

## CONFIGURABLE SECURITY FUNDAMENTALS

### Course Manual and Activity Guide

This booklet is for the personal use of only the individuals who have enrolled in this specific workday training course. You may make copies only as necessary for your own use. Any distribution, even within your organization, is strictly prohibited unless workday has authorized such distribution in writing.

© 2015 Workday, Inc. All rights reserved. Workday, the Workday logo, Workday Enterprise Business Services, Workday Human Capital Management, Workday Financial Management, Workday Resource Management and Workday Revenue Management are all trademarks of Workday, Inc. All other brand and product names are trademarks or registered trademarks of their respective holders. Version #24 v2 (May, 2015)

## CONTENTS

<b>Configurable Security Fundamentals .....</b>	<b>4</b>
<b>Security Landscape .....</b>	<b>5</b>
What Is Configurable Security .....	5
Security Landscape .....	7
Activity 1 – Navigate Functional Areas .....	10
A Closer Look at Security Policies.....	12
Inheritance in Domain Security Policies .....	13
Security Policy Reports.....	14
Activity 2 – Navigate Domain Security Policies.....	15
Activity 3 – Navigate Business Process Security Policies .....	19
Managing Security .....	20
Security Profiles.....	21
Workday Assigned Security Groups .....	21
Steps for Configuring Security .....	23
Proxy Sessions .....	24
Activity 4 – Create Proxy Access Policy .....	26
Security Policy Change Control .....	28
<b>Security Groups.....</b>	<b>30</b>
Context Sensitivity .....	30
User-Based Security Groups .....	32
Activity 5A – Create User-Based Security Group .....	35
Activity 5B – Edit Domain Security Policy And Activate Pending Security Policy Changes .....	38
Activity 5C – Investigate some security Reports .....	43
Role-Based Security Groups .....	46
Activity 6A – Create Role-Based Constrained Security Group .....	55
Activity 6B – Add Contingent Worker Expediter To The Business Process Security Policy .....	61
Service Center-Based Security Groups.....	67
Activity 7A – Create Service Center Called Outsourced Global HelpDesk & Representative.....	70
Activity 7B – Create and Deploy Service Center-Based Security Group .....	72
Activity 7C – Test Service Center-Based Security .....	76
Activity 7D – Optional - Configure Service Center manager Role.....	79

## Configurable Security Fundamentals 24

---

Job-Based Security Groups.....	82
Activity 8 – Create and Deploy Job-Based Security Group .....	86
Integration System Security Groups.....	94
Segment-Based Security Groups .....	96
Activity 9 – Configure & Deploy Segmented Security .....	101
Location Membership and Organization Membership Groups .....	107
Activity 10 – Create membership Based (location and Organization) security groups .....	109
Combinations of Security Groups .....	113
Activity 11A – Create an Intersection security group .....	117
Copy Security Groups.....	123
Activity 11B – OPTIONAL - Configure Intersection with Exclusion in membership .....	124
Activity 11C – Optional Challenge Activity .....	133
Level-Based Security Groups .....	134
Activity 12 Create Level-Based Security Group .....	138
<b>Security Tips.....</b>	<b>143</b>
Security Methodology.....	143
Managing Workforce Security Assignments.....	144
Security Policy Restrictions .....	144
Activating Previous Timestamps.....	146
Security-Related Reports.....	147
Optional Lab – Self Study: Security Reports .....	152
Troubleshoot Security - FAQ.....	155
Custom Security Reports .....	157
Review.....	158
Where to go from here .....	159
Appendix.....	160
Walkthrough Solution – One Role, Multiple Role-Based Security Groups.....	161
Workshop 1 –Role-Based Constrained Security Groups .....	162
Workshop 2 –Role-Based Unconstrained Security Group .....	170
Workshop 3 – Constrain Role-based Access To Both The Supervisory and Location Hierarchy .....	175
Review questions & Answers .....	181

## CONFIGURABLE SECURITY FUNDAMENTALS

In this course you will work through hands on activities that are designed to build a foundation of knowledge in Workday's Configurable Security model. You will gain an understanding of the various types of Security Groups including User-based, Role-based and Job-based. You will also learn how to navigate through Workday's Functional Areas, Domains and Sub-Domains. Lastly, you will edit both Domain Security Policies as well as Business Process Security Policies.

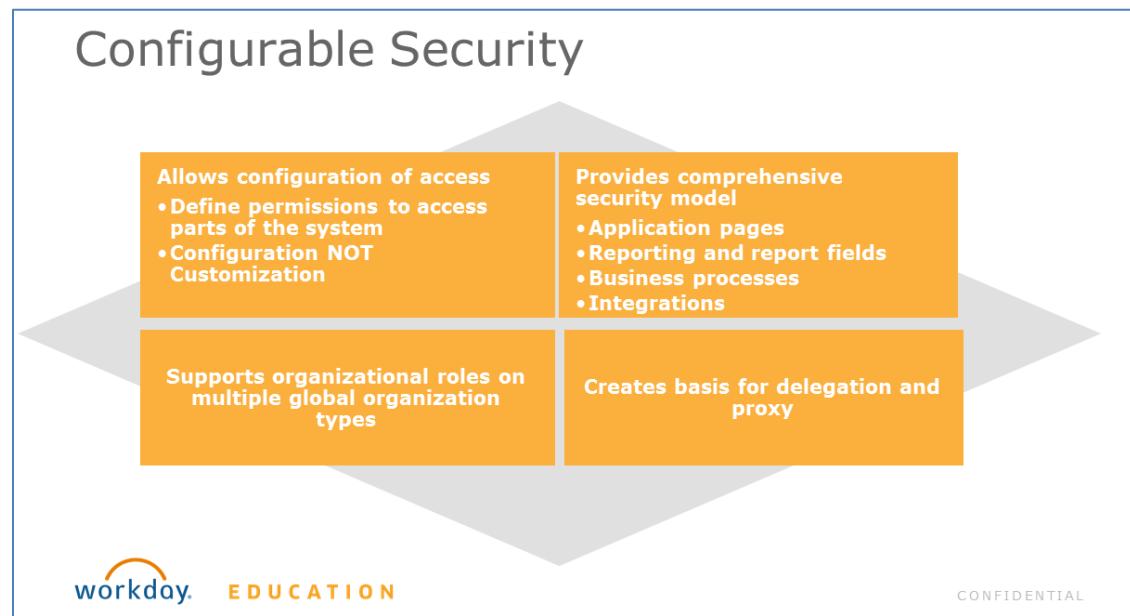
### AGENDA:

- Security Landscape
  - Functional Areas, Domains and Sub-Domains
  - Domain Security Policies
  - Business Process Security Policies
- Security Groups
  - Delivered & Assigned Security Group Types
  - User-Based Security Groups
  - Role-Based Security Groups
  - Service Center Security Groups
  - Job-Based Security Groups
  - Segment Security Groups
  - Membership Security Groups
  - Aggregation Security Groups
  - Intersection Security Groups
  - Level Based Security Groups
- Security Tips
  - Recommendations
  - Managing Workforce Security Assignments
  - Security Configuration Restrictions
  - Reports and Other Tools

# SECURITY LANDSCAPE

## WHAT IS CONFIGURABLE SECURITY

Workday provides a configurable security framework enabling customers to control view vs. modify access to the Workday application via security groups and security policy updates. Workday's security framework supports your organizational structures, roles, global models, and is integrated across the application, from the user interface pages, to reports, integrations and business processes. Workday security configurations are tenanted and update safe and provide a comprehensive model across the application.



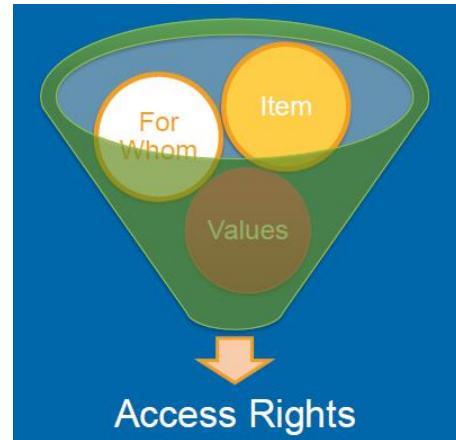
This class focuses on the configurable security framework where you can authorize access to the application via security groups and security policy updates. There are other areas of security that provide additional controls that are not in the scope of this class, but are important for your greater security strategy and implementation.

Please see related documentation and available resources around:

- Authentication
- Audit
- Data Masking
- Data Purging

Configurable Security helps to answer questions such as:

1. Can a given user run a task or get to a given secured **item** in Workday? (e.g., a delivered report or task)
2. Once there, what target instances does the user have access to for that item? "**for whom**" can they see data? (e.g., can the user see data for all workers when running a report about workers, or create an expense report for anyone?)
3. Can you segment the actual items or **values** a user sees? For what items/lines/values?



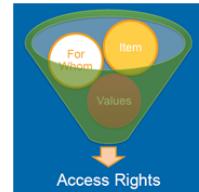
## Configurable Security Answers

1. Can you run the task or **item**?

Tasks and Reports

Create Expense Report for Applicant

**Create Expense Report**



2. **For whom?** (Context)

- o Yourself?
  - requires self-service access
- o Anyone?

### Create Expense Report

Use this task to enter an expense report into the system. Please determine if you would like to create

Expense Report Information

\* Employee: Logan McNeil

\* Global Modern Service

\* 02/10/2014

Create Blank Expense Report

Copy Details From Existing Expense Report

CONFIDENTIAL

3. For what **values**?

- o Do you have access to every value, or a subset?
  - Segments

Expense Report Line

Date: 02/10/2014

Credit Card Transaction

Expense Item:

search

Top > By Alphabetical Order

Airfare  
Car Rental & Gas  
Dues & Subscriptions  
Hotel Accommodations  
In Room Video  
International Airfare  
International Room Rates  
Internet Access Fees  
Laundry

Let's now take a closer look at the security framework.

## SECURITY LANDSCAPE

### FUNCTIONAL AREAS, DOMAIN AND BUSINESS PROCESSES

As you look to configure access in Workday, it is important to understand **how the system is packaged and delivered** and **how you can configure access to it**. At the highest level, Workday delivers the application in **functional areas**. Functional areas can include such areas as: Staffing, Benefits, Core Compensation, Financial Accounting or Procurement. Each functional area is then broken down into **Domains** and **Business Process Types**.

**Domains** are collections of items that share the same security. These items can include tasks, delivered reports, report data sources or custom report fields and web service operations and tasks.

- ✓ **Workday determines the secured items within each domain.**
- ✓ **You cannot change what delivered items are in what domains.**

#### Domain Security Policies

Every domain has its own domain security policy. It is in these domain security policies that you can configure which security groups have access to the items in the domain. Access can be configured as view only, or view and modify access. For web service operations secured in a domain, the access is configured with Get vs. Put permissions.

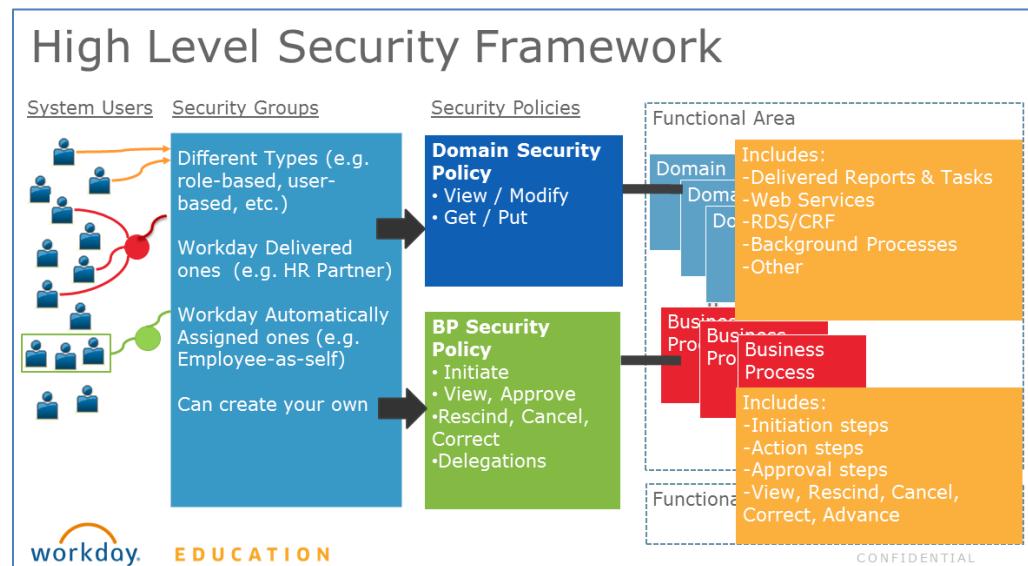
- ✓ **Access is configured at the domain level, not item-by-item. Users with access to a domain will have access to all items secured in that domain.**

Business process types represent the events or transactions in Workday that can be automated using Workday's business process framework.

#### Business Process Security Policies

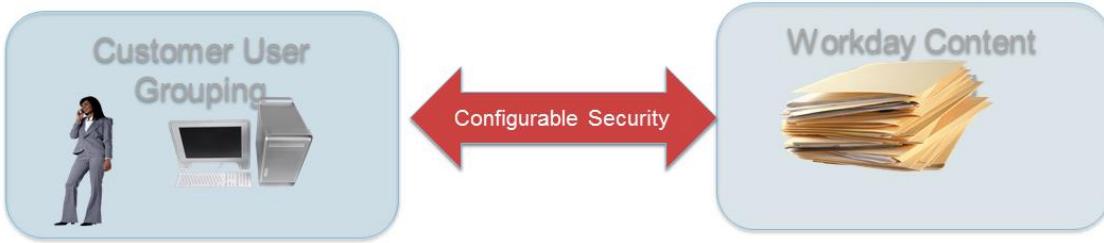
Each business process type has its own security policy. It is in these business process security policies that you can configure which security groups can for example, initiate the business process, or do actions steps, or approve, rescind, cancel or correct the business transaction.

Lastly, users are identified via security groups and security groups are configured in security policies.



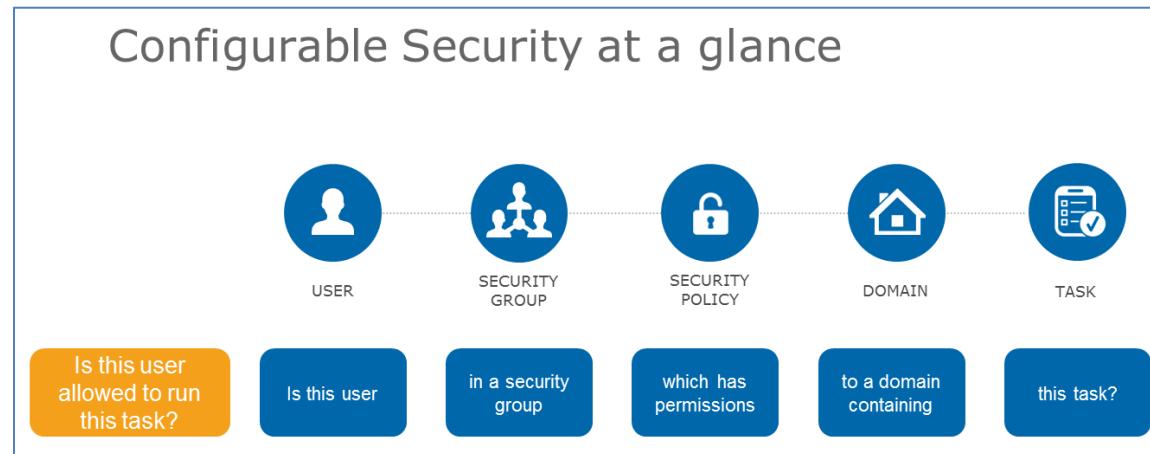
Workday's configurable security framework allows you to say **who can do what**.

Configurable security acts as a bridge between Workday-owned metadata and customer-owned tenanted access to functionality. By configuring domain or business process security policies with needed security groups, customers can configure the bridge between Workday's what and customers' who.



- ✓ **You can** configure access to domains by configuring domain security policies with needed security groups.
- ✓ **You can** configure access to business process types by configuring business process security policies with security groups
- ✓ **You can** create security groups
- ✓ **You cannot** change what delivered items are in a domain.
- ✓ **You cannot** add new BP types

As an example, to see if a user has access to a given task or item, that user must have a security group that is configured with permissions in the security policy that secures that item.



## DOMAIN SECURITY POLICY

Every domain has its own domain security policy. Domain security policies define what security groups have access to the securable items in that domain.

## BUSINESS PROCESS SECURITY POLICY

Business process security policies are collections of securable items related to business processes, including initiation steps and actions steps. They also are where you specify permissions for actions on events, for example the ability to view, approve, rescind, cancel, and correct a given event.

## SECURITY GROUPS

A security group allows you to identify a set of users to grant access in Workday. Users can have many security groups on their Workday account. A user must have access to a domain or business process security policy via at least one permitted security group in order to access secured items in that policy.



## THE FUNCTIONAL AREAS REPORT

Workday provides a helpful 'top down' report called the **Functional Areas** report. This report will show for a given Workday Solution, the functional areas and the domains and business process types for each functional area. You can also see if a given functional area is enabled in your tenant or not. To enable or disable a functional area, run the **Maintain Functional Areas** task. From this report, you can also drill into the details of a given domain to see the secured items and even the security policy.

The screenshot shows the "Functional Areas" report interface. Key elements include:

- Solution**: Labeled with a green callout, this section shows the "Core Compensation" solution.
- Functional Area**: Labeled with a green callout, this section lists functional areas such as Core Compensation, Customer Accounts, Customers, Endowment Accounting, Expenses, Financial Accounting, Grants Management, Implementation, Integration, Jobs & Positions, Onboarding, Organizations and Roles, Payroll Interface, Performance and Goals, and Personal Data.
- Business Processes**: Labeled with a green callout, this section shows the "Academic Unit" business process.
- Domains**: Labeled with a green callout, this section shows the "Academic Units" domain, which includes Academic Unit Hierarchies, Directors, Academic Unit Hierarchies, Roles, Academic Unit Hierarchies, View, Academic Units: Directors, Academic Units: Professors, Academic Units: Roles, Academic Units: View, Affiliate Data, and Contact Data.



## ACTIVITY 1 – NAVIGATE FUNCTIONAL AREAS

**Scenario:** In order to view the manner in which Workday is broken down, you will logon as Logan McNeil, the Security Administrator, to run the Functional Areas report. You will also use the View Domain report to look at the details for a particular Workday Domain.

### OVERVIEW

As the Security Administrator Logan McNeil will perform the following actions:

1. View Functional Areas
2. View Domain
3. View Domain Security Policy

### TASK 1: RUN FUNCTIONAL AREAS REPORT

#### ⊕ As Logan McNeil (lmcneil)

1. From the search box, search for the string '*fun area*'
2. Click on the **Functional Areas** report
3. How many business processes are in the **Expenses** functional area? \_\_\_\_\_
4. How many domains are in the **Expenses** functional area\_\_\_\_\_
5. Click on the **Manage: Expense Report** domain to *view the domain*:

#### View Domain Manage: Expense Report ...

Domain Name	Manage: Expense Report
Description	This domain provides access to manage expense reports on behalf of others and view related reporting.
Domain Security Policy	
Functional Areas	Expenses
Subdomains	Manage: Expense Report Attachments
Allowed Security Group Types	Roles - Company Unconstrained Groups

6. How many total items are secured in this domain? \_\_\_\_\_
7. How many reports & tasks are secured in this domain? \_\_\_\_\_

## Configurable Security Fundamentals 24

8. How many web services are secured in this domain? \_\_\_\_\_

9. Click on the  icon to view the **Domain Security Policy**

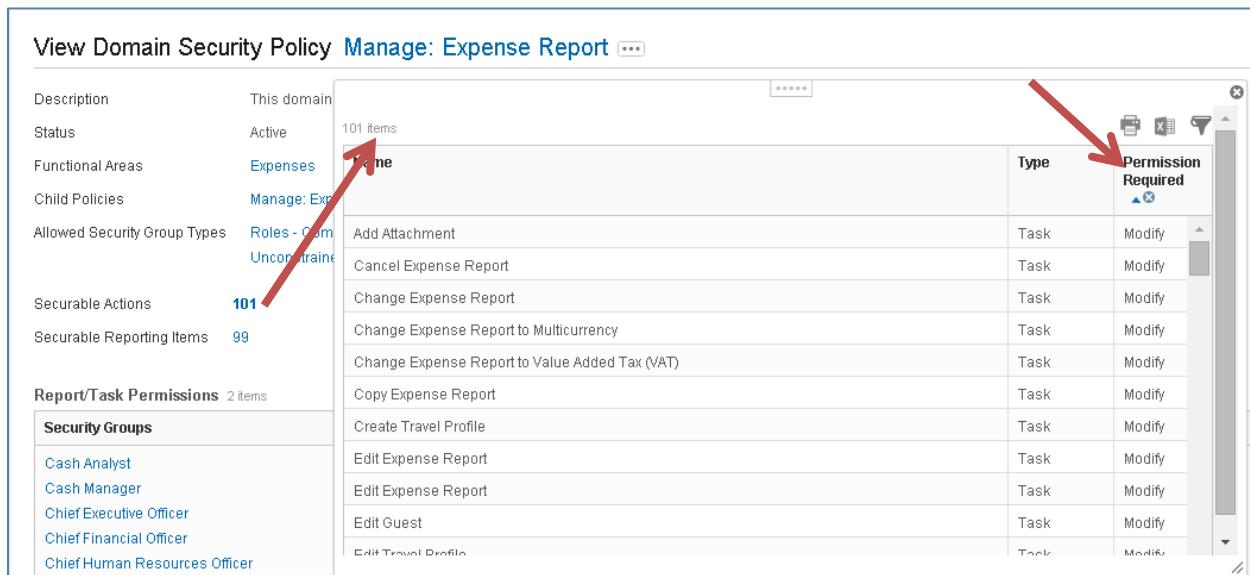
10. How many security groups have View only access under the Reports/Tasks Permissions? \_\_\_\_\_

11. Which Security Groups have View and Modify under the Reports/Tasks Permissions?

\_\_\_\_\_

12. Click on the **Securable Actions** link to see the list of securable actions. Sort the actions by *Permission Required* to see which actions require modify permissions vs. view. Users with security groups configured with modify permissions will be able to access these actions in Workday.

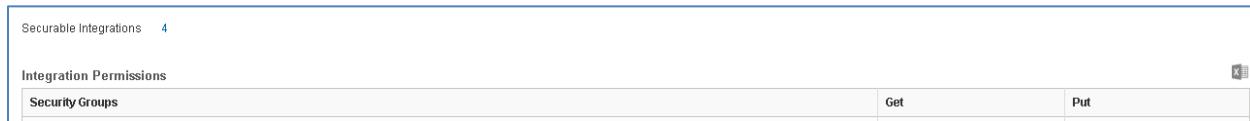
What permission (View or Modify) would a user need to run the delivered action: *Average Expense Report Total?* \_\_\_\_\_



The screenshot shows the 'View Domain Security Policy' page for the 'Manage: Expense Report' domain. On the left, there's a sidebar with various settings like Description (This domain), Status (Active), Functional Areas (Expenses), Child Policies (Manage: Expenses), Allowed Security Group Types (Roles - Compliant, Unconstrained), Securable Actions (101), and Securable Reporting Items (99). Below that is a 'Report/Task Permissions' section with 2 items, followed by a 'Security Groups' section listing several roles: Cash Analyst, Cash Manager, Chief Executive Officer, Chief Financial Officer, and Chief Human Resources Officer. The main content area is a table titled '101 items' showing securable actions. The columns are 'Name', 'Type', and 'Permission Required'. A red arrow points to the 'Name' column header, and another red arrow points to the 'Permission Required' column header, which is sorted in descending order (Modify at the top).

13. How many security groups have Get and Put access to the securable integrations (i.e. the 4 web services) in this security policy (hint: scroll down and see the Integration permissions)

\_\_\_\_\_



The screenshot shows the 'Integration Permissions' section. It displays a table with 4 rows, each representing a securable integration. The columns are 'Security Groups', 'Get', and 'Put'. In all four rows, the 'Get' checkbox is checked, while the 'Put' checkbox is unchecked. The table has a header row and 4 data rows.

Security Groups	Get	Put
	✓	✗
	✓	✗
	✓	✗
	✓	✗

(End of Activity)

## A CLOSER LOOK AT SECURITY POLICIES

Securable items are grouped into domains and business processes, and each grouping has a corresponding domain or business process security policy. These groupings are predefined and you cannot change them. You can edit which security groups can access the securable items in a domain or business process, but you cannot edit the securable items in a policy or delete a policy. Each functional area contains security policies for items such as actions, reporting items, or business process actions.

There are two types of security policies: domain and business process.

Let's take a closer look at domain security policies.

### DOMAIN SECURITY POLICIES

Domain Security Policies are the bridge between Domains and Security Groups. Domain Security Policy configurations involve two sections: **Report/Task Permissions** and **Integration Permissions**. You can add or remove security groups and grant security groups View only or View and Modify access to the reporting items and securable actions. If the domain contains web services, they will show as securable integrations whereby you can configure needed security groups with the Get ("view") or Put ("modify") access under integrations permissions.

Report/Task Permissions	
Security Groups	View      Modify
Accountant	Yes
Accounting Manager	
Controller	
Finance Auditor	
Credit Card Administrator	Yes
Implementers	Yes

Integration Permissions	
Security Groups	Get      Put
Credit Card Administrator	Yes
Credit Card System	
Implementers	Yes

Some secured items may be included in more than one domain security policy. Workers who are granted different levels of access permission in different domains get the most access granted.

## INHERITANCE IN DOMAIN SECURITY POLICIES

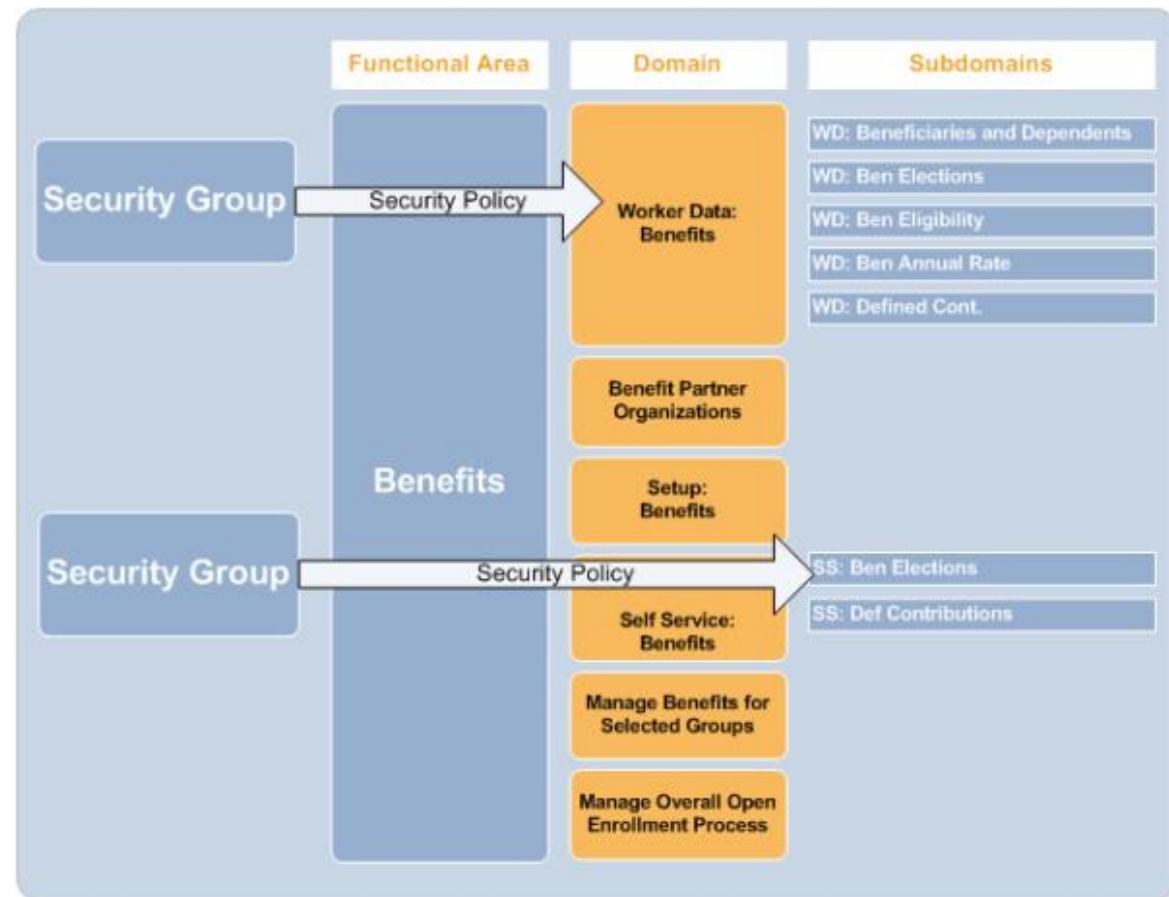
Some Domain security policies have a hierarchical relationship with child policies, which can **inherit the security policy settings of the parent**. There is no inheritance for business process security policies.

The parent security policy is actually a master control that allows you to set which security groups have access permissions in all the children. If you add or remove a security group in the parent policy, the change appears in all the children.

You can turn off inheritance in any child security policy by editing it using the **Override Parent Permissions** option. After that, changes made in the parent no longer have any effect in that child policy. Editing a child security policy does not affect inheritance in any of the others. You can restore inheritance in a child policy by clicking the **Use Parent Permissions** button.



Whether a child security policy is currently inheriting permissions from its parent is shown in the Status field, under the Security policy title. If it is inheriting, the status says "Active - Inheriting parent permissions".



## SECURITY POLICY REPORTS

The **Domain Security Policies for Functional Area** report provides a description of each domain, along with access to any sub-domains. From here you can access security policies. Domain security policies can be configured at either the domain or sub-domain level. Domain Policies are inherited by sub-domains, but inheritance is broken by editing the sub-domain policy.

You can see if a subdomain is inheriting or overriding its parent domain permissions. This information is visible in the domain security policy status and you can also see the option to “Override Parent Permissions” or “Use Parent Permissions”.

This screenshot shows the Workday interface for managing security permissions. On the left, a navigation tree lists various worker data categories. In the center, a "Report/Task Permissions" panel displays two sections: "Security Groups" and "Integration Permissions". A blue callout bubble points to the "Integration Permissions" section, stating: "This subdomain is overriding parent permissions, i.e. has its own permission configurations. You can go back and use parent permissions, i.e. inherit the permission from the parent domain's policy using the 'Use Parent Permissions' button." At the bottom of the panel are "Edit Permissions" and "Use Parent Permissions" buttons.

This screenshot shows the same Workday interface as above, but with a different configuration. The blue callout bubble now states: "This subdomain is inheriting the parent domain policy permissions. You can override the parent permissions and edit specific permissions for this subdomain using the 'Override Parent Permissions' button." The "Override Parent Permissions" button is highlighted with a blue arrow pointing to it.



## ACTIVITY 2 – NAVIGATE DOMAIN SECURITY POLICIES

Scenario: You will logon as Logan McNeil, the Security Administrator, to run the Domain Security Policies for Functional Areas report.

### OVERVIEW

As the Security Administrator Logan McNeil will perform the following actions:

1. Review Domain Security Policies

### TASK 1: RUN DOMAIN SECURITY POLICIES FOR FUNCTIONAL AREAS REPORT

**As Logan McNeil (lmcneil)**

1. Search for the string '*dom sec fun*'
2. Click on the **Domain Security Policies for Functional Area** report
3. Click the icon to select the **Core Compensation** functional area
4. Click the **OK** button
5. Click on the **Worker Data: Compensation** super domain
6. How many securable actions are in the Worker Data: Compensation Super-domain? \_\_\_\_\_
7. How many securable reporting items are in the Worker Data: Compensation Super-domain? \_\_\_\_\_
8. How many security groups have view and modify access? \_\_\_\_\_
9. How many Sub-domains exist in the Worker Data: Compensation Super-domain? \_\_\_\_\_
10. How many subdomains are inheriting the permissions from the Worker Data: Compensation domain?  
\_\_\_\_\_

(End of Activity)

## BUSINESS PROCESS SECURITY POLICIES

A business process security policy applies to a single business process type. It controls access to the securable items in the business process by specifying which security groups have permission to access each securable item. The securable items in a business process security policy are:

- Initiation steps
- Action steps
- Approvals
- Actions on the process: view, rescind, cancel, and correct

Business process security policies contain such securable items as initiation steps, step actions, and actions on the process as a whole: view, approve, rescind, cancel, and correct. A business process security policy also allows you to specify whether the business process can be delegated to others.

If you copy a business process definition, all definitions of the same business process type, will share the same security policy. **There is one business process security policy per business process type.**

Business Process security policies look very different than domain security policies. They include several sections:

- Who Can Start the Business Process (Initiating actions)
- Who can do Action Steps in the Business Process (Allowed Actions)
- Who can do Actions on Entire Business Process (View, Approve, Rescind, Cancel, Correct, Advance)
- Other Policy Restrictions & Settings

### Edit Business Process Security Policy Expense Report Event

Description	Create an expense report to reimburse an employee, contingent worker, or applicant.
Functional Area(s)	Expenses
Security Group Types Allowed for Initiating Actions	Roles - Business Unit Roles - Company 

#### Who Can Start the Business Process

Initiating Action	Create Expense Report
Description	Create Expense Report
Security Groups	<input type="text" value="search"/>  <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Contingent Worker As Self</li> <li><input checked="" type="checkbox"/> Employee As Self</li> </ul>
Security Groups who can delegate this action to others	<input type="text" value="search"/>  <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Contingent Worker As Self</li> <li><input checked="" type="checkbox"/> Employee As Self</li> </ul>

### Who Can Do Action Steps in the Business Process

Action Step      Review Expense Report

Security Groups

search	
✖ Expense Partner	
✖ HR Partner	

### Who Can Do Actions on Entire Business Process

Action      View All

Security Groups

search	
✖ Accounting Manager	

Action      Approve

Security Groups

search	
✖ Accounting Manager	
✖ Alternate Approver	

Action      Correct

Security Groups

search	
✖ Accounting Manager	
✖ Implementers	

Note      Security Groups on the Correct policy are also granted 'View All' access for transactions still possibly correctable.

Action      Reassign Tasks

Security Groups

search	
--------	--

Note      Security Groups assigned to the Business Process Administration domain will also be able to reassign tasks.

### Policy Restrictions

Allow Business Process Delegation     

Hide Comments from Worker     

Hide Details from Worker     

Disable Comments     

### Attachment Settings in BP Toolbar

Allow Attachments within Emails

The **Business Process Policies for Functional Area** report provides a description of the business process. It shows all business processes and sub-processes. From here you can view and edit security policy permissions. Business processes can have sub processes. Each process has its own bp security policy. There is no inheritance of business process security policy permissions.

Business Process Security Policies for Functional Area <a href="#">Core Compensation</a> <a href="#">...</a> <a href="#"></a>									
Description	Set up and manage compensation grades, pay ranges / levels, steps, and eligibility rules. Manage all core aspects of employee compensation, hourly, allowance, and commission. Manage plan and pay range adjustments, reimbursable allowance plans, severance pay and create...								
Status	Active								
<a href="#"> Acknowledge Compensation State...</a> <a href="#"> Automatic Employee Compensation...</a> <a href="#"> Change Default Compensation</a> <a href="#"> Compensation Change for Compe...</a> <a href="#"> Create Statutory Compensation St...</a> <a href="#"> Employee Compensation Event for...</a> <a href="#"> Propose Compensation</a> <a href="#"> Propose Compensation Change</a> <a href="#"> Propose Compensation Offer</a> <a href="#"> Propose Reimbursable Allowance ...</a> <a href="#"> Request Compensation Change</a> <a href="#"> Request Compensation Change fo...</a> <a href="#"> Request One-Time Payment</a> <a href="#"> Request One-Time Payment Offer</a>	<p>Business Process Type <a href="#">Propose Compensation</a></p> <h3>Who Can Start the Business Process</h3> <table> <tr> <td>Initiating Action</td> <td><a href="#">Propose Compensation</a></td> </tr> <tr> <td>Security Groups</td> <td><a href="#">Alternate Approver</a> <a href="#">Compensation Administrator</a> <a href="#">Compensation Partner</a> <a href="#">HR Administrator</a> <a href="#">HR Partner</a> <a href="#">HR Partner (By Location)</a> <a href="#">Manager</a></td> </tr> <tr> <td>Initiating Action</td> <td><a href="#">Propose Base Pay</a></td> </tr> <tr> <td>Security Groups</td> <td><a href="#">Alternate Approver</a> <a href="#">Compensation Administrator</a> <a href="#">Compensation Partner</a> <a href="#">HR Administrator</a> <a href="#">HR Partner</a></td> </tr> </table>	Initiating Action	<a href="#">Propose Compensation</a>	Security Groups	<a href="#">Alternate Approver</a> <a href="#">Compensation Administrator</a> <a href="#">Compensation Partner</a> <a href="#">HR Administrator</a> <a href="#">HR Partner</a> <a href="#">HR Partner (By Location)</a> <a href="#">Manager</a>	Initiating Action	<a href="#">Propose Base Pay</a>	Security Groups	<a href="#">Alternate Approver</a> <a href="#">Compensation Administrator</a> <a href="#">Compensation Partner</a> <a href="#">HR Administrator</a> <a href="#">HR Partner</a>
Initiating Action	<a href="#">Propose Compensation</a>								
Security Groups	<a href="#">Alternate Approver</a> <a href="#">Compensation Administrator</a> <a href="#">Compensation Partner</a> <a href="#">HR Administrator</a> <a href="#">HR Partner</a> <a href="#">HR Partner (By Location)</a> <a href="#">Manager</a>								
Initiating Action	<a href="#">Propose Base Pay</a>								
Security Groups	<a href="#">Alternate Approver</a> <a href="#">Compensation Administrator</a> <a href="#">Compensation Partner</a> <a href="#">HR Administrator</a> <a href="#">HR Partner</a>								



## ACTIVITY 3 – NAVIGATE BUSINESS PROCESS SECURITY POLICIES

**Scenario:** You will logon as Logan McNeil and run the Business Process Security Policies for Functional Area report to view Business Process Security Policies in a Functional Area

**As Logan McNeil (lmcneil)**

1. Search for the string '*bus sec fun*'
2. Click on the **Business Process Security Policies for Functional Area** report
3. Click the icon to select the **Core Compensation** Functional Area
4. Click the **OK** button
5. Click on the **Propose Compensation** business process.
6. What action(s) initiates this business process? \_\_\_\_\_
7. How many security groups can rescind a propose compensation event? \_\_\_\_\_
8. Rerun the **Business Process Security Policies for Functional Area** report by clicking the **change** icon

Business Process Security Policies for Functional Area **Core Compensation**

Description Set up and manage compensation grades, pay ranges / levels, steps, and eligibility rules. Manage all core aspects of employee compensation, including hourly allowance and commission. Manage plan and pay range adjustments, reimbursable allowance plans, severance pay and other related compensation.

Change

9. This time select the functional area: **Common Financial Management**
10. Which security groups can initiate a period close event? \_\_\_\_\_
11. How many security groups can view a period close event? \_\_\_\_\_

(End of Activity)

## MANAGING SECURITY

There are two main security groups that allow you to control who manages security in your tenant: **Security Configurator** and **Security Administrator**. The **Security Configurator** security group has greater access to such tasks as, creating security groups, modifying security policies and activating security in the tenant. The **Security Administrator** security group has access to tasks around maintaining Workday accounts, password rules and security assignments. You can either centralize or segregate these responsibilities amongst individual users by **assigning these security groups to the same or to different users.**

In our training tenant, Logan McNeil is assigned to both security groups.

The screenshot shows a report titled 'View Security Groups for User lmcneil / Logan McNeil'. It lists two security groups: 'Security Configurator' and 'Security Partner'.

Security Group
Security Configurator
Security Partner

*She is also a member of the Security Partner, role-based constrained security group. The **Security Partner** role-based constrained security group is a helpful way to decentralize security tasks to users by limiting their access to a given organization. More on role-based security groups later in this class.*

Run the **View Security Group** report to see details for each of these security groups. Remember that security groups are configured with access to domains and business process security policies. View each domain to see the secured items in the domain.

