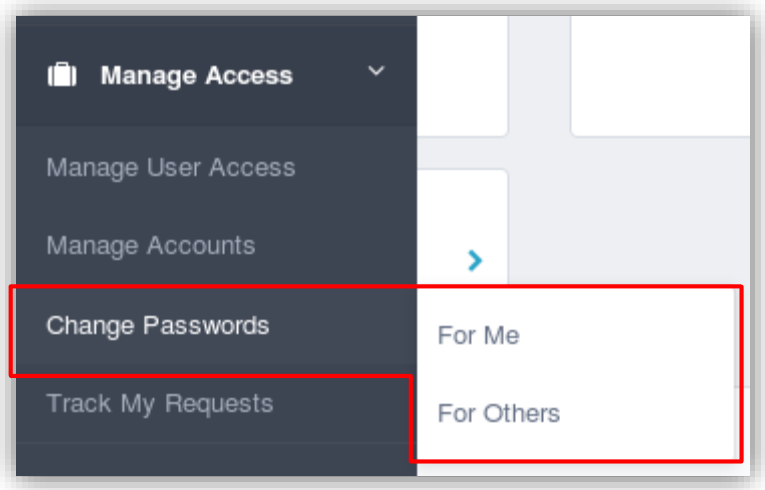
- Manage Existing Accounts
  - Enable, Disable, Unlock, Delete
- Request a new account (independent of entitlements)
  - One account or additional account
    - Configurable per application



SailPoint Copyright © SailPoint Technologies, Inc. 2015 All rights reserved.

Changing Passwords

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

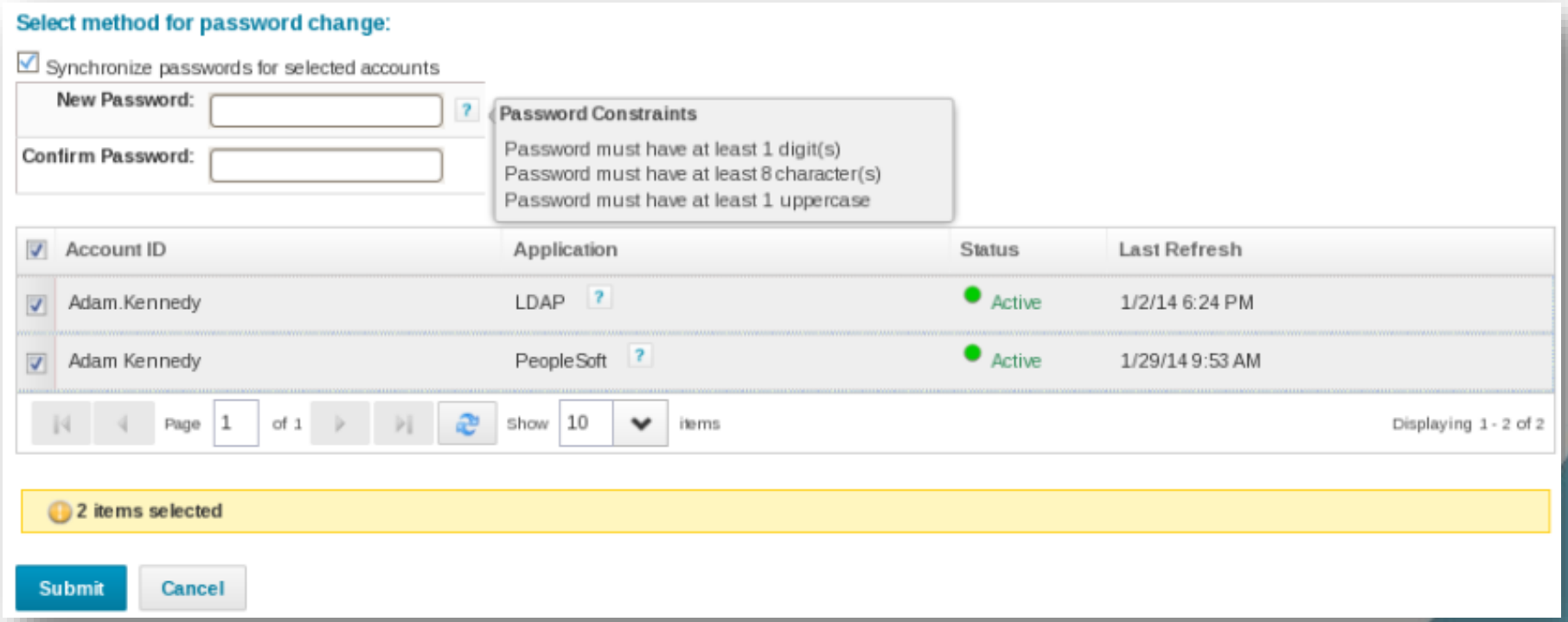


SailPoint Copyright © SailPoint Technologies, Inc. 2015 All rights reserved.

Changing Passwords

Synchronize Password and Multiple Application Policies

- Enforces strictest combination of password policy criteria
- Identifies applications with conflicting policies

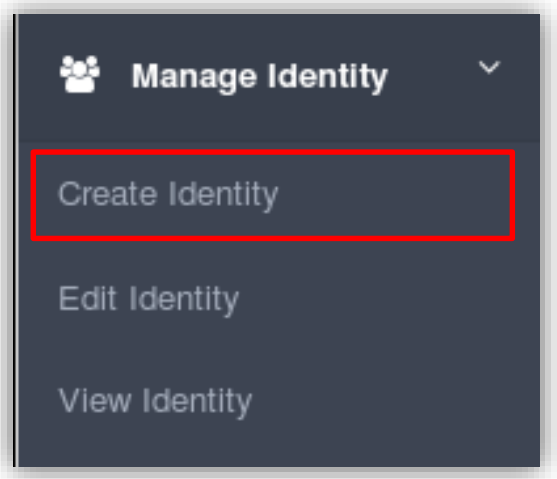


SailPoint Copyright © SailPoint Technologies, Inc. 2015 All rights reserved.

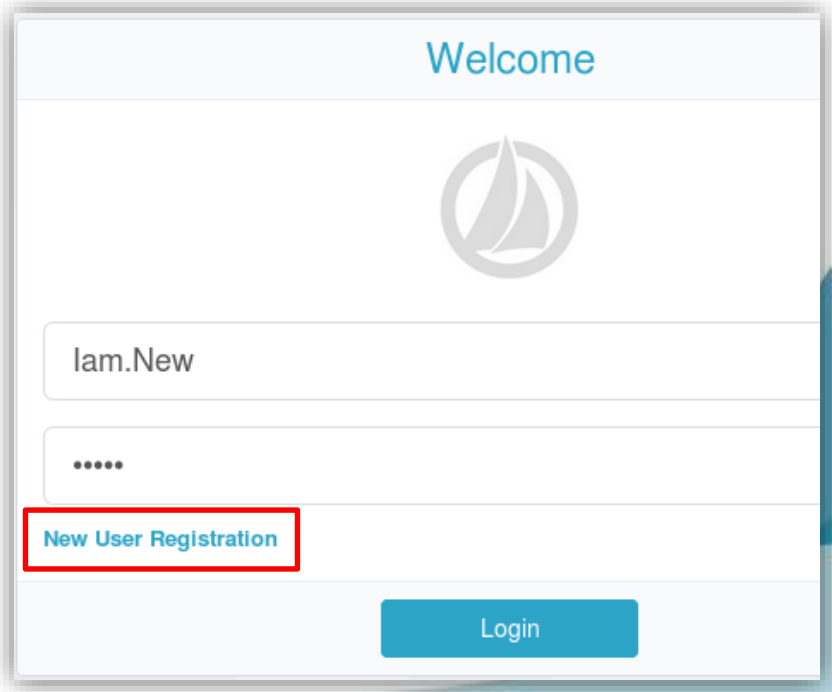
Requesting IdentityIQ Identities

Two Cases

- Requestor has IdentityIQ identity
  - Requesting identity from within IdentityIQ



- Requestor has no IdentityIQ identity (Self-service Registration)
  - Requesting new identity for themself
  - Default = off
  - Access registration form from
    - Login page
    - External link



SailPoint Copyright © SailPoint Technologies, Inc. 2015 All rights reserved.