The screenshot shows a report titled 'View User-Based Security Group Security Configurator'. It displays the following details:

- Name: Security Configurator
- Comment: Configure domain and business process security policies regardless of organization. Assign workers to security groups. No approval authority.
- Context Type: Unconstrained
- Administered by Security Groups: Security Configurator

Under the 'Members' section, there is a table for 'Domain Security Policy Permissions' with 9 items:

Operation	Domain Security Policy	Domain Security Policies Inheriting Permission	Functional Areas
View and Modify	Security Configuration		System
View and Modify	User-Based Security Group Administration		System
View Only	Landing Page - My Workday		System
View and Modify	Segmented Setup	Document Categories Segmented Setup	System
View and Modify	Compensation Segmented Setup		System
View and Modify	Expenses Segmented Setup		System
View Only	Landing Page - Workbench		System
View Only	Big Data Analytics: Administrative Access		System
View and Modify	Quotations Segmented Setup		Custom

## SECURITY PROFILES

Users in Workday can have many security groups on their security profile. These security groups can be:

- **Workday Assigned** (e.g. Employee-as-self, All Users)
- **Manually Assigned** (e.g. Report Writer, Finance Administrator)
- **Derived** (E.g. HR Partner, Expense Analyst)

Run: **View Security Groups for User** to see the security groups for a given Workday user

You can also test if a user is a member of a security group, using the report: **Test Security Group Membership**.



A user's access is a union of all of their security group permissions. A user must have access to a domain or business process security policy via at least one security group in order to have access to that area of Workday. Run **Security Analysis for Workday Account** to see a user's access at their account level, i.e. a union of all their security groups.

## WORKDAY ASSIGNED SECURITY GROUPS

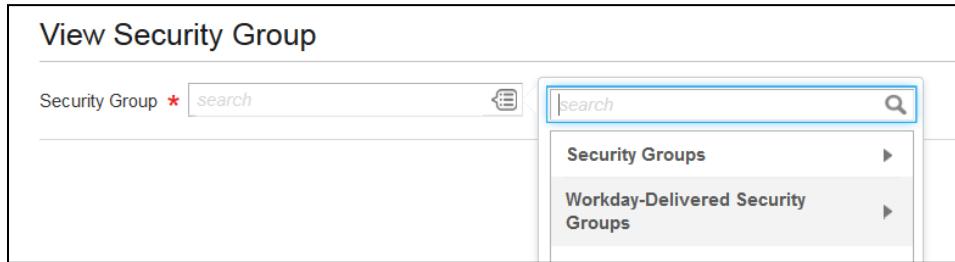
Workday delivers security groups as a starting point, including some security groups that are automatically assigned and cannot be changed. Membership in these Workday assigned security groups is automatically populated by Workday. You cannot create, edit, or delete these groups. Some examples of Workday assigned security groups are:

- All Contingent Workers
- All Employees
- All Project Members
- All Retirees
- All Terminees
- All Users
- Contingent Worker as Self
- Employee as Self
- Pre-Contingent Worker as Self
- Pre-Employee as Self
- Project Member as Self
- Retiree as Self
- Supplier Contact as Self
- Terminee as Self
- Implementers
- Initiator
- Manager's Manager
- Role Maintainer

For example, Pre-Employee As Self Security Access for Contingent Workers: Workday assigns a contingent worker who is being converted to an employee to the **Pre-Employee as Self** security group. This accommodates Onboarding tasks that the Pre-Employee needs to perform.

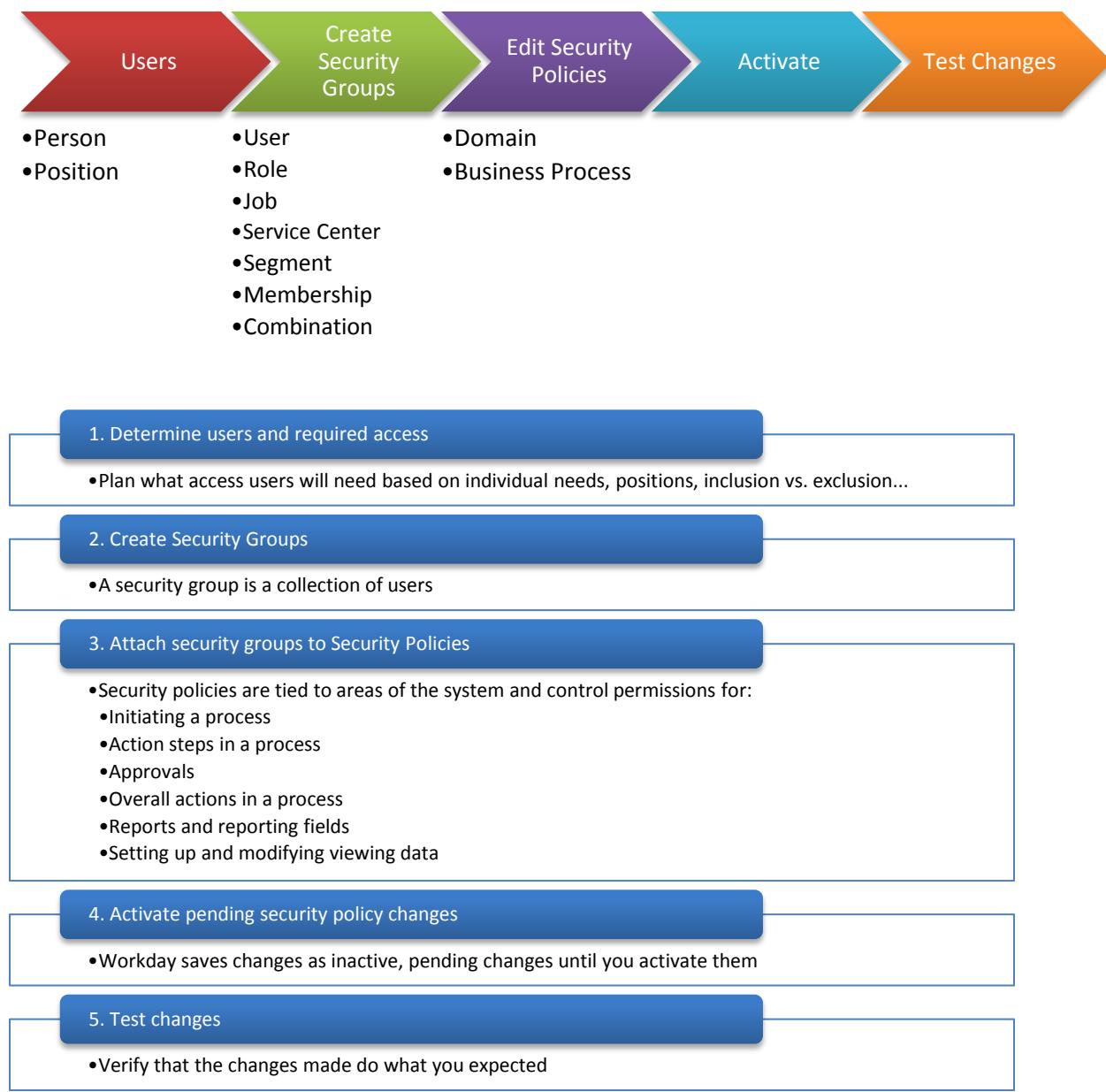
With every Workday update, there could be new delivered security groups that will be automatically assigned. Some recent examples include **Manager for Majority of Event** which is used only in employee reviews, and **Academic Affiliate as self**.

For a complete list of Workday delivered/assigned security groups, run View Security Group and select Workday Delivered Security groups.



## STEPS FOR CONFIGURING SECURITY

The following graphic outlines the steps for configuring security. In order to grant a user access in Workday, that **user must be associated with a security group**. You can use delivered security groups or create your own as needed. **Security groups come in different types:** user-based, role-based, job-based, etc. Workday determines the security group types. You cannot create new types. **Security groups must then be configured in security policies**, domain and/or business process security policies. You get to configure and control what domain or business process security policies a security group has access to. When changes are made to a security policy, those changes are saved, but are pending until the **Activate Pending Security Policy Changes** task is run. Once you activate those changes, **Test, Test, and Test!**



## PROXY SESSIONS

**Proxy Access Policies** are a very useful mechanism for testing. Proxy access can be set up for use in any tenant environment *except* production. This security configuration is a real time saver when testing business processes or reports in your Sandbox or implementation tenants, because you don't have to log in and out as multiple users.

When you are signed into a proxy session, you can perform any action in Workday that the user on whose behalf you are authorized to do. Functionality that requires connecting to another service is not supported, including integrations, scheduled reports, business form printing, background conversions. Additionally, proxy users cannot access documents on the W: drive, Apple Push Notifications, email, notifications received through the user interface nor solutions.

Some key points and restrictions to keep in mind around proxy access:

- You can only configure one policy per environment
- Proxy access policies apply to non-production environments only
- Only unconstrained security groups can be configured with proxy access
- You cannot start proxy session when acting as a delegate
- No support for connecting to another service when in proxy mode.
  - Integrations
  - Scheduled reports
  - Business Form printing
- No access to W: drive documents, notifications when in proxy mode.

The screenshot shows the 'Create Proxy Access Policy' page. At the top, there are two dropdown menus: 'Restricted to Environment' and 'Do Not Allow Proxy on Behalf Of'. A blue callout bubble points to the first dropdown with the text 'Select which environment to enable'. Below these are two tables. The first table has columns for 'Order', '+', '-' buttons, and search fields for 'Groups That Can Proxy' and 'On Behalf Of'. A blue callout bubble points to the 'Groups That Can Proxy' column with the text 'Select the security groups that can start proxy session'. The second table has a similar structure. A blue callout bubble points to the 'On Behalf Of' column with the text 'Select security groups to "act as"'. The bottom of the page features a navigation bar with links like 'Workday Home', 'Log Out', and 'Help'.

## ORDER MATTERS

Workday evaluates the proxy access rules **in the order in which they are listed**, until a rule applies. Rules are checked in **order based on the user on whose behalf you are trying to proxy**. Once the first rule is found for that proxy on behalf of user, the system will check if you have a permitted security group to proxy on behalf of that user or not and stops.

In the example below, if you have a requirement where:

- The **Finance Administrator** security group can proxy as the **Chief Financial Officer**.
- The **HR Administrator** security group can proxy as any employee (including the Chief Financial Officer).

When a user tries to proxy on behalf of a user in the **Chief Financial Officer** security group, the system will check the rules in order to see which rule would apply for proxying on behalf of the Chief Financial Officer security group.

Once the first rule is found that applies to proxying on behalf of the Chief Financial Officer, the system will then check to see if you have a permitted security group to start the proxy. If permitted, you can proxy. If not, you cannot proxy and no more conditions or rules are checked. In our example requirement, you must include HR Administrator in each rule order, else the HR Administrator would not be able to proxy as the Chief Financial Officer.

Create Proxy Access Policy		
Proxy Access Policy	(empty)	
Restricted to Environment	<input type="text"/> Implementation	
Do Not Allow Proxy on Behalf Of	<input type="text"/>	
2 Items		
Order	*Groups That Can Proxy	On Behalf Of
+ -	search x Finance Administrator	search x Chief Financial Officer
+ -	HR Administrator	All Employees

Create Proxy Access Policy		
Proxy Access Policy	(empty)	
Restricted to Environment	<input type="text"/> Implementation	
Do Not Allow Proxy on Behalf Of	<input type="text"/>	
2 Items		
Order	*Groups That Can Proxy	*On Behalf Of
+ -	search x HR Administrator x Finance Administrator	search x Chief Financial Officer
+ -	HR Administrator	All Employees

**If you have more than one rule in your proxy access policy, it is important to include all security groups that can proxy on behalf of a given security group in all rules.**



## ACTIVITY 4 – CREATE PROXY ACCESS POLICY

**Scenario:** You will logon as Logan McNeil, the Security Configurator, to create a security access policy. This policy will allow you to test configurations without logging out and back in as multiple users

### OVERVIEW

As the Security Configurator Logan McNeil will perform the following actions:

1. Create Proxy Access Policy
2. Test access

### TASK 1: CREATE PROXY ACCESS POLICY

#### As Logan McNeil (lmcneil)

1. Search for the string '*create proxy*'
2. Click on the link to run the task to **Create Proxy Access Policy**
3. In the Restricted to Environment field, use the prompt icon to select **Training**
4. Select **All Employees** as **Groups That Can Proxy**
5. Select **All Employees** in the **On Behalf Of** field
6. Click the **OK** button Your policy should look like this:

Create Proxy Access Policy									
Proxy Access Policy (empty)									
Restricted to Environment		<input style="width: 100px; height: 20px; border: 1px solid #ccc; border-radius: 5px; padding: 2px 5px; margin-right: 5px;" type="text" value="search"/> <span style="color: red;">*</span> <input style="border: 1px solid #ccc; border-radius: 5px; padding: 2px 10px;" type="button" value="Training"/>							
Do Not Allow Proxy on Behalf Of									
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 10%;">Order</th> <th style="width: 40%;">*Groups That Can Proxy</th> <th style="width: 10%;">*On Behalf Of</th> </tr> </thead> <tbody> <tr> <td style="text-align: center; vertical-align: middle;"> <span style="font-size: 2em;">+</span> <span style="font-size: 1.5em;">-</span> </td> <td style="text-align: center; vertical-align: middle;"> <span style="font-size: 1.5em;">▼ ▲</span> </td> <td style="text-align: center; vertical-align: middle;"> <input style="width: 100px; height: 20px; border: 1px solid #ccc; border-radius: 5px; padding: 2px 5px; margin-right: 5px;" type="text" value="search"/> <span style="color: red;">*</span> <input style="border: 1px solid #ccc; border-radius: 5px; padding: 2px 10px;" type="button" value="All Employees"/> </td> </tr> </tbody> </table>				Order	*Groups That Can Proxy	*On Behalf Of	<span style="font-size: 2em;">+</span> <span style="font-size: 1.5em;">-</span>	<span style="font-size: 1.5em;">▼ ▲</span>	<input style="width: 100px; height: 20px; border: 1px solid #ccc; border-radius: 5px; padding: 2px 5px; margin-right: 5px;" type="text" value="search"/> <span style="color: red;">*</span> <input style="border: 1px solid #ccc; border-radius: 5px; padding: 2px 10px;" type="button" value="All Employees"/>
Order	*Groups That Can Proxy	*On Behalf Of							
<span style="font-size: 2em;">+</span> <span style="font-size: 1.5em;">-</span>	<span style="font-size: 1.5em;">▼ ▲</span>	<input style="width: 100px; height: 20px; border: 1px solid #ccc; border-radius: 5px; padding: 2px 5px; margin-right: 5px;" type="text" value="search"/> <span style="color: red;">*</span> <input style="border: 1px solid #ccc; border-radius: 5px; padding: 2px 10px;" type="button" value="All Employees"/>							

Note: This 'wide-open policy' is for training purposes only and is not intended as a recommendation to be considered in your environment. Your policy will be much more restrictive.

## TASK 2: TEST PROXY ACCESS

1. Search for the string '*start proxy*' and click the link to execute the task
2. In the **Act As** field, enter *Jack Taylor* and click **OK**. Notice you are now acting on behalf of Jack.  


On behalf of: Jack Taylor 
3. Search for the string '*stop proxy*' and click the link to execute the task
4. Check the confirmation box and click **OK**. Notice you are acting as yourself (Logan McNeil) again.
5. As we work through activities in class, you will have the option to start/stop proxy sessions or to log out/in as different users.

(End of Activity)

## SECURITY POLICY CHANGE CONTROL

Security policy change control serves two purposes:

- It allows you to keep your security policies changes in a pending or inactive state until you are ready to deploy them. This can be a useful process for complex and far reaching security changes that require a coordinated activation.
- In the case of errors, it allows you to revert back to a previous version of your security configuration until you can resolve the error and reactivate.



**Note:** Security policy change control is not designed to keep alternate, valid security configurations. Once you revert from a security configuration, it is no longer available; you cannot inadvertently return to it.

## HOW CHANGE CONTROL WORKS

Four elements make Workday security policy change control possible:

- Workday records the time of every security change.
- Workday evaluates security as of a timestamp, ignoring later changes, which are "pending."
- You can activate pending changes by time-stamping your current security configuration.
- You can tell Workday Security to activate a previous timestamp.

When you tell Workday Security to use a timestamp as the security evaluation moment, changes made after that timestamp don't take effect until you activate them. Use the **Activate Pending Security Policy Changes** task to create a new, current timestamp.

For example, if you activate security policy changes in March, June, and September and then discover a serious error in the September security configuration, you can activate the March timestamp using the **Activate Previous Security Timestamp** task. The changes from June and September are considered pending changes along with whatever new changes you make to fix the problems with the September security configuration. When you run the Activate Pending Security Policy Changes task, it creates a new timestamp and activates all of the changes made since March.

Workday no longer allows you to activate the September timestamp, which it deems a bad configuration. It appears in the **View All Security Timestamps** report, but no longer appears on the list for activating previous timestamps. We recommend that you edit the timestamp comment to indicate that it is not a valid security configuration.

Security timestamps look at domain and business process security policies and functional areas. They include changes made by adding or removing security groups from policies, enabling or disabling domains or functional areas, and whether business processes can be delegated.

**Important:** **Security timestamps are only for security policy configurations** and do not affect security group definitions, and user assignments. Changes to security groups always take effect immediately and remain as defined, even if you activate a previously time stamped version of security.

## POLICY CHANGES

When you view a security policy, you can use the Edit Permissions button to add or remove, or otherwise make changes to the security groups that can access the securable items in the security policy.

When you change a security policy, for example by adding or removing a security group, Workday displays a message indicating that your changes have been saved but will not take effect until you activate security changes. This information is also reflected on the Edit Permissions page under the name of the securable item.

When you close the Edit Permissions page, the policy once again displays the security currently in effect. For example, when you delete a security group from a securable item and close the Edit Permissions page, the deleted group still appears on the Domain Security Policies for Functional Area report because the report displays the current state of security according to the timestamp that Workday Security is using to evaluate it. Your deletion is pending change and the report now includes the note "Has Pending Changes" for the affected security policy.

## SECURITY CHANGE REPORTS AND ACTIONS

Use the Domain Security Policies with Pending Changes and the Business Process Security Policies with Pending Changes reports to see which domains or business processes have pending changes. This includes any changes made after the current security timestamp. Select View Pending Changes from the related actions menu on either report to get a list of changes for any individual policy.

The **View All Security Timestamps** report shows all timestamps, both currently active and previous versions. You cannot activate any timestamp with an entry in the Reverted To column. (This column does not appear until you activate a previous timestamp.)

Select **Security Timestamp** > **Edit** from the related actions menu to change the comment on any timestamp. This is particularly useful when indicating timestamps with problems.

Select **Domain Security Policy or Business Process Policy** > **View Latest Version** from the related actions menu of a business process or domain security policy to see what the activated policy would look like. These reports include the changes pending for the selected security policy.

Select **Domain Security Policy or Business Process Policy** > **View Pending Changes** from the related actions menu of a business process or domain security policy to see the differences between the security policy being evaluated at the active timestamp and all the changes made since that time. These reports just show the selected security policy.

Other useful reports include:

- **Domain Security Policies with Pending Changes**
- **Business Process Security Policies with Pending Changes**
- **Domain Security Policy History**
- **Business Process Security Policy History**

## SECURITY GROUPS

A security group is a collection of system users. Users can either be grouped explicitly (user-based security group) or by deriving group membership from other relevant information about the user. Types can have unconstrained (U), constrained (C) or mixed content sensitivity.

Type	How does a user become a member?	If configured in a security policy, will resulting access be constrained? And if so, by what?	Example
<b>User-based (U)</b>	Manually assigned. Follows user.	Unconstrained	HR Administrator, Finance Administrator
<b>Role-based (C/U)</b>	Based on Role Assignment. Roles are assigned to Positions.	Organization(s) supported in role	HR Partner; Benefits Partner; Accountant
<b>Service Center-based (C/U)</b>	Based on Service Center. Service center representatives in service center will be members.	Organization	3rd Party Help Desk
<b>Job-based (C/U)</b>	Based on job details (e.g. job profile, management level).	Organization	Chief Financial Officer, IT Workers, Vice Presidents
<b>Integration System (C/U)</b>	Manually assigned to Integration System Users	Organization	Credit Card System
<b>Segment-based (C)</b>	Based on included security groups.	Segments	Documents – Benefits Categories Manager – Integrations
<b>Location Membership (U)</b>	Based on location membership.	Unconstrained	All USA Workers
<b>Organization Membership (U)</b>	Based on Organization Membership (e.g. Cost Center, Location Hierarchy)	Unconstrained	EMEA Workers IT Cost Center Workers
<b>Aggregate (Mixed)</b>	Members are those in ANY of included security groups.	Mixed – depends on included security groups.	Those in HR Partner OR Benefits Partner
<b>Intersection (Mixed)</b>	Members are those in ALL of included security groups	Mixed – depends on included security groups. Constraints intersected.	Those in HR Partner security group AND HR Partner by location
<b>Level-based (C)</b>	Based on included levels. Requires leveling hierarchy defined, either Compensation Grade or Management Level.	Lower Levels, regardless of organization	Those in Manager Management Level, can access talent card data for all those in lower management levels.

### CONTEXT SENSITIVITY

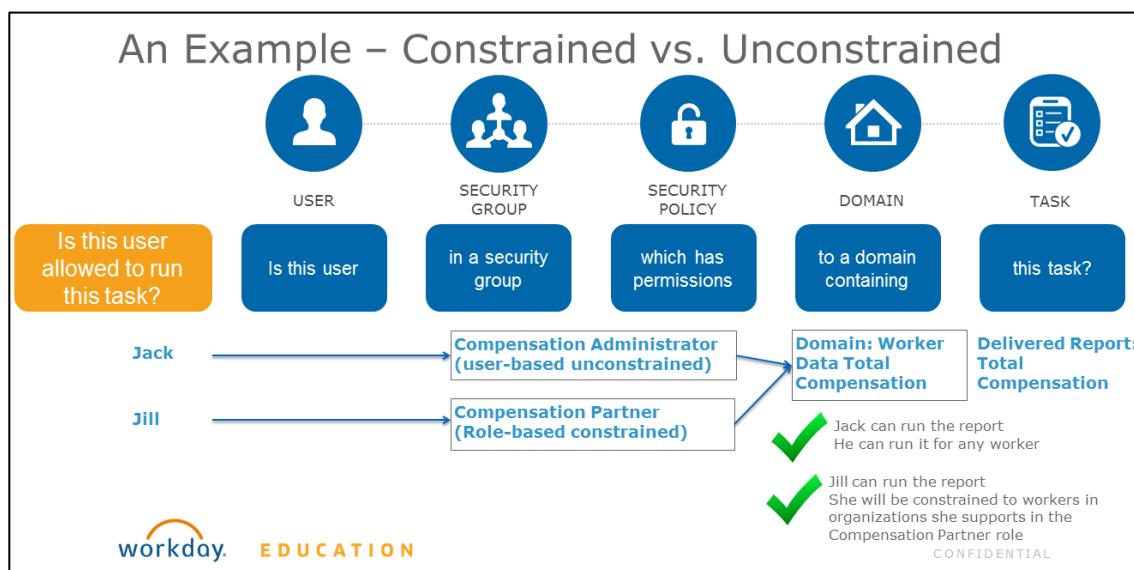
Security group types can be either constrained, unconstrained or mixed depending on configurations.

- **Unconstrained:** users have access to all data instances secured by the security group.
- **Constrained:** users have contextual access to a subset of data to which the security group has access. Constraints in Workday are typically to organizations, but can also be for levels and segments.
- **Mixed:** users may not have uniform access to data instances (Applies to intersection and aggregation security groups).

The following security group types are context-sensitive security groups:

- Constrained **Role-based** groups are sensitive to organization
- **Job-based** security groups are sensitive to organization
- Constrained **Service Center** security groups are sensitive to organization
- Constrained **Integration System** security groups are sensitive to organization
- "...-as-Self" security groups are sensitive to "own" data (e.g. Employee-as-self)
- **Level-based** security groups are sensitive to levels (not organizations)
- **Segment-based security groups** are sensitive to segments.

**Workers associated with a context sensitive group are granted access to target items when they and the item instance share the characteristic to which the group is sensitive.**



What if a user was a member of both an unconstrained and a constrained security group that are both configured for a given domain? A user's access will be the union of their access, so if the user has unconstrained access to a domain via one security group, unconstrained access will prevail.

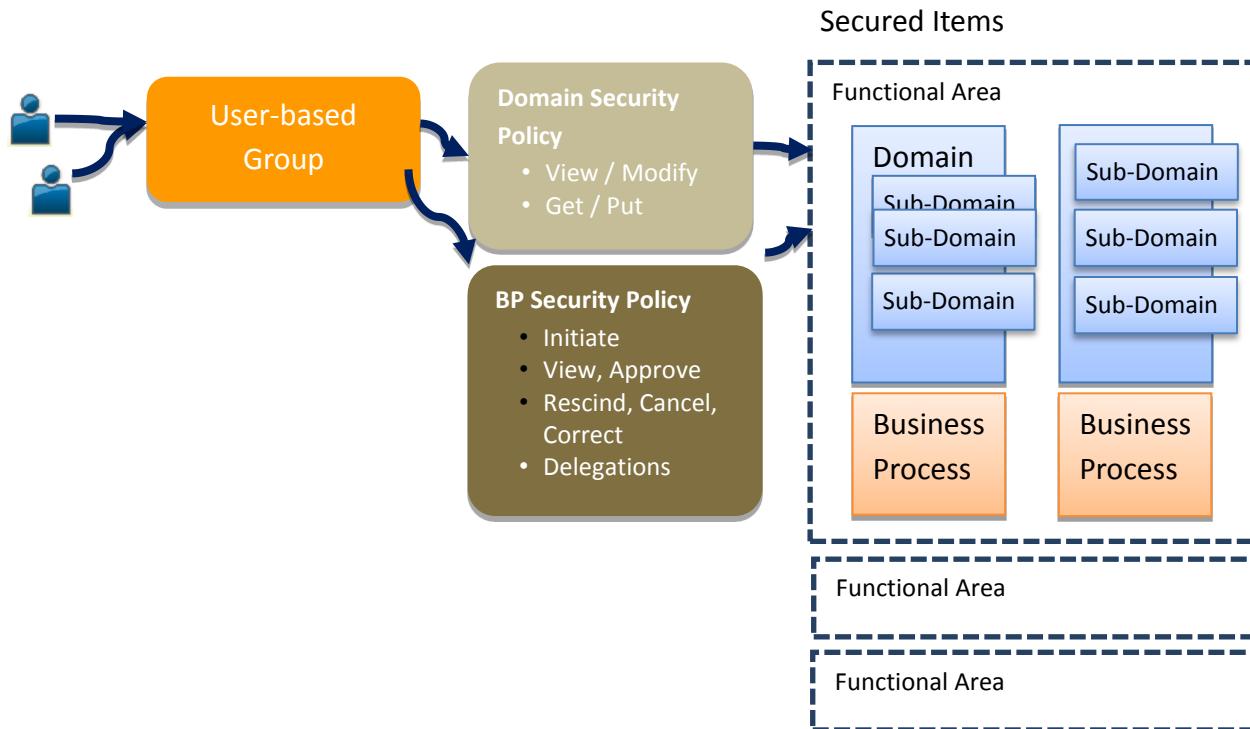
## USER-BASED SECURITY GROUPS

User based security groups are an essential security group type that you will use in your implementations. Characteristics of user-based security groups include:

- **Manually assigned** to a user. They **follow a user**.
  - *It is important to manually review and change user-based security group assignments as people leave your company or change jobs.*
  - *Workday delivers a service that you can add as a step in a termination business process that removes user-based security groups from the Workday account.*
- User-based security groups are **unconstrained** security groups.
  - If a user-based security group has access to a domain, members can access items in that domain, and their access will be unconstrained, i.e. system-wide. "Once there" they will see all data available for that item.
- Workday delivers several user-based security groups as starting points that you can leverage and assign to your workforce. These delivered security groups include such security groups as:
  - Security Administrator
  - Report Writer
  - HR Administrator
  - Finance Administrator
  - Setup Administrator
- You can also create your own user-based security groups as needed.

This is the least restrictive group. It is not context sensitive, in that it makes no attempt to match the context of the workers in the group (organization or ownership) with the context of the secured item. Use user-based security groups for administrators who you want to have global (enterprise-wide) access.

View User-Based Security Group <b>Finance Administrator</b> <span style="font-size: small;">...</span>			
Name	Finance Administrator		
Comment	Create and maintain all financial setup data regardless of organization. Examples include financial institutions, financial accounting data, ledgers, journal sources, account control rules, fiscal schedules, items, and taxes. No approval authority.		
Context Type	Unconstrained		
Administered by Security Groups	<a href="#">Security Administrator</a>		
<b>Members</b> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="padding: 2px;">System Users</td> <td style="padding: 2px; vertical-align: top;">           lmcneil / Logan McNeil            tenantowner /            tserrano / Teresa Serrano            wd-configuration / Workday Configurator            wd-implementer / Workday Implementer            wd-support / Workday Support         </td> </tr> </table>		System Users	lmcneil / Logan McNeil tenantowner / tserrano / Teresa Serrano wd-configuration / Workday Configurator wd-implementer / Workday Implementer wd-support / Workday Support
System Users	lmcneil / Logan McNeil tenantowner / tserrano / Teresa Serrano wd-configuration / Workday Configurator wd-implementer / Workday Implementer wd-support / Workday Support		
<a href="#">Domain Security Policy Permissions</a> <a href="#">Business Process Security Policy Permissions</a> <a href="#">Other Usages</a>			



You can assign users to user-based security groups in one of several ways:

- a. Run task: **Assign Users to User-based Security group**
- b. Run task: **Assign user-based Security group for Person**
- c. Bring up security group and use related actions to assign users

The screenshot shows the "View User-Based Security Group" page for the "Finance Administrator" group. The group name is "Finance Administrator" and the comment is "Create and maintain all financial setup data regardless of org schedules, items, and taxes. No approval authority." The "Available Actions" section includes "User-Based Security Group", "Audits", "Edit", and "Assign Users".

- d. Bring up user and use related actions to assign user-based Security groups

The screenshot shows the user profile for "Adam Carlton" (Staff Payroll Specialist Employee). The profile includes a photo, name, title, and a tip: "Tip: try selecting another category for this user". A context menu is open, listing actions such as "View Workday Account", "Assign Roles", "Assign User-Based Groups", "Edit Workday Account", "Manage Workday Account Credentials", "View Custom Reports", "View Role Assignments", "View Security Groups", "Security History for User", "View Signon History", "View Support Roles", and "View Update Audit".

## CREATE AND DEPLOY USER-BASED SECURITY GROUP

1. Run **Create Security Group** task
2. Find the Domains and/or Business Processes
3. Assign user to User Based Security group
4. Edit Security Policies
5. Activate Pending Security Policy Changes
6. Test



## ACTIVITY 5A – CREATE USER-BASED SECURITY GROUP

**Scenario:** Our goal is to allow Lillian Chu the ability to “find expense reports” and change them for any worker as our Expense Report Administrator. We will need to give her unconstrained access to manage expense reports in tenant. We will use a user-based security group to manually identify Lillian.

### OVERVIEW

Logan McNeil will perform the following actions:

1. Create Security Group
2. Assign User-based Security Groups

### TASK 1: VERIFY EXISTING SECURITY

#### ➊ Start a proxy session as Lillian Chu

1. Verify that Lillian does not currently have access to find expense reports in the tenant.
2. From the search box, enter: **Find Expense Reports**
3. No results should be returned

4. **Stop proxy** session. Confirm and click OK.

### TASK 2: CREATE USER-BASED SECURITY GROUP

#### ➋ As Logan McNeil

1. Search for ‘create sec gr’
2. Click on the **Create Security Group** task
3. Define the Security Group as follows:

<b>Field Name</b>	<b>Entry Value</b>
Type of Tenanted Security Group	User-Based Security Group

Name

Expense Report Administrator

4. Click the **OK** button
5. For the **Administered by Security Groups** Field, enter: Security Administrator and Finance Administrator.

Name	<input type="text" value="Expense Report Administrator"/>
Comment	<input type="text"/>
Context Type	Unconstrained
Inactive	<input type="checkbox"/>
Administered by Security Groups	<input type="text" value="search"/> <div style="border: 1px solid #ccc; padding: 2px; margin-top: 2px;"> <input checked="" type="checkbox"/> Finance Administrator  <input checked="" type="checkbox"/> Security Administrator         </div>

6. Click the **OK** button to save and click **Done**

### TASK 3: ASSIGN USER-BASED SECURITY GROUP

1. Search for '*Lillian*'
2. Click on the related action icon tied to Lillian Chu/Employee and select the **Security Profile > Assign User-Based Groups** task

The screenshot shows the Workday interface. In the top navigation bar, there is a search bar with the placeholder 'worker: lillian chu'. Below the search bar, the 'workday.' logo is visible. On the left, a sidebar titled 'Categories' lists various departments: Common, Assets, Banking, Expenses, Financial Accounting, Integrations, Organizations, Payroll, People, Processes, and Procurement. In the center, the 'Search Results' section displays one item: 'All of Workday' with a result for 'Lillian Chu'. Her profile picture is shown next to the name, which is described as 'Senior Benefits An Employee'. A context menu is open over her profile picture, listing several options: View Workday Account, Assign Roles, **Assign User-Based Groups**, Edit Workday Account, Manage Workday Account Credentials, View Custom Reports, View Role Assignments, View Security Groups, Security History for User, View Signon History, View Support Roles, View Update Audit, and Talent. The 'Assign User-Based Groups' option is highlighted with a blue background.

3. Click the icon for the **User-Based Groups to Assign** field
4. Select **Expense Report Administrator**

Assign User-Based Security Groups for Person

Person	Lillian Chu
User-Based Groups to Assign	<input type="text" value="search"/>  <input checked="" type="checkbox"/> Expense Report Administrator

5. Click the **OK** button to save

6. Click the **Done** button

Note that you can also assign user based security groups to users by running tasks:

- **Assign Users to user-based security group**
- **Assign user-based security group for person**
- Related action option to assign users off the security group.

(End of Activity)



## ACTIVITY 5B – EDIT DOMAIN SECURITY POLICY AND ACTIVATE PENDING SECURITY POLICY CHANGES

**Scenario:** Logan must now edit the domain security policy. Once the security policy has been modified, the pending security policy changes must also be activated. The new changes will need to be tested to ensure that Lillian has access to manage expense reports in the tenant.

### OVERVIEW

Logan McNeil will perform the following actions:

1. Edit Domain Security Policy
2. Activate Pending Security Policy Changes

### TASK 1: EDIT SECURITY POLICY PERMISSIONS FOR A DOMAIN

#### As Logan McNeil (lmcneil)

1. To determine what domain you need to edit, run the **View Security for Securable Item** report. From the search box, run **View Security for Securable Item**
2. In the Domain Item prompt, enter **Find Expense Reports** and select the **Find Expense Reports (Report (Report Writer))** item

**View Security for Securable Item**

Domain Item \* **Find Expense Reports (Report (Re**

3. Click **OK**.
4. Note how this task is secured to the **Domain: Manage Expense Report**.

**View Security for Securable Item Find Expense Reports ...**

Type	Report (Report Writer)								
On Menu	Menu: Expenses								
Permission Required	View								
Hidden Workday Delivered Report	No								
<input checked="" type="radio"/> <b>Domain Security</b> <input type="radio"/> Language Restrictions									
<b>Domain Security</b> <table border="1"> <thead> <tr> <th>Security Policy</th> <th>Domain</th> <th>Functional Areas</th> <th>Permitted Security Groups</th> </tr> </thead> <tbody> <tr> <td><a href="#">Manage: Expense Report</a> ...</td> <td><input type="text"/></td> <td>Expenses</td> <td>Cash Analyst Cash Manager</td> </tr> </tbody> </table>		Security Policy	Domain	Functional Areas	Permitted Security Groups	<a href="#">Manage: Expense Report</a> ...	<input type="text"/>	Expenses	Cash Analyst Cash Manager
Security Policy	Domain	Functional Areas	Permitted Security Groups						
<a href="#">Manage: Expense Report</a> ...	<input type="text"/>	Expenses	Cash Analyst Cash Manager						

## Configurable Security Fundamentals 24

5. Click on the Domain Security Policy for Manage Expense Report to view its details.
6. Note the allowed security group types. Since our user-based security group is unconstrained, we can configure our new Expense Report Administrator security group in the permissions.

The screenshot shows the 'View Domain Security Policy' page for 'Manage: Expense Report'. The page displays various policy details:

View Domain Security Policy Manage: Expense Report [...]	
Description	This domain provides access to manage expense reports on behalf of others and view related reporting.
Has Pending Changes	Yes
Status	Active
Functional Areas	Expenses
Child Policies	Manage: Expense Report Attachments
Allowed Security Group Types	Roles - Company Unconstrained Groups
Securable Actions	101
Securable Reporting Items	99

7. Using related actions off the domain security policy, select **Domain Security Policy > Edit Permissions**

The screenshot shows the 'Domain Security Policy' page for 'Manage: Expense Report'. The 'Edit Permissions' button is highlighted with a yellow box.

8. Under the Report/Task Permissions, add the *Expense Report Administrator* security group to the groups with **Modify** access. Note the warning to activate changes.

The screenshot shows the 'Report/Task Permissions' dialog box. It lists two items under 'Security Groups':

View	Modify
Chief Executive Officer	
Chief Financial Officer	
Chief Human Resources Officer	
Controller	
Executive VP of Sales & Marketing	
Expense Analyst	
Expense Partner [...]	
Expense Settlement Specialist	
Finance Auditor	

A red box highlights the search bar and the list of selected security groups:

- Expense Data Entry Specialist
- Expense Report Administrator
- Implementers

9. Click **OK** to save the changes
10. How many securable actions are in this domain? \_\_\_\_\_
11. Click on the number of securable actions and see which ones require modify vs. view permissions.

**Edit Permissions Manage**

Your changes have been saved but are not yet active.

Description	This domain
Has Pending Changes	Yes
Status	Active
Functional Areas	Expenses
Child Policies	Manage: Expenses
Allowed Security Group Types	Roles - Core, Unconstrained
Securable Actions	<b>101</b>
Securable Reporting Items	99

101 items

Name	Type	Permission Required
Add Attachment	Task	Modify
Cancel Expense Report	Task	Modify
Change Expense Report	Task	Modify
Change Expense Report to Multicurrency	Task	Modify
Change Expense Report to Value Added Tax (VAT)	Task	Modify
Copy Expense Report	Task	Modify
Create Travel Profile	Task	Modify
Edit Expense Report	Task	Modify

12. Remember that access to the domain will provide access to all items in the domain. We are granting Lillian Chu access to view and modify all items in this domain via the user-based security group: Expense Report Administrator.

13. Click the **Done** button

## TASK 2: ACTIVATE PENDING SECURITY POLICY CHANGES

- To see what domain security policies will be activated, let's run a report.
- Search for '*dom sec pend*' and run the **Domain Security Policies with Pending Changes** report
- Notice the security policy we edited awaiting activation along with the child domain that is inheriting parent permissions.

**Domain Security Policies with Pending Changes**

Security Evaluation Moment: 03/23/2015 02:58:11.272 PM

2 items

Domain Security Policy	Last Changed	By User
Manage: Expense Report Attachments	03/24/2015 07:44:38.799 AM	lmcneil / Logan McNeil
Manage: Expense Report	03/24/2015 07:44:38.799 AM	lmcneil / Logan McNeil

- Using related actions off the Manage: Expense Report domain security policy, select Domain Security Policy > View Pending Changes

5. See the details of the pending changes, what the current activated permissions are vs. the pending.

Current	Pending	Last Updated
Expense Data Entry Specialist	Expense Data Entry Specialist Expense Report Administrator Implementers	03/24/2015 07:44:38.799 by lmcnell / Logan McNeil

6. Search for '**Activate**' and run the task **Activate Pending Security Policy Changes**
7. Enter '**Activity 5**' into the comment box
8. Click the **OK** button
9. Check the **Confirm** check box
10. Click the **OK** button

### TASK 3: TEST THE SECURITY CHANGES

⊕ **Start proxy as Lillian Chu**

1. Run the **Find Expense Reports** task to see if Lillian now has access.
2. See how Lillian can now not only have access to this task, but that her access is unconstrained. She can access any worker's expense report across any company.

Find Expense Reports

Company	<input type="text" value="search"/>
Pay To	<input type="text" value="search"/>
Type	<input type="text" value="search"/>
Report Date On or After	<input type="text" value="1/1/"/>
Report Date On or Before	<input type="text" value="1/1/"/>
Supplier for Contingent Worker	<input type="text" value="search"/>
Corporate Credit Card Accounts for Expense Report	<input type="text" value="search"/>
Document Number	<input type="text"/>
Expense Report Status	<input type="text" value="search"/>
Expense Report Worker Payment Status	<input type="text" value="search"/>

Top > Company

- Global Modern Services, Inc. (USA)
- Global Modern Services, Ltd (Canada)
- Global Modern Services, PLC (U.K.)
- Global Modern Services AB (Sweden)
- Global Modern Services AG (Switzerland)
- Global Modern Services ApS

3. Select Company: Global Modern Services (USA)
4. Pay to: Logan McNeil (Employee)
5. Click OK
6. See all the expense reports for Logan and see the actions Lillian can take on the expense reports.

Available Actions    Expense Report EXP-00004979

Expense Report	Add Attachment	Expense Lines 7 items
Accounting	Cancel	
Favorite	Change	
Navigate	Copy	
	Enable VAT	
	Print	
	Date 01/16/2015	
	Memo Internal Team Meeting	
	Payment Type Direct Deposit	
Expense Report: EXP-00004890	Employee: Logan McNeil	Item Amount Currency
		Taxis / Trains / Shuttles 19.86 USD
		Meals 47.90 USD
		Parking 124.00 USD
		Car Rental & Gas 194.58 USD
		Total 2,167.11

## 7. Stop proxy

(End of Activity)



## ACTIVITY 5C – INVESTIGATE SOME SECURITY REPORTS

**In this activity, you will run the following reports:**

- Domain Security Policy History
- Security Analysis for Security Group
- Test Security Group Membership
- Security Analysis for Action
- View Security Group

### TASK 1 – INVESTIGATE SECURITY RELATED REPORTS

1. As Logan McNeil (lmcneil) (make sure to stop your proxy session if still proxied as Lillian Chu)
2. Search for and run the **Domain Security Policy History** report
  - a. In the Domain Security Policy prompt, select By Functional Area > Expenses> **Manage Expense Report**
  - b. Enter today's date for From
  - c. Click OK
  - d. Note your changes showing the added security group.

Domain Security Policy History							
Domain Security Policy	From	Changed On	By User	Modified Object	Object Type	Related Object Type	Added
							Removed
Manage: Expense Report	04/08/2015 12:00:00.000 AM	04/08/2015 05:08:55.798 PM	lmcneil / Logan McNeil	View and Modify for Manage: Expense Report	Security Policy Permission	Security Group	Expense Report Administrator

3. Reports can be run from the search box, or can be configured as related action options. Using related actions off the security group, Expense Report Administrator, select **Security Group> Security Analysis for Security Group**

Domain Security Policy History							
Domain Security Policy	From	Changed On	By User	Modified Object	Object Type	Related Object Type	Added
Manage: Expense Report	03/24/2015 12:00:00.000 AM	03/24/2015 07:07:55.798 PM	lmcneil / Logan McNeil	View and Modify for Manage: Expense Report	Security Policy Permission	Security Group	Expense Report Administrator
<b>Available Actions</b>		<b>User-Based Security Group Expense Report Administrator</b>					
<a href="#">User-Based Security Group</a> <a href="#">Audits</a> <a href="#">Favorite</a> <a href="#">Integration IDs</a> <a href="#">Reporting</a> <a href="#">Security Group</a>		<a href="#">Security Group</a> <b>Expense Report Administrator</b> Context Type: Unconstrained <a href="#">Security Analysis for Security Group</a> <a href="#">Copy</a> <a href="#">Test Membership</a> <a href="#">View Action Summary</a>					

4. Click **OK**

5. Note reports and tasks accessible to the Expense Report Administrator. This report, Security Analysis for Security Group, can be run from the search box too.

Security Group	Reports and Tasks - Modify Access	Reports and Tasks - View Access	Business Process Types granted to Security Group - Initiate Access	Business Process Types granted to Security Group - Enrichment Access	Business Process Types granted to Security Group - Approve Access	Business Process Types granted to Security Group - View Access	Business Process Types granted to Security Group - View Completed Access
Expense Report Administrator	Average Expense Cycle Times Average Expense Cycle Times (Deprecated) Average Expense Report Total Average Expense Report Total (Deprecated) Cancel Expense Report Change Expense Report Change Expense Report to Multicurrency Change Expense Report to Value Added Tax (VAT) Copy Expense Report Create Travel Profile <a href="#">More (73)</a>						

6. Using related actions off the **Expense Report Administrator** security group, select **Security Group > Test Membership**. This related action option runs the delivered report: *Test Security Group Membership*.

7. Enter Lillian Chu and click OK. Note how Lillian is a member.

8. Rerun the report by clicking on the change icon

**Test Security Group Membership** |

9. Enter Logan McNeil (Imcneil). Note how Logan is **not** a member.

Is User	Imcneil / Logan McNeil
In Security Group	Expense Report Administrator
for Target Instance	(empty)
Answer	No

## Configurable Security Fundamentals 24

10. Lastly, from the search box, run the **Security Analysis for Action** report.

11. Run for Action: **Find Expense Reports** and Account: Ichu/ Lillian Chu

Security Analysis for Action

Select the Account and Action (task, report, business process, or web service) that you would like to analyze.

Action	* Find Expense Reports
Account	* Ichu / Lillian Chu
Show Details	<input type="checkbox"/>

12. See how on the far right, we can see how Lillian has access to this action via the security group: *Expense Report Administrator*.

Security Analysis for Action					
Action	Domain Security Policy	Securable Actions	Securable Reporting Items	Securable Integrations	via Security Groups
Manage: Expense Report	Q	101	99	4	Expense Report Administrator

13. Rerun the **Security Analysis for Action** report. This time run for Imcneil (Logan McNeil) and the same **Find Expense Reports** action.

14. See how Logan has access to this action, Find Expense Reports, via the *Chief Human Resources Officer* security group.

Security Analysis for Action					
Action	Domain Security Policy	Securable Actions	Securable Reporting Items	Securable Integrations	via Security Groups
Manage: Expense Report	Q	101	99	4	Chief Human Resources Officer

*Users can have access to a given item or action via different security groups permitted for the domains securing the given item.*

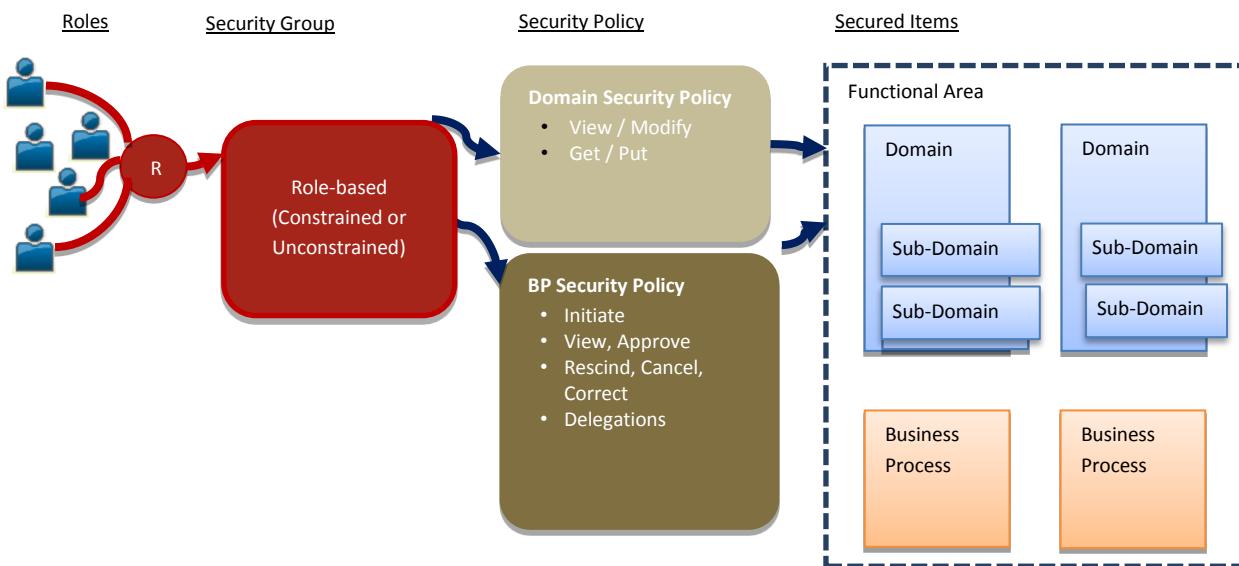
15. **Optional** - Check out other examples of user-based security groups in tenant. (run **View Security Group** and select **user-based**)

(End of Activity)

## ROLE-BASED SECURITY GROUPS

Role based security groups are a very essential and very powerful way of granting needed access to Workday. Role-based security groups allow you to identify users based on role-assignments. Role-based security groups are commonly used to **identify users in key support or leadership roles supporting different organizations.**

Role-based security groups can be defined as **constrained** or **unconstrained**. Constrained Role-based security groups, for example, are a common way to identify and constrain your support staff to target instances in a given organization (or organizations) that they support or lead.



For example, the **Manager role-based constrained security group** shown below,

- Identifies those assigned to the **Manager role**
- Constrains their target access to the organizations to which they are assigned to in that role** and any subordinate organizations where there is no Manager role assigned.

The screenshot shows the 'Edit Role-Based Security Group (Constrained)' dialog box with the following details:

- Name:** Manager
- Comment:** Perform actions on members of assigned supervisory organizations. Examples include hiring employees, contingent workers, compensation changes, job changes, performance reviews, creating positions and headcount, stock grants, staffing, recruiting, leaves, and time off. Approval authority for HCM, expense, and nonmanagement business processes.
- Context Type:** Constrained by Role Access
- Inactive:**
- Group Criteria:** Assignable Role: Manager
- Access Rights to Organizations:**
  - Applies to Current Organization Only
  - Applies To Current Organization And Unassigned Subordinates
  - Applies to Current Organization And All Subordinates
  - Applies to Current Organization and Subordinates to Level
- Access Rights to Multiple Job Workers:**
  - Role has access to the positions they support
  - Role for primary job has access to all positions
  - Role has access to all positions

Annotations on the form:

- A green callout bubble points to the 'Name' field with the text: "Members will be those assigned to the role"
- A green callout bubble points to the 'Access Rights to Organizations' section with the text: "Members access will be constrained to:"

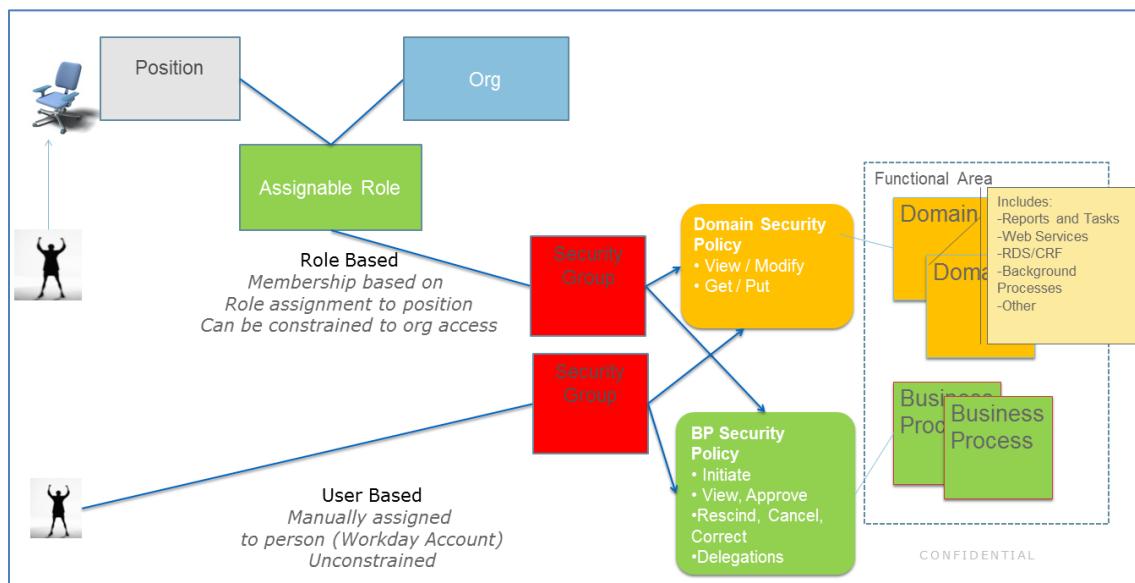
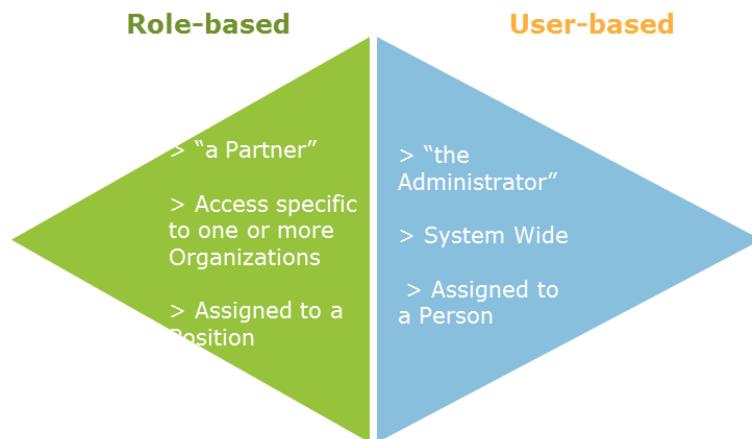
## HOW ARE ROLE-BASED SECURITY GROUPS DIFFERENT THAN USER-BASED SECURITY GROUPS?

User-based security groups are manually assigned to a person (or Workday account) and follow that person. Membership in a role-based security group is determined via role assignment. Roles must be defined for organization types and roles must then be assigned.

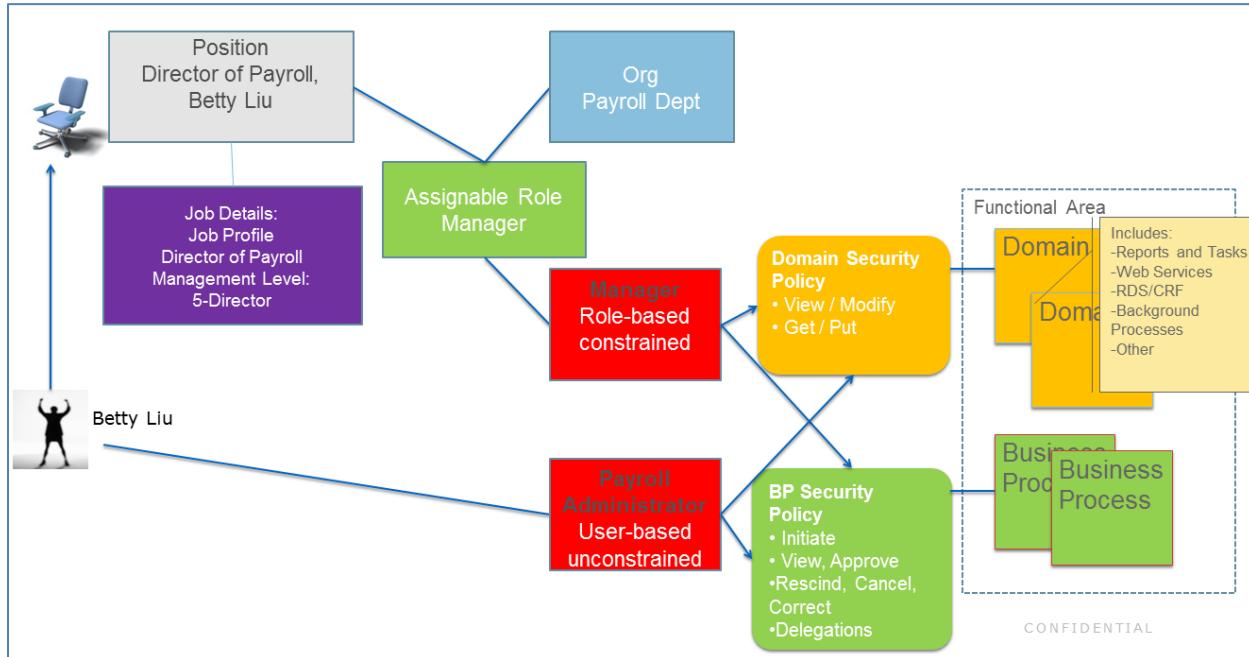
**Role-assignments are to positions, not to the worker directly.**

**Members of a role-based security group will automatically be those in positions assigned to the role referenced in the role-based security group.**

Role based security groups are commonly constrained, limiting members' target data access to instances in organizations to which they are assigned to in the role.



Below is an example of a Worker, Betty Liu. Betty is manually assigned the **Payroll Administrator** user-based security group. She will have access to domains and business processes configured with the Payroll Administrator security group. Her access to items in these domains and business processes will be unconstrained. Betty's position is also assigned to the Manager role, since she is the manager of the Payroll Department and has direct reports in that organization. With this role assignment on her position, Betty is also a member of the **Manager** role-based constrained security group. She can also access domains and business processes configured with the Manager security group. Her access in these areas will be constrained to target instances in the organization she is assigned to in the role, i.e. the Payroll Dept.



## A CLOSER LOOK AT ROLE-BASED SECURITY GROUPS

- The **role must be defined and enabled for the given organization type**.

Some examples include:

Role	Enabled for Organization Type
HR Partner	Supervisory
Accountant	Company
Cost Center Manager	Cost Center
Compensation Partner by Location	Location Hierarchy

- The **role must be assigned to a position**, not directly to a worker or person.

- Roles can be assigned at the organization level.

The screenshot shows the Global Modern Services application. On the left, there's a navigation bar with tabs: Members, Details, Staffing, and Roles. The Roles tab is currently selected. In the center, there's a table titled 'Members' with two columns: 'Worker' and 'Position'. A single row is visible, showing 'Steve Morgan' in the Worker column and 'Chief Executive Officer' in the Position column. To the right of the table is a vertical sidebar with a list of options: Hire, Integration IDs, Job Application, Job Change, Organization, Reorganization, Reporting, Reports, Roles, Sort Order, Staffing, Staffing Reports, Succession, Talent, and Time and Leave. A dropdown menu is open under the 'Assign Roles' section, listing: Assign Self-Assign Roles, Assign Unassigned Self-Assign Roles, View Role Assignment History, View Roles, Security History, and View Worker Roles Audit.

- Roles can also be assigned off the worker. This initiates the Assign Roles business process.

The screenshot shows the Workday application. At the top, it says 'Search Results 1 items' and 'All of Workday'. Below that, there's a search result for 'Dawn Myers' (Staff HR Representative Employee). To the right of the search result is a vertical sidebar with a list of options: Safety Incident, Talent, Time and Leave, Workday Account, Worker History, Audits, Favorite, Integration IDs, Preferences, Reporting, and Security Profile. A dropdown menu is open under the 'Assign Roles' section, listing: Assign User-Based Groups, Edit Workday Account, Manage Workday Account Credentials, Start Proxy, View Custom Reports, View Role Assignments, View Security Groups, Security History for User, View Signon History, View Support Roles, and View Update Audit.

3. Create the **role-based security group (constrained or unconstrained)**.

The role-based security group will reference the role and **members** of the role-based security group will be **those assigned in that role**.

- If constrained, you must specify the access rights**

4. Configure the role-based security group in needed **domain and/or business process security policies**

- If constrained, target access to secured items will be constrained by the organization access rights defined in the security group.

**5. Activate**

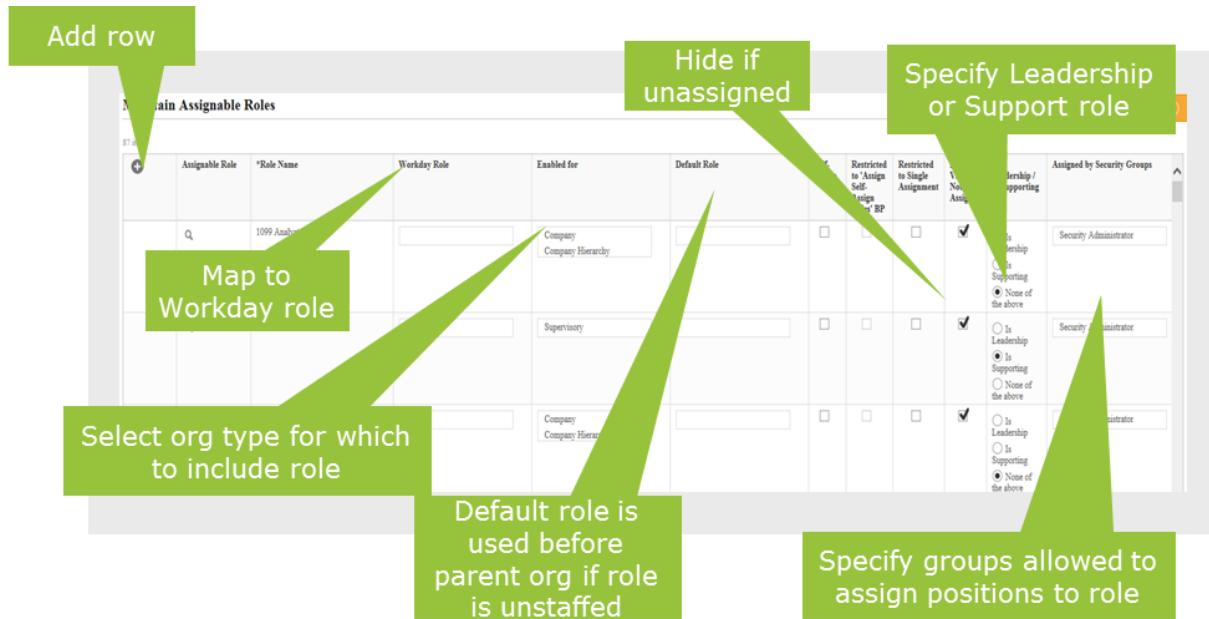
**6. Test**

Workday delivers some starting roles enabled for organization types and delivers corresponding role-based security groups that use these delivered roles. You can also create your own roles and corresponding role-based security groups.

## MAINTAIN ASSIGNABLE ROLES

Roles must be defined in Workday before creating role-based security groups. Workday delivers starting roles and role-based security groups.

You can also create and maintain your own roles. You create or edit these roles with the **Maintain Assignable Roles** task, which enables you to maintain roles for numerous role-enabled objects simultaneously. The Maintain Assignable Roles task is secured to the *Set Up: Assignable Roles* security domain.



When maintaining assignable roles, members of the security group you specify as the 'Assigned by Security Group' will be considered members of the Workday automatically assigned "**Role Maintainer**" security group for that role.

In addition to the Maintain Assignable Roles task, which enables you to maintain roles for numerous role-enabled objects at once, there are options available to quickly assign these roles in "self-service" fashion at the level of an individual organization, or other role-enabled object using *Select Roles > Assign Roles* as a related action. You can also use the *Assign Roles* business process as a stand-alone business process or as a subprocess on most inbound and outbound staffing events.

The values determined by the radio buttons *Is Leadership* and *Is Supporting* are used in reports, such as [My Leadership Roles](#) and [My Supporting Roles](#). If a role is configured as a leadership role, members can also be configured to show in organization chart displays.

Defined roles will show as assignable roles for the given enabled organization type.

Shown below are roles defined for the Pay Group organization type. Roles can then be assigned for a given organization, e.g. Pay Group.

**Administrative - Corporate (Weekly)**

View As Of 03/07/2015

Details | Pay Group | Members | Staffing | Unavailable to Fill | **Roles** | Security Groups

4 items

Assignable Role	Assigned To	Role From	Current Effective Date
Owner	Logan McNeil	Assigned	01/01/2000
Payroll Accountant	Sara Goldstein	Assigned	01/01/2000
Payroll Partner	Betty Liu	Assigned	01/22/2009
	Logan McNeil	Assigned	01/22/2009

Another example is assigning enabled roles for a location hierarchy.

**Global Modern Services Locations**

View As Of 04/08/2015 Subordinates EMEA  
Type Location Hierarchy Japan & Asia/Pacific  
Latin America  
North America

Members | Details | **Roles** | Security Groups | Org

11 items

Assignable Role		
Business Site Buyer		
Compensation Partner (by Location)		
Global Mobility Partner		
Health Partner		
Hierarchy Owner		
HR Partner (By Location)		
Owner		
Safety Partner		
Stock Partner		
Top Performer Committee (By Location)	Logan McNeil	
Works Council	Logan McNeil	Assigned

**Available Actions**

Organization	Global Modern S	
Audits	Type	Location Hierarchy
Business Process	Manager	(empty)
Compensation	Total Headcount	0
Compensation Review	Subordinates	EMEA
Process		Japan & Asia/Pacific
Favorite		Latin America
Hierarchy Structure		North America
Integration IDs	External URL	Business Site Website
Organization		
Reorganization		
Reporting		
Reports		
<b>Roles</b>	<b>Assign Roles</b>	
Sort Order	Assign Self-Assign Roles	
Staffing Reports	Assign Unassigned Self-Assign Roles	
Succession	View Role Assignment History	
Talent	View Roles	
Time and Leave	Security History	
Translation	View Worker Roles Audit	

## ROLE BASED CONTEXT: ACCESS RIGHT TO ORGANIZATIONS

Role-based constrained security groups are most commonly used to identify your support staff where you can then **constraint members to target instances in the organizations to which they are assigned to in that role.**

For constrained role-based security groups, there are **four main constraints** you can configure:

**Edit Role-Based Security Group (Constrained) Manager ...**

Name \* Manager

Comment Perform actions on members of assigned supervisory organizations. Examples include hiring employees or contingent workers, compensation changes, job changes, performance reviews, creating positions and headcount, stock grants, staffing, recruiting, leaves, and time off. Approval authority for HCM, expense, and procurement business processes

Context Type Constrained by Role Access

Inactive

**Group Criteria**

Assignable Role \* Manager

**Access Rights to Organizations**

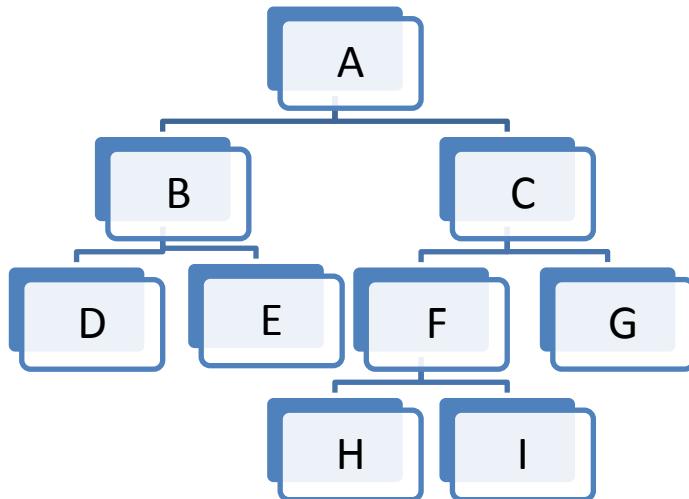
- Applies to Current Organization Only
- Applies To Current Organization And Unassigned Subordinates
- Applies to Current Organization And All Subordinates
- Applies to Current Organization and Subordinates to Level

Subordinate Levels 0

**Access Rights to Multiple Job Workers**

- Role has access to the positions they support
- Role for primary job has access to all positions
- Role has access to all positions

1. **Current Organization Only** – constrains members to target instances in the organization that they are assigned to in that role.
2. **Current organization and unassigned subordinates** – constrains members to target instances in the organization that they are assigned to and any subordinate organizations that do not have someone directly assigned to the role.
3. **Current organization and all subordinates** – constrains members to target instances in the organization they are assigned to and all subordinate organizations, regardless of whether others are assigned in that role in subordinate organizations.
4. **Current organization and subordinates to level** – constrains members to target instances in the organization they are assigned to and subordinate organizations down to a number of levels in the hierarchy.



## CREATE AND DEPLOY ROLE-BASED SECURITY GROUP

1. Run Maintain Assignable Roles task
2. Run Create Security Group task – reference the role
3. Use Assign Roles task
4. Edit Security Policies
5. Activate Pending Security Policy Changes
6. Test

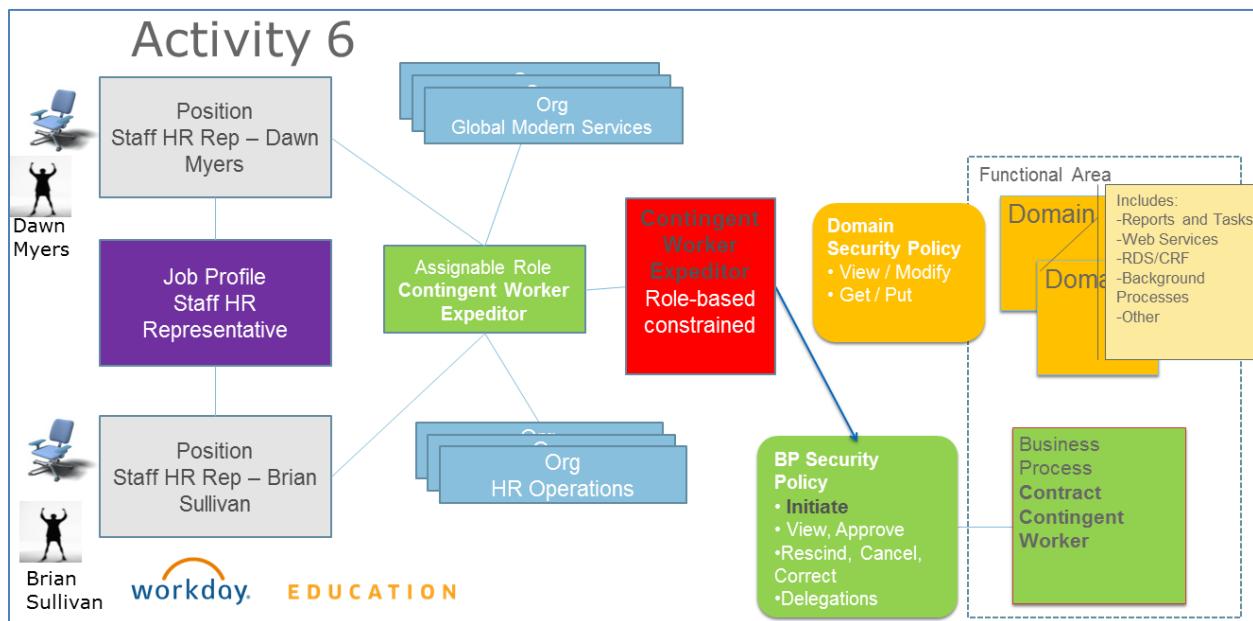


## ACTIVITY 6A – CREATE ROLE-BASED CONSTRAINED SECURITY GROUP

**Scenario:** A new role is to be created called Contingent Worker Expediter to process the on-boarding of contingent workers. The Staff HR Representative, Dawn Myers, has been identified as the support person for the top level supervisory organization structure and unassigned subordinate organizations. Brian Sullivan, Staff HR Representative will be the support person for the HR Operations Department.

As the Security Configurator, you will create a new assignable role and new role-based security group called Contingent Worker Expediter with the needed constraints of Current Organization and Unassigned Subordinates.

### OVERVIEW

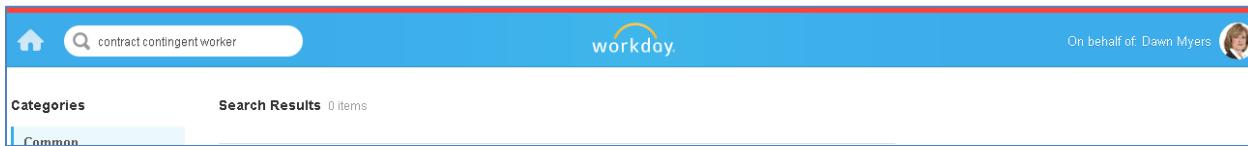


Logan McNeil will perform the following actions:

1. Maintain Assignable Roles
2. Create Security Group
3. Assign Role

## TASK 1: VERIFY EXISTING SECURITY

1. From the search box, run the **Start Proxy** task and start a proxy session as Dawn Myers (dmyers)
2. As Dawn, see if Dawn has access to the **Contract Contingent Worker** task. from the search box, enter *Contract Contingent Worker* and see how no results are returned.



3. **Stop Proxy**

## TASK 2: MAINTAIN ASSIGNABLE ROLES

### ⌚ As Logan McNeil (lmcneil)

1. Create the new role by first searching for '*maintain role*'
2. Click on the **Maintain Assignable Roles** task
3. Note and then collapse the warnings in the upper right.
4. Add a row by clicking the icon
5. Configure the Assignable Role as follows:

<b>Field Name</b>	<b>Entry Value</b>
Role Name	Contingent Worker Expediter
Enable for	Supervisory
Hide on View if Not Assigned	Do Not Check the Box
Is Leadership/Is Supporting	Is Supporting
Assigned by Security Groups	Security Administrator Security Partner

*Note: the security group(s) you designate as the 'Assigned by Security Group' for this role, will automatically be assigned the "Role Maintainer" security group for this role.*

Maintain Assignable Roles								
	Enabled for	Default Role	Self-Assign	Restricted to 'Assign Self-Assign Roles' BP	Restricted to Single Assignment	Hide on View if Not Assigned	Is Leadership / Is Supporting	Assigned by Security Groups
	<input type="text" value="search"/> <input checked="" type="checkbox"/> Supervisory	<input type="text" value="search"/> <input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="radio"/> Is Leadership <input checked="" type="radio"/> Is Supporting <input type="radio"/> None of the above	<input type="text" value="search"/> <input checked="" type="checkbox"/> Security Partner <input checked="" type="checkbox"/> Security Administrator

6. Click the **OK** button to save

7. Click the **Done** button

### TASK 3: CREATE SECURITY GROUP

1. Search for 'create sec gr'
2. Click on the **Create Security Group** task
3. Set the type and name as follows:

<b>Field Name</b>	<b>Entry Value</b>
Type of Tenanted Security Group	Role-Based Security Group (Constrained)
Name	Contingent Worker Expediter

4. Click the **OK** button

5. Configure the Security Group as follows:

<b>Field Name</b>	<b>Entry Value</b>
Group Criteria -> Assignable Role	Contingent Worker Expediter
Access Rights to Organizations	Applies to Current Organization and Unassigned Subordinates
Access Rights to Multiple Job Workers	Role has access to the positions they support

Edit Role-Based Security Group (Constrained) Contingent Worker Expeditor ...

Name <span style="color: #800000;">*</span>	Contingent Worker Expeditor
Comment	   
Context Type	Constrained by Role Access
Inactive	<input type="checkbox"/>
<b>Group Criteria</b>	
Assignable Role <span style="color: #800000;">*</span>	Contingent Worker Expeditor <span style="color: #800000;">...</span>
<b>Access Rights to Organizations</b>	
<input type="radio"/> Applies to Current Organization Only <input checked="" type="radio"/> Applies To Current Organization And Unassigned Subordinates <input type="radio"/> Applies to Current Organization And All Subordinates <input type="radio"/> Applies to Current Organization and Subordinates to Level	
Subordinate Levels 0	
<b>Access Rights to Multiple Job Workers</b>	
<input checked="" type="radio"/> Role has access to the positions they support <input type="radio"/> Role for primary job has access to all positions <input type="radio"/> Role has access to all positions	

6. Click the **OK** button to save
7. Click the **Done** button

#### TASK 4: ASSIGN ROLE

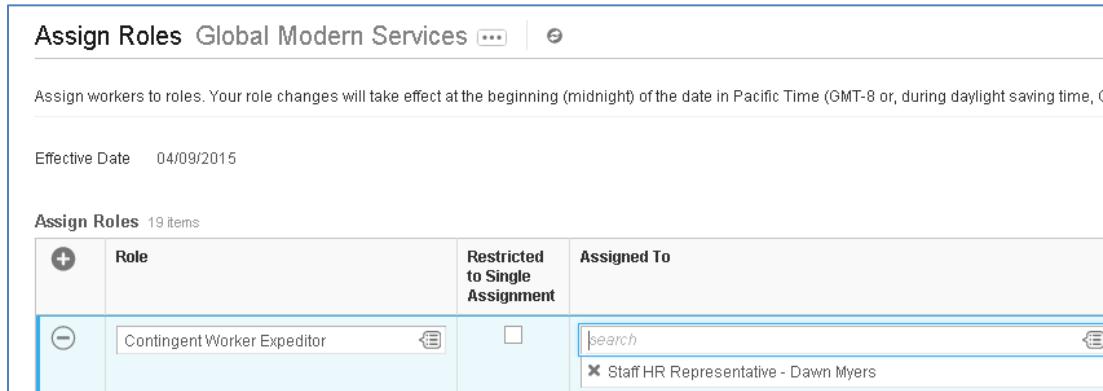
1. Let's assign our new role off of an organization. From the search box, search for **org: glo mod serv**
2. From the related action icon on the **Global Modern Services** Supervisory Organization, select **Roles -> Assign Roles**

The screenshot shows the Workday interface with a search bar at the top containing "org: glo mod serv". Below the search bar, there is a sidebar with categories like "Supervisory Organizations" and "Locations". The main area displays "Search Results 43 items" under "All of Workday". A specific entry for "Global Modern Services" is selected, and a context menu is open over it. The menu is titled "Assign Roles" and contains the following options:

- Assign Roles
- Assign Self-Assign Roles
- Assign Unassigned Self-Assign Roles
- View Role Assignment History
- View Roles
- Security History
- View Worker Roles Audit

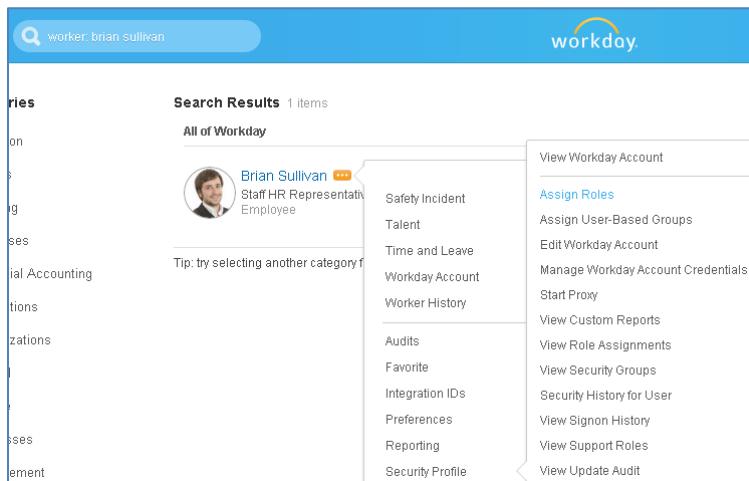
3. Click the **OK** button to accept today as the Effective Date.
4. Click on the + icon to add a new row
5. Click on the **Role** ... icon to select **Contingent Worker Expediter**

6. Click on the \*Assigned To  icon to select **Staff HR Representative - Dawn Myers** (Tip: enter the name *Dawn* and you can quickly find Dawn's position)



The screenshot shows the 'Assign Roles' page for 'Global Modern Services'. At the top, it says 'Assign workers to roles. Your role changes will take effect at the beginning (midnight) of the date in Pacific Time (GMT-8 or, during daylight saving time, G...'. Below that, the 'Effective Date' is listed as '04/09/2015'. The main section is titled 'Assign Roles 19 items' and contains a table with four columns: '+', 'Role', 'Restricted to Single Assignment', and 'Assigned To'. The first row has a minus sign and the role 'Contingent Worker Expeditor'. The second row is highlighted with a blue border and has a checkmark in the 'Assigned To' column, with the text 'Staff HR Representative - Dawn Myers' in the search bar.