Configuring Access Requests

SailPoint

Request Configuration Process

Overview

- Install LCM
  - In the console
    - >import init-lcm.xml
- Configure Quicklink Populations
  - Who can request what for whom
- Configure LCM
  - Options related to Role/Entitlement/Account requests and other general options
- Configure associated items outside of LCM
  - Requestable Items
    - Entitlement Catalog
    - Roles
  - Provisioning Policies (Application/Identity Create)
  - Business Processes (Workflows)

SailPoint Copyright © SailPoint Technologies, Inc. 2015 All rights reserved.

Configuring Quicklink Populations

SailPoint

Quicklink Populations

Default Access

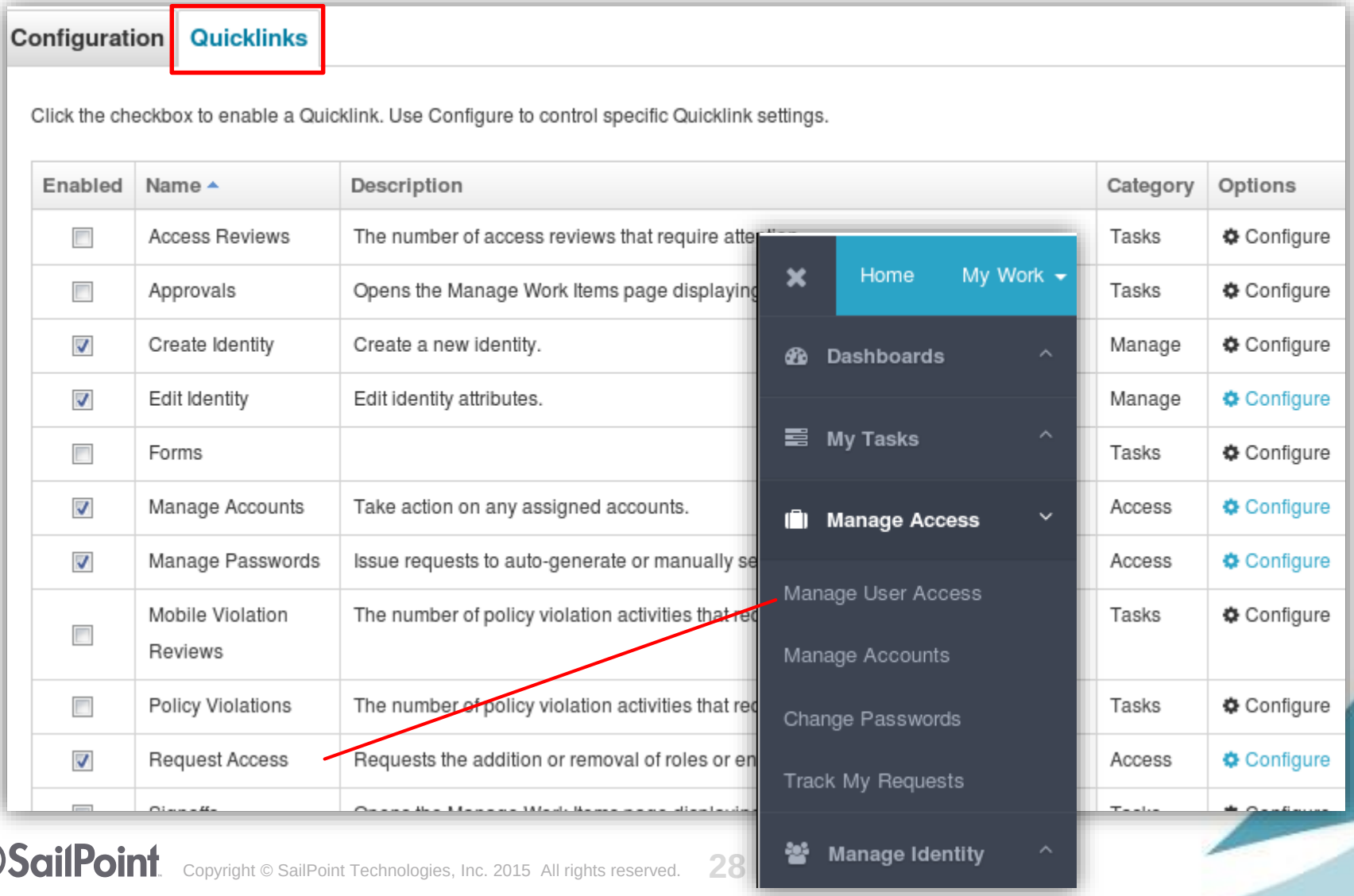
Population

Quicklink	Everyone	Help Desk	Manager	Self-Service
Access Reviews	✓			
Approvals	✓			
Create Identity		✓	✓	
Edit Identity		✓	✓	✓
Forms	✓			
Manage Accounts		✓	✓	✓
Manage Passwords		✓	✓	✓
Policy Violations	✓			
Request Access		✓	✓	✓
Signoffs	✓			
Track Requests				✓
View Identity		✓	✓	✓
Work Items	✓			

SailPoint Copyright © SailPoint Technologies, Inc. 2015 All rights reserved.

Manager Population Example

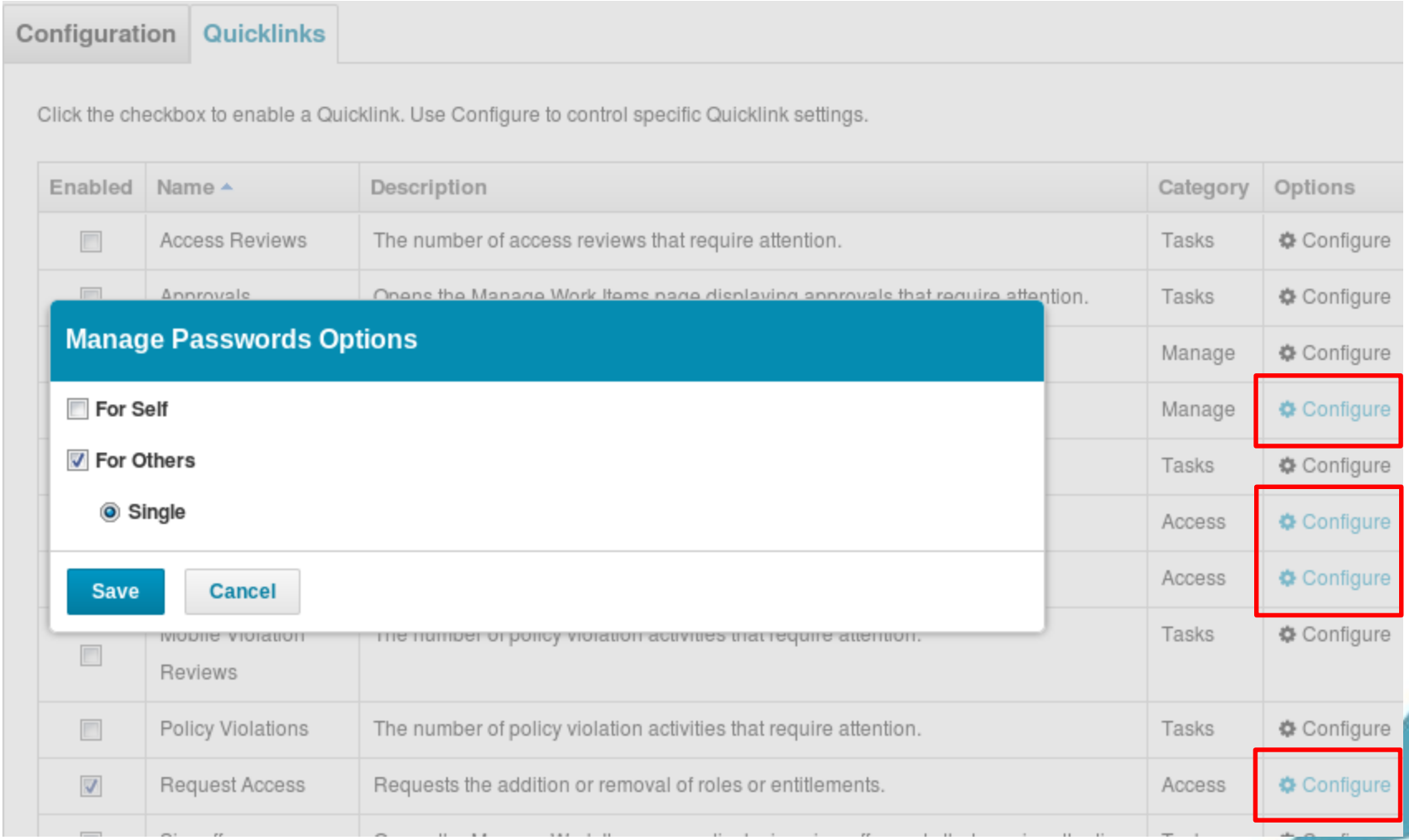
Which Quicklinks can population access?



SailPoint Copyright © SailPoint Technologies, Inc. 2015 All rights reserved.

Manager Population Example

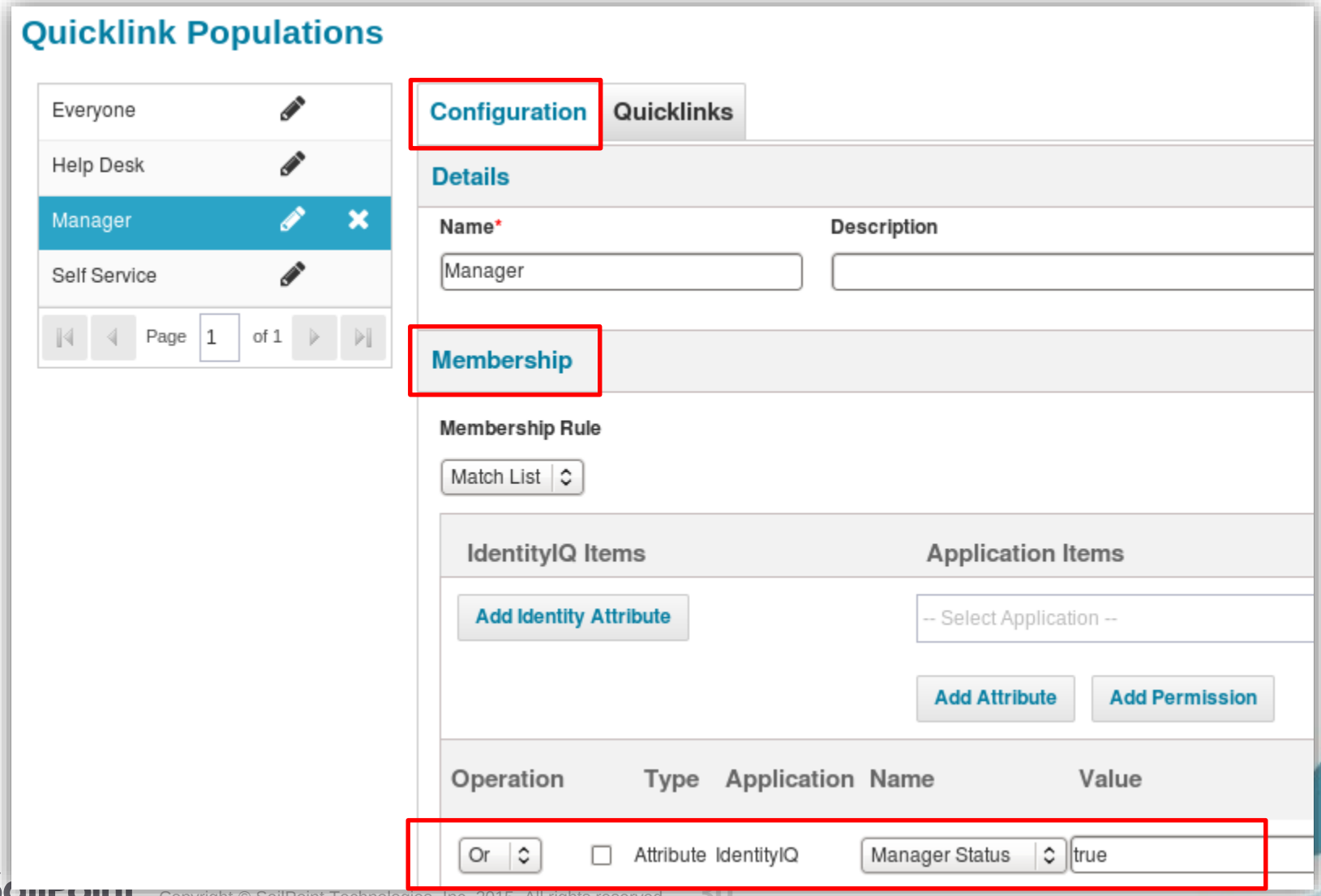
For each quicklink, which options will be allowed?



SailPoint Copyright © SailPoint Technologies, Inc. 2015 All rights reserved.

Manager Population Example

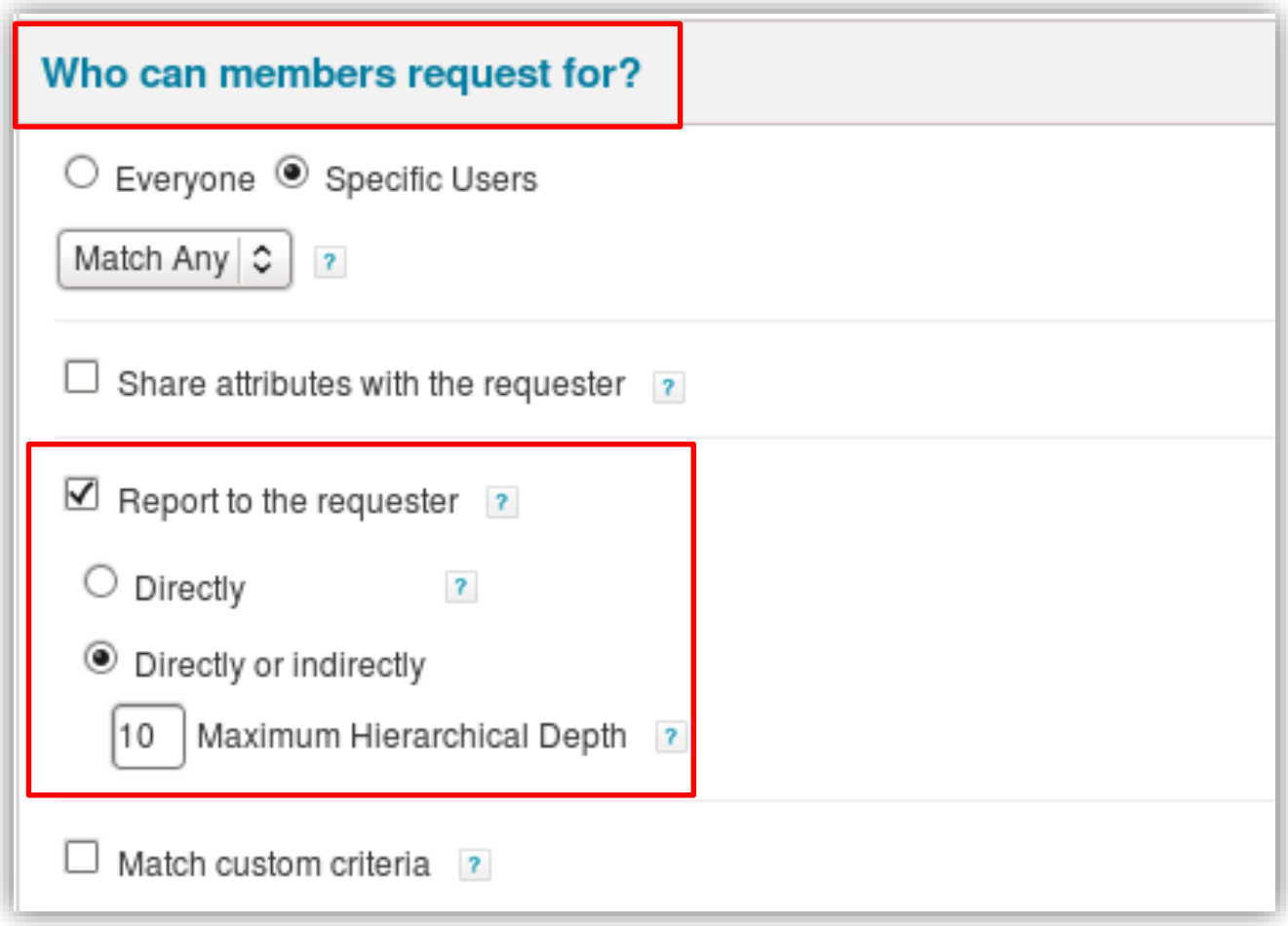
Who is included in the population?