7. Click the **OK** button  
 8. Click the **Done** button  
 9. From the search box, search for **worker: Brian Sullivan**  
 10. Using related actions, select **Security Profile > Assign Roles**



The screenshot shows a search results page for 'worker: brian sullivan'. The search bar at the top shows the query. The results are filtered by 'All of Workday'. One result is shown: 'Brian Sullivan Staff HR Representative Employee'. A context menu is open over this result, listing various actions such as 'View Workday Account', 'Assign Roles', 'Assign User-Based Groups', etc.

11. Click **OK** to accept the effective date of the change as today.  
 12. Add a row for a new role assignment.  
 13. Populate the assignment as follows:

<b>Field Name</b>	<b>Entry Value</b>
Role Enabled for	HR Operations Department

Role	Contingent Worker Expeditor
Assigned to	Brian Sullivan – Staff HR Representative (hint: type 'brian' to quickly find the position)

Assign Organization Roles Staff HR Representative - Brian Sullivan  

Effective Date 04/09/2015

+ *Role Enabled For	*Role	Assigned To	Single Assignment	Default Worker
 HR Operations Department 	Contingent Worker Expeditor 	<input data-bbox="807 570 1052 601" type="text" value="search"/> x Brian Sullivan - Staff HR Representative		Dawn Myers

14. Click **Submit**. This initiates the *Assign roles* business process. Roles can be assigned at the organization level or by using this business process at the worker level.

15. Click **Done**

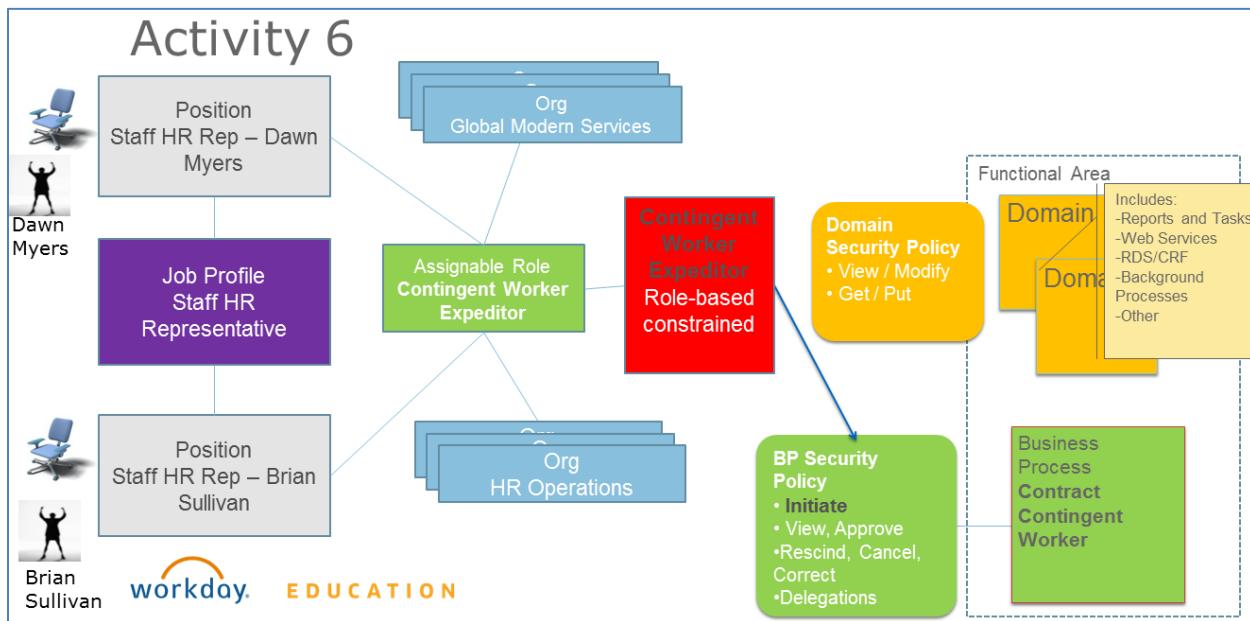
(End of Activity)



## ACTIVITY 6B – ADD CONTINGENT WORKER EXPEDITER TO THE BUSINESS PROCESS SECURITY POLICY

Now that you have created the new Contingent Worker Expediter security group you must modify the business process policy Contract Contingent Worker, activate, and test your changes.

## OVERVIEW



Logan McNeil will perform the following actions:

1. Business Process Security for Functional Area
  2. Activate Pending Security Policy Changes
  3. Test

## TASK 1: EDIT THE BUSINESS PROCESS SECURITY POLICY

### ⊕ As Logan McNeil (lmcneil)

1. Search for 'bp: contr cont worker glob mod serv'
2. Click the related action icon next to the business process definition for *Contract Contingent Worker for Global Modern Services*
3. Select **Business Process Policy > Edit** task

4. Go to the section **Who Can Start the Business Process (Contract Contingent Worker)**
  - a. Remove **HR Partner** and **HR Partner (By Location)** security groups
  - b. Add your new **Contingent Worker Expeditor** role-based constrained security group

5. Click **OK** to save the changes, then click **Done**

## TASK 2: ACTIVATE PENDING SECURITY POLICY CHANGES

1. From the search box, run the task: **Activate Pending Security Policy Changes**
2. Enter 'Activity 6' into the comments section
3. Click the **OK** button
4. Click the **Confirm** checkbox
5. Click the **OK** button

## TASK 3: TEST THE SECURITY CHANGES

### ⌚ Start proxy as Brian Sullivan (bsullivan)

1. Proxied as Brian, from the search box, run the task: **Contract Contingent Worker** (*Brian should now have access to this task that initiates the bp: Contract Contingent Worker*)

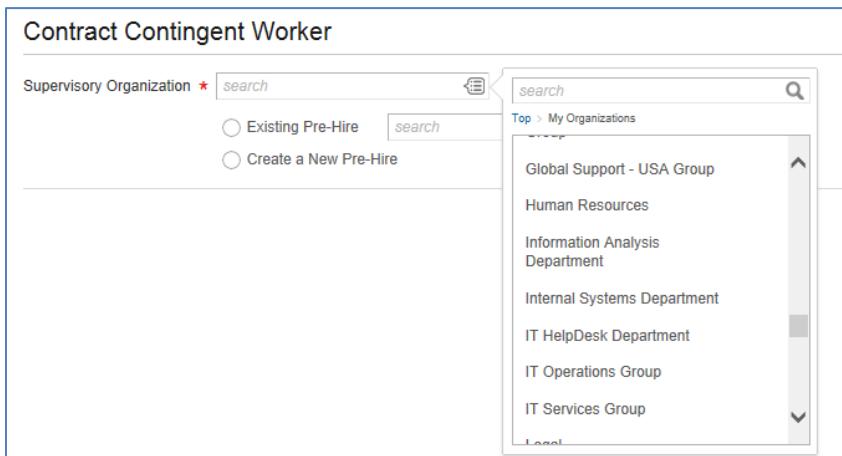
The screenshot shows the Workday search interface. The search bar at the top contains the text "contract contworker". Below the search bar, there is a blue header bar with the Workday logo and a user profile for "On behalf of: Brian Sullivan". The main area is titled "Search Results 1 items". Under the "Categories" section, "Common" is selected, and under "Assets", "Contract Contingent Worker" is listed under "Tasks and Reports".

2. When Brian executes this task, note how he is constrained to certain supervisory organizations. He only has access to target instances in the **HR Operations Department** as well as its subordinate organizations given the role-based constrained security group organization access rights.

The screenshot shows a modal dialog box titled "Contract Contingent Worker". It has a search field for "Supervisory Organization" with a red asterisk indicating it is required. There are two radio button options: "Existing Pre-Hire" and "Create a New Pre-Hire". At the bottom are "OK" and "Cancel" buttons. To the right of the dialog, a dropdown menu is open, showing a list of organizations under "Top > My Organizations": "HR Operations Americas Group", "HR Operations APAC Group", "HR Operations Department", and "HR Operations EMEA Group".

3. He cannot complete the contracting of contingent workers into other organizations (e.g. Accounts Payable Department) since he does not have access to the securable items (e.g. positions) in that organization.
4. Click **Cancel**

5. **Start proxy** as Dawn Myers (dmyers)
6. Proxied as Dawn, search for and execute the **Contract Contingent Worker** task.
7. From the Supervisory Organization prompt, under My Organizations, see how Dawn can pick any supervisory organization except the HR Operations Department and its subordinates. The role-based constrained security group organization access rights give her access to 'unassigned subordinates' and since the HR Operations Department is assigned to Brian Sullivan, Dawn does not have access to secured target items in those organizations.



Note: Though Dawn does not see Brian's assigned organizations in the My Organizations prompt as expected, she can enter the HR Operations department organization by name since the organization itself is visible in the tenant. Her access constraint will take effect when she tries to access target instances in the HR Operations department. She will not have access to the secured items in those organizations, e.g. the positions to contract a pre-hire.

8. **Stop proxy**

(End of Activity)

## ONE ROLE, MULTIPLE SECURITY GROUPS

Each role-based security group can only reference one role. However, you can have several role-based security groups for the same role, where each security group has a different constraint configuration.

This is easily shown with the **Manager** role. You can use the same Manager role in a number of role-based security groups, to express whether the user:

1. Has a direct relationship to the worker (role based constrained security group: Manager)
2. Is in the organization chain for the worker (role based constrained security group: Management Chain)
3. Has a direct relationship to which of the worker's multiple positions (role-based constrained security group: Primary Manager)
4. Is anyone in the role (role based unconstrained security group: Manager (Unconstrained))

The image displays three screenshots illustrating the configuration of role-based security groups for the Manager role:

- Screenshot 1: View Assignable Role Manager**  
Shows the properties of the Manager role. Key details include:
  - Role Name:** Manager
  - Workday Known Organization Role:** Manager
  - Role Usages:** Supervisory
  - Restricted to Single Provider:** No
  - Hide on View If Not Assigned:** No
  - Is Leadership:** Yes
  - Is Supporting:** No
  - Self-Assign:** No
  - Restricted to 'Assign Self-Assign Roles' BP:** No
  - Default to:** (empty)
  - Default for:** (empty)
  - For Security Groups:** Management Chain, Manager, Manager (Unconstrained), Primary Manager
  - Administered by Security Groups:** Security Administrator
- Screenshot 2: Edit Role-Based Security Group (Constrained) Primary Manager**  
Shows the configuration for the Primary Manager security group. Key details include:
  - Name:** Primary Manager
  - Comment:** Primary Manager
  - Context Type:** Constrained by Role Access
  - Group Criteria:** Assignable Role: Manager
  - Access Rights to Organizations:**
    - Applies To Current Organization Only
    - Applies To Current Organization And Unassigned Subordinates
    - Applies To Current Organization And All Subordinates
    - Applies To Current Organization And Subordinates To Level
  - Access Rights to Multiple Job Workers:**
    - Role has access to the positions they support
    - Role for primary job has access to all positions
    - Role has access to all positions
  - Subordinate Levels:** 0
- Screenshot 3: Edit Role-Based Security Group (Constrained) Management Chain**  
Shows the configuration for the Management Chain security group. Key details include:
  - Name:** Management Chain
  - Comment:** View members of assigned supervisory organizations and subordinates. Approval authority for HCM, expense, and procurement business processes.
  - Context Type:** Constrained by Role Access
  - Group Criteria:** Assignable Role: Manager
  - Access Rights to Organizations:**
    - Applies To Current Organization Only
    - Applies To Current Organization And Unassigned Subordinates
    - Applies To Current Organization And All Subordinates
    - Applies To Current Organization And Subordinates To Level
  - Access Rights to Multiple Job Workers:**
    - Role has access to the positions they support
    - Role for primary job has access to all positions
    - Role has access to all positions
  - Subordinate Levels:** 0

## WALKTHROUGH

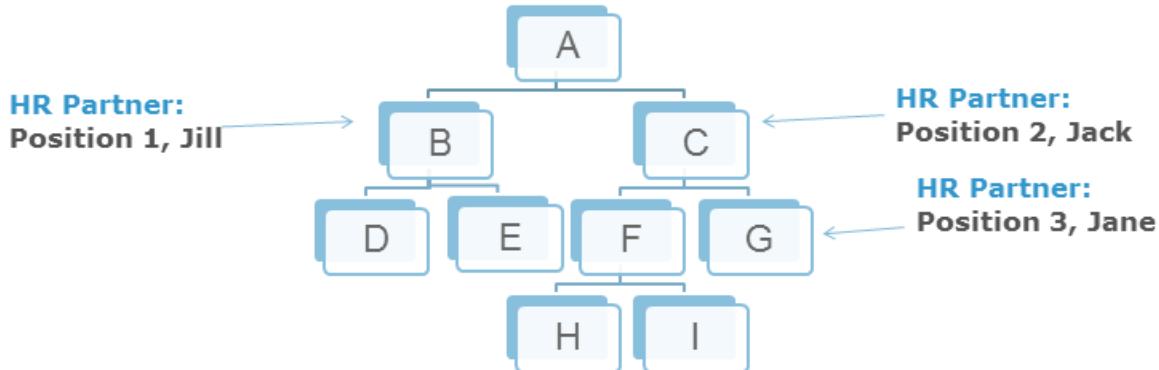
Using the graphic below, determine who has access to what, dependent on the configuration of the constraint.

COO = Current Organization Only

COUS = Current Organization and Unassigned Subordinates

COAS = Current Organization and All Subordinates

<u>Role</u>	<u>Security Group</u>	<u>Constraint</u>	<u>Members of Security Group</u>	<u>Domain or BP Sec Policy Access</u>	<u>Resulting access</u>
HR Partner	HR Partner1	COO		Initiate Hire	
HR Partner	HR Partner2	COUS		Worker Data: Personal Data	
HR Partner	HR Partner3	COAS		Initiate Request Comp Change	
HR Partner	HR Partner4	Unconstrained		Worker Data: Emergency Contacts	



*The completed walkthrough solution can be found in the back of this guide.*

## SERVICE CENTER-BASED SECURITY GROUPS

Workday enables you to grant **third-party users access to Workday** to perform configured tasks using service center based security groups. A common use case is an outsourced helpdesk, where helpdesk users need access to Workday to reset and manage workday accounts for Workday users. These helpdesk staff **users are not workers in the Workday tenant** and are not in your organization headcounts. These third party users need to be able to login to the Workday tenant and need to perform certain Workday tasks with access to Workday data.

Service Center representatives can be given limited access to Workday to support specific organizations only, using **Service Center Security Group (constrained)**. You can also configure unconstrained service center based security groups. When creating a service center based security group, you must specify a service center as the security group's criteria.

Group Criteria		Access Rights to Organizations	
Service Center	GMS Service Center	Organizations	Green Planet Solutions, Inc. (USA)
		<input type="radio"/>	Applies to Current Organization Only
		<input checked="" type="radio"/>	Applies to Current Organization And All Subordinates

To use service-center based security groups, you must first **define a service center** and **then create service center representatives for that service center**. Service Center representatives will show as members of the Service Center.

Members 3 items						
Service Center Representative	Active	Assigned to Service Center	Phone	Email	Work Address	Website
Erin Ford	06/27/2012	06/27/2012	+1 (800) 831-9663 x354 (Landline)	eford@gmsservicecenter.com		http://www.gmsservicecenter.com
Josh Wood	06/27/2012	06/27/2012	+1 (800) 831-9663 x356 (Landline)	jwood@gmsservicecenter.com		http://www.gmsservicecenter.com
Caroline Allen	06/27/2012	06/27/2012	+1 (800) 831-9663 x358 (Landline)	callen@gmsservicecenter.com		http://www.gmsservicecenter.com

When you create a service center representative you must also **create a Workday account** for the service center representative. These service center representative accounts will get some Workday delivered **automatically assigned security groups**, such as:

- **Service Center Representative as Self**
- **All Service Center Representatives**
- **All users**

View Security Groups for User jwood / Josh Wood [...]

Security Groups 4 items

Security Group	Type	Valid for Security Group Restrictions
All Service Center Representatives [...]	All Service Center Representatives Group	Public Groups
All Users	All Users Group	Public Groups
GMS Service Center	Service Center Security Group (Constrained)	Roles - Company
Service Center Representative as Self	Self Service Center Representative Group	Self-Service - Service Center

You can **inactivate Service Center Representatives** with the *Inactivate Service Center Representative* business process. Different *Inactivate Service Center Representative* business process definitions can be created for each Service Center.

Inactivating a representative:

- Disables the Workday account for the representative.
- No longer actively associates the representative with any Service Center.
- Removes the representative from delegation and all Service Center type security groups.

The screenshot shows the Workday interface for managing a Service Center Representative. On the left, there's a sidebar with 'View Service Center' and 'Members' sections. The main area displays 'Service Center Representative Josh Wood'. A context menu is open over his name, listing options like 'Edit', 'Assign Service Center', 'Inactivate', and 'Edit Workday Account'. The 'Inactivate' option is clearly visible and highlighted. Below the menu, there are tabs for 'Service Center Representative' and 'Service Center'. At the bottom, there's a table with columns for 'Name', 'Last Modified', 'Phone', and 'Email'.

## SERVICE CENTER BASED SECURITY GROUP DEPLOYMENT

- 1) **Create a Service Center** – a service center must exist.
- 2) **Create Service Center Representatives** for the service center. Service Center Representatives will be for each third party user.
- 3) **Create a Workday Account** for each Service Center Representative so that they can sign in to the tenant.
- 4) **Create a Service Center based security group** (Constrained or Unconstrained) for the Service Center.
  - a. **Members of the security group will be all service center representatives in that service center.**
  - b. **Configure access rights to target instances for defined organizations if constrained.**
- 5) **Configure the Service Center Based security group in needed domain or bp security policies.**
- 6) Activate
- 7) Test



## ACTIVITY 7A – CREATE SERVICE CENTER CALLED OUTSOURCED GLOBAL HELPDESK & REPRESENTATIVE

**Scenario:** Team members of a 3rd party IT outsourcing company need access to update worker account passwords. They will not be set up in Workday as workers. They should not be able to create new Workday accounts.

### TASK 1: CREATE THE SERVICE CENTER AND SERVICE CENTER REPRESENTATIVE

#### ⊕ As Logan McNeil (lmcneil)

1. Search for 'cr serv cent'
2. Select the **Create Service Center** task
3. Define the Service Center as follows:

<b>Field Name</b>	<b>Entry Value</b>
Name	Global Outsourced IT HelpDesk

4. Click the **OK** button
5. Click the related action icon for the service center
6. Select **Service Center -> Create Service Center Representative**
7. Enter data as follows:

<b>Field Name</b>	<b>Entry Value</b>
First Name	John
Last Name	Johnson

8. Click the **OK** button to save the changes
9. Click **Done**

## TASK 2: CREATE WORKDAY ACCOUNT FOR SERVICE CENTER REPRESENTATIVE

1. From the search box, enter **servicecenter: John** (*servicecenter: is the search prefix you can use to search for service centers or service center representatives. Remember that search prefixes must be lower case. For a full list of search prefixes, enter ? in the search box and hit enter.*).
2. Click the related action icon next to the name of the representative
3. Select **Security Profile -> Create Workday Account**
4. Enter Account Information as follows:

<b>Field Name</b>	<b>Entry Value</b>
User Name	jjohnson.scr
New Password	<use class assigned password>
Re-Enter Password	<use class assigned password>
Require New Password at Next Sign In	Deselect checkbox

5. Click the **Submit** button
6. Click the **Done** button
7. From the search box, run **View Security Groups for User**, and select *jjohnson*.

View Security Groups for User

Person ★ jjohnson.scr / John Johnson (Work)

8. See how John's Workday account has several automatically assigned security groups, allowing John to do what, for example, All Users can do, and what All service center representatives can do.

View Security Groups for User jjohnson.scr / John Johnson

Security Groups 3 items

Security Group	Type	Valid for Security Group Restrictions
All Service Center Representatives	All Service Center Representatives Group	Public Groups
All Users	All Users Group	Public Groups
Service Center Representative as Self	Self Service Center Representative Group	Self-Service - Service Center

(End of Activity)



## ACTIVITY 7B – CREATE AND DEPLOY SERVICE CENTER-BASED SECURITY GROUP

Now that you have created the Service Center and Service Center Rep, create the security group and edit the domain security policy (System –Security Administration - Workday Accounts).

### OVERVIEW

Logan McNeil will perform the following actions:

1. Create Security Group
2. Edit Domain Security Policy
3. Activate
4. Test Membership

### TASK 1: CREATE THE SECURITY GROUP

#### As Logan McNeil (lmcneil)

1. Search for '*cr sec gr*'
2. Select the **Create Security Group** task
3. Set the type and name as follows:

<b>Field Name</b>	<b>Entry Value</b>
Type of Tenanted Security Group	Service Center-Based Security Group (Constrained)
Name	Outsourced IT

4. Click the **OK** button
5. Configure the Security Group as follows:

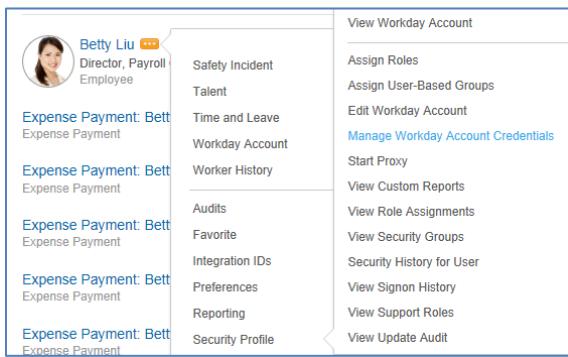
<b>Field Name</b>	<b>Entry Value</b>
Service Center	Global Outsourced IT HelpDesk

Organizations	All Organizations by Type > Supervisory -> Global Modern Services > <b>Human Resources</b>
Applies to Current Organization and All Subordinates	Selected

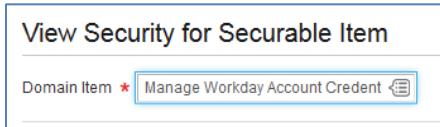
- Click the **OK** button, then click the **Done** button

## TASK 2: EDIT THE DOMAIN SECURITY POLICY

- Passwords are changed using the **Manage Workday Account Credentials** task. Let's now determine which domain(s) secure this item.



- Run the report **View Security for Securable Item** for the item: *Manage Workday Account Credentials* task.



- Click OK.
- From the *Workday Account Passwords* security policy, use related actions and select **Domain Security Policy > Edit Permissions**

Type Task

Related Menu Path Security Profile > Manage Workday Account Credentials

Permission Required Modify

Hidden Workday Delivered Report No

**Domain Security**

Domain Security 2 items

- Security Policy
- Workday Accounts

Workday Account Passwords

**Available Actions**

Domain Security Policy Workday Account Passwords

- Edit Permissions
- Disable
- Favorite
- Functional Area
- Integration IDs
- Reporting
- View All for Functional Area
- View Domain
- View History

## 5. Remove the following security group: **All Service Center Representatives**

This unconstrained security group allows any service center representative access to the tasks for anyone. **Since we want to constrain the access, we are deleting this group and will next add our constrained security group instead.**

## 6. Add the **Outsourced IT** security group for **View and Modify** access

**Edit Permissions Workday Account Passwords**

Description This domain provides access to password maintenance only. For the ability to edit accounts, you must also have access to the Workday Accounts domain.

Status Active

Functional Areas System

Parent Policy Security Administration

Securable Actions 1

Report/Task Permissions 2 items

	*Security Groups	View	Modify
(+)	Outsourced IT	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

**Alerts: 1**

Activate your security policy changes using the Activate Pending Security Policy Changes task, and update the security evaluation moment, which is currently set to 03/24/2015 09:54:07.838.

## 7. Click **OK** to save the changes

## 8. Click the **Done** button

## TASK 3: ACTIVATE PENDING SECURITY POLICY CHANGES

- Search for '*activate*'
- Click the **Activate Pending Security Policy Changes** task
- Enter '*Activity 7*' into the comments section

4. Click the **OK** button
5. Click the **Confirm** checkbox
6. Click the **OK** button to activate the changes

(End of Activity)



## ACTIVITY 7C – TEST SERVICE CENTER-BASED SECURITY

Sign in as a Service Center Rep and verify that you have access to change passwords for the organization you support.

### TASK 1: TEST SERVICE CENTER ACCESS TO MANAGE PASSWORDS

**Sign in as John Johnson (jjohnson.scr)** (Proxy session is not available since John is not an employee – remember the scope of the proxy access policy we configured in Activity 4 only allows employees to proxy on behalf of employees. If we had allowed proxy on behalf of ‘All users’ instead, we could have proxied as John Johnson.)

1. Enter login information as follows:

<b>Field Name</b>	<b>Entry Value</b>
User Name	jjohnson.scr
Password	<use class assigned password>

2. Configure challenge questions, using the drop-down menu as follows:

<b>Field Name</b>	<b>Entry Value</b>
What city were you born in?	Boston
What city was your mother born in?	Boston

3. And click OK.
4. Search for ‘bette’ and click on the related action.
5. Note John’s access under **Security Profile**, and the task **Manage Workday Account Credentials**

The screenshot shows the Workday search interface. A search bar at the top contains the query 'bette'. Below the search bar, the 'Categories' sidebar is visible with 'Common' selected. The main area displays 'Search Results' for 'Common' items, showing one result: 'Betty Liu' (Human Resource Employee). On the right side, there is a 'Available Actions' panel for 'Worker Betty Liu' which includes the 'Manage Workday Account Credentials' task. The top right corner of the screen shows the user's session information: 'jjohnson.scr / John Johnson'.

6. Search for Bettina Strauss.
7. Note there is no Security Profile option. Why? Bettina is a member of Global Support – EMEA Group organization, which John Johnson does not support. Recall that the Outsourced IT service center security group was constrained to Human Resources and subordinate organizations.

The screenshot shows a Workday search interface. The search bar at the top contains the text "bettina straus". The results section is titled "Search Results 1 items". A single result is listed under the "Common" category: "Bettina Strauss" (Global Support - EMEA Employee). To the right of the result, there is a "Available Actions" panel with options like "Favorite" and "Additional Data". Below the result, a "Worker" card displays "Bettina Strauss" with icons for export and print. A "Contact" link is also visible.

8. Sign Out

(End of Activity)

## ROLES FOR SERVICE CENTERS

Since Service Centers are an organization type in Workday, you can **assign roles to Service Centers** to identify support or leadership staff for a service center. A common use case would be creating a role of **Service Center Manager**. This role can then be assigned to a position (or service center representative) and a role-based constrained security group can be leveraged to allow those in the role to, for example, create service center representatives for their assigned service center.

The screenshot illustrates the process of managing roles for Service Centers in Workday. It consists of two main panels:

- Left Panel: Edit Role-Based Security Group (Constrained) Service Center Manager**
  - Name:** Service Center Manager
  - Comment:** Perform service center functions for assigned service centers. Examples include maintaining service center representatives. Approval authority for service center business processes.
  - Context Type:** Constrained by Role Access
  - Inactive:**
  - Group Criteria:** Assignable Role: Service Center Manager
  - Access Rights to Organizations:**
    - Applies to Current Organization Only
    - Applies To Current Organization And Unassigned Subordinates
    - Applies To Current Organization And All Subordinates
    - Applies to Current Organization or Subordinates to Level
  - Access Rights to Multiple Job Workers:**
    - Role has access to the positions they support
    - Role for primary job has access to all positions
    - Role has access to all positions
  - Domain Security Policy Permissions:**

Operation	Domain Security Policy	Domain Security Policies Inher.
View and Modify	Manage: Service Center	
  - Business Process Security Policy Permissions:**
- Right Panel: View Service Center GMS Service Center**
  - Available Actions:** Service Center, GMS Service Center
  - Contact Information:** Name: GMS Service Center
  - Members:** Roles
  - Assignable Role:** Service Center Manager
  - Actions:**
    - Assign Roles
    - View Role Assignment History
    - View Roles
    - Security History

Annotations with green callouts point to specific features:

- A callout labeled "Configure Needed Constraints" points to the Context Type section.
- A callout labeled "Role enabled for org type: Service Center" points to the Group Criteria section.
- A callout labeled "Grant Access to Tasks" points to the Domain Security Policy Permissions section.
- A callout labeled "Assign Role" points to the Assignable Role section in the right panel.



## ACTIVITY 7D – OPTIONAL - CONFIGURE SERVICE CENTER MANAGER ROLE

**Scenario:** A new role is to be created called IT Service Center Manager. The IT Service Center Manager will have permission to create and manage service representatives for his service center. Jack Taylor will be assigned to this role.

Jack Taylor currently cannot access Create Service Center Representatives. Verify this by running the [View Security for Securable Item](#) report. Jack is not a member of these security groups. You could use the Test Membership action off each Permitted Security Group to verify.

Another option is to run the [Security Analysis for Action](#) report. You will find that Jack Taylor does not have permission to access create service center representative task.

View Security for Securable Item Create Service Center Representative [...]			
Type	Task		
On Menu	Menu: Security Administration		
Related Menu Path	Service Center > Create Service Center Representative		
Permission Required	Modify		
Hidden Workday Delivered Report	No		
<a href="#">Domain Security</a>		Language Restrictions	
Domain Security			
Security Policy	Domain	Functional Areas	Permitted Security Groups
<a href="#">Manage: Service Center</a>	Q	System	Implementers Security Administrator Service Center Administrator Service Center Manager

### TASK 1: MAINTAIN ASSIGNABLE ROLES

#### ⊕ As Logan McNeil (lmcneil)

1. Search for 'maintain role' and click the **Maintain Assignable Roles** task
2. Add a row and configure the role as follows:

Field Name	Entry Value
Role Name	IT Service Center Manager
Enable for	Workday Organization Types > Service Center
Hide on View if Not Assigned	Do Not Check the Box
Restricted to Single Assignment	Check the box
Is Leadership/Is Supporting	Select Is Leadership
Assigned by Security Groups	Security Administrator

3. Click **OK**, then **Done**

## TASK 2: CREATE SECURITY GROUP

1. Search for 'create sec gr'
2. Click on the **Create Security Group** task
3. Set the type and name as follows:

<b>Field Name</b>	<b>Entry Value</b>
Type of Group	Role-based Security Group (Constrained)
Name	IT Service Center Manager

4. Click the **OK** button
5. Configure the security group as follows:

<b>Field Name</b>	<b>Entry Value</b>
Group Criteria > Assignable Role	By Organization Type > Service Center > IT Service Center Manager
Access Rights to Organization	Applies to Current Organization and Unassigned Subordinates
Access Rights to Multiple Job Workers	Role has access to the positions they support

6. Click **OK** to save
7. Click **Done**

## TASK 3: ASSIGN ROLE

1. Search for 'servicecenter: glob out'
2. From the related action icon on the Global Outsourced IT HelpDesk, select **Roles > Assign Roles**.
3. Click the **OK** button to accept today as the Effective Date
4. Click to add a new row in the **Assign Roles** section
5. Click on the **Role** prompt and select **IT Service Center Manager**
6. Click on the **Assigned To** prompt to select Job Profile prompt Manager, IT HelpDesk > Jack Taylor

7. Click **OK**, then click **Done**

#### TASK 4: EDIT SECURITY POLICY

1. Which security policy do we need to edit?
2. Run **View Security for Securable Item** for the **Create Service Center Representative** task.
3. From the **Manage Service Center** Security Policy, use related actions and select Domain Security Policy > Edit Permissions
4. Add **IT Service Center Manager** to the list of security groups with **View and Modify** access
5. Click **OK** and **Done**
6. Search for '*activate*'
7. Click the **Activate Pending Security Policy Changes** task
8. Enter 'Activate IT Service Center Manager'
9. Click **OK**
10. Click the **Confirm** checkbox
11. Click **OK**

#### TASK 5 TEST SERVICE CENTER ROLE

1. **Start proxy** as Jack Taylor (jtaylor)
2. Search for 'create serv cent rep'
3. Jack can now create service center representatives for Global Outsourced IT HelpDesk.
4. Cancel and Stop proxy

(End of Activity)

## JOB-BASED SECURITY GROUPS

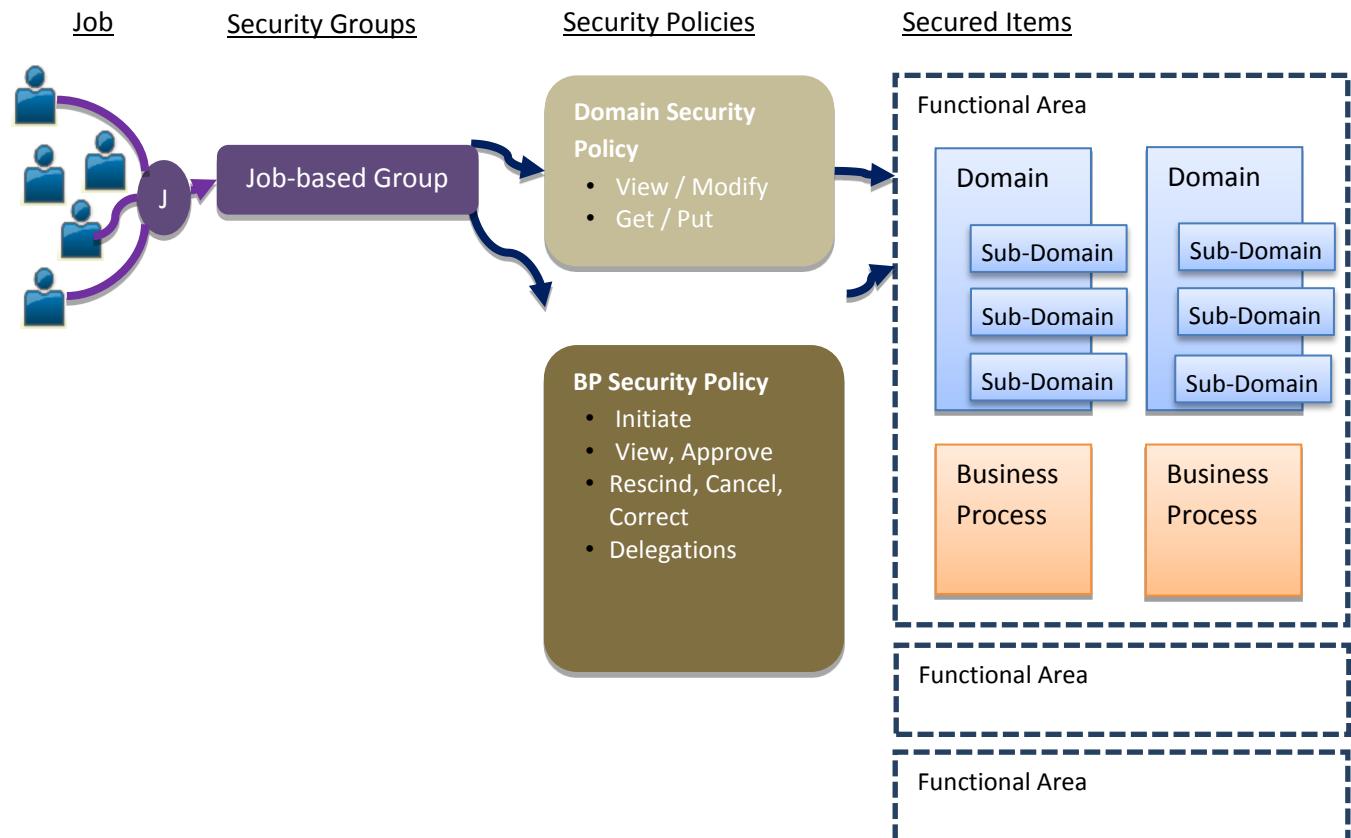
Job-based security groups can be used to identify members based on **job details** such as job profile, job family, management level or exempt vs. non exempt jobs. They can be defined as either **constrained** or **unconstrained**. **Membership is automatically derived** for workers that match the defined job criterion. System users in this group can only be workers since they require job-relevant criteria. The selection will be made from currently active workers.

Relevant job criteria are:

- Job Profile
- Job Category
- Job Family
- Management Level
- Work Shift
- Include Exempt Jobs
- Include Non Exempt Jobs

Examples of Job-Based Security Groups are:

- Employee Type - Exempt; non-Exempt
- Job Profile - CEO; CHRO
- Job Family - HR-Payroll
- Management Level – Vice President



**Note:** You can only specify and grant access based on one job criterion in a job-based security group. For example, you can create a job-based security group for Exempt Employees, but not one for Exempt employees AND Management Level: Vice President.

## Configurable Security Fundamentals 24

In the following example, using a **job-based constrained** security group, we are identifying members as those in the IT related job families. We are then also constraining them to target instances in the Company Hierarchy that they are currently in and all subordinate nodes in the hierarchy.

This security group will identify IT Workers constrained to their company hierarchy organization.

View Job-Based Security Group (Constrained) [IT Workers](#) [...](#)

Security Group Name: IT Workers  
Context Type: Constrained by Organization Access

**Group Criteria**

Job Profile  
 Job Category  
 Job Family: [Information Technology](#)  
[IT-HelpDesk](#)  
[IT-Management](#)  
[IT-Services](#)  
[IT-Support](#)  
[IT-Systems](#)  
 Management Level

**Access Rights**

Apply to Organization Type: [Company Hierarchy](#)  
 Applies to Current Organization Only  
 Applies to Current Organization And All Subordinates

If we look at a **job-based unconstrained** example, we are identifying members based on a job criterion, similar to the above example, however, if we use this security group in domain or business process security policies, access will be unconstrained. Workday will not attempt to enforce target constraints based on organization.

View Job-Based Security Group (Unconstrained) [Chief Financial Officer](#) [...](#)

Security Group Name: Chief Financial Officer  
Context Type: Unconstrained

**Group Criteria**

Job Profile: [Chief Financial Officer](#)  
 Job Category  
 Job Family  
 Management Level  
 Work Shift  
 Include Exempt Jobs  
 Include Non Exempt Jobs

## HOW IS JOB BASED DIFFERENT THAN ROLE BASED?

Role-based security groups derive membership based on role assignment to a position. Positions represent a 'chair' that a worker is filling and 'sitting in'. Positions have job details, e.g. an associated job profile. **Job based security groups derive membership based on the job details.**

In the example, below, Dawn Myers the worker is in a position **Staff HR Representative – Dawn Myers**. This position, ties to the job profile: Staff HR Representative. Her job details show a Management level of 8- Individual Contributor.



Dawn Myers ...

Staff HR Representative

Available Actions		Position Staff HR Representative - Dawn Myers	
Position	Worker	Dawn Myers	
Audits	Supervisory Organization	HR Operations Americas Group	
Business Process	Job Profile	Staff HR Representative	
Compensation	Favorite	Location	
Integration IDs		New York	
Job Change			
Organization			
Payroll			
Reporting			

**WORK ADDRESS**

1155 Avenue of the Americas  
New York, NY 10036  
United States of America

**Job Details**

Employee ID	21144
Organization	<a href="#">Global Modern Services &gt;&gt; HR</a>
Position	Staff HR Representative <span style="color: orange;">...</span>
Business Title	Staff HR Representative
Job Profile	Staff HR Representative
Employee Type	Regular
Management Level	8 Individual Contributor

If we look at the worker, Brian Sullivan. Brian sits in the chair or position is **Staff HR Representative – Brian Sullivan**. This position is tied to the same job profile, Staff HR Representative. Brian's job details also show a management level of 8-individual contributor.