Copyright © SailPoint Technologies, Inc. 2015 All rights reserved.

Manager Population Example

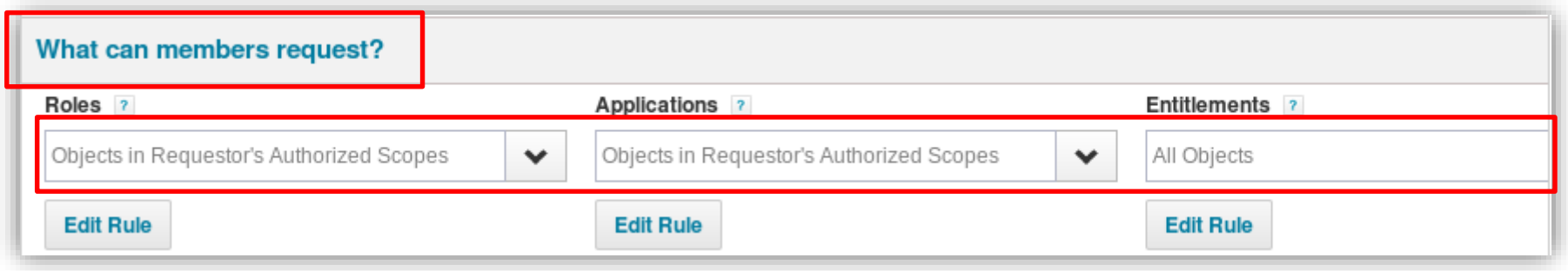
Who can population act upon?



SailPoint Copyright © SailPoint Technologies, Inc. 2015 All rights reserved.

Manager Population Example

What can population request?



- Availability based on requestor and/or requestee
- Configured through rules
  - Multiple rule options provided
  - Can create own rules

SailPoint Copyright © SailPoint Technologies, Inc. 2015 All rights reserved.

Extending Quicklinks

- Custom Quicklink populations
  - Define business specific groups of users (i.e. Team Leads)
  - Configure Quicklink access per population
- Custom Quicklinks
  - Add business specific Quicklinks to the Quicklink menu
  - Options
    - Execute custom workflow (i.e. Emergency termination)
    - Deep link into IdentityIQ (i.e. Bypass navigation for a common task)
    - Link to external UI

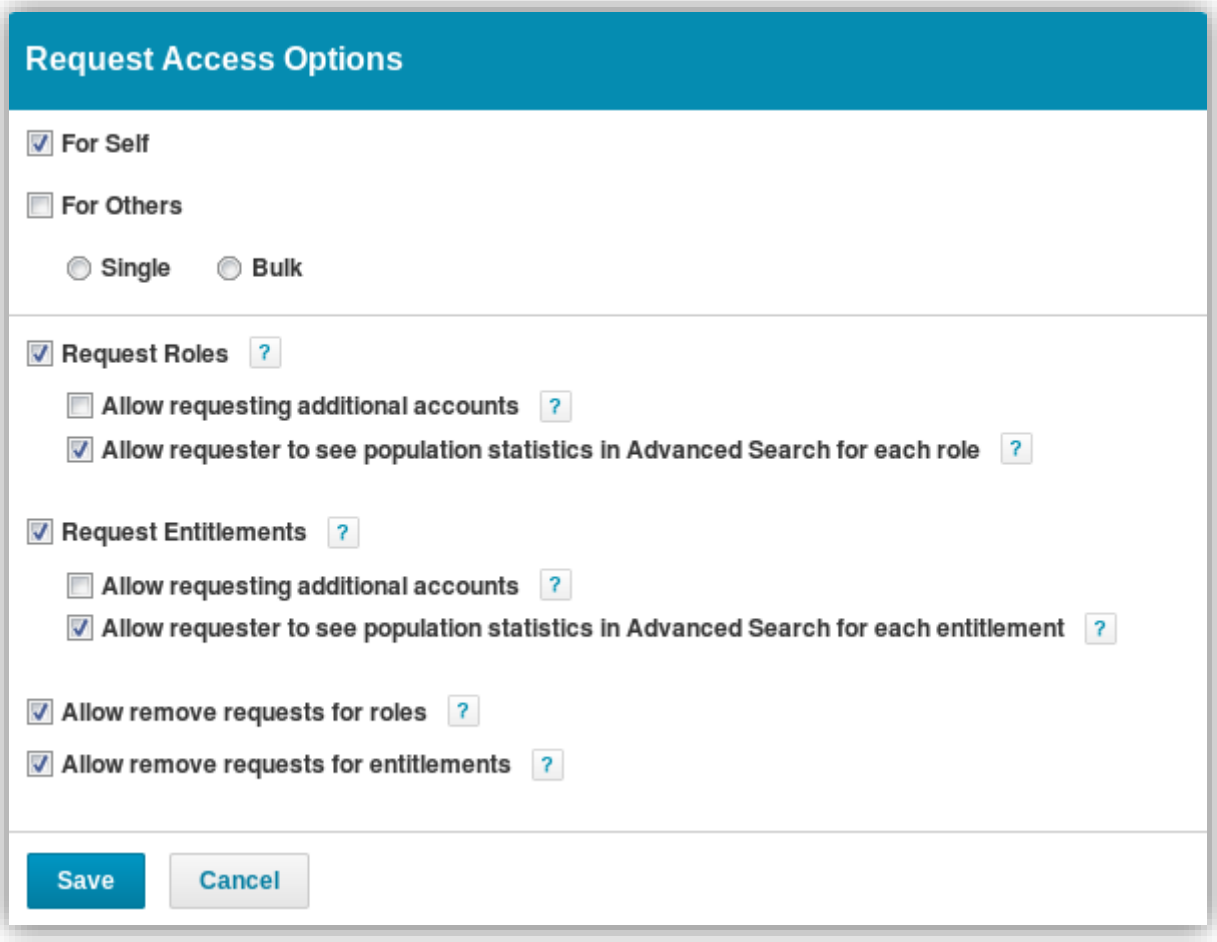
SailPoint Copyright © SailPoint Technologies, Inc. 2015 All rights reserved.

Configuring Role and Entitlement Requests – Manage User Access

SailPoint

Request Access Quicklink

Options

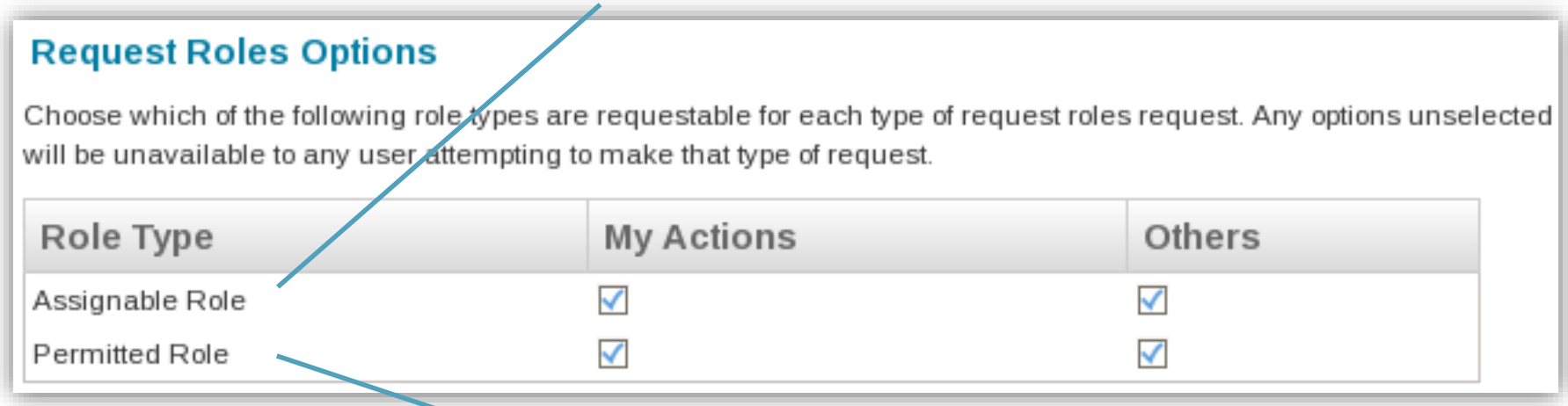


SailPoint Copyright © SailPoint Technologies, Inc. 2015 All rights reserved.

LCM Configuration

Supporting Roles Requests

Allow requests for business roles



Allow requests for permitted IT roles granted by currently-held business roles

SailPoint Copyright © SailPoint Technologies, Inc. 2015 All rights reserved.

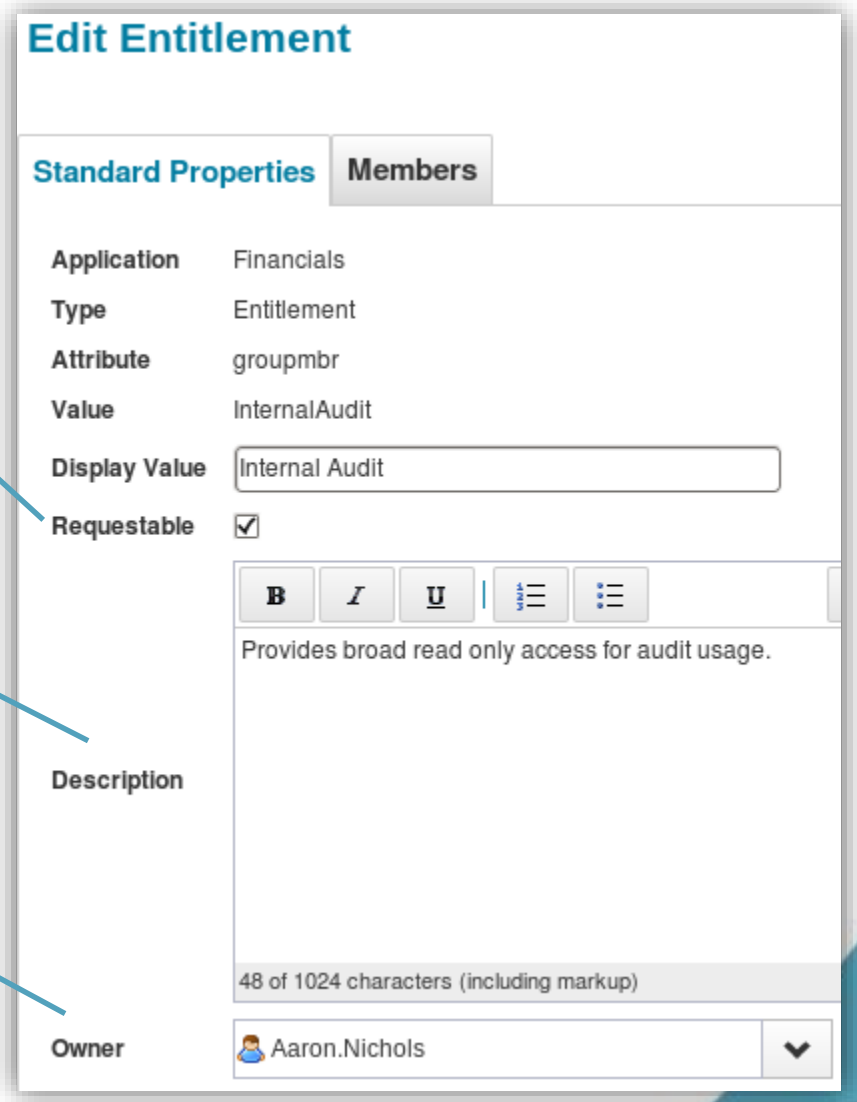
Requestable Entitlements

Entitlement Catalog

- Entitlement is requestable through LCM
- Default = Requestable

- Displayed in LCM

- Access request approver



SailPoint Copyright © SailPoint Technologies, Inc. 2015 All rights reserved.

Restricting Access Based on Data

Example: Security Level Attribute

CONFIGURATION

Access

Spy Super User
Security Level: 10

Spy Data Entry
Security Level: 5

Spy Audit
Security Level: 10

Identity Cubes

John
Security Level: 7

Susan
Security Level: 12

Ian
Security Level: 2

ACCESS REQUESTS

Access Options

Spy Data Entry

Spy Super User
Spy Data Entry
Spy Audit

<No Spy Options>

Rule

```
import sailpoint.object.Filter;
return Filter.le(”security_lev”,requestee.getAttribute(“security_lev”));
```

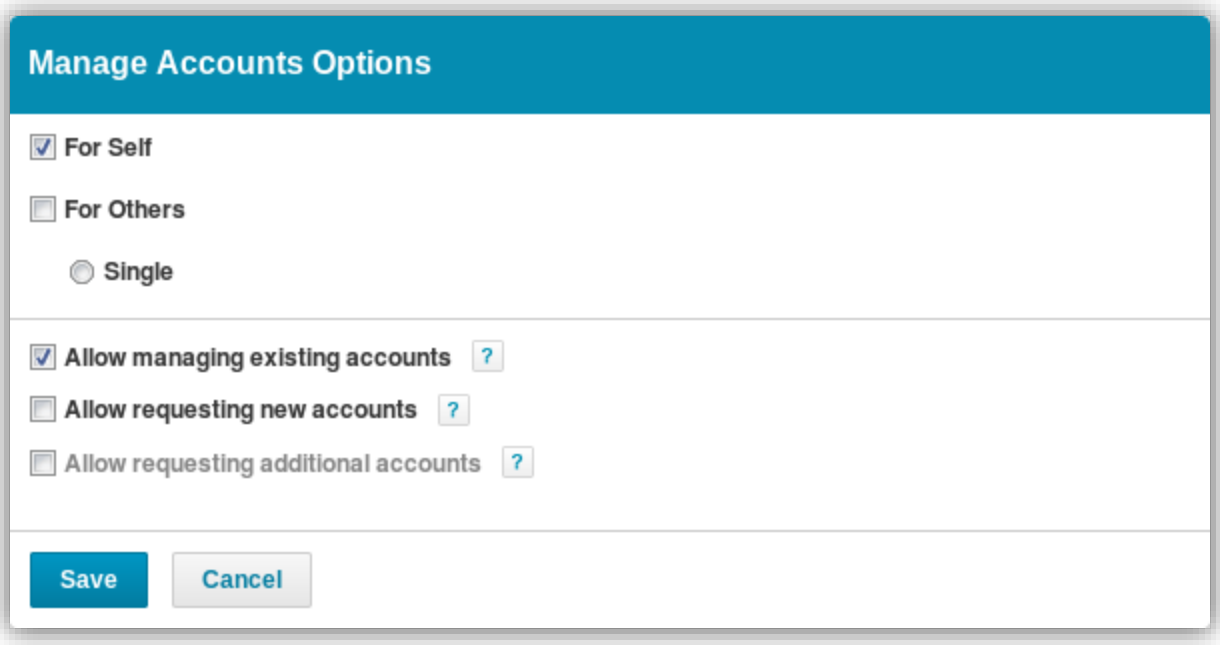
SailPoint Copyright © SailPoint Technologies, Inc. 2015 All rights reserved.