Staff HR Representative

Available Actions		Position Staff HR Representative - Brian Sullivan	
Position	Worker	Brian Sullivan	
Audits	Supervisory Organization	HR Operations Americas Group	
Business Process	Job Profile	Staff HR Representative	
Compensation	Favorite	San Francisco	
Integration IDs			
Job Change			
Organization			
Payroll			
Reporting			

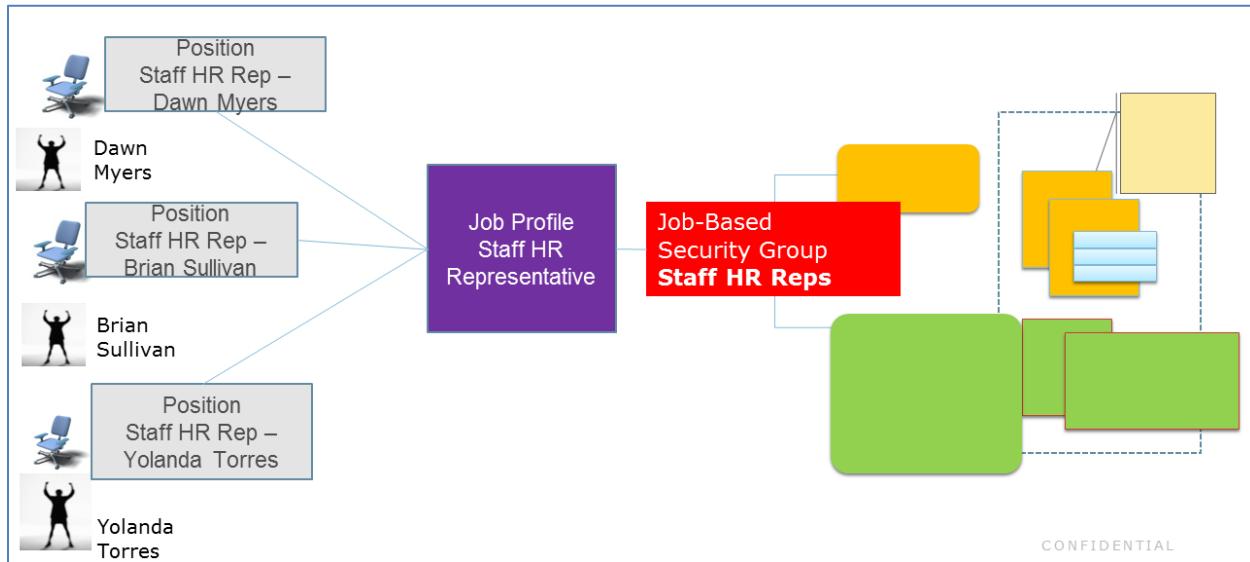
**WORK ADDRESS**

3939 The Embarcadero  
San Francisco, CA 94111  
United States of America

**Job Details**

Employee ID	21143
Organization	<a href="#">Global Modern Services &gt;&gt; HR</a>
Position	Staff HR Representative <span style="color: orange;">...</span>
Business Title	Staff HR Representative
Job Profile	Staff HR Representative
Employee Type	Regular
Management Level	8 Individual Contributor

Using job based security groups, we can identify workers based on job details such as job profile or management level. The example below shows a job based security group identifying workers in the job profile: Staff HR Representative. Dawn, Brian and Yolanda would be automatic members.



CONFIDENTIAL

## CREATE AND DEPLOY JOB-BASED SECURITY GROUP

1. Run Create Security Group task
2. Identify needed access to domains or business processes
3. Edit Security Policies
4. Activate Pending Security Policy Changes
5. Test



## ACTIVITY 8 – CREATE AND DEPLOY JOB-BASED SECURITY GROUP

**Scenario:** Expense reports should be approved by director level workers for the given company

### OVERVIEW

Logan McNeil will perform the following actions:

1. Create Security Group
2. Test Membership
3. Edit Business Process Security Policy to allow new security group to approve
4. Activate
5. Edit Business Process Definition
6. Test

### TASK 1: CREATE THE SECURITY GROUP

⌚ As Logan McNeil (@mcneil)

1. Search for and execute **Create Security Group** task
2. Define the Security Group as follows:

<b>Field Name</b>	<b>Entry Value</b>
Type of Tenanted Security Group	Job-Based Security Group (Constrained)
Name	Director Level Approval

3. Click the **OK** button
4. Edit the Job-Based Security Group (Constrained) as follows:

<b>Field Name</b>	<b>Entry Value</b>

Group Criteria > **Management Level**

5-Director

Organization Access

Company

Company Hierarchy

Current Organization and all subordinates

Edit Job-Based Security Group (Constrained) Director Level Approval ...

Security Group Name *	<input type="text" value="Director Level Approval"/>
Comment	<input type="text"/>
Context Type	Constrained by Organization Access
Inactive	<input type="checkbox"/>
<b>Group Criteria</b>	
<input type="radio"/> Job Profile	<input type="text" value="search"/> <input type="button" value="..."/>
<input type="radio"/> Job Category	<input type="text" value="search"/> <input type="button" value="..."/>
<input type="radio"/> Job Family	<input type="text" value="search"/> <input type="button" value="..."/>
<input checked="" type="radio"/> Management Level	<input type="text" value="search"/> <input type="button" value="..."/> <input checked="" type="checkbox"/> 5 Director
<b>Access Rights</b>	
Apply to Organization Type *	<input type="text" value="search"/> <input type="button" value="..."/>
<input checked="" type="checkbox"/> Company Hierarchy <input checked="" type="checkbox"/> Company	
<input type="radio"/> Applies to Current Organization Only <input checked="" type="radio"/> Applies to Current Organization And All Subordinates	

5. Click the **OK** button to save the changes

6. Click the **Done** button

## TASK 2: SEE SECURITY GROUP MEMBERSHIP

1. With Job-based security groups, members are automatically derived given their job details.
2. Run a custom report in the tenant: **WDINST – Who are the members of a security group**

The screenshot shows the Workday navigation bar with a home icon and a search bar containing 'wd who are sec'. Below the bar, the title 'WDINST-Who are the members of a security group' is displayed. Underneath the title, there is a search input field with 'search' placeholder text and a 'Director Level Approval' filter button.

3. See the members. Members shown are all workers in the tenant in positions where the job profile is a director level.

Security Group	Type	Members
Director Level Approval	Job-Based Security Group (Constrained)	abianchi / Angela Bianchi arizzo / Anthony Rizzo bharper / Brad Harper bliu / Betty Liu bmuller / Boris Müller cabott / Carol Abbott calves / Carlos Alves cgibson / Catherine Gibson cstewart / Camilla Stewart dshaw / Dylan Shaw <a href="#">More (27)</a>

4. We will focus on 2 members: Camila Stewart and Carlos Alves.
  - a. Camila Stewart is in the Company, Global Modern Services, PLC (U.K.)
  - b. Carlos Alves is in the Company, Global Modern Services SA (Brazil)

## TASK 3- EDIT BUSINESS PROCESS SECURITY POLICY

1. In a business process definition, you can only route approval steps to permitted security groups. Permitted security groups for approval steps are configured in the business process security policy. If we want to route an approval step to our new job based, Director Level Approval, security group, we must first configure it in the bp security policy as an allowed security group for approvals.
2. From the search box, search for the **bp: expense report event**
3. Using related actions off of any of the definitions for this bp type (remember there is **only one security policy per bp type**, not per bp definition copy), select **Business Process Policy > Edit** task

Search Results 4 items  
All of Workday

- Expense Report Event (Default Definition)  
Business Process Definition
- Expense Report Event for Global Modern Services Companies  
Business Process Definition
- Expense Report Event for Global Modern Services GmbH (Germany)  
Business Process Definition
- Expense Report Event for Global Modern Services, Ltd (Canada)  
Business Process Definition

**Available Actions**

- Audits
- Business Process
- Business Process Policy
- Edit**

4. Scroll down to find the **Approval section** and add your security group, **Director Level Approval**.

Action View Completed Only

Security Groups

Action Approve

Security Groups

Director Level Approval

Job-Based Security Group (Constrained) Director Level Approval

Security Group Director Level Approval

Context Type Constrained by Organization Access

Alerts: 1

Activate your security policy changes using the [Activate Pending Security Policy Changes](#) task, and update the security evaluation moment, which is currently set to 03/24/2015 10:27:27.695.

5. Click **OK** to save the changes
6. Click the **Done** button

## TASK 4: ACTIVATE PENDING SECURITY POLICY CHANGES

1. From the search box, run the task: **Activate Pending Security Policy Changes**
2. Enter 'Activity 8' into the comments section
3. Click the **OK** button
4. Click the **Confirm** checkbox
5. Click the **OK** button to activate the changes

## TASK 5: EDIT THE BUSINESS PROCESS DEFINITION

1. Search for 'bp: Expense Report Event Glob'
2. Use the related action icon off of the business process definition for **Expense Report Event for Global Modern Services** and select **Business Process < Edit Definition** task

The screenshot shows the Workday search interface. The search bar at the top contains the query 'bp: exp rep even glo'. The results section displays three items under 'Search Results 3 items' and 'All of Workday'. The first item, 'Expense Report Event for Global Modern Services Companies', is selected and highlighted with a blue border. A context menu is open over this item, with the 'Edit Definition' option highlighted. Other options in the menu include 'Audits', 'Business Process', 'Business Process Policy', 'Favorite', 'Add Notification', 'Copy or Link Business Process Definition', and 'Edit Definition'.

3. Click **OK** to accept today as the Effective Date
4. Click the icon to add a new step
5. Configure the step as follows:

<b>Field Name</b>	<b>Entry Value</b>
Order	Ab
Type	Approval
Group	Director Level Approval <i>(Security groups shown in the prompt for this</i>

approval step are those with Approval permissions in the bp security policy)

*Order	If	Notes	^Type	Specify	Optional	Group
ab			Approval		<input type="checkbox"/>	<input type="button" value="search"/> <input checked="" type="checkbox"/> Director Level Approval

6. Click the **OK** button
7. Click the **Done** button

#### TASK 6: TEST

1. **Start proxy** as Benjamin Green (bgreen).
2. Benjamin is a worker in the UK. His company assignment is Global Modern Services, PLC UK. We will have Benjamin submit an expense report and see how Camilla, a director in the same company will receive the approval.
3. As Benjamin, from the search box, run **Create Expense Report**
4. **Click OK to start a new expense report**
5. Scroll down and enter a sample expense item as follows
  - a. Expense Item: International Airfare
  - b. Enter amount: \$100
  - c. Airline: British Airways
  - d. Destination: Amsterdam

Expense Report Lines
Attachments

[+ Add](#)
[+ Import Existing Record](#)

03/08/2015    100.00  
 International Airfare

**Expense Report Line**

Date	<b>*</b> 03/08/2015	<input type="button" value=""/>
Expense Item	<b>*</b> International Airfare	<input type="button" value=""/>
Quantity	<b>*</b> 1	
Per Unit Amount	<b>*</b> 100.00	
Total Amount	<b>*</b> 100.00	
Currency	<b>*</b> GBP	<input type="button" value=""/>
Currency Rate	1	
Converted Amount	<b>*</b> 100.00	
Converted Currency	GBP	

**Item Details**

Airline	<b>*</b> British Airways	<input type="button" value=""/>
Origination	<input type="button" value="search"/>	<input type="button" value=""/>
Destination	<b>*</b> Amsterdam, Netherlands	<input type="button" value=""/>
Country	<input checked="" type="checkbox"/> Netherlands	<input type="button" value=""/>
Ticket Number	<input type="text"/>	

© 2015 Workday, Inc.

91

6. Click on Submit
7. Note the next step in the business process is your director level approval step.
8. Expand the **Details and Process** and click on the **Process** tab to see the awaiting recipients.
  - a. The awaiting recipients are those in Director management levels that are in the Company: Global Modern Services, PLC UK (Benjamin's company and company hierarchy).

The screenshot shows a business process details page. At the top, there are links for 'Up Next' (Director Level Approval, Approval by Director Level Approval), 'Do Another' (Create Expense Report), and 'Related Links' (Business Policy Document). Below this, the 'Details and Process' section is expanded, showing:

- For: Expense Report EXP-00005059
- Overall Process: Expense Report: Benjamin Green on 04/11/2015 for £100.00
- Overall Status: In Progress
- Due Date: 04/18/2015

Below this is a table with two tabs: 'Details' and 'Process'. The 'Process' tab is selected, showing a 'Process History' table with 7 items. The table has columns: Process, Step, Status, Completed On, Due Date, and Person. The rows are:

Process	Step	Status	Completed On	Due Date	Person
Expense Report Event	Expense Report Event	Step Completed	04/11/2015 04:01:19 PM	04/18/2015	Benjamin Green
Expense Report Event	Approval by Director Level Approval	Awaiting Action			Boris Müller (Director Level Approval)
					Camilla Stewart (Director Level Approval)
					Dylan Shaw (Director Level Approval)
					Ella Phillips (Director Level Approval)
					Katarina Lindgren (Director Level Approval)
					Oscar Bell (Director Level Approval)

9. Click Done.
10. **Start proxy** as Carolina Souza (csouza). Carolina is a worker in Brazil.
11. As Carolina, from the search box, run **Create Expense Report**
12. **Click OK to start a new expense report**
13. Scroll down and enter a sample expense item as follows
  - a. Expense Item: International Airfare
  - b. Enter amount: \$100
  - c. Airline: American
  - d. Destination: Las Vegas, United States of America
14. Click on **Submit**
15. Note the next step in the business process is your director level approval step. Expand the **Details and Process** and click on the **Process** tab to see the awaiting recipients.

- a. The awaiting recipients are those in Director level management jobs that are in the Company: Global Modern Services, SA (Brazil) or company hierarchy. Note Carlos Alves. He is a worker in the Director management level in Company Brazil.

<b>Up Next</b>	<b>Do Another</b>	<b>Related Links</b>			
Director Level Approval	Create Expense Report	<a href="#">Business Policy Document</a>			
Approval by Director Level Approval					
<b>⊕ Details and Process</b>					
For	<a href="#">Expense Report: EXP-00005060</a>				
Overall Process	<a href="#">Expense Report: Carolina Souza on 04/11/2015 for R\$100.00</a>				
Overall Status	In Progress				
Due Date	04/18/2015				
<input type="button" value="Details"/> <input style="border: 1px solid #ccc; padding: 2px 10px; border-radius: 5px; background-color: #f0f0f0; color: #0070C0; font-weight: bold; margin-left: 10px;" type="button" value="Process"/>					
<b>Process History</b> 4 items					
Process	Step	Status	Completed On	Due Date	Person
<a href="#">Expense Report Event</a>	Expense Report Event	Step Completed	04/11/2015 04:03:55 PM	04/18/2015	<a href="#">Carolina Souza</a>
<a href="#">Expense Report Event</a>	Approval by Director Level Approval	Awaiting Action			<a href="#">Carlos Alves (Director Level Approval)</a>
					<a href="#">Elsa Ramos Vasquez (Director Level Approval)</a>
					<a href="#">Juan-Carlos Salazar Jimenez (Director Level Approval)</a>

## 16. Stop Proxy

(End of Activity)

## INTEGRATION SYSTEM SECURITY GROUPS

An Integration System security group is a group to which you add system users (accounts, not people) as members. This group does not have access to the user interface.

Workday's delivered integrations use web service operations (or web service tasks) to get data from Workday to include on outbound integrations, and to put data received from inbound integrations into Workday. Cloud Connect and Studio integrations require an Integration System User account for authentication and access to web service tasks. Each integration system must have its own Integration System User account. Integration System Users are always members of Integration System Security Groups (constrained or unconstrained); they cannot be included in any other type of security group.

In order for the integration to work correctly, the Integration System User's security group must have Put and Get access to the domains that contain the web service operations that interact with the necessary data.



**Note:** Enterprise Interface Builder (EIB) integrations are secured through the current user's logon credentials and do not require an integration system user account.

Workday recommends, as a security best practice, that you set up integrations (RaaS, EIB, public API) and schedule them to be run by integration system users. In this way, your audit trails for the user interface track actions taken by people in Workday, thus ensuring that people are accountable for the changes or actions they take.

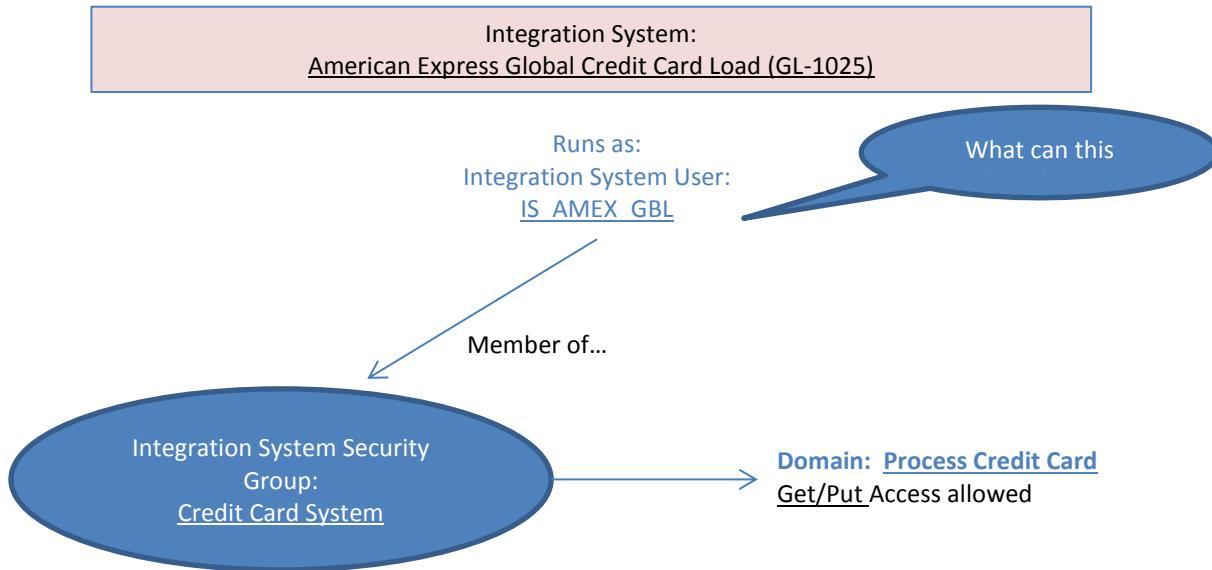
## CONSTRAINED VS. UNCONSTRAINED INTEGRATION SECURITY GROUPS

An Integration System Security Group (Constrained) serves the same general purpose as an Integration System Security Group (Unconstrained). The only difference is that the constrained group type enables you to filter data results contextually based on Organization. For example, you can set up an integration that exports data only for workers who are members of a specific supervisory Organization. Filtering varies depending on how the data is accessed:

Public web service: Workday filters by element, not by row, based on the security of the underlying web service operation. For example a Workday integration that returns worker data will return one row for each worker, but may filter out some data for that worker. Data is filtered out if the underlying web service operation's element is secured to a different domain than the web service operation itself. To determine which elements (if any) are filtered out, see the [Workday Public API](#) documentation.

Reports as a Service (RaaS): Workday filters by row based on the security of the underlying report data source.

EXAMPLE:



### CREATE AND DEPLOY INTEGRATION SYSTEM SECURITY GROUPS

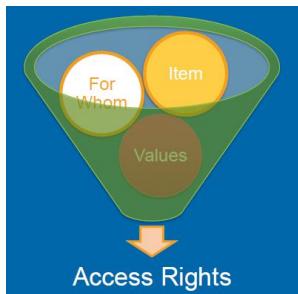
1. Create Integration System User accounts
2. Run Create Security Group task
3. Add Integration System Users to Group
4. Edit Security Policies
5. Activate Pending Security Policy Changes
6. Test

## SEGMENT-BASED SECURITY GROUPS

A segment-based security group grants access to members of other security groups. It grants access to selected components or **values** (a segment) of the secured item. The security group definition specifies the segment to which it grants access. That is, you use this security group to control access to policies whose secured items include components in the segment.

**Note:** Before implementing segmented security, it is important to analyze the organization's needs and decide whether segmented security is truly required, as it adds additional maintenance and overhead to the security implementation.

Segmented security is that "third level" of access in Workday. It assumes the user (1) has access to the **item** in Workday, (2) the user will be constrained to organizations or targets "**for whom**" they can see data given the security group that is configured, and then (3) determines which **values** the user will have access to given the configured segments.



## Segmented Areas

- Compensation Setup
- Pay Components
- Business Process Types
- Customers
- Document Categories
- Compensation Plan assignments
- Expense Items
- Integration Systems
- Investors
- Message Queues
- Questionnaires
- Requisition Spend Categories
- Requisition Suppliers
- Supplier Contracts
- Supplier Links

1	Who can see worker documents	Who can see pay components	Who can create a requisition	Who can create an expense report
2	For whom can you see worker documents ?	For whom can you see pay components?	For what organization can you create a requisition	For whom can you create an expense report
3	Which document categories	Which pay components	Which spend categories can you see	Which expense items can you see

## Segmented security groups allow you to configure which security groups have access to which segments

- ✓ Security groups must exist and can be constrained or unconstrained
- ✓ Segments must be defined and maintained.
- ✓ Segment based security groups must then be used in needed domain security policies to enable segmented access

View Segment-Based Security Group Documents - Compensation Categories

Name: Documents - Compensation Categories

Context Type: Constrained by Segment Access

Group Criteria:

- Security Groups: Compensation Administrator
- Compensation Partner

Access Rights:

- Access to Segments: Document Categories - Policy
- Document Categories - Worker Event

Domain Security Policy Permissions			
Operation	Domain Security Policy	Domain Security Policies Inheriting Permission	Functional Areas
View Only	Worker Data: Documents		Personal Data

## WHAT AREAS OF WORKDAY CAN YOU SEGMENT?

To see what areas of Workday can be segmented, run: **Domain Security Policies for Functional Area** (functional area: **System**)

See the Domain: **Segmented Setup**. See the securable actions in this domain and the subdomains.

Domain Security Policies for Functional Area System

Description: Set up, maintain, and report on Business Processes, Report Writer, Scheduling, Security, Calendar, Landing Pages, Data Translation and other system-wide objects.

Status: Active

Report/Task	9 items	Security	Implementation
Create Ad Hoc Payment Spend Category Security Segment	Task	Modify	
Create Document Category Security Segment	Task	Modify	
Create Ledger Account Security Segment	Task	Modify	
Edit Ad Hoc Payment Spend Category Security Segment	Task	Modify	
Edit Document Category Security Segment	Task	Modify	
Edit Ledger Account Security Segment	Task	Modify	
View Ad Hoc Payment Spend Category Security Segment	Report (XpressO)	View	
View Document Category Security Segment	Report (XpressO)	View	
View Ledger Account Security Segment	Report (XpressO)	View	

## EXAMPLES OF SEGMENTED SECURITY

**1. Pay Component Security Segments** can be defined to control who has access to what components. In the training tenant, you can see this by running the **All Pay Components Security Segments** report. Review the screen captures below to see access provided to Benefits Administrator and Benefits Partners is to the Benefits Pay Component Visibility components (first graphic):

All Pay Components Security Segments [...]			
Pay Component Security Segment	Pay Components	Pay Component Security	
		Segment-Based Security Group	Security Groups Constraining Segment Group
Benefits Pay Component Visibility	401(k) [USA] 401(k) Catch-up [USA] 401(k) Employee Match [USA] 401(k) Roth [USA] Basic Life - Liberty Mutual - EE [USA] Basic Life - Liberty Mutual - ER [USA] Basic Life - Standard Life - EP [CAN] Canada Savings Bond Deduction [CAN] Canada Savings Bond Purchase Amount [CAN] Deferred Compensation [USA] More (18)	Benefits Pay Component Visibility	Benefits Administrator Benefits Partner

Employee Pay Components visible to Employees as Self (second graphic):

Pay Component Security Segment	Pay Components	Pay Component Security	
		Segment-Based Security Group	Security Groups Constraining Segment Group
Employee Pay Component Visibility	1042-S Wages [USA] 401(k) [USA] 401(k) Catch-up [USA] 401(k)-EE (P) 401(k) Employer Match [USA] 401(k)-ER (P) 401(k) Roth [USA] Additional Medicare Tax [USA] Additional Medicare Tip Tax [USA] AL - Alabama Security Assessment - Employee Paid [USA] More (39)	Employee Pay Component Visibility	Employee As Self

Manager Pay Components visible to Management Chain and Manager security groups (third graphic):

Pay Component Security Segment	Pay Components	Pay Component Security	
		Segment-Based Security Group	Security Groups Constraining Segment Group
Manager Pay Component Visibility	Base Pay Base Pay by Project Bonus Bonus - FLSA Eligible [USA] Call Out Pay - Minimum [USA] Car Allowance [USA] Cell / Mobile Allowance Commission Compensatory Hours Compensatory Time Paid [CAN] More (47)	Manager Pay Component Visibility	Management Chain Manager

**2. Procurement** - Only IT Department can purchase computer equipment

The screenshot shows the 'Create Requisition' screen. At the top, there's a blue callout pointing to the 'Create Requisition' button with the text 'Task available for'. Below the header, there's a 'Checkout' section with fields for 'Total Amount' (234.00), 'Currency' (USD), and 'Status' (Draft). Under 'Summary', there are fields for 'Company' (Global Modem Services, Inc. (USA)), 'Requester' (\* Logan McNeil), 'Ship-To Address' (\* 3939 The Embarcadero, San Francisco, CA), 'High Priority' (checkbox), and 'Create Ad Hoc Address' (checkbox). To the right, there's an 'Additional Information' section with 'Request Date' (02/13/2014) and 'Memo' fields. A large blue callout on the left points to the 'Goods Lines' tab with the text 'Available for all users to select'. The main table has columns for Image, Item, Item Description, \*Spend Category, Supplier, and \*Quantity. Two items are listed: 'GMS Logowear - Polo' (Item Description: GMS Polo Shirts, Spend Category: Marketing Collateral) and 'Dell E198WFP 19-inch Widescreen' (Item Description: Dell E198WFP 19-inch Widescreen, Spend Category: Computer Accessories). A blue callout on the right points to the 'Supplier' and 'Supplier Contract' fields with the text 'Available for only IT buyers to select'.

**3. Integration** - Workday provides Integration System Security Segments to enable you to apply finer control to who can do what with a given integration template, system, or entire category. Shown here only members of Finance Administrator security group has access to the segments indicated.

The screenshot shows the 'View Segment-Based Security Group' page for 'Finance Administrator - Integrations'. It includes fields for 'Name' (Finance Administrator - Integrations) and 'Context Type' (Constrained by Segment Access). Under 'Group Criteria', there's a 'Security Groups' field containing 'Finance Administrator' (highlighted in yellow). On the right, there's an 'Access Rights' section with 'Access to Segments' and a note: 'Templates: 1099 Templates: E103s' (also highlighted in yellow). Below this is a 'Domain Security Policy Permissions' table with 5 items:

Operation	Domain Security Policy	Functional Areas
View Only	Integration Reports	Integration
View and Modify	Integration Event	Integration
View Only	Integrations: EIBs	Integration
View Only	Integration Build	Integration
Get Only	Integration Process	Integration

## SEGMENT-BASED SECURITY STEPS

1. Create item security segments
2. Create Segment-based security groups
3. Edit Domain Security Policy to enable members to access restricted segment
4. Activate Pending Security Policy Changes
5. Test



## ACTIVITY 9 – CONFIGURE & DEPLOY SEGMENTED SECURITY

It has been determined that Executive Management should have access to the First Class Airfare Expense Item for use in expense reports. Non-executives should not be able to see the item when creating an expense report.

### OVERVIEW

Logan McNeil will perform the following actions:

1. Create Expense Item
2. Create Expense Item Security Segments
3. Create Segment-Based Security Groups
4. Edit domain security policy to enable members of the new expense item segment security groups to access expense items
5. Activate Pending Security Policy Changes
6. Test

### TASK 1: CREATE EXPENSE ITEM

#### ⌚ As Logan McNeil (lmcneil)

1. Search for '*exp item*'
2. Click on the **Create Expense Item** task
3. Enter '*1st Class Airfare*' in the Item Name field
4. Click on the Spend Category prompt and select **Travel & Entertainment**
5. Click the **OK** button to save

### TASK 2: CREATE EXPENSE ITEM SECURITY SEGMENTS

1. We can either add our new expense item to an existing expense item security segment or create a new one. We will create a new expense item security segment.
2. Search for '*cr exp sec*'

3. Click the **Create Expense Item Security Segment** task
4. Enter Name of **Restricted Executive Travel Expense Segment**
5. Click the Expense Item prompt  icon and select **By Alphabetical order >1st Class Airfare**
6. Click the **OK** button
7. Click the **Done** button

### TASK 3: CREATE SEGMENT-BASED SECURITY GROUP

1. We can either add our new expense item security segment to an existing segmented based security group, or create a new one. We will create a new segmented security group.
2. From the search box, run the task **Create Security Group**
3. Select Type of Tenanted Security Group **Segment-Based Security Group**
4. Enter the Name **Executive Travel**
5. Click **OK**
6. Edit the Segment-Based Security Group as follows:

<b>Field Name</b>	<b>Entry Value</b>
Security Groups > All Security Groups	Chief Executive Officer Chief Financial Officer Chief Human Resources Officer Chief Information Officer Chief Operating Officer
Access to Segments	Expense Item Security Segment -> Restricted Executive Travel Expense Segment

7. Click the **OK** button
8. Click the **Done** button

## TASK 4: EDIT THE DOMAIN SECURITY POLICY DEFINITION



**Note:** The security group does not need to be added to the Business Process Security Policy for creating an expense report (bp: Expense Report Event) since we already have the needed access to the task. We are restricting what *values* they can see within that task so we must configure access to a domain that allows access to segmented expense items.

1. Search for 'dom sec fun'
2. Click on **Domain Security Policies for Functional Area** report
3. Select the functional area: **Expenses**
4. Click the **OK** button
5. In the left frame, select the domain **Access Expenses Item (Segmented)**
6. In the right frame domain security policy, click the **Edit Permissions** button

Domain Security Policies for Functional Area **Expenses** ... ...

Description	Set up self-service payment elections, travel profiles, spend authorization, and expense reporting for both employees and contingent workers. Administer expense items, attributes, rate tables, rules and expense travel profiles, prenote processing, and expense report tasks. Configure rules for capturing recoverable tax based on country and expense item. Set up, report, and process travel booking records. View and analyze spend across your organization and analyze expense reporting compliance.																
Status	Active																
<span style="border: 1px solid #ccc; padding: 2px;">Access Expense Item (Segmented)</span> <span style="border: 1px solid #ccc; padding: 2px;">Manage: Expense Report</span> <span style="border: 1px solid #ccc; padding: 2px;">Manage: Expense Report for Pre-H...</span> <span style="border: 1px solid #ccc; padding: 2px;">Manage: Payment Election</span> <span style="border: 1px solid #ccc; padding: 2px;">Manage: Spend Authorization</span> <span style="border: 1px solid #ccc; padding: 2px;">Print: Expense Report</span> <span style="border: 1px solid #ccc; padding: 2px;">Process: Expense Report Payment...</span> <span style="border: 1px solid #ccc; padding: 2px;">Process: Spend Control and Analy...</span> <span style="border: 1px solid #ccc; padding: 2px;">Process: Travel Booking</span> <span style="border: 1px solid #ccc; padding: 2px;">Reports: Expense Report Payment</span> <span style="border: 1px solid #ccc; padding: 2px;">Self-Service: Expense Report</span> <span style="border: 1px solid #ccc; padding: 2px;">Self-Service: Payment Election</span> <span style="border: 1px solid #ccc; padding: 2px;">Self-Service: Spend Authorization</span>	<b>Domain Security Policy</b> Status: Active Allowed Security Group Types: <b>Public Groups</b> , Segment - Expense Item, Unconstrained Groups  Securable Actions: 5  Report/Task Permissions <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 80%;">Security Groups</th> <th style="width: 10%;">View</th> <th style="width: 10%;">Modify</th> </tr> </thead> <tbody> <tr> <td>Finance Auditor</td> <td>Yes</td> <td></td> </tr> <tr> <td>Restricted Expense Items / Sales &amp; Services</td> <td></td> <td></td> </tr> <tr> <td><b>Sweden - Expenses</b> <span style="border: 1px solid #ccc; padding: 2px;">...</span></td> <td></td> <td></td> </tr> <tr> <td>Unrestricted Expense Items / All Employees</td> <td></td> <td></td> </tr> </tbody> </table>	Security Groups	View	Modify	Finance Auditor	Yes		Restricted Expense Items / Sales & Services			<b>Sweden - Expenses</b> <span style="border: 1px solid #ccc; padding: 2px;">...</span>			Unrestricted Expense Items / All Employees			<span style="border: 1px solid #ccc; padding: 2px;">Edit Permissions</span>
Security Groups	View	Modify															
Finance Auditor	Yes																
Restricted Expense Items / Sales & Services																	
<b>Sweden - Expenses</b> <span style="border: 1px solid #ccc; padding: 2px;">...</span>																	
Unrestricted Expense Items / All Employees																	

7. Under Report/Task Permissions, click the prompt icon in the row with **View** permissions.
8. Include the **Executive Travel** security group (note the unrestricted group)
9. Click the **OK** button to save
10. Click the **Done** button

## TASK 5: ACTIVATE PENDING SECURITY POLICY CHANGES

1. Search for '*Activate*'
2. Click the **Activate Pending Security Policy Changes** task
3. Enter '*Activity 9*' into the comments section
4. Click the **OK** button
5. Click the **Confirm** checkbox
6. Click the **OK** button to activate the changes

## TASK 6: TEST SECURITY POLICY CHANGES

1. As Logan, search for '*cr exp rep*'
2. Click the **Create Expense Report** task
3. Click the **OK** button to Create a New Expense Report
4. Click the **Expense Item**  prompt icon
5. Select **By Alphabetical Order** folder
6. Notice the option to select *1st Class Airfare* since Logan is a member of the **Chief Human Resources officer** job-based security group that has access to the segment that secures this expense item.
7. **Cancel**
8. **Start Proxy as Jared Ellis (jellis)**
9. Search for '*cr exp rep*'
10. Click the **Create Expense Report** task
11. Click the **OK** button to create a new expense report.
12. Click the **Expense Item**  icon - Select **By Alphabetical Order**
13. Notice there is no option to select *1st Class Airfare* since Jared is not a member of Executive Travel security group
14. **Cancel** the expense report
15. **Stop proxy**

## TASK 6 - OPTIONAL

*As Logan (be sure to stop proxy if still proxied as Jared)*

1. View other expense security segments in tenant: run **View Expense Item Security Segments**
2. View other segmented security groups around expenses in tenant: Run **View Security Group**

3. See how the existing segmented security groups give access to the existing segments. We could have added our new expense item to an existing segment, or added our new segment to an existing security group.

Domain Security Policy Permissions			
Operation	Domain Security Policy	Domain Security Policies Inheriting Permission	Functional Areas
View Only	Access Expense Item (Segmented)		Expenses

4. View what areas of Workday you can segment.
  - a. Run: Domain Security Policies for Functional Area, Area=System
  - b. Find **domain: Segmented Setup**
  - c. Note the securable actions in this domain and the subdomains.

Domain Security Policies for Functional Area **System**  

Description Set up, maintain, and report on Business Processes, Report Writer, Scheduling, Security, Calendar, Landing Pages, Data Translation and other system-wide objects.

Status Active

**Security Administration**

- Segmented Setup**
- Cash Management Segment Setup
- Compensation Segmented Setup
- Customer Segmented Setup
- Document Categories Segmented Setup
- Expenses Segmented Setup
- Investor Segmented Setup
- Ledger Account Segmented Setup
- Procurement Segmented Setup
- Questionnaire Segmented Setup
- Self-Service: Account
- Self-Service: Activity Stream
- Self-Service: Manage Authorized Applications
- Self-Service: Mobile Notifications
- Self-Service: Service Center Representative

Domain Security Policy **Segmented Setup**

Status Active

Securable Actions **9**

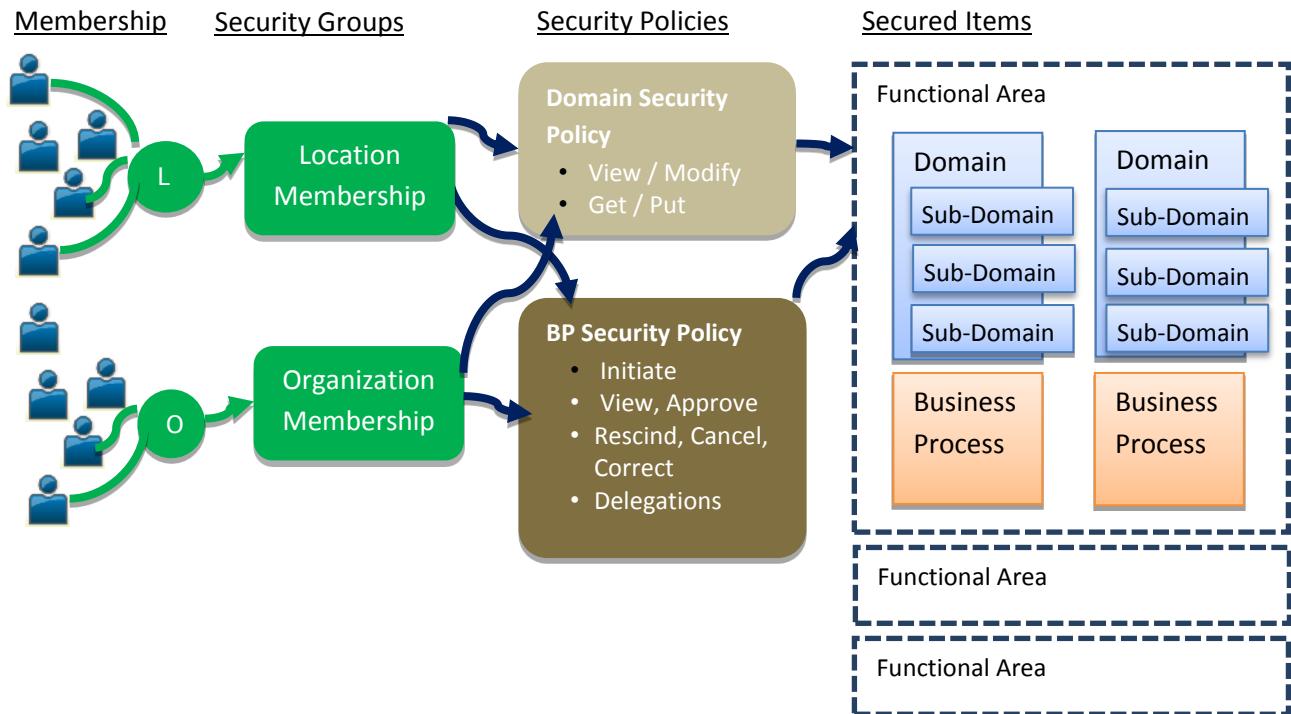
Name	Type	Permission Required
Create Ad Hoc Payment Spend Category Security Segment	Task	Modify
Create Document Category Security Segment	Task	Modify
Create Ledger Account Security Segment	Task	Modify
Edit Ad Hoc Payment Spend Category Security Segment	Task	Modify
Edit Document Category Security Segment	Task	Modify
Edit Ledger Account Security Segment	Task	Modify
View Ad Hoc Payment Spend Category Security Segment	Report (XpressO)	View
View Document Category Security Segment	Report (XpressO)	View
View Ledger Account Security Segment	Report (XpressO)	View

(End of Activity)

## LOCATION MEMBERSHIP AND ORGANIZATION MEMBERSHIP GROUPS

There are two types of security groups that are based on membership: Location Membership and Organization Membership. These are similar to job-based security groups in that the membership groups are *automatically* populated based on criteria.

Membership security groups are commonly used in Aggregation and/or Intersection security groups.



## LOCATION MEMBERSHIP SECURITY GROUP

You can define a location-based security group to include one or more Locations. Workers are granted access to items in a policy secured with a location-based security group if they are in any of the Locations included in the group. This is not a context-sensitive security group. Location Based security groups are **unconstrained**. Workday does not attempt to match the workers location to the location of the secured item. Membership in location based security groups is automatically assigned based on a worker's location.

Examples of Location Membership-Based Security Groups:

- Workers in Amsterdam location
- Workers in US locations
- Workers in San Francisco location

View Location Membership Security Group <a href="#">San Francisco - All Workers</a>	
Name	San Francisco - All Workers
Comment	San Francisco - All Workers
Context Type	Unconstrained
Locations	<a href="#">San Francisco</a>

## ORGANIZATION MEMBERSHIP SECURITY GROUP

You can define an organization-based security group to include one or more organizations of any type (e.g. Company, Cost Center, Location Hierarchy, Pay Group). You can optionally include subordinate organizations. Workers are granted access to items in a policy secured with an organization-based security group if they are in any of the organizations included in the group. This is not a context-sensitive security group. Organization membership security groups are **unconstrained**. Workday does not attempt to match the workers organization to the organization of the secured item. Membership in organization membership security groups is automatically assigned based on a worker's organization assignments.