Configuring Account Requests – Manage Accounts

SailPoint

Manage Accounts Quicklink

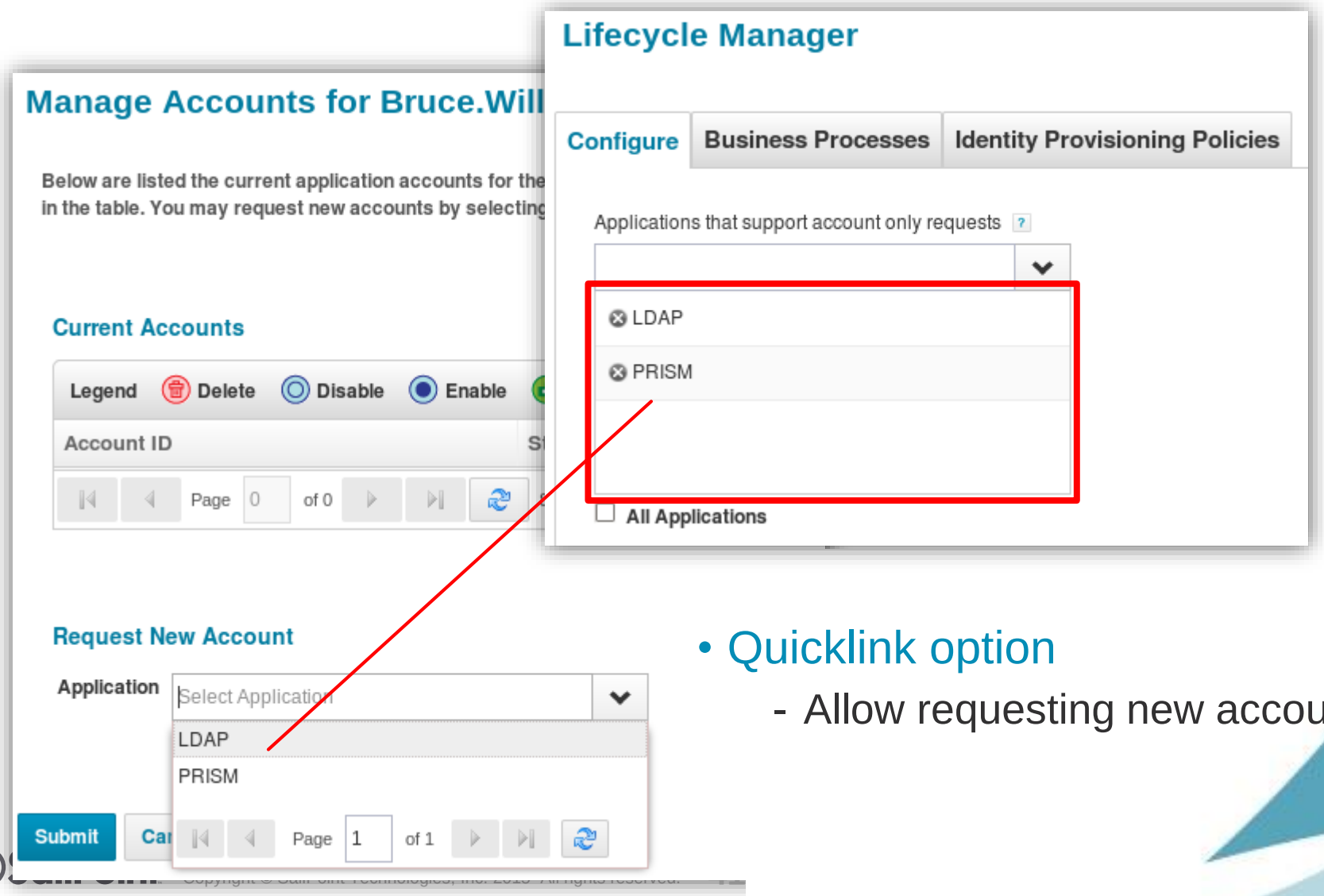
Options



SailPoint Copyright © SailPoint Technologies, Inc. 2015 All rights reserved.