Examples of Organization Membership-Based Security Groups:

- Workers in Cost Center: IT Services
- Workers in Pay Group: Administrative Weekly
- Workers in Company: Global Modern Services AB (Sweden)

View Organization Membership Security Group <a href="#">Sweden</a>	
Name	Sweden
Context Type	Unconstrained
Organizations	<a href="#">Global Modern Services AB (Sweden)</a>
<input checked="" type="radio"/> Applies to Current Organization Only <input type="radio"/> Applies to Current Organization And All Subordinate Organizations	
Available Actions	Company <a href="#">Global Modern Services AB (Sweden)</a>



## ACTIVITY 10 – CREATE MEMBERSHIP BASED (LOCATION AND ORGANIZATION) SECURITY GROUPS

Only US employees should be able to request time off in Workday. This will be a multi-part activity. First we'll need to create a location membership security group for US Locations. We will also create an organization membership security group to leverage location hierarchies. This is the first of a 2-part activity.

### OVERVIEW

Logan McNeil will perform the following actions:

1. View existing security
2. Create Security Group

### TASK 1: VERIFY EXISTING SECURITY

1. **Start Proxy as Benjamin Green (bgreen)**
2. Note the **Time off** Worklet on Benjamin's home page and note how from the search box, he has access to the **Request Time Off** task

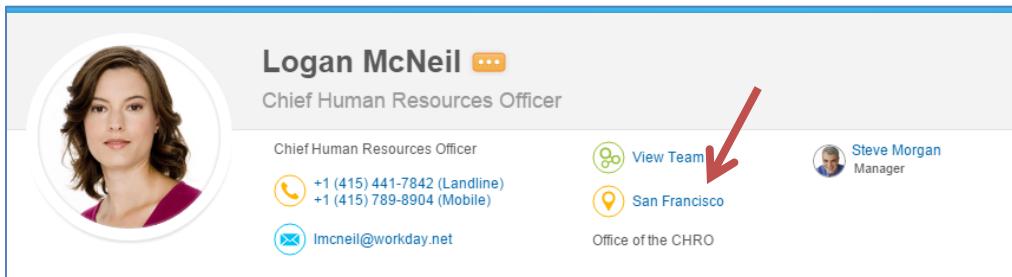
3. Click Benjamin's picture in the upper right, and select **View Profile**
4. Notice that his Location is London, UK.
5. **Stop proxy**

### TASK 2: CREATE SECURITY GROUP

↻ **As Logan (lmcneil)**

1. Search for '*cr sec gr*'

2. Click the **Create Security Group** task
3. Select **Location Membership Security Group** as the Type of Tenanted Security Group
4. Enter the Name **All US Locations**
5. Click the **OK** button
6. Click on the Locations prompt  icon to include the following **Active Locations**.
  - Atlanta
  - Berwyn
  - Boston
  - Chicago
  - Dallas
  - Las Vegas
  - New York
  - San Francisco
7. Click the **OK** button
8. Click the **Done** button
9. From the search box, run **View Security Groups for User**
10. Choose person: **lmcneil / Logan McNeil (Workday Account)**
11. Click OK.
12. Notice that Logan is in the All US Locations security group. Why? Because Logan's location is San Francisco.



The image shows a Workday employee profile card for Logan McNeil. The card has a blue header bar with her name and title. Below the header, there is a circular profile picture of Logan. To the right of the picture, her title is listed as "Chief Human Resources Officer". Underneath her title, there are several contact details: a phone icon followed by "+1 (415) 441-7842 (Landline)" and "+1 (415) 789-8904 (Mobile)". There is also an email icon followed by "lmcneil@workday.net". On the right side of the card, there is a "View Team" button with a green icon and a "San Francisco" location entry with an orange location pin icon. A red arrow points from the text in step 12 to the "San Francisco" location entry. At the bottom right of the card, there is a "Steve Morgan Manager" entry with a blue icon.

13. Search for '*ben green*'
14. Using the related action for employee Benjamin Green, select **Security Profile -> View Security Groups**

The screenshot shows a user profile for Benjamin Green, a Regional Sales Manager Employee. The sidebar menu includes options like Recruiting, Reports, Safety Incident, Talent, Time and Leave, Workday Account, Worker History, Audits, Favorite, Integration IDs, Preferences, Reporting, Security Profile, View Workday Account, Assign Roles, Assign User-Based Groups, Edit Workday Account, Manage Workday Account Credentials, Start Proxy, View Custom Reports, View Role Assignments, View Security Groups, Security History for User, View Signon History, View Support Roles, and View Update Audit.

15. Notice that he is not a part of the All US Locations security group. Why? Benjamin Green is in London.

## TASK 2- CREATE AN ORGANIZATION MEMBERSHIP SECURITY GROUP FOR USA

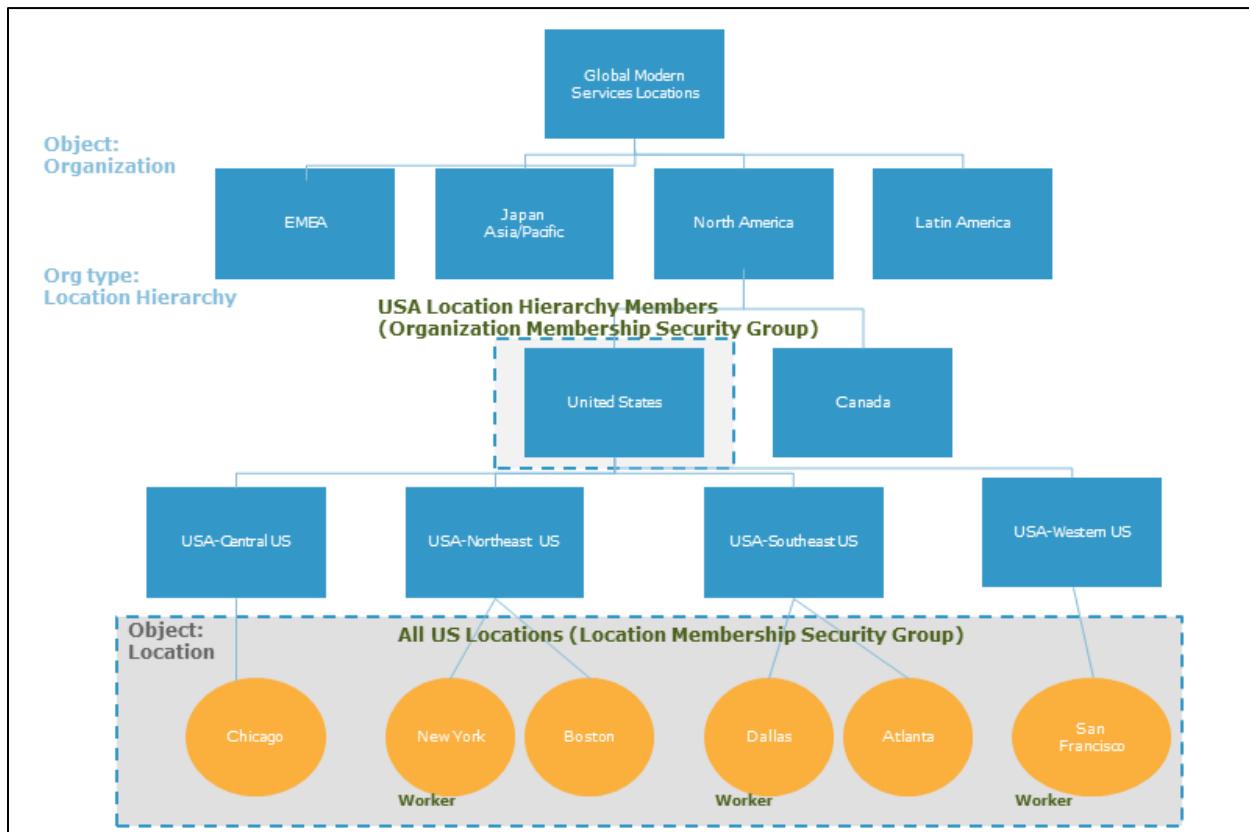
- From the search box, run the task: **Create Security Group**
- Select **Organization Membership Security Group** as the Type of Tenanted Security Group
- Enter the Name **USA Location Hierarchy Members**
- Click the **OK** button
- Click on the Organizations prompt icon. Select **All Organizations by Type > Location Hierarchy > Global Modern Services Locations** and select **United States**.
- Select **Applies to Current Organization and All Subordinates**.

The dialog shows the following fields:

- Name: USA Location Hierarchy Members
- Comment: (empty)
- Context Type: Unconstrained
- Inactive:
- Organizations: United States
- Applies to Current Organization Only:
- Applies to Current Organization And All Subordinates:

A dropdown menu for 'Organizations' is open, showing a search bar and a list of locations under 'Top > All Organizations by Type > Location Hierarchy > Global Modern Services Locations'. The 'United States' option is selected.

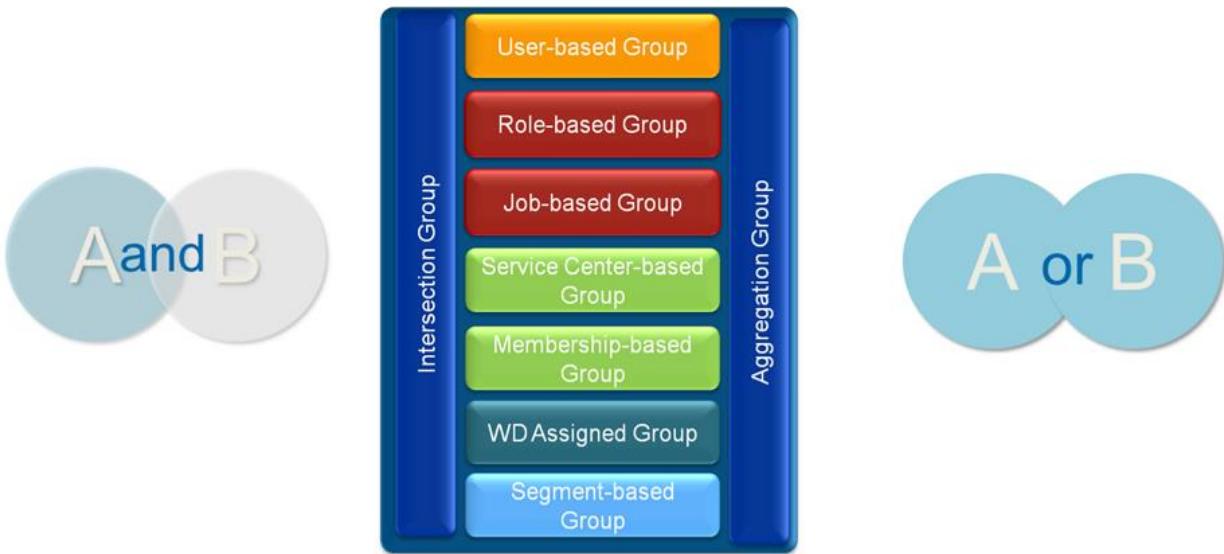
7. Click the **OK** button
8. Click the **Done** button
9. Is there a benefit gained using an **Organization Membership** security group based on a Location Hierarchy **vs.** our **Location membership** security group? Organization Membership security groups based on Location Hierarchy are more commonly used and easier to maintain.



(End of Activity)

## COMBINATIONS OF SECURITY GROUPS

Workday provides two types of security groups: **Intersection** and **Aggregation**, where you can combine security groups to meet security configuration needs. Combinations of security groups are made up of one or more security groups. You can also filter out, or exclude, one or more security groups from the resulting membership, as well as exclude target instances to support the ability to hide data that a member would have otherwise seen.

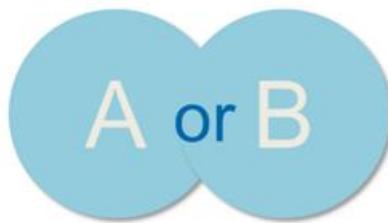


Note: You cannot intersect an intersection security group. You cannot aggregate an aggregation security group. You can however, aggregate an intersection, or intersect an aggregation.

## AGGREGATION SECURITY GROUP

To define an aggregation security group, you simply pick which security groups you want to include. The aggregation security group includes users who are in **ANY** of the selected security groups. That is, one does not have to be in every included group; being in any one group is sufficient.

- Includes users are those in **any** of the selected security groups ("OR" Statement)
- User does not have to be in every included group
  - Can use exclusion logic
- Very useful to **ease maintenance** when you have several security groups with common access
- Constraint – mixed –depends on what's being aggregated
- Restriction:** Cannot aggregate other aggregation security groups.
- You can aggregate intersection security groups.

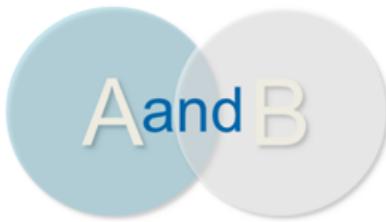


View Aggregation Security Group [Workbench Group](#) ... | [e](#)

Name	Workbench Group
Context Type	Mixed
Security Groups to Include	<a href="#">Business Process Administrator</a> <a href="#">Finance Integration Administrator</a> <a href="#">HR Integration Administrator</a> <a href="#">Integration Administrator</a> <a href="#">Payroll Integration Administrator</a> <a href="#">Security Administrator</a> <a href="#">Security Configurator</a> <a href="#">Setup Administrator</a> <a href="#">System Auditor</a>
Security Group to Exclude	<a href="#">Non-Workbench User</a>

## INTERSECTION SECURITY GROUPS

The intersection security group includes only users who meet **all** of the specifications. They must qualify for **ALL** of the security groups without exception. Both this group and the aggregation group can use exclusion logic as well. You can intersect two or more security groups.



- Grants access based on membership in **all** of the included security groups
- Includes only users who meet all of the specifications . Constraints are also intersected.
- Constraint – Mixed –depends on security groups intersected
- **Restriction – cannot intersect other intersection security groups.**
- You can intersect aggregation security groups

Example: Offer self service PTO to exempt employees in Canada. This configuration uses Employee as Self + Canada Location + Job based (Exempt) security groups. In the diagram below, ***only the small area where all three groups meet will get the security access.***



## COMMON USE CASES FOR INTERSECTION SECURITY:

1. **Limiting self service** or certain functionality to only employees in certain regions or locations (vs. All Employees or any Employee-as-self)
2. **Intersecting role-based security groups constrained and enabled for different organization types.** e.g. Constrain access to workers in a given supervisory organization that are also in a given Location hierarchy (e.g. Canadian Workers in Sales Organization)
3. **Hiding populations** – excluding target instances - that you would have otherwise seen (e.g. to meet FERPA regulations, Hide HR from HR, Hide sensitive workers)

## COMMON USE CASE #1 – LIMITING SELF SERVICE TO CERTAIN POPULATIONS

For **ESS (Employee-self-service) scenarios where you need to limit the population access** to say, self-service benefits or time off and leave, you can use intersection security groups to only identify certain employees, while still constraining them to their own data (self service).

Examples:

- Only those in the US can do Benefits ESS
- Only those in EMEA can Add Dependents

### High Level Steps:

- 1) Identify the needed population with a security group. Typically this is done using the **Organization Membership** (or Location Membership) if populations are location specific.
- 2) **Create an intersection security group** that intersects the organization membership security group with the **employee-as-self** security group.
- 3) **Replace all needed domain and business process security policies** with the intersection security group instead of employee-as-self (remove employee-as-self).
- 4) **Activate & Test! Test! Test!**



**Important:** If using intersection security groups, be sure to **add** the intersection security group in needed domain or business process security policies, and **remove** references to the security groups that are being used in the intersection.



## ACTIVITY 11A – CREATE AN INTERSECTION SECURITY GROUP

In the last activity, we created a Location Membership Security Group called All US Locations. Next, we will use that group to create an Intersection Security Group and update the Request Time Off business process to ensure only US based employees can request time off in Workday. All international employees will submit time off requests outside of Workday.

### OVERVIEW

Logan McNeil will perform the following actions:

1. Create Security Group
2. Edit Domain and Business Process Security Policies
3. Activate security changes
4. Test

### TASK 1: CREATE THE INTERSECTION SECURITY GROUP

#### As Logan McNeil (lmcneil)

1. Search for '*cr sec gr*'
2. Click the **Create Security Group** task
3. Select **Intersection Security Group** as the Type of Tenanted Security Group
4. Enter the Name *US Employee-as-self*
5. Click the **OK** button
6. Click on the prompt icon to define the following as **Security Groups to Include**
  - **USA Location Hierarchy Members** (*you can use your location or organization membership security group from the last activity. Common practice is to use organization membership.*)
  - **Employee as Self**

**Intersection Criteria**

Security Groups to Include \*

search	edit
<input checked="" type="checkbox"/> Employee As Self	
<input checked="" type="checkbox"/> USA Location Hierarchy Members	

7. Click the **OK** button
8. Click the **Done** button

## TASK 2 - NOW, LET'S IDENTIFY ALL THE **NEEDED SECURITY POLICIES TO EDIT** WITH THIS NEW INTERSECTION SECURITY GROUP INSTEAD OF EMPLOYEE-AS-SELF.

1. From the search box, run: **Domain Security Policies for Functional Area**
  - a. Functional Area: **Time off and leave**
  - b. Click OK

**Domain Security Policies for Functional Area**

Functional Area \* **Time Off and Leave**

2. In the left frame, find the Domain: Self Service Time off

<ul style="list-style-type: none"> <li><input type="checkbox"/> Process: Calculated Balances           <ul style="list-style-type: none"> <li><input type="checkbox"/> Process: Calculated Balances ...</li> <li><input type="checkbox"/> Process: Calculated Balances ...</li> </ul> </li> <li><input type="checkbox"/> Process: Delete Accrual and Time O...         </li> <li><input type="checkbox"/> Process: Enter or Correct Time</li> <li><input type="checkbox"/> Self-Service: Leave of Absence</li> <li><input type="checkbox"/> Self-Service: Time Off</li> <li><input type="checkbox"/> Self-Service: Worklets: Time O...         </li> <li><input type="checkbox"/> Self-Service: Time Off Balances</li> <li><input type="checkbox"/> Set Up: Leave of Absence</li> </ul>	<p><b>Domain Security Policy</b>    <a href="#">Self-Service: Time Off</a></p> <p>Status Active</p> <p>Securable Actions 13</p> <p>Securable Reporting Items 3</p> <p><b>Report/Task Permissions</b></p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Security Groups</th> <th>View</th> <th>Modify</th> </tr> </thead> <tbody> <tr> <td>Employee As Self</td> <td>Yes</td> <td>Yes</td> </tr> </tbody> </table> <p><a href="#">Edit Permissions</a></p>	Security Groups	View	Modify	Employee As Self	Yes	Yes
Security Groups	View	Modify					
Employee As Self	Yes	Yes					

3. See how the current access is for employee-as-self.
4. Click on **Edit permissions**
  - a. **Remove** the employee-as-self security group
  - b. **Add** your intersection security group: US Employee-As-Self
  - c. **When adding your intersection security group, it is very important to remove the security group that is included in your intersection security group.**

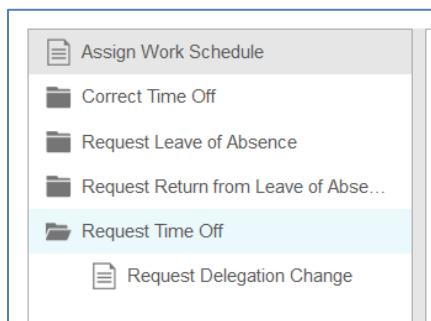
Report/Task Permissions		View	Modify
<input data-bbox="225 206 257 236" type="button" value="+"/>	*Security Groups		
<input data-bbox="225 249 257 278" type="button" value="-"/>	search x US Employee-as-self	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

5. Click **OK** to save and **Done**.
6. Now let's check business process security policies for Time off and Leave
7. From the search box, run: *Business Process Security Policies for Functional Area*
8. Select functional area: Time off and leave

**Business Process Security Policies for Functional Area**

Functional Area	<input type="text" value="Time Off and Leave"/> <input type="button" value="edit"/>
Business Process	<input type="text" value="search"/> <input type="button" value="edit"/>

9. Click OK
10. In the left frame, note the business process types we should consider for our limited self-service access. For purposes of this activity, we will only configure the 'Request time off' business process with our intersection security group, recognizing the other business process types that would also need to be modified in an implementation. Select **Request Time off** in the left frame.



11. Scroll to the bottom of the security policy on the right and click on **Edit Permissions**
12. Under the *Who can start this business process* section, find the places where **employee-as-self** has access to initiate and replace with your intersection security group: **US Employee-As-Self** (There should be 3 replacements made.)

Initiating Action Request Time Off

Description Request Time Off by a worker using a self service link in Time Off and Leave worklet using the Workday system

Security Groups    
X US Employee-as-self

Security Groups who can delegate this action to others    
X US Employee-as-self

Initiating Action Request Time Off

Description Request Time Off by a worker using a related action off the worker using the Workday system

Security Groups    
X US Employee-as-self

13. Scroll down in the security policy, to the *Who can do actions on entire business process* and under the *View All action*,

- a. Remove the **employee-as-self**, security group
- b. Replace with **US Employee As Self**

Action	View All
Security Groups	<input type="text" value="search"/> <input type="button" value="refresh"/> <ul style="list-style-type: none"> <li>X US Employee-as-self</li> <li>X Absence Administrator</li> <li>X Absence Partner</li> <li>X Alternate Approver</li> <li>X Benefits Administrator</li> <li>X Benefits Partner</li> <li>X HR Administrator</li> <li>X HR Analyst</li> <li>X HR Auditor</li> <li>X HR Executive</li> </ul> <p><a href="#">More (11)</a></p>

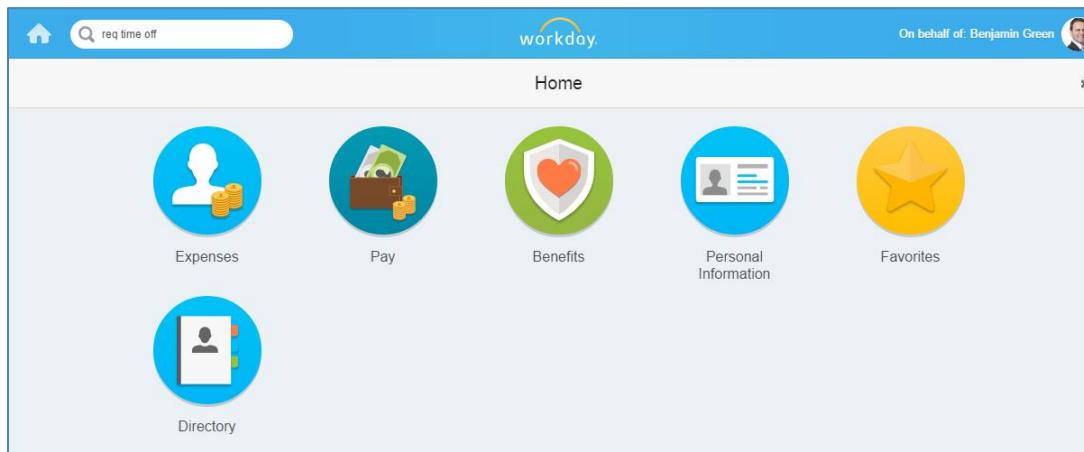
14. Click **OK** to save the change and **Done**.

15. Now we have edited one self-service domain and one business process security policies. Now let's activate the security changes and test.

### TASK 3– ACTIVATE AND TEST

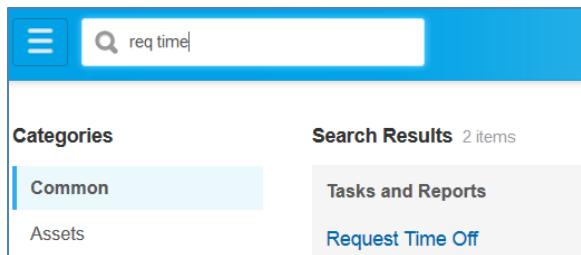
1. From the search box, run **Activate Pending Security Policy Changes**
2. Enter a comment, such as: "Activity 11A"
3. Click OK to save

4. Confirm the domain and business process security policies with edits to be activated
5. Click **OK**.
6. **Start proxy** as Benjamin Green
  - a. Remember that Benjamin is in the UK, not in the USA.
  - b. See how Benjamin no longer has the **Time off** Worklet on his home page.
  - c. From the search box ,try running the task: **Request time off**
  - d. See how Benjamin no longer has access to this task.



## 7. **Stop Proxy**

8. As Logan, see how Logan still has access to the task: Request time off and she also has the Time off Worklet on her home page.



## CONCLUSION

- Intersection security groups can be useful in limiting self-service functionality, by intersecting a security group that identifies the population (typically an organization membership security group type), with the employee-as-self security group.

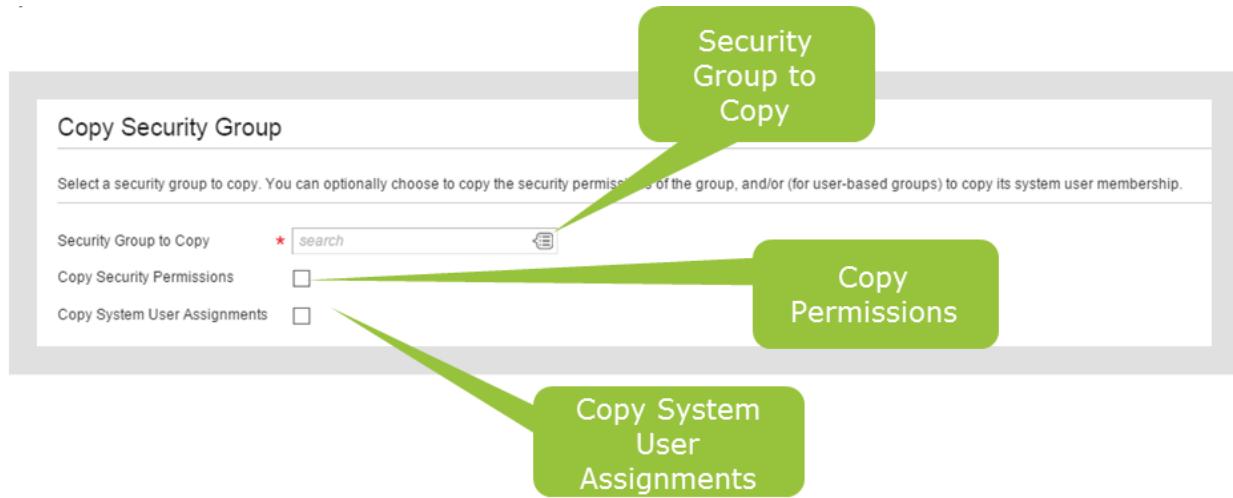
- Use the *Domain Security Policies for Functional Area* and the *Business Process Security Policies for Functional Area* to assess the needed security policy implications and replacements when using intersection security.
- Be sure to remove the employee-as-self security group and replace with the intersection security group to configure the needed intersecting access.

(End of Activity)

## COPY SECURITY GROUPS

In addition to creating, deleting, and editing security groups, you can also copy existing security groups to simplify security maintenance.

Use the **Copy Security Group** task to select the existing group to copy. You can optionally copy security permissions to add new security group to all domain security policies and business process security policies where the existing group is used. The addition of the new group to all the security policies that specified the copied group becomes a pending security change. The new group is copied to the policies where the copied group appears regardless of whether the copied group's association with a policy is currently active or itself a pending change. Another option includes the ability to copy users of the existing group for User-Based Security groups.





## ACTIVITY 11B – OPTIONAL - CONFIGURE INTERSECTION WITH EXCLUSION IN MEMBERSHIP

Next, copy the Only US Employees Intersection Security Group to create a new security group that excludes US employees in San Francisco as members. All San Francisco employees will need to submit time off requests outside of Workday as well as international employees.

### TASK 1: COPY SECURITY GROUP

#### ⌚ As Logan McNeil (lmcneil)

1. Search for 'copy sec gr'
2. Click the **Copy Security Group** task
3. Select **Intersection Security Group > US Employee-as-self** as the Security Group to copy
4. Check the box to **Copy Security Permissions**

**Copy Security Group**

Select a security group to copy. You can optionally choose to copy the security p

Security Group to Copy \*

Copy Security Permissions

Copy System User Assignments

5. Click OK.
6. Change the Name to **US Employee-as-self Except San Francisco**
7. Click on the  icon Security Groups to Exclude and select **All Security Groups > San Francisco – All Workers**

Name	* <input type="text" value="US Employee-as-self Except San Fran"/>
Comment	<input type="text"/>
Context Type	Mixed (Subset)
Inactive	<input type="checkbox"/>
<b>Intersection Criteria</b>	
Security Groups to Include *	<input type="text" value="search"/> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Employee As Self</li> <li><input checked="" type="checkbox"/> USA Location Hierarchy Members</li> </ul>
Security Group to Exclude	<input type="text" value="San Francisco - All Workers"/>

8. Click **OK**, then click **Done**

## TASK 2: EDIT THE BUSINESS PROCESS SECURITY POLICY

1. Search for 'bp: time off'
2. Click on the related action icon for **Request Time Off**, select **Business Process Policy -> Edit**
3. Locate the *Who Can Start the Business Process* section. In the Request Time Off sections, click on the **X** to remove the **US Employee-as-self** security group. Notice the **US Employee-as-self Except San Francisco** security group you just created is there. Why?

Initiating Action Request Time Off

Description Request Time Off by a worker using a self service link in Time Off

Security Groups

search	<input type="checkbox"/> US Employee-as-self Except San Francisco
--------	---

Security Groups who can delegate this action to others

search	<input type="checkbox"/> US Employee-as-self Except San Francisco
--------	---

Initiating Action Request Time Off

Description Request Time Off by a worker using a related action off the worker using the Workday system

Security Groups

search	<input type="checkbox"/> US Employee-as-self Except San Francisco
--------	---

Activate your security policy changes using the  
 Activate Pending Security Policy Changes task,  
 and update the security evaluation moment which

4. Still editing the bp security policy, scroll down to the *Who can take actions on entire business process* "View All" section. Remove the US Employee-as-self and leave your copied security group permissions.

**Who Can Do Actions on Entire Business Process**

Action	View All
Security Groups	<input type="text" value="search"/> <input type="button" value="..."/> <ul style="list-style-type: none"> <li>✗ Absence Administrator</li> <li>✗ Absence Partner</li> <li>✗ Alternate Approver</li> <li>✗ Benefits Administrator</li> <li>✗ Benefits Partner</li> <li>✗ HR Administrator</li> <li>✗ HR Analyst</li> <li>✗ HR Auditor</li> <li>✗ HR Executive</li> <li>✗ HR Partner</li> <li>✗ HR Partner (By Location)</li> <li>✗ Implementers</li> <li>✗ Information Administrator</li> <li>✗ Management Chain</li> <li>✗ Manager</li> <li>✗ Manager's Manager</li> <li>✗ Payroll Administrator</li> <li>✗ Payroll Interface Administrator</li> <li>✗ Payroll Interface Partner</li> <li>✗ Payroll Partner</li> <li>✗ Time and Leave System</li> <li>✗ US Employee-as-self Except San Francisco</li> </ul> <p><input type="button" value="Less (12)"/></p>

Activ  
Activ  
and  
is cu

5. Click the **OK** button
6. Click the **Done** button
7. From the search box enter **domain: self service time off**
8. Using related actions, select **Domain > Edit Security Policy Permissions**

domain: self service time off

workday

Search Results 3 items

All of Workday

Self-Service: Time Off Domain

Self-Service: Time Off Balance Domain

Available Actions

Domain Self-Service: Time Off

Domain Audits

Edit Security Policy Permissions

View Security Policy

9. Remove the US Employee-as-self security group and leave your copy.

Report/Task Permissions

*Security Groups	View	Modify
<input type="text" value="search"/> <input type="button" value="..."/> <ul style="list-style-type: none"> <li>✗ US Employee-as-self Except San Francisco</li> </ul>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

10. Click OK and Done.

### TASK 3: ACTIVATE THE SECURITY CHANGES

1. Search for '*activate*'
2. Click on the **Activate Pending Security Policy Changes** task
3. Enter the comment *Activity 11B*
4. Click the **OK** button
5. Click the **Confirm** checkbox
6. Click **OK**

### TASK 4: TEST THE SECURITY CHANGES

1. Search for '*req time*' - notice that Logan can no longer request time off from the search box.
2. **Start Proxy as Jeff Gordon (jgordon)**
3. Click the Time Off icon on his Home page
4. Notice that Jeff does have access to the Request Time Off task.
5. Why? Take a look at Jeff Gordon's worker profile. (Click on his picture in the upper right and then click **View Profile**.) He is located in Dallas. We only excluded employees from the San Francisco location.

The screenshot shows a worker profile for Jeff Gordon. At the top, there is a search bar with the query 'req time off' and a button labeled 'Request Time Off - Task'. Below the search bar is a large circular profile picture of Jeff Gordon, followed by his name 'Jeff Gordon' and a three-dot menu icon. Underneath his name, it says 'IT HelpDesk Specialist'. To the right of his name are two buttons: 'View Team' with a globe icon and 'Dallas' with a location pin icon. At the bottom of the profile card, there are icons for phone (+1 (972) 533-9898 (Landline)), email (jgordon@workday.net), and another 'View Team' button.

6. **Stop proxy**

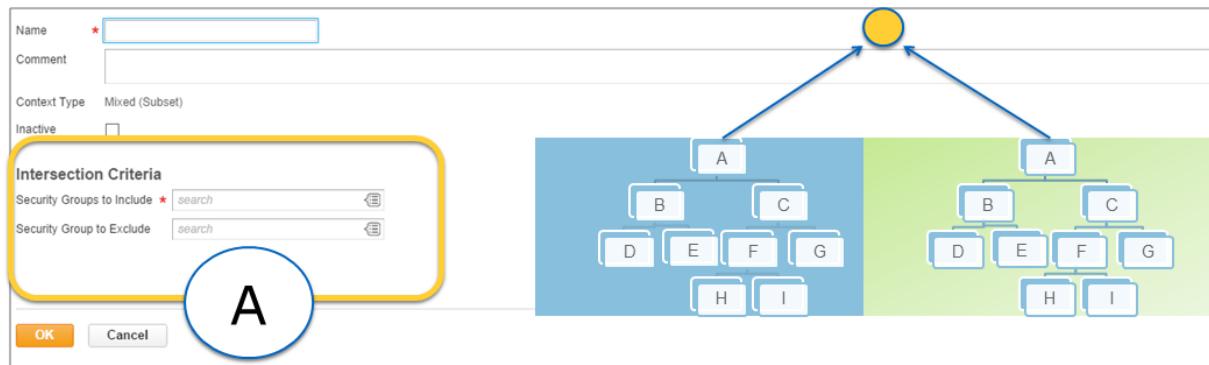
(End of Activity)

## COMMON USE CASE #2 - INTERSECTING ROLE-BASED CONSTRAINTS

Intersection security groups can also be useful when you need to 'intersect' role-based constraints for roles enabled for different organization types.

For example, you can assign a **Compensation Partner** role to a supervisory organization, say, Sales, and then assign a **Compensation Partner (by location)** role to a location hierarchy, say, North America. You can then intersect these 2 role-based constrained security groups, where the resulting constraint will be: *Workers in the Sales supervisory organization that are also in North America.*

### A – include security groups to intersect and determine members and constraints



View Intersection Security Group <a href="#">Compensation partner by Supervisory and Location Hierarchy</a> ...	
Name	Compensation partner by Supervisory and Location Hierarchy
Comment	intersect 2 role-based constrained security groups: Compensation partner (supervisory org/role: Comp Partner) and Compensation partner by location (location hierarchy/role: Comp Partner by Location). Members will those in both sec groups and constraints will be targets in both.
Context Type	Mixed (Subset)
<b>Intersection Criteria</b>	
Security Groups to Include	<input type="checkbox"/> Compensation Partner <input type="checkbox"/> Compensation Partner (by Location)
Security Group to Exclude	(empty)
<b>Exclusion Criteria (Constrained Context)</b>	
Exclude Target Position in Organization (empty)	
<input type="radio"/> Applies to Current Organization Only <input type="radio"/> Applies to Current Organization And All Subordinates	

### High Level Steps:

- 1) Roles must exist, for example: **Compensation Partner** enabled for Supervisory and **Compensation Partner by Location** enabled for Location Hierarchy
- 2) Roles must be assigned. Assign the same position to both roles.
- 3) Create role-based constrained security groups for each role.
- 4) Create intersection security group that intersects both role-based constrained security groups
- 5) Configure needed domains or business process security policies with the intersection security group.  
Remove references to the role-based constrained security groups if in those policies.

Another example. Here we are intersecting 2 role-based constrained sec groups: **Business Site Buyer** and **Spend category buyer**. Our intersection security group will identify: Those assigned to both roles: Business Site Buyer and Spend Category Buyer and will constrain them to the "Location Hierarchy" AND Spend Category/Spend Category Hierarchies that they are assigned to in those roles.

## Intersecting Role Based Constrained Security Groups

**View Intersection Security Group Category Buyer**

Name: Category Buyer  
Context Type: Mixed (Subset)

**Intersection Criteria**

Security Groups to Include: Business Site Buyer, Spend Category Buyer  
Security Group to Exclude: (empty)

Domain Security Policy Permis...  
Business Process Security Policy Per...

**Intersect 2 role-based constrained security groups**

**View Role-Based Security Group (Constrained) Business Site Buyer**

Name: Business Site Buyer  
Context Type: Constrained by Role Access

**Group Criteria**

Assignable Role: Business Site Buyer

**Access Rights to Organizations**

Available Actions	Assignable Role
Assignable Role	Business Site Buyer
Audits	Role Name
Favorite	Workday Known Organization Role (empty)
Integration IDs	Role Usages
Reporting	Location Hierarchy

**View Role-Based Security Group (Constrained) Spend Category Buyer**

Name: Spend Category Buyer  
Context Type: Constrained by Role Access

**Group Criteria**

Assignable Role: Spend Category Buyer

**Access Rights to Organizations**

Available Actions	Assignable Role
Assignable Role	Spend Category Buyer
Audits	Role Name
Favorite	Workday Known Organization Role (empty)
Integration IDs	Role Usages
Reporting	Spend Category Bi...

**See Workshop 3 in back of guide for an example of intersecting role-based constrained security groups.**

## INTERSECTION SECURITY GROUP LIMITATIONS

Though powerful and commonly used, it is important to be aware of limitations around intersection security groups.

- Intersection security groups cannot be used to intersect other intersections
- Certain **Workday-delivered reports with organization filters** may not work if user has intersection security access to report.
- Not all functionality can handle intersections
  - **Compensation**
  - **Talent**
- Intersection security does not work well for **merit processing or year-end performance calibration**
- Restrictions **around intersection security groups with multiple contextual groups**.
  - Workday can disallow Intersection security groups that intersect two or more constrained security groups from being applied to
    - Initiating actions on business processes
    - Processing actions on business processes
    - Security domains
  - This can prevent you from applying security groups to policies for secured content that must run with a single contextual filter
  - Example: If you create a security group that intersects a security group of HR partners for supervisory organizations and a security group for HR partners in Spain (location hierarchy), and Workday has disallowed the Intersection Groups Containing Multiple Contextual Groups security group type on a business process or security domain policy, you can't add the intersection security group to the policy.
- *As with any security configuration, be sure to test extensively to confirm that intersection security configuration meets your needs.*

## COMMON USE CASE #3 – HIDING TARGETS

Intersection security groups can also be used to exclude target instances from members' otherwise access. Exclusion criteria can be configured by referencing organizations. Those you want to exclude must be identified via organizations and the **exclusion applies to positions in those organizations** (not workers), so be sure to account for all positions a worker may have.

### Common Scenarios:

- To meet FERPA regulations at educational institutions. Per FERPA, students working at the education institution may opt out (or opt in) of having their information be public. Access to public worker information in Workday must make the exception to not show these students.
- Hiding sensitive workers, e.g. political dissidents, undercover agents at a police agency, or famous people you do not want to show in public worker directories.
- Hiding HR from HR. There are cases where an HR Partner, that say, supports a given organization, should not have target access to a worker's position in that organization if that worker is their HR peer.

Using Intersection Security groups with target exclusion, we can configure these exceptions to "hide" or exclude certain positions from the members' otherwise access.