LCM Configuration

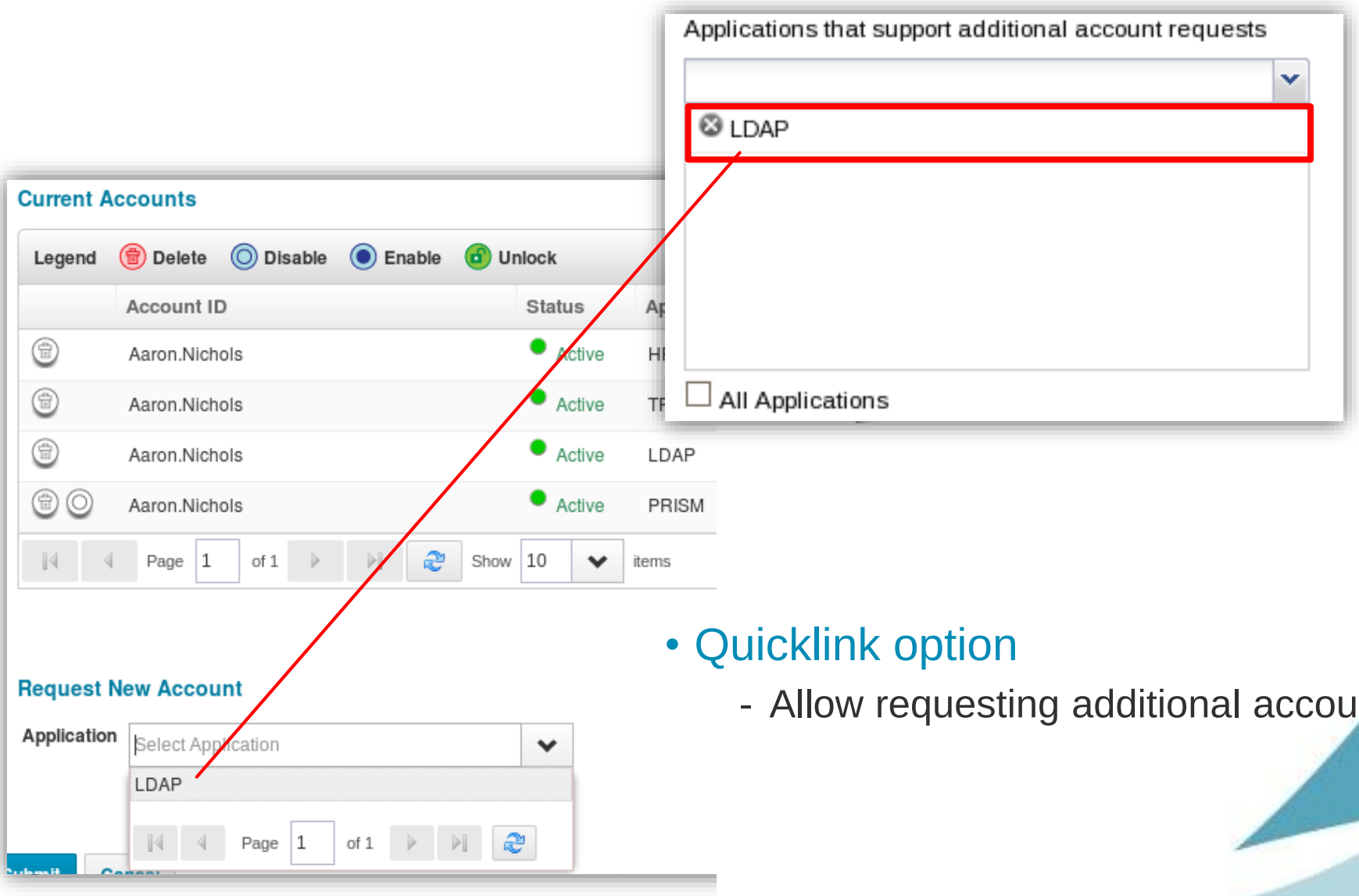
Supporting Account Only Requests



- Quicklink option
  - Allow requesting new account

LCM Configuration

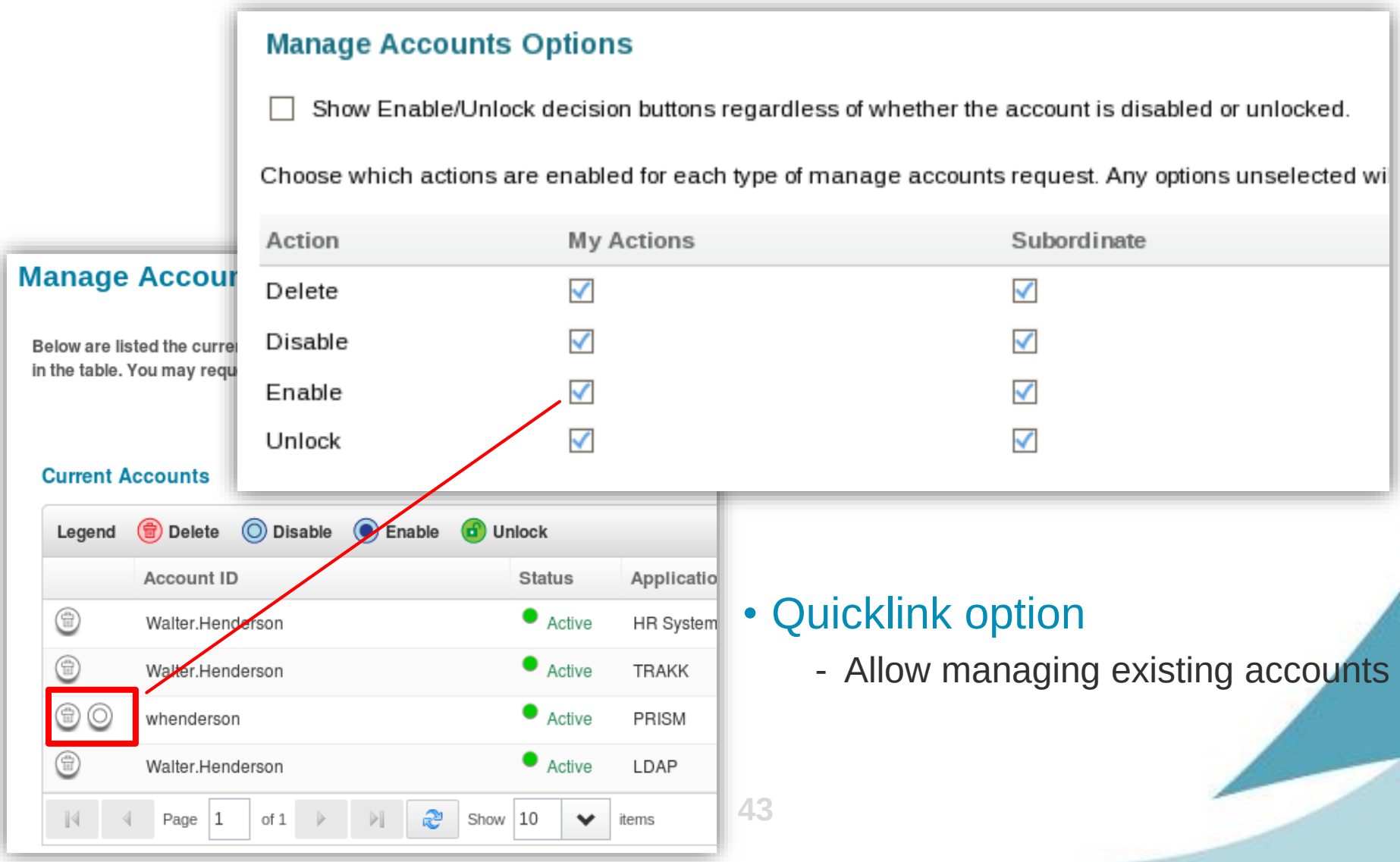
Supporting Requests for Additional Account



- Quicklink option
  - Allow requesting additional accounts

LCM Configuration

Supporting Account Operations



- Quicklink option
  - Allow managing existing accounts

Configuring Provisioning Policies

SailPoint

Provisioning Policies

- Specify attributes to include in provisioning requests
  - Values can be provided manually by user
  - Values can be provided by IdentityIQ (auto-calculated or static)

Example: Create an account on PRISM

PRISM Create Provisioning Policy

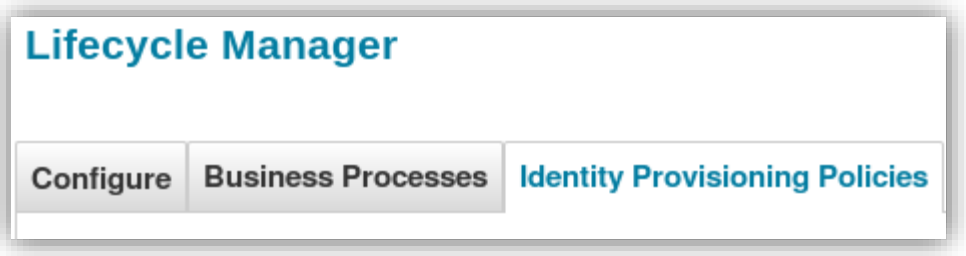
Attribute	Value
First	return identity.firstname;
Last	return identity.lastname;
Login	return identity.name;
Status	A
Locked	N

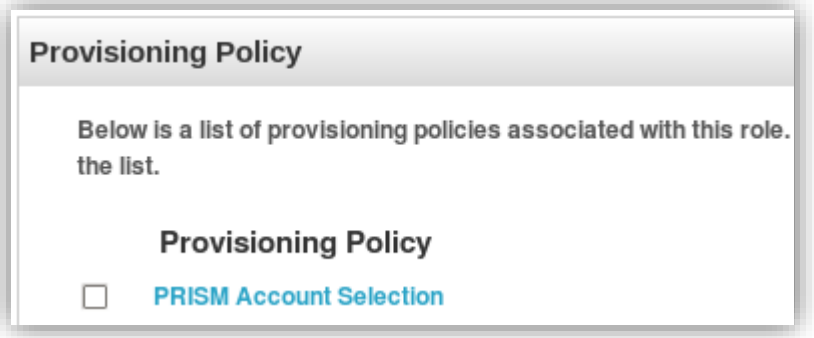
Plan
First: John
Last: Jones
Login: John.Jones
Status: A
Locked: N

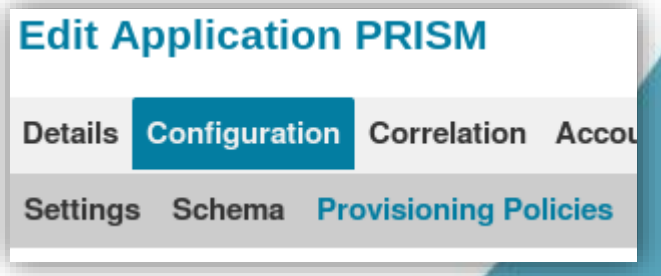
SailPoint Copyright © SailPoint Technologies, Inc. 2015 All rights reserved.

Provisioning Policy Configuration

- Identity Provisioning Policy
  - Supports
    - *Create* identity cube
    - *Update* identity attributes
    - Self-service Registration
- Role Provisioning Policy
  - Support for Create
- Application Provisioning Policy
  - Supports
    - Account *create*, *update*, and *delete*
    - Group *create* and *update*
      (if groups are supported by connector)

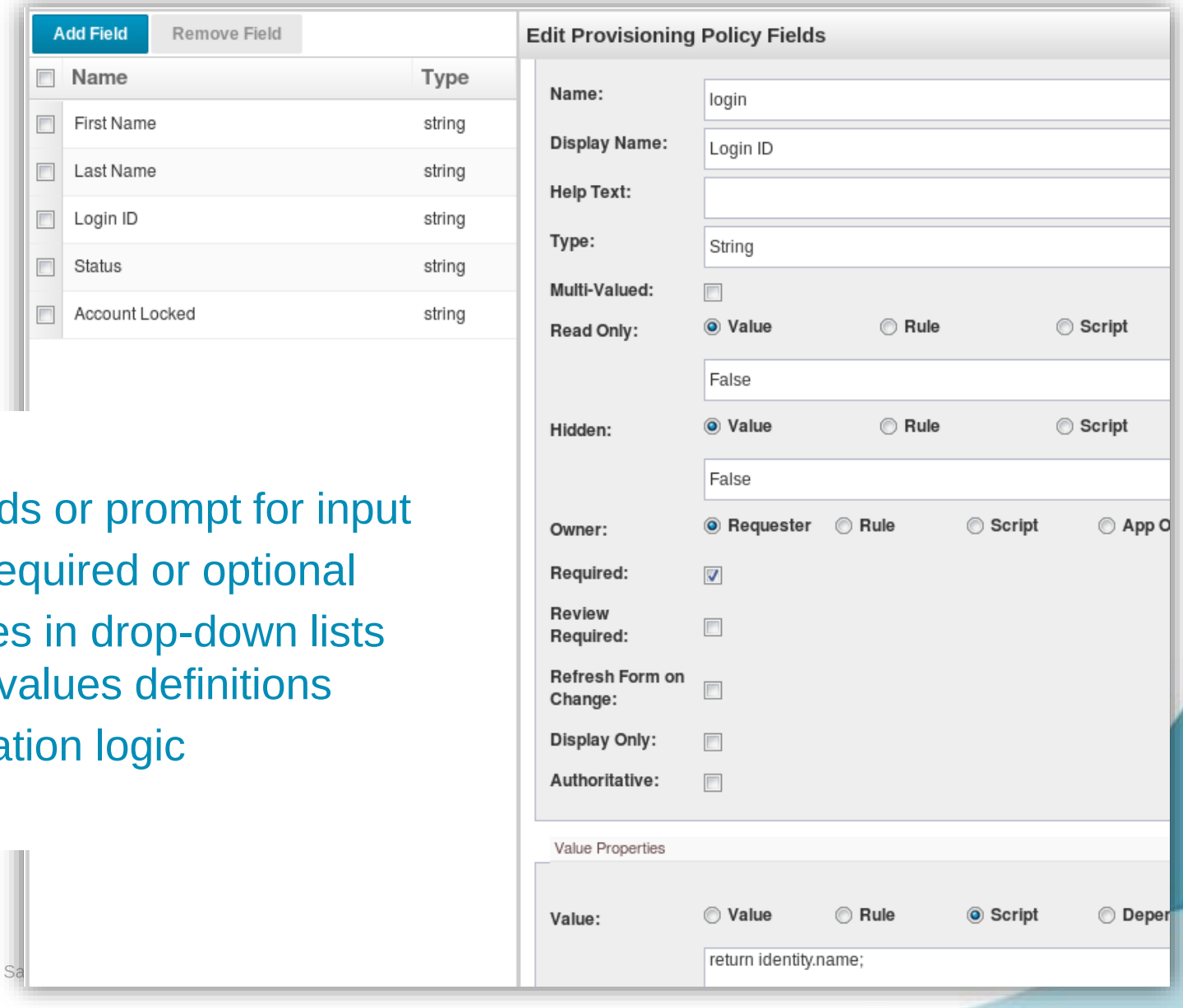






SailPoint Copyright © SailPoint Technologies, Inc. 2015 All rights reserved.

Provisioning Policy



- Calculate fields or prompt for input
- Make fields required or optional
- Specify entries in drop-down lists with allowed values definitions
- Include validation logic

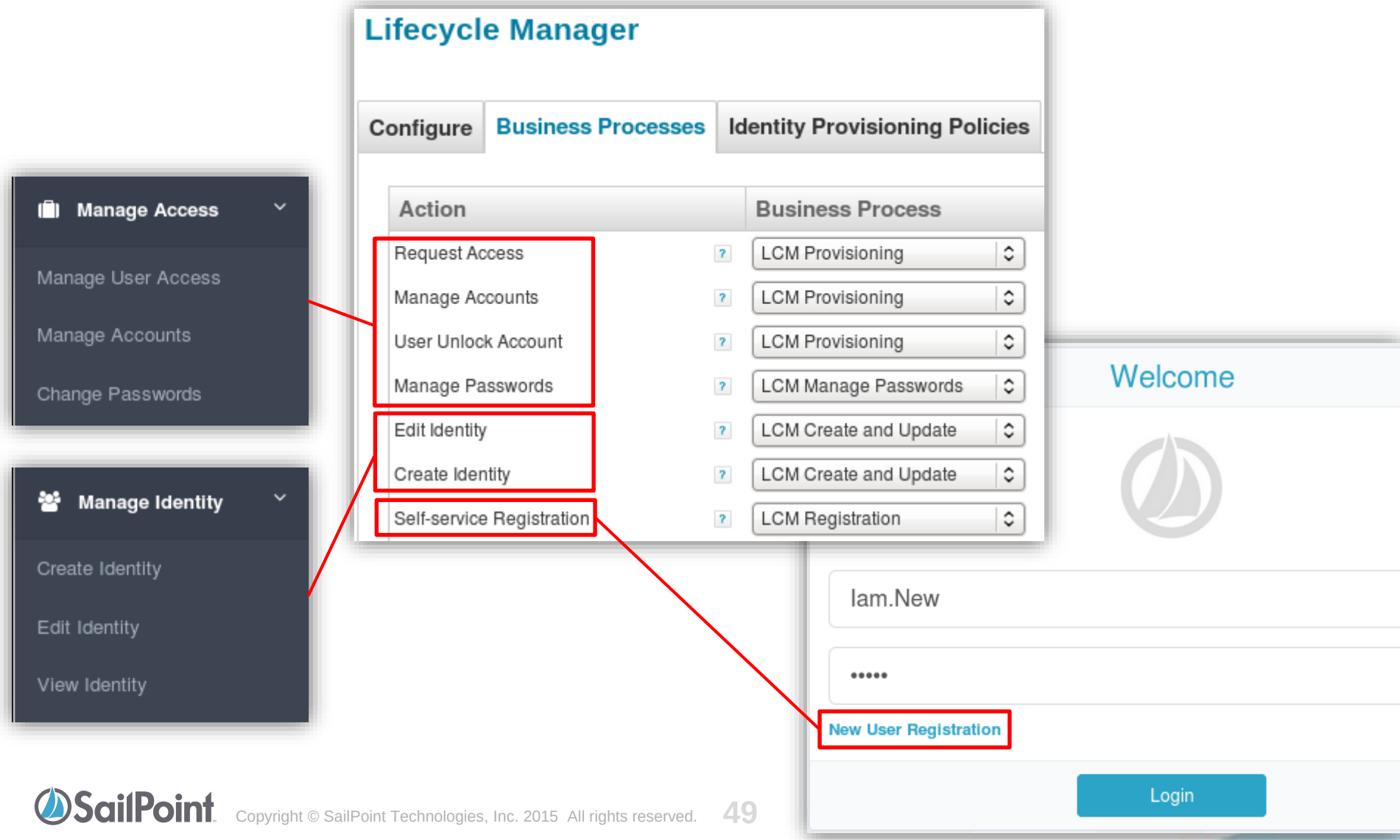
SailPoint Copyright © Sa

Associate Business Processes

SailPoint

LCM Configuration

Associate Business Processes with Actions



SailPoint Copyright © SailPoint Technologies, Inc. 2015 All rights reserved.

Exercise Preview

Section 4, Exercises 1, 2, 3

- Exercise 1: Enabling Lifecycle Manager
- Exercise 2: Create and Manage Identities in IdentityIQ
- Exercise 3: Account Management with Lifecycle Manager

SailPoint Copyright © SailPoint Technologies, Inc. 2015 All rights reserved.