### High Level Steps

1. Identify the "hidden" worker positions by organization. Create a custom organization if needed and place the "hidden" worker positions in that custom organization.
  - For FERPA, place students in a custom organization
  - For sensitive worker positions, identify these positions via an organization or create a custom organization if needed with membership rules if possible.
  - For Hiding HR from HR, identify your HR worker positions via an organization, create a custom organization if needed with membership rules if possible.
2. Create an intersection security group that excludes access to the hidden population using the organization(s) defined.

3. **Replace security groups on needed domains.** In the example below, the "All Employees" security group was removed from the Worker Data: Public Worker Reports domain and replaced with the intersection security group that has the configured target exclusion to hide certain positions from public access.



- Use caution when excluding as the **exclusion applies to the position, not to the worker** – thus all the workers' positions must be included in the exclusion criteria to 'hide that worker'.
- Intersection security groups with exclusions should not be used in business process routings.



## ACTIVITY 11C – OPTIONAL CHALLENGE ACTIVITY

Configure an intersection security group to restrict access to worker profiles. This challenge will provide hints, but not step by step instructions.

**GOAL:** Workers should not be able to view profiles of workers who are located in Northern Europe.

Before you start your security configuration, verify the default configuration allows workers to search for and view any worker profile.

As a test, proxy as Adam Carlton (acarlton) and search for Alejandro Ruiz. Adam is an employee in Boston and Alejandro is located in London. When you have completed the configuration, Adam should no longer be able to see Alejandro's profile.

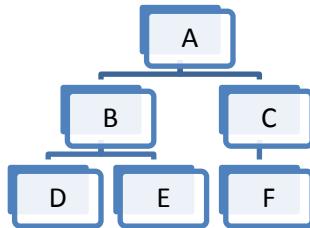
**HINTS:**

- Create an intersection security group called **All Employees (Inter)**
- Use the location hierarchy **EU - Northern Europe** for the *Exclude Target Object in Organization apply to Current Organization and All Subordinates (COAS)*
- Domain: Worker Data Public Reports is the domain you want to restrict access to
- Activate and Test

## LEVEL-BASED SECURITY GROUPS

Workday enables you to create a security group based on a **leveling mechanism**, where you can:

- **Identify members based on level**
- **Constrain member target access to lower levels, across organizations.** Target access is only to workers in lower levels, **not same level, nor higher levels. No organization constraint.**



Level based security groups are primarily used and needed for **Talent Management**.

In order to use level-based security groups and identify and constrain workers based on levels, you must **define and maintain a leveling mechanism or hierarchy in the tenant**. Leveling mechanisms supported include:

### Compensation Grade Hierarchy

Maintain Compensation Grade Hierarchy		
Lowest order value indicates highest hierarchy rank order.		
WARNING: All active Grades should belong to a rank in order to be secured by the hierarchy.		
4 items		
<input type="button" value="+"/>	*Order	*Name
	1	Senior Executive Compensation Grade
	2	Executive Compensation Grade
	3	Management Compensation Grade
	4	Individual Contributor Compensation Grade
		*Compensation Grades
		search
		Executive Level 1
		Executive Level 2
		Management
		Sales Management
		Support Management
		Field Sales
		Hourly (Reduced Wage)
		Hourly Non-Union (No Steps)
		Hourly Non-Union (Steps)
		Hourly Union
		Non-Management

### Management Level Hierarchy

Management Level Hierarchy		
Management Hierarchy		
8 items		
Order	Management Level	Job Profile
1	1 Board of Directors	
2	2 Chief Executive Officer	Chief Executive Officer
3	3 Executive Vice President	Chief Data Officer Chief Financial Officer Chief Information Officer Chief Operating Officer Chief Risk Management Officer Executive VP, Sales & Marketing
4	4 Vice President	Chief Human Resources Officer Controller General Counsel Vice President, Consulting Services Vice President, Global Support Vice President, Marketing Vice President, Program Management Vice President, Real Estate & Facilities Vice President, Research & Development

**Example:**

Level based security groups allow users to access talent related data for workers across organizations, but only limited to those in lower levels, not same, nor above.

In the example below,

- We are identifying those in Compensation Grades 1 and 2 as members.
- We are then configuring this level based security group in the domain: Worker Data Confidential Feedback.
- Members, i.e., those in Compensation Grades 1 and 2, can access Worker Data Confidential feedback items in Workday, but *only for those in lower compensation grades than themselves*.
  - Those in Level 1 – Senior Executive Compensation Grade can only access target data for those in Levels 2,3 and 4 (not others in Level 1).
  - Those in Level 2 – Executive Compensation Grade can only access target data for those in Levels 3 and 4 (not for those in Levels 1 or 2).

Operation	Domain Security Policy	Functional Areas
View Only	Worker Data: Confidential Feedback	Talent Core

## CREATE AND MAINTAIN LEVELING HIERARCHIES

The **Maintain Compensation Grade Hierarchy** task enables you to set up a compensation grade hierarchy. You can only create one compensation grade hierarchy per tenant.

Lower order numbers indicate higher levels. So, for example:

- Those in Level 1 can access data for those in Levels 2,3,4.
- Those in Level 2 can access data for those in Levels 3,4
- Those in Level 3, can access data for those in Level 4.
- Those in Level 4, cannot access data for anyone since no lower levels defined in hierarchy.

Maintain Compensation Grade Hierarchy			
Lowest order value indicates highest hierarchy rank order.			
WARNING: All active Grades should belong to a rank in order to be secured by the hierarchy.			
4 items			
+	*Order	*Name	*Compensation Grades
	1	Senior Executive Compensation Grade	search Executive Level 1
	2	Executive Compensation Grade	Executive Level 2
-	3	Management Compensation Grade	Management Sales Management Support Management

Management levels are created using the **Management Level Hierarchy** task. The **Maintain Management Types** task is used to define the individual management types required to build a management level hierarchy.

Management Level Hierarchy			
Management Hierarchy			
8 items			
	Order	Management Level	Job Prof
	1	1 Board of Directors	
	2	2 Chief Executive Officer	Chief Exec
	3	3 Executive Vice President	<div style="border: 1px solid #ccc; padding: 5px; display: inline-block;"> <span>Available Actions</span> <span>Management Level</span> </div> <div style="display: flex; justify-content: space-between; width: fit-content;"> <div style="flex: 1;"> <a href="#">Audits</a>  <a href="#">Competency</a>  <a href="#">Favorite</a>  <a href="#">Integration IDs</a> </div> <div style="flex: 1;"> <a href="#">Management Type</a>    <a href="#">Executive</a>  <a href="#">Edit</a>  <a href="#">Insert Peer Level</a>  <a href="#">Insert Subordinate Level</a> </div> </div>
	4	4 Vice President	<div style="border: 1px solid #ccc; padding: 5px; display: inline-block;"> <span>Level</span> <span>Translation</span> </div>

## CREATING A LEVEL BASED SECURITY GROUP

Once you have created the hierarchy and leveling mechanism with the defined orders, you can **create a Level-Based security group** to identify members to include by level.

- You can include “**all levels**” – so all workers across all levels will be members of the security group.
- You can **include specific levels** – so only workers in specified levels will be included as members of the security group.

Then when you use the security group in a security policy, members will be constrained to accessing data for **those in lower levels**.

This feature is intended for use with Talent Management functionality. We will edit the Worker Data: Talent Card security policy in the activity to demonstrate the feature.

## CREATE AND DEPLOY LEVEL-BASED SECURITY GROUPS

1. Verify the leveling mechanism or hierarchy. Run: Maintain Compensation Grade Hierarchy task or Create Management Level Hierarchy task
2. Create a **Compensation Level-based** or **Manager Level-based security group**
3. Select: Applies to All or Applies to Levels (then choose level(s) from the prompt). **Levels included will determine the members of the security group**
4. Edit Security Policies
5. Activate Pending Security Policy Changes
6. Test (members target access will be constrained to those in lower levels)



## ACTIVITY 12 CREATE LEVEL-BASED SECURITY GROUP

Logan will use the Management Level hierarchy that has been created in the GMS tenant to create a level based security group that grants Manager access to all workers Talent Card below their level. This allows managers to recruit workers from organizations other than their own.

### TASK 1: CHECK OUT EXISTING SECURITY

1. **Start Proxy** as Jack Taylor (jtaylor)
2. On Jack's **Home** page, click on the **My Team** worklet. At the bottom, see his team. See how Jack can access Jeff Gordon's, his direct report's, Talent Card. Using related actions, select **Jeff Gordon > Talent > View Talent Card**

The screenshot shows the Workday Home page with the 'My Team' worklet. Below it, there are two team member profiles: 'Ariceli Bermudez [C]' and 'Jeff Gordon'. A context menu is open over 'Jeff Gordon', with 'Talent' being the selected option. The menu includes actions like 'Get Feedback', 'View Feedback', and 'View Employee Potential', along with 'View Talent Card' at the bottom.

3. Now from the search box, search for *Chad Anderson* and click to view his worker profile. Chad does not report to Jack Taylor. Using related actions, navigate to Talent and review the options. Note Jack **does not have an option to View Talent Card for Chad**.

The screenshot shows the Workday search results for 'worker: Chad Ander'. It displays one search result: 'Chad Anderson' (Senior Benefits Analyst, Employee). A context menu is open over his profile, with 'Talent' being the selected option. The menu includes actions like 'Give Feedback', 'View Feedback', and 'Add Skills'.

4. **Stop Proxy**

## TASK 2: REVIEW MANAGEMENT LEVEL HIERARCHY

1. As Logan McNeil (lmcneil)
2. From the search box, run the task: **Management Level Hierarchy**
3. From the prompt, select **Management Hierarchy**. You will see 2 listed in the training tenant. Choose the second one, as the first one is empty. Here you can see job profiles designated to Management Levels.

The screenshot shows a table titled "Management Level Hierarchy" with the sub-section "Management Hierarchy". The table has 8 items and 3 columns: Order, Management Level, and Job Profile. The data is as follows:

Order	Management Level	Job Profile
1	<a href="#">1 Board of Directors</a>	
2	<a href="#">2 Chief Executive Officer</a>	Chief Executive Officer
3	<a href="#">3 Executive Vice President</a>	Chief Data Officer Chief Financial Officer Chief Information Officer Chief Operating Officer Chief Risk Management Officer Executive VP, Sales & Marketing
4	<a href="#">4 Vice President</a>	Chief Human Resources Officer Controller General Counsel Vice President, Consulting Services Vice President, Global Support Vice President, Marketing Vice President, Program Management Vice President, Real Estate & Facilities

## TASK 3: CREATE LEVEL-BASED SECURITY GROUP

1. From the search box, run the task: **Create Security Group**
2. Select **Manager Level-Based Security Group** as the Type of Tenanted Security Group
3. Enter the Name **Manager Talent Access**

The screenshot shows the "Create Security Group" dialog box. The "Type of Tenanted Security Group" dropdown is set to "Manager Level-Based Secur...". The "Name" field contains the value "Manager Talent Access".

4. Click the **OK** button
5. Set **Applies to Levels** to **6 Manager**

We are going to **include those in level 6 as members** of our level-based security group.

**Edit Manager Level-Based Security Group**

Manager Level-Based Security Group	<input type="text"/> Manager Talent Access
Name	<input type="text"/>
Comment	<input type="text"/>
Context Type	Constrained
Inactive	<input type="checkbox"/>
<b>Group Criteria</b>	
<input type="radio"/> Applies to All Levels <input checked="" type="radio"/> Applies to Levels	
<input type="text"/> search <span>x 6 Manager</span>	
<div style="border: 1px solid #ccc; padding: 5px; width: fit-content;">           search            1 Board of Directors            2 Chief Executive Officer            3 Executive Vice President  <b>4 Vice President</b>            5 Director  <b>6 Manager</b>            7 Supervisor            8 Individual Contributor  <a href="#">Management Hierarchy</a> </div>	

6. Click **OK**

7. Click **Done**

#### TASK 4: EDIT SECURITY POLICY

1. From the search box, run the **View Security for Securable Item** report
2. Search for item: *View Talent Card*.
3. Select **Talent Cards for Employee – Profile View (Report (XpressO))** from the prompt

**View Security for Securable Item**

Domain Item * view talent card	<input type="text"/> view talent card <a href="#">Top &gt; view talent card</a>
<div style="border: 1px solid #ccc; padding: 5px; width: fit-content;">           view talent card            Print Talent Cards for Organization XSLT (Report (XpressO))            Print Talent Cards for Talent Pools XSLT (Report (XpressO))            Print Talent Cards for Talent Review XSLT (Report (XpressO))  <b>Talent Cards for Employee - Profile View (Report (XpressO))</b> </div>	

4. Click **OK**

5. Click the related action off the Security policy **Worker Data: Talent Card**
6. Navigate to **Domain Security Policy > Edit Permissions**

The screenshot shows a 'Domain Security Policy Worker Data: Talent Card' card. On the left, there's a sidebar with 'Domain Security' and 'Security Policy' sections. A context menu titled 'Available Actions' is open over the card, listing: Domain Security Policy, Audits, Favorite, Functional Area, Integration IDs, Reporting, Edit Permissions, Disable, View All for Functional Area, View Domain, and View History.

## 7. Add **Manager Talent Access** Security Group to provide **View** access

The screenshot shows the 'Edit Permissions' page for the 'Worker Data: Talent Card'. It displays security settings for actions and reporting items, and a search bar for security groups. An 'Alerts: 1' box contains a message about activating pending security policy changes. The search bar shows results for 'Manager Talent Access' and 'HR Auditor'.

8. Click **OK** and then click **Done**

9. From the search box, run the task **Activate Pending Security Policy Changes**

10. Enter a comment, such as 'Activity 12'

11. Click OK

12. Check the Confirm checkbox

13. Click OK

## TASK 5: TEST ACCESS

1. **Start Proxy** as Jack Taylor (**jaylor**)
2. Search for *Chad Anderson*
3. From the related action icon, navigate to **Talent > View Talent Card**. Jack can now view the Talent Card of workers that do not report to him as long as they are in a lower management level.

The screenshot shows the Workday interface with a search result for 'chad anderson'. The search results page displays Chad Anderson's profile as a common item. A tooltip over the 'View Team' button in the 'Available Actions' sidebar indicates that Jack can only access talent cards for workers below his management level.

4. Note that Jack can only access talent cards for workers who are below his management level.
5. To test further, see if Jack can *View Talent Card* for workers in same level or higher levels than him. His level based security group access to the domain to view talent card data should prevent him from accessing targets in same or higher levels, i.e. workers in management levels 1-6.
  - a. James Walker (another manager at the same level as Jack)
  - b. Steve Morgan (the CEO is at a higher level than Jack).

### 6. **Stop proxy**

(End of Activity)

## SECURITY TIPS

### SECURITY METHODOLOGY

Try to keep it as simple as possible. Start with user-based groups. Layer in role-based (constrained) groups. Think of your business partners first. Assign permissions at the highest node in the hierarchy to take advantage of inheritance, using the option for current and unassigned subordinates. Only assign at the lower levels when necessary.

Leverage the default delivered security whenever possible. **More security groups, more edited permissions mean more MAINTENANCE!**

#### Model your organization structure

- Supervisory organization
  - Reporting structure (managers)
  - Functional/line of business
- Location hierarchy
  - Global/regional partners
- Company hierarchy
  - Financial transactions

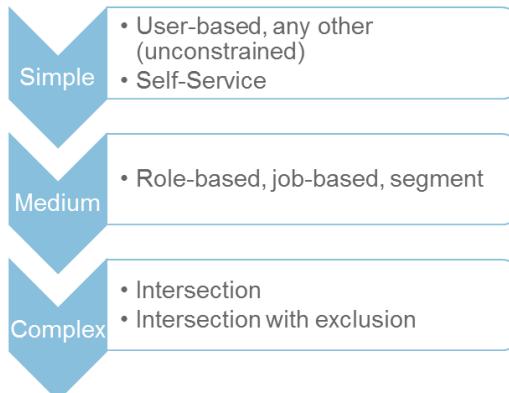
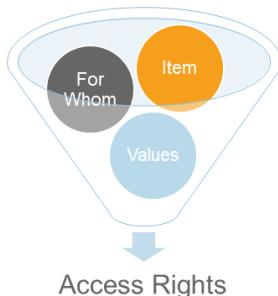
### DESIGN TOP DOWN

Remember that execution time and performance will be impacted as you configure greater constraints and filters on access. Keep efficiency and maintenance in mind.

- Start with user-based – ensure access to items and all instances.
- Move next to role-based and self-service.
- Use job-based only where role-based or user-based does not work.
- Be careful with intersection security groups as not all areas supported. Test!

### Keep Efficiency in Mind

- Less "context filtering", better performance



## MANAGING WORKFORCE SECURITY ASSIGNMENTS

As part of staffing transactions where workers are terminating or changing jobs, it is important to ensure security group membership, specifically revisiting **role-assignments** and **removing user-based security groups assignments**.

- Use the **Assign Roles** sub-process in staffing transaction business process definitions.
- Use delivered services, add service steps to staffing transaction business process definitions:
  - Service step to **Remove User-Based Security Groups**
  - Service step to **Terminate User Account**

In addition, leverage delivered reports and shared solutions to audit changes.

Audit Workday Account Changes - Changes to User-Based Groups and/or Organization Role Assignments (for selected roles)	Custom Report Definition	Configurable Security, Cross Application Services	May-06-13 fwalterhouse
--	--------------------------	---	------------------------

## SECURITY POLICY RESTRICTIONS

As you design your security configuration and determine needed security groups and constraints, be aware that some domain and business process security policies can be **restricted to certain security group types**. Workday now explicitly disallows you from adding some security group types to business process or security domain policies to prevent applying security groups to policies for secured content. Workday provides these new report fields that enable you to report on disallowed security group types:

- Disallowed Security Group Types
- Security Group Types Disallowed for Initiating Actions
- Security Group Types Disallowed for Processing Actions

View Business Process Security Policy Accounting Journal Event 

Description	Create an accounting journal.
Functional Area(s)	Financial Accounting
Security Group Types Allowed for Initiating Actions	Roles - Company  Unconstrained Groups
<b>Who Can Start the Business Process</b>	
Initiating Action	Create Journal
Security Groups	Accountant Accounting Manager Implementers
Initiating Action	Import Accounting Journal (WS Background Process)
Security Groups	Accountant Accounting Manager Financial Management System Implementers
Security Group Types Allowed for Processing Actions	Roles - Business Unit Roles - Company  Roles - Cost Center

Configured **Organization type constraints** must match **the security policy type restrictions**.

- For example, when creating an Integration System or Service Center Based Security group constrained to a *company*, you cannot add this security group to a domain or to a business process security policy that is restricted to organization types other than *company*.
- Similarly, when you include a role-based security group with the role usage of *Company* (such as Accountant or Expense Analyst) in the Intersection Criteria or specify a *Company* in the Exclusion Criteria (Constrained Context), you cannot add the Intersection Security Group to a domain or to a business process security policy that is restricted to Organization types other than *Company*.

Check the Solution Catalog on Community for shared security configurations for specific products or features, like Recruiting, Performance Reviews, Staffing Actions and more!

Solution Type	Title	Update	Product / Features	Post date	Author
Security Configuration	New Worktags - Fund, Business Unit, Grant, Program and Object Class: Recommended Security Configuration		Financial Management, Worktags	Mar-24-15	jgeasa
Security Configuration	Authentication Policy SAML_EEOnly Outside Network	Workday 23 - Retired	Authentication, Authentication Policies, Cross Application Services	Feb-06-15	tmarquez2
Security Configuration	Resource Booking Request: Recommended Security Configuration	Workday 24	Financial Management, HCM, Projects	Oct-13-14	cyuan
Alternate Approach, Business Process Definition, Security Configuration	Route Financial Transactions to Non-Company Role for Review	Workday 23 - Retired	Financial Management	Sep-07-14	dwhite
Security Configuration	Recommended Security Configurations: Committees	Workday 23 - Retired	Cross Application Services, Education and Government, HCM	Aug-15-14	ljohnson10
Security Configuration	Recommended Supply and Demand Analytics Setup		HCM, Workforce Planning, Staffing	Aug-11-14	nsharma3
Security Configuration	Enhanced Resource Management: Recommended Setup	Workday 23 - Retired	Financial Management, Project Plans, Projects	Jul-21-14	cyuan

## ACTIVATING PREVIOUS TIMESTAMPS

Every time you activate security, you establish a **Security Evaluation Moment** or “**Timestamp**” capturing the state of the domain and business process security policies as of that moment. All pending domain or business security policy edits *since the last activation are activated with each timestamp.*

The **View All Security Timestamps** report will show all the security policy activations in the tenant.

View All Security Timestamps			
Security Evaluation Moment in Use 04/12/2015 10:28:13.593 AM			
507 items			
Security Timestamp	Security Evaluation Moment	Active?	Comment
04/12/2015 10:28:13.593 AM		Yes	Act 12
04/11/2015 06:35:38.310 PM			Act 11B
04/11/2015 06:23:29.816 PM			Act 11 A
04/11/2015 04:11:08.942 PM			Activity 9
04/10/2015 06:31:04.611 PM			Activity 8

If there are issues with your security policies and you need to revert back to a previous timestamp, you can use the task: **Activate Previous Security Timestamp**.

- *All security policy edits since the reverted timestamp will go into a pending state.*
- *Activating a previous security timestamp will not impact security groups and membership, just security policies.*

Activate Previous Security Timestamp																			
Previous Security Timestamps *	<input type="text"/> search																		
<div style="border: 1px solid orange; padding: 2px;">           Sorry, this field is not search enabled.         </div>																			
<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="padding: 2px;">04/11/2015 06:35:38.310 PM</td> <td style="width: 10px;"></td> </tr> <tr> <td style="padding: 2px;">04/11/2015 06:23:29.816 PM</td> <td></td> </tr> <tr> <td style="padding: 2px;">04/11/2015 04:11:08.942 PM</td> <td></td> </tr> <tr> <td style="padding: 2px;">04/10/2015 06:31:04.611 PM</td> <td></td> </tr> <tr> <td style="padding: 2px;">04/09/2015 07:18:20.397 AM</td> <td></td> </tr> <tr> <td style="padding: 2px;">04/08/2015 05:08:55.798 PM</td> <td style="width: 10px; text-align: right;">...</td> </tr> <tr> <td style="padding: 2px;">03/23/2015 02:59:05.905 PM</td> <td></td> </tr> <tr> <td style="padding: 2px;">03/20/2015 08:42:50.411 AM</td> <td></td> </tr> <tr> <td style="padding: 2px;">03/20/2015 08:22:42.474 AM</td> <td></td> </tr> </table>		04/11/2015 06:35:38.310 PM		04/11/2015 06:23:29.816 PM		04/11/2015 04:11:08.942 PM		04/10/2015 06:31:04.611 PM		04/09/2015 07:18:20.397 AM		04/08/2015 05:08:55.798 PM	...	03/23/2015 02:59:05.905 PM		03/20/2015 08:42:50.411 AM		03/20/2015 08:22:42.474 AM	
04/11/2015 06:35:38.310 PM																			
04/11/2015 06:23:29.816 PM																			
04/11/2015 04:11:08.942 PM																			
04/10/2015 06:31:04.611 PM																			
04/09/2015 07:18:20.397 AM																			
04/08/2015 05:08:55.798 PM	...																		
03/23/2015 02:59:05.905 PM																			
03/20/2015 08:42:50.411 AM																			
03/20/2015 08:22:42.474 AM																			
<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td colspan="2" style="padding: 2px; text-align: center;"> <b>Security Timestamp 04/08/2015 05:08:55.798 PM</b> </td> </tr> <tr> <td style="width: 50%; padding: 2px;">Security Evaluation Moment</td> <td style="width: 50%; padding: 2px;">04/08/2015 05:08:55.798 PM</td> </tr> <tr> <td style="padding: 2px;">Comment</td> <td style="padding: 2px;">Activity 5</td> </tr> </table>		<b>Security Timestamp 04/08/2015 05:08:55.798 PM</b>		Security Evaluation Moment	04/08/2015 05:08:55.798 PM	Comment	Activity 5												
<b>Security Timestamp 04/08/2015 05:08:55.798 PM</b>																			
Security Evaluation Moment	04/08/2015 05:08:55.798 PM																		
Comment	Activity 5																		

## SECURITY-RELATED REPORTS

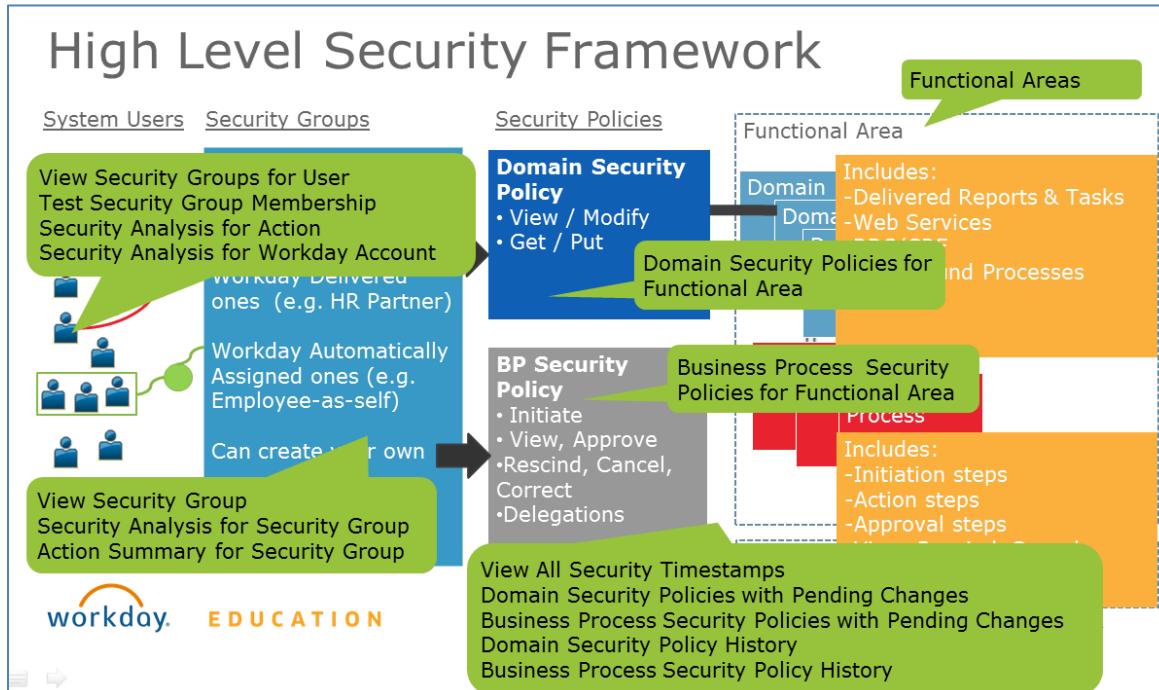
Workday delivers many security and audit related reports. To see the full list of delivered reports, run **Workday Standard Reports** for security related reporting categories.

The screenshot shows a search bar with the placeholder 'search' and a list of report categories:

- System: Data Access (Audits)
- System: Security (Audits)
- Security Administration
- Security Configuration

Some useful ones:

1. How can someone get access to this item?  
**View Security for Securable Item**
2. How did user X get access to this action?  
**Security Analysis for Action**
3. Does user X have access to instance 1, and through which security group  
**Test Security Group Membership**
4. What can a member of this group see and do?  
**Action Summary for Security Group**
5. Why can('t) a user can access something on the landing page?  
**Security Analysis for Landing Page**
6. What can a given user access?  
**Security Analysis for Workday Account**



## AUDIT TRAILS

A great report for example for audit information is: **View User or Task or Object Audit trail**. You can see an audit trail for a user, for a given task, or for a business object.

You can even schedule this report to run on a recurring basis.

Below is a list of sample delivered reports.

## SECURITY GROUPS

To Report on...	Look at this Report
A functional area's security policies	<ul style="list-style-type: none"> <li>• Security Policies for Functional Area</li> <li>• Business Process Security Policies for Functional Area</li> <li>• Maintain Functional Areas (You can enable/disable them from here.)</li> </ul>
Security group's access, policies, and components	View Security Group
User-based security group's access, policies, and members	View Security Group
All security policies in all functional areas	Functional Areas

## ORGANIZATIONS AND ROLES

To Report on...	Look at this Report
All assignable roles	Maintain Assignable Roles
A worker's organization roles	Role Assignments for Worker
Organization role assignments	Roles for Organization and Subordinates

## SECURITY POLICIES

To Report on...	Look at this Report
Securable items that are accessible to a specific security group	Action Summary for Security Group
Security for securable items in a domain security policy	View Security for Securable Item
Securable items that are secured separately in more than one security policy	Secured Items in Multiple Domains
Domain security policies	Domain Security Policies for Functional Area
Who has changed which policies (and security groups) in the time range, and when	Domain Security Policies Changed within Time Range Business Process Security Policies Changed within Time Range
Policy changes that will go into effect the next time you activate pending changes.	Domain Security Policies with Pending Changes Business Process Security Policies with Pending Changes
What has changed for a specified policy	Domain Security Policy History Business Process Security Policy History
Business process Security policies	Business Process Security Policies for Functional Area
Securable items in a functional area grouped	Domain Security Policy Summary

## SECURITY POLICIES

To Report on...	Look at this Report
by domain and security group	
Content of a domain	View Domain
Disabled or unused domains	Inactivated Domains
Security problems	Security Exception Audit
All domain and business process security policy changes you have made but have yet to activate	Domain Security Policies with Pending Changes Business Process Security Policies with Pending Changes

## USERS

To Report on...	Look at this Report
A user's roles	Worker Roles Audit Role Assignments for Worker
A user's management level	Active Employees or view current job details on the View Worker page
A user's job profile	Worker Change History or view current job details on the View Worker page
A user's security groups	View Security Groups for User
How a specified user has access to a specified action	Security Analysis for Action
Is a user in a security group that has access to a target instance of a securable item?	Test Security Group Membership
An overview of a user's access	Security Analysis for Workday Account

**JOB INFORMATION**

<b>To Report on...</b>	<b>Look at this Report</b>
A list of workers by job profile	Directory by Job Profile
A list of workers by job family	Directory by Job Family
The details of a job profile	Job Profile
A list of job profiles by job family and job family group that details a job profile's management level, job classification and exempt/non-exempt status	Job Catalog



## OPTIONAL LAB – SELF STUDY: SECURITY REPORTS

This FAQ is designed to introduce you to the various configurable security reports that are available. These reports can provide answers to many of the Frequently Asked Questions regarding Workday's Configurable Security.

### ⊕ As Logan McNeil (lmcneil)

#### TASK 1 - TO WHICH SECURITY GROUPS DOES A USER BELONG?

1. Search for '*Cardoza*'
2. Use Maria Cardoza's related action icon to initiate the Security Profile > View Security Groups report
3. How many security groups is Maria Cardoza a member of? \_\_\_\_\_
4. Click on the **Benefits Partner Security Group**
5. What kind of Security Group is Benefits Partner? \_\_\_\_\_
6. How many domains does this security group have access to? \_\_\_\_\_
7. How many business processes does this security group have access to? \_\_\_\_\_

#### TASK 2 - IF I KNOW THE REPORT OR TASK THAT I WANT TO PROVIDE ACCESS TO, HOW CAN I FIND THE SECURITY GROUPS THAT CAN BE USED?

1. Search for '*View Sec*'
2. Click the **View Security for Securable Item** report hyperlink
3. For Domain Item find and enter '*Maintain Role*'
4. Choose the **Maintain Assignable Roles** task
  - a. Which Functional Area is this item in? \_\_\_\_\_
  - b. What domain is this task secured in? \_\_\_\_\_
  - c. Which Security Groups have access to this task? \_\_\_\_\_

TASK 3 - I KNOW THE SECURITY GROUPS TO WHICH A USER BELONGS. HOW DO I DETERMINE WHICH TASKS THE USER HAS ACCESS TO?

1. Run the **Security Analysis for Workday Account** report for Noah to see an analysis of all actions available to Noah via each security group on his account.
2. What security group allows Noah to initiate the Period Close business process event? \_\_\_\_\_
3. What security group allows Noah to initiate the Request Budget Approval business process event?  
\_\_\_\_\_

TASK 4 - HOW DO I FIND OUT WHICH SECURABLE ITEMS ARE IN A FUNCTIONAL AREA OR A DOMAIN?

1. From the search box, run **View Domain**
2. Choose the **Worker Data: Compensation** domain
3. How many secured items are in the Worker Data: Compensation domain? \_\_\_\_\_
4. Click on the **Worker Data: Market Position Details** sub-domain hyperlink
5. Expand the Reports and Tasks section
6. How many reports and tasks are in this domain? \_\_\_\_\_
7. Click the related action icon off of the **View Market Position** task to initiate the Security > View Security Analysis for Action report
8. Enter *Noah Pierce* as the user
9. Click **OK**
10. What security group (s) allow Noah Pierce to get to the View Market Position task in the Worker Data: Market Position Details domain? \_\_\_\_\_

TASK 5 - HOW DO I ASSIGN SOMEONE TO BE A MEMBER OF A USER-BASED SECURITY GROUP? HOW DO I SEE A USER'S SECURITY GROUP MEMBERSHIP AND SECURITY HISTORY?

1. Search for *Noah Pierce*
2. Use the related action icon to initiate the **Security Profile > Security History for User** report

3. Enter *1/1/2000* and *today's date* for the date range
4. Click the **OK** button
5. After reviewing the report use the related action icon for Noah Pierce to initiate the **Security Profile > Assign User-Based Security Groups** task
6. Add the **Costing Administrator** security group
7. Is activation required to provide Noah access to Costing Administrator tasks? \_\_\_\_\_

(End of Activity)

## TROUBLESHOOT SECURITY - FAQ

### WHAT IF USERS CAN ACCESS AN ACTION TO WHICH THEY SHOULD NOT HAVE ACCESS?

1. Run the Security Analysis for Action report, specifying the name of the user and the action. This report shows all the ways in which the user is granted access to the action, even if the action appears in multiple domains.
2. Determine whether a security group needs to be removed from the security policy or the user needs to be removed from a security group.

This report is useful if you're trying to troubleshoot a user's access to a task, report or business process. It doesn't apply if you're trying to figure out why a person has access to a specific item, such as a data source, report field, or specific object, such as worker, position, or organization. The following reports can help in other cases:

**View Security for Securable Item.** This provides information about how an item is secured and what security groups are authorized for it.

**Test Security Group Membership.** This enables you to see a particular user's security group membership. This ability can be useful, for example, if you're trying to determine why a particular HR PARTNER can or cannot access a particular worker.

Which change you make might depend on how many other users there are in the security group. If you decide to remove the worker and it is not a user-based security group, you might have to unassign an organization role, modify the job profile or remove the worker from the organization or location, depending on what type of security group it is. Other options include removing a job profile, management level, organization, or location from a security group.

Be sure to consider how your change affects other access that the security group and the user might have. All changes to security groups or security policies are effective immediately.

Keep in mind that some secured items might appear in more than one domain. Workers who are granted different levels of access permission in different domains get the most access granted. For example, a worker who gets view permission (or no permission) to a secured item in one domain and modify permission to the same secured item in another domain, will get modify permission to the secured item. When a worker has access to a secured item to which access should be denied, run the Secured Items in Multiple Domains report to see if that item appears in another domain, and check to see if access is granted there.

You might also need to review the Access Rights to Organizations section in the security group definition and inheritance.

### WHAT IF USERS CANNOT SEE AN ITEM TO WHICH THEY SHOULD HAVE ACCESS?

1. Run the View Security for Securable Item report, specifying the name of the securable item, such as a data source, report field, task, report, or business process.
2. Make a note of the security groups that have permission to access this securable item.
3. Run the View Security Groups for User report and specify the user who should be able to see the securable item.
4. Compare the security groups for the worker with the security groups for the securable item.
5. Determine whether the worker should be added to one of the security groups that has access to this item, or if a security group the worker is already in should be granted permission to access the item.

Which change you make might depend on how many other users there are in the security groups that the worker is in or what other access is granted if you associate the worker with a security group that already has access.

If trying to view a business process event, the user needs to be in a security group included in the View All or View Completed Only sections of the business process security policy. You also should look at Access Rights to Organizations in the security group definition (and at access rights gained through inheritance, if applicable).

### HOW CAN SECURABLE ITEMS END UP WITH EXCEPTIONS AND HOW DO I FIX THEM?

Security exceptions usually happen when a legitimate security configuration encounters a change in the security policy that makes some access assignment invalid. Two possible causes are when you activate a pending security policy change in which a:

security policy specifies a group that you have deleted from Workday.

business process security policy is missing a group that the business process still uses.

Before you remove a security group from a business process security policy, remove the group from the various business processes in each organization that has a custom version defined. However, if you do not know all the places where a security group is used, or you have processes that are already running, you can still change the policy. You get a warning that the change will cause an exception.

The Security Exception Audit report identifies any problem area. The problem and solution are explained for each exception. Generally, all you have to do is remove the invalid security group from the policy or business process.

For business processes that are already started, reassign the step that is routed to an invalid user, or rescind the process. In either case, be sure to change the business process definition for that organization to specify only valid security groups.

## WHERE CAN I SEE ALL THE PERMISSIONS GRANTED TO A SECURITY GROUP?

Use the View Security Group report. This report has a Security Permissions tab for the domain security policies and a Business Process Permissions tab for the business process security policies. Navigate to any security policy and see the securable items to which access permission is granted. You also can use the Action Summary for Security Group report to view details regarding domain security policies and business process security policies for a specific security group.

## WHERE CAN I FIND OUT WHERE AND HOW SECURABLE ITEMS ARE SECURED?

Run the View Security for Securable Item report.

## HOW DO I ADD USERS TO A USER-BASED SECURITY GROUP?

To add members to a user-based security group use the Assign User to User-Based Security Group task.

To add a user to more than one user-based security group at a time, use the Assign User-Based Security Groups for Person task.

## WHY DOES A USER RECEIVE AN ERROR WHEN ATTEMPTING TO ACCESS AN INBOX ITEM OR EMAIL NOTIFICATION LINK?

It's possible that you configured a user to perform a step in a business process but, after the process was initiated, someone changed the security policy for that business process. Now the user does not have access permission and cannot respond. Usually, this is caused when the security group assigned to the step does not have View All access (for in-process events) or View Completed Only access (for completed events).

Run the Security Exception Audit report and look for that business process.

Also run the Business Process Policy View Audit report to identify security groups that do not have view access to particular components of business process types that might involve them.

The appropriate person should reassign the errant step and redefine the process to ensure that only valid security groups are specified.

## HOW DID A USER GET ACCESS TO A PARTICULAR INSTANCE, SUCH AS A WORKER?

It is possible for a user to get access to a worker through several different role-based security groups. If you want to remove that user's access to the worker, it is useful to know which of the user's role-based security groups are providing that access.

1. Use the Security Analysis for Action report to determine how the user got access to the action that accessed the worker. Make note of the security groups the user has that provide access to that action.
2. Obtain the instance ID for the worker the user can access.
3. Run the Test Security Group Membership report, supplying the user and the instance. Supply one security group at a time, until you determine which security group is providing that access. Or you can look at the security groups assigned to the user or the role assignments for the user.

## HOW DO I SET UP SECURITY FOR EXTERNAL APPLICATIONS THAT USE THE WORKDAY WEB SERVICES API?

For information on setting up security for the Workday Web Services API, see [Set Up Authorization Security for Workday Web Services](#).

## CUSTOM SECURITY REPORTS

You can also write **custom reports** using report data sources that allow you to report on security related objects. You can, for example, report on domains, security groups, policies and accounts. To see list of available data sources, run the Data Sources report for security related categories.

Data Sources <a href="#">...</a>					
9 items					
Data Source	Primary Business Object	Description	Built-in Prompts	Security Groups	Category
<a href="#">filter</a>	<a href="#">filter</a>	<a href="#">filter</a>	<a href="#">filter</a>	<a href="#">filter</a>	<a href="#">Security</a> <a href="#">Security Administration</a> <span style="border: 1px solid blue; padding: 2px;">a</span> <a href="#">Security Configuration</a> <span style="border: 1px solid blue; padding: 2px;">a</span> <a href="#">Security</a> <span style="border: 1px solid blue; padding: 2px;">a</span> <a href="#">Security Configuration</a>

All Domains Domain Returns one row for each instance of the Implementers [Security](#) [Security Administration](#) a [Security Configuration](#)

Check out a shared customer example of a reporting tool used to manage security configurations:

Search for: "Security Review Reporting" in the Workday Community

Link: <https://community.workday.com/node/96768>



The screenshot shows a Workday Community page for a 'Shared Solution' titled 'Security Review Reporting'. The page includes a navigation bar with links like Home, Getting Started, Releases, Collaborate, News, Calendar, Rising, and Developers. Below the navigation is a breadcrumb trail: Home > Collaborate > Solution Catalog. There are tabs for View, Outline, and Revisions, with 'View' being the active tab. The main content area displays the solution details, including its title, posted by 'jstevens2' from Nissan North America, Inc., on Sep 24, 2014, and updated on Oct 31, 2014. It has 689 reads and is categorized under Configurable Security, Cross Application Services, Custom Report Definition, and Reporting and Analytics. The average rating is 4.9 stars from 11 votes. The solution content discusses the development of custom reports for security configuration review and includes an attached ZIP file containing report definitions and an Excel template. The ZIP file is named 'Security Review Reporting.zip' and is 1 MB in size.

Included are the report definitions, excel template and steps. This solution was shared at Rising 2014.  
See presentation and video for more background:

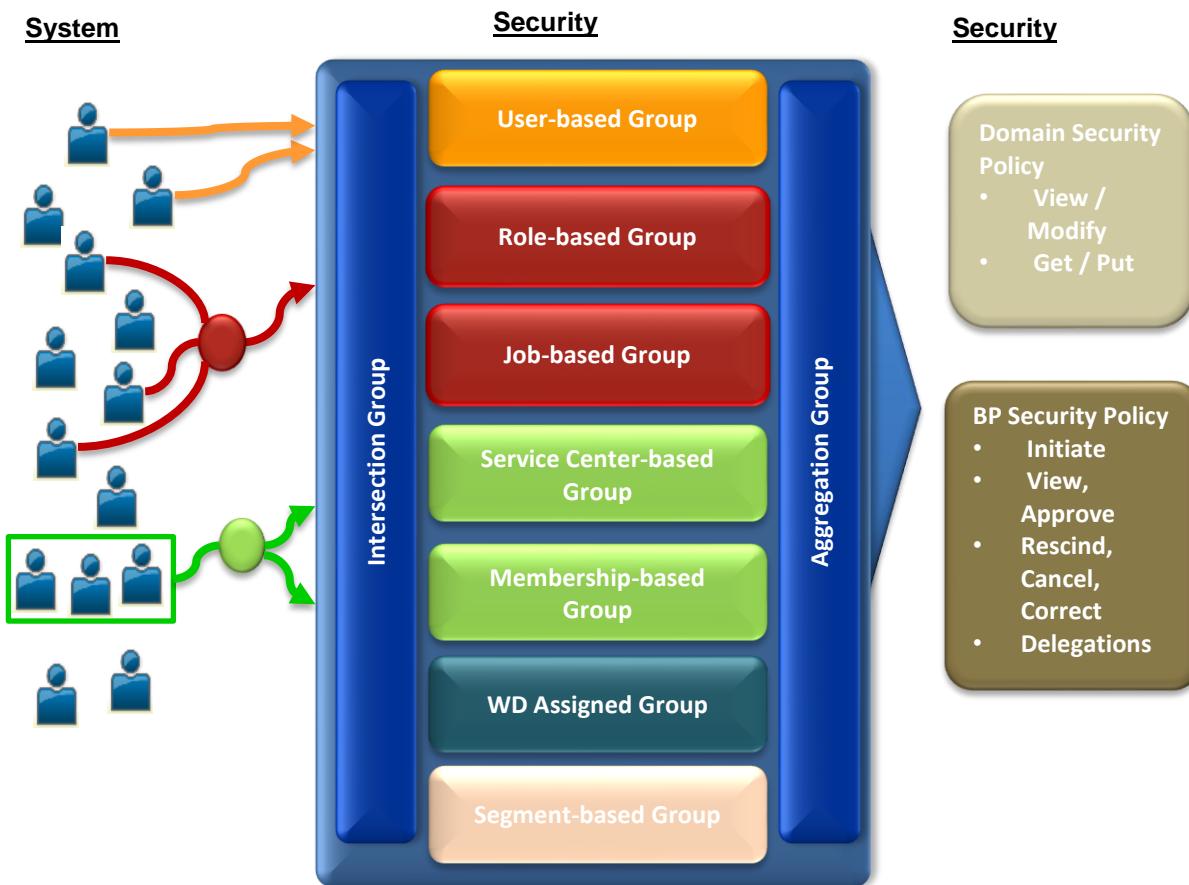
<https://community.workday.com/event/rising2014/95166>

Other helpful tips and reports:

- Audit account activity: <https://community.workday.com/node/95570>
- Audit group/role changes: <https://community.workday.com/node/60388>
- Compare security group permissions between accounts  
<https://community.workday.com/node/81569>
- Compare security groups' permissions <https://community.workday.com/node/81498>

## REVIEW

Workday's security framework allows you to configure which users have access to the delivered content via security policy configurations. **Security groups are the bridge between system users and security policies.** You can configure security groups in needed domain or business process security policies to grant access to security group members to delivered areas of Workday.



17

## WHERE TO GO FROM HERE

Be sure to visit the Community **Product Dashboard on Configurable Security** for more information around:

- Documentation
- Shared Solutions – Solution Catalog
- Posts & Ideas
- Presentations
- Training

The screenshot shows the Workday Product Dashboard for 'Configurable Security'. The top navigation bar includes links for Home, Getting Started, Releases, Collaborate, News, Calendar, Rising, and Developers. The main content area has three columns: 'Configurable Security' (with a 'workday' logo and a post about 'UXT4101: Deep Dive Into Configurable Security'), 'Deep Dive Into Configurable Security' (with a description and a 'Join us to review practical applications of configurable security' button), and 'Recent Brainstorm Ideas' (listing items like 'Ability to Mass "Remove Roles"', 'Breakout Domains by Worker Type', and 'Preparing for Business Process Discovery'). On the left, there's a 'References' section with links to 'Set up the Workday application for OIDC in Google Developers Console' and 'Set up Workday as an application in Google Developer Console so that you can:'. The bottom left corner of the dashboard features a 'Training' section with links to 'Business Process Event: Understanding the Full Process Record (Free)', 'Business Process Overview (Free)', and 'Preparing for Business Process Discovery'.

Be sure to check out shared solutions, reports and tools, as well as presentations that can serve as great refreshers and supplements.

## APPENDIX



## WALKTHROUGH SOLUTION – ONE ROLE, MULTIPLE ROLE-BASED SECURITY GROUPS

### One Role, Multiple Role-based Security Groups

Role	Security Group	Constraint	Members of Security Group	Domain or BP Sec Policy Access	Resulting access
HR Partner	HR Partner1	COO	Jack, Jane, Jill Joe	Initiate Hire Joe hire into F	Jack hire into C Jane hire into G hire into B
HR Partner	HR Partner2	COUS	Jack, Jane, Jill Joe	Worker Data: Personal Data Joe F, H, I	Jack C, F, H, I Jane G Jill B, D, E
HR Partner	HR Partner3	COAS	Jack, Jane, Jill Joe	Initiate Request Comp Change Joe F, H, I	Jack C, F, G, H, I Jane G Jill B, D, E
HR Partner	HR Partner4	Unconstrained	Jack, Jane, Jill Joe	Worker Data: Emergency Contacts Joe Everyone	Everyone



CONFIDENTIAL

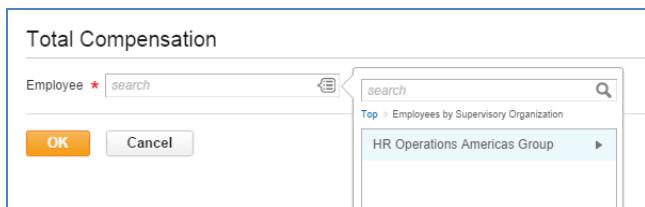


## WORKSHOP 1 –ROLE-BASED CONSTRAINED SECURITY GROUPS

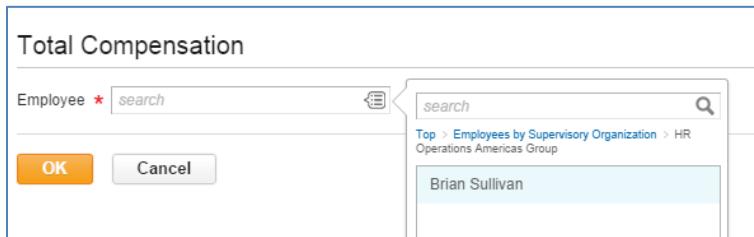
Scenario: Assign Yolanda Torres to the Compensation Partner role for Supervisory Organization: Field Sales North America. Assign Brian Sullivan to the Compensation Partner by Location role for the Location Hierarchy USA-Northeast, USA-Southeast, Canada – Eastern. See how their access can be configured and constrained to different organization types.

### TASK 1: VERIFY EXISTING SECURITY

1. **Start proxy** as Yolanda Torres
2. Run the *Total Compensation* report
3. See how she only has access to her own supervisory organization and within that organization, only to her own data



4. **Start proxy** as Brian Sullivan
5. Run the *Total Compensation* report
6. See how Brian similarly, only has access to his own supervisory organization and his own data only.



7. **Stop Proxy**

## TASK 2 – ASSIGN ROLES

1. **As Logan (lmcneil),** from the search box, let's look at a supervisory organization

- a. Run *org: Field Sales North America Group*

Categories	Search Results
Common	1 items
Assets	All of Workday
Banking	
	<b>Field Sales - North America Group</b> Supervisory Organization

2. Click on the supervisory organization to see the members.

Worker	Position	Phone	Email	Instant Messenger	Location
Brandon Harris	Regional Sales Manager	+1 (404) 772-5323 (Landline)	bharris@workday.net	bharris	Atlanta
Cheryl Edwards	Regional Sales Manager	+1 (617) 344-5221 (Landline)	cedwards@workday.net	cedwards	Boston

3. Let's assign Yolanda Torres' position as the Compensation Partner for this supervisory organization, where she will support and be constrained to these 12 target members.
4. Using related actions off the organization, select **Roles > Assign Roles**

**Assign Roles**

- Assign Self-Assign Roles
- Assign Unassigned Self-Assign Roles
- View Role Assignment History
- View Roles
- Security History
- View Worker Roles Audit

5. Click OK to accept the effective date of the role assignment.

- Add a row and assign Yolanda's position to the Compensation Partner role. Note how the role assignment is not to the worker or person, but to a position.

- Click OK to save.

**Yolanda is now in the role and thus a member of any role-based security groups that use the Compensation Partner role.**

- Now let's assign a role to Brian's position. From the search box, search **worker: Brian Sullivan**
- Using related actions, select **Security Profile > Assign Roles**

- Click OK to accept the effective date of the role assignment.
- Add a row and enter as follows:

<b>Field Name</b>	<b>Entry Value</b>
Role Enabled for	USA – Southeast US <i>(be sure to pick the location hierarchy instance, not region)</i>
Role	Compensation Partner by Location
Assigned to	Brian Sullivan, Staff HR Representative

12. Add a second row and enter:

<b>Field Name</b>	<b>Entry Value</b>
Role Enabled for	USA – Northeast US <i>(be sure to pick the location hierarchy instance, not region)</i>
Role	Compensation Partner by Location
Assigned to	Brian Sullivan, Staff HR Representative

13. Add a third row and enter:

<b>Field Name</b>	<b>Entry Value</b>
Role Enabled for	CAN – Eastern Canada <i>(be sure to pick the location hierarchy instance, not region)</i>
Role	Compensation Partner by Location
Assigned to	Brian Sullivan, Staff HR Representative

Assign Organization Roles Staff HR Representative - Brian Sullivan [...](#) [e](#)

Effective Date 10/22/2014

3 items

<a href="#">+</a>	*Role Enabled For	*Role	Assigned To
<a href="#">-</a>	CAN - Eastern Canada	Compensation Partner (by Location)	Brian Sullivan - Staff HR Representative
<a href="#">-</a>	USA - Southeast US	Compensation Partner (by Location)	Brian Sullivan - Staff HR Representative
<a href="#">-</a>	USA - Northeast US <a href="#">...</a>	Compensation Partner (by Location) <a href="#">...</a>	<input type="text" value="search"/> <a href="#">...</a> <input checked="" type="checkbox"/> Brian Sullivan - Staff HR Representative

14. Click **Submit** when done.

**Brian is now in the role and thus a member of any role-based security groups that use the Compensation Partner by Location role. He now supports and can be constrained to those in the selected location hierarchies.**

### TASK 3 – VERIFY THE ROLE-BASED SECURITY GROUPS AND ACCESS TO POLICIES

- From the search box, run **View Security Group**
- Select the role-based constrained security group: *Compensation Partner*
- See how this security group is constrained (Access Rights to Organization) and has access to the Domain: Worker Data Total Compensation

View Role-Based Security Group (Constrained) **Compensation Partner** [...](#) [e](#)

Name Compensation Partner

Comment Perform compensation management tasks for assigned organizations. Examples include approving worker compensation plans, packages, and salary ranges. Approval authority for compensation and staffing business processes.

Context Type Constrained by Role Access

Group Criteria	Access Rights to Organizations	Access Rights to Multiple Job Workers
Assignable Role <a href="#">Compensation Partner</a>	<input type="radio"/> Applies to Current Organization Only <input checked="" type="radio"/> Applies To Current Organization And Unassigned Subordinates <input type="radio"/> Applies to Current Organization And All Subordinates	<input checked="" type="radio"/> Role has access to the positions they support

Domain Security Policy Permissions	Business Process Security Policy Permissions	Other Usages												
Domain Security Policy Permissions	Business Process Security Policy Permissions	Other Usages												
<table border="1"> <thead> <tr> <th>Operation</th> <th>Domain Security Policy</th> <th>Domain Security Policies Inheriting Permission</th> <th>Functional Areas</th> </tr> </thead> <tbody> <tr> <td><a href="#">filter</a></td> <td><input checked="" type="checkbox"/> Worker Data: Total Compensation</td> <td><a href="#">filter</a></td> <td><a href="#">filter</a></td> </tr> <tr> <td>View Only</td> <td>Worker Data: Total Compensation</td> <td></td> <td>Core Compensation</td> </tr> </tbody> </table>	Operation	Domain Security Policy	Domain Security Policies Inheriting Permission	Functional Areas	<a href="#">filter</a>	<input checked="" type="checkbox"/> Worker Data: Total Compensation	<a href="#">filter</a>	<a href="#">filter</a>	View Only	Worker Data: Total Compensation		Core Compensation	Business Process Security Policy Permissions	Other Usages
Operation	Domain Security Policy	Domain Security Policies Inheriting Permission	Functional Areas											
<a href="#">filter</a>	<input checked="" type="checkbox"/> Worker Data: Total Compensation	<a href="#">filter</a>	<a href="#">filter</a>											
View Only	Worker Data: Total Compensation		Core Compensation											

- Rerun the **View Security Group** report. This time select the security group: *Compensation Partner (by Location)*.
- See how this security group is constrained (Access Rights to Organizations) but does NOT have access to the domain: Worker Data Total Compensation.

## Configurable Security Fundamentals 24

**Group Criteria**

Name: Compensation Partner (by Location)  
Comment: Compensation Partner (by Location)  
Context Type: Constrained by Role Access

**Access Rights to Organizations**

- Applies to Current Organization Only
- Applies To Current Organization And Unassigned Subordinates
- Applies to Current Organization And All Subordinates

**Access Rights to Multiple Job Workers**

- Role has access to the positions they support

**Domain Security Policy Permissions**

Domain Security Policy Permissions 4 items			
Operation	Domain Security Policy	Domain Security Policies Inheriting Permission	Functional Areas
View and Modify	Worker Data: Propose Stock Award as Part of Merit		Advanced Compensation
View Only	Worker Data: Onboarding		Onboarding
View Only	Staffing Actions: Primary Job		Staffing
View Only	Staffing Actions: Move Manager's Team		Staffing

6. Let's configure access to this domain.
7. From the search box, run *domain: Worker Data Total Compensation*
8. Using related actions, select **Domain > Edit Security Policy Permissions**

**Categories**

- Common
- Assets
- Banking
- Expense

**Search Results** 1 items

All of Workday

Worker Data: Total Compensation ... Domain

**Available Actions**

- Edit Security Policy Permissions
- View Security Policy

9. Add the *Compensation Partner (by Location)* Security Group

**Securable Actions** 2  
**Securable Reporting Items** 8

**Report/Task Permissions**

**\*Security Groups**

Search: Compensation Partner (by Location), Benefits Administrator

**Alerts: 1**

Activate your security policy changes using the Activate Pending Security Policy Changes task, and update the security evaluation moment, which is currently set to 10/21/2014 19:08:02.073.

10. Click OK to save
11. From the search box, run **Activate Pending Security Policy Changes**

The screenshot shows the Workday search interface. At the top, there is a search bar containing the text "Activ pend sec pol changes". To the right of the search bar is the Workday logo. Below the search bar, there are two columns: "Categories" and "Search Results". The "Categories" column contains "Common" and "Assets". The "Search Results" column shows "1 items" and a link "Tasks and Reports" under the heading "Activate Pending Security Policy Changes".

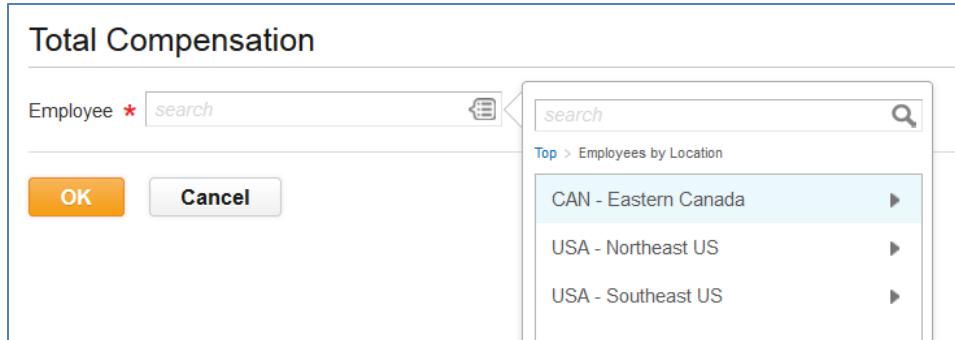
12. Capture comments: *Allow Comp Partner By Location Access to domain: Worker Data Total Compensation*
13. Click OK
14. Confirm by selecting the checkbox and click OK.
15. Now, Brian and Yolanda should have access to the Total Compensation report with their new role-based access.

### TASK 3 – TEST

1. **Start proxy** as Yolanda Torres
2. Run the *Total Compensation* report
3. See how Yolanda can now access the target instances in the Field Sales North America Group (the organization she supports in the Comp Partner role), along with her own data too.

The screenshot shows the "Total Compensation" report search interface. On the left, there is a search field labeled "Employee \* search" with an orange "OK" button and a grey "Cancel" button. On the right, there is a detailed search interface with a "search" field and a navigation breadcrumb: "Top > Employees by Supervisory Organization > Field Sales - North America Group". Below the breadcrumb, there is a list of employees: Brandon Harris and Cheryl Edwards. A vertical scrollbar is visible on the right side of the list.

4. **Start proxy** as Brian Sullivan
5. Run the *Total Compensation* report
6. See how Brian can now access target instances for locations in USA Northeast, Southeast and Eastern Canada.



## 7. Stop proxy

### CONCLUSION

- Role-based security groups allow you to identify users by role-assignment on their positions.
- Role-based security groups can be configured with constraints, where members are constrained to secured items or target instances in organizations for which their position is in that role.
- By configuring a role-based constrained security group to, for example, a domain security policy, you are allowing all members (all those in the role) to 'get there', i.e. get to items in that domain, however 'once there' you can then constrain their target context "for whom" they see data to the organizations that they are supporting in that role.

(End of Activity)



## WORKSHOP 2 –ROLE-BASED UNCONSTRAINED SECURITY GROUP

**Scenario:** Those in the Manager role cannot currently view emergency contacts. Create an unconstrained role-based security group for the Manager role and give it access to domain: worker data emergency contacts, allowing any user in the manager role to view emergency contacts for anyone in the tenant (unconstrained)

### TASK 1: VERIFY EXISTING SECURITY

1. **Start Proxy** as Maria Cardoza
2. See what emergency contacts tasks Maria has access to. From the search box, run *emergency contacts*
  - a. See how Maria can only access self-service emergency contact items. She cannot view emergency contacts for other workers

3. **Stop Proxy**
4. As Logan, let's first determine how the 'View emergency contacts for worker' item is secured.
  - a. From the search box, run **View Security for Securable Item**
  - b. Select item: *View Emergency Contacts for Worker*

5. Click OK

## Configurable Security Fundamentals 24

6. See how this item is secured in the **domain: Worker Data Emergency Contacts**. See the permitted security groups. Maria does not have any of these permitted security groups on her profile.

Domain Security		Language Restrictions	
Domain Security			
Security Policy	Domain	Functional Areas	Permitted Security Groups
Worker Data: Emergency Contacts	Q	Contact Information	GMS Service Center HR Administrator HR Analyst HR Auditor HR Executive HR Partner HR Partner (By Location) Implementers

7. From the search box, run *worker: Maria Cardoza*

- a. Using related actions, select **Security Profile > View Role Assignments**

The screenshot shows the Workday search interface. A search bar at the top contains the query "worker: Maria Cardoza". Below the search bar, the results are displayed under "Search Results" with 1 item found. The result is "Maria Cardoza" (Director, Employee Benefits Employee). To the right of the search results, a context menu is open, listing various actions such as "View Workday Account", "Assign Roles", and "View Role Assignments". The "View Role Assignments" option is highlighted with a blue background.

8. See how she is assigned several roles. She is the manager of the benefits department

Role Assignments for Worker Maria Cardoza			
Assignable Role	Organizations with Role Filled by Worker		
	Role Enabled	Role From	Inactive
Manager			
Manager	Benefits Department	Assigned	

9. We will now give all those in the manager role access to view emergency contacts for workers, even if the workers are not in their managed department, i.e. unconstrained access using a role-based unconstrained security group type.

## TASK 2 – VIEW EXISTING ROLE-BASED UNCONSTRAINED SECURITY GROUP

1. Still logged in as Logan, from the search box, run the task: **View Security Group**
2. From the prompt, select *Security Groups > Role-based Unconstrained > Manager (Unconstrained)*
  - a. See how the security group just references the '**Assignable Role**: Manager'
    - i. Anyone assigned in the manager role will be a member of this security group.
    - b. See how there are no organization access rights configured. This is an **unconstrained** security group.
    - c. This security group currently has unconstrained access to 13 domains in the tenant.
    - d. We will next add this security group to the domain: Worker Data Emergency Contacts.

Operation	Domain Security Policy	Domain Security Policies Inheriting Permission	Functional Areas
View and Modify	Custom Report Creation		System
View and Modify	Report Definition Sharing - Specific Users		System

3. Click OK

## TASK 3- GIVE THE MANAGER UNCONSTRAINED ROLE BASED SECURITY GROUP ACCESS TO VIEW EMERGENCY CONTACTS FOR WORKERS

1. From the search box, run: *domain: worker data emergency contacts*
  - a. Using related actions, select **Domain > Edit Security Policy Permissions**

## Configurable Security Fundamentals 24

2. Add the 'Manager (Unconstrained)' security group to the view only permissions set of security groups (not Modify permissions).

The screenshot shows the 'Report/Task Permissions' dialog box with 2 items. On the left, there is a tree view with nodes like 'HR Administrator', 'HR Partner', 'HR Partner (By Location)', and 'Implementers'. On the right, there is a list of security groups. A search bar at the top contains the text 'Manager (Unconstrained)'. Below the search bar, the 'Manager (Unconstrained)' group is selected, indicated by a checked checkbox in the 'Permissions' column. A tooltip above the list area says: 'Activate your security policy changes using the Activate Pending Security Policy Changes task, and update the security evaluation moment, which is currently set to 10/22/2014 15:13:14 560.' An orange box highlights the search bar and the selected 'Manager (Unconstrained)' group.

3. Click OK to save. Remember that edits to security policies are saved and pending until you activate.
4. From the search box, run the task: **Activate pending security policy changes**
5. Enter a comment: *Allow Manager Unconstrained security group access to view Domain: Worker Data Emergency Contacts*
6. Click OK
7. Confirm change and click OK.

## TASK 4 - TEST

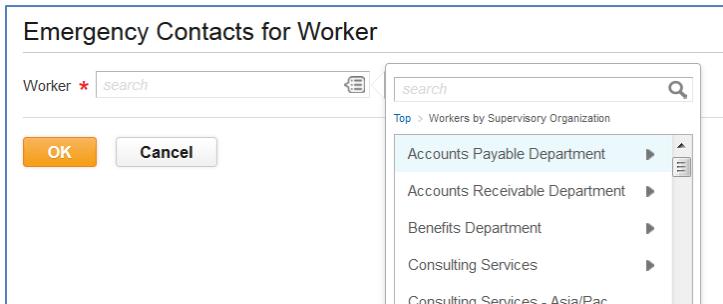
1. **Start Proxy** as Maria Cardoza
2. From the search box, run *emergency contact*
  - a. *See how now Maria has access to view emergency contacts for workers, not just her own.*

The screenshot shows the Workday search interface. The search bar at the top contains the text 'emergency contact'. The search results are displayed in a grid format. On the left, there is a sidebar with categories: Common, Assets, Expenses, Integrations, Organizations, Payroll, People, and Processes. The 'Common' category is selected. The search results show 5 items:

- Tasks and Reports**
  - Most Recent Completed Emergency Contact Business Process for Workers**
  - My Emergency Contacts**  
View your emergency contacts, including the name, relationship, contact priority, preferred language, and address of each contact person. Enables you to confirm and maintain your emergency contact information.
  - Emergency Contacts for Worker**  
View a worker's emergency contacts, including the contact person's name, relationship, contact priority, preferred language, and email address. Enables you to confirm, edit, add, or delete emergency contacts ..
  - Add Emergency Contact**
  - Change My Emergency Contacts**

3. Run the **Emergency Contacts for Worker** report

- a. See how Maria can run this for ANY worker in any supervisory organization. Her access 'once here' is unconstrained.



#### 4. Stop proxy

### CONCLUSION

- Role-based unconstrained security groups can be effective and easy ways to identify those in a given role to then grant them unconstrained access.
- There may be areas of Workday that require unconstrained security groups, so if you are looking to grant access to such areas for those in a given role, a role-based unconstrained security group could be easier to maintain than manually assigning user-based security groups.
- Examples, can include:
  - a. All those in a manager role can create custom reports
  - b. All those in an HR Partner role can proxy on behalf of All Employees

(End of Activity)



## WORKSHOP 3 – CONSTRAIN ROLE-BASED ACCESS TO BOTH THE SUPERVISORY AND LOCATION HIERARCHY

Brian Sullivan is currently the Compensation partner by Location for USA-Northeast, USA-Southeast and Canada Eastern. Let's intersect his access to only be for those in the *Field Sales North America Group supervisory organization that are in those locations*.

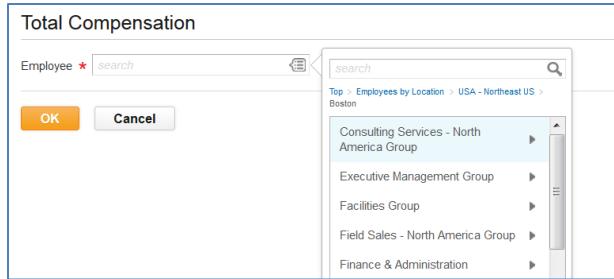
**\*\*\* THIS WORKSHOP ASSUMES WORKSHOP 1 HAS BEEN COMPLETED \*\*\***

### TASK 1: CURRENT ACCESS

1. Let's check Brian Sullivan's role-assignments and security groups.
2. From the search box, run *worker: Brian Sullivan*
  - a. Using related actions, select **Security Profile > View Role Assignments**

Role Assignments for Worker <a href="#">Brian Sullivan</a> <span style="float: right;">...</span>			
Assignable Role	Organizations with Role Filled by Worker		
	Role Enabled	Role From	Inactive
Compensation Partner (by Location)	CAN - Eastern Canada	Assigned	
	USA - Northeast US	Assigned	
	USA - Southeast US	Assigned	

3. See how Brian's position is assigned to the role: Compensation Partner (by location).
  - a. Given the role assignment, Brian is therefore a member of the Compensation Partner (by Location) security group that uses this role.
4. As we saw in an earlier activity, this security group has access to the domain: Worker Data: Total Compensation
  - a. Brian can run the *Total Compensation* report for any worker (target instance) in these locations, across supervisory organizations.



5. We will now limit his access to only those workers in the **supervisory organization: Field Sales North America Group that are in the locations that he supports.**

Worker	Supervisory Organization	Location	Location Hierarchy
Brandon Harris	Field Sales - North America Group	Atlanta	USA - Southeast US
Cheryl Edwards	Field Sales - North America Group	Boston	Storage North America
Donna Owens	Field Sales - North America Group	Dallas	USA - Northeast US Storage North America
Isabelle Blanc	Field Sales - North America Group	Montreal	USA - Southeast US CAN - Eastern Canada
Jennifer Carter	Field Sales - North America Group	Chicago	USA - Central US
Juan Delgado	Field Sales - North America Group	New York	USA - Northeast US
Madeline Fleming	Field Sales - North America Group	San Francisco	USA - Western US
Melanie Watson	Field Sales - North America Group	New York	USA - Northeast US
Neal Jackson	Field Sales - North America Group	Chicago	USA - Central US
Rodrigo Sanchez	Field Sales - North America Group	San Francisco	USA - Western US
Ryan Taylor	Field Sales - North America Group	Vancouver	CAN - Western Canada
Tyler Ross	Field Sales - North America Group	Chicago	USA - Central US

## TASK 2 – ASSIGN BRIAN AS THE COMPENSATION PARTNER FOR THE SUPERVISORY ORGANIZATION: FIELD SALES NORTH AMERICA GROUP

1. **As Logan**, from the search box, run *worker: Brian Sullivan*

- a. Using related actions, select **Security Profile > Assign Roles**

2. Click ok to accept the effective date of the role assignment
3. Add a role,
  - a. \*Role Enabled for: *Field Sales North America Group* (this is a supervisory organization)
  - b. \*Role *Compensation Partner*.
  - c. Assigned to: Keep Yolanda's position in the role, and add Brian Sullivan's position.

	*Role Enabled For	*Role	Assigned To	Default Worker
	<input type="text" value="Field Sales - North America Group"/>	<input type="text" value="Compensation Partner"/>	<input type="text" value="search"/> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Brian Sullivan - Staff HR Representative</li> <li><input checked="" type="checkbox"/> Yolanda Torres - Staff HR Representative</li> </ul>	Logan McNeil

4. Click **Submit**
5. Brian is now also a member of the Compensation partner security group (like Yolanda).
6. Let's now intersect the access.

### TASK 3: INTERSECT THE COMPENSATION PARTNER AND COMPENSATION PARTNER BY LOCATION SECURITY GROUPS TO INTERSECT THE MEMBERS AND CONSTRAINTS

1. From the search box, run the task: **Create Security Group**
  - a. **Type:** Intersection
  - b. **Name:** Compensation Partner Sup and Loc Intersected

- c. Click **OK**
- d. For the Intersection Criteria, include the two security groups:
  - i. Compensation partner
  - ii. Compensation partner by location

**Edit Intersection Security Group Compensation partner sup and loc intersected**

Name	<input type="text" value="Compensation partner sup and loc intersected"/>
Comment	<input type="text"/>
Context Type	Mixed (Subset)
Inactive	<input type="checkbox"/>
<b>Intersection Criteria</b>	
Security Groups to Include	<input type="text" value="search"/> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Compensation Partner (by Location)</li> <li><input checked="" type="checkbox"/> Compensation Partner</li> </ul>
Security Group to Exclude	<input type="text" value="search"/>
<b>Exclusion Criteria (Constrained Context)</b>	
Exclude Target Position in Organization	<input type="text" value="search"/> <ul style="list-style-type: none"> <li><input type="radio"/> Applies to Current Organization Only</li> <li><input type="radio"/> Applies to Current Organization And All Subordinates</li> <li><input checked="" type="radio"/> None of the above</li> </ul>
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

- e. Click OK to save.
- 2. Now, let's replace the security group access for the **domain: worker data total compensation**
- 3. From the search box, search **domain: Worker data total compensation**
  - a. Using related actions, select **Domain > Edit Security Policy Permissions**
  - b. **Remove** the *Compensation partner* security group
  - c. **Remove** the *Compensation partner by location* security group
  - d. Add the new intersection security group: *Compensation Partner sup and loc intersected*

**Report/Task Permissions**

<input type="button" value="-"/>	<input type="text" value="search"/> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Compensation partner sup and loc intersected</li> <li><input checked="" type="checkbox"/> Benefits Administrator</li> <li><input checked="" type="checkbox"/> Benefits Partner</li> <li><input checked="" type="checkbox"/> Chief Executive Officer</li> <li><input checked="" type="checkbox"/> Chief Financial Officer</li> <li><input checked="" type="checkbox"/> Chief Operating Officer</li> <li><input checked="" type="checkbox"/> Compensation Administrator</li> <li><input checked="" type="checkbox"/> HR Administrator</li> </ul>
----------------------------------	---

- e. Click ok to save
- 4. From the search box run the task: **Activate Pending Security Policy Changes**

5. Add comment – *limit comp partner access to locations AND sup orgs that they support.*

6. Click OK

7. Confirm and Click OK

#### TASK 4 - TEST

1. **Start proxy** as Brian Sullivan

2. Run the *Total Compensation* report

3. See how now Brian only has access to target instances in the Fields Sales North America organization who are in locations that he supports.

**Total Compensation**

Employee \*

search

Top > Employees by Supervisory Organization > Field Sales - North America Group

Brandon Harris
Cheryl Edwards
Donna Owens
Isabelle Blanc
Juan Delgado
Melanie Watson

Worker	Supervisory Organization	Location	Location Hierarchy
Brandon Harris	Field Sales - North America Group	Atlanta	USA - Southeast US
Cheryl Edwards	Field Sales - North America Group	Boston	Storage North America
Donna Owens	Field Sales - North America Group	Dallas	USA - Northeast US Storage North America
Isabelle Blanc	Field Sales - North America Group	Montreal	USA - Southeast US CAN - Eastern Canada
Jennifer Carter	Field Sales - North America Group	Chicago	USA - Central US
Juan Delgado	Field Sales - North America Group	New York	USA - Northeast US
Madeline Fleming	Field Sales - North America Group	San Francisco	USA - Western US
Melanie Watson	Field Sales - North America Group	New York	USA - Northeast US
Neal Jackson	Field Sales - North America Group	Chicago	USA - Central US
Rodrigo Sanchez	Field Sales - North America Group	San Francisco	USA - Western US
Ryan Taylor	Field Sales - North America Group	Vancouver	CAN - Western Canada
Tyler Ross	Field Sales - North America Group	Chicago	USA - Central US

#### 4. Stop proxy

**Important:** In this activity we only changed one domain to demonstrate the intersection security. It will be imperative to **review and replace all existing references** to compensation partner security group, or compensation partner by location security group, and to replace as needed with the intersection security group.

#### CONCLUSION

Intersection security groups can help enforce constraints where targets need to be intersected between different organization types (e.g. sup organization and location hierarchy, cost center and supervisory organization)

(End of Activity)

## REVIEW QUESTIONS & ANSWERS

What report shows a top down view of how the Workday application is delivered?

- **Functional Areas**

Can you change what items are in what domains?

- **No**

What are the 2 types of security policies?

- **Domain Security Policies**
- **Business Process Security Policies**

What is the purpose of the 2 tasks associated with change control?

- **Activate Pending Security Policy Changes**
  - To make saved security changes effective
- **Activate Previous Time Stamp**
  - To revert to the last known good version of your security configuration

When a security group is constrained or context sensitive, what will members be constrained to?

- **Organization(s)**
- **Segment(s)**
- **Level(s)**

True or False: When editing a security policy, users are added to policies to grant permissions.

- **False – security groups are added to security policies to grant permissions.**

If a domain has 100 items, you can grant access to 50 of the 100

- **False – access is at the domain level, to all items in the domain.**

What are characteristics of User- Based Security Groups?

- **Manually assigned to a user**
- **Follows the user**
- **Unconstrained access**

What are some characteristics of a role-based security group?

- **References a role**
- **Membership based on role assignment**
- **Roles are assigned to positions**
- **Members can be constrained to organizations they support in role**
- **Workday delivers starting roles and role-based security groups**

When would you use a service center based security group?

- **When you need to configure access in Workday for third party users (not workers)**

(Yes or No) Can you grant access to only one item in a domain? (E.g. if a domain contains 12 secured items, can you grant access to only one of the items and not the other 11 items?)

- **No – security is granted at a domain level, i.e. to all secured items in that domain.**

(Yes or No) Can you change what items are in what domains?

- **No – Workday delivered secured items in defined domains**

How can you find out what's delivered in terms of delivered areas/domains/business processes?

- **Functional Areas report**
- **Domain Security Policies for Functional Area**
- **Business Process Security Policies for Functional Area**

If you know the item you need to give access to, how do you know what security policy to update?

- Run **View Security for Securable Item** to determine the domain or BP the item is in

(Yes or No) Can you create new security groups beyond what's delivered?

- **Yes, you can configure new security groups**
  - **Create Security Group**

(Yes or No) Can you create new security group types beyond what's delivered?

- **No – Workday determines the different types of security groups you can configure**
  - e.g. role-based, job-based, etc.

In order to give a user access to a given item (e.g. a delivered report, task, data source), what do you have to do?

- **Identify the domain or business process security policy that secures the given item**
- **Identify user via a security group**
- **Modify corresponding security policy with security group**
- **Activate Pending Security Policy Changes**
- **Test**

How can you find out what a security group has access to?

- **View Security Group**
- **Action Summary for Security Group**
- **Security Analysis for Security Group**

How can you find out what a given user has access to?

- **Security Analysis for Workday Account**
- **View Security Groups for User**

When would you use a user-based security group?

- **Workday delivers many**
- **Tends to be for your Administrators**
- **Target access needs to unconstrained (system-wide/tenant wide)**
- **Assignment is manual/specific to a person/follows the person**

When would you use a role-based security group?

- **For your support or leadership staff**
- **Helps you identify members by role assignment on their position**
- **Allows you to constrain target access to organizations supported in role**
- **Workday delivers starting roles and role-based security groups**

True/False – you must manually assign and re-assign job-based security groups as workers terminate and change jobs?

- **False – Job based security group membership is automatically maintained as workers change jobs and terminate.**

What are some example criteria that you can use in a job based security group to identify members?

- **Job Profile**
- **Job Category**
- **Job Family**

- **Management Level**
- **Work Shift**
- **Include Exempt Jobs**
- **Include Non Exempt Jobs**

True/False – You can segment any area of Workday

- **False – Workday determines what areas can be segmented.**
  - Compensation Setup
  - Compensation Plan Assignments
  - Expense Items
  - Pay Components
  - Integrations
  - Etc.

True/False – You must manually assign location and organization membership security groups to workers.

- **False - Workers are automatically members of Location or Organization Membership Security Groups if they are in Locations or Organizations included in the security group**

True/False - If you configure a location or organization membership security group in a domain or bp security policy, resulting access will be constrained to the location or organization specified

- **False – location and organization membership security groups are unconstrained.  
Workday does not make any attempt to match the context or constraint.**
- **The location and organization specified are only the criteria for identifying members.**

When would you consider an intersection security group?

- **Limiting self-service to a given population**
- **Need to constrain target access by different organization types**
- **Need to exclude target instances from context the user would have otherwise seen**

True/False – Intersection security groups perform similarly to any other security group type (e.g. user-based, role-based) and can be used in any area of Workday.

- **False – Intersection security groups are more complex and can impact performance.**
- **Intersection security groups have limitations.**
- **Intersection security groups should be used sparingly and should be carefully tested.**

What must be done before you can use Level-Based security groups?

- **A Leveling mechanism (hierarchy) must be set up**

NOTES: